Avaya DECT R4

Installation and Administration Manual

Software version 7.2.x
21-603363
Issue 8

© 2013-2016 Avaya Inc. All Rights Reserved.

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

"Documentation" means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya may generally make available to users of its products and Hosted Services. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website:

https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 under the link "Warranty & Product Lifecycle" or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

"**Hosted Service**" means a hosted service subscription that You acquire from either Avaya or an authorized Avaya Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Avaya or Avaya Channel Partner (as applicable) for more information.

Hosted Service

THE FOLLOWING APPLIES IF YOU PURCHASE A HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO UNDER THE LINK "Avaya Terms of Use for Hosted Services" OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE. YOUR USE OF THE HOSTED SERVICE SHALL BE LIMITED BY THE NUMBER AND TYPE OF LICENSES PURCHASED UNDER YOUR CONTRACT FOR THE HOSTED SERVICE, PROVIDED, HOWEVER, THAT FOR CERTAIN HOSTED SERVICES IF APPLICABLE, YOU MAY HAVE THE OPPORTUNITY TO USE FLEX LICENSES, WHICH WILL BE INVOICED ACCORDING TO ACTUAL USAGE ABOVE THE CONTRACT LICENSE LEVEL. CONTACT AVAYA OR AVAYA'S CHANNEL PARTNER FOR MORE INFORMATION ABOUT THE LICENSES FOR THE APPLICABLE HOSTED SERVICE, THE AVAILABILITY OF ANY FLEX LICENSES (IF APPLICABLE), PRICING AND BILLING INFORMATION, AND OTHER IMPORTANT INFORMATION REGARDING THE HOSTED SERVICE.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLEON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO, UNDER THE LINK "AVAYA SOFTWARE LICENSE TERMS (Avaya Products)" OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. " Software" means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be accessed by multiple users. "Instance" means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine ("VM") or similar deployment.

License type(s)

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, and the product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Third party components

"Third Party Components" mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya's website at:

https://support.avaya.com/Copyright or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components, to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

The following applies if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES

IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Service Provider

THE FOLLOWING APPLIES TO AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS MUST BE AUTHORIZED IN WRITING BY AVAYA AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE AVAYA CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE AVAYA CHANNEL PARTNER'S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, H.264 CODEC, OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE WWW.SIPRO.COM/CONTACT.HTML. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Compliance with Laws

Customer acknowledges and agrees that it is responsible for complying with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

Preventing Toll Fraud

"Toll Fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: https://support.avaya.com , or such successor site as designated by Avaya.

Security Vulnerabilities

Information about Avaya's security support policies can be found in the Security Policies and Support section of https://support.avaya.com/security

Suspected Avaya product security vulnerabilities are handled per the Avaya Product Security Support Flow (https://support.avaya.com/css/P8/documents/100161515).

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners.

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: https://support.avaya.com , or such successor site as designated by Avaya.

Contact Avaya Support

See the Avaya Support website: https://support.avaya.com for product or Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: https://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Avaya IP-DECT System Description 19
Introduction 19
System overview 20
Supported Standards 21
System functions 21
DECT functions 22
LAN/WAN 23
LDAP 23
Supported third-party functions 23
IP-DECT System 24
System layout 24
Device Management 30
Device Management in Multiple Site System 31
Synchronization 31
IP-DECT System Management 33
VoIP signalling protocols 35
H.323 35
IP-DECT planning and deploying 36
Avaya IP-DECT system components 36
DECT cordless handsets 36
IPBS 38
IPBL 38
RFP 38
IP-PBX 39
Communication Manager 39
Avaya In-Building Wireless Server (AIWS or AIWS2) 39
System capacity 40
Messaging capacity 41

Planning an IP-DECT system 43
Introduction 43
Wired LAN and backbone requirements 44
End-to-end QoS 44
Base station planning 44
Client requirements 46
Base station coverage 46
Architecture 46
Building elements 47
Metal halls 51

Determining the average cell size 53
Principles to perform a site survey: 53
Traffic capacity of the system. 55
Traffic capacity of the base stations 56
Trunk capacities 57
Location of the base stations 58
Air Synchronization 58
LAN access. 58
Power the base stations. 58
Antennas 58
Base station planning tips 59
Making a base station plan 60
Finalizing the plan 61

Installing and operating the IPBS and IPBL 63
Introduction 63
Description 64
IP-DECT Base Station 64
AC-adapter 67
Safety instructions. 72
Safety symbols. 73
Protection against electrostatic discharge (ESD) 73
Safety Aspects 74
Regulatory Compliance Statements - EU/EFTA only 74
Regulatory Compliance Statements (USA and Canada only). 75
IP security 76
IP security terminology 76
Introduction to IP Security in IP-DECT 77
IP-DECT administrative functions 79
Installing the Base Station 80
Base station cables 80
Installing the base station. 80
Turning on the base station. 87
Installing and operating the IP-DECT Gateway (IPBL) 88
Mounting the IP-DECT Gateway (IPBL). 89
Cable instructions for the IPBL 90
Powering the IPBL 92
Accessing the IPBL 93
Configuration 96

Requirements . . . 96
Accessing the GUI . . . 96
GUI Web Access . . . 100
Simplified GUI . . . 106
Configuring the Master . . . 107
Configuring the Standby Master . . . 109
Configuring the Slave/Radio . . . 110
Multibase Station Master configuration . . . 111
Adding users . . . 112
Logout/Login for users . . . 115
Operation . . . 115
General . . . 115
Provisioning . . . 138
LAN . . . 140
IP . . . 144
LDAP . . . 145
DECT . . . 148
UNITE . . . 169
Users . . . 171
Device overview . . . 174
Traffic . . . 180
Backing up . . . 182
Updating . . . 183
Diagnostics . . . 186
Reset . . . 190
Reset using the reset button . . . 191
Quit operation . . . 192
Commissioning . . . 192
Radio coverage verification tests . . . 193
Cordless extension number test . . . 194
Troubleshooting . . . 195
Using the Update Server . . . 195
Summary . . . 195

Configuring Avaya DECT phones . . . 203
Introduction . . . 203
Getting started . . . 203
PDM . . . 204
Configuration of phones on AIWS (Avaya In-Building Wireless Server) . . . 204
Installation of telephones . . . 205

Preparing PDM/AIWS for handling of 372x/374x . . . 205
Installation of a new telephone . . . 205
Configuring a telephone with a template . . . 208
Synchronizing a telephone with PDM/AIWS . . . 209
Maintenance . . . 210
Definitions . . . 210
Upgrading telephone software . . . 210
Performing a Factory reset . . . 210
Replacement procedure choice guide . . . 210
Easy Replacement . . . 211
Replacement of a telephone with the AIWS/AIWS2 . . . 213
Replacement of the telephone with the PDM . . . 215
Telephone configuration . . . 218
Voice mail . . . 218
Contacts . . . 218
Central phonebook . . . 219
Company phonebook . . . 219
Call services . . . 220
In Call Menu . . . 221
My Favorites . . . 223
Own In Call functions . . . 224
Replacing R Soft Key . . . 224
Own line settings . . . 225
Uploadable language . . . 225
Customizing the GUI . . . 226
Missed call indication . . . 226
Configuring telephone restrictions . . . 227
Actions when telephone is placed in charger . . . 228
Clearing lists when inserted in charger . . . 229
Disabling Homebase GAP registration . . . 230
Making encrypted Base Station mandatory . . . 230
Early Encryption . . . 230
Out of range beep . . . 231
Handset idle roaming . . . 231
Site survey tool . . . 232
Protect registration from user deletion . . . 232
Emergency call number . . . 232
Alarm ringing volume (Integral Systems) . . . 232
Common alarm settings . . . 233
Push button alarm . . . 233

Man-down alarm and No-Movement alarm . . . 234
Messaging settings . . . 235
Audio adjustment . . . 236
Headset configuration . . . 236
Owner identification in the idle display . . . 237
Profiles . . . 237
Importing contacts . . . 240
Shortcuts . . . 240
Administration . . . 242
Admin menu tree . . . 242
Quick access to the telephone information/SST menu . . . 244
LED indications . . . 245
Characters for SMS . . . 245
Troubleshooting . . . 246

Configuring Avaya Aura® Communication Manager . . . 247
General usage and important notes . . . 247
Communication Manager system administration . . . 249
SRTP Configuration . . . 264

Installing and operating the Advanced Charger . . . 269
Introduction . . . 269
Safety . . . 270
Technical solution . . . 270
Requirements . . . 271
Installation and configuration . . . 272
Advanced Charger installation . . . 272
Advanced Charger configuration . . . 273
Security . . . 274
Commissioning . . . 275
Maintenance . . . 276
Software update . . . 276
Operation . . . 277
Charger operation . . . 277
LED indications . . . 278
Troubleshooting . . . 279

Installing Multiple Battery Charger . . . 281
Introduction . . . 281

Safety . . . 282
Compliance . . . 283
Technical solution . . . 284
Installation and Configuration . . . 285
Multiple Battery Charger Installation . . . 285
Commissioning . . . 292
Operation . . . 293
Troubleshooting . . . 293

Installing and operating the Rackmount Charger . . . 295
Introduction . . . 295
Safety . . . 296
Compliance . . . 297
Technical Solution . . . 298
Requirements . . . 298
Installation and configuration . . . 299
Rackmount Charger installation . . . 299
Rackmount Charger configuration . . . 307
Commissioning . . . 309
Installation test . . . 309
Charging . . . 309
Communication with AIWS or PDM . . . 309
Operation . . . 310
Charger operation . . . 310
LED indications . . . 312
Maintenance . . . 313
Software upgrade . . . 313
Administration . . . 313
Data backup . . . 313
Troubleshooting . . . 313

Installing and operating the Portable Device Manager (WinPDM) . . . 315
Introduction . . . 315
How to use this chapter . . . 316
Technical solution . . . 316
Requirements . . . 317
WinPDM description . . . 318
WinPDM terminology . . . 318
PDM usage . . . 318

Installation and configuration 320
Software installation 320
Software configuration 320
Initial Configuration of Devices 321
Import Package Files 322
Create Template with Common Settings 322
Create Numbers and Apply Template 324
Connect Device to Computer 325
Associate Number with Device 326
Upgrade a Device with New Software 327
Operation 328
The WinPDM GUI 328
The Device Wizard 333
Open the WinPDM 334
Site Management 334
Numbers 336
Create New Numbers 336
Devices 341
Templates 344
File Management 347
Import and Export of Numbers and Templates 351
Administration 353
Data Backup 353
Uninstall the WinPDM 353
Troubleshooting 354
WinPDM Keyboard Shortcuts 357
General 357
Devices 357
Numbers 357
Templates 358
File Types 358

Installing and operating the AIWS and the AIWS2 359
Introduction 359
Licenses 361
Overview 362
How to use this chapter 362
Included in the delivery 364
Technical solution 364
Requirements 364

Installation and configuration. 365
Required information 365
Hardware installation and configuration 365
Software installation 366
Configuration and AIWS setup Wizard 366
Updating AIWS for Elise 2 Server (AIWS Hardware). 368
Updating Elise 3 Server (AIWS2 Hardware): 368
Multiple AIWS configuration 369
AIWS configuration for Multi Base Station Masters 375
Administration 377
Data backup 377
AIWS Overview. 378
Authentication Levels and Default Passwords 378
Functionality matrix 379
Setting passwords 379
Password policy 380
Web access security settings 380
Disabling the NetBIOS Service 381
Configuration Page 382
Advanced Configuration page 383
Icons 384
Certificates 384
Demonstration Mode 386
Operation 387
Messaging 387
Phonebook Administration 390
Phonebook editing. 390
Importing and exporting a phonebook 393
Device Management 395
Device Manager 397
Device Manager description 398
Logging on to the Device Manager 404
Closing the Device Manager 404
Templates in Device Manager. 405
Saving a device configuration as a template 407
Numbers 410
Devices 417
License restrictions for device handling 422
File management. 426
Importing/Exporting Numbers and Templates 437

Other settings 438
Closing the Device Manager 439
DECT Interface 440
Cordless telephone system 440
DECT Interface settings 441
Basic Configuration 443
Central Phonebook Configuration 443
Export activity logs to a Syslog server 454
Status 455
Backing up the configuration 460
Restoring the configuration 461
Device configuration 461
Additional System settings 465
Call Diversion 473
Absence Handling 474
Remote Management 474
Administration of language and user interface 477
Customizing the language 477
Customizing the user interface (GUI) 482
Password Protected Access to NetPage 492
Accessing NetPage from a Cordless Unit with WAP 492
Testing the new user interface 493
Updating the user interface after a new AIWS Release 493
Messaging 494
Messaging Tool configuration 494
NetPage configuration 494
Predefined groups 498
Creating messaging groups 499
Predefined messages 500
Message history status 502
Backing up and restoring NetPage files 502
Open Access Protocol (OAP) 504
Configuration 504
Software administration on the AIWS 505
Getting Started with the AIWS 505
Software administration on the AIWS2 507
Software information 507
Toggling with software 507
Installing new software 508

Creating a software backup . . . 508
Upgrading the boot software . . . 508
Getting started with AIWS2 . . . 509
Accessing the Product . . . 510
Access via a Network with a DHCP Server . . . 510
Access via the Management port . . . 510
Install the Port Driver on Windows XP/Vista . . . 511
Install the Port Driver on Windows 7 . . . 512
Configuration . . . 513
Setup via the Setup Wizard . . . 514
Setup from the Advanced Configuration Page . . . 514
Safety and Regulatory Instructions for Elise3 . . . 514
Device Manager Keyboard Shortcuts . . . 516
General . . . 517
Devices . . . 517
Numbers . . . 517
Templates . . . 517
Function Indicator and Error Relay Output . . . 519
For Elise 2 (AIWS Hardware) . . . 519
For Elise 3 (AIWS2 hardware) . . . 520
File types . . . 521

Installing Elise 2 Server (AIWS Hardware) . . . 523
Introduction . . . 523
FCC Compliance Statements for Class A Digital Device . . . 524
EU Compliance statements for Class A device . . . 524
Board description . . . 525
General information . . . 527
License . . . 527
Powering down and restarting the Elise 2 Server (AIWS Hardware) . . . 527
Operating Modes . . . 528
Selecting operating mode . . . 529
Function indicator . . . 530
Administration and authentication . . . 531
Installation . . . 532
Opening the housing . . . 533
Wiring runs . . . 533
Selection of A or B-bus . . . 534
Elise 2 Server (AIWS Hardware) controlling the communication on the A/B-bus 535
Mounting . . . 537

Mounting together with other units . . . 537
System 900 addressing . . . 538
Connection of system bus . . . 538
Connection of supply voltage . . . 540
Additional connections . . . 540
Activation of battery . . . 543
Connection of ethernet . . . 544
Setup of network parameters . . . 545
Installation test procedure . . . 546
Clock synchronisation and time settings . . . 547
Message distribution . . . 548
Unite Name Server (UNS) . . . 550
Maintenance information for the AIWS . . . 550
Replacement of the Compact Flash . . . 550
Updating application software . . . 550
Replacing an image on the Compact Flash . . . 551
Installing an image on an empty Compact Flash . . . 552
Updating the software license . . . 553
Circuit board replacement . . . 553
LON Piggy Back Circuit Board (LPB) . . . 554

Installing Elise 3 Server (AIWS2 Hardware) . . . 557

Introduction . . . 557
FCC Compliance statements for Class B Digital device . . . 559
IC Requirements for Canada . . . 560
EU Compliance Statements for Class A Device . . . 560
AIWS2 Overview . . . 560
Connectors, LEDs and buttons . . . 560
License . . . 563
Mac address . . . 563
Powering down and restarting the Elise 3 Server (AIWS2 Hardware) . . . 564
Operating modes . . . 564
Selection of operating mode . . . 565
Status LED indicators . . . 566
Authentication and administration . . . 569
Installing the Elise 3 Server (AIWS2 Hardware) . . . 570
Installation procedure . . . 571
Mounting . . . 571
Supply voltage . . . 576
Connections . . . 578

Accessing the Elise 3 Server (AIWS2 Hardware) . . . 580
Basic configuration . . . 586
Clock synchronisation and time Settings . . . 588
Message distribution . . . 589
Maintenance information for the AIWS2 . . . 590
Software management - . . . 590
Working in boot mode . . . 593
Replacing an existing Elise 2 module with Elise 3 . . . 594
Moving a license from Elise 2 Server (AIWS Hardware) to the Elise 3 Server (AIWS2 Hardware) . . . 595
Datasheet for the Elise 3 hardware (AIWS2) . . . 597

Technical Data . . . 601
Introduction . . . 601
IP-DECT Base Station (IPBS1) . . . 602
IP DECT Base Station (IPBS2) . . . 604
TDM-DECT Base Station (DB1) . . . 607
IP DECT Gateway (IPBL) . . . 609
Base Station RM627 (BS330) . . . 612
Base Station RM637 (BS340) . . . 613
Avaya 3725 DECT Telephone . . . 615
Avaya 3720 DECT Telephone . . . 621
Avaya 3740 DECT Telephone . . . 625
Avaya 3745 DECT Telephone . . . 631
Avaya 3749 DECT Telephone . . . 637
Advanced Charger for 3720 and 3725 DECT Telephones . . . 643
Advanced Charger for 3740, 3745, and 3749 Telephones . . . 645
Basic Charger for 3720 and 3725 DECT Telephones . . . 647
Basic Charger for 3740, 3745, and 3749 Telephones . . . 649
Multiple Battery Charger . . . 651
Rackmount Charger . . . 653
Portable Device Manager (WinPDM) . . . 655
Avaya In-Building Wireless Server (AIWS) . . . 656
Variants . . . 658
Avaya In-Building Wireless Server 2 (AIWS2 hardware) . . . 659
Variants . . . 665
Omnidirectional single antenna . . . 667
Directional dual antenna . . . 669

Directional single antenna 671
TDM DECT Base Station. 672
Outdoor housing DECT base stations 674

Troubleshooting 675
Introduction 675
IP-DECT Base Station (IPBS) 676
Remote LAN sniffer traces 679
Avaya 3720/3725 and 3740/3749 DECT Telephones 681
Fault symptoms 681
Display information 684
LED error indications 686
Advanced Charger. 687
Multiple Battery Charger 688
Rackmount Charger 689
Portable Device Manager (PDM) 691
Avaya In-Building Wireless Server (AIWS). 693
General troubleshooting 693
Centralized phonebook via LDAP to Active Directory. 694
NetPage troubleshooting 695
Reboot after image installation w/o restoring the parameters 695
Troubleshooting the Elise 3 Server (AIWS2 Hardware) 696
Built-in tools in AIWS 698
Built-in tools in AIWS2 700
Advanced troubleshooting 702
AIWS factory reset. 703
What to consider when replacing a module 703

Configuring PTT on Meeting Exchange 705
Introduction 705
Creating a DDI on the SMGR (Session Manager) 705
Adding a call branding entry 709
Procedure on SMGR. 710
Configuring patterns for dialing out 711
Configuring patterns for dialing in 713

Glossary 719
Related documents 723

Index 725

Avaya IP-DECT System Description

Introduction

Avaya IP-DECT is an IP-based cordless telephony and messaging system to connect to private telephone exchanges.

The IP-DECT system supports the DECT standard which gives a full integration of messaging and voice functions. You can also integrate the DECT-system with external applications such as different alarm systems. This system gives features such as; messages to telephone, alarm from telephone, message acknowledgment, and absent handling.

Abbreviations and Glossary

AIWS2	Avaya In-Building Wireless Server:. An application suite running on an Elise3 server. It enables wireless services to and from handsets and chargers.
CKI	The CKI, Cipher Key Index, is stored in both the handset and in the system and is used for Early Encryption. It uniquely identifies a DefCK and is used for Early Encryption.
DECT	Digital Enhanced Cordless Telecommunications: global standard for cordless telecommunication.
DefCK	The DefCK, Default Cipher Key, is stored in both the handset and in the system and is used for Early Encryption.
GAP	Generic Access Profile: communication protocol standard within DECT, that guarantees compatibility of systems and components.
IP	Internet Protocol: global standard that defines how to send data from one computer to another through the Internet
IPBS	IP-DECT Base Station
IPBL	IP-DECT Gateway
ISDN	Integrated Services Digital Network
LAN	Local Area Network: a group of computers and associated devices that share a common communication line.
LDAP	Lightweight Directory Access Protocol

OAP	Open Access Protocol: XML based protocol used to create customized applications for Unite access.
PBX	Private Branch Exchange: telephone system within an enterprise that switches calls between local lines and allows all users to share a certain number of external lines.
PSTN	Public Switched Telephone Network
RFP	Radio Fixed Part. DECT base station part of the DECT Infrastructure. TDM-DECT base station connected to an IPBL or the local RFP part in an IPBS.
Roaming	The procedure of moving the handset from one IPBS/IPBL to another and still be able to place outgoing and receive incoming calls.
External Handover	The procedure of moving an active call from one IPBS/IPBL to another.
QSIG	Q-signalling: a set of standards defined by ECMA, ESTI and ISO for connection PBX to PBX in networks.
SMS	Short Message Service: global protocol for sending messages between cordless telephones.
VoIP	Voice over IP

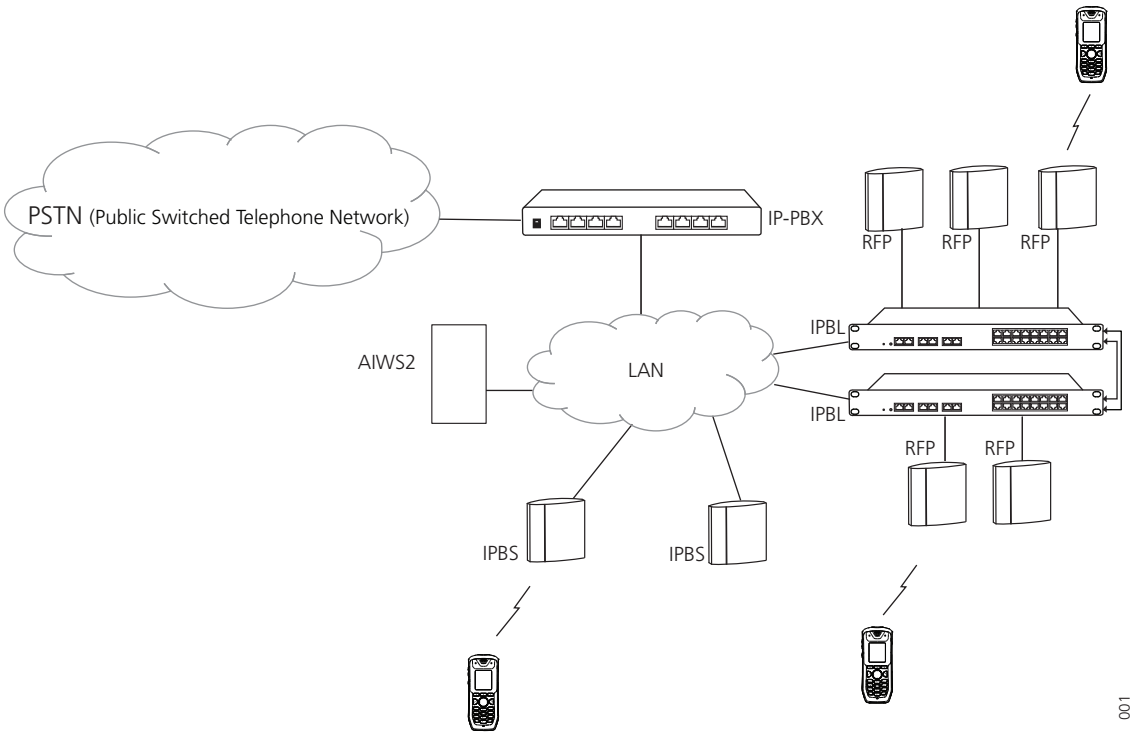
System overview

Avaya IP-DECT System is a wireless communication system that is cost efficient with modularity up to very large installations. Avaya IP-DECT system is a feature-rich distributed system that can be installed at local office or on-site and a wide variety of connection possibilities.

Avaya IP-DECT system components:

- DECT Cordless Handsets
- IP-DECT Base Station (IPBS)
- IP-PBX
- IP-DECT Gateway (IPBL)
- Radio Fixed Part (RFP)
- Avaya In-Building Wireless Server (AIWS2)

Figure 1: IP-DECT System Overview



IP-DECT System Overview

Supported Standards

- H.323 XMobile incl. H.450
- G.711 (a-law and mu-law)
- G.723-53
- G.729-A/AB

System functions

Avaya IP-DECT system is designed to enable voice traffic, messaging, and alarms between cordless telephones within an enterprise LAN. For details see *Function Description Document, Avaya IP-DECT System*.

DECT functions

DECT is a digital wireless technology that originated in Europe, but is now being adopted increasingly worldwide, for cordless telephones, wireless offices, and even wireless telephone lines to the home. DECT has been designed and specified to interwork with many other types of network, such as the PSTN, ISDN, and GSM.

Common IP-DECT functions are handled entirely within the IP-DECT system.

Roaming and handover

The IP-DECT system supports roaming between all base stations and gateways in the system. The IP-DECT system also supports handover if there is overlapping speech coverage.

Enhanced DECT Security

The enhanced DECT security feature is a mechanism to enhance DECT security by introduction of early encryption and re-keying during an ongoing call. It also addresses the security risk of staying permanently open for registration.

Early Encryption

This procedure is used for encryption of each DECT link, directly after establishment. The purpose is to protect data like caller ID and dialed digits, exchanged before encryption with the handsets private cipher key can start.

When a handset that supports early encryption is registered, a CKI with a corresponding DefCK is allocated/calculated and stored both in the handset and in the IP-DECT system. The CKI uniquely identifies the corresponding DefCK for each handset within the system. Later at each DECT link establishment this CKI is used to identify the DefCK to be used for early encryption of the link. The handset will release the connection in case early encryption activation is rejected.

Re-keying

This procedure periodically modifies the handsets private cipher key used for encryption of an ongoing call. The purpose is to protect against any attempts to crack the ciphering e.g. like super-computing.

Subscription Requirements

This procedure is used to control if registration is allowed or not. A system that permanently allows registration will make it possible for an attacker to do over-the-air subscriptions using exhaustive testing of AC-codes.

The subscription method “With System AC”, used to allow anonymous registrations, will permanently allow subscription attempts.

Therefore, for safety reasons, when the anonymous registration is finished change the Subscription Method to "Disable"or "With User AC".

With the subscription method “With User AC”, the system will allow subscription attempts only after activation in the IPBS/IPBL web GUI. The system will thereafter remain in enabled subscription mode for a maximum time of two minutes. After successful registration of the activated IPEI, the system will not allow registrations any longer.

LAN/WAN

Several vendors provide components needed to deploy a LAN or WAN. For optimal performance for IP-DECT the following is recommended:

- Administer Quality of Service (QoS)
- Connect the infrastructure to a switched network. (i.e hubs or repeaters should be avoided)
- Use a backbone of least 100 Mbps depending on the network size.

LDAP

The LDAP protocol is used in the IP-DECT system between two or more Master IPBSs/IPBLs if different network regions shall be used.

Supported third-party functions

IP-PBX are examples of third-party products required when setting up the DECT infrastructure. The Avaya developed products are designed to work in system provided by different vendors.

IP-DECT System

The major parts of the Avaya IP-DECT system are the IP-DECT Base Station (IPBS) and IP-DECT Gateway (IPBL) consisting of the software components DECT Radio (interface) and DECT Master.

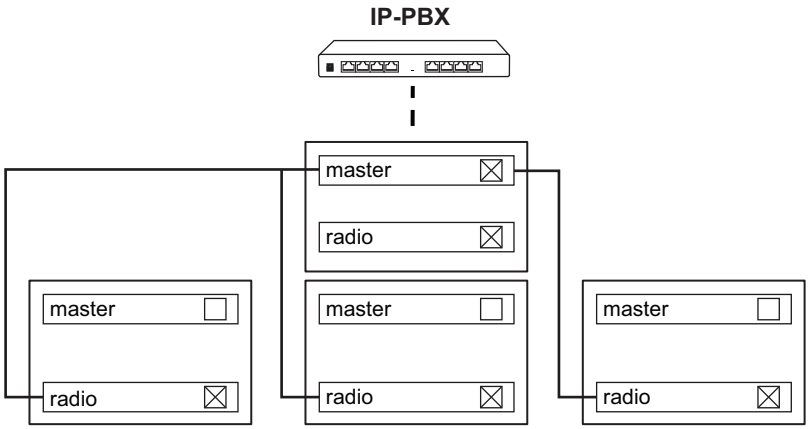
There is only one DECT Master in a single site IP-DECT system. In a multiple site IP-DECT system, each site is connected with the PBX through an own DECT Master and an H.323 XMobile trunk.

The IPBS/IPBL is connected to an IP network through the LAN interface, which provides connectivity to the IP-PBX.

System layout

All IPBSs/IPBLs are connected to the LAN, but it is only the DECT Master that have a logical connection to the IP-PBX. It is a flat layout where all DECT Radios are logically communicating directly to the DECT Master, see figure 2 on page 24.

Figure 2: Logical connections of the software components DECT Master and DECT Radio



DECT Master

The DECT Master is a software interface between the IP-DECT system and the IP-PBX. The DECT Master is responsible for all DECT handsets in the system.

The DECT Master knows which DECT Radio the handsets are located to, that is which DECT Radio in the system that received the latest location registration message from the handset. A call to a handset is directed only to the DECT Radio where the handset is located. Thus limiting the H.323 XMobile and DECT load in the system.

DECT radio

The DECT Radio is a software interface between DECT and H.323 XMobile. A DECT Radio always communicates with one DECT Master. The DECT Radio only has information of the DECT handset which currently are on the same radio channel.

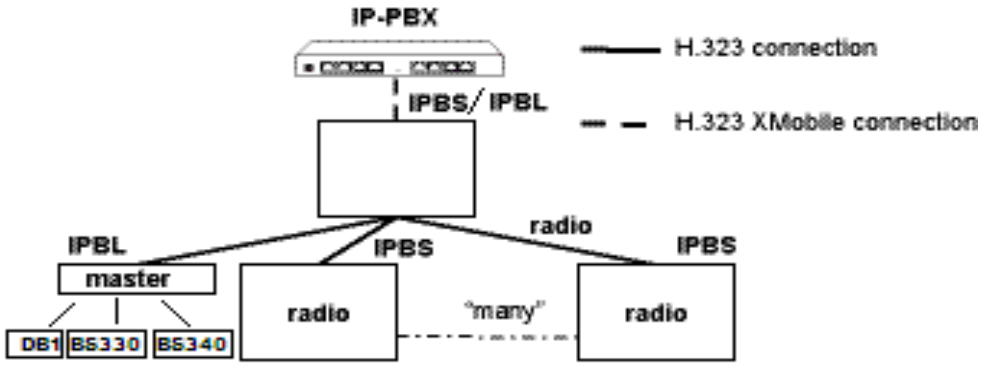
Single Site Installation Example Layout

Customers who require a single-site installation can use the layout in figure 3 for installation.

The system capacity for a single-site layout is:

- Up to 1000 users
- If the number of system IDs used in the installation is between 1 to 36:
  - Max. 1023 IPBS / Master
  - Max. 240 IPBL / Master
- When the number of system IDs used in the installation is between 37 to 292:
  - Max. 127 IPBS / Master
  - Max. 127 IPBL / Master

Figure 3: Single site layout with one IP-DECT Master



In figure 3, the lines that connect Communication Manager (IP-PBX), DECT Master, and DECT Radios indicate the logical connection between the software modules.

Note:

The figure 3 shows the software components. An IPBS includes both the software components DECT Master and DECT Radio.

Assign the role of master to one IP base station or gateway. The IPBS/IPBL can also act as a DECT Radio and have an active DECT Radio and an active DECT Master software component. All other IPBS/IPBLs will only have the software component "DECT Radio" active. The software component "DECT Master" will only be active in the Master, in all other cases it will be deactivated.

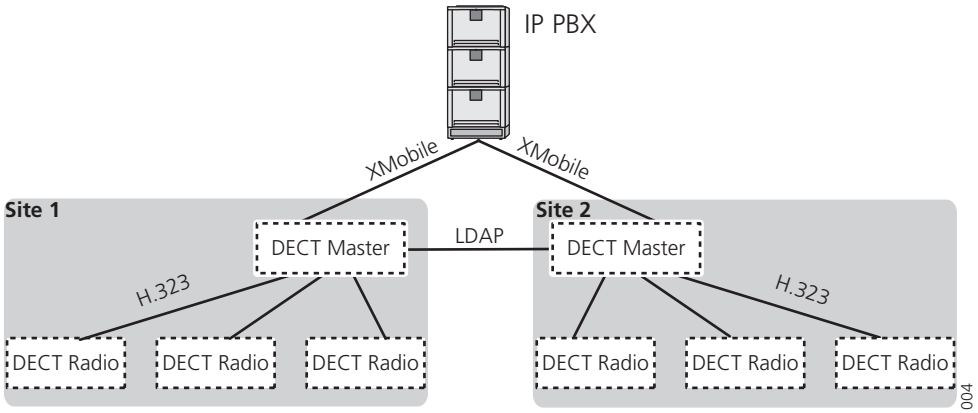
Multiple-site installation

You can use the single site layout for installation on several sites. The sites may have one DECT Master per site and one or several base stations at each site. Communication Manager is centrally located (may be one of the sites), see figure 4.

The system capacity for a multiple-site layout is:

- Up to 1000 users
- When the number of system IDs used in the installation is between 1 to 36:
  - Max. 1023 IPBS / Master
  - Max. 240 IPBL / Master
- When the number of system IDs used in the installation is between 37 to 292:
  - Max. 127 IPBS / Master
  - Max. 127 IPBL / Master

Figure 4: Multiple site layout with one IP-DECT Master per site



The lines displayed between the Communication Manager, the respective DECT Master and the DECT Radios in figure 4 are used to indicate the logical connection between the software modules.

Note:

An IPBS/IPBL includes both the software components DECT Master and DECT Radio.

External handover is only possible to do within each site, not between sites.

Each IP-DECT Master must be assigned an unique master identity to update the IP-PBX with correct information about the handset's location when it is roaming between different sites. See the following example for more information.

Example:

The identity for each IP-DECT Master is set according to the table below.

Site	IP-DECT Master ID
Site 1	1
Site 2	2

A handset being on Site 1 and Master 1 has indicated to the IP-PBX that Master 1 shall be used for incoming calls to the handset. When the handset is entering Site 2, the LDAP database will be updated with the new location of the handset, in this case, Master 2 shall be used for incoming calls to the handset.

Standby Devices

It is recommended to have Standby devices in an IP-DECT system. When a Master goes down the corresponding Standby Master takes over.

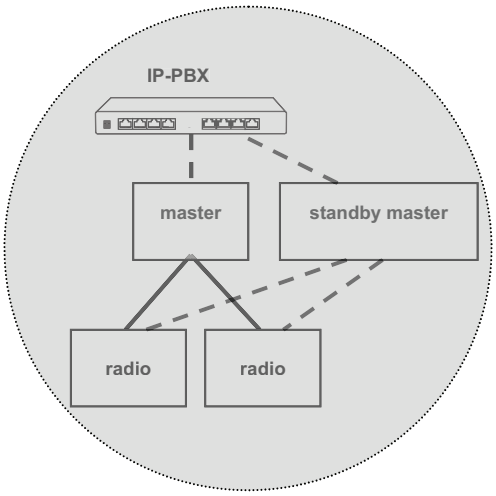


Figure 5. An IP-DECT system with a Standby Master.

Mirror Devices

For redundancy purposes, the Master can act in two ways: As Standby Master and Mirror. However, there are some limitations when using Standby Masters and in these cases using Mirror Masters can be a solution.

Description of Mirror Mode

Mirror Masters are configured in pairs in the same way as Active and Standby Masters are. A Mirror Master can act in both the two previous modes, Active and Standby. One Mirror will initially take the Active role while the other Mirror becomes the Standby. Both the previously used modes "Active" and "Standby" can now instead be set to "Mirror". It is not possible to mix the Mirror mode with any other modes, both masters must be set to Mirror.

The administrator decides which Mirror that initially should be the active one by clicking on the "Activate mirror" link in that device. When the active Mirror fails, the Mirror acting as the standby will automatically become the active Mirror. When the failing Mirror is in operation again it will take the role as the standby and stay inactive.

The administrator can, when both Mirrors are in operation, switch the active role by clicking on the "Switch active mirror" link. This should then be done within a maintenance window as all ongoing calls will be lost.

In the special case where both Mirrors become active due to a network error between the Mirrors, conflicts might arise when the connection between the Mirrors is established again. In this case the Mirror that became active most recently will "win" and changes made to the other mirror will be lost.

The LDAP replication of the user database between Mirrors will be done automatically when needed and no configuration of this is necessary when using the Mirror mode.

If LDAP replication is also used towards an IP6000 or an Active Directory this must be configured at both Mirrors. This replicator will be disabled automatically when the Mirror is inactive.

The Mirror mode will not affect the communication towards the IP-PBX except for the change of master IP address after a fail over.

Benefits With Mirror Mode Compared to Standby Mode

Note: For new installations we recommend to use the Mirror mode.

The functionality will not be limited when failing over to the Mirror that has acted as Standby. It will still be possible to add/edit/delete users, login/logout shared phones and subscribe new handsets. With the Standby mode this is not possible.

When the failing Mirror becomes available again the system will not automatically fall back to this Mirror and this is not necessary from a functional point of view. If the administrator anyway wants this to happen it is possible to manually switch back to the previously active Mirror. This should then be done at an appropriate time as ongoing calls will be lost. With the Standby mode the fallback is uncontrolled and can be brutal as ongoing calls are lost.

The LDAP replication of users will be done automatically when needed and no configuration of this is necessary with the Mirror mode.

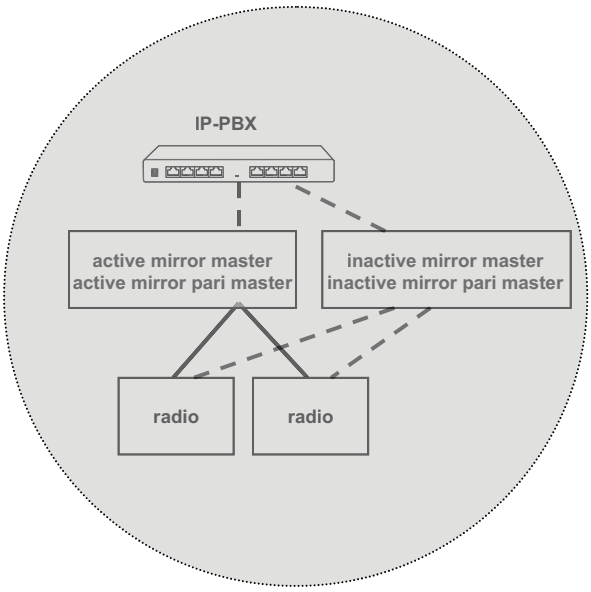


Figure 6. An IP-DECT system with Mirror Masters.

Messaging in Multiple Site Systems

For messaging purposes, the IP-DECT system can be connected to one or several Avaya In-Building Wireless Server (AIWS2). To have messaging functionality for all handsets in a multiple site system, each Master with handsets assigned must have a connection to an AIWS2

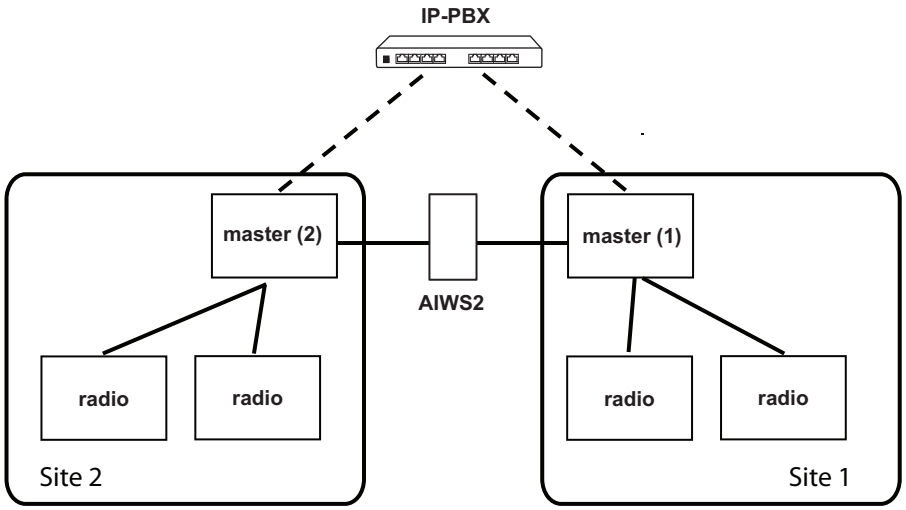


Figure 7. Messaging in Multiple Site Systems.

Example

A handset with extension 1111 is located at Site 1. In this case, the AIWS2 is configured to route all messages to handsets with extensions between 1000-1200 via the Master 1. The AIWS2 will route all messages to handsets with extensions between 1201-1300 via Master 2.

Device Management

A Device Manager (included in the AIWS2) is an application for managing handsets and chargers in wireless systems.

The Device Manager supports software downloads to handsets. The table below shows approximately download times for DECT handsets 3720, 3725 and 3745 when done over-the-air.

	IPBS	***IPBL***
3720	approx. 17 min.	approx. 102 min.
3725, 3745	approx. 25 min.	approx. 189 min.

The software downloads capacity is depending on call traffic in the following way:

IPBS: 0-4 simultaneous downloads depending on call traffic, see below.

Number of calls	*Number of possible simultaneous downloads*
0	4
1	3
2	2
3	1
4 or more	0

IPBL: 0-4 simultaneous downloads depending on call traffic. Same limitations as for IPBS, see above.

AIW2: Max. 10 simultaneous downloads (max. 20 when using an external web server).

There are a number of factors that affect the software download time:

- The number of base stations.
- The number of handsets per base station.
- How much the handsets are moving between the base stations. When moving between RFPs there will be a 1-2 minute break in the software download.
- Speech calls will delay the software download.

Device Management in Multiple Site System

If a handset is moved between several system/sites, it is possible to determine on which site/system the handset shall synchronize with the Device Manager.

For example, a handset with extension number 1111 is registered in System A. When the handset is present in this system, it will synchronize with Device Manager. If the same handset is registered with number 2222 in System B, no synchronization will be performed.

In this case, the System A is considered as the handset's "home" system and it can only be synchronized within this system and only when present in this system.

See the handset's Configuration Manual for more information about the settings.

Synchronization

Synchronization within the IP-DECT system is done by:

- Air synchronization (IPBS)
- Ring Synchronization (IPBL)

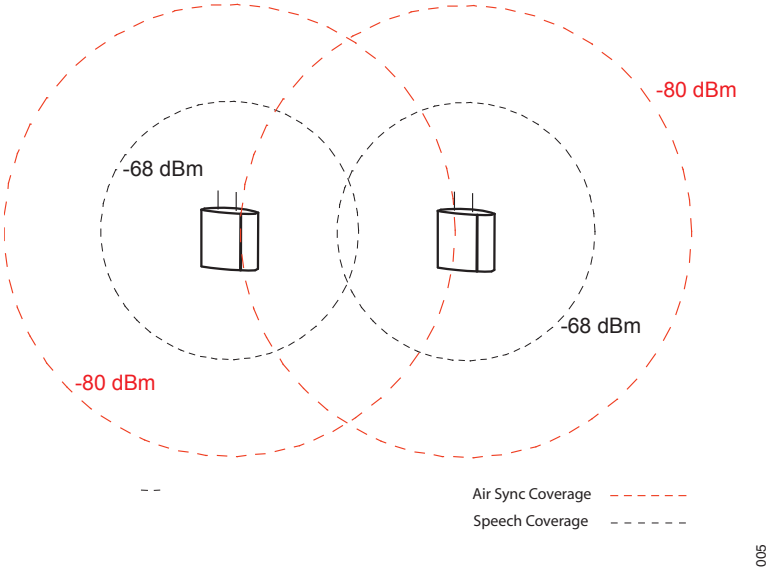
Air synchronization

IP-DECT base stations use the DECT air interface to synchronize to each other. This makes it possible to fulfill the Common Alerting Protocol (CAP) standard and to use the existing portables.

Configure one IPBS as a synchronization master. From this sync master all other IP base stations adjust their internal crystal oscillator to have the same frequency drift as the master. All base stations need not be within coverage of the master base, a IPBS running in slave mode can synchronize to another IPBS in slave mode.

You need not configure which IPBS to synchronize to. This is handled automatically by introducing a proprietary message called "air sync hop" that is sent from the IPBSs.

Figure 8: Air and speech sync radius.



A single IPBS failure may spread to other IPBSs. Therefore, for critical systems you need to install the IPBSs within coverage of at least two alternative IPBSs to sync with.

It is also possible to configure one backup sync master in case of failure of the sync master.

Speech radius: The radius of the circle (circular radiation patterns of the IPBS antennas are assumed), around a particular IPBS, in which portable parts can communicate with that IPBS. See figure 8: Air and speech sync radius.

Note:

The signal strenth must be at least -68 dBm for good speech quality. The -68 dBm circles must overlap to ensure seamless handover between 2 base stations (The handset should receive the next base station with -62 dBm at the -68 dBm circle of the first base station).

Sync radius: The radius of the circle, around a particular IPBS, in which other IPBSs lose synchronization with that IPBS with a given synchronization loss probability. The size of the sync radius depends on requested probability of losing synchronization. See figure 8: Air and speech sync radius.

Note:

A value of -80 dBm is a recommendation to ensure good sync conditions.

Ring synchronization

Each synchronization port sends and receives synchronization signals. Each IPBL has two ports *in* and *out* for ring synchronization and two ports *in* and *out* for reference synchronization.

The ring synchronization can be made in two different ways:

- Redundant (preferred)
- Non-redundant

Each synchronization ring dynamically assigns a sync master.

IP-DECT System Management

Onsite management

To manage IPBS and IPBL, use the web GUI that can be accessed over the LAN.

Remote management

The IPBS and IPBL have support for remote setup and configuration over the Internet.

IP administration security

All IP administration is based on secure IP. IPBS and IPBLs are password protected in order to prevent unauthorized access.

IPBS,IPBL, AIWS, and AIWS2 offer a set of default passwords for several user accounts in a factory fresh installation. During installation, you must change the default password for all existing accounts according to the described installation process for each particular device.

Software upgrade

IPBS and IPBL support:

- Software download using the web interface.

- Software upgrade using the web interface.
- Automatic firmware update from a web server or a TFTP server.

VoIP signalling protocols

The protocol used for VoIP signalling is H.323 XMobile which is a proprietary extension of H.323. H.323 was the first standard and is in fact a set of protocols designed to enable multimedia traffic in single LANs. One protocol of many in the set of protocols defined in H.323, is H.450, which is a series of protocols which defines Supplementary Services for H.323.

H.323

The International Telecommunications Union (ITU) developed H.323 from a telecommunications perspective. Ratified in 1996, H.323 has become a common choice for interoperability among VoIP equipment. H.323 is a standard that provides specifications for computers, equipment, and services for multimedia communication over networks that do not provide guaranteed QoS.

H.323 equipment can carry real-time video, audio, and data, or any combination of these elements. The H.323 standard includes H.225, H.245, and the IETF protocols RTP and RTCP, with additional protocols for call signalling and data and audiovisual communications.

Benefits of using H.323 products and services:

- Products and services developed by multiple manufacturers under the H.323 standard can interoperate without platform limitations. H.323 conferencing clients, bridges, servers, and gateways support this interoperability.
- H.323 provides multiple audio and video codecs that format data according to the requirements of various networks, using different bit rates, delays, and quality options. Users can choose the codecs that best support their computer and network selections.

H.323 XMobile

The protocol between the IP-PBX and the Master IPBS is based on H.323 with some minor differences called XMobile, such as:

- No need to register the DECT Wireless Terminal with the Gatekeeper. No RAS procedure necessary.
- Shared trunk between the IP-PBX and the Master IPBS where all telephony signalling is going

QSIG

- QSIG is a standardised signalling protocol, that is mainly used for signaling between traditional PBXs. This allows interoperability between communications platforms provided by different vendors.

- QSIG has two layers, called BC (basic call) and (GF) generic function. QSIG BC describes how to set up calls between PBXs. QSIG GF provides supplementary services for large-scale corporate, educational, and government networks, such as line identification, call intrusion and call forwarding. Thus for a large or very distributed company that requires multiple PBXs, users can receive the same services across the network and be unaware of the switch that their telephone is connected to. This greatly eases the problems of management of large networks.

IP-DECT planning and deploying

Each unit of IP-DECT provides radio access within a pre-defined area called a cell. To enable seamless handover for the mobile devices, cell planning is important when deploying the IP-DECT System. See the documentation from the DECT supplier if you are using a 3rd party DECT system. Also see Planning an IP-DECT system on page 43.

Avaya IP-DECT system components

The Avaya IP-DECT system is created using Avaya developed products, as well as third-party products. This section gives a brief description of the components needed.

DECT cordless handsets

The DECT Cordless Handsets are available in a number of versions. From handsets with basic functionality suitable in office environments to handsets suitable in environments with needs like supervision, alarm functions and EX-classification.

The IP-DECT system has support for all DECT Cordless Handsets. No changes of the handset is needed.

Handset installation on the DECT System/I55 System

Note:

The handset to be installed must not have any previous valid registrations. If it has a valid registration, unsubscribe the handset

Installation of Handsets

Subscribing a handset

1. Assign an extension number for the handset in the DECT/I55 system. See the corresponding manual for the DECT/I55 system.
2. Subscribe the handset towards the DECT/I55 system. The subscription procedure is described in the handset's User Manual.

During the subscription procedure, the handset's User ID will automatically be set to the same as the extension number. The User ID is used to identify the handset when it is connected to PDM/Device Manager and will be visible in the Number column.



Tip:

The User ID can be viewed in the handset by navigating to the menu as follows: **Admin menu** > **Device info** > **User ID**

Handset Replacement with Device Manager in DECT/I55 System

Note:

The replacement handset must not have any previous valid registrations. If it has a valid registration, unsubscribe the handset.

1. Unsubscribe the old handset. If the unsubscribtion cannot be performed in the handset, unsubscribe the handset via the DECT/I55 interface. See the corresponding documentation for your system.
2. Subscribe the new handset with the same extension number as the old handset. The subscription procedure is described in the handset's User Manual. During the subscription procedure, the handset's User ID will automatically be set to be the same as the extension number.



Tip:

The User ID can be viewed in the handset by navigating to the menu as follows: **Admin menu** > **Device info** > **User ID**.

3. Insert the handset into a desktop charger or charging rack connected to Device Manager (not needed if an over the air connection is used). Navigate to the Numbers tab in the Device Manager.
   The new handset now has the same User ID as the old handset. It will automatically be synchronized and data and parameter settings from the old handset will be transferred to the new handset.
   The synchronization will take a while if the Contacts in the original handset contains a large number of contacts.

IPBS

The IP Base Station or the IPBS is available in two versions: IPBS1 and IPBS2. The IPBS has eight channels for speech and messaging and one channel which is reserved for broadcast messages.

For more information on the IPBS, see Installing and operating the IPBS and IPBL on page 63.

Compact IPBS

The Compact IPBS is identical to IPBS, but has only four channels used for speech. A basic administration interface is used for the Compact IPBS. For more information on the simplified interface, see *Installation and Operation Manual, IP-DECT Base Station and IP-DECT Gateway for Avaya, TD 92604EN*.

IPBL

You must use the IPBL (IP-DECT Gateway) if you plan to use legacy base stations (RFPs) with the IP-DECT system. Up to 16 RFPs can be connected to the IPBL. The IPBL has a total of 40 channels of which eight channels are used for each RFP for speech, message, and alarm. Two channels are reserved for messaging and alarm.

You can connect he following legacy DECT base stations to the IPBL in order to use them in an IP-DECT system:

- BS330-9131 with Internal antenna (EU)
- BS330-9134 with Internal antennas (US)
- BS340-9131 with External antenna (EU)
- DB1-C3 and DB1-C4

RFP

The following TDM-DECT base stations can be connected to the IPBL in order to use them in an IP-DECT system:

- BS330-9131 (EU) with Internal antenna
- BS330-9134 (US) with Internal antenna
- BS340-9131 with External antenna
- DB1-C3 (EU and US) with Internal antenna
- DB1-C4 (EU) with External antenna

IP-PBX

The IP-PBX is a private branch exchange that switches calls between VoIP users on local lines while allowing all users to share a certain number of external phone lines. The typical IP-PBX can also switch calls between a VoIP user and a traditional telephone user.

With a conventional PBX, separate networks are necessary for voice and data communications. One of the main advantages of an IP-PBX is the fact that it employs converged data and voice networks. This means that Internet access, as well as VoIP communications and traditional telephone communications, are all possible using a single line to each user. This provides flexibility as an enterprise grows, and can also reduce long-term operation and maintenance costs. Like a traditional PBX, an IP-PBX is owned by the enterprise.

Communication Manager

Avaya Aura(R) Communication Manager is a private branch exchange that transfers calls between VoIP users on local lines while all users share a certain number of external phone lines. Communication Manager can also move calls between a VoIP user and a traditional telephone user.

With Communication Manager, you do not require a separate network for voice and data communications. CM employs converged data and voice networks. Converged networks make Internet access, VoIP communications, and traditional telephone communications possible using a single line to each user.

Avaya In-Building Wireless Server (AIWS or AIWS2)

Avaya In-Building Wireless Server (AIWS) offers wireless services in IP-DECT such as SMS from cordless telephone to a cordless telephone, sending text messages from a web browser and access to a central phonebook. AIWS is also a messaging and alarm gateway between open messaging communication protocols and IP-DECT telephones.

AIWS is linux-based and runs on a highly reliable solid state appliance. AIWS operates on two hardware platforms:

- Elise 2 server (AIWS hardware)
- Elise 3 server (AIWS2 hardware) that is an updated hardware version of the Elise 2.

Both platforms offer the same functionalities, and the following functions are valid for both AIWS and AIWS2. For variations, see Variants on page 658:

- Sending messages from cordless telephone to cordless telephone
- Access to a built-in central phonebook

- Access to an external directory over LDAP
- OAP messaging and alarm protocols
- NTP support (master and radio)
- AIWS configuration that is fully web based
- Push to talk (PTT)

System capacity

Max No. of Devices in an Avaya IP-DECT System

Cordless telephones	2000
IP-DECt Gateways (IPBLs)	100
IP-DECT Base Stations (IPBSs):	1000
Base Stations BS330/BS340	16 connected to an IPBL that is, total 1600 in an IP-DECT system
Compact IP-DECT Base Stations	5

Traffic Capacity

Speech calls:	10000/hour
SMS:	10000/hour

Speech Channels on each device

IP-DECT Base Station (IPBS)	8 simultaneous calls
IP-DECT Gateways (IPBLs)	40 simultaneous calls

Speech Channels on each device

Base Stations BS330/ BS340	8 simultaneous calls
Compact IP-DECT Base Stations	4 simultaneous calls

Messaging capacity

Alarm Messages from DECT handset

Time until received in the Unite system:	*~ 2 sec*

No Highspeed Data to DECT handset 3720

Incoming Messages to DECT handset 3720

The time for a message to be delivered differ dependent on how many characters the message contain and if it is delivered to a single handset or a group of handsets.

Number of message characters:	*No of DECT handsets:*	*For **IPBL**: Time in seconds until **one handset** is paged:*	*For **IPBS**: Time in seconds until **one handset** is paged:*
20 characters	1	*~ 4*	*~ 3*
120 characters	1	*~ 5*	*~ 3*
240 characters	1	*~ 6*	*~ 4*
500 characters	1	*~ 9*	*~ 7*

Number of message characters:	*No of DECT handsets:*	*For **IPBL**: Time in seconds until **all handsets** are paged:*	*For **IPBS**: Time in seconds until **all handsets** are paged:*
20 characters	1 10 30 100	*~ 4* *~ 6* *~ 14* *~ 43*	*~ 3* *~ 4* *~ 11* *~ 32*
120 characters	1 10 30 100	*~ 5* *~ 7* *~ 17* *~ 56*	*~ 3* *~ 4* *~ 13* *~ 39*

Highspeed Data to DECT handset 3725/3745

Incoming Messages to DECT handset 3725/3745

The time for a message to be delivered differ dependent on how many characters the message contain and if it is delivered to a single handset or a group of handsets.

Number of message characters:	*No of DECT handsets:*	*For **IPBL**: Time in seconds until **one handset** is paged:*	*For **IPBS**: Time in seconds until **one handset** is paged:*
20 characters	1	*~ 4*	*~ 3*
120 characters	1	*~ 5*	*~ 3*
240 characters	1	*~ 6*	*~ 3*
500 characters	1	*~ 9*	*~ 3*

Number of message characters:	*No of DECT handsets:*	*For **IPBL**: Time in seconds until **all handsets** are paged:*	*For **IPBS**: Time in seconds until **all handsets** are paged:*
20 characters	1 10 30 100	*~ 4* *~ 6* *~ 14* *~ 43*	*~ 3* *~ 3* *~ 6* *~ 23*
120 characters	1 10 30 100	*~ 5* *~ 7* *~ 17* *~ 56*	*~ 3* *~ 3* *~ 9* *~ 27*

Planning an IP-DECT system

Introduction

IP-DECT system is an IP based cordless telephony and messaging system for connection to private telephone exchanges.

The IP-DECT system supports the DECT standard that fully integrates messaging and voice functions. You can integrate the DECT system with external applications such as different alarm systems, networks, and email to obtain the following features:

- Messages to cordless telephones
- Alarm from cordless telephones
- Message acknowledgment
- Absent handling

Wired LAN and backbone requirements

To ensure voice quality, perform a Network Assessment of the LAN before an installation or when you add new applications or users.

When you design a network, ensure the following to obtain optimal performance:

- The infrastructure should be connected to a switched network without hubs or repeaters.
- When you set up a network that supports both voice and data, voice and data must be on different VLANs.
- The maximum capacity of the VoIP traffic must not exceed 25% of the network capacity.
- Maximum capacity of the network may not exceed 75% of the total capacity of the network, including the VoIP traffic.
- The network must not use firewalls. If required, use tunneling or application aware firewalls.
- Use a backbone of at least 100 Mbps depending on the network size.

In a switched network, the transmission delay should not be a problem but if voice traffic is routed, a significant transmission delay might be added. If the transmission delay is too long an echo appears in the voice path impacting the systems voice quality. The transmission delay also adds to the speech delay. Jitter in voice packages also adds to the speech delay.
You can use several tools from third-party vendors that can provide detailed and useful information when performing site surveys.

End-to-end QoS

To achieve QoS for a phone call, you must manage QoS all the way between the two end points. By following a speech packet as the packet travels along the path between the end points, you can identify all network segments and transitions where QoS needs to be managed.

Base station planning

The major task in installing an IP-DECT system is defining the number of base stations required to cover an area to a satisfactory level. Small sites usually have a homogeneous layout, and therefore you can easily predict and plan the field pattern of the base station. The larger sites are more

complex and less homogenous, and placing the base station is more difficult. The client might also have specific requirements that you must take into account such as coverage in a lift, underground car park, conference rooms, and outdoors.

Base station planning is not difficult, but the size, architecture, and structure of buildings all influence the field pattern which you cannot foresee. The quickest and simplest way is therefore to measure WHAT. During a site survey, determine an average cell size with the help of a site survey tool. The average cell size is the foundation of a base station planning.

To perform base station planning:

1. Determine the client specific requirements, see Client requirements on page 46.
2. Determine the average cell size using the site survey tool. See Determining the average cell size on page 53.
3. Decide base station positions, see Location of the base stations on page 58.
4. Make a base station plan, see Making a base station plan on page 60.
5. Measure and confirm that speech and air sync coverage is as expected using the site survey tool.

Client requirements

When you plan an IP-DECT system, ensure that the system meets the needs and requirements of the customer. Discuss with the customer in which area the customer requires high quality network access and where lower network sound quality is sufficient, for example, outdoors or in a production hall.

Also discuss coverage in special areas such as lifts, stairwells, basements, indoor car parks, toilets and maintenance shafts.

The customer might need higher traffic capacity in some areas or departments, for example, sales, purchase, technical support departments, and canteens. So you must add base stations in these areas. For information on how to calculate traffic capacity, see Traffic capacity of the system on page 55

Base station coverage

Architecture, building elements, and special areas affect the coverage and the placing of the base stations.

The radio environment or the cell that a base station covers is not spherical in shape but much more irregular. The momentary size and shape depend on the material of the walls and floors, the position and material of the furniture, machines, air-conditioning, and the position of the base station in such an environment. While these unpredictable conditions make formulating specific rules on how to calculate the number of base stations in a given situation difficult, the following are some guidelines:

- The in-house cell size in offices can have a radius of between 10 and 30 meters, see Example of base station location in a building. on page 47. The cell size in exhibition or production halls can have a radius of up to 200 metres.
- The free space outdoors cell radius can be up to 300 metres.
- Base stations might partially cover the floors immediately above and below. The useful range through floors and ceiling varies between 0 and 8 m (2 floors) radius.
  See Example of base station location in a building. on page 47.

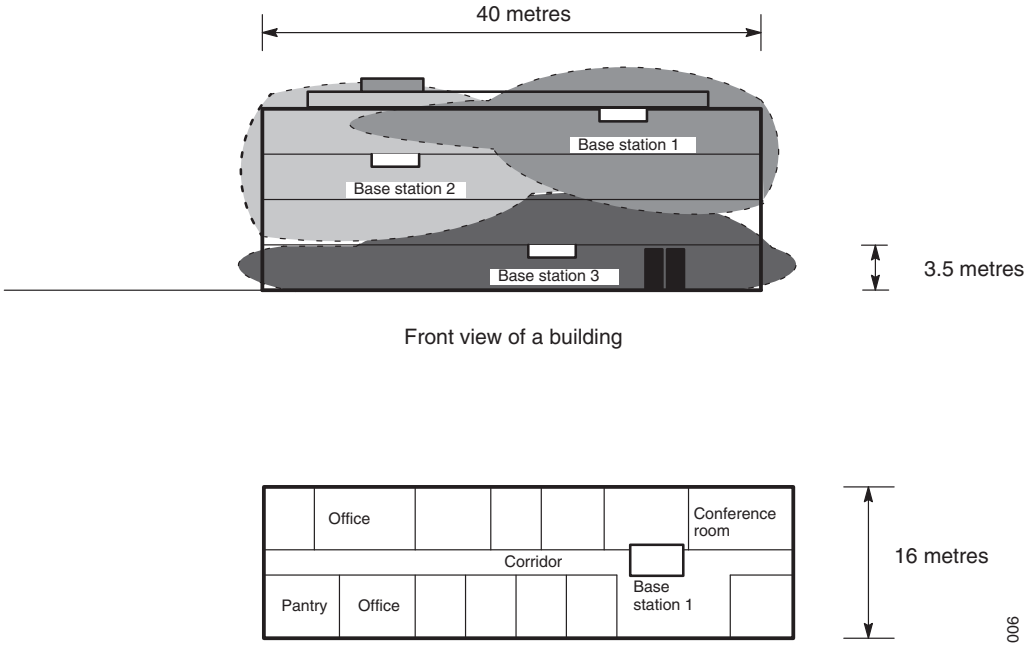
Architecture

This section describes how the architecture of the building can affect the base station coverage.

- Central areas giving access to stairs and lifts might require extra base stations due to heavier constructions.

- Coverage in lifts might require base stations closer to or in the lift shaft.
- Corners and irregularities in the construction such as partial renovation, extensions of older buildings influence base station coverage.
- Technical installations such as concentration of air-conditioning ducts might influence the field pattern and therefore the coverage.

Figure 9: Example of base station location in a building.



Building elements

Different building elements can affect coverage. For example:

- The cell size depends on the material of the walls, ceilings, and floors.
- Plain, light, or reinforced concrete, wood, and plaster differ in the way the materials absorb and pass radio waves.
- Metal walls and large metal cabinet rows reflect all signals, resulting in a greatly reduced coverage in areas behind these objects. Radio signals cannot enter X-ray rooms in hospitals that are protected by lead walls and computer rooms in buildings that are protected against unwanted interference such as banks.

- Exhibition halls or production halls may give reflections due to large metal structures. This causes interference which reduces the capacity and coverage range of the base station.

Walls

Walls, ceilings, and floors have a significant impact on the coverage range. Different types of walls have different impacts on the signal range. The following table lists the most common types of walls and the approximate range achieved through these materials:

Type of wall	Examples	Range in meters
Stud wall	Plaster	30-60
Concrete		10-30
Reinforced concrete	Fire wall	0-10
Stone/brick		30-50
Metal	A panel on brickwork	0-10
Wood		30-60
Wired glass	Fire protection	0-10
Surface coated float glass	Only of importance for coverage outside if the base station is installed inside	30-50
None	Open-plan office or outdoors	150-300

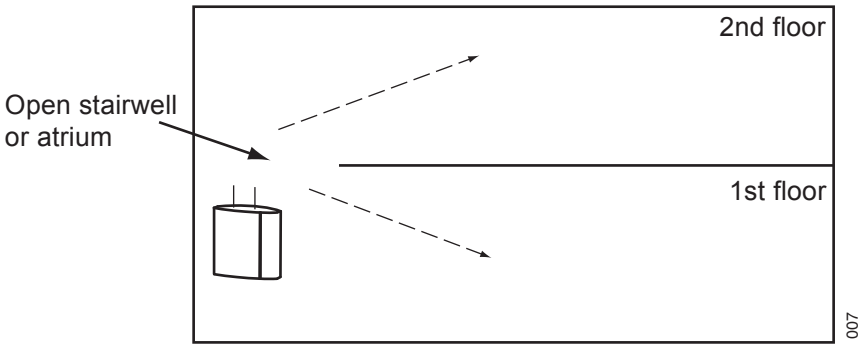
Note:

The values in this table are approximate only. The furniture in the coverage area and the amount of movement also affect coverage range. For example, cranes in a production hall. See Metal halls on page 51.

Ceilings and floors

The difference between ceilings and floors and walls is in the materials used. If concrete and reinforced concrete are the main materials, determine the level of coverage of a base station on the floor above and below. The coverage for concrete walls and ceilings extends to a radius of approximately 15-20 metres providing coverage for the floors below and above. AIn some cases, you can use an open stairwell or an atrium to provide coverage to two floors at the same time. See Base station covering two floors on page 49.

Figure 10: Base station covering two floors



Fire-resistant walls and doors

The same facts apply for fire walls as for normal walls mentioned in the section above. Coverage for fire walls is the same as for concrete walls. See Ceilings and floors on page 41. If fire doors are open during the site survey, close the fire doors before performing the final site survey measurement and finalizing the base station plan. If a fire breaks out and the doors are closed, sufficient coverage is still required.

Special areas

Special areas affect base station planning, and you must ensure full DECT coverage in the following areas:

Outdoors and car parks

Coverage outdoors is usually not a problem as there are minimal obstacles. The base station location depends on the client and on the size of the area to be covered. If the client wants to have a minimum number of base stations in the outdoors because of the cost of outdoor housing, you can install one or more indoor base stations with antennas in front of a window.

Ensure that the base station can see as much of the outdoor area to be covered as possible. The number of obstacles between the base station and the covered area must be minimal. Ensure that you perform a measurement to check how much coverage a base station provides to the outdoor area.
Installing all the base stations in front of windows is not the ideal position to provide indoor coverage. Normally, one or two base stations near a window are sufficient.

Type of glass	Range in meters
Normal glass	150-300
Surface coated float glass	30-50
Wired glass (fine-mesh)	0-20

Lift

the client requires coverage in lifts, locate the base station close to the lift, preferably at the front of the lift. A lift is usually surrounded on three sides by a reinforced lift shaft, and the front of the lift is the only opening. Locating a base station in front of a lift is not the most ideal position for planning coverage. You might require one or more extra base stations to provide coverage to a

lift. The same base station also provides coverage for the storey above and below the floor on which you install the base station.

Stairwell

To provide coverage to a stairwell, analyze the type of stairwell, open or closed, and the location, in a corner of the building or in the centre. In the context of the overall planning, you can install the base station directly in the stairwell as a dedicated base station or in the vicinity of a stairwell.

Toilet rooms

To provide coverage to a set of toilet rooms, analyze the the location, in a corner of the building or in the centre. In the context of the overall planning, you can install the base station directly in the toilet rooms as a dedicated base station or in the vicinity of the toilet rooms. Place the base station where the base station can see as much as possible of the toilet room as wooden entrance doors do not hamper signals. You might place the base station to also provide coverage to as much of the rest of the floor as possible.

Maintenance shaft

The client might want coverage in other rooms in the building such as the maintenance rooms and rooms for the lift and ventilation systems, which are generally on the roof or in the basement. A well-positioned base station that is 20 to 30 metres at most from the room where coverage is required provides sufficient coverage for the maintenance rooms on the top floor or the basement.

Basement and indoor car park

Providing sufficient coverage in basements and indoor car parks is difficult due to the usually heavy construction in these areas.

Metal halls

Providing coverage in a metal hall such as a production hall or storage building requires attention to the dimensions of the hall and the material used in the roof, floor, and walls. For example, metal, concrete, or brick. While every hall is different and predicting the radio reception is difficult, you must check whether:

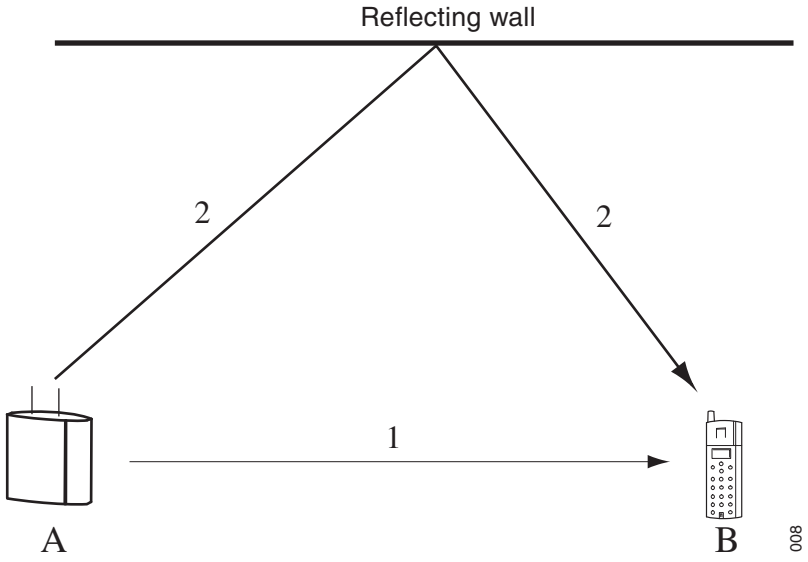
- The roof is reflective.
- The hall has many objects.
- The objects in the hall are stationary or constantly moving.

Poor speech quality in a metal hall can be due to time delay spread or the actuation of the soft suppressor or both. Both are explained in greater detail in the following topic.

Time delay spread

Radio signals can travel by various paths to reach the user, either directly but through reflections. This feature is called Time delay spread. For a graphic representation of Time delay spread, see the following figure:

Figure 11: Time delay spread



The base station at corner A reaches the cordless phone at corner B by means of a direct signal (signal 1) and by means of a reflected indirect signal (signal 2). Many reflected signals reach the cordless phone. The paths that these signals travel are not equal, and so the signals arrive at the cordless phone at different times.

A DECT signal consists of frames of 420 bits transmitted every 10 ms. The bit length for DECT is 0.868 µs. Mutes or Interruptions in your conversation and clicks on the line will occur if the time difference between the various received signals is of the order of 1/10 bit length. If this occurs, the receiver hcannot distinguish between the different transmitted bits. Therefore, you must place the base stations in a metal hall to minimize the time delay spread and the number of reflections.This means in turn that you must locate the base stations such that the number of reflections is minimized.

Locations for base stations in metal halls

Apart from the time delay spread, adhere to the following general rules when you place a base station:

- Install a base station in line of sight (The base station ‘sees’ the user).
- When you increase the number of base stations at locations that are important to the client, the speech quality can deteriorate in other places in the hall because the cordless phone must carry out more handovers.
- Place the base station at a minimum height of 3 metres as otherwise it is highly possible that something will be placed in front of the base station, and this prevents the materials and machines in the hall reflecting the signal.
- Place the base station at a minimum height of 3 metres. At a lower height, something that is placed in front of the base station prevents the materials and machines in the hall from reflecting the signal.

The rules depend on the dimensions of the hall and the type of antenna in use.

Determining the average cell size

Survey the site to determine the number and position of base stations required to match coverage and traffic needs. For a site survey, you need a site survey tool and floor plans. Take samples to determine an average cell size and indicate base station positions on the map and the area covered by each base station. After this, you can verify the planned positions with the site survey tool and can make a final plan with help of the traffic requirements.

Because coverage for air sync and speech differs, two average cell sizes need to be determined, one for the speech coverage and one for the air sync coverage.

For information on how to use the site survey tool, please refer to the appropriate user guide.

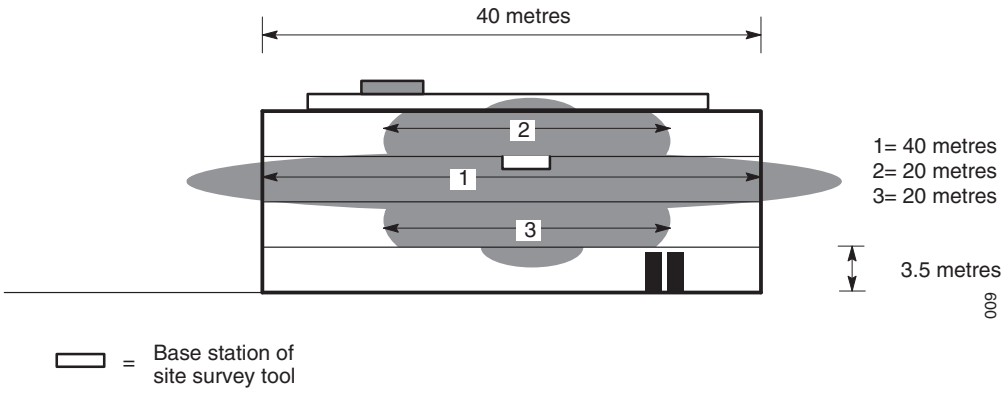
Principles to perform a site survey:

Observe the building to find a typical area

Due to renovations or expansions, older buildings might have areas with different structures. However, within these areas you can find a certain uniformity in structure.

Find an area in the building with a typical structure and the expected cell size. Use this area to determine the typical cell size. When you have a building with different structures, determine the typical cell size for each of those areas to detect the differences in the typical cell size.

Figure 12: Measurement of typical cell size



Measure the horizontal cell size on the middle floor. See (1) in figure 12.

To determine the cell size:

1. Install the site survey base station in the middle of the ‘typical area’.

2. Walk away from the base station with the cordless phone. Also enter rooms to the left and right.
3. Determine the edge of the cell. You can know the edge of the cell by the limit warning or by looking at the *Link Info* display and listening to the sound quality.
4. Walk in the opposite direction, and determine the edge of the cell. This is the horizontal coverage on the floor of the base station.

Measure horizontal range on floor above, see (2) in figure 12

Leave the base station at its current location, and go to the floor above. Measure the horizontal coverage here.

Measure horizontal range on floor below, see (3) in figure 12

Leave the base station at its current location, and go to the floor below. Measure the horizontal coverage here.

.

Note:

If the building is receptive to radio signals, the vertical coverage reaches yet another floor above and below.

After you determine the horizontal and vertical coverage of a single base station in a typical area, you can determine the average of the cell size and use the average to calculate the total number of base stations. Depending on the size of the building and the type of construction, perform one or two more random checks in typical areas to verify the first measurement. Calculate the average of the values you obtain to determine the typical cell size.

Traffic capacity of the system

The traffic capacity of the IP-DECT system is mainly determined by the number of base stations and in exceptional cases also by the LAN bandwidth. A single base station has a capacity of eight simultaneous calls.

The traffic capacity of the IP-DECT system is determined by:

- Grade Of Service (GOS) accepted by the customer.
- Number of speech circuits available - 8 circuits for each IPBS.

GOS is the probability that a call cannot be made because of congestion in the system. The customer must indicate the acceptable grade of service. A grade of service of 1%, or 0.01, means an average of 1 lost call in every 100 calls.

The two parameters, GOS and the number of speech circuits, and the total amount of traffic that is required are related to each other. The total traffic generated by all cordless phone users is called the erlang value. The following table shows an example of these relations. You can use this table to calculate the number of base stations required based on GOS and the erlang value.

A base station provides for 8 speech circuits.

Number of base stations	**Speech circuits**	**Grade Of Service (GOS)**			
		2%	**1%**	**0.5%**	**0.1%**
1	8	3.6	3.2	2.7	2.1
2	16	9.8	8.9	8.1	6.7
3	24	16.6	15.3	14.2	12.2
4	32	23.8	22.1	20.6	18.2
5	40	31.0	29.0	27.3	24.5
6	48	38.4	36.1	34.2	30.9
7	56	45.9	43.3	41.2	37.5
8	64	53.4	50.6	48.3	44.2

The table below shows what erlang values practically mean in call-minutes for a cordless phone.

mE	Minutes per hour	mE	Minutes per hour
50 100 150 200	3 6 9 12	250 300 500 750	15 18 30 45

Example:

A customer ordering a system with 55 cordless phones, generating 200 mE each in average, requires a system with a traffic capacity of 11 E. With an accepted GOS of 0.5% the number of base stations is found as follows:

The total traffic is 11 E. In the column of 0.5% GOS, the next higher value of 11 E is 14.2 E, resulting in 3 base stations. The system shall be equipped with 3 base stations, offering the client 14.4 E instead of 11. This means that the system has an over-capacity 3.2 E, which allows expansion of the system with 16 cordless phones without reducing the grade of service or the need of more base stations.

Traffic capacity of the base stations

The total traffic that all cordless phones on a system generate must comply with the capacity of the cordless network. A base station with 8 channels has an erlang value of 2.7 and a GOS of 0.5%. See the table to read the value. This means that each base station can serve 18 cordless phones, assuming that each cordless phones generates 150 mE during busy hours and 13.5 cordless phones if each phone generates 200 mE.

Example:

Referring to the building of the customer in the example Traffic capacity of the system on page 55, you can achieve full coverage by 4 base stations. This means that all cordless phones generate together 55 x 0.200 = 11 E, while the base stations traffic capacity is only 4 x 2.7 = 10.8 erlang. The erlang value falls below requirement. This discrepancy can be solved by adding another base station nearby the busiest part of the company.

From an average usage point of view, the total capacity that the cordless network offers might be adequate. In certain locations in a building however, traffic demands may vary at different times of the day. At such times, users experience network blocking, or the network has a lower GOS than required. For instance, a purchase department might generate 300 mE per cordless phone during peak hour, when usage by six personnel generates a high load on the closest base station. You must add a base station in this area to provide adequate capacity for calls by other personnel. Also factor in the fluctuation in traffic generated in specific areas during specific time of the day, for example, a canteen during lunch time.

Trunk capacities

While designing an IP-DECT system, it is important to consider the required trunks to connect to Communication Manager.

The number of signaling and trunk groups strongly depends on the system architecture of the IP-DECT system. For example, the number of users, number of locations, and redundancy requirements. For more information, see Configuring trunks on page 156.

Location of the base stations

After you analyze the surroundings and determine the average cell size, you must decide the location of each base station. The best location ensures sufficient coverage and traffic capacity.

Location depends on the following factors:

- Client's requirements. See Client requirements on page 46.
- Coverage and traffic capacity. See Base station coverage on page 46.
- Synchronization. See Air Synchronization on page 58.
- LAN Access. See LAN access on page 58.
- Power the base stations. See Power the base stations on page 58.
- Different types of antennas. See Antennas on page 58.

Air Synchronization

Place each IPBS within the air sync coverage of at least one other base station. The air sync cover radius is larger than the speech radius. Therefore, calculate only the speech coverage when placing the base stations. Ensure that all base stations synchronize with preferably two but at least one other base station.

LAN access

Access to the LAN is important for base stations. Place the IPBS as close as possible to existing LAN ports. The cable length can be a limitation. The ethernet 802.3 10/100base-T cable is 100 meters.

Power the base stations

Plan how you will power the base stations. For information about the various ways of providing power and power supply requirements, see Installing and operating the IPBS and IPBL on page 63.

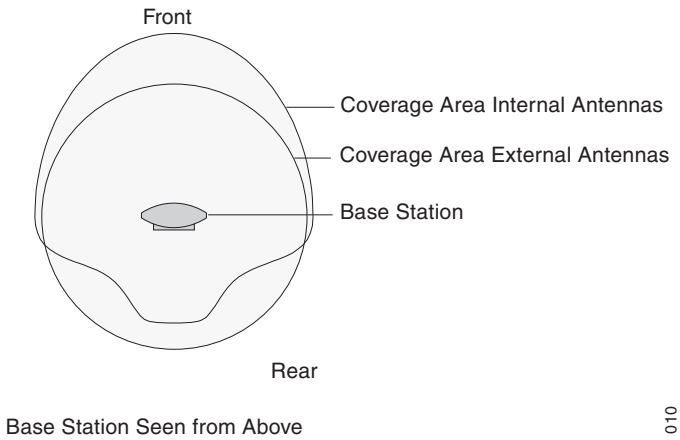
Antennas

Different types of antennas have different functions.

Internal and external antennas

In an environment with high reflections, such as most office environments, the difference in coverage of the internal and external antennas is negligible. Both types of antennas provide coverage to different areas. In an environment with low reflections, forward bias or directional behavior of internal antennas is noticeable. For more information , see Antenna pattern of the Internal and External Antennas on page 59. It may be worth trying to place base stations horizontally in order to get more vertical coverage in for example stair wells.

Figure 13: Antenna pattern of the Internal and External Antennas



Directional antennas

Use directional antennas in small corridors and halls. Different types of antenna have different radiation patterns. Therefore, determine the type of antenna that is appropriate for your application. For best results, mount the base stations on the ceiling, so that the antennas can radiate vertically downwards. You can also use a beam that is very directional horizontally but has a wider radiation pattern vertically or vice versa. For example, in an extremely high hall ceiling. For this reason, you must always carry out a measurement to ensure the best possible operation.

Base station planning tips

For information about base station planning, see Client requirements on page 46 and Location of the base stations on page 58.

Some important guidelines for base station planning:

- Always involve the client in the site survey and the decision-making process for siting of base stations. Inform the client about the problems that you encounter such as a difficult area to cover. Ensure that the client does not face uncovered issues later.
- Discuss with the client whether to install the base stations visibly or out of sight. If the base stations must be out of sight, explore the possibility of installing the base stations with antennas pointing to the ceiling. In this position, ventilation ducts, metal panels, or other obstacles on the ceiling do not obstruct the base station. If the base stations must be visible, install the base station at a location where disruption by obstacles above the ceiling or behind walls is minimal.
- Pay particular attention to nonstandard areas such as toilet rooms, stairwells, lifts, and maintenance shafts.
- Always mount a base station at least 30 cm away from a metal wall, to avoid a substantial impedance change for the antennas.
- Always try to place the base station in a way that it can "see" as much as possible of the area to be covered.
- Locate the base stations so that minimum obstacles exist between the base station and the coverage area.
- Place the base station strategically. For example, do not place the base station on a large concrete pillar in the middle of a hall as coverage behind the pillar will be poor.
- For outdoor coverage, mount a base station on a wall with a window. Place the base station with antennas in front of the window or in a way that the base station can see as much as possible of the outdoor area.
- Do not place base stations near the outer walls of the building as this reduces effective coverage inside the buidling. Place base stations near the outer walls of the building only for outdoor coverage.
- Discuss with the client the expected traffic capacity during the site survey. For example, the number of persons in a particular department, the number of calls made on an average, and the length of such calls on and average. Follow a thumb rule of one base station for 27 persons. If you are dealing with a high-volume center such as a purchase department, the ratio will change.
- Ensure a minimum space of 30 cms between two base stations.
- Ensure extra length of cable, 5 to 10 meters, for each base station so that you can move the base station, if required.

Making a base station plan

Determine the average cell size before you make a base station plan. See Determining the average cell size on page 53.

1. Make a sketch of all base station positions on the ground plan.
2. Indicate the expected speech and air sync coverage for each base station on the map.
3. Using the site survey tool, verify that the expected speech coverage matches the requirement.
4. Using the site survey tool, verify that the air sync coverage matches the requirement even in a worst-case scenario with all doors and windows closed. See Installing and operating the IPBS and IPBL on page 63.
5. Ensure that each IPBS synchronizes with at least two other base stations.
6. Verify coverage in out-of-the-way areas such as lifts, stairwells, and add-on construction.
7. If coverage is inadequate, reposition the base stations or plan an extra base station.
8. Select the IPBS for the master role, and place that IPBS in a central location to configure as air synchronization master. Ensure that the bandwidth between the master and the IP-PBX is sufficient.

Finalizing the plan

After you verify all base station positions on the map, discuss the need for extra base stations with the client to address local traffic requirements in high-volume areas. Integrate the extra base stations with the plan. This base station plan is now final and fully tested.

Installing and operating the IPBS and IPBL

Introduction

This chapter describes how to install and operate the following equipment:

- IP-DECT Base Station (IPBS1)
- IP-DECT Base Station (IPBS2)
- IP-DECT Gateway (IPBL)

The chapter is intended as a guide for installation, troubleshooting and maintenance purposes and is relevant for the following personnel:

- System administrator
- Service technician

For information on the IP-DECT system, see Avaya IP-DECT System Description on page 19.

Description

This section gives a general description of the IP-DECT Base Station and DECT Base Station.



IP-DECT Base Station

The following versions of the IPBS are available:

- IPBS1
  - IPBS1 with internal antenna
  - IPBS1 with external antennas
- IPBS2
  - IPBS2 with internal antenna
  - IPBS2 with external antennas

IP-DECT Base Station IPBS1 with internal antenna

Figure 14: IPBS Overview

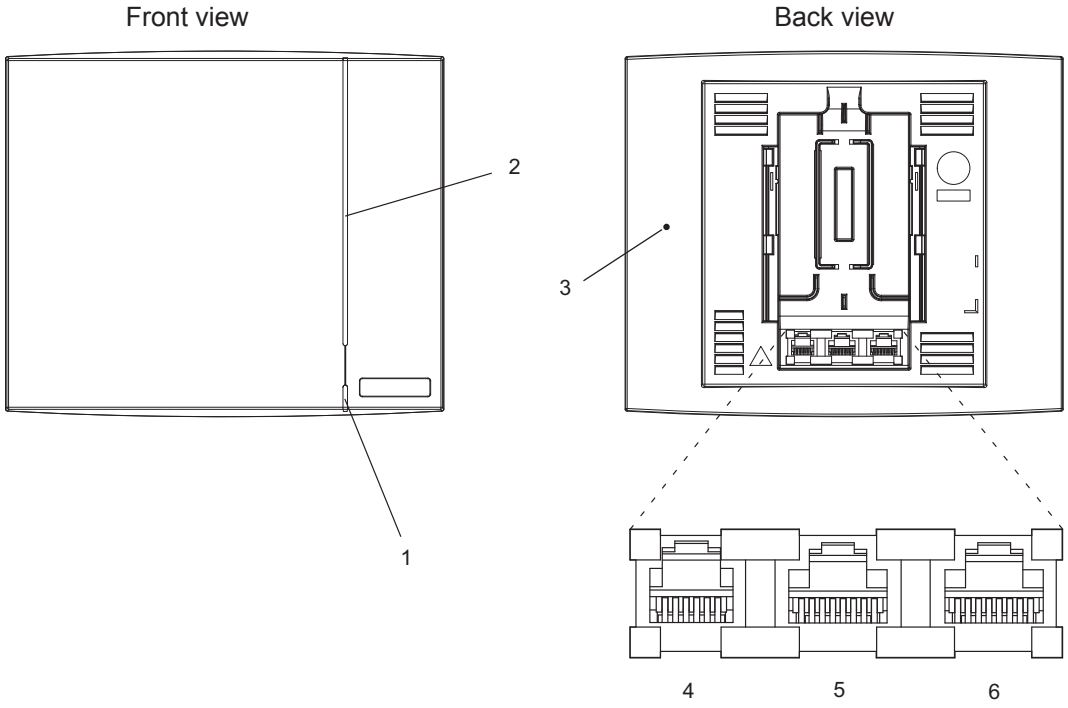


Figure notes:

1. LED 1
2. LED 2
3. Reset
4. Test (RJ12)
5. LAN (RJ45)
6. Power Supply (RJ45)

Contents of the box

The box in which the IPBS1 is packed contains:

- An IPBS1 with integrated antennas
- A patch cable (approx. 1 m)
- A mounting bracket
- Two screws with wall plugs

Power distribution

To provide power to IPBS1, use the following:

- Power over Ethernet, IEEE 802.3af

Note:

For more information about power distribution, see Turning on the base station on page 87.

Software

To update software in the IPBS1, download new software without disconnecting the equipment. The new software is stored in flash memory. For more information See Updating on page 183.

Connectors

- One 8-pin RJ45 modular jack for LAN/PoE
- One 8-pin RJ45 modular jack for an external power supply
- One 6-pin RJ12 modular jack for factory testing

LEDs

Status of LED1 (lower LED)	Description
Steady Green	Operational
Quick flashing amber	Download of firmware in progress.
Steady Amber	TFTP mode
Alternating red/green	No Ethernet connection

Status of LED2 (upper LED)	Description
Not lit	IPBS operational and **no** traffic Air synchronization OK
Steady green	IPBS operational **and** traffic Air synchronization OK
Slow flashing green	Air synchronization OK and fully occupied with traffic
Flashing amber	Air synchronization inadequate and **no** traffic
Slow flashing amber	Air synchronization inadequate and fully occupied with traffic
Steady amber	Air synchronization inadequate and traffic
Flashing red	No air synchronization - searching for air sync candidates

Quick flashing red	Download of RFP software in progress
Flashing/steady amber Alternating red and green	The radio is switched off in the Master because of a missing air synchronization.

Note:

All amber statuses are warnings that Air synchronization, although still adequate, is fading and might be lost. A flashing red indicates lost Air synchronization.

IP-DECT Base Station IPBS1 with external antennas

The IPBS1 is available with two omni-directional external antennas. You can mount other external antennas also. For all other information see IP-DECT Base Station IPBS1 with internal antenna on page 65.

Contents of the Box

The box in which the IPBS1 is packed contains:

- An IPBS1 with external antennas
- A patch cable (approx. 1 m)
- Two antennas
- A mounting bracket
- Two screws with wall plugs

Note:

Do not mount the IPBS1 with the antennas pointing downwards as the mounting bracket does not support that position.

Insert the antennas into the IPBS1 before following the installation instructions in Installing the base station on page 80.

AC-adapter

The AC-adapter is used to power a base station locally.

Note:

The maximum length of cable from adapter must not exceed 10 meters.

Versions or different type of mains plug

700466436	DECT RBS POWER SUPPLY UK
700466444	DECT RBS POWER SUPPLY EU
700466451	DECT RBS POWER SUPPLY US
700466469	DECT RBS POWER SUPPLY AU

IP Base Station IPBS2

The following three versions of the IPBS2 are available:

- IPBS2 with internal antenna: IPBS2-C3A/1A
- IPBS2 with internal antenna for IP Office: IPBS2-Z3A/1A
- IPBS2 with external antenna: IPBS2-C4A/1A

IPBS2 with internal antenna

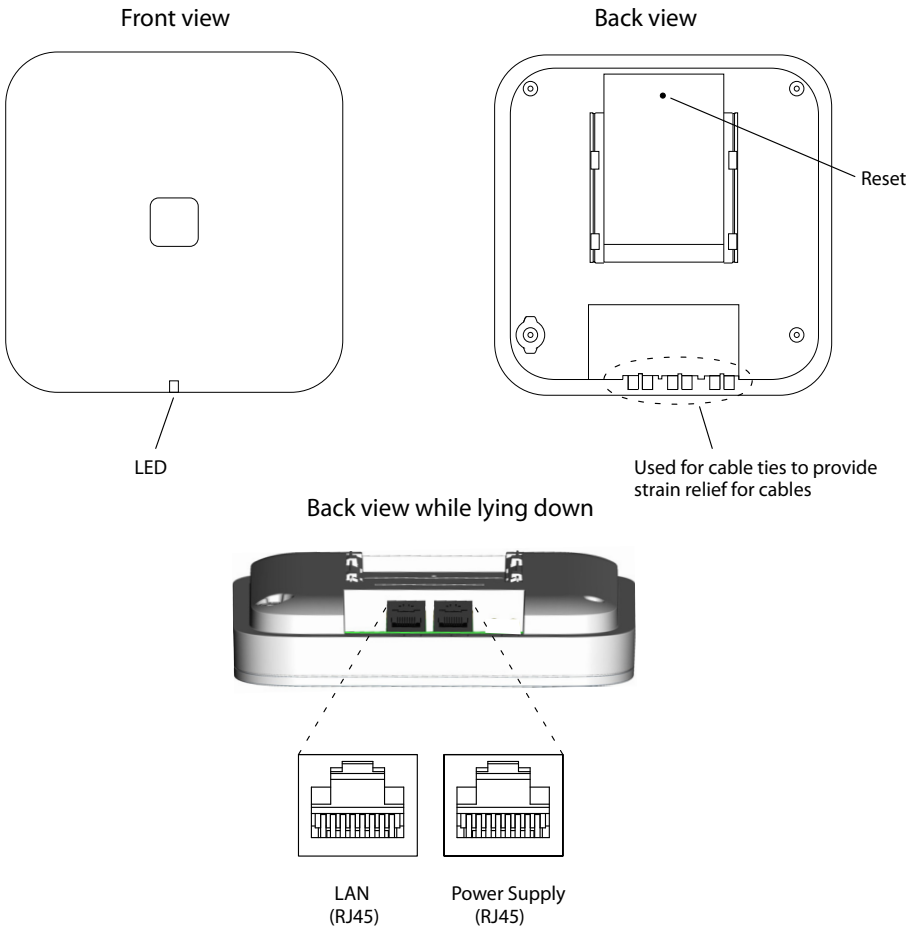
This description also applies to the IPBS2 with internal antenna for IP Office. The following versions are available:

- IPBS2-C3A/1A,
- IPBS2-Z3A/1A

IPBS2 with internal antenna

IPBS2-C4A/1A e version is available for IPBS2 with internal antenna.

Figure 15: IPBS2 with internal antenna



Contents of the box

The box in which the IPBS2 is packed contains:

- An IPBS2 with integrated antenna
- A mounting bracket
- Two screws with wall plugs

Power distribution

The IPBS2 can be powered using the following method:

- Power over ethernet IEEE802.3af.

Note:

Brazil is a POE only solution.

Note:

For more information about power distribution, see Turning on the base station on page 87.

Software

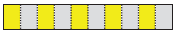
The software in the IPBS2 can be updated by downloading new software without disconnecting the equipment. The software is stored in the flash memory. See section Updating on page 183.

Connectors

Two eight-pin RJ-45 modular jacks for LAN/PoE and powering.

LEDs

The IPBS2 has one RGB LED to indicate status. Different indications have different uses. In the following table, each blink pattern is represented by a number of blocks where each block is 100 ms. Light grey blocks indicate that the LED is off. Whenever the indication changes, a new pattern starts from the first block.

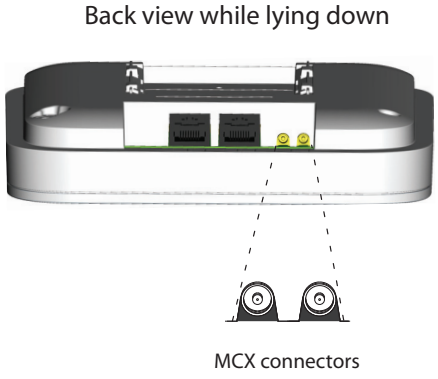
Status	Color of LEDs	Indication
Idle/OK		IPBS2 operational and no traffic on the IPBS2.
Start up/Searching		The IPBS2 is in the start-up phase and waiting for parameters from PARI master, or searching for air synchronization.
Active Traffice		IPBS2 operational and traffic on the IPBS2.
Fully occupied for speech traffic		Fully occupied with traffic.
Software download		Download of firmware in progress.
Mini firmware		The IPBS2 is in mini firmware mode.

Status	Color of LEDs	Indication
TFTP mode		TFTP mode.
Error		No ethernet connection.
Fatal error		Fatal hardware error.
Deployment: Good sync		The IPBS2 is in deployment mode and has good air sync coverage.
Deployment: Bad sync		The IPBS2 is in deployment mode and does not have adequate air sync coverage.
Deployment: No sync		The IPBS2 is in deployment mode and has no air sync coverage.

IPBS2 with connectors for external antenna

This section contains the differences between the IPBS2 with internal antenna and the IPBS2 with connectors for external antennas. For all other information see IPBS2 with internal antenna on page 68.

Figure 16: IPBS2 with MCX connectors for external antennas.



Contents of the box

The box in which the IPBS2 is packed contains:

- An IPBS2 with connectors for external antennas
- A mounting bracket
- Two screws with wall plugs

External antennas

Connect external antennas through the MCX connectors on the IPBS2 before following the installation instructions in Installing the base station on page 80.

Safety instructions

For safe and efficient operation, follow the operating instructions and adhere to all warnings and safety precautions located on the product and this manual. Follow the operating instructions and adhere to all warnings and safety precautions located on the product and this manual.

- Only service persons must perform installation and service.
- The voltage and frequency of the mains power socket must match the voltage and frequency inscribed on the electrical rating label of the equipment.
- Never install telephone wiring during a thunderstorm.

Note:

Do not touch or punch the IPBS/RFP signal and power pairs as 48Vdc or 24Vdc is present on these wires at all times.

- Ensure that the base station installation conforms to relevant national installation rules.
- Disconnect all power sources before servicing the equipment.
- Use only approved spare parts and accessories. Non approved parts might not work and might cause damage or danger.
- Only approved power supplies according to valid editions of EN/IEC/CSA/UL/AU/NZS 60950 when the IPBS/RFPs are powered by local power supplies.

Safety symbols

For protection and to avoid damage to the IP-DECT system, you will find stickers with the following symbols:

Caution



Read and follow the safety rules and warning messages in this manual to prevent risk of damage to the equipment.

Caution ESD



Read and follow the handling instructions described in chapter ESD handling on page 73.
This safety symbol appears on boards which contain Electrostatic Sensitive Devices (ESD).
For handling these boards safely, see Protection against electrostatic discharge (ESD) on page 73.

Warning



Read and follow the safety rules and warning messages in this manual.
Hazardous voltages are present.
If the instructions are not followed, there is risk of electrical shock and danger to personal health.

Protection against electrostatic discharge (ESD)

Integrated circuits are sensitive to ESD. To avoid damage caused by ESD, service engineers and other people must handle equipment and boards carefully.

Electronic equipment has become more resistant to ESD, however, you might face situations where static electricity can build up. Such situations are caused by an increasing application of man–made fibres like nylon, acrylic, etc. which can generate ESD of 10,000 Volts and more.

For example, walking across a nylon carpet for a few feet can cause a person to be charged–up to more than 10,000 Volts of ESD.
Under these conditions, you can easliy damage a a system board or a (C)MOS device by touching the device. The device might be degraded and not totally defective, but the device might fail at a later date without apparent reason.

To make sure that equipment and parts are well protected during shipment, special packaging materials are utilized. System boards are shipped in anti–static bags and (C)MOS devices and other sensitive parts in small shielded boxes.

ESD handling

In the interest of quality and reliability, observe the following rules when handling system parts:

- Keep parts in their protective packaging until required.
- To return system parts like EEPROMS to the factory, use the protective packaging as described.
- Never underestimate the damaging power of ESD. Take special care in temperatures below freezing point and during very warm weather with low humidity. Ensure that environmental conditions remain within the limits specified in the component data sheets.

Important:
In the interest of quality and reliability, you may be refused return or exchange of system boards and other parts that are sent without proper protective packaging.

Safety Aspects

IP-DECT Base Station

The IP-DECT Base Station meets the valid editions of safety standard EN/IEC/CSA/UL/AU/NZS 60950-1. The system is a class III equipment for stationary wall mounting.

Regulatory Compliance Statements - EU/EFTA only

Permission and Conformity

We, Avaya GmbH & Co. KG, declare that the product line Avaya IP-DECT concurs with the basic requirements and other relevant provisions of EU Directive 1999/5/EU concerning radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity.

Intended use

This equipment is intended for connection to radio interfaces (DECT) of Avaya PABX systems.

It is compliant with the essential requirements of the EU-Directive 1999/5/EU (Radio and Telecommunication Terminal Equipment, R&TTE).

Due to the differences of the individual public networks and network operators this compliance does not by itself give an unconditional assurance of successful operation at every network termination point. For the time being we are not aware of any network on which the equipment will not work due to its design.

In the event of problems, you should contact your equipment supplier or your Avaya service.

The conformity declaration can be accessed at the following Internet address:

http://support.avaya.com/DoC

or search the index using the key term "Conformity".

CE.

Regulatory Compliance Statements (USA and Canada only)

FCC compliance statements

The equipment have been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. The equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.

However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment and the receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/tv technician for help.

Information to user

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) this device may not cause harmful interference, and

(2) this device must accept any interference received, including interference that may cause undesired operation.

IC Requirements for Canada

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la Classe B conforme á la norme NMB-003 du Canada.

Modifications

Any modifications not expressly approved by Avaya could void the user's authority to operate the equipment.

Exposure to radio frequency signals

This device complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. The antenna used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.

IP security

IP security terminology

SSL/TLS

Note:

Secure Socket Layer (SSL) has been renamed Transport Layer Security (TLS). TLS 1.0 is based on SSL 3.0/3.1. This document hereafter uses the term TLS.

TLS is a security mechanism based on cryptography. See Cryptography on page 77. TLS is used for encrypting communications between users and TLS-based Websites. The encryption prevents eavesdropping and tampering with any transmitted data.

TLS operates on the OSI Model Level 5 and uses PKI. For more information see Public Key Infrastructure on page 76.

Public Key Infrastructure

Public Key Infrastructure (PKI) is a component of Public Key Cryptography (PKC) that uses:

- Public Key Certificates. See Public key certificates (Digital Certificates) on page 76
- Certificate Authorities. See Certificate Authorities on page 77

Public key certificates (Digital Certificates)

Public Key Certificates are used for key exchange and authentication. The certificates are electronic document files that incorporate a digital *signature* to bind together a *public key* with an *identity* (information such as the name or a person or organization, their address, and other details.

The signature may be signed by a trusted entity called a Certificate Authority (CA). See Certificate Authorities on page 77.

The most common use of public key certificates is for TLS certificates. For example, https websites.

Certificate Authorities

A Certificate Authority or Certification Authority (CA) is a trusted entity that issues public key certificates. The certificates contain a public key and the identity of the owner. The CA asserts that the public key belongs to the owner, so that users and relying parties can trust the information in the certificate.

Certificate Signing Request (CSR) or **Certification Request** is a message that is generated and sent to a CA in order to apply for a TLS certificate. Before the CSR is created, a key pair is generated and the private key kept secret.
The CSR will contain the corresponding public key and information identifying the applicant such as distinguished name. The private key is not part of the CSR but is used to digitally sign the entire request. Other credentials may accompany the CSR.

If the request is successful, the CA will send back an identity certificate that has been digitally signed with the CA's private key.

A CSR is valid for the server where the certificate will be installed.

Cryptography

Cryptography is the encoding of messages to render the messages unreadable by anyone other than their intended recipient or recipients. Modern cryptography uses complex algorithms implemented on modern computer systems.

Cryptography is divided into the two general categories: Encryption and Authentication.

Encryption

Encryption is the scrambling of information so that unauthorized recipients cannot determine the original message by applying an encryption algorithm to the message plaintext producing ciphertext, or apparently random bits. With the correct key, a decryption algorithm converts the ciphertext back into plaintext. Public key algorithms use paired keys, one for encryption and the other for decryption.

Authentication

Authentication is the verification of a sender of a message. Authentication requires the message to be protected so it cannot be altered, usually by generating a *digital signature* formed by a hash of the message. Only the correct key can generate a valid signature.

Introduction to IP Security in IP-DECT

A secure system requires more planning than an unsecured system.

Secure Web Access (https)

For IP-DECT devices

- To ensure secure communications, https access should be enabled.
- Correspondingly, http access should be disabled

For more information see Configuring the HTTP settings on page 131.

TLS Certificates.

Security in Web-based applications rely on cryptography. Cryptographical systems are only as secure as their *keys. Key Management* a critical and often neglected concern. *TLS Certificates* have emerged as a clever way of managing large scale key distribution.

Certificate handling options

1. Default Device certificate

   This certificate is a self-signed certificate supplied with the device. Self-signed certificates provide only encryption, not authentication.

   For more information, see Default device certificate on page 135.

2. Self-signed certificates

   This certificate is for customers who do not plan to have their certificates signed by public or private CAs. Self-signed certificates provide encryption but do not provide authentication in all cases.

   For more information see Self-signed certificates on page 135.

3. Certificates signed by a Certificate Authority (CA)

   These certificates have two options:

   a. Certificates signed by the **customer's own CA**. Customers possessing the knowledge and infrastructure to house their own CA can build an internal enterprise CA, enabling them to sign or approve their own certificate requests. This would make the customer a private CA.

   b. Certificates signed by a **trusted public third-party entity/organization**. Only about a dozen issuers have the authority to sign certificates for servers worldwide. An example is VeriSign. To use a public CA for certificate approvals, you must connect the IP-DECT system to the Internet and obtain a fully qualified domain name.

   For more information see Certificate Signing Request (CSR) on page 137.

WARNING:
Este equipamento opera em caráter secundário, isto é, não tem direito à proteção contra interferência prejudicial, mesmo de estações do mesmo tipo, e não pode causar interferência a sistemas operando em caráter primário.

IP-DECT administrative functions

Configuration - HTTP

Use the HTTP Tab to configure the type of web access that should be allowed for the device. The HTTP tab includes a field for configuring https access.

For more information see Configuring the HTTP settings on page 131.

Configuration - Certificates

The *Certificates* tab lists the certificate used by web browsers to authenticate the identity of the device (Web server).

For more information see Certificates on page 133.

Configuration - Secure RTP

Secure RTP (SRTP) is used to encrypt the voice communication between the end user equipments.

Note:
SRTP is not supported when connected to IP Office.

Installing the Base Station

This section describes how to install the IPBS1 and IPBS2. To install the IPBS1 and IPBS2, fix the base station to a wall, a ceiling, a pole, or a beam. Use the mounting bracket included in the shipment. To fix the base station to a wall or ceiling, use the plugs and screws included in the shipment.

To fix the base station to a pole or beam, use a strap or a flexible metal band. This strap or band is not included in the shipment.

Note:

Do not fix the base station to metal surfaces. If you must, ensure a minimum distance of 1 meter between the base station and the metal surface. If this distance is not possible, use a base station with internal antennas.

Base station cables

Use a standard CAT5 unshielded ethernet cable with minimum 26 AWG copper conductors. You can also provide power the base station with this cable. Ensure that the installation personnel know how to crimp RJ45 connectors to a cable.

Note:

Since the distance between the base station and the wall is limited, you must use a RJ45 modular jack without cable retention.

Note:

Ensure that each base station has an extra length of cable, 5 to 10 meters, to facilitate moving of the base station from the currect location.

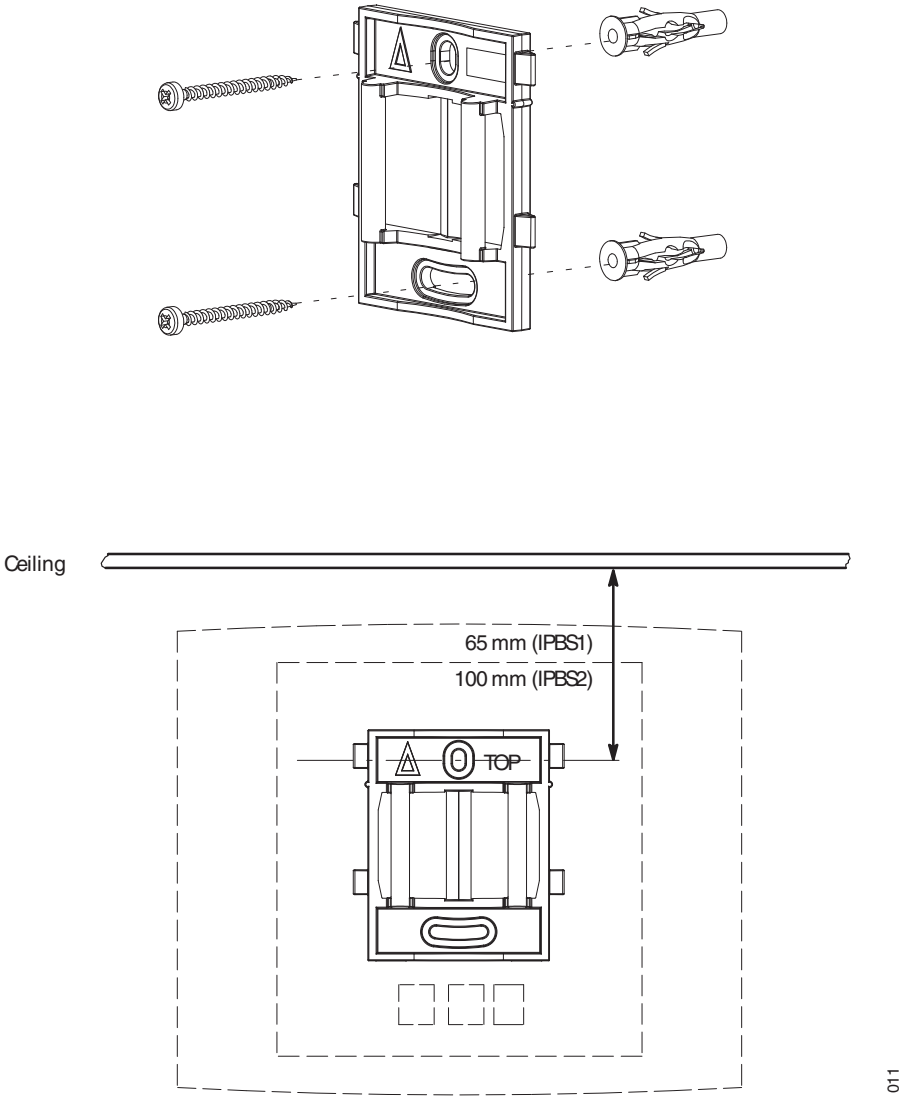
Installing the base station

You can mount the base station vertically or horizontally. Conform to the base station plan while mounting the base station. See Planning an IP-DECT system on page 43. Place the base station so that the base station does not face large metal objects such as large heating pipes.

Fixing the mounting bracket to a wall

1. Hold the mounting bracket with its flat side against the wall with the text ‘TOP’ upwards and mark the two holes. The minimum distance between the upper hole and the ceiling or any object above the base station must be at least 65 mm for the IPBS1 and 100 mm for the IPBS2. See figure 17. If the distance is less than 65/100 mm, you cannot slide the the base station on to the bracket.
2. Drill the two holes using a □ 6 mm drill, and insert the wall plugs included in the box.
3. Position the mounting bracket with its flat side to the wall and fasten it with the two ∅ 3.5 mm screws that are included in the box.

Figure 17: Fixing the mounting bracket to a wall



Fixing the mounting bracket to a ceiling

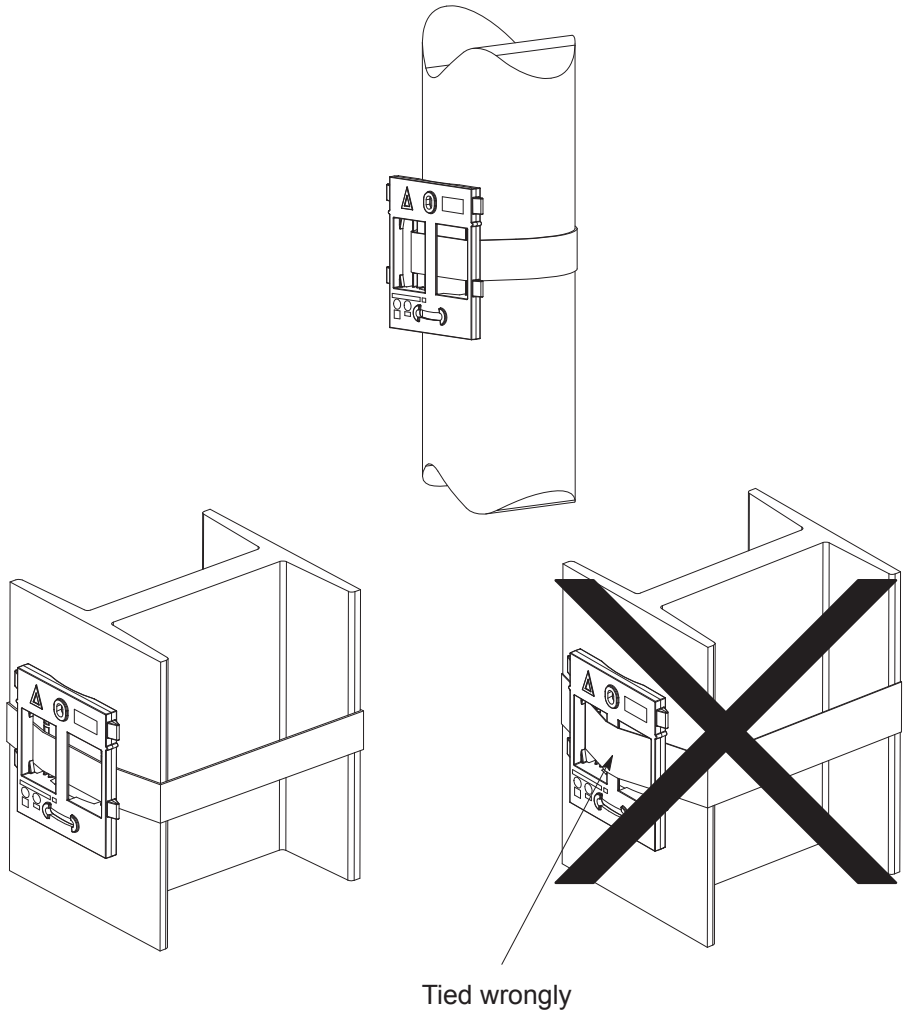
To fix a base station to a ceiling, follow the same method as for fixing to a wall. For more information, see Fixing the mounting bracket to a wall on page 81. To position the base station above a suspended ceiling, ensure that the front of the base station points downwards.

Fixing the mounting bracket to a pole or beam

To fix the mounting bracket to a pole (diameter ¡Ý 45 mm) or a beam (wider than 50 mm), use a strap or flexible metal band less than 30 mm wide. The strap or flexible metal band is not included in the box.

1. Fix the mounting bracket to a pole or beam using the metal band, see figure 18.

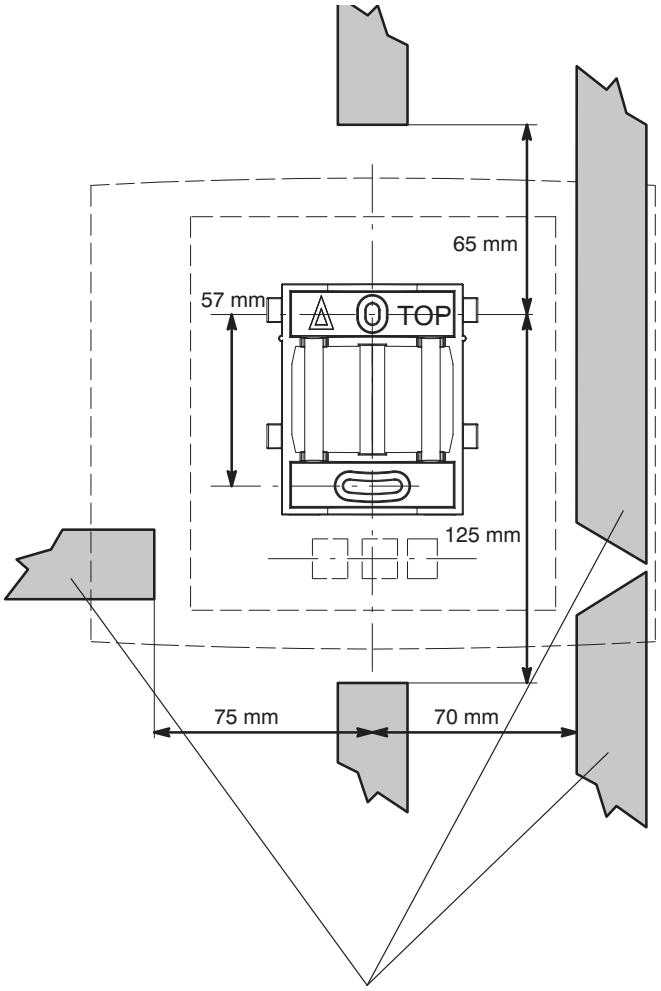
Figure 18: Fixing the mounting bracket to a pole or beam



Using the cable ducts for IPBS1

When the IPBS1 base station is mounted to the wall, you can route the wiring through the cable ducts. See figure 19 on page 83 to fix the cable duct to the wall in one of the shown positions.

Figure 19: Minimum distances between a cable duct and the mounting bracket



15 mm thick cable ducts

Securing the cable

For safety reasons secure the base station cable to a convenient point at about 30 cm from the base station. If for some reason the base station drops, it is secured by the cable.

Pinning

1. Cut the cable to the correct length and connect the cable to a RJ45 modular jack.
2. For more information on pinning the data jack of the IPBS1, see Pinning the IPBS cable on page 84.
3. For more information on pinning the data jack for the IPBS2, see Pinning the IPBS2 on page 85

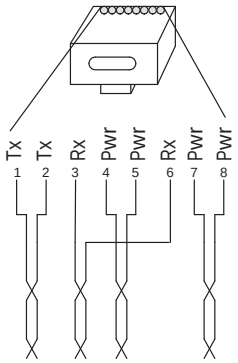
   Do **not** plug the connector in the base station yet.

Note:

Because the distance between the base station and the wall is limited, a RJ45 modular jack without cable retention must be used.

Pinning the IPBS cable

Figure 20: Connector pinning of the LAN/PoE connector, power feed over the spare cable pairs



RJ 45 Modular Jack

Figure notes:

Tx = Transmitter data pair

Rx = Receiver data pair

Pwr = Power pairs

Figure 21: Connector pinning of the LAN/PoE connector and power feed over the Rx/Tx data cable pairs.

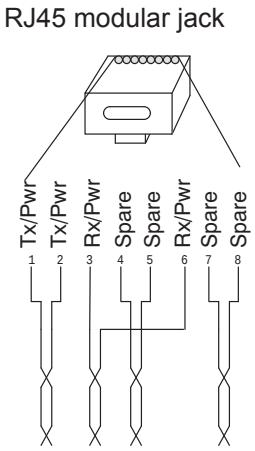


Figure notes:

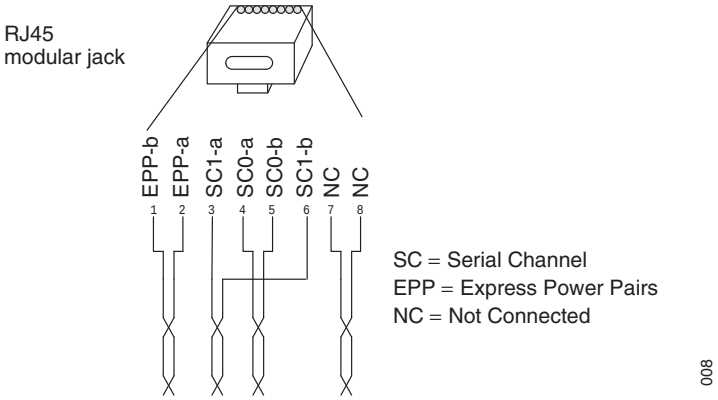
Tx/Pwr = Transmitter & power pair

Rx = Receiver & power pair

NC = Not connected

Pininng the IPBS2 (BS3x0)cable

Figure 22: Pinning the IPBS2



Important:
If you are using local power supply, the EPP cable pair must NOT be connected.

Connecting the Base Station cables

1. If the cables must enter the base station centrally from above, guide the cables through the recess in the middle of the base station. See Cables entering centrally from above on page 86.

Note:

Applicable to the IPBS1 only.

Figure 23: Cables entering centrally from above

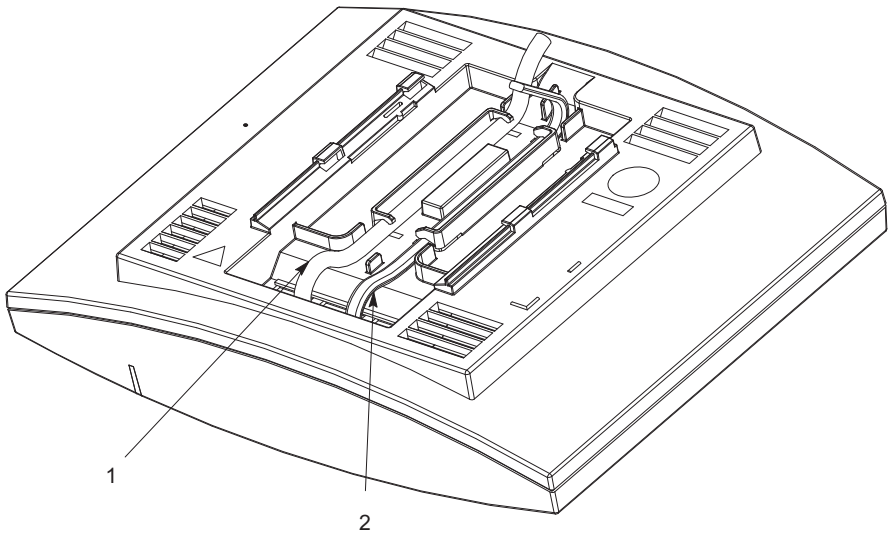


Figure notes:

1. Data cable

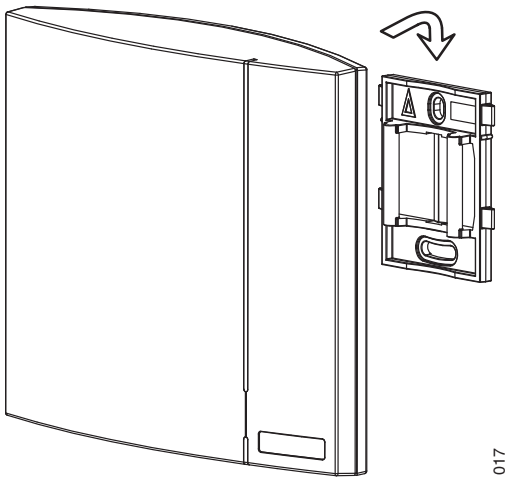
2. Power cable (if used)

2. Plug the modular jack of the data cable into one of the data/power connectors.
3. To use an AC-adapter:
   - Plug the modular jack of the AC-adapter into one of the data/power connectors.
   - Plug the AC adapter into a wall outlet.

Mounting the Base Station

1. Hold the base station flat against the mounting bracket and move the base station downwards until the base station clicks, see figure 24.

Figure 24: Mounting the base station IPBS1



Turning on the base station

To turn on the base station use of the following methods:

- Power over Ethernet (PoE) (applicable only to the IPBS)
- Power over Express Powering Pairs (EPP) and data pairs (only BS3x0 and DB1)
- A local power supply

Note:

Do not turn on the base station using two power supplies. Parallel powering does not harm the base station but can disturb the signalling.

Powering the IPBS over ethernet

The IPBS supports PoE, IEEE 802.3af, class 2. The IPBS power consumption is maximum 5W. But according to the PoE standard for class 2 the PoE power source allocates 7W to the IPBS. Factor in this information when you plan the power requirement of the IPBSs so that the power limit of the PoE power source is not exceeded.

The PoE standard supports:

1. Power over the Rx/Tx data pairs.
2. Power over the spare cable pairs.

The IPBS supports both power feed methods. The IPBS is not affected by change of the polarity.

Powering the BS3x0 and DB1over Express Powering Pair (EPP) and data pairs

When you power a base station remotely using the IPBL, the maximum length between the base station and the IPBL depends on the supply voltage, the number of twisted pairs used, and the wire size.

Note:

The maximum cable length for base stations connected to the IPBL must not exceed 1500 meters.

Powering the Base Station with a local power supply

You can powering the base station with a local power supply using the second data/power inlet on the base station. You can also power on the base station individually by an AC-adapter. The AC-adapter is provided with an 8-pin RJ45 plug that can be plugged into the *Power Supply* jack. For specifications, see AC-adapter on page 67.

Note:

Use only approved power supply according to valid editions of EN/IEC/CSA/UL/AU/NZS 60950 when you power the base station by a local power supply.

Installing and operating the IP-DECT Gateway (IPBL)

This section contains details for installing and operating the IP DECT Gateway also called the IPBL.

Note:

Before getting started, read the Safety Instructions Leaflet enclosed with the product.

Figure 25: IP DECT Gateway

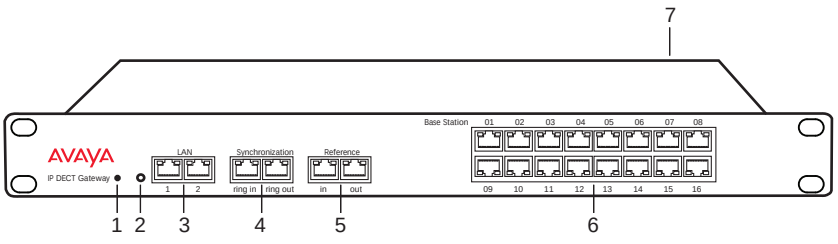


Figure 26: Placement of connectors, LED and button.

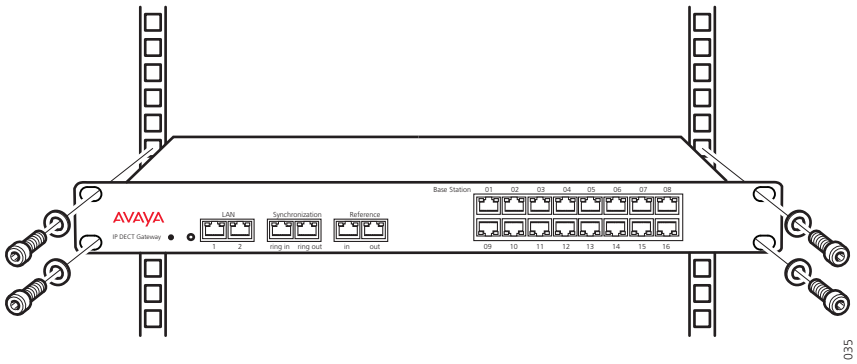
Pos	Name	Function
1	Reset	Button used to reset the IPBL.
2	Status LED	LEDs that indicate the status on the IPBL.
3	LAN	Port used to connect 10BASE-T/100BASE-T Ethernet connection. LAN1 port must be used in the IP-DECT system. The LAN2 port is for administration only. If you enable RSTP, both the ports are utilized by the system. See Enabling RSTP (only for IPBL) on page 142.
4	Synchronization	Interfaces used for synchronizing ring-in and ring-out.
5	Reference	Interfaces used to reference sync-in and reference sync-out .
6	Base Station 01-16	Interfaces used to connect ISDN UPN DECT base station.
7	Power Supply	Interfaces used for power connection (located at the rear of the IPBL).

Power supply

The power supply jacks are located at the rear of the IPBL. The IPBL can be powered with 110/230 VAC, 60/50 Hz. The power supply feeds both the IPBL and the connected RFPs.

Mounting the IP-DECT Gateway (IPBL)

Mount the product in a standard 19” rack according to the following figure.



Cable instructions for the IPBL

Pinning the cable for IPBL

All data cables used for the IPBL is standard CAT5 unshielded cable. Ensure that installation personnel know how to crimp these connectors to a cable.

Preparing the synchronization cable

1. The maximum cable length between two IPBLs must not exceed 2000 meters. Cut the cable to the correct length.
2. Connect the cable to an RJ45 modular jack.

Figure 27: Pin diagram for Sync IN cable connections

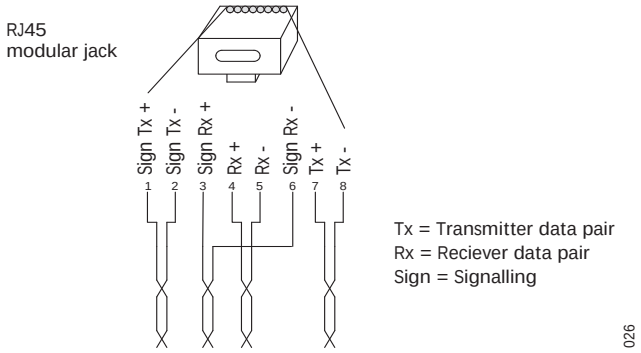
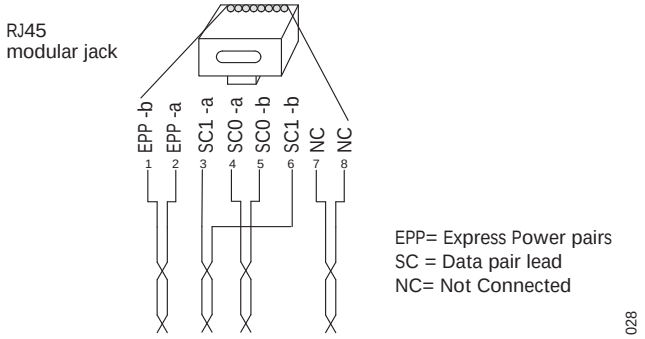


Figure 28: Pin Diagram for Sync OUT cable connections



3. Label the cable.

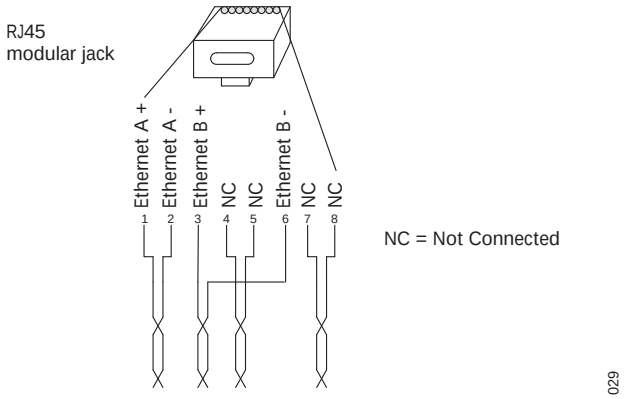
Preparing the LAN cable for IPBL

Note:

The TX/RX crossover/straight cable feature does not work for the IPBL. Connect a straight cable between the IPBL and the switch port.

1. Cut the cable to the correct length.
2. Connect the cable to a RJ45 modular jack.

Figure 29: Pin connections for the lan cable

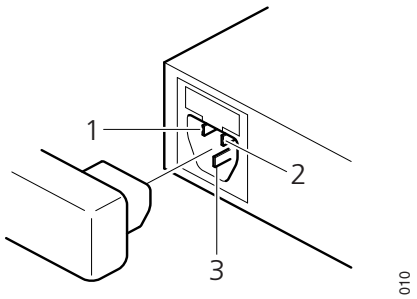


3. Lable the cable.

Powering the IPBL

The IPBL power supply connector is located at the rear. The power supply feeds both the IPBL and the connected RFPs. The IPBL is powered with 110/230 VAC, 60/50 Hz.

A 4A fuse protects the 110/230VAC (100 – 240 VAC) power input against overload.



The IEC 60320 type C14 (male) connector consists of:

- One - Live lead
- Two - neutral lead
- Three - Protective earth lead

Installing the IPBL

1. Install the IPBL in the standard 19-inch rack.
2. Connect the synchronization cables and the RFP cable as necessary.
3. Attach the power cable to a wall socket with protected earth and switch on the IPBL.
4. Connect the cables in the following order:

- Ethernet cable (A) LAN1 port must be used (LAN2 port is for administration only).

  If you enable RSTP, both the ports are utilized by the system. See Enabling RSTP (only for IPBL) on page 142
- Synchronization cable (ring sync, reference sync) (B)
- Base station cable (RFP cable)

Note:

The connected RFPs must not be connected to protective earth.

5. Monitor the total current consumption from the GUI.
6. Ensure that the current consumption does not exceed the following values:
   - Max current consumption is 1,9/0,9 A when supplied with 110/230 VAC.

Note:

The IPBL current consumption is 0.3 A .

Accessing the IPBL

You can access the IPBL through the IP network using a web browser. You can use the following browsers to access the web interface of the IPBL.

- Internet Explorer 7.x
- Firefox 3.x or later

The network administrator can reserve a fixed IP address for the IPBL on the DHCP server. A fixed IP addresss ensures that the device gets the same IP address if it restarts and the device can still communicate with other equipment.

You can use the name, ipbs-xx-xx-xx and ipbl-xx-xx-xx, where xx-xx-xx is the end of the MAC address. It is also accessed by entering http://xxx.xxx.xxx.xxx.

Note:

NOTE: The IPBL name is always ipbl-xx-xx-xx whether you use LAN1 (MAC xx-xx-xx-xx-xx) or LAN2 (MAC yy-yy-yy-yy-yy) is used.

Change the default password through the GUI.

Accessing the web interface of the IPBL without a DHCP Server

1. Connect the power cable to the interface and turn on the device.
2. Connect the computer and the Gateway's LAN1 port with an ethernet cable.
3. Ensure that the computer has an IP address within the same IP address range as the IPBL (192.168.0.1).
4. Perform a hardware reset by pressing the reset button.
5. The product will be assigned the IP address 192.168.0.1 and the netmask 255.255.255.0.
6. Enter the IP address http://192.168.0.1 in a web browser to access the Gateway's web interface.
7. Select **System Administration**.
8. Enter user name as **admin** and the password as **changeme**.
9. After the first startup, change the DHCP mode to **disabled**.

Accessing the Gateway in a network with a DHCP server

If the network has a DHCP server, the DHCP server assigns an IP address to the Gateway. The Gateway's MAC address can be found on the label on the box. The hexadecimal numbers (xx-xx-xx-xx-xx-xx) represent the MAC address.

1. Connect the power cable.
2. Connect the ethernet cable between the IP network and the Gateway's LAN1 port.

Note:

NOTE: In order to determine the IP address connect the computer to the same LAN (broadcast domain) as the Gateway.

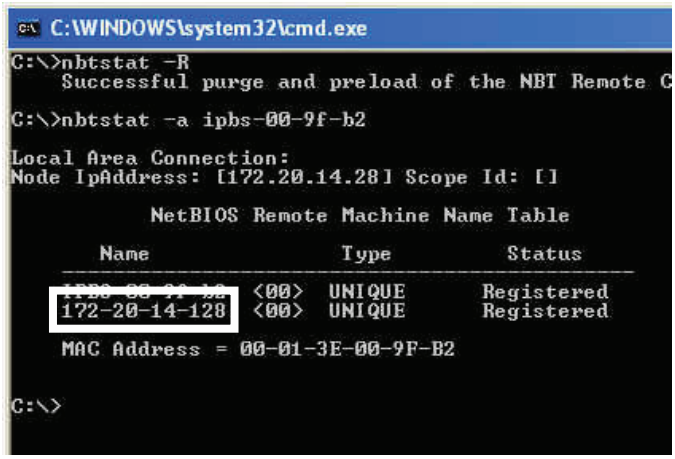
3. Open a **Command** window in Windows and enter the following commands:

```
C:\nbtstat -R

C:\nbtstat -a ipbl-xx-xx-xx where xx-xx-xx represents the last six
  characters of the MAC address.
```

The IP address is displayed in the highlighted white frame as in the following figure.

Figure 30: MAC and IP address using nbstat command



4. Enter http://xxx.xxx.xxx.xxx (where xxx.xxx.xxx.xxx is the determined IP address) in the web browser to access the web interface of the Gateway.

Configuration

Configure the IPBS and the IPBL using the web interface in the following order:

1. Configure the Master, see Configuring the Master on page 107.
2. Configure the Standby Master, see Configuring the Standby Master on page 109.
3. Configure the slaves/radios, see Configuring the Slave/Radio on page 110.

Requirements

To configure the IP-DECT system, you require:

- A personal computer (PC)
- A 10/100base-T Ethernet connection

Web browser requirements

The web browser must meet the following requirements:

- HTTP 1.1 protocol
- HTML 4.0 protocol
- XML/XSL Version 1.0

The GUI has been tested with Internet Explorer 7.x and Firefox 3.x, but can also be operated with other browsers in compliance with the requirements above.

Accessing the GUI

The GUI interface is accessed through a standard web browser. It is possible to use the name, ipbs-xx-xx-xx (IPBS1), ipbs2-xx-xx-xx (IPBS2) and ipbl-xx-xx-xx (IPBL), where xx-xx-xx is the end of the MAC address.

The IPBL name is always ipbl-xx-xx-xx regardless if LAN1 (MAC xx-xx-xx-xx-xx) or LAN2 (MAC yy-yy-yy-yy-yy) is used.

It is also accessed by entering http://xxx.xxx.xxx.xxx. In this address, xxx.xxx.xxx.xxx should be replaced with the IP address determined in 7.2.1 Determine the IP Address on page 40.

Access the GUI and change the default password as described in 7.2.2 Change the Default Password on page 42.

Note:

If the GUI cannot be accessed with Internet Explorer 8 or newer, check that the TLS 1.0 option is activated in the web browser under menu Tools > Internet Option > Advanced > Use TLS 1.0.

Determining the IP address

The factory setting of the DHCP mode for the LAN port is ***automatic***. At first power up, the IPBS/IPBL acts as a DHCP client. If the network has a DHCP server, the DHCP server assigns an IP address to the IPBS/IPBL. If the network does not include a DHCP server, the IPBS/IPBL can be assigned a predefined IP address.

Note:

After the first startup, change the DHCP mode from ***automatic*** to either ***client*** or ***off***, see Setting DHCP mode on page 140.

Use the IP address to reach IPBS through a Web browser. To determine the dynamically allocated IP address, you can use one of the following methods:

- In a network without a DHCP Server on page 97.
- In a network with a DHCP Server on page 98.

In a network without a DHCP Server

To determine the IP address in a network that does not have a DHCP server and the DHCP mode is set to automatic, that is the factory default use the following procedure:

Note:

If you have used the IPBS/IPBL before, restore the IPBS/IPBL to factory default settings by performing a long hardware reset, see Reset using the reset button on page 191.

1. Connect the IPBS/IPBL and the computer with a ethernet cable.

   Note:

   Use a power adapter for IPBS. For IPBL, use the LAN1 port.

2. Ensure that the computer has an IP address in the range of 192.168.0.2 to 192.168.0.254 This range is the same range as the IPBS/IPBL.
3. Perform a hardware reset by pressing the reset button. The IPBS/IPBL is then assigned the IP address 192.168.0.1 and the netmask 255.255.255.0.
4. Enter http://192.168.0.1 in the browser address field to access the IPBS/IPBL GUI.
5. After the first startup:
   - On the IPBS: Select LAN > DHCP
   - On the IPBL: Select LAN1 > DHCP

6. In the Mode drop-down list, change the DHCP mode from ***automatic*** to disabled. See Setting DHCP mode on page 140.

In a network with a DHCP Server

The MAC address for the IPBS can be found on the label on the box and on the label on the backside. The mac number for the IPBL can be found on a label on the box.The hexadecimal numbers (xx-xx-xx-xx-xx-xx) represent the MAC address.

Note:

Use LAN1 port for the IPBL.

Note:

To determine the IP address using this method, you must have a PC with MS Windows. You must connect the PC to the same network domain as the IPBS/IPBL.

To determine the IP address if the network has a DHCP server.

Note:

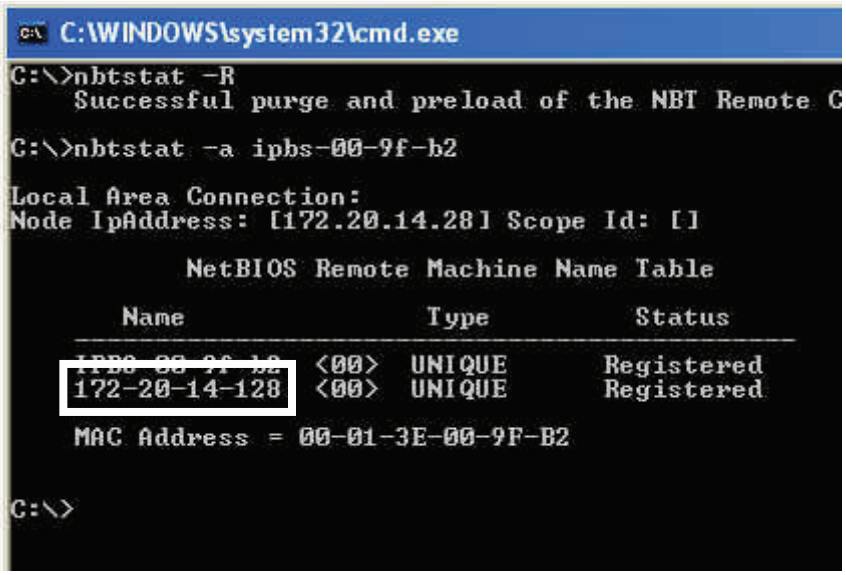
If you have used the IPBS/IPBL before, you must restore the IPBS/IPBL to factory default settings by performing a long hardware reset. See Reset using the reset button on page 191. Then remove the power supply cable and connect it again.

1. Open a command window on the PC and enter the following commands:

- C:\>nbtstat -R
- For IPBS1: C:\>nbtstat -a ipbs-xx-xx-xx
- For IPBS2: C:\>nbtstat -a ipbs2-xx-xx-xx
- For IPBL: C:\>nbtstat -a ipbl-xx-xx-xx

Where xx-xx-xx should be replaced with the last 6 hexadecimal digits of the MAC-address. Replace xx-xx-xx with the last 6 hexadecimal digits of the MAC-address.In case of IPBL, enter "ipbl-xx-xx-xx".
With IPBS2 use the command: **C:\ nbstat -a ipbs2-xx-xx-xx**
The command window displays the IP address. See the white frame in figure 31.

Figure 31: Determine the IP address



2. To access the GUI, enter http://xxx.xxx.xxx.xxx in the browser address field where xxx.xxx.xxx.xxx is the determined IP address.
3. After the first startup of the IPBS/IPBL:

- On the IPBS: Select LAN > DHCP
- On the IPBL: Select LAN1 > DHCP

In the Mode drop down list, change the DHCP mode from ***automatic*** to either ***client*** or disabled (***off***). See Setting DHCP mode on page 140.

Changing the default password

1. Enter the determined IP address in *Determining the IP address* in the web browser address field.
2. Select **General** > **Admin**.
3. Enter user name and password in the dialogue box.
   The default user name is: admin.
   The default password is: changeme.
4. Enter a user name in the **User Name** text field.
5. Enter a password in the **Password** text field. Repeat the password in the second text field.
6. Click **OK**.

GUI Web Access

Login page

When accessing the IPBS/IPBL through a web browser the initial page is the login page. This page has two hyperlinks: **System Administration** and **User Administration**.

Note:

Logging out of the IPBS/IPBL application is done by closing the Internet Explorer, to be completely logged out.

Access levels

Three types of web users (or *Access Levels*) are authorized to access the IPBS/IPBL:

- Auditors
- User Administrators
- System Administrators

The following table lists the different types of access levels:

Access Level	Authorization	Login hyperlink on login page [1]	Related information
Auditors	• Read access to device parameter settings. • Ability to generate Service Reports.	System Administration	Auditors on page 101
User Administrators	• Abilty to add, update, and remove users.	User Administration	User Administrators on page 101
System Administrators	• Write access to all device parameter settings. For example IP addresses, software upgrades. • Ability to assign and modify access to other System Administrator and User Administrator account settings • Ability to add, update, and remove users	System Administration	System Administrators on page 102

1. Users must use the hyperlink related to their access level. You cannot use a login link that is not related to your access level.

Auditors

Auditors have read access to device parameter settings but are not authorized to update those settings. Auditors are also allowed to generate Service Reports through **Administration** > **Diagnostics** > **Service Reports**.

The login steps for an auditor follow the steps of a normal system administrator login. for more information, see System Administrators on page 102.

User Administrators

The IPBS and the IPBL do not have preinstalled user administration accounts. Therefore, the system administrator must first create a user administration account. See System Administrators on page 102. If you require additional user administration accounts, ensure that a system administrator creates these accounts. For more information, see Managing User Administrators on page 104.

User administrators can only administer users. User administrators can view but not create or manage other user administrator accounts.

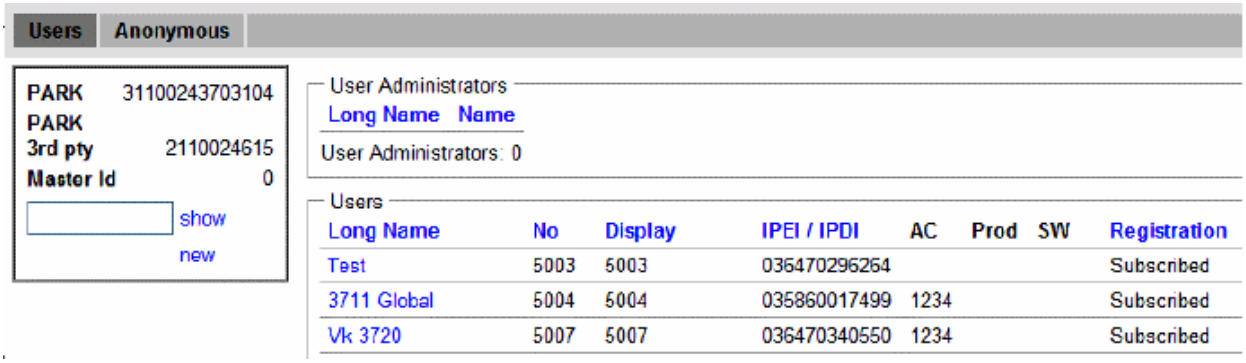
Logging in as User Administrator

To log in as a user administrator:

1. Reach the device GUI using a web browser. See Accessing the GUI on page 96.
2. Click the link labeled **User Administration**.
   The browser displays a login window.
3. Enter the user name and password for a user administrator.
4. Click **OK** to log in.
5. Click the show link. The browser displays the User Administration.

   See the following figure for a sample User Administration page.

Figure 32: User Administration Page Sample



The right side of the page displays two list sections:

- **User Administrators** in the upper right section.

  Note:

  This section is read-only since a user administrator cannot manage other user administrators. See Managing User Administrators on page 104.

- **Users** in the lower right section. See Adding users on page 112.

System Administrators

IPBS/IPBL devices are factory delivered with a default system administrator account.

Logging in as System Administrator

To log in as a system administrator:

1. Reach the device GUI using a web browser. See Accessing the GUI on page 96.
2. Click the link labeled **System Administration**.

   The system displays a login window.
3. Enter user name and password for a system administrator.
4. Click **OK** to log in.

Modifying the default System Administrator Account

You can modify the default account but cannot delete it.

1. Log in as system administrator. See Logging in as System Administrator on page 102.
2. Select **Configuration** > **General** > **Admin**.
3. Configure the following settings:

Field name	Description
• Device Name	Enter a description for the device.
• User Name	Enter a login user name.
• Password	Enter a password.
• Confirm Password	Confirm the password.

Note:

Changing the password does not ensure that the setting is saved. To save the settings, update the user name and password at the same time.

4. Click **OK**.

Additional Administrator Accounts

The **Additional Administrator Account** section on the lower part of the page displays a list of existing additional system administrator accounts.

Moving administrator accounts when upgrading to Edition 3

When upgrading an IPBS software Edition 1, 2, or 3 to Edition 4 above, the existing system administrator accounts remain configured locally in the IPBS(s). Avaya recommends that you configure the system administrator accounts centrally by moving the accounts to the Kerberos server to prevent a potential security risk.

To create additional administrator accounts, you must configure the Kerberos server. See Centralized management of Administrator or Auditor Accounts using Kerberos on page 117.

To move the system administrator accounts to the Kerberos server:

1. On each IPBS where system administrator accounts are configured locally:
   a. Select **General** > **Admin**.
   b. Go to the Additional Administrator and Auditor Accounts section.
   c. Write down each accounts configuration data, such as the user name, password (when known), and role.
2. On the Kerberos server, do the following:
   a. Select **General** > **Kerberos Server**.
   b. Go to the Users section and enter the configuration data that you wrote down down in step 1 for each account.
   c. Click **OK**.
3. For each IPBS where system administrator accounts are configured locally, delete the local system administrator accounts:
   a. Select **General** > **Admin**.
   b. Go to the Additional Administrator and Auditor Accounts section.
   c. For each account row, select the **Delete** check box.

Creating an Additional Account

To create an additional administrator account:

1. Log in as system administrator. See Logging in as System Administrator on page 102.
2. Select **Configuration** > **General** > **Kerberos Server**.
3. On the next free account row in the Users section:
   a. Enter a user name.
   b. Enter a password.
   c. Enter the password again.

d. Select **Administrator** or **Auditor** in the drop-down list. See Access levels on page 100 for a description of access levels.

4. Click **OK**. The system creates the account row.

Modifying an Additional Account

To modify an additional administrator account:

1. Login as system administrator. See Logging in as System Administrator on page 102.
2. Select **Configuration** > **General** > **Kerberos Server**.
3. On an existing account row in the Users section:
   a. Enter a new user name.
   b. Enter a new password.
   c. Enter the password again.
   d. Select **Administrator** for System Administrator or **Auditor** in the drop-down list. See Access levels on page 100 for a description of access levels.
4. Click **OK**. The system updates the account row.

Deleting an additional account

To delete an additional administrator account, do the following:

1. Login as system administrator. See Logging in as System Administrator on page 102.
2. Select **Configuration** > **General** > **Kerberos Server**.
3. On the row to be deleted, select the **Delete** check box.
4. Click **OK**. The system deletes the account row.

Managing User Administrators

Creating a User Administrator

The IPBS/IPBL is not supplied with preinstalled user administration accounts. Therefore, a system administrator must create the first user administration account. If additional user administration accounts are required, ensure that a system administrator creates these accounts.

1. Log in as System Administrator. See Logging in as System Administrator on page 102.
2. Select **Administration** > **Users**.
3. Click **Show**.

   The browser displays a User Administration page. See User Administration Page Sample on page 101 for a sample page.
4. Click the **new** hyperlink. The browser opens a window.
5. Select the **User Administrator** radio box. The window layout transforms.

6. Enter the long name.
7. Enter a short user name.

   Note:
   Use this field is used for logging in.
8. Enter a password.
9. Confirm the password.
10. Click **OK**.

Viewing and modifying a User Administrator

1. Log in as System Administrator. See Logging in as System Administrator on page 102.
2. Select **Administration** > **Users**.
3. Click **Show**.

   The browser displays a two-part list page. The upper part displays the user administrator accounts and the lower part displays the user accounts.
4. In the **User Administrators** section, click on a hyperlink below the **Long Name** heading. The browser displays a detail window.
5. Select/Edit any of the following settings as required:
   - Long Name
   - Name

   Note:
   Use this field is used for logging in.
   - Password
   - Confirm Password
6. Click **OK**.

Deleting a User Administrator

1. Log in as System Administrator. See Logging in as System Administrator on page 102.
2. Select **Administration** > **Users**.
3. Click **Show**.
4. In the **User Administrators** section, click on a hyperlink below the **Long Name** heading. The browser displays a details window.
5. Click on **Delete**.

   The User Administrator is deleted and the details window is closed.

Simplified GUI

Note:

The simplified GUI feature is applicable to the IPBS only. You require the Advanced View on the IPBS Master and Standby Master to configure an IP-DECT system connected to Communication Manager.

The simplified Graphical User Interface (GUI) makes it very easy to configure small IP-DECT systems.In the basic administration interface, the required configuration settings are kept to a minimum, and you can only see the GUI pages that are required for basic configuration.

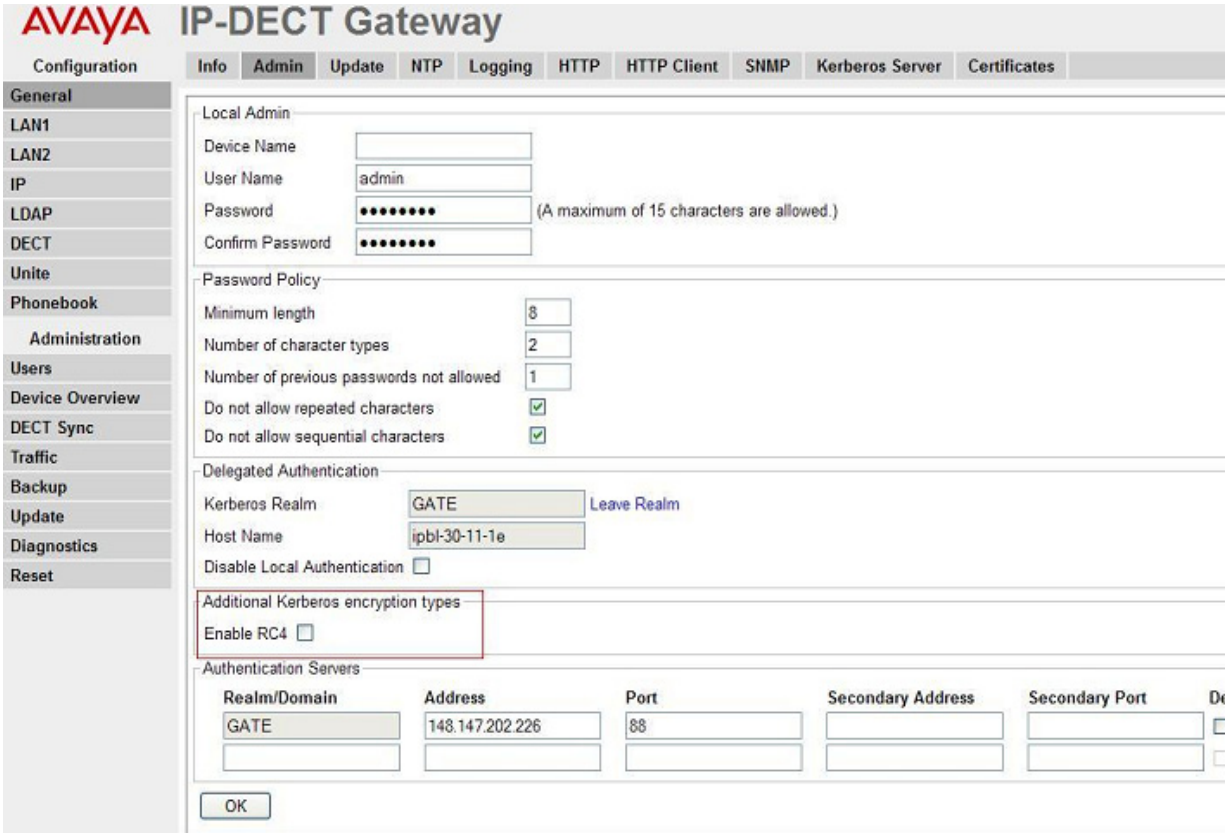
The basic administration interface is the default setting for Compact IPBS.

Changing the interface to advanced view

To change the basic administration interface to the advanced view:

1. Select **General** > **Admin**.
2. In the **Administration Mode** section, select the **Show Advanced Options** check box.
3. Click **OK**.
4. Refresh the web browser to make the hidden sub menus and tabs visible.

Figure 33: Configuring Simplified GUI



Changing the interface to basic view

To change the advanced administration interface to the basic view:

1. Select **General** > **Admin**.
2. In the **Administration Mode** section, clear the **Show Advanced Options** check box.
3. Click **OK**.
4. Refresh the web browser to decrease the number of visible sub menus and tabs.

Configuring the Master

1. Determine the address and access the GUI. See Accessing the GUI on page 96.
2. Change the default password. See Changing the default password on page 99.
3. Configure LDAP user name and password, mark the *Write Access* check box. See Configuring LDAP Server on page 145.

4. Set a static IP address and set DHCP to off, See Setting a static IP address on page 141.
5. Set the mode to Master. See Selecting Mode on page 154.
6. Reset to restart the IPBS in Master mode. See Reset on page 190.
7. Select **DECT** > **System** and enter the password.
8. Select the system name and password. See Changing the system name and password on page 149.
9. Set the default language. See Setting the default language on page 150.
10. Select the supplementary services. See Configuring Supplementary Services on page 153.
11. Set the frequency band. See Setting the frequency band on page 152.
12. Configure the Master ID. See Configuring Master ID on page 155.
13. Select the PBX. See Configuring IP-PBX on page 155.
14. Set the Master IP address to 127.0.0.1. See Entering the IP address to the PARI Master on page 162.
15. Reset and restart the IPBS/IPBL in Master mode. See Reset on page 190.

    If you cannot access the Master from a certain PC after the reset;

    - Open a command window in windows by selecting **Start** > **Run** and enter `cmd` in the **Open:** text field.
    - Enter the following commands

      arp -d (Delete the *arp* cache)

      nbtstat -R (Empty the *nbtstat* cache)
    - Restart the we browser.
16. Select supplementary services. See Configuring Supplementary Services on page 153.
17. Assign PARI. See PARI on page 163.
18. Enter SARI. See SARI on page 164.
19. Enter the AIWS2 IP address. See Configuring messaging on page 169, Device management on page 169 and Configuring the location on page 169.
20. Configure air synchronization. See Configuring air synchronization on page 164.
21. Enter the Time Server address. See Configuring the NTP settings on page 128.
22. Reset the system so that the configuration changes take effect. See Reset on page 190.

For more detailed information, see the corresponding subsection in Operation on page 115.

Configuring the Standby Master

Ensure that you have a Standby Master in the IP-DECT system. For more information, see the corresponding subsection in Operation on page 115.

Note:

Make or change the configuration of the Standby Master only when the Master is running.

1. Determine the address and access the GUI. See Accessing the GUI on page 96.
2. Change the default password. See Changing the default password on page 99.
3. Configure LDAP replicator, enter the IP address, user name and password to the LDAP server. Alternative LDAP server must not be entered. Select the **Enable** check box. See Configuring LDAP Replicator on page 147.
4. Set a static IP address and set DHCP to off. See Setting a static IP address on page 141.
5. Enter system name and password, this should be the same system name and password as in the Master. See Changing the system name and password on page 149.
6. Enter the Primary Master IP Address.
7. Set the mode to Standby Master. See Selecting Mode on page 154.
8. Configure the Master ID. See Configuring Master ID on page 155.
9. Select PBX. See Configuring IP-PBX on page 155.
10. Enter Master IP address. See Entering the IP address to the PARI Master on page 162.
11. Select supplementary services. See Configuring Supplementary Services on page 153.
12. Assign PARI, see PARI on page 163.
13. Configure air synchronization. See Configuring air synchronization on page 164.
14. Enter AIWS IP address. See Configuring messaging on page 169, Device management on page 169 and Configuring the location on page 169.
15. Enter the Time Server address. See Configuring the NTP settings on page 128.
16. Configure the LDAP replicator and enter the IP address, user name, and password to the LDAP server. Write access is required for the Standby Master replication. New users in the IP-DECT system must be created on the IPBS Master holding the database even if the LDAP write is configured for the Standby Master. Do not enter the Alternative LDAP server. Select the **Enable** check box. See Configuring LDAP Replicator on page 147.
17. Enter the AIWS IP address. See Configuring messaging on page 169, Device management on page 169 and Configuring the location on page 169.
18. Reset in order to make the configuration changes take effect. See Reset on page 190.

    If you cannot access the Standby Master from a certain PC after the reset;

- Open a command window in windows by selecting **Start** > **Run** and enter `cmd` in the **Open:** text field and enter the following commands:

  arp -d (Delete the *arp* cache)

  nbtstat -R (Empty the *nbtstat* cache)

- Restart the browser.

Configuring the Slave/Radio

Note:

After you configure one slave, you can save the configuration and upload the configuration to the other slaves in the system.

1. Determine the address and access the GUI. See Accessing the GUI on page 96.
2. Change the default password. See Changing the default password on page 99.
3. Set DHCP mode to **Client**. See Dynamic IP address using DHCP on page 141.
4. Enable the radio on the IPBS/IPBL.

   If the radio acts as a Standby Master, perform the following: Configure the LDAP replicator, enter the IP address, user name, and password to the LDAP server. The alternative LDAP server is not required. Read only access is sufficient for the Standby Master. Select the **Enable** check box. See Configuring LDAP Replicator on page 147. For normal radios LDAP replication is not recommended.
5. Set the mode to Slave. See Selecting Mode on page 154.
6. Enter the system name, the password, and the Master and Standby Master IP addresses in the **DECT** > **Radio** tab. See Enter Entering the IP address to the PARI Master on page 162. The system name and password must be the same system name and password as set in the Master. See Changing the system name and password on page 149.
7. Configure air synchronization. See Configuring air synchronization on page 164.
8. Enter the Time Server address. See Configuring the NTP settings on page 128.
9. Reset in order to make the configuration changes take effect. See Reset on page 190.
10. Save the configuration of the Slave. See Backing up on page 182.

Configure the rest of the IPBS following the steps below:

Note:

You can upload the same configuration to all slaves only if the DHCP is set to client.

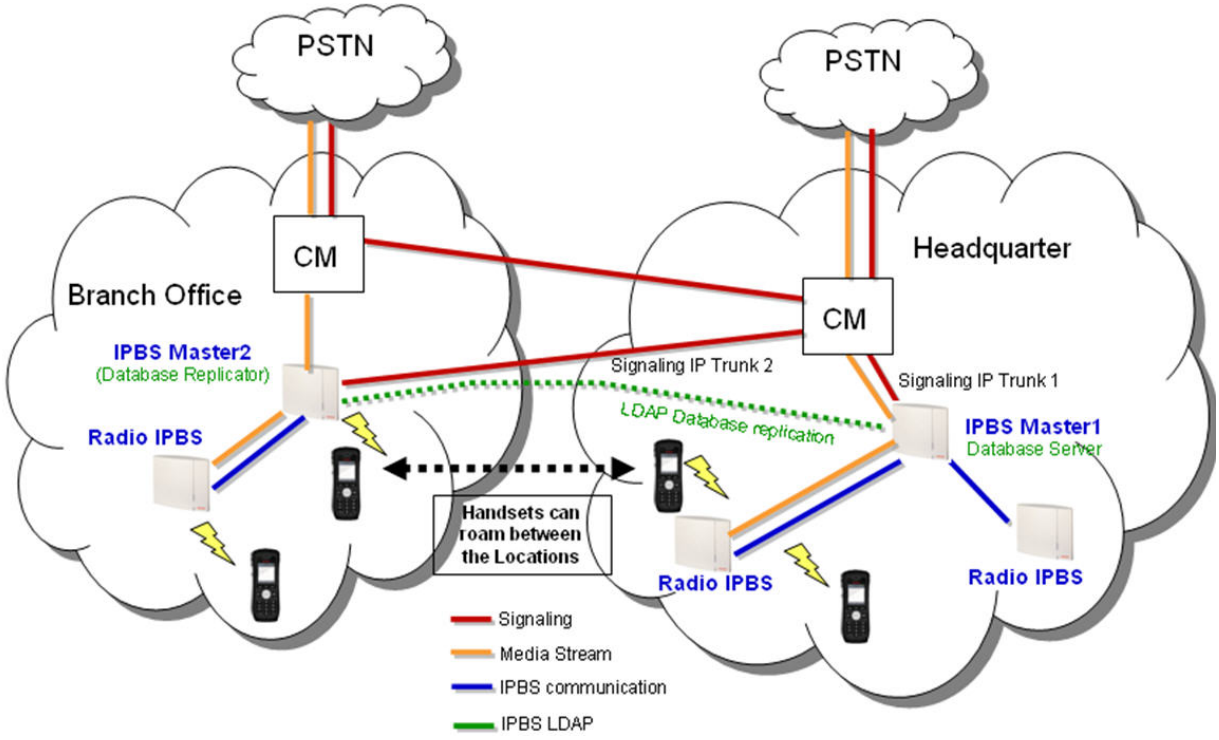
11. Determine the address.
12. Select **Update** > **Config** and browse to the previously saved configuration. Click **OK**.

13. Reset in order to make the configuration changes take effect. See Reset on page 190.
14. Repeat step 11 to step 13 for all Slaves.

For more detailed information, see the corresponding subsection in Operation on page 115.

Multibase Station Master configuration

Multi IP-DECT Master configuration



If you have multiple offices running one common IP-DECT system, ensure that you have one IPBS Master at each location (coverage area). The coverage areas of different locations must not overlap. The IPBS Master1 in the main location holds the DECT database including the system information data as System name, password, SARI, and user subscription data. The IPBS Master1 is the LDAP server of the IP-DECT system. The IPBS Master2 is a LDAP Replicator of the DECT database. Ensure that you grant write access to the LDAP database for the IPBS Master2 LDAP Replicator. Otherwise, roaming between the locations will not be possible. You alsp require write access to be able to subscribe handsets and modify user data in the Branch office. You can create new users only on the database server IPBS Master1 in the Main Location.

Roaming between the different locations is possible for all the handsets. Remember handover will not be possible between the two locations if you have overlapping coverage areas. Handover is only possible within the same IPBS Master.

In addition to the basic configuration for the IPBS Master, perform the following steps for a Multi Base Station Master system:

On IPBS Master1:

- In **LDAP > Server** tab, create a user with write access.

On IPBS Master2:

- In **DECT > System**, use same system name, password, subscription, and authentication settings as in IPBS Master 1 to get a common system.
- In **DECT > Radio**, use the same system name as in the DECT System.
- In **DECT > Master**, configure an individual Master ID for each IPBS Master in the range of 0 and 250. Use Master ID “0” for IPBS Master1, which is the LDAP server of the IP-DECT system. All further IPBS Masters doing the LDAP replication should use a Master ID from 1 to 250. A standby Master must use the same Master ID as the corresponding IPBS Master.
- In **DECT > SARI**, do not configure any value. SARI is part of the IP-DECT database and is configured automatically when the LDAP replication is enabled. Use the same SARI value in each IPBS Master that is part of the common DECT system.

  Important:
  Using a different SARI value causes invalid subscriptions for all the subscribed devices. Changing the SARI in one of the IPBS Masters changes the SARI on all other IPBS Masters using the same LDAP database as well.
- In **DECT > PARI**, you can use the same PARI value as used in IPBS Master1 if you do not have an overlapping Coverage area of the two locations. If you have an overlapping coverage area of both locations, you must use different PARI values.
- In **LDAP > Replicator**, enable replication of the IPBS Master1, use the user with write access.

Adding users

You can register cordless telephones in two ways:

- Use the telephone to automatically associate the IPEI number to a user. See Registration on page 113.
- Enter the IPEI number of the telephone manually. See Performing individual registrations on page 114.

  You can find the PARK to subscribe the DECT handsets on the user page of the IPBS Master web interface. Use the PARK for the third-party devices to subscribe other DECT GAP/CAP devices.

Note:

You cannot subscribe telephones on a base station that is busy with 8 active calls. Subscription will fail in this case due to system limitations. Change to another base station or wait until a call has ended.

Registration

The system automatically assigns the IPEI to a user. IPEI is the unique identification number of the telephone. You do not have to enter the IPEI number manually.

Adding users in the IP-DECT System

1. On the **Administration menu**, select **Users**.
2. Click **New**.
3. Enter the following information in the corresponding text fields, leaving the **IPEI** and the **Auth. Code** text fields empty:

Field name	Description	Max. characters
• Long Name	The name of the user, need to be unique throughout the system. This is the name presented in a called party´s display, unless this is configured in the IP-PBX.	30
• Display Name	Optional, will be shown in the handset display when the handset is idle.	30
• Name	Optional, the user name.	30
• Number	Mandatory, the phone number extension, need to be unique throughout the system.	30
• Password	Optional, is used for registration towards the gatekeeper.	30

4. Click **OK**.
5. Repeat step 2 to step 4 for all users.

Assigning cordless telephones to users

1. Select **DECT** > **System**.
2. Enable anonymous registration by selecting **With System AC** in the **Subscriptions** drop-down list.
3. Click **OK**.
4. Perform an "over air subscription" using the system Authentication Code.
   The telephones' IPEI/IPDI number appears in the Anonymous list.
   To view the list: Select **Users > Anonymous**.

5. Assign the Portable Device to any user, subscribed or unsubscribed, on any Master defined in the system. To assign the Portable Device, go off hook and dial the desired Master ID, extension and optional individual AC code and then hang up. The master ID can be found on the Users page of the IPBS or in **DECT** > **Master**. You must use the Master ID of the currently connected IPBS master in a Multi Base Station Master scenario.

   Example where 0 is the Master id, 200 is the extension and 1234 is the AC code dial, *0*200*1234#.

   Note:

   When you use an AC code, start with the star sign (*) and end with the pound sign (#). Otherwise, skip the *# characters. If the user is already assigned to a Portable Device, the user is moved to the anonymous list when logging in a new Portable Device. It is recommended to go off hook as the first step. When dialling the login or logoff sequence in on hook mode and pressing off hook at the end of the sequence, the dialled digits will be added to the call list. Therefore, the individual AC can be found in clear text as well.

6. Repeat step 4 to step 6 for all telephones.
7. Under the Configuration menu, select **DECT > System**.
8. Disable anonymous registration by selecting **Disable** in the **Subscription** drop-down list.
9. Click **OK**.

Performing individual registrations

1. Select **Users**.
2. Click **New**.
3. Enter the following information in the corresponding text fields:

Field name	Description	Max. characters
• Long Name	Mandatory, the name of the user, need to be unique throughout the system. This is the name presented in a called party´s display, unless this is configured in the IP-PBX.	30
• Display Name	Optional, will be shown in the handset display when the handset is idle.	30
• Name	Optional, the user name.	30
• Number	Mandatory, the phone number extension, need to be unique throughout the system.	30
• Password	Optional, is used for registration towards the gatekeeper.	15
• IPEI / IPDI	Mandatory, the unique identification number of the handset.	

- Auth. Code — Optional, the individual authentication code for this user. Automatically created by default. Can be modified manually.

4. Perform an "over air subscription" using the individual authentication code.
5. Click **OK**.

Logout/Login for users

This section describes how to logout and login users to the IP-DECT system. For example, when using a shared Portable Device for shift workers.

Logging out users

To logout the Portable Device for any subscribed user in the system, dial the supplementary services feature, optional individual AC code and hang up. See Configuring Supplementary Services on page 153.

Example: If #11*$# is the feature for logout and 1234 is the AC code dial #11*1234#.

Logging in users

To log in a user, see Assigning cordless telephones to users on page 113.

Operation

This section describes the settings in the Configuration and Administration menu, each subsection represents a sub menu to the Configuration and Administration menu.

Some changes require a reset in order to take effect. It is possible to do several changes before resetting the IPBS/IPBL. The following sections show screenshots from the IPBS.

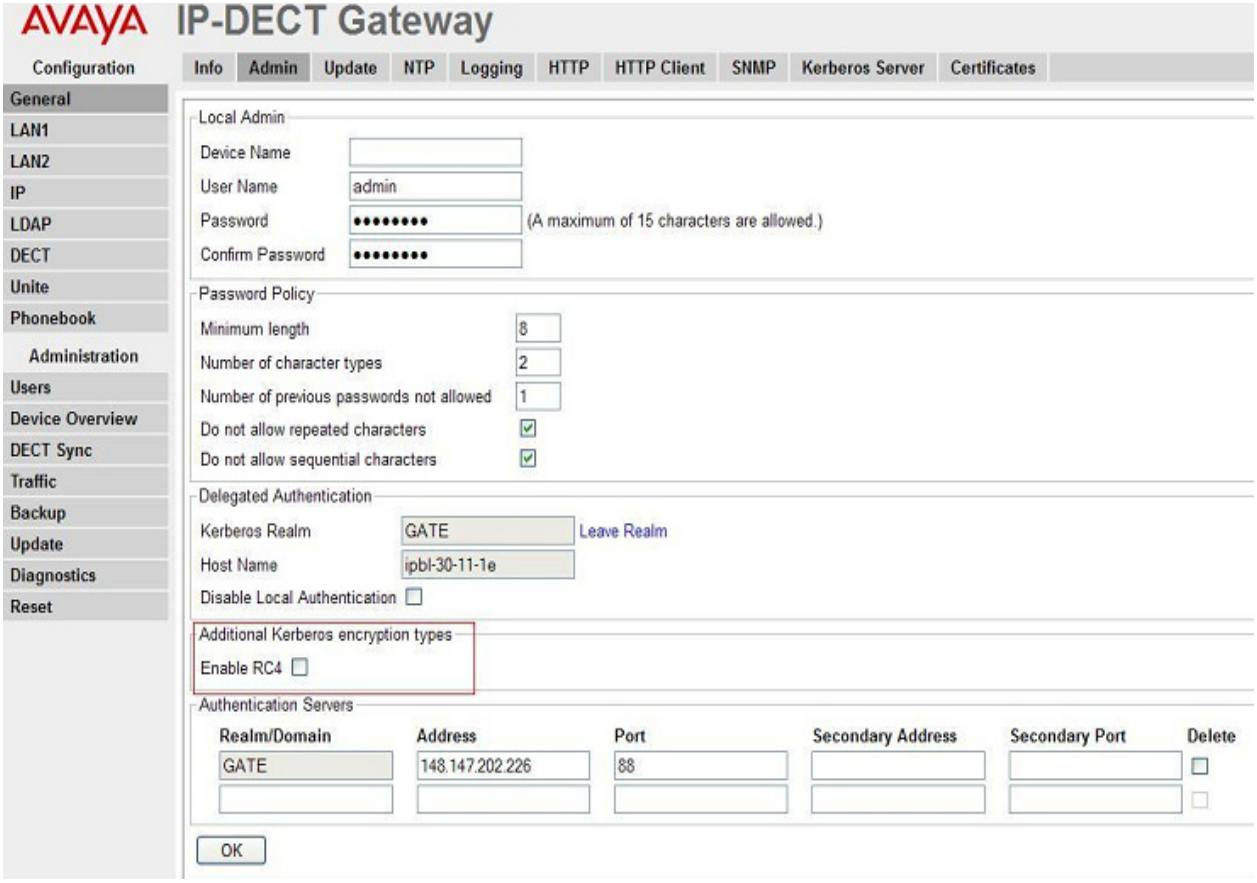
General

This section describes the following configurations and settings.

- Change the user name and the password
- Name the equipment
- Configure automatic firmware update

- Configure the NTP settings
- Configure Logging
- Configure the HTTP settings

Figure 34: Assigning a name, username, and password.



Changing user name and password

You require the user name and password to gain access to the IPBS through the web GUI.

1. Select **General** > **Admin**.
2. Enter a user name in the **User Name** text field.
3. Enter a new password in the **Password** text field. Repeat the password in the second text field.
4. Click **OK**.

Naming the IPBS/IPBL

You can assign a name to each IPBS/IPBL. Assign a descriptive name, for example, IPBS/IPBL location.

1. Select **General** > **Admin**.
2. Enter a name in the **Device Name** text field.
3. Click **OK**.

Centralized management of Administrator or Auditor Accounts using Kerberos

In IPBS Edition 2, each IPBS had an independent set of administrator or auditor accounts. IPBS/IPBL Edition 3 introduced Kerberos.

Kerberos is a network authentication protocol that is used when you want to have the same set of user accounts for several IPBSs/IPBLs and then want to administer these user accounts from one central location, that is, a Kerberos server.

When an IPBS/IPBL is set up as a Kerberos server, the IPBS/IPBL acts as an authentication server for the rest of the IPBSs/IPBLs that are set up as client devices in the installation. The Kerberos server and the group of client devices constitute a domain called a realm. During Kerberos communication, no password is actually sent over the network. Kerberos uses encrypted data packets (tickets) which are time-stamped and expire after a certain period. Therefore, getting the correct time across the system for which an NTP server must be used is critical.

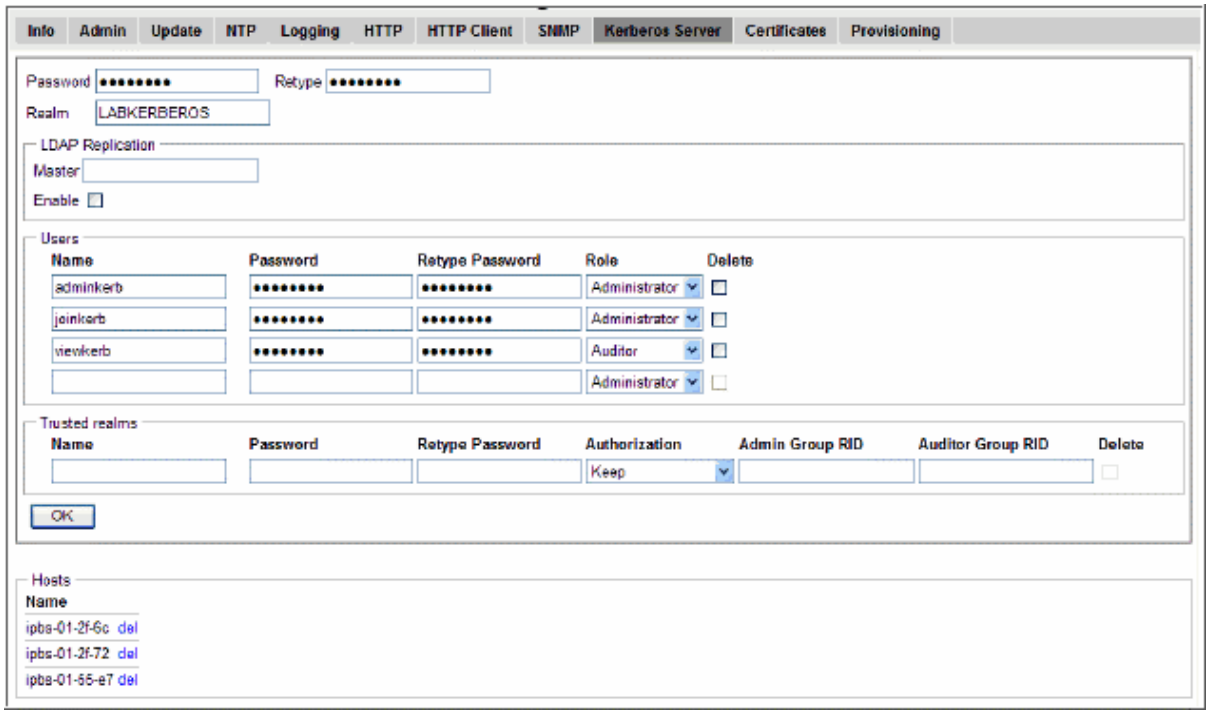
Note:

To configure additional administrator accounts on the IPBS, see Additional Administrator Accounts on page 103.

Setting up the Kerberos Server

Ensure that you set up the Kerberos server on the Master. To configure an IPBS/IPBL to act as a Kerberos server, do the following:

Figure 35: Configure Kerberos server



1. Ensure that the IP address of an NTP time server is specified. Select **General** > **NTP**.
2. Select **General** > **Kerberos Server**.
3. Enter a root password for the Kerberos server. TThe system uses this password to encrypt the information stored on the server.
4. Click **OK**. The Kerberos server is enabled.
5. Enter the realm name of your choice in the **Realm** field in upper-case letters.
6. Enter the following information for the users of the realm.

Field Name	Description
Name	Enter a login user name.
Password	Enter a password.
Retype Password	Confirm password.
Role	• Administrator: Write access to all device parameter settings. • Auditor: Read access to device parameter settings. • Join Realm: Add devices to the realm.

Note:

Ensure that the password follows the password policy set in the General > Admin tab.

7. Click **OK**.

   The host list at the bottom of the page lists the connected Kerberos clients (IPBS radios) that are configured successfully.

Setting up the client

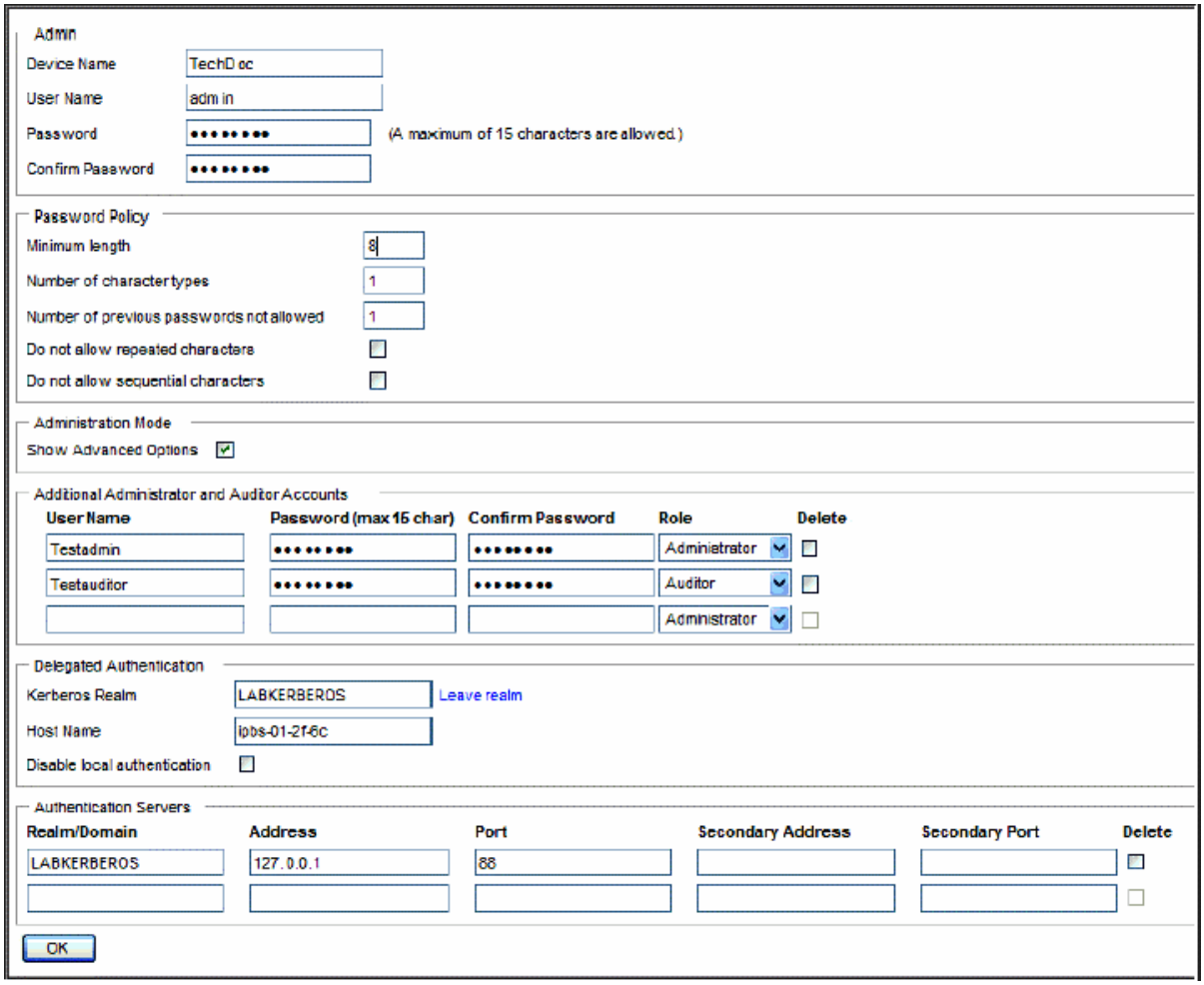
Depending on the type of system, you can configure the IPBS to act as a client in three different ways:

- To configure IPBS as a client in a small existing system that has few clients, see Configuring IPBS as a client in a small existing system on page 119.
- To configure IPBS as a client in a large existing system that has many clients, See Configuring the IPBS as a client in a large existing system (many clients) on page 121.
- To configure IPBS as a client in a new system, see Configuring the IPBS/IPBL as a client in a new system on page 122.

Configuring IPBS as a client in a small existing system

You must configure the location of the Kerberos server locally on each client. You must configure the server as a client also, so that the server can also join the realm.
To configure each IPBS/IPBL as a client, do the following:

Figure 36: Configuring Kerberos client



1. Ensure that the IP address of an NTP time server is specified. Select **General** > **NTP**.
2. Select **General** > **Admin**.

   Note:

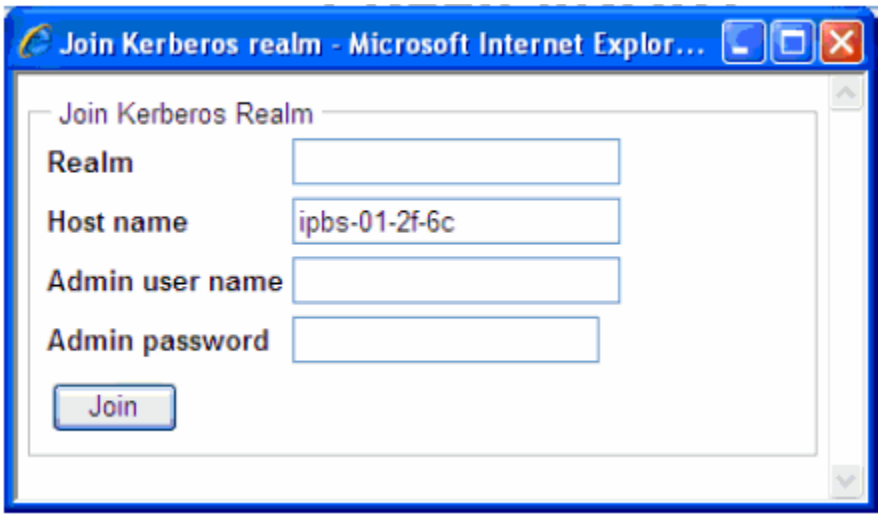
   Ensure that the password policy is configured in the Admin page because an upgrade from earlier releases might not include valid default settings.
3. In the Authentication Servers section, select the Realm/Domain field and enter the realm name specified in the Kerberos server.
4. In the **Address** field, enter the IP address of the Kerberos server. In the Kerberos server, enter 127.0.0.1 (localhost) as the IP address. The values in the Port text field fill by default.
5. Click **OK**.

To enable delegated authentication using the Kerberos server, each client must join the Kerberos realm of the server. To join the realm:

1. Select **General** > **Admin**.
2. In the **Delegated Authentication** section, click **Join realm**.
3. In the Join Kerberos realm window, enter relevant information in the following fields:

   Realm: The realm name of the Kerberos server.
   Host name: The MAC address of the device. The system uses the default value.
   Admin user name and **Admin password**: The user name and password for a user with administrator or join the realm account on the Kerberos server.

Figure 37: Joining the Kerberos Realm



4. Click **Join**.

Configuring the IPBS as a client in a large existing system (many clients)

Prerequisite: All Masters and Radios must run on software version 3.x.x. Software version 6.1.X is required if Windows 2008 R2 server is used.

1. Install the new software version 4.1.x using the update server and an update script. See Configuring automatic Firmware update on page 127.
2. Setup the update server using the update script. See Updating script for configuration of Kerberos clients on page 200 to configure the kerberos client on each radio.
3. Select **DECT** > **Radio config**.
4. Go to the **Update** section, select the **Command File URL** field, enter the path to the update server and the name of the update script.
5. In the **Interval (min)** field, enter the update period.
6. Click **OK**.

After the script is executed and each Radio is restarted, the Kerberos client joins the Kerberos Server. You can see all joined Kerberos clients at the bottom of the **Kerberos Server** tab.

The update script automatically disables the local login possibilities if the Kerberos client joining was successful. SeeUpdating script for configuration of Kerberos clients on page 200.

You can now change the password used in the script to a more secret password from the Kerberos server page.

You can now log in to the Radio using the Kerberos login credentials. See Logging in using Kerberos on page 122.

Configuring the IPBS/IPBL as a client in a new system

Prerequisite: The IPBSs/IPBL delivered from the factory must have software version 4.1.x pre-installed.

You can configure the Radios and the Kerberos Client by using Device Overview > Add and not by browsing each Radio for configuration.

The Radios are in broadcast mode. None of the Radios are attached to the Master and configured. If any of the Radios are attached to the Master and configured, detach the Radios for this procedure to work.

1. Select **Device Overview** > **Radios**.
2. Click **Add** to add the Radio to the Master.
3. In the Add Radio window, enter a name for the device. You can also add a Standby Master IP Address.
4. Go to the **Kerberos** section and enter the appropriate information in the following fields:

   Realm: Enter the realm name of the Kerberos server.
   Host name: (Optional) Enter the host name.
   User: Enter the same user name defined in the Kerberos server.
   Password: Enter the same password defined in the Kerberos server.
   Disable local authentication: (Recommended) Select the check box.
   Overwrite existing: (Optional) Select the check box.
5. Go to the **Authentication Servers** section.
6. In the **Realm/Domain** field, enter the realm name specified in the Kerberos server.
7. In the **Address** field, enter the IP address of the Kerberos server. In the Kerberos server, enter 127.0.0.1 (localhost) as the IP address. The **Port** field is filled out automatically.
8. Click **OK**.

The Radio restarts and establishes a connection to the PARI Master only.

Logging in using Kerberos

1. Make sure that secure HTTPS protocol is used when logging in.
2. Log in on the client using a server account. When prompted for the user name, enter the name of the realm in front of the user name, separated by a backslash in the following way: REALM\username.

Disabling local authentication

After Kerberos authentication is configured, you must disable local authentication for additional security. You can then change the password of a user account or delete a compromised user account more easily on the Kerberos server than changing the local user accounts on each IPBS.

Note:

Make sure that the Kerberos authentication is working properly before disabling local authentication. If the Kerberos authentication is not working and local authentication is disabled, you cannot gain access to the IPBS in any other way.

1. In the **Delegated Authentication** section, select the **Disable local authentication** check box.
2. Click **OK**.

Configuring cross-realm authentication

Cross-realm authentication authenticates users from another trusted realm. In this way, IP-DECT users can log in to the IPBS/IPBL using their Windows user name and password in the Active Directory (AD).

Configuring a shared password on both servers confirms the trust relationship between the two realms. This password is used to encrypt communication between the realms.

Ensure that a Kerberos Server on the IPBS/IPBL side is already configured and the radios have already joined the Realm using a Kerberos account configured on the Kerberos server. With cross-realm authentication, accounts configured in the AD are added for login to the Web interface.

To configure cross-realm authentication, do the following:

Requirements for IPBS1, IPBS2 and IPBL:

- Software version 6.1.X and later
- NTP configured
- Make sure that the device has been configured as a client in the system, see Set up the client on page 24.
- Make sure that the AES and RC4 encryption types are enabled. Select General > Admin and select the Enable AES and RC4 check box.

AD Server configuration for Windows 2003 servers

Configure the trust relationship in the AD server.

1. On the Windows Start menu, click **Administrative Tools** > **Active Directory Domains and Trusts**.
2. Right-click the domain name and select **Properties**.
3. Select the **Trusts** tab and click **New Trust**. The system displays the New Trust Wizard. Click **Next**.

4. Enter the name of the Kerberos realm that is already configured on the IPBS acting as Kerberos server (use capital letters), and click **Next**.
5. Select **Realm trust** and click **Next**.
6. Select **Nontransitive** and click **Next**.
7. Select **Two-way** and click **Next**.
8. Enter a password that will be a shared secret between the AD server and the Kerberos server. Click **Next**.

   Note:

   Do not use the same password as used in the IPBS Kerberos Server to create and encrypt the Kerberos database.
9. Check the configuration and click **Next**.
10. Click **Finish**.

Kerberos Server configuration

The trust relationship must also be configured in the Kerberos server.

1. Select **General** > **Kerberos Server**.
2. Enter the following information in the **Trusted realms** section:

Field Name	Description
Name	Enter the name of the trusted Windows domain. The domain name must be in capital letters.
Password	Enter the shared password specified in the AD server
Retype Password	Confirm password
Authorization	Set user access rights from the Windows domain • Use domain group: Specify a Windows group with Administrator or Auditor rights • Administrator: All Windows domain users have administrator access rights • Auditor: All Windows domain users have auditor access rights

Admin Group RID	Specify the Relative Identifier (RID) of a Windows group with administrator rights. The RID is the last part of the Security Identifier (SID) of a group. Determine the SID of a group by entering the following in the Windows command line: `whoami /groups` This command displays the group information of the user logged in to the Windows domain.
Auditor Group RID	Specify the Relative Identifier (RID) of a Windows group with auditor rights. The RID is the last part of the Security Identifier (SID) of a group. Determine the SID of a group by entering the following in the Windows command line: `whoami /groups` This command displays the group information of the user logged in to the Windows domain.

3. Click **OK**.

Kerberos Client configuration

The location of the Windows server must be configured locally on each client similarly to the Kerberos server. The client configuration must be done on the Kerberos server as well so that it can also join the Windows domain. To configure the clients do the following:

1. Select **General** > **Admin**.
2. Go to the **Authentication Servers** section.
3. In the **Realm/Domain** field, enter the name of the trusted Windows domain.
4. In the **Address** field, enter the IP address of the Windows server. The **Port** field is filled out automatically.
5. Click **OK**.

Logging in using Kerberos cross-realm authentication

1. Make sure that secure HTTPS protocol is used when logging in.
2. Log in on the client using a Windows server account. When prompted for user name, enter the name of the Windows domain in front of the user name, separated by a backslash in the following way: DOMAIN\username. The domain name must be in capital letters.

Configuring the secondary Kerberos server

The Kerberos server is crucial when using Kerberos authentication. Therefore, Avaya recommends having a secondary Kerberos server in the IP-DECT system. The secondary server is used if the primary server is not working properly. Set up the secondary Kerberos server on the Standby Master.

To configure an IPBS as a secondary Kerberos server:

1. Ensure that the IP address of an NTP time server is specified. Select **General** > **NTP**.
2. Select **General** > **Kerberos Server**.
3. Enter the root password for the secondary Kerberos server, which should be the same as the password used for the primary server. This password is used to encrypt the information stored on the server.
4. Click **OK**. The secondary Kerberos server is enabled.
5. Enter the realm name in the **Realm** field.
6. Enter the IP address of the primary Kerberos server in the **Master** field in the **LDAP Replication** section. LDAP is used to replicate the primary server database. For more information about LDAP, see LDAP on page 145.
7. Select the **Enable** check box.
8. Click **OK**.
9. Click **OK** again to perform the LDAP replication.

   Each client must also be configured with the secondary server information.
10. Select **General** > **Admin**.
11. Go to the **Authentication Servers** section.
12. In the **Secondary Address** field of the Kerberos server, enter the IP address of the secondary Kerberos server. In the secondary Kerberos server, enter 127.0.0.1 (localhost) as the IP address. The **Port** field is filled out automatically.
13. Click **OK**.

Deleting a user or trusted realm

To delete a user account from the Kerberos server:

1. Select **General** > **Kerberos Server**.
2. In the **Users** section, select the **Delete** check box to delete the user.
3. Click **OK**.

To delete a trusted realm relationship from the Kerberos server:

1. Select **General** > **Kerberos Server**.
2. In the **Trusted Realms** section, select the **Delete** check box to delete the realm.

3. Click **OK**.

Deactivating Kerberos realm membership

Make sure that local authentication is enabled and working properly before leaving the Kerberos realm. If local authentication is still disabled and the IPBS is no longer a member of the realm, you cannot gain access the IPBS in any other way.

1. Select **General** > **Admin**.
2. In the **Delegated Authentication** section, clear the **Disable local authentication** check box.
3. Click **OK**.

To deactivate the Kerberos membership for a client, do the following:

1. Select **General** > **Admin**.
2. Go to the **Kerberos** section, and click the link **Leave realm**.
3. Deactivate the Kerberos realm membership using one of the following two ways:
   - Deregister:To remove the client from the server database.
     a. In the Leave Kerberos realm window, enter the user name and password for a user with administrator or join the realm account in the **Deregister with Kerberos server** section.
     b. Click **Deregister**.
   - Delete: To leave the realm without removing data from the server.
     - Click **Delete**.

Configuring automatic Firmware update

You can configure IPBS/IPBL to automatically update IPBS/IPBL firmware. You must upload a script file to a suitable directory on an internal web server. For information on the script file syntax, see Using the Update Server on page 195.

1. Select **General** > **Update**
2. In the URL text field, enter the URL of the script file.
3. In the Interval (min) text field, enter the poll interval in minutes.
4. Click **OK**.

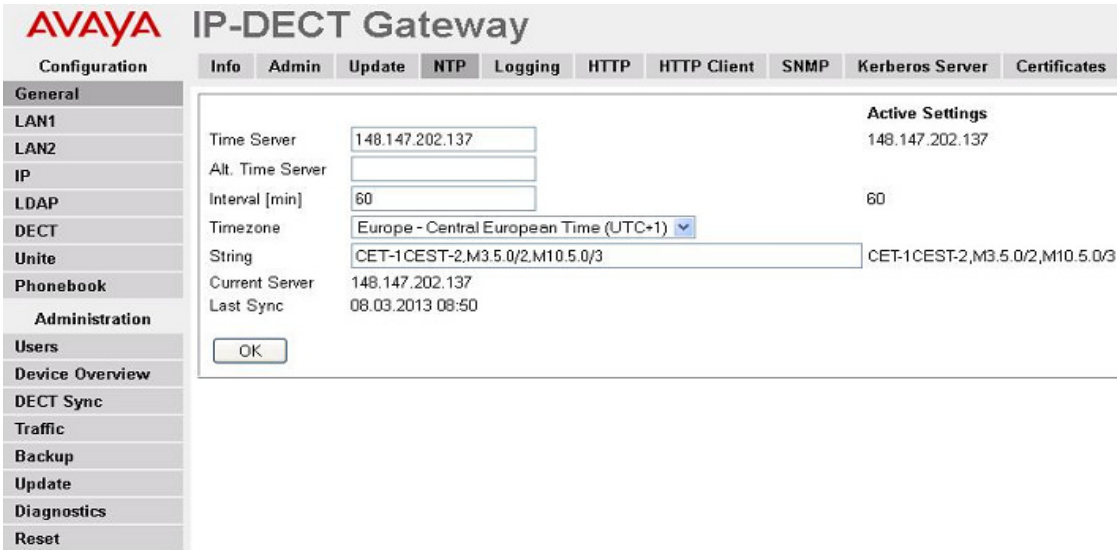
The Current Update Serials section shows the values of variables that were set after the last associated command was run.

Configuring the NTP settings

The IPBS/IPBL does not have a battery-backed real-time clock. Therefore, the internal time is set to 0:00 hrs and to 1.1.1970 in case of a restart.

In order to get the correct time in the system, specify the IP address of a NTP time server. The IPBS/IPBL will synchronize its internal clock to the time server at startup and at the specified intervals. The clock is, for example, used by the telephones and log files.

Figure 38: Configuring NTP settings



1. Select **General** > **NTP**.
2. Enter the IP address to the NTP server.
3. Enter a time interval in the **Interval (min)** text field.
4. Select time zone in the **Time zone** drop-down list. If the time zone that you want is not in the list, select **Other** and edit the **String** text field following the instructions in step 5.
5. Enter the following timezone string if you want the summer and winter times to update automatically:

   <String = StdOffset [Dst[SecondOffset], Date/Time, Date/Time]>

   - where Std is the name of time zone and can be freely defined. You can use the characters: a-z, A-Z. You cannot use numbers, blanks, or special characters. For example, EST for Eastern Standard Time.
   - where Offset is the time difference between the timezone and the Universal Time Coordinator (UTC).
     - *Example 1:* Eastern Standard Time (EST) is 5 hours behind UTC (EST=UTC-5). You have to input the difference between your timezone and UTC. in this case, enter plus 5 (UTC=EST+5), but without the „+“ sign: "EST5“.

  - *Example 2:* Use the hh:mm format for timezones that have less than a full hour difference with UTC. For example, for Indian Standard Time (IST=UTC+5:30), enter -5:30 (UTC=IST-5:30).

- Dst = Name of summertime zone (for example EDT for Eastern Daylight Time).
- Second Offset = time difference between the summer time and the UTC.
- Date/ Time, Date/ Time = beginning and end of summertime.
  - date format = Mm.n.d (d day of n week in the m month)
  - time format = hh:mm:ss in 24-hour format.

Note that a week always starts on a Sunday and the number for Sunday is 0.

Example 1:
North Carolina is located in the Eastern Time Zone, and the Eastern Standard Time (EST) is 5 hours behind UTC (StdOffset = EST5). Eastern Daylight Time (EDT) is 4 hours behind UTC (DstOffset = EDT4). Summertime for the year 2006 begins at two o'clock, on a Sunday, the first week in April (M4.1.0/2). Summertime ends at two o'clock, on a Sunday, the fifth week in October (M10.5.0/2).

<String = EST5EDT4,M4.1.0/2,M10.5.0/2>

Example 2:
Indian Standard Time (IST) is 5:30 hours ahead of UTC (StdOffset = IST-5:30). India has no daylight saving time:

<String = IST-5:30>

6. Click **OK**.

Note:
If you remove or change this value, the new value takes up to 24 hours to reflect on the cordless telephone. If you switch a cordless telephone off and on again, the changes take effect immediately.

Configuring logging

You can collect logs in the following three ways:

TCP	The syslog entries are transmitted using a TCP connection.
SYSLOG	The entries are reported to a "syslogd" server in the network, which further evaluates or stores the entries.
HTTP	The syslog entries are transferred to a Web server for further processing. Each individual syslog entry is transmitted as form data to the web server in HTTP GET format.

Storing Syslog entries using a TCP Connection

1. Select **General** > **Logging**

2. Select **TCP** in the **Type** drop-down list.
3. Enter the **IP address** of the logging server in the **Address** text field.
4. Enter the **Port** of the logging server in the **Port** text field.
5. Click **OK**.

Storing the Syslog entries in a Syslogd

1. Select **General** > **Logging**.
2. Select **SYSLOG** in the **Type** drop-down list.
3. Enter the **IP address** of the syslogd in the **Address** text field.
4. Enter the desired syslogd message class in the **Class** text field.
5. Click **OK**.

Storing the Syslog entries on a Web Server

1. Select **General** > **Logging**.
2. Select **HTTP** in the **Type** drop-down list.
3. Enter the **IP address** in the **Address** text field.
4. Enter the "relative URL of the form program" on your web server in the **Path** text field.
5. Click **OK**.

Note:

The IPBS will make an *HTTP GET* request to the web server on the registered URL followed by the URL-encoded log entry.

Example:

Enter the value **`/cdr/ cdrwrite.asp`** in the **URL-Path** field if a page is on the web server with the name **`/cdr/cdrwrite.asp`** with a form that expects the log message in the ***`msg`*** parameter.
In this example, the IPBS will make a *GET* **`/cdr/cdrwrite.asp?event=syslog&msg=logmsg`** request to the server.

Forwarding alarms and events

You can forward alarms and events to an HTTP server destination. Typically, this destination can be a Master base station. This configuration for forwarding alarms and messages can be done in the Pari Master (**DECT** > **Radio config**) or locally as described below.

1. Select **General** > **Logging**.
2. If the HTTP server destination requires HTTPS, then select **HTTPS** in the **Type** drop-down list.
3. Enter the IP Address of the IPBS, where you want to have an overview of all faults, in the **External HTTP Server Address** field.

4. Enter the HTTP/HTTPS server port in the **External HTTP Server Port** field. The default value is 80.

Configuring the HTTP settings

The IPBS/IPBL is usually administered over the network using the http protocol. The default port is 80.

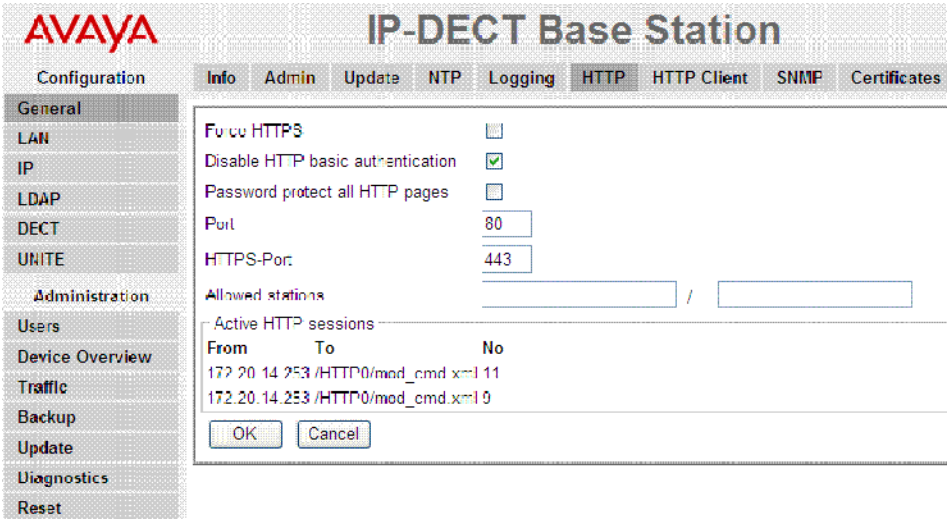
In a secure system, you must administer the IPBS/IPBL through the https protocol with the default port 443. If you cannot use port 443, use another port for the local https server and then reach the IPBS/IPBL using this port.

Http and https traffic, respectively, are disabled if their port values are set to zero (0). Therefore:

- To disable http traffic, set Port to 0. Avaya recommends that you disable http traffic in a secure system. Attempts to contact the device using the http protocol will result in an *Unable to connect* message.
- To disable https traffic, set HTTPS Port to 0. Avaya does not recommend that you disable https traffic.

Any other port values would enable http and https traffic, respectively, for the port specified.

Figure 39: Configuring the HTTP settings



1. Select **General** > **HTTP**
   - Select the Force HTTPS check box to allow only HTTPS sessions and redirect all HTTP requests as HTTPS requests.
   - Select the Disable HTTP basic authentication check box so that all administrative and program clients support HTTP digest authentication.
   - Select the **Password protect all HTTP pages** check box to password protect all HTTP pages.

- Enter **Port number** in the Port text field. The IPBS/IPBL is by default administered over the network via the TCP port 80 (http). If you cannot use port 80, set up another port for access.
  Set this value to 0 to disable http traffic (recommended). Attempts to contact the device using the http protocol will result in an *Unable to connect* message.
- Enter **HTTPS Port** in the HTTPS Port text field. To access IPBS/IPBL securely, use the TCP port 443 (https). Set this value to anything except zero (0) to enable https traffic. The default value is 443. The value zero (0) disables https traffic which is not recommended.
- Enter ***Network Base Address*** / ***Network Base Mask*** in the **Allowed stations** text fields to allow access only from matching network, for example:172.16.0.0/255.255.0.0
- In the Active HTTP sessions field, you can see all the ongoing HTTP traffic.

2. Click **OK**.

Configuring the HTTP Client settings

You can specify the list of URLs that require authentication.

1. Select **General** > **HTTP Client**.
2. Enter the **URL** in the **URL** text field.
3. Enter **User** and **Password** in the **User** and **Password** text fields.
4. Click **OK**.

   The system displays a new row in which you can add more URLs.

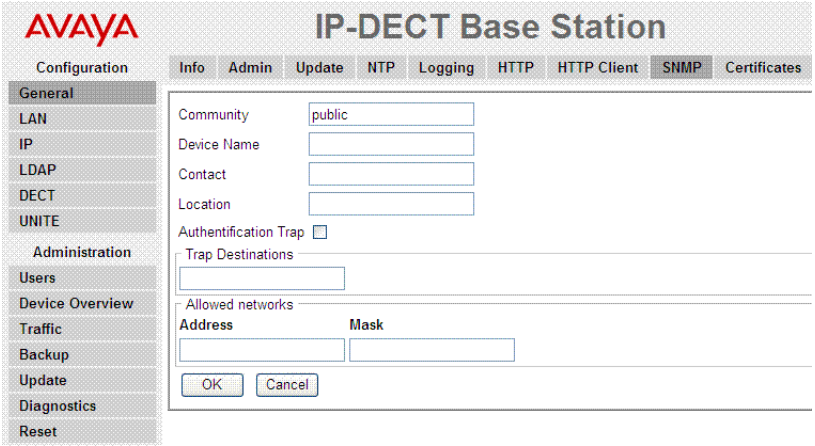
SNMP

To report faults in the IP-DECT system, use the Simple Network Management Protocol (SNMP). The SNMP framework has three parts:

- An SNMP manager: For the system to control and monitor the activities of network hosts using SNMP.
- An SNMP agent: The software component within the managed device that maintains data for the device and reports data, as needed, to managing systems.
- A MIB: A virtual information storage area for network management information.

The agent and MIB reside on a network device, for example, router, access server, or switch. To enable the SNMP agent on the IPBS, define the relationship between the manager and the agent.

Figure 40: Configuring the SNMP settings

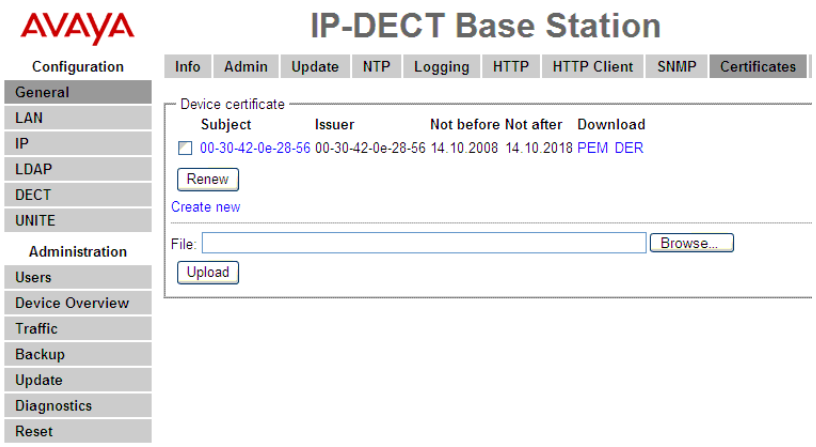


1. Select **General** > **SNMP**
2. Enter a name in the **Community** field if you are not using the standard community name (public). The community text string acts like a password to regulate access to the agent on the Base Station.
3. Enter a device name in the **Device Name** field. This field is optional and serves only informational purposes.
4. Enter the name and phone number of the contact person in the **Contact** field. This field is optional and serves only informational purposes.
5. Enter a location in the **Location** field. This field is optional and serves only informational purposes.
6. Select the **Authentification Trap** check box to enable the sending of authentification traps. To gain access through SNMP, enter the correct Community Name. If enabled, the system generates a trap to prevent access with an incorrect Community Name.
7. Enter the IP address of the desired trap destinations in the **Trap Destinations** field. SNMP traps are sent to all destinations.
8. Enter the IP address and mask of the networks that have the permission to send SNMP requests. If the field is empty, all networks can send SNMP requests.
9. Click **OK**.

Certificates

The **Certificates** tab is part of IP Security in IP-DECT. For more information on IP Security, see chapter IP security on page 76.

Select **Configuration** > **General** > **Certificates**.



You can select from three possible certificate options. See Certificate handling options on page 78,

- Default device certificate, see Functions description.: on page 134.
- Self-signed certificates, see Self-signed certificates on page 135.
- Certificates signed by a Certificate Authority (CA), see Certificate Signing Request (CSR) on page 137.

Figure 41: Functions description.:

Field name	Description
Subject	Click the hyperlink below the *Subject* header to display certificate details in a window.
PEM	Click the *PEM* hyperlink below the *Download* header to download the certificate in PEM format.
DER	Click the *DER* hyperlink below the *Download* header to download the certificate in DER format.

Create New	The *Create New* hyperlink is used for two purposes: • Self-signed certificates on page 135 • Certificate Signing Request (CSR) on page 137
Upload	Use the Upload function to upload a certificate file to the device. 1. Click the **Browse** button. 2. Select a certificate file. 3. Click the **Upload** button to upload the file to the device. **Note:** The Upload function requires a previously issued CSR to exist.

Default device certificate

This section corresponds to option 1 in Certificate handling options on page 78.

If the default device certificate is missing, the system generates the default device together with a key pair when you upgrade the IPBS to version R3. The default certificate contains the MAC address of the device and is valid for 10 years.

If the self-signed certificate is deleted and the device is restarted, a new certificate and key pair will be generated.

HTTPS is deactivated during the generation (creation) of the certificate.

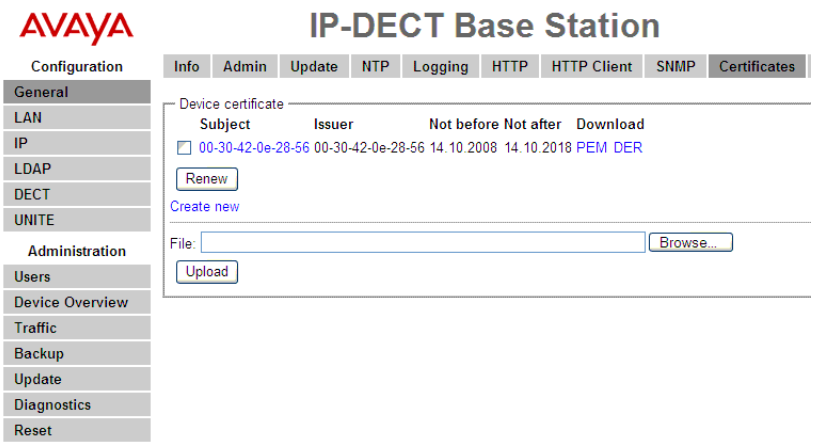
The default certificate is a self-signed certificate. This means that certificates cannot be verified, and the browser prompts the user or administrator to accept the certificate before being used. If the certificate is not changed, communication between the browser and the device takes place from this point on without further accept operations from the user or administrator.

If the device certificate is replaced or regenerated the user/administrator has to manually accept the new certificate.

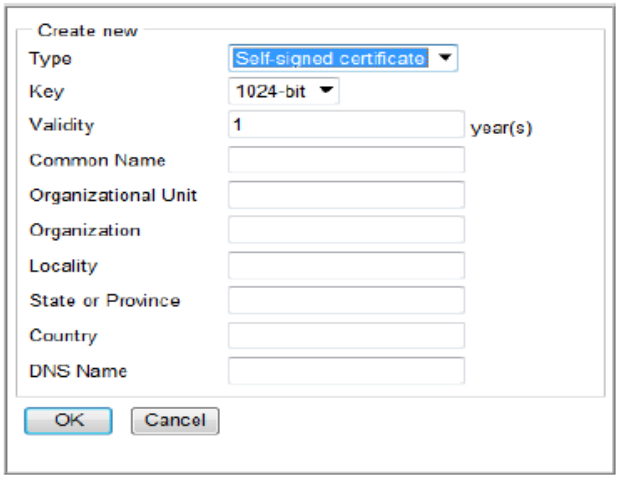
Self-signed certificates

This section corresponds to option 2 in TLS Certificates. on page 78.

1. Select **Configuration** > **General** > **Certificates**.



2. Click the **Create New** hyperlink in the **Device Certificate** section. The system displays a new window.
3. In the window, select **Self-signed certificate** in the **Type** drop-down list.



4. Select/Enter the following settings:

Field name	Description
• Validity	Enter the default validity in years. This field is mandatory.
• Key	Select either the desired key strength (1024-bit, 2048-bit, 4096-bit).
• Common Name	Enter the domain name or IP address for the device. This is the same value as entered in the web browser when accessing the device.

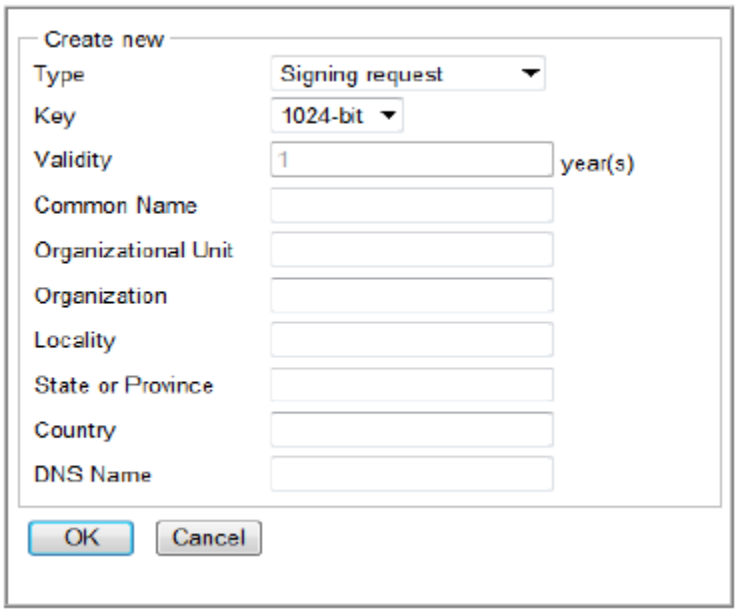
5. Click **OK**.

6. A new key pair and a certificate will be created. This may take up to one hour depending on the key strength selected. During this time the device will be fully operational with the exception of https not working and the certificate tab pane not being visible.

Certificate Signing Request (CSR)

This section corresponds to option 3A & 3B in TLS Certificates. on page 78. CSR is the most common option for IP-DECT systems. For more information on CSRs, see Certificate Authorities on page 77.

1. Select **Configuration** > **General** > **Certificates**.
2. Click the **Create New** hyperlink in the **Device Certificate** section. The following window opens.



3. In the window, select **Signing Request** in the **Type** drop-down list.
4. Select/Enter the following settings:

Field name	Description
• Validity	Enter the validity in years. This field is a read-only information field indicating a default validity of 1 year. The time length of the validity is defined by the CA.

• Key	Select the desired key strength. Select the key strength: 1024-bit, 2048-bit, or 4096-bit or reuse the old key pair. Note: This option is not recommended.
• Common Name	Enter the domain name or IP address for the device. This value is the is the same value that you entered in the web browser when accessing the device.

5. Click **OK**. The browser window closes.

   A key pair and a CSR file is created. Creation may take up to one hour depending on the key strength selected. During this time the device will be fully operational with the exception of https not working and the certificate tab pane not being visible.

   When the CSR file is generated, the Signing Request section of the Certificates page displays the file.

6. Download the CSR file by clicking the PEM or DER link in the **Signing Request** section.
7. Send the CSR file to your CA. If successful, your CA will send back a digitally signed certificate file to upload.
8. Select the certificate file and click **Upload**.

Note:

If the CSR file generated in step 5 is deleted before receiving the reply from the CA (in step 8) it will not be possible to upload the signed certificate file in step 10. The system will automatically delete the CSR file when step 10 has completed.

Provisioning

Provisioning makes it easy to manage IP-DECT users from the IP-PBX without using the IP-DECT GUI. Provisioning is mainly configured in the IP-PBX but it must be enabled in the IPBS/IPBL. If provisioning is enabled user records in the IPBS/IPBL cannot be modified since all user data is mapped from the IP-PBX to the IPBS/IPBL.

Note:

Local users created in the IPBS/IPBL will be deleted when provisioning is enabled if no corresponding user exists in the IP-PBX.

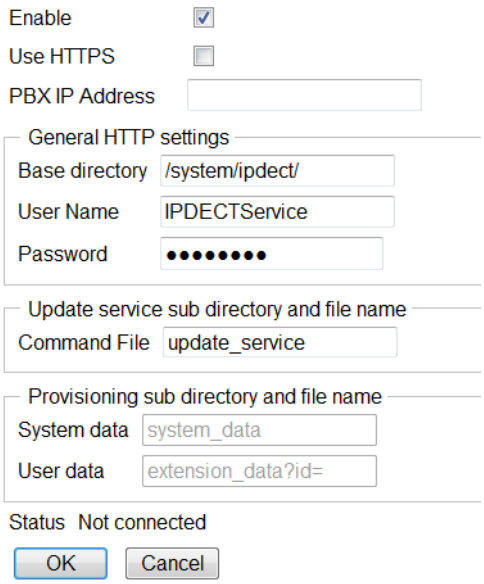


Figure 42. Configure Provisioning

To enable provisioning do the following:

1 Select General > Provisioning.

2 Select the Enable check box.

3 The communication between the IPBS and the IP-PBX can be encrypted using https. Select the Use HTTPS check box to enable the encryption.

4 Specify the IP address of the IP-PBX in the PBX IP Address field.

5 The other values on the page are default values and filled out automatically.

Click "OK".

6 Reset the IPBS/IPBL to make the changes take effect, see Reset on page 190.

If the https protocol is used the IPBS/IPBL downloads a certificate from the IP-PBX to ensure a secure transaction. The IPBS/IPBL does not initially trust the certificate so it must be added manually to the trust list of the IPBS/IPBL. It is also possible that more than one certificate is downloaded creating a certificate chain. The root CA certificate is at the end of the chain which contains a self-signed signature and it is able to approve other certificate requests. It is recommended to add the root CA certificate to the IPBS trust list.

Note: The connection to the IP-PBX will only be established after the certificate is acknowledged.

If the certificate expires, the ongoing connection is maintained but it will not be possible to start a new connection until the certificate is renewed.

To add a certificate to the trust list do the following:

1 Select General > Certificates.

2 In the Rejected certificates section select the check box of the certificate you want to trust.

3 Click "Trust".

For more information about certificate handling, see Creating a certificate on page 385.

Provisioning Modes

There are three different modes.

Active	The connection is up.
Inactive	Provisioning is not enabled for the currently viewed IPO PBX or the connection is used for the other IPO PBX.
Not connected	Provisioning is enabled for the currently viewed IPO PBX but the connection cannot be established or the connection is being established.

LAN

This section describes how to do the following configurations and settings.

- Set DHCP mode
- Set IP static address
- Set dynamic IP address
- Set link type
- Configure VLAN
- Enable RSTP (only for IPBL)
- View LAN statistics

Note:

The IPBL has two LAN ports. LAN1 port must be used in the IP-DECT system and LAN2 port must be used for administration only.

Setting DHCP mode

The IPBS/IPBL can have the following DHCP modes:.

Off	Used if the IPBS/IPBL has a static IP address.
Client	Acts as a DHCP Client, if there is a DHCP server in the network it will be assigned an IP address
Automatic	Acts as a DHCP client on start up. If you reset he IPBS/IPBL by pressing the reset button, it will get the IP address 192.168.0.1 and the netmask 255.255.255.0 for the LAN port.

To change the DCHP mode.

1. On the IPBS: Select LAN > DHCP.
   On the IPBL: Select LAN1 > DHCP
2. Select DHCP mode in the **Mode** drop-down list.
3. Click **OK**.
4. Reset in order to make the changes take effect, if you set **Client** or **Automatic**. See Reset on page 190.

Setting a static IP address

You must configure the Master and the Standby Master to have static IP addresses. The slaves can have dynamic IP addresses retrieved from the network DHCP server.

Ask the network administrator to reserve an IP address for the Master and Standby Master.

1. On the IPBS: Select LAN > DHCP.
   On the IPBL: Select LAN1 > DHCP
2. Select **Disabled** in the **Mode** drop-down list.
3. Click **OK**.
4. Do NOT reset the device yet. Set a static IP address first.

- On the IPBS: Select LAN > IP.
- On the IPBL: Select LAN1 > IP

5. Select **LAN** > **IP**.
6. Enter **IP Address**, **Network Mask**, **Default Gateway** and **DNS Server** addresses provided by the network administrator in the text fields.

   You can also enter an alternative DNS Server in the **Alt. DNS Server** text field and select the **Check ARP** check box to detect and prevent ARP poisoning attacks.
7. Click **OK**.
8. Reset in order to make the changes take effect, see Reset on page 190.
9. Start the web-based configuration, using the static IP address.

Dynamic IP address using DHCP

You can configure the Slaves/Radios to obtain dynamic IP address allocation if the network has an DHCP server.

1. On the IPBS: Select LAN > DHCP.
   On the IPBL: Select LAN1 > DHCP.
2. Select **Client** in the **Mode** drop-down list.
3. Click **OK**.

4. Reset in order to make the changes take effect. See Reset on page 190.

Note:

If the DHCP lease time is shorter than the time-to-live of the name/IP address association in the Windows Internet Name Service (WINS) server, it may cause a mismatch, and a wrong device may be reached if its WINS name is used.

Link

On the IPBS: Select LAN > Link.
On the IPBL: Select LAN1 > Link.

Set the link setting to auto in all normal circumstances.

Configuring VLAN

Perform identity and priority settings for VLAN in the LAN > VLAN sub menu.

Note:

VLAN must have the same ID as the ID configured in the IPBS/IPBL. If not, you cannot gain access to the IPBS/IPBL.

Note:

If VLAN is set to 0, Quality of Service (QoS) is inactive according to 802.1q. Do not set VLAN to 1 as this setting is a default VLAN setting.

Viewing LAN statistics

To view statistics of LAN events: Select **LAN** > **Statistics**

On the IPBS: Select LAN > Statistics
On the IPBL: Select LAN1 > Statistics

To reset the ethernet statistics counters: Click the **clear** button.

Enabling RSTP (only for IPBL)

The RSTP (Rapid Spanning Tree Protocol) function is provided for IPBLs connected to a redundant bridged network when an IPBL must stay operational even if a network port or a bridge in the network fails. If RSTP is enabled LAN1 is assumed to be the primary port and LAN2 the backup port. RSTP packets are sent over both ports. From received RSTP packets it is learned which port shall be used for data traffic. The port to be used for data traffic may change whenever the network topology changes, i.e. when a link between bridges goes down or up or a bridge is added. On each such change the IP stack is moved to the selected port without disruption of data traffic.

Before RSTP can be enabled, you must fulfill the following preconditions:

- The bridges in the network should support RSTP.
- LAN1 and LAN2 should be connected to RSTP enabled bridge ports.
- LAN1 and LAN2 should be connected to different bridges.
- LAN1 must be configured for a static IP address. See Setting a static IP address on page 141.
- Select LAN1 > IP. Make sure that the Check ARP and the Disable check boxes are unchecked.
- Select LAN2 > IP. Select the Disable check box.
- Select LAN2 > DHCP. Select disabled in the Mode drop-down list.
- Select LAN1 > VLAN. Check that VLAN is not enabled.
- Select LAN2 > VLAN. Check that VLAN is not enabled.

To enable RSTP

1. Select LAN1 > RSTP.
2. Select the **Enable** check box.
3. To trace events triggering RSTP state machine actions and the associated events, select the **Trace Actions** check box.
4. Click **OK.**

Deactivate LAN port (only for IPBL)

To deactivate LAN port:

1. Select LAN2 > IP.
2. Select the **Disable** check box.
3. Click **OK**.

The LAN2 port is for administration only and can be deactivated. However when using RSTP you cannot deactivate the LAN2 port as both ports are required for RSTP.

IP

Configuring IP settings sub menu

Figure 43: Menu options and functions:

ToS priority, RTP Data and VoIP Signalling:	This setting determines the priority from the ToS field in the IP header. You can use this function if the router can use ToS priority control. You can use hexadecimal, octal, or decimal values as 0x10, 020, and 16 are all equivalent. ToS priority has two fields; one for RTP Data and one for VoIP Signalling. VoIP Signalling includes roaming, handover, and registrations towards the IP-PBX. Other types of traffic, for example http and ldap, are not prioritized and use 0x00. **Note:** Ensure that the same value is set in the ToS field for all devices.
RTP ports:	If you leave the ports fields blank, the system uses the ports 16384 to 32767. The rules for defining the ports are: 2050 <= 'First UDP-RTP Port' 128 <= 'Number of Ports' <= 16384 'First UDP-RTP Port' + 'Number of Ports' <= 65534 **Note:** Use the **DECT - Radio config** tab to configure the RTP ports on each radio.

1. Select **IP** > **Settings**.
2. In the T**oS Priority - RTP Data** text field, enter the ToS priority value. The recommended value is **0xb8**.
3. In the **ToS Priority - VoIP Signalling** text field, enter the ToS priority value. The recommended value is **0x68**.
4. Select the ports to be used for RTP traffic by entering the first port in the **First UDP-RTP Port** text field.
5. Enter the number of ports to use in the **Number of Ports** text field.
6. Click **OK**.

Routing

To view IP routing, select IP > Routing.

LDAP

Systems in which the server and a replicating client share a joint user database require the Lightweight Directory Access Protocol (LDAP) protocol. All base stations or IPBLs in the system have access to the database, so you can configure one of the IPBSs/IPBLs to be the LDAP server.

The joint user database contains information about the users registered in the system. The joint user database also contains the system configuration information about the configurations made under the **DECT** menu.

This section describes the following configurations and settings.

- Configure LDAP Server
- Check LDAP server Status
- Configure LDAP Replicator
- Check LDAP Replicator Status

Configuring LDAP Server

The IP-DECT system needs an LDAP server. If the PBX is set up as an LDAP server, the IPBS Master should be set up as an LDAP Replicator. If the IPBS Master is set up as an LDAP Server, the Standby Master could be set up as an LDAP Replicator, see Configuring LDAP Replicator on page 147.

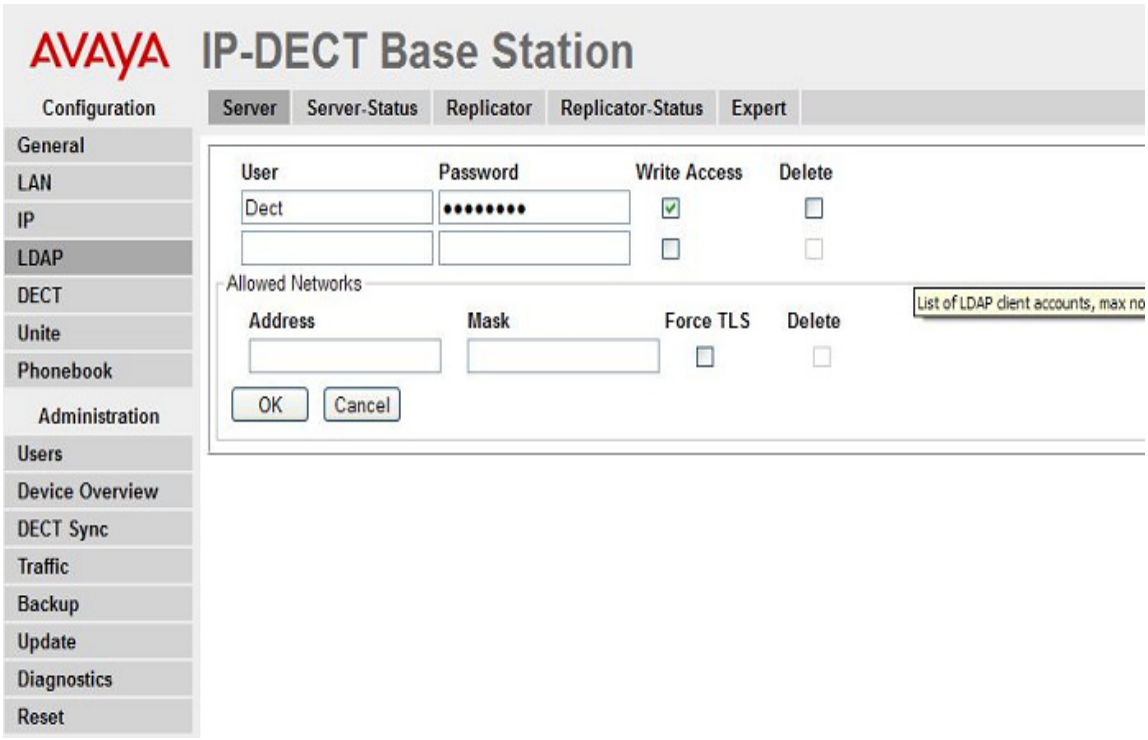
Setting up the IPBS/IPBL as an LDAP server:

Note:

Select the same user name and password for both Master and Standby Master. If you use a multi-Master System, all the Masters must have the same user name and password.

1. Select **LDAP** > **Server**.
2. Add a user, for example ldap-user, in the **User** field.
3. Enter a password in the **Password** field.
4. Select the Write Access check box.
5. Click **OK**.

Figure 44: Setting the LDAP User Name and Password



Checking LDAP Server status

1. Select LDAP > Server Status

Check the following information:

- connections - Total number of active connections to the LDAP server
- write connections - Number of write-enabled connections
- rx search - Number of received search requests
- rx modify - Number of received change requests
- rx add - Number of added objects
- rx del - Number of deleted objects
- rx abandon - Number of lost connections
- tx notify - Number of sent change notifications
- tx error - Number of sent error notifications
- tx error 49 - Number of sent error notifications due to invalid credentials
- tx error 50 - Number of sent error notifications due to insufficient access rights

Configuring LDAP Replicator

Configure LDAP Replicators in the following cases:

- User data is replicated from the Master to the Standby Master. The replicator is configured on the Standby Master (Full Directory Replication).
- User data is replicated from the Master to other Masters in a Multi Master System. The replicator is configured on the Masters not hosting the LDAP Server. To have full roaming between Masters, the LDAP user must have write access to the LDAP server.

WARNING:
You must not configure the LDAP replication on the IPBS master hosting the LDAP Server (replication to itself). This configuration is invalid and may result in failure to subscribe users.

Configuring full directory replication

1. Select **LDAP** > **Replicator**.
2. Select the **Enable** check-box.
3. Enter the IP address to the LDAP server in the **Server** field.
4. Enter the IP address of the alternative LDAP server in the **Alt. Server** field.

Note:
If this IPBS/IPBL is configured as a standby LDAP server, enter **0.0.0.0** in the **Alt. Server** text field.

5. Select a filter method from the following drop-down lists. As this step is an advanced LDAP configuration, Avaya recommends that you use the default settings in a standard system.
   - **Filter Type** - Enter an LDAP filter to limit replication to certain LDAP objects. The default is **DECT Gateway Name**.
   - **Dect Gateway Name** - Enter the name of the DECT gateway to limit the replication to users of a certain group. As default setting, keep the field empty.
6. Enter the LDAP User name and Password in the **User** and **Password** text fields.
7. Click **OK**.

Note:
In the case of Master to Standby Master Full Directory Replication, do not register new Portable Devices when the LDAP Server when the LDAP Server is nonfunctional even if the system has a Standby LDAP Server.

Checking LDAP Replicator

1. Select **LDAP > Replicator-Status**.

   Check the following information:

- Server: The IP address and port of the LDAP server
- Remote: The state of replication in the source directory that includes the three possible states: *Stopped, Active, Completed*
- Notify: The number of change notifications received from the server
- paged: The number of objects received from AD server in response to paged search requests
- No match: The number of objects received that do not match the configured LDAP filter condition
- Discarded: The number of objects discarded because no suitable map is found
- Local: The state of replication in the destination directory. Three states are possible: *Stopped, Active, Completed*
- Notify: The number of change notifications sent to the server
- Add: The number of locally added objects
- Del: The number of locally deleted objects
- Modify: The number of locally modified objects
- Pending: The number of local objects waiting to be sent to the server

Expert tool

Consult Avaya Technical Support before using the Expert tool.

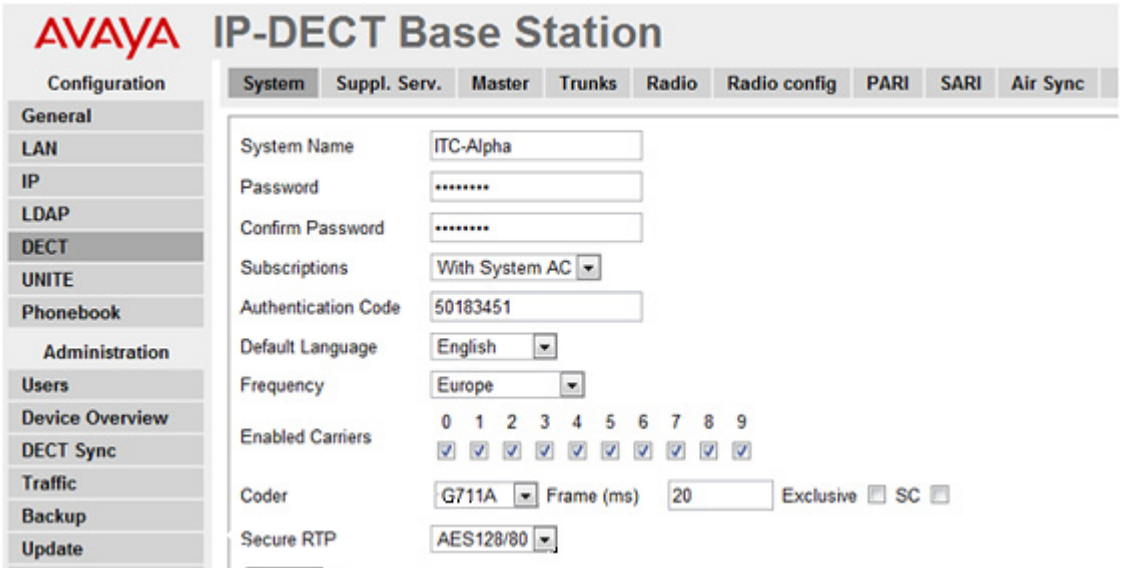
DECT

This section describes how to do the following configurations and settings.

- Change DECT user name and password
- Change Subscription Method
- Configure Authentication Code
- Set Default Language
- Set Frequency Band
- Enable or Disable Carriers
- Configure Coder
- Configure Supplementary Services
- Select Master Mode
- Configure Trunks

- Enable or disable Radio
- Configure multiple Radios
- Assign PARI
- Enter SARI
- Configure Air Synchronization
- Enable SRTP

Figure 45: The DECT System configuration page



Changing the system name and password

Note:

This configuration only applies to a Master IPBS/IPBL, not to a Slave IPBS/IPBL.

The system name and password must be the same for all base stations/IPBLs throughout the system. Reset in order to make the changes take effect, see Reset on page 190.

1. Select **DECT** > **System**.

   Note:

   To access the System tab, activate the Master mode. See Selecting Mode on page 154.

2. Write a system name in the System **Name** text field.
3. Enter a new password in the **Password** text field. Repeat the password.

4. Click **OK**.

Changing the subscription method

Set the IP-DECT system to use the following subscription methods:

- ***With User AC***: For individual registration with User AC.
- ***With System AC***: For anonymous subscription. Individual registration with User AC is also possible.
- ***Disable***: For disabling the subscription.

To select a subscription method:

1. Select **DECT** > **System**.

   Note:
   To access the **System** tab, the Master mode has to be activated, see Selecting Mode on page 154.

2. Select subscription method in the **Subscriptions** drop-down list.
3. Click **OK**.

Configuring authentication code

If you select the **Allow anonymous subscription** method, you must configure the IP-DECT system to have an authentication code. The authentication code is generated automatically but you can modify it manually by selecting a code consisting of 4 to 8 numbers (0-9).

1. Select **DECT** > **System**.

   Note:
   To access the **System** tab, the Master mode has to be activated, see Selecting Mode on page 154.

2. Enter an authentication code in the **Authentication Code** field.
3. Click **OK**.

Setting the default language

If the telephone does not send language information to the system, this setting determines the language that the telephone displays for some text messages, for example, hung-up and disconnected.

1. Select **DECT** > **System**.

   Note:
   To access the System tab, the Master mode has to be activated, see Selecting Mode on page 154.

2. Choose the language in the **Default Language** drop-down list.
3. Click **OK**.

DECT frequency band configuration

Note:

The frequency band configuration is only needed if other frequencies than EU US China shall be used. Additionally, if the handset has been returned from repair, the applicable frequency band might require configuration again.

To change the operating frequency band, the following preconditions must be fulfilled:

- The frequency is set to Not initiated. This can be checked by entering the Admin menu, follow the path: Admin menu > Device info > Hardware.
  Scroll down to “Frequency band”.
- The handset must not have a DECT registration. If it already has, perform a Factory reset. See Performing a Factory reset on page 210

1. Enter the Admin Menu.
2. Select "Frequency band" and select the desired band.
   - EU US China (default)
   - LA (Latin America)
   - Brazil (This is a POE only solution)
   - 1900 - 1920 MHz
   - Multifrequency, See Multiple frequency support on page 151
3. Restart the handset.
4. Register the handset. The frequency band option will no longer be available.

Note:

The selection is persistent and will stand a factory reset.

Multiple frequency support

You can use the handset in a system that changes frequency by selecting *Multifrequency* as frequency band in the handset. See DECT frequency band configuration on page 151. This setting is applicable for handsets used in different regions of the world. For example for users working on a ship that visits different countries.

When the frequency band is set to *Multifrequency*, the handset will adopt to the applicable frequency band (EU, US or Brazil) used in the specific region after it has been restarted.

Note:

The handset will adopt to the frequency band configured in the DECT system.

The recommended procedure when changing frequency band is as follows:

1. The site administrator sends out broadcast message to all handsets informing that

the handsets need to be restarted at a specific time.

2. The site administrator enters IP-DECT master and change setting for the frequency and carriers just before the specific time.
3. All handset users restart their handsets. After the restart the handsets have changed to the applicable frequency band (EU, US or Brazil).

Setting the frequency band

The IPBS/IPBL can operate in the following frequency bands:

- 1880 - 1900 MHz, Europe, Africa, Middle East, Australia, New Zealand and Asia
- 1910 - 1930 MHz, South America
- 1920 - 1930 MHz, North America
- 1910 - 1920 MHz, Brazil. (Brazil is a POE only solution)

1. Select **DECT** > **System**.

   Note:
   To access the System tab, the Master mode has to be activated, see Selecting Mode on page 154.

2. Select frequency area in the **Frequency** drop-down list.

   Important:
   You must select the correct frequency band for your region. **Otherwise you will violate local laws!**

3. Click **OK**.
4. Reset in order to make the changes take effect, see Reset on page 190.

Enabling carriers

The IPBS/IPBL has 5 carriers for the North American frequency band and 10 carriers for the other frequency bands. Normally you must enable all carriers.

To enable or disable carriers:

1. Select **DECT** > **System**.

   Note:
   To access the System tab, the Master mode has to be activated, see Selecting Mode on page 154.

2. Select the **Enabled Carriers** check boxes.

Note:

For Brazil, the following carriers shall be selected only: 0, 1, 2 and 3.

3. Click **OK**.

Configuring coder

Select the preferred coder, and enter the desired frame length. If you select exclusive for the coder, the IPBS/IPBL is forced to use that coder. When you enable Silence Compression no information is sent during pauses in the conversation which saves bandwidth.

Note:

If you enable exclusive for a coder you cannot make calls outside the IP-DECT system. G450 system only supports G.711A/ µLaw, G.729a, Coder G723-53 is not supported.

See Enabling SRTP on the base stations. on page 166

1. Select **DECT** > **System**.

Note:

To access the System tab, the Master mode has to be activated, see Selecting Mode on page 154.

2. Choose the applicable coder in the Coder drop-down list.
3. Enter the sample time in milliseconds in the **Frame** text field.
4. Select or clear the **Exclusive** check box.
5. Select or clear the Silence Compression check box.
6. Click **OK**.

Configuring Supplementary Services

The supplementary services handle the defined dial codes locally in the IPBS/IPBL master. All other dial codes to be forwarded to the Call Manager must be configured on Master and Standby Master.

1. Select **DECT** > **Suppl. Serv**.

Note:

You must activate the Master mode to access the System tab. See Selecting Mode on page 154.

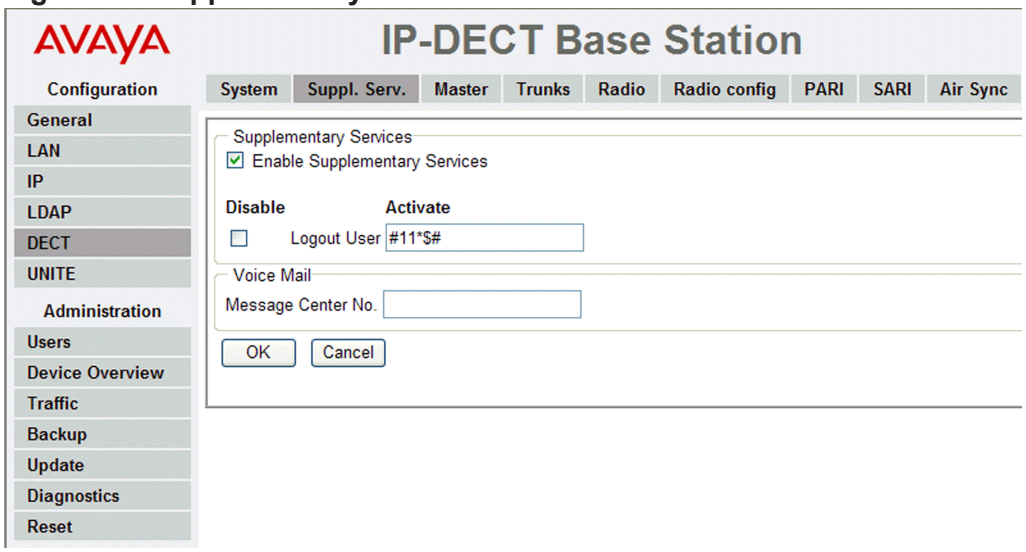
2. Select the **Enable Supplementary Services** check box to activate the supplementary services below. The default **Activate** feature code is preset.

Note:

To disable a specific service, select the Disable check box next to the option.

3. Enter the Message Center Number in the **Fix Message Center No.** field.
4. Click **OK**.
5. Reset in order to make the changes take effect, see Reset on page 190.

Figure 46: Supplementary services



Selecting Mode

The IPBS/IPBL can operate in four different modes: Master, Standby Master, deployment and off.

1. Select **DECT** > **Master**.
2. In the **Mode** drop-down list, select:
   - "Off", if this IPBS/IPBL is not a Master.
   - "Active", if this IPBS/IPBL is the Master.
   - "Standby", if this IPBS/IPBL is the Standby Master.
   - "Deployment" is used for coverage test only. The speech from the handset is looped back to the handset.
   - "Mirror", if this IPBS/IPBL is the Mirror. For information about Mirror devices, see the system description for IP-DECT.

3. If you have selected the "Mirror" mode enter the IP address to the other Mirror Master in the Mirror Master IP address text field.
   For the Master that initially shall be the active Mirror: Click on the text link "Activate mirror". Any user and handset data in the inactive Mirror will be replaced with the user and handset data stored in the active Mirror.
   To switch the active role between the Mirror Masters, click on the text link "Switch active mirror". Note: This should be done within a maintenance window as all active calls will be lost.
4. Click **OK**.
5. Reset in order to make the changes take effect, see Reset on page 190.

Entering admin password

1. Select **DECT** > **System**.
2. Enter password.

Note:

Create a backup of the IPBS/IPBL configuration when you change the administrator password. See Backing up on page 182.

Configuring Master ID

Only applicable on the Master and standby Master.

You only need the Master ID configuration in a Multi Base Station Master scenario. For a single IPBS/IPBL Master, use Master ID 0.

In a Multi Base Station Master scenario, configure an individual Master ID for each IPBS/IPBL Master in the range of 0 and 250. Use Master ID “0” for IPBS/IPBL Master1, which is the LDAP server of the IP-DECT system. All further IPBS/IPBL Masters doing the LDAP replication should use a Master ID from 1 to 250.

A standby Master must use the same Master ID as the corresponding IPBS/IPBL Master.

Configuring IP-PBX

Only applicable on the Master.

1. Select **DECT** > **Master**.
2. Select PBX.
3. Enter the ARS Prefix, for example, 00 for calling outside the building.
4. Enter the International CPN Prefix, for example, 0046 for Sweden.
5. Enter the National CPN Prefix, for example, 031 for Göteborg.

Configuring trunks

Trunks cannot be configured (configuration sets will be greyed out) in the IPBS/IPBL when Provisioning is used with IPO PBX. However, it will still be possible to activate a primary trunk manually (see Activation of Primary Trunks on page 83). About Provisioning, see 4.1.6 Provisioning on page 37.

A shared trunk is used for connection between the IP-DECT system and an PBX which can be an ACM PBX or an IPO PBX.

There are two kinds of trunks; primary and redundant. One or more primary trunks can be configured. They are used in the first place. One or more redundant trunks can also be configured. They are only used if none of the primary trunks are in "Active" mode. That is, all primary trunks must be in "Down" mode.

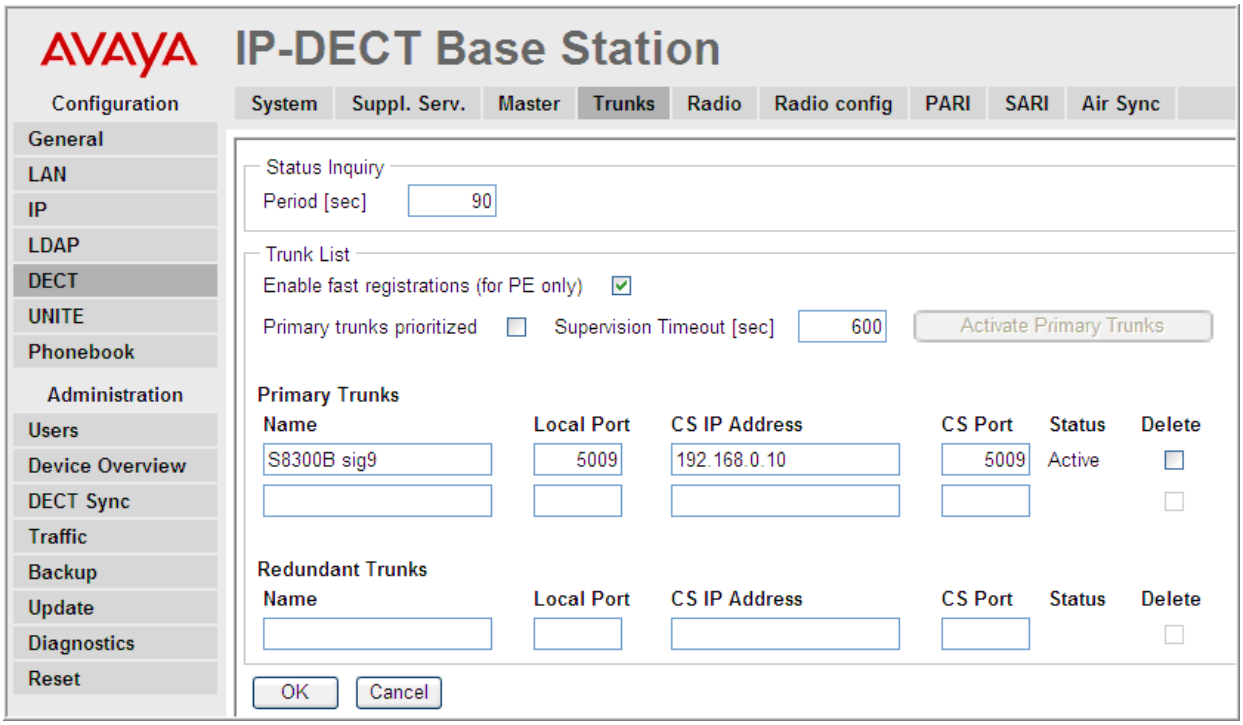
Note:

Only one primary and one redundant trunk can be configured for the IPO PBX.

To configure primary and redundant trunks, do as follows:

1. Select DECT > Trunks.
2. To determine the status of the trunks towards the IP-PBX, enter in the Period (sec) field how often the IPBS/IPBL shall send status inquiry messages to the IP-PBX.
3. Enter the IP Address of the IP-PBX in the CS IP Address field and the port of the IP-PBX in the CS Port field.
4. Enter port address of the IPBS in the Local Port field.
5. If a redundant trunk shall be configured for connection to the IPO PBX, make sure that the PBX Resiliency check box has been selected (DECT > Master).
6. Note: The PBX Resiliency check box will be disabled (greyed out) when Provisioning is enabled in the IPBS/IPBL. About Provisioning, see 4.1.6 Provisioning on page 37.

Figure 47: Trunks



Primary and Redundant are the two types of trunks. You can configure one or more Primary Trunks. Primary Trunks are used in the first place. You can configure one or more Redundant Trunks that are used when all Primary Trunks are inactive.

Trunk modes

Primary and Redundant Trunk have four different modes.:

Active	The trunk is active and currently used for traffic to PBX.
Up	The trunk is active but currently not used for traffic to PBX.
Down	The trunk is inactive and communication to PBX is not working.
Standby	The trunk is currently not supervised but could be used for redundant purpose.

Note:

Do not set a Primary Trunk to Standby.

Up or Down mode indicates weather the trunk is connected with the PBX and is correctly configured in both the PBX and the IP-DECT system. A trunk that is Active or Up is correctly configured and correctly attached. A trunk that is Down has a fault, either in the configuration or the hardware. For example, a broken cable. Fault finding can include checking the IP address and port as well as the PCB and the cable.

Trunk supervision on IPBS/IPBL Master and Standby Master is a regular testing to see if the IP communication with the Communication Manager still works. Status inquiry messages are sent periodically for all trunks in Active, Up, and Down state to Communication manger to test if the status has changed. Redundant Trunks in Standby mode are not supervised. Supervision of Redundant Trunks starts only if all the Primary Trunks are in Down status and the Redundant Trunks requires to be used instead.

Load Balancing

You can configure several Primary trunks and Redundant trunks for communication between the IPBS/IPBL Master and Communication Manager. One trunk can support up to 250 simultaneous IP-DECT calls. If you configure more than 250 IP-DECT users on the IPBS Master, perform an Erlang traffic calculation to decide the number of Active trunks required to meet customer requirements.

Note:

To overcome limitations related to number of simultaneous calls and performance when the trunks are connected to CLAN boards, keep the traffic on the system within the following limits:

- Maximum 600 DECT users per CLAN
- Maximum 1500 calls/hour per CLAN

Example: When one of the active CLAN trunks goes down, the users are moved to the remaining active trunks. Ensure that the recommendation matches such a situation as well.

If possible, follow the recommendation to use Processor Ethernet (PE) instead of CLAN for IP-DECT trunks.

The IPBS master automatically assigns an IP-DECT user to one of the Active trunks. So a kind of static load balancing exists in the system. However, if the number of Active trunks is not sufficient for the configured number of DECT users, the reason might be that some users on one active trunk are busy while users on another active trunk are still available.

Note:

Do not configure more than 10 Primary Trunks and 10 Redundant Trunks in the IPBS Master. The group of Primary Trunks are usually configured on the same Communication Manager system. You can even configure a group of Primary Trunks on a Communication Manager network, for example, several Communication Manager systems connected to a trunk and working on the same numbering plan. The same applies to a group of Redundant Trunks.

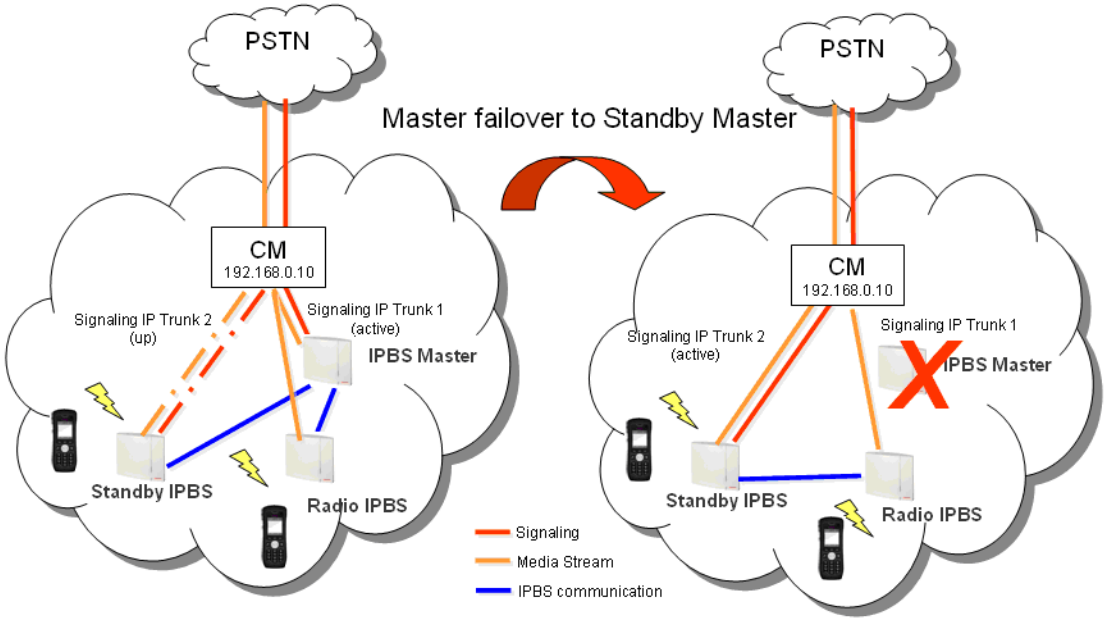
Basic trunk configuration for IPBS Master and Standby Master

Configure at least one Primary Trunk on the IPBS Master for communication with Communication Manager. This trunk goes to Active mode during normal operation of the IPBS Master. Additionally, configure an IPBS Standby Master to handle a failover if the IPBS Master is out of operation. Configure a second trunk to Communication Manager on the IPBS Standby Master. When the IPBS Master operates nomally, this trunk remains in the Up state, that is, communication with Communication Manager is established but currently not in use.

If the IPBS Master goes out of operation, the Standby Master takes over after some time. The trunk on the IPBS standby Master now goes to Active mode and the communication with Communication Manager is done through this trunk. On Communication Manager side, the DECT XMobile stations are moved to the trunk group connected to the Standby Master. Therefore a proprietary H.323 X-Mobile message from the Standby master to the Communication Manager for each DECT user is sent.

If IPBS Master comes back into operation, IPBS Master again sends a message to change the trunk group configuration on Communication Manager side back to the trunk used by the Master.

Figure 48: Basic Trunk configuration for IPBS Master and Standby Master

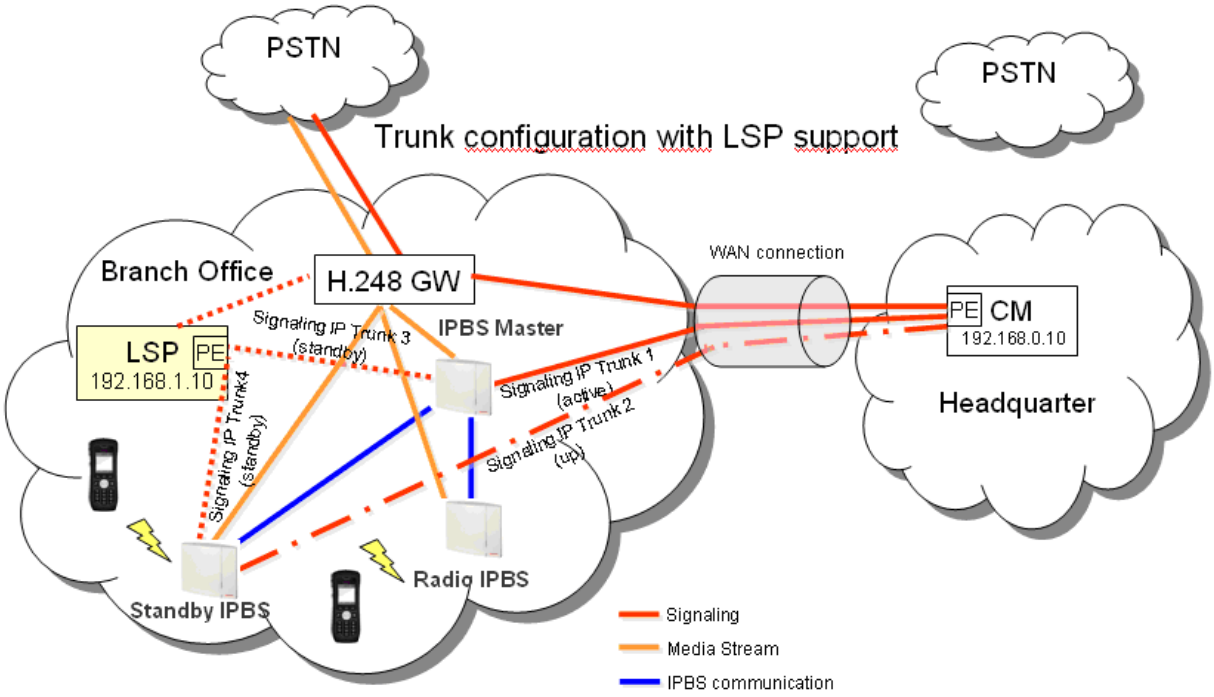


Redundant Trunk Configuration

Redundant Trunks on IPBS Master and Standby Master handle outages on the Communication Manager side or on the network, for example, on WAN. A Redundant Trunk configuration is supports, for example, a LSP failover in a Branch office in case of an outage of the IP-connection to the headquarters. A Redundant Trunk configuration can also be used to different CLAN boards for redundancy reasons in case of single CLAN outages.

A Redundant Trunk is configured as a backup to the Primary Trunk either on the IPBS Master or Standby Master. If the Primary Trunk is Active or Up, the status of the Redundant Trunk remains as Standby. The status of the Redundant Trunk changes to Active or Up if all the configured Primary Trunks are Down. If the Redundant Trunk returns to Active status, the calls go through the Redundant Trunk until at least one Primary Trunk comes back to Active status.

Figure 49: Redundant Trunk Configuration



In such scenario, a Primary Trunk to the *main* Communication Manager in the headquarters is configured on the IPBS Master (and Standby Master). These trunks are used as long as communication with the Communication Manager in the Headquarter is possible. The Redundant Trunk on the IPBS Master (and Standby Master) is in Standby status.

In case of an outage of the main Communication Manager or a broken WAN connection, the Primary Trunk on the IPBS Master (and Standby Master) will go to status Down and the Redundant Trunk on the IPBS Master will go to Active mode. On the Standby Master, the Redundant Trunk will come to status Up. Now the communication with the LSP will be done through the active Redundant Trunk.

Switching back to Primary Trunks

When Redundant Trunks are active and at least one Primary Trunk is in the Up mode, you can go back to the Primary Trunks using either the Manual or the Automatic mode.

Manual

1. Click the **Activate Primary Trunks** button. (This button is only available if there is any Primary Trunk in Up mode.)

The Primary Trunks then enter Active mode and the Redundant Trunks cease to be active and go to Standby mode. New calls go through the Primary Trunks and ongoing calls go through the Redundant Trunks until the calls are finished.

Automatic

1. Select the **Primary trunks prioritized** check box.
2. Set the **Supervision Timeout** to the required time.
   When the Primary Trunk returns back to Up mode, the Primary Trunk automatically changes to Active mode when the supervision timer elapses. The timer is stopped if the Primary Trunk goes to Down mode again and is restarted if the Primary Trunk returns back to Up mode. This timeout ensures a stable Primary Trunk connection before switching back the trunks for normal operation.

Enabling the radio

If the IPBS/IPBL is not used as a Radio, for example, only used as a PARI Master, select the **Disable** check box to disable IPBS/IPBL.

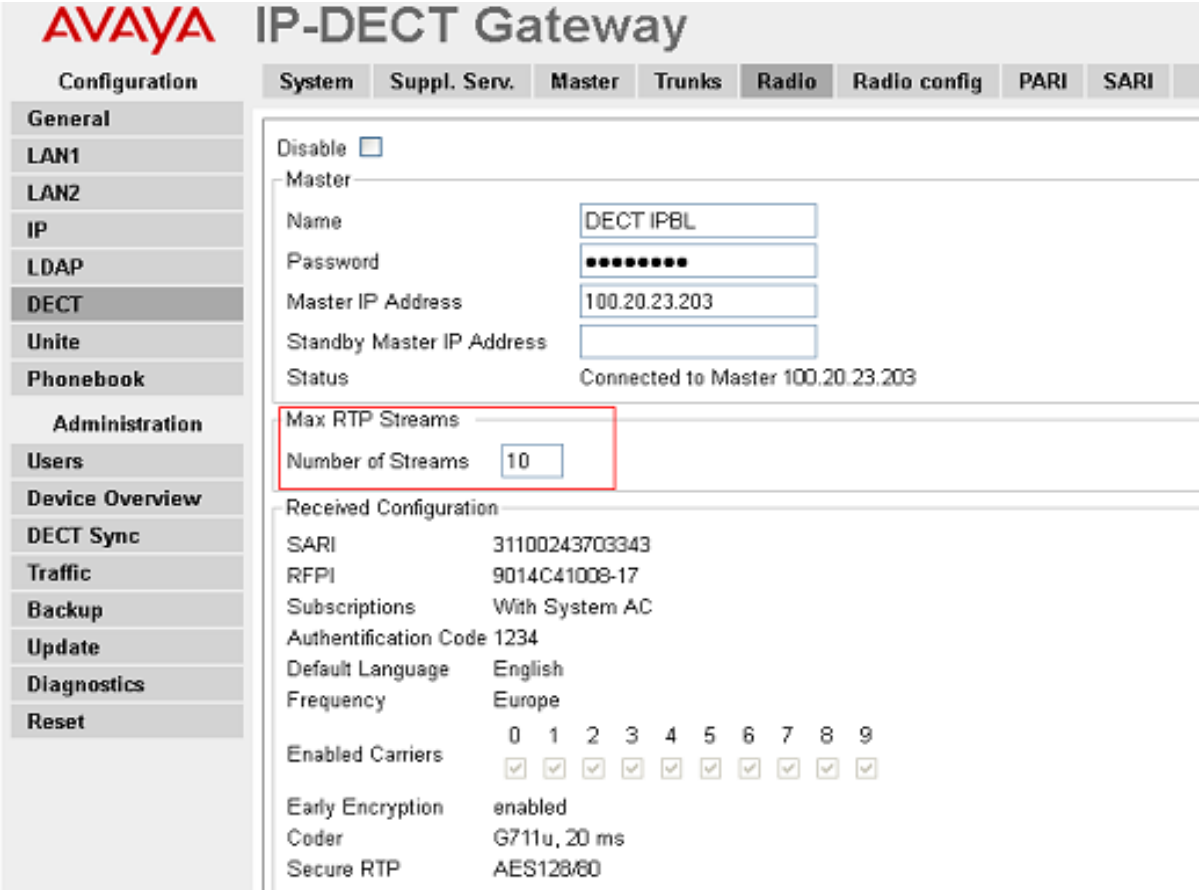
1. Select **DECT** > **Radio**
2. Clear the **Disable** box.
3. To assign a PARI Master (see Entering the IP address to the PARI Master on page 162 for explanation of PARI Master), enter the name and password of the PARI Master to connect to. If this is the PARI Master, the internal name and password (found under **DECT** > **System**) and the loopback address 127.0.0.1 should be used.

Configuring limit for RTP streams

You can limit the maximum number of RTP voice streams to the Base Station so that during a handover, the traffic on ISDN lines to distant IPBS does not exceed the bandwitdh capacity of the connecting links.

Note:

This configured limit includes the sum of calls over the air interface and forwarded calls.



Entering the IP address to the PARI Master

All base stations/IPBL need to know the IP address of the PARI Master.

1. Select **DECT** > **Radio**.
2. Write the name for the PARI Master in the **Name** text field.
3. Enter the password for the PARI Master in the **Password** text field.
4. Enter the address to the PARI Master in the **PARI Master IP Address** text field. If this is the PARI Master, enter **127.0.0.1**.
5. Click **OK**.
6. Reset in order to make the changes take effect, see Reset on page 190.

Multiple Radio configuration

The PARI Master can configure the same Radio settings for all Radios in the system. All settings configured in the Radio Config page replace the local Radio settings. This means that all settings in the **Radio Config** menu will have precedence over values configured locally or received via DHCP options.

- Events and Alarms: See Configuring logging on page 129
- Update: See Configuring automatic Firmware update on page 127
- Network Time: See Configuring the NTP settings on page 128
- Priority/Diff/Serv: See Configuring IP settings sub menu on page 144
- Port Ranges: See Configuring IP settings sub menu on page 144

1. Select **DECT** > **Radio Config**.
2. Configure alarm and event forwarding, seeForwarding alarms and events on page 130.
3. Configure automatic firmware update, see Configuring automatic Firmware update on page 127.
4. Configure NTP settings, see Configuring the NTP settings on page 128.
5. Configure IP settings, see Configuring IP settings sub menu on page 144.
6. Click **OK**.

PARI

PARI is a part of the broadcast identity, which uniquely identifies an IPBS/IPBL. This PARI is automatically assigned to each IPBS/IPBL in the system. But if more than one Avaya IP-DECT system operates within the same coverage area, the systems need to have a unique system identity in the PARI assigned in order to differentiate the systems.

To see the occupied system IDs of other Avaya IP-DECT systems within the coverage area, perform an RFP scan, see Backing up on page 182.

1. Select **DECT** > **PARI**.

- Select a number between 1 and 35. If this is not done the IPBS/IPBL will randomly select a number.
- Select a number between 1 and 292. If this is not done, the IPBS/IPBL will randomly select a number.

Note:

The number of system IDs will affect how many IPBSs/IPBLs that can be used per Master in an installation, as shown below:

- System ID = 1 to 36:
- Max. 1023 IPBS per Master or max. 240 IPBL per Master.

- System ID = 37 to 292:
- Max. 127 IPBS per Master or max. 127 IPBL per Master.

2. Click **OK**.
3. Reset in order to make the changes take effect, see Reset on page 190.

SARI

SARI is the system broadcast identity, which uniquely identifies an IP-DECT system. It is needed to make the IP-DECT system operate. The SARI is added in the Master.

Note:
When changing the SARI the subscription data of all subscribed cordless telephones will get invalid even if they are shown as subscribed in the **User** tab. So they have to be unsubscribed manually and subscribed again.

1. Select **Dect** > **SARI**.
2. Enter the license number delivered by your supplier in the **SARI** text field.
3. Click **OK**.
4. Reset in order to make the changes take effect, see Reset on page 190.

Configuring air synchronization

This section is applicable only to the IPBS System

The IPBSs use the DECT air interface to synchronize to each other. For an individual IPBS it is not required to configure with which IPBS it needs to synchronize. It is needed to manually select one or several IPBSs as synchronization master candidate. PARI Master assigns one of these IPBS as an active Sync Master. The remaining candidates act as sync slaves and can be new Sync Masters in case the active Sync Master fails. When using one sync region it is recommended to configure at least two base stations in the middle of the building as synchronization masters.

All IPBSs in sync slave mode sends its list over received sync candidates to the Master. The Master informs the IPBS sync slaves which sync candidate it shall synchronize to.

Mixed System

All IPBLs are synchronization masters in region 0. Any IPBS in this region will receive its synchronization over the air from the RFPs, which are connected to the IPBL.

Sync regions

Sync regions are used when, for example, several buildings are located in the same coverage area and all radios are using same PARI Master but where the synchronization coverage between buildings is not good enough for a stable synchronization.

A solution may be to use separate synchronization regions for the buildings and have reference synchronization between the regions. Each region has its own Sync Master but can take reference sync from another region and handover between the buildings is possible. If a region should lose the reference synchronization with another region, the internal synchronization in respective region will still work but there can be no handover between the regions.

Note:

For the synchronization to work, it is not allowed to configure reference sync in a ring.

Configuring Sync Slave IPBS

All base stations in sync slave mode sends its list of sync candidates to the PARI Master. The PARI Master informs the IPBS sync slave with which sync candidate it shall synchronize.

In addition to the above automatic synchronization procedure, it is also possible to use static synchronization, that is, manually lock on to a specific RFPI. However when specifying a specific RFPI the RFPI must be within the same synchronization region.

Configure Sync Slave as follows:

1. Select **DECT** > **Air Sync**.
2. Select **Slave** in the **Sync Mode** drop-down list.
3. For static air synchronization (if required), manually lock the sync slave to a specific RFPI by entering the sync RFPI in the **Sync RFPI** field.
4. Enter an alternative sync RFPI in the **Alternative Sync RFPI** field (optional).
5. Enter a region ID between 0 and 63 in the **Sync Region** field.

   Note:

   An empty **Synch Region** parameter is equal to synch region 0.
6. Click **OK**.

Configuring Sync Master IPBS

Radios configured as Sync Master report to the PARI Master that it wants to be a Sync Master. The PARI Master then selects one of them to be the active Sync Master.

When a Sync Master has been assigned to be active, it searches for other IPBSs/IPBLs within the same region during 30 seconds. If any IPBS is found, the values for slot, frame, multi frame and PSCN are received and applied to the Sync Master. After receiving all these values or after the time-out of 30 seconds, the Sync Master enters the master state.

With this method, it is possible to restart only the Master in the region. The remaining slaves can maintain synchronization for a few minutes during restart of the Master. The Master adjusts itself to the other IPBSs at startup. The slaves notice that the Master is back and the synchronization is received from the Master.

In master state, the values are updated locally during all further operation of the Master IPBS and no synchronization to other IPBSs in the same region is done.

It is possible to configure the Sync Master to synchronize to a reference base station (another DECT system or the same DECT system but a different sync region). In this case, the Sync Master will try to synchronize to the reference system if the reference system is found, but it will not require the reference system to be available. The Sync Master will operate even though the reference system is not available. During startup, the Master will prefer to synchronize to a slave base in the same system before synchronizing to the reference base station.

Configure Sync Master as follows:

1. Select **DECT** > **Air Sync**.
2. Select **Master** in the **Sync Mode** drop-down list.
3. To synchronize the Sync Master to a reference base station, enter the reference base station in the **Reference RFPI** field.
4. Enter an alternative reference base station in the **Alternative reference RFPI** field (optional).
5. Enter a region ID between 0 and 63 in the **Sync Region** field.

   Note:
   An empty **Synch Region** parameter is equal to synch region 0.
6. Select **Action at reference sync failure** as one of the following:
   - Resynchronize on command (manually)
   - Resynchronize every day (automatically)
   - Resynchronize once per week (automatically)

   If automatic resynchronization is selected, the master will restart the synchronization at the scheduled time if the synchronization to the reference system is lost. If manual resynchronization is selected, the administrator can manually restart the synchronization to the reference system if required. See Reference synchronization on page 179.
7. Click **OK**.

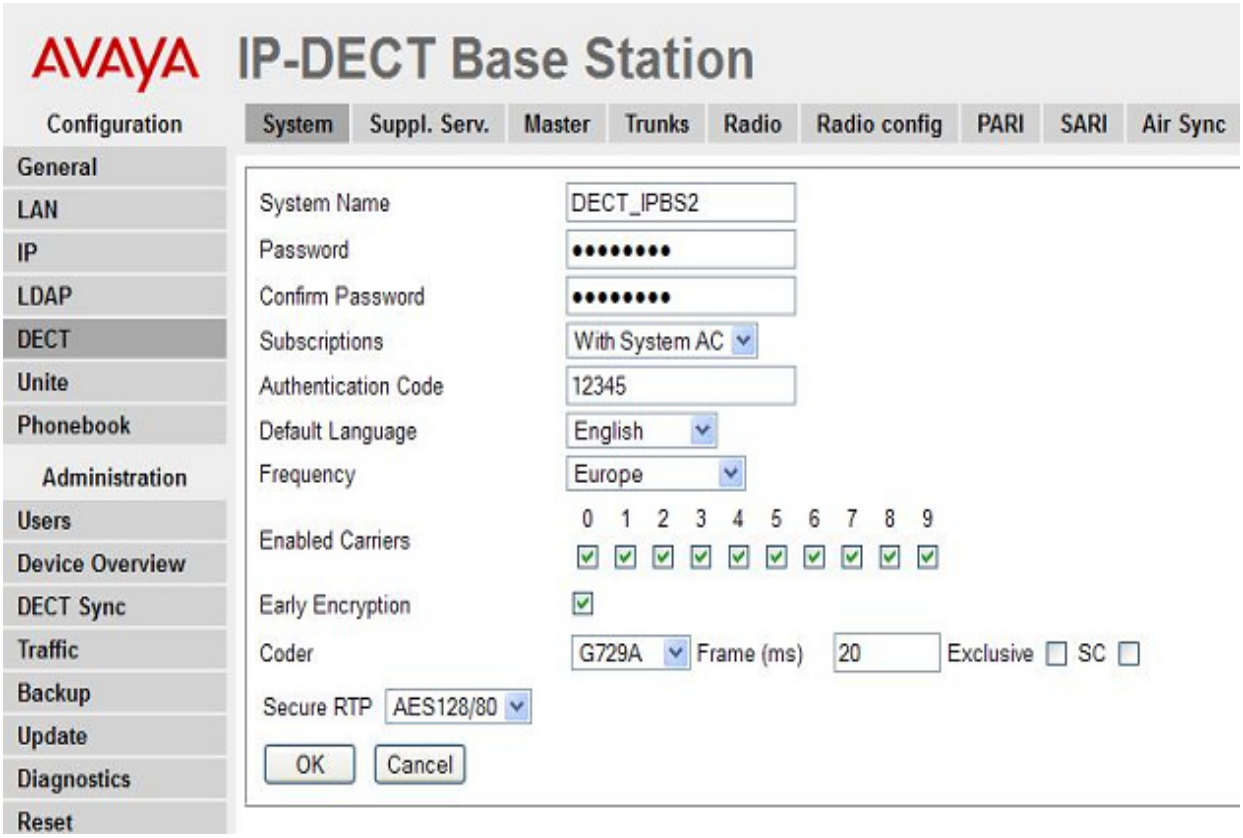
Enabling SRTP on the base stations.

Before you enable SRTP on the base station, see Verifying License Grant permissions for configuring SRTP on page 264.

Important:
SRTP is not supported on IPBS1 as of DECT R4 Edition 4. SRTP is supported only on IPBS2 and IPBL. In any environment that includes IPBS1, you muse not enable SRTP on the master IPBS/IPBL.

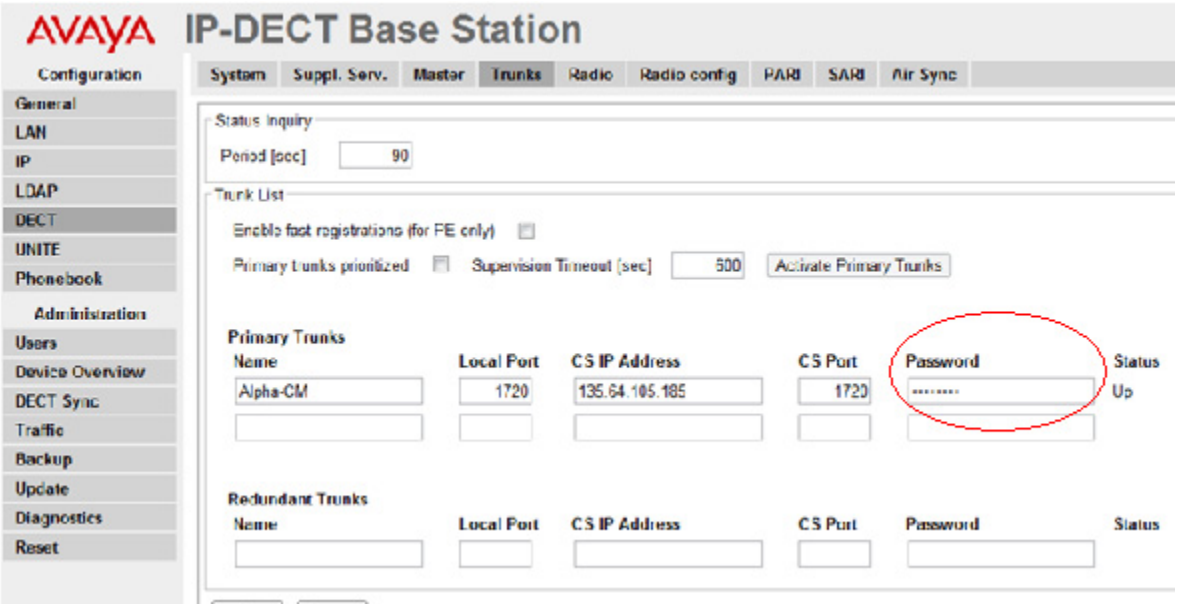
1. Select **DECT > SYSTEM**
2. To enable SRTP, select a cryptographic suite from the Secure RTP drop-down list.

   To disable select the empty row at the top of the Secure RTP list.

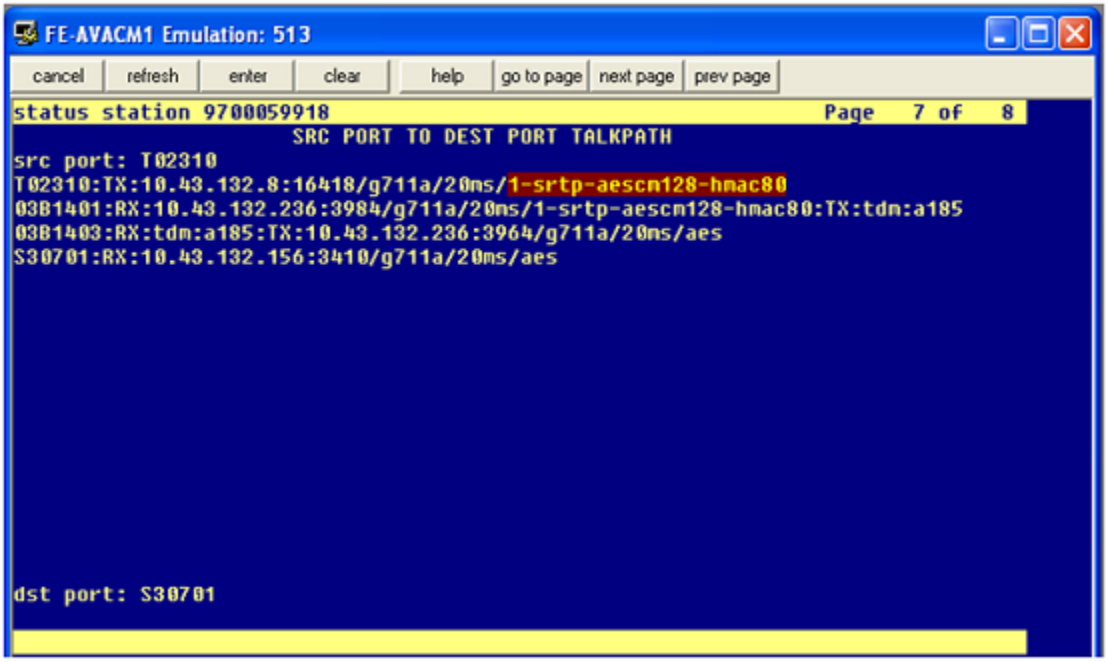


3. Select **DECT > Trunks**

   Enter a password – Ensure that this password is the same the signaling group passphrase.
   See see Verifying License Grant permissions for configuring SRTP on page 264.



4. Use station status command in CM SAT terminal to verify if SRTP is enabled.



UNITE

Configuring messaging

If an AIWS is to be used in the IP-DECT system, enter the IP address following the steps below.

1. Select **UNITE** > **SMS**.

   Note:
   To access the SMS tab, the Master mode has to be activated, see Selecting Mode on page 154.

2. Enter the address to the AIWS in the **IP Address** text field.
3. Click **OK**.

Device management

If a specific Device Manager (e.g. AIWS2) is to be used in the Avaya IP-DECT system, enter the IP address to the Device Manager following the steps below. To set the Master to search for an existing Device Manager on the network, go to Service discovery on page 170.

1. Select **UNITE > Device Management**.

   Note:
   To access the **Device Management** tab, the Master mode has to be activated, see Selecting Mode on page 154.

2. Enter the address to the Device Manager in the **Unite IP Address** text field.

   The IP address for the Device Manager that the Master is currently connected to is shown under **Active Settings**.

3. Click **OK**.
4. Reset in order to make the changes take effect, see Reset on page 190.

Note:
However if device management is used the IP-Address of the AIWS needs to be configured in the **UNITE -> SMS** tab as well, see Configuring messaging on page 169.

Configuring the location

In a bigger IP-DECT system with offices on several locations it is possible to configure one Master Base Station on each office.

The location ID defined in the AIWS describes the digit handling for centralized phonebook search depending on the location of each Master Base Station. For each Master Base Station and Standby Master Base Station the Location ID needs to be defined to select the appropriate digit treatment for your location. The AIWS supports 100 locations. The location ID need to be between 1 and 250.

Each Master Base Station and standby is identified from the AIWS by a unique number. The AIWS currently supports 100 network regions.

1. Select **UNITE > SMS**.

   Note:

   To access the SMS tab, the Master mode has to be activated, see Selecting Mode on page 154.

2. Enter a number identifying the Location in the **Location ID** field.

   The region ID set in the IPBS Master or Standby Master needs to correspond to one of the configured Region IDs in the AIWS. The digit treatment for a central phonebook query in the cordless telephones will be done according to the defined rules for the region ID of the IPBS Master or Standby Master the telephone is connected to. IPBS Masters and Standby Masters can use the same IP-Region ID, so they will use the same digit treatment rules.

3. Click **OK**.

Service discovery

If no Device Manager (e.g. AIWS) has been selected to be used in the Avaya IP-DECT system, see Device management on page 169, then the Master will automatically search for an existing Device Manager on the network. To set the Master to search in a specific domain on the network or to stop the search, follow the steps below.

1. Select **UNITE > Service Discovery**.

   Note:

   To access the **Service Discovery** tab, the Master mode has to be activated, see Selecting Mode on page 154.

2. Do one of the following:

   - To stop the Master to search for a Device Manager, select the **Disable** check box.
   - To set the Master to search for a Device Manager in a specific domain on the network, enter the domain id in the **Domain ID** text field. The domain id must be the same as the one entered in the Device Manager.

3. Click **OK**.

Sending status log

It is possible to send alarm and event reports to the Unite system. For example, directly to the Unite CM (Connectivity Manager) fault handler or to the UNA (Unite Node Assistant) which in turn forwards the alarm event according to distribution lists.

1. Select **UNITE** > **Status Log**.
2. Enter the address to the server where the Status Log should be sent in the **Unite IP Address** text field.
3. Enter the Resource Identity/Service in the **Unite Resource Identity** text field. If this field is left empty, then the default will be UNA (Unite Node Assistant).

Users

This section describes the **Users** sub menu and how to do the following:

- Add a user.
- Add a user administrator.
- Search for user information.
- Show all registered users in the IP-DECT system.
- Import a csv file with user information.
- Export a csv file with user information.

Adding a user

For information on how to add users to the IP-DECT system, see Adding users on page 112.

Add a User to Another IP-DECT System

To allow handsets to identify the system to which the subscription shall be directed (e.g. the same physical area may be covered by different systems), it may be necessary to enter an initial PARK into a handset.

To view the PARK and the PARK 3rd pty code:

1. Select Users > Users.
   - *PARK*: Must be used for Avaya handsets. Can also be used for other handsets if they support a PARK that matches the SARI.
   - *PARK 3rd pty*: Must be used for handsets that do not support a PARK that matches the SARI.

Note:

For information on how to subscribe the user's handset to the other IP-DECT system, see the reference guide for the handset.

Import Users from a csv file

If many users should be added it is possible to import a csv file with the IPEI / IPDI.

Field name	Description	Max. characters
Long Name	Mandatory, the name of the user, need to be unique throughout the system. This is the name presented in a called party´s display, unless this is configured in the IP-PBX.	30
Display Name	Optional, will be shown in the handset display when the handset is idle.	30
Name	Optional, the user name.	30
Number	Mandatory, the phone number extension, need to be unique throughout the system.	30
Password	Optional, is used for registration towards the gatekeeper.	15
IPEI / IPDI	The unique identification number of the handset.	
Auth. Code	Optional, the individual authentication code for this user. Automatically created by default. Can be modified manually.	

The csv file may have the following format:

Long Name;Display Name;Name;Number;Password;IPEI/IPDI;Auth Code;

Different separators may be used in a delimiter-separated file. Import of files with the separators semicolon or TAB is supported.

1. Select Users.
2. Click “Import”.
3. Click “Browse” to locate the csv file.
4. Click Open > Next Make sure the correct number of entries are correct.
5. Click Next

Limitations

- Maximum 1000 rows in the csv file.
- The maximum csv file size is 128 Kb. If the file is to large, divide the file into several files.
- Only the new user data is imported. The old user data is not deleted.
- Existing user data cannot be updated.

- If the separator is wrong an error message will be displayed.
- The Authentication Code (AC) can not be entered in the csv file for safety reasons. The system generates a AC for every user in the list. If the user needs the AC the administrator will have to use Show, see Showing all registered users in the IP-DECT system on page 173.

Export the Users to a csv file

The Users can be exported to a csv file, for example for editing or backup reasons.

1. Click “Export”.
2. Click “Save” in the dialog window that appears.
3. Enter a name of the file and select in which folder the file should be saved.
4. Click "Save".

For safety reasons, the Auth. Code and Password will not be included in the csv file.

Searching for user information

It is possible to search for users registered in the system by name or extension number. Search for a user following the steps below:

1. Select **Users** > **Users**.
2. Enter the name or number to search for in the text field. It is possible to enter only the beginning of the name or number.
3. Click **show**.

Showing all registered users in the IP-DECT system

1. Select **Users** > **Users**.
2. Click **show**.

Note:

Only the first 12 digits of IPEI/IPDI of the cordless telephone will be shown in the IPBS users tab even if all 13 digits needed to be entered when cordless telephone is subscribed (13th digit is the checksum).

Showing Anonymous

The IPEI number is displayed on anonymous registered telephones.

1. Select **Users** > **Anonymous**.

Unsubscribing users

1. Select **Users** > **Users**.
2. Click **show**.
3. Click ***User*** to unsubscibe.
4. Click **Unsubs.**

   The user is now shown as **Not Subscribed**.

When a user has been unsubscribed in the IPBS the subscription will automatically be deleted in the telephone when the telephone is currently connected to this system.

Note:

The user ID of the telephone is reset when you remove the last subscription on the telephone.

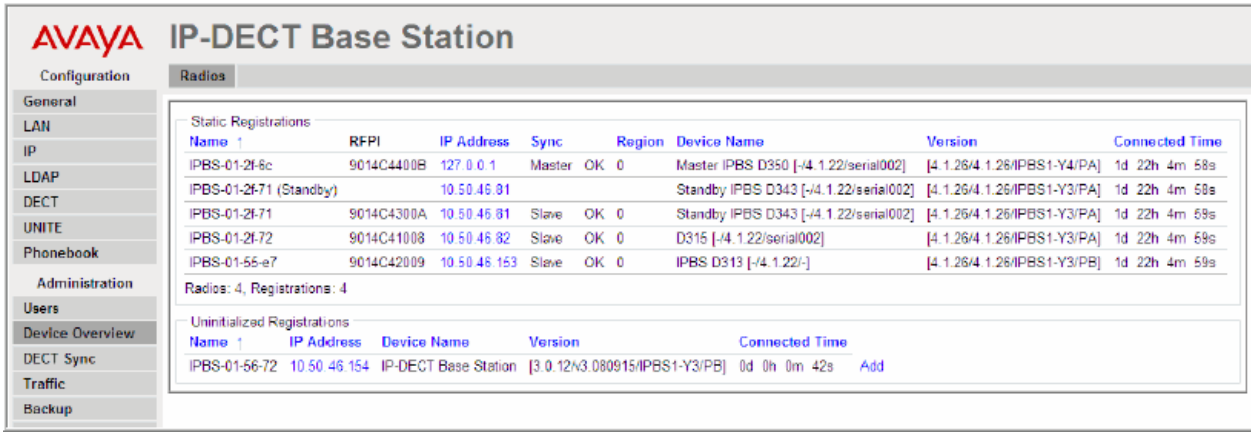
Device overview

Radios

Information about the devices in the IP-DECT system.

1. Select **Device Overview** > **Radios**.

Figure 50: Device Overview in the Master IPBS



Adding Radios

In the Uninitalized Registrations section newly added Radios are shown.

1. Select **Device Overview** > **Radios**.
2. Click **Add** to add the Radio to the Master.

3. In the **Add Radio** window enter a name for the device. You can also add a Standby Master IP Address.
4. Click **OK**.

The Radio restarts and it establishes a connection to the PARI Master only.

Name	The unique identification name. The name syntax is ipbs-xx-xx-xx, where xx-xx-xx should be replaced with the last 6 hexadecimal digits of the MAC address.
RFPI	Radio Fixed Part Identity.
IP Address	The IP address, click on the IP address to access the configuration GUI of that IPBS.
Sync	The current synchronization status. Should be **Master OK** or **Slave OK** if synchronized.
Region	Sync region, the radio is currently assigned.
Device Name	The name entered in the general menu.
LDAP	The LDAP status, can be "" (blank), "-", "up", "server" or "down". Should be "-", "up" or "server".
Version	The current software version.
Connected Time	The elapsed time since connected to the Master.

Add Radios

1. In the Uninitalized Registrations section, uninitialized Radios not registered to a Master are shown.
2. Select Device Overview > Radios
3. Click "Add" to add the Radio to the Master.
4. In the Add Radio window enter a name for the device. You can also add a Standby Master IP Address and a Sync Region.
5. Click "OK".
6. The Radio restarts and it establishes a connection to the Master only.

Deleting radios

In the Static Registrations section, initialized Radios no longer registered to the PARI Master are shown.

1. Select Device **Overview > Radios**
2. In the Static Registrations section, click **Delete** to delete the Radio.
   The Radio's RFPI is now released and can be reused. All other RFPIs in use are not affected.

Moving RFPIs

In the Static Registrations section, initialized Radios no longer registered to the PARI Master are shown. If it is vital that the new device keeps the RFPI for the broken device, move the RFPI for the broken device to the new device registered to the PARI Master.

1. Connect the replacing device.
2. Add the Radio to the PARI Master, see Adding Radios on page 174.
3. Select Device **Overview > Radios**
4. In the Static Registrations section, click **Move** for the Radio that is broken.
5. In the Move RFPI window, select in the Destination section the new Radio that you want to move the broken Radio's RFPI to.
6. Click the **Move** button.

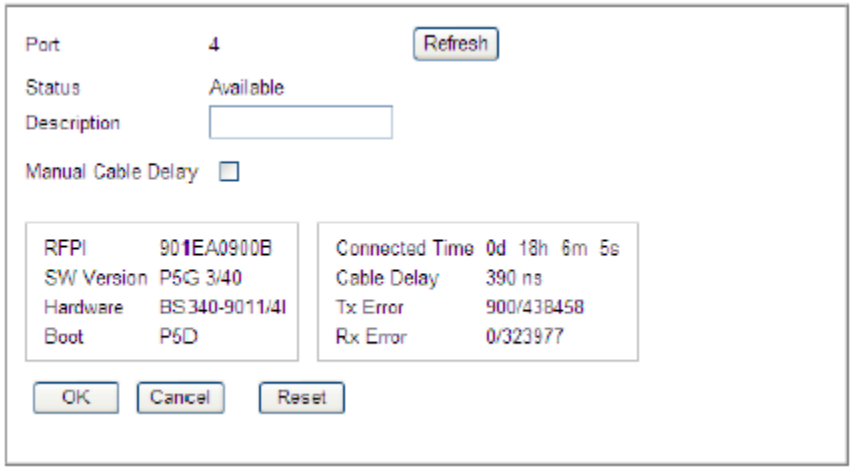
Existing RFPI on the new Radio is replaced by the broken Radio's RFPI. The new Radio's RFPI is now released and can be reused. All other RFPIs in use are not affected. The broken Radio will be deleted from the Static Registrations section.

RFPs

This section applies only to the IPBL.

Information about the DECT devices connected to the IPBL is available through RFPs.

1. Select **Device Overview** > RFPs.
2. Click the applicable port to open the RFP details pop-up window.



3. The following actions are available:

- Click **OK** to save your settings and close the pop-up window.
- Click **Cancel** to close the pop-up window.

- Click **Refresh** to update the information.
- Click **Reset** to reset the RFP.

Synchronizing ring

This section only applies to the IPBL.

A wire map of the synchronization ring is available in the GUI. The identities (IPBL-xx-xx-xx)

of the IPBLs and the position in the ring is displayed. If the ring is broken it is possible to locate where. Click the IP address to access another IPBL.

1. Select DECT Sync > Sync Ring.

Synchronizing ports

Sync Ports displays the current status of the synchronization ports.

1. Select DECT Sync > Sync Ports.

Status	The current status of the port.
Sync Offset	The synchronization offset for the IPBL.
Cable Delay	The delay caused by the cable.
Sync Lost Counter	The number of times synchronization lost.
Communication	The present status of communication.
Connected to	The IP address of the IPBL connected.
Tx Error	The number of transmitting errors.
Rx Error	The number of receiving errors

DECT Sync

Air sync overview

This section only applies to the PARI Master.

To see a graphical presentation of the air synchronization in a system, select **DECT Sync** > **Air Sync Overview**.

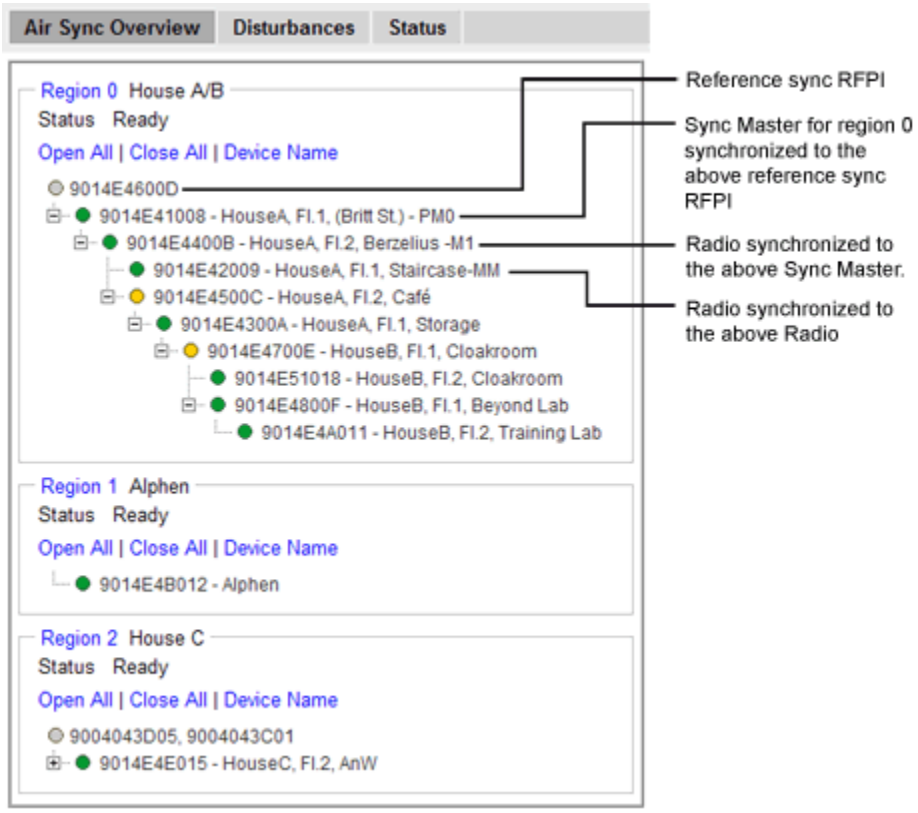
The internal synchronization for each region is shown separately by an expandable tree view, see figure 51. The green, yellow and red dots in the sync tree show the following sync status for the Radios:

- Green: Synchronized
- Yellow: Synchronized but poor received signal strength (RSSI < -83 dBm)
- Red: Unsynchronized

The grey dot at the top in the sync tree shows that it is a reference sync RFPI.

RFPI	Radio Fixed Part Identity is the Id number of the sync bearer.
Carrier	The carrier used for air synchronization
Slot	The slot used for air synchronization
Hop	The number of hops from the Sync Master to the sync bearer
RSSI	Received Signal Strength Indication
FER	Frame Error Rate, a value between 0 and 100%. Should be below 80% to be able to keep the synchronization.

Figure 51: The sync trees for region 0, 1 and 2 where region 0 is fully expanded.



Region details

1. Select **DECT Sync** > **Air Sync Overview**.
2. Click on the region ID text at the top of the sync tree.
3. If this has not already been done, in the Region Details window, enter a name for the region.
4. In section **Statistics**, there are two counters:

- Calculations: Is increased each time the sync tree is calculated.
- Configurations: Is increased when an IPBS has received a new sync instruction.

To clear the counters, click **Clear**.

Reference synchronization

To get the Sync Master to resynchronize to the reference sync, do as follows:

1. Select **DECT Sync** > **Air Sync Overview**.
2. Click on the region ID text at the top of the sync tree.
3. In the Region Details window, click **Start**.
   When resynchronizing, all ongoing calls in the region will be disconnected.

Disturbances

This section only applies to the PARI Master.

Select **DECT Sync** > **Disturbances**. A list of potential disturbances is displayed. That is, list contains alien DECT systems that have a higher signal strength than the current sync signal.

Status

This section only applies to active radios.

Air Sync status is displayed in the **DECT Sync** > **Status** menu. For explanation on the information shown for the active and the alternative sync bearers, see the table below.

Sync offset	Adjustment of frequency in progress performed by the current IPBS so it can be in synchronization with the sync source.
Drift	The time difference between the current IPBS and its sync source.
Sync lost counter	A counter that is incremented when the IPBS stops to handle radio traffic for a while and after that restarts the synchronization procedure.
RFPI	Radio Fixed Part Identity is the Id number of the sync bearer.
Carrier	The carrier used for air synchronization
Slot	The slot used for air synchronization
Hop	The number of hops from the Sync Master to the sync bearer
RSSI	Received Signal Strength Indication
FER	Frame Error Rate, a value between 0 and 100%. Should be below 90% to be able to keep the synchronization.

Sync lost counter

This section briefly describes the different situations when the *sync lost counter* is incremented and what impact it has for the users.

When an IPBS increaments the sync lost counter, it means that the IPBS stops to handle all radio traffic for a while and after that restarts the synchronization procedure. The radio part is not really restarted, but goes out of service for a short time period. The IP-part of the IPBS is not affected by this, but is in service all the time.

There are five reasons for which increment of the sync lost counter happens:

- The IPBS has not been able to find a synchronization source within 9 minutes.
- The PSCN value is changed.
- The value for frame number is changed.
- The value for multi frame number is changed.
- The number of enabled carriers is changed.

If the PSCN, frame number, multi frame number, and/or the number of enabled carriers are changed, then the radio stops to handle traffic immediately.

Impact for the users during speech

If the radio stops handling traffic as described, it does not necessarily mean a disconnected call. In a system with good overlapping coverage it might be possible to make a handover to another IPBS without disconnecting the call. If the portable device doesn't quickly find any other IPBS the call will be disconnected and the portable device will indicate `No System`. As soon as the IPBS is synchronized it is available again for portable device communication. The portable device will then connect to the system in the same way as for a normal power on.

Impact for users In idle mode

In idle mode, a user will most likely not discover any problem. Since the portable devices have a short delay before showing `No System`, the portable device has time to roam to another IPBS. A good overlap between radio cells is required to make it possible for the portable device to roam to another IPBS. If no other IPBS is available, the portable device(s) will indicate `No System`. As soon as the IPBS is synchronized, it is available again for portable device communication. The portable device will then connect to the system in the same way as for a normal power on.

Traffic

Traffic information is displayed in the Traffic sub menu. For the Master, traffic information for the IP-DECT system is displayed as well as traffic information for the Radio itself (if this Radio is enabled).

Displaying all ongoing calls in the System

All ongoing calls in the IP-DECT system can be displayed by selecting **Traffic** > **Master Calls** in the Master. See the table below for information about the different statistics fields.

Master	
Calls In	The total number of incoming calls to the Master.
Calls In Delivered	The number of connected incoming calls in the Master.
Calls Out	The number of outgoing calls from the Master.
Handover	The number of handovers in the Master.
Handover Canceled	The number of cancelled handovers in the Master. Occurs when the handset decides to stay on the original Base Station.
Abnormal Call Release	The number of abnormal call terminations. A call release can occur if for example the user leaves the system's coverage area. To analyze the events, select Diagnostics > Events. To analyze how calls are connected and disconnected, select Diagnostics > Logging and select the DECT Master check box.
Busy Hour Call Attempts	The number of calls under the busiest hour counting from when pressing the Clear button.
Busiest hour start time	The start time of the busiest hour counter which was started when pressing the Clear button.

Displaying calls

All ongoing calls on an IPBS/IPBL can be displayed by selecting **Traffic** > **Radio Calls**. See the table below for information about the different statistics fields.

Radio	
Calls In	The number of incoming calls to the Radio.
Calls Out	The number of outgoing calls from the Radio.
Handover	The number of handovers in the Radio.
Handover Canceled	The number of failed handovers in the Radio. **Note:** There can be several reasons for uncompleted handovers occurring. This will in most cases not cause dropped or disconnected calls.

Handover

During call, all ongoing handovers in the IP-DECT system can be displayed by selecting **Traffic** > **Handover** in the Master. Cordless telephones are shown by their IPEI/IDSI number.

RFP calls

RFP Concurrent call statistics gives an overview about how often simultaneous calls (1-8) on a specific radio took place.

SMS

Overview of sent and delivered SMS in the system:

Master	
Mobile originated attempts	Number of SMS sent by handsets.
Whereof delivered	Number of delivered SMS sent by handsets forwarded to the AIWS.
Mobile terminated attempts	Number of SMS received from AIWS (sent by Handset or Web interface).
Whereof delivered	Number of SMS received from AIWS and forwarded to a handset.
Busy hour attempt	Number of SMS during the busy hour of the system.

Backing up

The IPBS/IPBL configuration can be downloaded and saved on a disc or a server. This is useful when identical configuration should be applied to several IPBSs/IPBLs, for example when you configure the slaves in a system. For information on how to load a saved configuration on the IPBS/IPBL, see Updating on page 183.

1. Select **Backup** > **Config**
2. Click **download** or

   Click **download with standard password** to save the configuration with the default system password.
3. Click **Save** in the dialogue window and browse to the place where the configuration should be saved.
4. Click **Save.**

Note:

Ensure that you create a backup of the IPBS/IPBL configuration when the administrator password has been changed.

Updating

This section describes how to do the following configurations and settings.

- Update Configuration
- Update Firmware
- Update the Boot File
- Update the RFPs

Updating configuration

A previously saved configuration can be loaded and activated on the IPBS/IPBL. See Backing up on page 182 for information on how to save a configuration.

1. Select **Update** > **Config**
2. Click **Browse...** and browse to the saved configuration.
3. Click **Upload**
4. Reset in order to make the changes take effect, see Reset on page 190.

Considerations when updating of configuration

Configuration files are only fully compatible if the backup and restore are done on products that have CPUs with the same endianess. Both IPBS1 and IPBL have "big-endian" CPUs compared to IPBS2 which have "little-endian" CPU. Hence, IPBS1 and IPBL are compatible.

If a device (e.g. IPBS2) is configured and the configuration is taken from another type of device (e.g. IPBS1), some lines in the configuration will be skipped by the configured device (IPBS2). This is because devices of different types do not have the same hardware and some configuration lines are therefore not applicable in the configured device (IPBS2).

Updating firmware

The software can be updated. Follow the steps below to update IPBS/IPBL with the firmware. Download firmware from the IP-DECT system provider.

Note:

If this operation is interrupted, the firmware in the device will be defect. If a firmware upload is for any reason interrupted, the firmware must be uploaded again. Do not execute a reset before the firmware upload is complete. For information on how to load new firmware if the IPBS/IPBL is unreachable through the web GUI,see Troubleshooting IP-DECT Base Station (IPBS) on page 676.

1. Select **Update** > **Firmware**.
2. Click **Browse...** and browse to the firmware file.
3. Click **Upload**
4. Reset in order to make the changes take effect, see Reset on page 190.

Updating the Boot file

1. Select **Update** > **Boot**.
2. Click **Browse...** and browse to the boot file.
3. Click **Upload.**
4. Reset in order to make the changes take effect, see Reset on page 190.

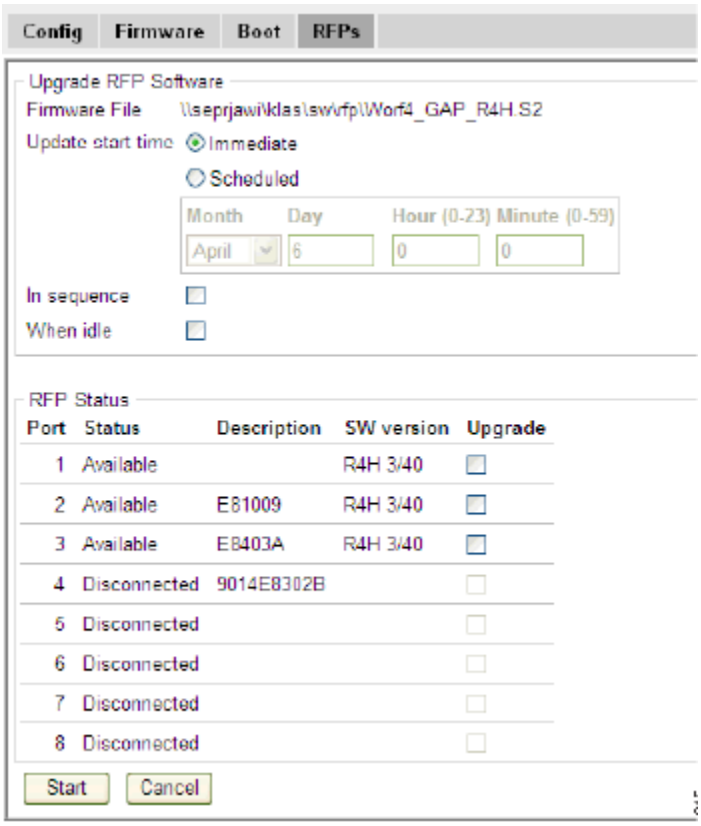
Updating the RFPs

This section applies only to the IPBL.

The firmware can be updated. Follow the steps below to update RFP. Download firmware from the IP-DECT system provider. In the RFP status list, information on connected RFPs is displayed.

1. Select **Update** > **RFPs**.
2. Click **Browse..** and browse to the RFP update file.
3. Click **Upload**.

Figure 52: Upgrading the RFPs



4. Select **Immediate** or **Scheduled** update.
5. Select the **In sequence** check box to update the selected RFPs one by one.
6. Select the **When idle** check box to start the update when the RFP is idle.
7. Mark the applicable RFPs to be updated.
8. Click **Start** to upgrade the selected RFPs.
9. The RFP restarts after the upload is finished.

Diagnostics

Logging

The IPBS/IPBL can generate a number of logs which can be useful when supervising and troubleshooting the IP-DECT system. For information on how to collect the log files, see Configuring logging on page 129. For a description of each log, see the table below.

Setting	Description
TCP	Logs generated upon TCP connection set-ups in the H.225 / H.245 protocol.
Gateway Calls	Logs generated by calls that go through the gateway interface.
Gateway Routing	Logs generated by calls that are routed through the gateway interface.
H.323 Registrations	Logs generated upon RAS registration.
DECT Master	Logs generated by the Master software component in the IPBS/ IPBL.
DECT Radio	Logs generated by the Radio software component in the IPBS/IPBL.
DECT Stack	A low level DECT log, intended for support departments.
Config Changes	Logs generated upon configuration changes in the IPBS/IPBL or the IP-DECT system.

1. Select **Diagnostics** > **Logging**.
2. Select which logs to generate by marking the check box next to the log name.
3. Click **OK**.
4. View the logs by clicking the **syslog** link. The logs are updated in real-time.

Tracing

The information gathered from the trace functionality is mainly used for troubleshooting in case of failure in the system. The trace information is intended for the support departments.

It is possible to trace traffic information on the LAN for troubleshooting purposes.

1. Select the **Enable** check box in the **Remote PCAP** section to enable the use of a network protocol analyzer program, for example Wireshark.
   The **Trace** check box in the **Remote PCAP** section is mainly used by the R&D department to follow the desired network attributes.

2. Select the **TCP/UDP Traffic** check box in the **IP** section to capture traffic information.
3. Click **OK**.

Alarms

All active alarms are displayed here. An alarm is a fault that affects the normal service of the IP-DECT system and may require action from personnel to correct it. An IP-DECT Master can collect alarms from Radios and it can display all active alarms in the system. If an object is removed from the system, object-related alarms are automatically cleared after a timeout period of 30 minutes. Active alarms are also cleared if the related object is restarted.

For a description of the attributes, see the table below.

Attribute	Description
Time	The date and time when the alarm is issued.
Code	A unique number that identifies the alarm. Click the code to get more detailed information about the alarm. For a list of possible codes and their descriptions, see Fault Code Descriptions on page 676.
Severity	It has three possible states: • Critical - Immediate action is required. It is displayed, for example, if a managed object goes out of service. • Major - Urgent action is required. It is displayed, for example, if the capability of the managed object is severely degraded. • Indeterminate - Level of severity cannot be determined
Remote	The IP Address of the object that reported the alarm. Click the IP address to access the object.
Source	The software module that reported the alarm. Together with the code it uniquely identifies an alarm.
Description	A textual description of the alarm.

Events

A history of alarms and errors is displayed here including active alarms. Click **Clear** in the top-right corner to clear the list of alarms and errors.

For a description of the attributes, see the table below.

Attribute	Description
Time	The date and time when the alarm, error is issued or cleared.
Type	The status of the fault. It has four possible states: • Alarm - Alarms displayed in red are active alarms • Alarm cleared - The alarm is already cleared • Alarm timeout - The alarm exceeded the timeout period • Error - Refers to faults that are not active for a specific time.
Code	A unique number that identifies the alarm. Click the code to get more detailed information about the alarm.
Severity	It has three possible states: • Critical - Immediate action is required. It is displayed, for example, if a managed object goes out of service. • Major - Urgent action is required. It is displayed, for example, if the capability of the managed object is severely degraded. • Indeterminate - Level of severity cannot be determined
Remote	The IP Address of the object that reported the alarm. Click the IP address to access the object.
Source	The software module that reported the alarm. Together with the code it uniquely identifies an alarm.
Description	A textual description of the alarm.

Performance

It is possible to check different performance parameters. For a description of the parameters, see the table below.

Parameter	Description
CPU	Shows CPU utilization
CPU-R	Shows utilization of CPU resources allocated by different tasks

MEM	Shows memory utilization
Concurrent calls	Shows the number of ongoing calls
Temperature (applicable only for IPBL)	Shows the temperature of the cabinet.
Voltage (applicable only for IPBL)	Shows the power supply voltage level
Current (applicable only for IPBL)	Shows the power supply current consumption

1. Select **Diagnostics** > **Performance**
2. Select the check box(s) for the desired performance statistics.
3. Click **OK**.

One window shows statistics for the last 24 hours. The maximum possible value is displayed in the top-left corner. Click the left or right arrow buttons to see different time frames.

Config Show

Under Diagnostics > Config Show, the configuration is displayed as a text output.

Ping

The ping function is used to determine the response time from the IPBS/IPBL to a certain IP address. It can be used to analyze the connection between the IP-DECT system components.

1. Select **Diagnostics** > **Ping**.
2. Enter an IP address in the **IP Address** text field.
3. Press **Enter** on the keyboard.

Traceroute

The traceroute function displays how packets travel from the IPBS to a certain IP address. The result is an ordered list of IP addresses with the measured round trip time.

1. Select **Diagnostics** > **Traceroute**.
2. Enter an IP address in the **IP Address** text field.
3. Press **Enter** on the keyboard.

RFP Scan

This section only applies to the IPBS.

To scan for occupied system IDs of other Avaya IP-DECT systems within the coverage area, perform an RFP scan following the steps below.

Note:
Executing an RFP scan will terminate all calls on the IPBS/IPBL.

1. Select **Diagnostics** > **RFP Scan**
2. Click **Start Scanning**

Service Report

To download a service report do the following:

1. Select **Diagnostics** > **Service Report**.
2. Click **download**.
3. Click **Save** and browse where to save the service report.

Environment

This section only applies to the IPBL. The **Environment** tab gives information power supply and consumption. It also displays the temperature and the fan status.

1. Select Diagnostics > Environment.

The following information is available in the Power section:

- Power supply - AC or DC power port.
- Voltage - input voltage.
- Current consumption - total consumption for the IPBL an the connected RFPs.
  - Max 4,0 A when supplied with AC power port
  - Max 5,2 A when supplied with DC power port

The following information is available under the Environment tab:

- •Temperature - °C
- •Fan status - OK, not OK

Reset

Some configuration changes requires a reset in order to take effect. A reset reboots the software. There are two ways to perform a reset:

- Idle reset - waits until there are no active calls in the IPBS/IPBL.
- Immediate reset - clears all calls and resets the IPBS/IPBL.

Idle Reset

1. Select **Reset** > **Idle Reset**.
2. Click **OK**.
3. The IPBS will reset when there are no active calls.

Immediate reset

1. Select **Reset** > **Reset**.
2. Click **OK**.
3. The IPBS will terminate all active calls and reset.

TFTP mode

Note:

When the IPBS/IPBL is in TFTP mode it can only be reached using the gwload utility. This mode should not be used during normal operation.

Boot

When the IPBS/IPBL is in Boot mode, it uses a small version of the firmware (minifirmware) which contains only the IP stack and the web interface.

1. Select **Reset** > **Boot**.
2. Click **OK**.

Reset using the reset button

It is possible to perform a hardware reset of the IPBS and the IPBL by pressing the reset button. The button is accessed through a hole in the back of the IPBS (figure 14 on page 65).

Note:

Use a pointed object in an non conducting material to perform a reset.

Short press < 1 sec	Restart
Medium press ~ 3 sec For IPBS2: When 3 seconds have passed, the LED on IPBS2 will start flashing in blue and the reset button can be released.	Restart in TFTP mode. In TFTP mode the IPBS and IPBL can be accessed only through the gwload application. This mode is intended for support and development departments.
Long press ~ 10 sec For IPBS2: When 10 seconds have passed, the LED on IPBS2 will start flashing in blue. The reset button can then be released. When the LED (LED 1 for IPBS1) is steady amber/yellow, the factory reset process is complete.	Factory reset - all configuration parameters will be set to default values.

Quit operation

To end operating the IPBS/IPBL web interface simply close the web browser. There is no logout or change account option in the web application.

Commissioning

This section describes the visual inspection and tests that must be executed after completing the installation and initialization of the IP-DECT system. The purpose of the visual inspection and tests is to verify that all installation activities have resulted in a correctly functioning system. If it appears that a part is malfunctioning while the system is installed correctly (i.e.: no cabling faults, no configuration faults), the technician must consult the maintenance section included in this manual for fault finding.

Radio coverage verification tests

The Radio coverage verification consists of two tests:

- Base station operation test
- Coverage area test

Note:

Be sure that the battery in the cordless phones are charged before executing the tests.

Base Station operation test

The purpose of this test is to check if all base stations are operational.

1. Use the base station plan (see Planning an IP-DECT system on page 43) to localize the installed radio base stations.
2. Open the Master IPBS web interface **Device Overview** > **Radios** to get a list of all base station radios connected to the IP-DECT system. The RFPI of each radio base station is the unique identifier.
3. On a DECT phone enter the Admin menu (see Admin menu tree on page 242). go to **Dect Info** > **Link**. In the first line you can find the signal strength SS -xx dBm of the connected base station. The PARI is a unique identifier of the connected base station.
4. Move close to each base station. Verify lower LED is steady green and upper LED is either steady green or off.
5. Check if the DECT phone is connected to it. The PARI in the link display needs to match with the RFPI of the device overview radio list.

After having checked that all base stations are operational proceed with the coverage area test.

Coverage area test

The purpose of this test is to verify that there is satisfactory field strength to enable good speech quality everywhere within the covered area (rooms, lift shafts, staircases). This test is executed with two cordless phones and requires two persons.

1. Open the administrator menu in the DECT telephone. (see Admin menu tree on page 242)
2. Go back to idle and make a call to the 2nd telephone.
3. Select softkey **More** > **DECT Info** > **Link**. In the first line you can find the signal strength SS -xx dBm of the connected base station. The PARI is a unique identifier of the connected base station.

4. One user of the cordless telephone should now start moving around the covered area. Both users must check that a good speech quality is maintained everywhere. Special attention should be paid to areas such as edges of the building and areas behind metal structures where there is a possibility of reduced speech quality.
5. Check signal strength should be better than -68 dBm, speech will get affected at about -75dBm.
6. Mark areas where cracking sounds or mutes are heard.

Evaluation

After having performed the coverage area test, the results should be evaluated. If the coverage is not sufficient you should review the planning and move or add equipment.

Cordless extension number test

This test checks for each cordless phone the complete connection from the IP-DECT system to the PBX. Furthermore it checks that the cordless phones' numbers have been correctly programmed. The test is performed by calling all cordless phone from one specific cordless phone.

1. Put all cordless phone together in order of extension number on a table.
2. Go off-hook with each cordless phone and check that the dial tone is heard.
3. Call with a cordless phone (cordless phone A) all other cordless phones sequentially and check that the cordless phone with the corresponding number on its display rings when called.
4. Call cordless phone A and check if it rings.

Troubleshooting

See Troubleshooting on page 675.

Using the Update Server

Summary

Automatic update is based on configuration and firmware information stored on a standard web server and retrieved by the devices on a regular basis.

There are 2 modules in the device which work in tandem. The first is known as "UP0" and actually executes the upload and download of configuration information as well as the download of updated firmware. UP0 is controlled by commands as described below.

The second module is known as "UP1". It serves to poll a given website for changed configuration information. If certain conditions are met, UP1 will issue commands to UP1 to perform the requested updates.

UP0 can also receive commands from the **Update clients** page of the PBX Administration user interface.

System requirements

One or more regular Web Server that can be accessed by all devices are required. This has been tested with Microsoft IIS and Apache, but any regular Web Server should do.

For best results, the Web Server should be able to maintain a large number of HTTP sessions simultaneously, since potentially all devices may attempt a configuration update at the same time. For example, Microsoft's Personal Web Server is not adequate, since it only supports\ 10 simultaneous sessions. The following URLs are supported:

- HTTP
- HTTPS
- TFTP

Installation

To be able to upload (save) device configuration information on the web server, it must allow HTTP PUT requests. All other functions require HTTP GET permissions only.

Since all HTTP requests are performed unauthenticated, the website used must allow anonymous read (and potentially write) access. You may want to restrict access to that site to certain network address ranges.

Configure a Microsoft IIS URL to allow PUT commands:

1. Create a directory where you want to save configurations to
2. Create a virtual directory in Microsoft's IIS manager
3. Select **read** and **write** access

No installation is needed on the IPBSs.

Configuration

See Configuring automatic Firmware update on page 127 on how to configure the IPBSs for automatic update.

The URL parameter must point to the site where the file containing the maintenance commands is stored. Note that in this URL, no host names are supported. The web servers IP address must be used.

Setting the UP1 Parameters

The applet saves the configuration in a line starting config change UP1.

The full syntax is:

config change UP1 /url *<url>* [/poll *<slow>*] [/poll-fast *<fast>*] [/disc]

If the URL ends with a '/' then a default filename is used based upon the product in question. If for example the URL is http://1.2.3.4/configs/, it is expanded to http://1.2.3.4/configs/update-IPBS.htm.

The product type name used is the one used in the Version line on the devices Info page. Note that the extension is irrelevant, .htm or .txt or no extension at all may be used. On some Web servers, URLs are case sensitive.

The maintenance command file is retrieved initially after the configured poll interval (in minutes) is expired after boot. Short poll intervals can create substantial load on a big network. A value less than 15 minutes (which is the default) is therefore not recommended.

However, for new devices (that is, devices which have been reset to factory settings and never had a successful download of a maintenance command file), the command file is retrieved every minute (for up to 30 minutes). This is done so that a fresh device can quickly retrieve a site depending standard configuration when it is installed. You can change this initial polling interval using the /poll-fast <fast> parameter (this is not recommended).

The /disc parameter can be specified to force the device to close the http sessions used immediately.

When the maintenance command file is retrieved, the commands found in the file are executed in sequence. Theoretically, all commands which can be typed in to a telnet session to the device or which appear in a config file can be used in the maintenance file. However, in most cases, you will use config change commands and commands to the UP0/UP1 modules.

The command file is executed every time it is retrieved (depending on the poll interval). However, in most cases, you don't want it to be executed each time, but only once. For example, if you are about to deploy a certain configuration change to all base stations, then you want this change to be done once per IPBS only. This can be achieved by the check command:

mod cmd UP1 check *<final-command>* *<serial>*

The devices maintain an internal variable UPDATE/CHECK which is initially (or when the device is reset to factory settings) empty. The check command will compare the <serial> parameter with the UPDATE/CHECK variable. If it is equal, any further processing of the command file is cancelled.

If it differs, the remainder of the file will be processed and, after the last command is executed, the UPDATE/CHECK variable will be set to <serial> and the <final-command> will be executed. The following commands are useful values for <final-command>:

ireset	resets the device as soon it is idle
reset	resets the device immediately
iresetn	resets the device as soon it is idle, only if a reset is required
resetn	resets the device immediately, only if a reset is required
ser	this is a no-op

Often, configuration changes shall be made only during certain times (e.g. non-working hours). This can be achieved using the times command:

mod cmd UP1 times [/allow *<hours>*] [/initial *<minutes>*]

The times command will check the current time against <hours>. If it does not match this restriction, any further processing of the command file is cancelled. <hours> is a comma separated list of hours. Only those hours listed are considered valid times for execution of the command file.

mod cmd UP1 times /allow 12,23,1,2,3,4

The command above allows command executions only between 12:00 and 12:59 and 23:00 and 4:59 local time (on a 24h clock). Note that if the device has no time set, all command executions will be cancelled.

If the /initial parameter is set, the no commands will be executed within the first <minutes> minutes after the device has been booted. This is done to avoid firmware download and flashing when installing devices.

mod cmd UP1 times /allow 12,23,1,2,3,4 /initial 6

The command above suppresses any command file processing within the first six minutes after each boot of the device. If /initial is set, new devices (or those that have been reset to factory settings), the command file will be retrieved even if it normally would be suppressed by the / allow parameter. This allows new devices to retrieve a site specific standard configuration quickly.

Setting the UP0 Parameters

To perform a firmware update, use the following command:

mod cmd UP0 prot <url> <final-command> <build-serial>

The command above downloads the new firmware from <url> and flash it to the device, then <final-command> is executed.

The IPBSs maintain an internal variable UPDATE/PROT which is initially (or when the device is reset to factory settings) empty. The prot command will compare the <build-serial> parameter with the UPDATE/PROT variable. If it is equal, no firmware will be loaded or flashed. If there is no UPDATE/PROT yet (like for a new device), <build-serial> is compared against the build number of the current firmware. After a successful download, UPDATE/PROT is set to <build-serial>. Note that <build-serial> is not checked against the firmware version actually loaded. It is your responsibility to keep this consistent.

If <url> ends with a slash ('/'), then a default firmware filename is added to the URL depending on the type of the device (e.g. ipbs.bin).

Firmware Filename

IPBS1	ipbs.bin
IPSBS2	ipbs2.bin
IPBL	ipbl.bin

mod cmd UP0 prot http://192.168.0.10/firm ireset 5.0.0

The command above determines if firmware 5.0.0 is already installed. If not, new firmware will be downloaded fromthe following locations depending on the device type:

IPBS1: http://192.168.0.10/firm/ipbs.bin,

IPBS2:http://192.168.0.10/firm/ipbs2.bin

IPBL: http://192.168.0.10/ipbl.bin

The UPDATE/PROT variable will be set to 5.0.0 and the device will be reset as soon as it is idle.

Similar to the prot command, the boot command will update the boot code.

IPBS1	boot_ipbs.bin
IPBS2	boot_ipbs2.bin
IPBL	boot_ipbl.bin

mod cmd UP0 boot http://192.168.0.10/firm ireset 5.0.0

The command above determines if the boot code 5.0.5 is already installed. If not, new boot code will be downloaded fromthe following locations:

IPBS1: http://192.168.0.10/firm/boot_ipbs.bin,

IPBS2:http://192.168.0.10/firm/boot_ipbs2.bin

IPBL: http://192.168.0.10/boot_ipbl.bin

The UPDATE/BOOT variable will be set to 5.0.5 and the device will be reset as soon as it is idle.

Using UP0, device configurations can be saved to a web server.

mod cmd UP0 scfg <url>

This command will cause the device to upload its current config to url This will be done using an HTTP PUT command. url must be writable thus. With url, some meta character strings are replaced as follows:

Sequence	Replacement	Example
#d	Current date and time	20040319-162544
#m	Primary device mac address	00-90-33-03-0d-f0
#h	Device hardware ID	ipbs-03-0d-f0

Setting the RFP_UPDATE0 parameter

To perform a RFP firmware update, use the following commands.

mod cmd RFP_UPDATE0 firmware http://192.168.0.10/Worf4_GAP_R4H.s2

The command above specifies the url to the RFP firmware to use.

mod cmd RFP_UPDATE0 select 0x2753

Specifies which RFPs to update using a hex-encoded bit-mask. Each bit represents an RFP port starting with port 1 at the LSB (0x0001) up to port 16 (0x8000).

0x2753 specifies RFP "1,2,5,7,9,10,11,14" to be updated.

mod cmd RFP_UPDATE0 schedule DD.MM.YYYY-HH:MM

Specifies when the update shall start. If no date is provided, the update will be immediate when the start command is issued.

mod cmd RFP_UPDATE0 start /idle

Starts the update or activates the schedule. Normally the /idle command is selected and an update starts only if the RFP is idle.

If multiple RFPs are selected for update, they will be updated one at a time If /sequence command is used.

Example IPBS/IPBS2/IPBL

This example shows an "update file" for the IPBS, IPBS2, and the IPBL.

mod cmd UP0 prot http://172.20.8.128/Avaya/firmware/ ireset 5.0.0

mod cmd UP0 boot http://172.20.8.128/Avaya/boot/ ireset 5.0.0

Example Update RFP firmware

This example shows an update file for the IPBL.

mod cmd UP1 check ser 20070316 - 1

mod cmd RFP_UPDATE0 firmware http://172.20.8.125/avaya/rfp/Worf132.s2

mod cmd RFP_UPDATE0 select 0xxffff idle

mod cmd RFP_UPDATED start /idle

Configuration file backup

To make a backup of the configuration file, use the following command:

mod cmd UP0 scfg <url> [<final-command> <save-serial> [/force <hours>]]

The scfg command uploads the current configuration file to the specified <url>.

Example:

mod cmd UP0 scfg http://192.168.0.10/configs/saved/#h#b5.txt no-op WEEKLY /force 168

The command above saves the device configuration file once a week with a backlog of 5 weeks.

To load a configuration file on the IP-DECT device use the following command:

mod cmd UP0 cfg <url> <final-command> <serial>

The command loads the configuration file, and all commands in it are executed.

Updating script for configuration of Kerberos clients

The update script is as follows:

```
mod cmd UP1 check resetn serial002

config add NTP0 /addr 192.168.42.136

vars create CMD0/KCMD p
<join+realm="negrealm1"+user="neguser1"+password="negpwd1"+
force="true"+disable-local="true"><server+realm="negrealm1"+
address="192.168.42.34"/><server+realm="negrealm2"+address=
"192.168.42.99"/></join>
```

Description of the update script:

Command line 1:

```
mod cmd UP1 check resetn serial002
```

By inserting this into the update script file the update server will check the variable “check” and if the value (serial002) is different from the value in the update server this script will be executed and the box will be rebooted afterwards.

Command line 2:

```
config add NTP0 /addr 192.168.42.136
```

By inserting this into the update script the local Time server is configured with ip address to valid time server and active time can be retrieved. Correct time is very important in Kerberos for joining of realm and for login purpose.

Command line 3:

```
vars create CMD0/KCMD p ....
```

The format of this line is very important. It is very important to only modify the data surrounded with double quote (“”). This script describes the mandatory data, the other data is set to default values. All parameters set by the Add-tab (see section 1) is possible to set with this script.

The XML format is as follows:

```
<join realm="..." host="..." user="..." password="..."
disable-local="..." force="..."><server realm="..." address="..."
port="..." secondary-address="..." secondary-port="..."/></join realm>
```

`realm`: The realm to join
`host`: The host name for the box (optional, otherwise the hardware id will be used)
`user`: Admin user name from the Kerberos server
`password`: Admin password from the Kerberos server
`disable-local`: the config flag will be set accordingly (true or false, optional, defaulting to false)
`force`: tells if an existing realm membership shall be discarded (true or false, optional, defaulting to false)
`server`: multiple servers may be given

In the above example, two servers are configured: one for the Kerberos server and one if using an Active Directory. The secondary address and the secondary port will be used if a Standby Kerberos server is configured.

Configuring Avaya DECT phones

Introduction

This chapter is intended as a guide when installing, configuring and maintaining functionality of the Avaya 3720, 3725, 3740, 3745, and 3749 DECT telephones.

The 372x/374x can be used straight away in your system but it is highly recommended to install the Portable Device Manager (PDM) or the Avaya In-Building Wireless Server (AIWS/AIWS2). This enables customization of the behavior of the telephone to suite each user profile and the specific PBX used in the system.

The PDM is aimed for smaller sites where the telephones are within reach. The AIWS makes it possible to administrate the telephones centrally via a web interface without the need to collect the telephones.

Ensure that you have a basic knowledge of the Avaya system and of subscribing telephones to the PBX.

Getting started

You configure the 3725/3720 and 3740/3745/3749 telephone by inserting it into a Advanced Charger, Rackmount Charger or directly over the air (OTA). The charger is connected via USB or ethernet to Portable Device Manager (PDM) or Avaya In-Building Wireless Server (AIWS/AIWS2).

In the case of IP-DECT, it is possible to configure over the air.

Note:

Ensure that you place the handset in idle state in the advanced charger, otherwise you might get synchronization issues between handset and device manager.

Note:

Uploading a language file, phonebook file, or a software download is not possible for 3720 telephone while in a call.

PDM

PDM runs on a PC. The telephone is configured via PDM as follows:

- Connect a Advanced Charger or a Rackmount Charger via USB to the computer running PDM.
- Start PDM.
- Place the telephone on a charger that is connected to PDM. The telephone can either be turned off or turned on when placing it in the charger. A telephone that is turned off will start up automatically and the battery charging symbol will be displayed.

For instructions on how to use PDM, see Installing and operating the Portable Device Manager (WinPDM) on page 315.

Configuration of phones on AIWS (Avaya In-Building Wireless Server)

The AIWS2 is run on an Elise 3 server. For instructions on how to use AIWS2, see Installing and operating the AIWS and the AIWS2 on page 359.

Using charger

- Connect a Advanced Charger or a Rackmount Charger via the Ethernet port to your network.

  The charger is by default configured to connect to the network using DHCP. If DHCP is not used in the network, connect each charger via USB to a PDM and configure a static IP address.
- Start AIWS.
- Place the telephone on a charger that is connected to AIWS2.The telephone can either be turned off or turned on when placing it in the charger. A telephone that is turned off will start up automatically and the battery charging symbol will be displayed.

Over-the-air (OTA) via IP-DECT

If OTA is configured in the IPBS the cordless telephones can be administered by the Device Manager without connecting to a charger.

There is no external equipment needed besides AIWS and IP-DECT. Please proceed with Installation of telephones on page 205.

Installation of telephones

This section describes the recommended procedure for installing and configuring telephones. There are several ways to install a telephone but the procedures described here guarantees simple maintenance of the system.

If possible, use the AIWS to install and maintain telephones in a large system. The reason is that it enables to install, upgrade and configure a large amount of telephones simultaneously. Another benefit is that the collection of the telephones from the user is not needed. They can be maintained while placed in network connected Advanced Chargers on the users desks. Network connected Rackmount Chargers can also be used, or over the air in the case of IP-DECT.

The PDM enables administration of telephones inserted in a Advanced Charger or a Rackmount Charger connected via USB to the administrator's computer.

For AIWS, see Installing and operating the AIWS and the AIWS2 on page 359. For PDM, see Installing and operating the Portable Device Manager (WinPDM) on page 315.

Preparing PDM/AIWS for handling of 372x/374x

If the parameter definition file (.def file) for the telephone is not present in the PDM or AIWS, it can be added by following the procedure below. The parameter definition file and software files are delivered as a package file with the extension '.pkg'. Note that template files (.tpl) may also be included in a package file.

1. Open PDM or AIWS.
2. In the **File** menu, select **Import** > **Packages**.
3. Select the package and click **OK**.

The package will imported and the files will be created; one definition file with the extension .def and one software file with the extension .bin. Template files may also be created.

File extensions are further explained in an appendix in Installation and Operation Manual, PDM, see File Management on page 347, and Installation and Operation Manual, AIWS, see File types on page 521.

Installation of a new telephone

The installation basically contains three steps:

- Subscription towards the DECT-system – needed to be able to make calls and send messages (Mandatory).

- Create an identity for the telephone in the PDM/AIWS – needed to be able to configure the behavior of the telephone and take backups of the telephone configuration (Recommended).
- Configure the telephone using PDM/AIWS – customize the behavior of the telephone to suite each user profile and the specific PBX used in the system (Recommended).

Note:

If no system name is assigned while subscribing a handset on the DECT R4 IPBS master, the system name as set in the IPBS master System Name will be used.

The installation is described in two different scenarios, see below. Before starting, check which scenario that suits best.

Scenario 1

Note:

This scenario is valid for Avaya IP-DECT and Integral Enterprise Systems. If subscribing towards Integral 5 or other systems, follow Scenario 2.

Note:

The telephone to be installed must not have any previous valid registrations. If it has a valid registration, unsubscribe the telephone or use Scenario 2. The user ID of the telephone is reset when you remove the last subscription.

Subscribing and creating an identity

1. Subscribe the telephone towards the DECT system. The subscription procedure is described in User Manual, Avaya 372x/374x telephone. During the subscription procedure, the PDM/AIWS identity (User ID) will automatically be assigned to be the same as the extension number.

Note:

The User ID can be viewed by navigating to the menu:
Settings > Device info > User ID or in the Admin menu:
Settings > Admin menu > Device info > User ID.
To find the Admin menu, see Admin menu tree on page 242.

Configuring the telephone

1. Insert the telephone into a Advanced Charger or Rackmount Charger connected to PDM/AIWS (not needed if an over the air connection is used). The telephone can be identified by finding the extension number of the telephone in the Number column or IPDI of the telephone in the Device ID column.
   In Telephone configuration on page 218 there are examples of configurations that can be made.
2. Configure the telephone using the PDM/AIWS, see Configuring a telephone with a template on page 208.

Scenario 2

Creating an identity

1. Insert the telephone in a desktop charger or rack charger connected to PDM/AIWS.

   Note:

   The telephone must not have a User ID. If a User ID exists, it can be removed by performing a factory reset, see Performing a Factory reset on page 210. In addition, a valid parameter definition file for the telephone has been imported to the PDM/AIWS.

2. The Found Device wizard opens. Select **Do nothing**.
3. In PDM/AIWS, navigate to the **Devices** tab and locate the telephone in the list of devices. The telephone is identified by finding the IPDI of the telephone in the Device ID column.
4. Select the telephone, make a right-click, click **Assign number...** and preferably enter the extension number for the telephone.
   The number that is assigned must not be present under the **Numbers** tab. If this is the case, it is recommended to delete the number before **Assign number...** is performed.
   After a few seconds, the Found new number wizard opens. You can save the device in the database or select **Do nothing**.

   Note:

   It is possible to enter any number or name. For IP-DECT systems, it is recommended to use the extension number of the phone.This number will now be the User ID of the telephone. The User ID can be viewed in the telephone by navigating to the menu:
   Settings > Device info > User ID.

Configuring the telephone

In Telephone configuration on page 218 there are examples of configurations that can be made.

1. Configure the telephone using the PDM/AIWS, see Configuring a telephone with a template on page 208.

Subscribing the telephone

1. 1 Subscribe the telephone towards the DECT system.
   The subscription procedure is described in User Manual, Avaya 372x/374x telephone.
   In order to easily identify the telephone, both the IPDI and the User ID are shown in the telephone when initiating the subscription procedure.

Configuring a telephone with a template

Note:

Sample templates are included in the provisioning packages for the handset software available on the Avaya support pages.

It is possible to select a telephone in PDM and directly change one or more configuration parameters. It is recommended to use a template to apply configuration changes to telephones. A template contains one or more parameter settings. By using a template, the same configuration can easily be applied to many telephones simultaneously. Templates are an efficient way to give good control over which changes that are applied to each telephone.

This enables configuration of all aspects of a telephone from sound volume to keypad shortcuts.

Your supplier can provide example templates for different PBX's. The telephone will have full functionality towards the PBX even without such a template. By using such a template, though, the telephone will be customized for that PBX with menu options for PBX specific functions such as Callback.

Creating a template

To create a parameter template see chapter PDM Create a Parameter Template on page 344, or chapter AIWS Creating a parameter template on page 405.

Applying a template

To apply a parameter template see AIWS Running a template to set parameter values on page 413.

Saving a telephone configuration as a template

You can save all settings of a telephone as template. Note that this does not include contacts and other personal data. The template will only contain configuration data.

This template can be used as a backup if your want to restore the configuration of the telephone at a later stage or as a template that can be applied to a number of telephones.

Some parameters are user specific. If you decide to apply this type of template to several telephones, the following parameters may be excluded:

- Owner ID - A text string specified in the standby mode. The parameter is located directly under **Settings > User ID**.
- Phone lock PIN code - The security code used to unlock the keypad. The parameter is located under **Settings > Locks**.

To save a telephone configuration as a template see chapter PDM Create a Parameter Template from a Number on page 345, or chapter AIWS Creating a parameter template from a number on page 406.

Synchronizing a telephone with PDM/AIWS

After installing and saving a telephone, it will be synchronized each time it is connected to the PDM/AIWS. The synchronization transfers parameter changes between the telephone and the PDM/AIWS and vice versa as follows:

- If a parameter has been changed in the telephone, it will be transferred to PDM/AIWS.
- If a parameter has been changed in PDM/AIWS while the telephone was disconnected, it will be transferred to the telephone.
- If the same parameter has been changed in both PDM/AIWS and the telephone, the value in PDM/AIWS will be transferred to the telephone.

Maintenance

Definitions

In the replacement descriptions, the telephones are defined as:

- "old telephone" is the telephone to be replaced, possibly damaged but still working
- "new telephone" is the replacement telephone that will get the settings used in the old telephone

Upgrading telephone software

It is possible to upgrade or reinstall the software on a telephone. When upgrading the software of the telephone, any data (for example, messages) may be deleted.

For upgrading a telephone see chapter PDM Delete Imported Files for Devices on page 351, or chapter AIWS Upgrading a device with new software on page 433.

Performing a Factory reset

When you perform a Factory reset on a telephone, all configuration settings will be restored to default values, PBX subscriptions will be removed and all data are removed. This includes contacts, messages etc. The software will be left intact.

Factory reset is activated from the Admin menu. See Administration on page 242 to see how to activate the Admin menu, and Admin menu tree on page 242 to see where in the menu to find "Factory reset". It can also be activated from PDM.

After a Factory Reset, you should follow the steps under Installation of a new telephone on page 205.

Replacement procedure choice guide

Depending on situation, two different replacement procedures can be chosen; replacement via PDM/AIWS and Easy Replacement. Use the following list as a guide to choose which procedure to use.

- If a telephone needs to be replaced due to for example a broken display, see Easy Replacement on page 211.

- If the electrical connection is damaged, it might not be possible to follow the Easy Replacement procedure. Depending on fault, it might work to do a replacement via PDM/AIWS, see Replacement of a telephone with the AIWS/AIWS2 on page 213 or Replacement of the telephone with the PDM on page 215.
- If two telephones and their settings shall be switched between two users, follow Replacement of a telephone with the AIWS/AIWS2 on page 213 or Replacement of the telephone with the PDM on page 215.

Easy Replacement

The easy replacement procedure is done via the telephone display and does not involve a PDM/AIWS. Instead a Advanced Charger or a Rackmount Charger is used.

The following settings are replaced during easy replacement:

- DECT registration
- User parameters (including User ID)
- Contacts

The following settings are *not* replaced:

- Call list
- Messages
- Bluetooth pairing list

Note:

Both the old telephone and the new telephone must be of the same model. The same extension number is assigned to the new telephone.

Note:

If you are using the Rack Charger, the *same charging slot* has to be used for both telephones. Currently, only the left charging slot is activated for easy replacement.

Easy Replacement procedure

During the Easy Replacement procedure, the LEDs of the telephone and the charger follow the same LED indications. This means that if the old telephone has a broken display, the LED indications on the charger and on the telephone can be used to follow the replacement procedure. Before and after easy replacement, the LEDs may have different LED indications. For more details, see also LED indications on page 245.

Note:

It is recommended to make sure that the telephone batteries are charged before starting the easy replacement procedure.

Important:
Never remove a telephone from the charger until the instructions in the display or the LED tells you to do so (see status on the LED if the display is broken). If there is an error indication it may be allowed to remove the phone, see troubleshooting Avaya 3720/3725 and 3740/3749 DECT Telephones on page 681 for further instructions.

Important:
After the old telephone has been in the charger, the new telephone needs to be placed in the charger regardless if the replacement was successful or not. Failing to do so may result in malfunction and the new telephone will need to be sent for service.

1. Start the procedure with the **new** telephone. The telephone shall be switched off. Press and hold the Off-hook key and in the mean time put the new telephone in the charger. **In charger** is displayed.

   Hold the key for at least 3 seconds until **Start phone replacement?** is displayed. The telephone LED changes to flashing orange. Press **Yes**.

2. Press **OK** when the text **Follow the instructions. Each step can take several minutes.** appears in the display.

3. When the telephone is ready, the text **Please insert old phone in charger** appears. The charger LED changes to quick orange flashing.

   Remove the new telephone from the charger. The text **Please insert this phone in charger when old phone is ready.** appears.

4. Put the **old** telephone in the charger (the telephone can either be switched on or off). After a few seconds, the text **Saving settings. Do not remove phone from charger** appears. The charger LED changes to slow orange flashing.

Important:
Do not remove the telephone while the text **Saving settings** is displayed. It may take several minutes.

Important:
If the old telephone can not communicate with the charger due to any destroyed, the LED will not change to slow orange. It will remain at quick orange flashing. As the easy handset replacement is already started with the new phone (steps 1 – 3) it needs to be continued by placing a working phone into the charger. Otherwise the new phone will not come back to operation and will need service, too. Any other phone of the same type (for example, from a customer installation) can be used to continue step 4. At the end of the replacement procedure the configuration of the “old” and new phone will be exchanged. Starting the easy handset replacement again with the same both phones gives the option to exchange the configuration again. So finally both phones will have the same configuration as they had before.

5. Remove the old telephone from the charger when the text **Please insert new phone in charger.** appears in the display and the charger LED changes to quick orange flashing. (The old telephone is reset to factory settings and automatically restarted.)
6. Put the **new** telephone in the charger. The text **Restoring settings** appears in the display. The charger LED changes to orange slow flashing.

Important:
Do not remove the telephone while the text **Restoring settings** is displayed. It may take several minutes.

7. Remove the new telephone from the charger when the text **Phone successfully replaced. Please remove phone to restart.** appears in the display. The LED changes to orange quick flashing. The new telephone is automatically restarted.

Error cases

If there is a battery failure (low battery) for the *old* telephone during Easy Replacement and the charger flashes orange, the procedure can be continued. Charge the battery and put the telephone back into the charger. The easy replacement procedure should be continued. If the LED is red, the procedure cannot be continued.

Replacement of a telephone with the AIWS/AIWS2

Both the old telephone and the new telephone must be of the same device type. The same extension number is assigned to the new telephone.

Make sure that the old telephone is saved in the AIWS. Start the Device Manager in the AIWS and navigate to the **Numbers** tab. There shall be a tick in the **Saved** column for the old telephone.

If the telephone is not saved, insert it into a Advanced Charger or Rackmount Charger connected to AIWS and perform a save, see Installing and operating the AIWS and the AIWS2 on page 359.

If it would be impossible to save the old telephone settings, stop this replacement procedure. Instead unsubscribe the old telephone from the PBX, register the new telephone and follow the instructions for installing a telephone, see Installation of a new telephone on page 205.

When the telephone is saved, unsubscribe the old telephone from the PBX.

The following steps are described in two different scenarios, check which one suits the best before proceeding.

Data included in a replacement transfer

The following data is replaced during a replacement with AIWS/AIWS2:

- User parameters (including User ID)
- Contacts (entered by the user)

Note that the following data is *not* replaced:

- DECT registration
- Call list
- Messages (3725 only)
- Bluetooth pairing list (3725 only)
- Company phonebook
- Downloaded Language

Telephone replacement with AIWS/AIWS2, Scenario 1

Note:

This scenario is valid for Avaya IP-DECT and Integral Enterprise Systems. If subscribing towards other systems, follow Scenario 2. If the handset is used on Integral 5, make sure an AIWS/AIWS2 identity (User ID) has already been assigned. If not, follow Scenario 2.

Note:

The telephone to be installed must not have any previous valid registrations. If it has a valid registration, unsubscribe the telephone or use Scenario 2.The user ID of the telephone is reset when you delete the last subscription.

1. Subscribe the new telephone with the same extension number as the old telephone. During the subscription procedure, the AIWS identity (User ID) will automatically be set to be the same as the extension number.

   Note:

   The User ID can be viewed in the telephone by navigating to the menu **Admin menu > Device info > User ID**

2. Insert the telephone into a desktop charger or rack charger connected to AIWS/AIWS2 (not needed if an over the air connection is used). Navigate to the Numbers tab in AIWS/AIWS2 Device Manager.

   The new telephone now has the same User ID as the old telephone. It will automatically be synchronized and data and parameter settings from the old telephone will be transferred to the new telephone.

   The synchronization will take a while if the Contacts in the original telephone contains a large number of contacts.

Telephone replacement with AIWS/AIWS2, Scenario 2

1. Make a note of the IPDI of the new telephone. It is found by pressing ***#06#** on the telephone.
2. Insert the new telephone into a desktop charger or rack charger connected to the AIWS/AIWS2 and navigate to the **Numbers** tab in the Device Manager in AIWS/AIWS2.
3. Select the old telephone in the list and make a right-click. Click **Associate with device...**. Select the device with an IPDI that matches your new telephone from the list that appears.

   The new telephone is automatically synchronized and all data and parameter settings will be transferred to the new telephone.

   The synchronization will take a while if the Contacts in the original telephone contains a large number of contacts.
4. Subscribe the new telephone.

Replacement of the telephone with the PDM

To see *which* data that is replaced during this process, see Data included in a replacement transfer on page 214.

Both the old telephone and the new telephone must be of the same device type. The same extension number will be assigned to the new telephone.

The new telephone should not be subscribed towards the PBX yet.

1. Perform a factory reset, see Performing a Factory reset on page 210, if the new telephone has been previously used.
2. Make sure that the old telephone is saved in the PDM by starting PDM and navigating to the **Numbers** tab. There shall be a tick in the **Saved** column for the old telephone.

   If the telephone is not saved, insert it into an Advanced Charger or Rackmount Charger connected to the PDM and perform a save.

Note:

If it would be impossible to save the old telephone settings, stop this replacement procedure. Instead register the new telephone and follow the instructions for installing a telephone, see Installation of a new telephone on page 205.

The following steps are described in two different scenarios, check which one suits the best before proceeding.

Telephone replacement with PDM, Scenario 1

Note:

This scenario is valid for Avaya IP-DECT and Integral Enterprise Systems. If subscribing towards other systems, follow Scenario 2. If the handset is used on Integral 5, make sure a User ID has already been assigned. If not, follow Scenario 2.

Subscribe the new telephone with the same extension number as the old telephone. During the subscription procedure the PDM identity (User ID) will automatically be set to be the same as the extension number.

Note:

The User ID can be viewed by navigating to the menu **Admin menu > Device info > User ID**.

1. Insert the new telephone into a desktop charger or rack charger connected to the PDM.
2. A pop-up dialogue appears, asking the user to decide whether to use the Number settings in PDM or the Number settings in the device. Select **PDM**.

   The telephone will automatically be synchronized and all data and parameter settings will be transferred to the new telephone. The synchronization will take a while if the Contacts in the original telephone contains a large number of contacts.

Note:

This scenario is valid for Avaya Integral Enterprise and IP-DECT. If subscribing towards other systems, follow Scenario 2.

Note:

The telephone to be installed must not have any previous valid registrations. Unsubscribe telephone or use Scenario 2.

Telephone replacement with PDM, Scenario 2

1. Insert the new telephone into an Advanced Charger or Rackmount Charger connected to the PDM.
2. A pop-up will be displayed. Select the option **Associate with number**. Follow the instructions and select the number of the old telephone, see Associate a Number with a Device on page 338.

3. The telephone will automatically be synchronized and all data and parameter settings will be transferred to the new telephone. The synchronization will take a while if the Contacts in the original telephone contains large number of contacts.
4. Subscribe the new telephone.

Telephone configuration

Note:

This chapter describes settings in parameter definition files (.def). These files are regularly updated and settings may change slightly. For example, "On" to "Enable" or a parameter can be moved to another directory.

Voice mail

In some systems it is needed to assign the telephone number of the Voice Mail service. The parameter can be set specifically for each PBX subscription on the telephone and is accessed from **Systems > *System x* > PBX Settings > Numbers**. "System x" is replaced with the subscription (System A - System H) that is configured.

When programming voice mail dial strings in PDM/Device Manager it is possible to use a wildcard character, N, to represent the phone's extension number.

For example, a PBX uses voicemail numbers that are a combination of a base voice mail number and the phone's extension number. If the base voice mail number is 2222 and the extension number is 4455, the voicemail number is 22224455. Using the N wildcard character this can be written as: 2222N.

Contacts

It is possible to create a local phonebook that is administered centrally and uploaded to the telephone from PDM/AIWS. The contacts will only include work number and can be edited in the telephone. You can also import the phonebook through WinPDM.

Creating a local phonebook file

The local phonebook file is created by the tool Local Phonebook.xls.

Uploading a local phonebook file

Important:
When uploading a local phonebook file, local phonebook entries (if any) in the telephone will be replaced by the entries in the file.

1. In PDM or the Device Manager in the AIWS, go to the **Numbers** tab and select device(s).
2. In the **Number** menu, select **Import contacts** > **From file**.

3. Find and select a file containing the contacts, and click **Open**.

   The contacts in the imported file are synchronized with the handset.

See also Import Contacts on page 340 in PDM section, and Importing contacts on page 416 in AIWS section.

Central phonebook

If the system is equipped with a messaging server with a phonebook service, the Central Phonebook on that server can accessed from the telephone. The number to be used is set to default 999999. It can be changed by editing parameters in a Number or a template.

If the system is not equipped with a Central Phonebook, this menu option can be removed from the telephone by entering an empty value for the corresponding parameter.

The parameter can be set specifically for each PBX subscription on the telephone and is accessed from **Systems > *System x* > PBX Settings > Numbers**. "System x" is replaced with the subscription (System A - System H) that you are configuring.

Allowing spaces in Central phonebook

If the Central phonebook contains first names and/or family names that include spaces, it is recommended to enable the parameter **Central Phonebook Allows Space** using WinPDM/ AIWS Device Manager. This makes it possible to search for contacts that include spaces.

1. Select ***Edit parameters*** for the handset device.
2. Select **Systems** > **System X** > **Numbers**.
3. Set **Central Phonebook Allows Space** parameter as one of the following:
   - Yes - The user can search for names that include spaces.
   - No - The user cannot search for names that include spaces.

Company phonebook

It is possible to create a phonebook that is administered centrally and uploaded to the telephone from PDM/AIWS. If this feature is used, entries from Contacts and Company Phonebook are merged. The Company Phonebook entries are locked and cannot be edited in the telephone.

Creating a company phonebook file

The company phonebook file (.cpb) is normally created from an Excel file using a script to extract the information and create the company phonebook file (.cpb). The Excel file, **`Company Phonebook.xls`** is delivered from your supplier.

The format of the rows in the phonebook file is:
<Name><tab><phone number>
followed by additional rows for each entry.

The telephone supports a maximum length of 24 characters in each field, additional characters are truncated when the phonebook file is created. The following characters are accepted in the telephone number field in the phonebook file, but are ignored when the phonebook file is created: ( ) - and " "(space).

Uploading a company phonebook file

In PDM or the Device Manager in the AIWS, go to the **devices** tab and select ***device(s)***. In the **Device** menu, select **Upload phonebook**.

Note:
Uploading a new company phonebook will delete the existing company phonebook in the phone. The local contacts will not be affected.

See also Upload a Company Phonebook on page 351, or Installing and operating the AIWS and the AIWS2 on page 359.

Deleting Company phonebook entries

You can delete Company phonebook entries in a handset by downloading an empty company phonebook file to the handset.

Call services

Call services is a configurable menu in the telephone. The purpose of the Call services menu is to provide a user friendly access to system dependent functionality such as Absence handling and Call Diversion. The settings for the Call services menu are system dependent.

The menu is described in *User Manual, Avaya 372x/374x telephone.*

Besides the default Call services functions, it is possible to define 16 extra system-specific call services by codes. The codes can be programmed with pause (P) and auto disconnection (H = Hook). Both Name and Data must be defined for the option to be displayed. Possible values:

- Digits 0-9, #,*
- H: Hook
- P: Pause
- T: DTMF tone on
- t: DTMF tone off

- U: user input, the telephone prompts for user input with the possibility to enter and edit numerical characters or even select a number from the local contacts (procedure call).

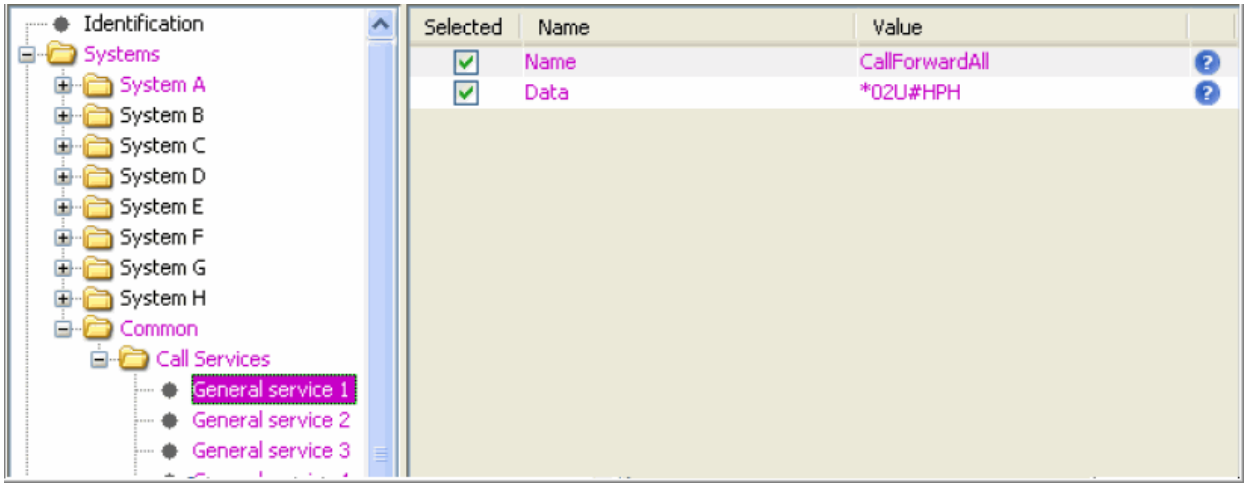
Additional codes in stimulus mode:

- A: Prog
- B: List
- C: Redial
- D: Shift
- E: Speed dial

The programming of the menu is done with PDM or AIWS. For instructions on how to edit parameters with PDM, see Edit Parameters on page 337, or with AIWS see Editing Parameters on page 412.

Using the PDM and the Edit template feature, the parameter can be found at **Systems** > **Common** > **Call Services** > **General Service X**.

Figure 53: Examples for Call services settings



Note:

Changing the language on the telephone will not affect the Call services menu entries. The text entered in PDM/AIWS will not be changed.

In Call Menu

In Call Menu is a configurable menu in the telephone. The setting for the incall menu entries are system dependent! The purpose of the In Call Menu is to provide a user friendly access to system dependent functionality during a call such as:

- Start a New Call during Conversation

- Switch between Calls
- End a Call
- Transfer a Call
- Transfer to new Call
- Make Conference Call
- Activate Call Back
- Sending Call Waiting
- Open Contacts (that is, Local phonebook and Company phonebook)
- Open Messaging menu[1]
- Send DTMF
- Viewing DECT information (visible when the Admin menu is activated)
- Turning microphone on/off (always visible, can not be disabled)

Note:

The “Transfer to a new call” option will be visible in the telephone when the parameters "Transfer call" and "New call" are set.

The menu is described in *User Manual, Avaya 372x/374x telephone*.

It is also possible to configure your own general purpose In call functions that can be used similar as the **call services** functions.

Note:

If the handset is connected to an Integral system, the preconfigured In call menu items cannot be used. Use the general purpose options of the In call functions instead.

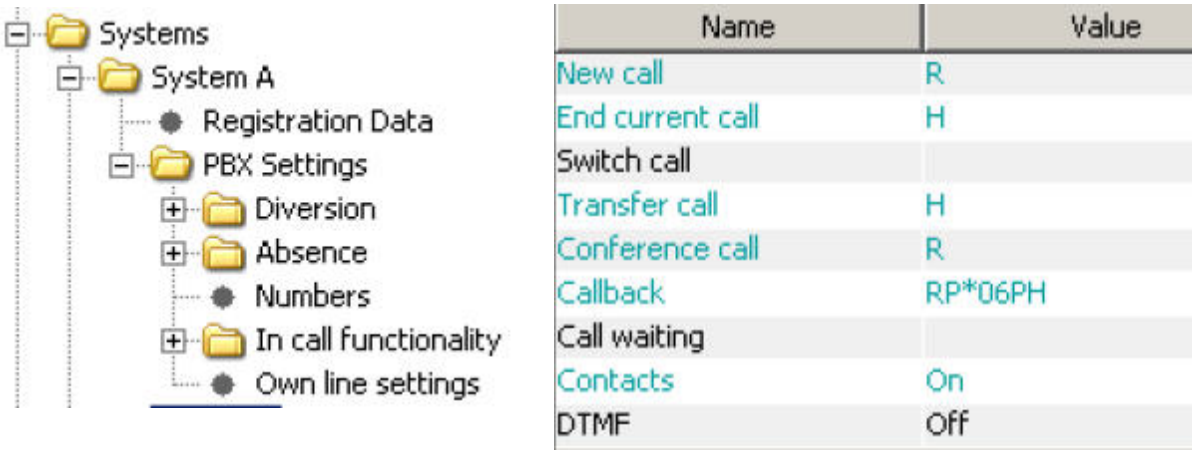
Additionally, there is an option to create a shortcut to a certain In call function (see Replacing R Soft Key on page 224).

The programming of the menu is done with PDM or AIWS. For instructions on how to edit parameter with PDM, see Edit Parameters on page 337, or with AIWS see Editing Parameters on page 412.

Ask your supplier for example templates that will configure In Call Menu for your PBX.

1. This option is always visible and cannot be disabled in handset.

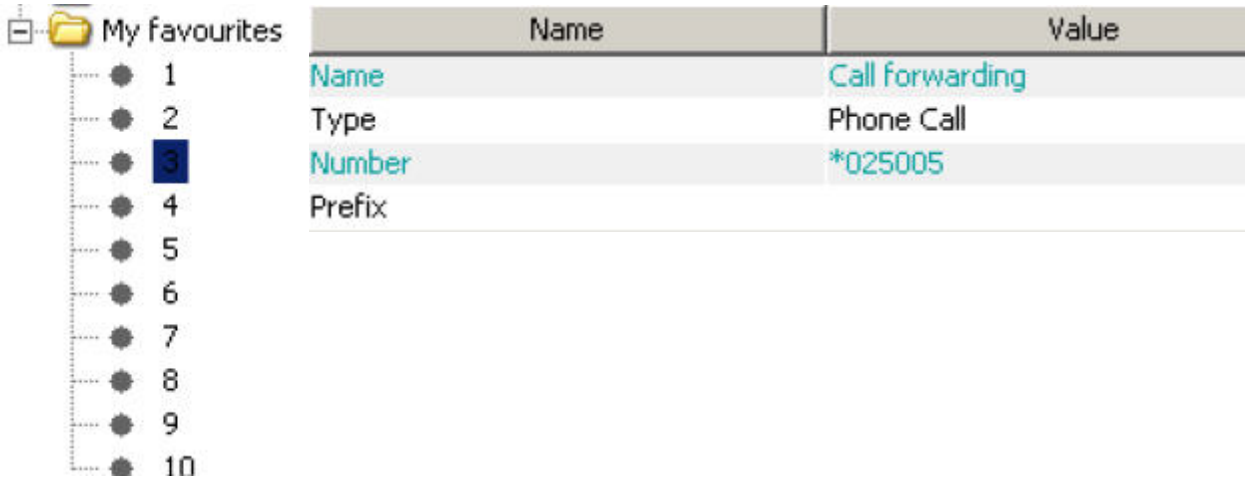
Figure 54: Examples for In Call Menu settings



My Favorites

Entries in the **My Favorites** can be used similar as the **Call Service** menu. They can be configured by the user itself. Additionally it is possible to configure a short cut to open the **My Favorites** menu or to assign a **My Favorites** entry directly to a short cut. The settings in the **My Favorites** are system dependent.

Figure 55: Examples for My Favourites



Note:

If no number is entered for the Phone Call function, the user must enter the number when the dial tone is heard (post-dial). If the character U is entered in the **Number** field, the Enter number dialogue appears in the telephone before the phones goes off hook (procedure call).

Own In Call functions

It is possible to add own In call functions as follows:

1. Select **Systems** > **System X** > **PBX Settings** > **In call functionality** > **General purpose X**.
2. In the **Name** field, enter the name of the In call function. The name will be displayed in the telephone's In call menu.
3. In the **Data** field, enter the system specific code for the command. The following values can be used: Digits 0-9, #, *, P – pause, H – hook, U – the telephone prompts for user input with the possibility to enter numerical characters or select a number from the contacts (procedure call).

Replacing R Soft Key

It is possible to replace the right Soft key as a shortcut to a certain In call function. By default, the right Soft key is configured as R-key. If needed, configure the In Call functionality to be used. See In Call Menu on page 221. This is not needed if the Loudspeaking function or R-key function shall be used on this button.

1. Select **Systems** > **System X** > **PBX Settings** > **In call functionality** > **Soft Key Right**.
2. In the **Name** field, enter a descriptive name of the Soft key. This is not needed if the Loudspeaking function or R-key function shall be used.
3. Select the newIin call function to be used:
   - Loudspeaking function
   - Start a new call during a conversation
   - End a call
   - Switch between calls
   - Transfer a call
   - Transfer to a new call
   - Make a conference call
   - Activate call back
   - Sending call waiting
   - General purpose 1 -10

Resetting R Soft Key

1. Select **Systems** > **System X** > **PBX Settings** > **In call functionality** > **Soft Key Right**.
2. In the **Function** drop-down list, select **R**.

The R Soft key will now be visible during a call.

Own line settings

Use the Own Line Settings when you want to use the same phonebook in different systems and in different countries.

The own line settings enables:

- Calling numbers stored with a "+" sign for the international access code. The same phonebook can be used in different countries.
- Recognizing incoming internal or external calls as numbers stored on international format in the phonebook. The same phonebook can be used in different systems.

In order for this feature to work, numbers must be stored in the phonebook in international format with a "+" sign for the international access code. Also, the Own Line parameters must be configured with the PDM/AIWS.

For instructions, see Installing and operating the Portable Device Manager (WinPDM) on page 315, or Installing and operating the AIWS and the AIWS2 on page 359.

Uploadable language

It is possible to upload *one additional* language to the telephone. The language file is generated via an Excel file. The Excel file used to generate language files is delivered from your supplier.

Note:
If another language file is uploaded, the first additional language is overwritten.

Certain special characters are allowed when generating the language file, see information in the Excel file.

To upload an additional language, the PDM or the Device Manager in the AIWS is used, go to the **devices** tab and select ***device(s)***. In the Device menu, select **Upload language**.

A parameter can be altered to match the uploaded language. The parameter controls:

- The characters available for text input.
- The sort order in the phonebook.

See also on the PDM, Upload a Language to Devices on page 350, or the AIWS, Installing and operating the AIWS and the AIWS2 on page 359.

Customizing the GUI

This feature is included in 3725, 3740, 3745, and 3749, but not in 3720.

It is possible to customize the telephone Graphical User Interface (GUI) by turning certain menus On or Off. This is done in the PDM/AIWS by editing a template (or a Number setting) for the corresponding portable (or Number).

The path to these settings in the template depends on the version of the parameter definition file (.def). In the current version the path is:

Customization > **Visibility** > ***X***

where "X" can be System, Settings, and so on.
The parameters are found under "X".

The settings for the parameters may have three alternatives, such as:

- Show
- Hide all
- Hide admin (All settings can be viewed but not modified by the telephone user)

Missed call indication

A missed call is by default indicated by a Missed call window. It is possible to hide this window and is recommended if a user has, for example, both a telephone and a mobile.

Example:

If configured in the PBX, an incoming call to the telephone can either be answered using the telephone or mobile. If the user answers the call using the mobile, the Missed call window will not be displayed in the telephone.

1. Select Settings > Answering.
2. In the Missed Call Indication drop-down list, select one of the following:
   - Not used - The Missed Call window appears immediately.
   - 1 to 20 seconds - The telephone will register a call as missed if it not answered within the specified time.

Configuring telephone restrictions

Enabling/Disabling System ring signals (Stimuli)

Note:
This function is applicable in Integral legacy systems only.

It is possible to force the telephone to use the system-provided ring signals instead of the local ring signals.

1. Select **Customization** > **Phone restrictions**.
2. In the **Force stimuli ringing** drop-down list, select one of the following:
   - On - The system-provided ring signals will be used.
   - Off - The local ring signals will be used.

Enabling/Disabling local phonebook lookup (Stimuli)

Note:
This function is applicable in Integral legacy systems only.

It is possible to force the telephone to display the system-provided call information instead of the information saved in the local phonebook (this is only valid when the phone is connected to an Integral system).

1. Select **Customization** > **Phone restrictions**.
2. In the **Stimuli call phonebook** lookup drop-down list, select one of the following:
   - On - The information saved in the local phonebook will be displayed.

   Note:
   Ensure that the number of the calling party is saved in the local phonebook.
   - Off - The system-provided call information will be used.

Enabling/Disabling mute function

It is possible to prevent a user from muting the telephone.

1. Select **Customization** > **Phone restrictions**.
2. In the **Possible to turn off sound** drop-down list, select one of the following:
   - Yes - The mute restriction is disabled.
   - No - The user will no be able to mute the telephone or set the ring volume to silent.

Enabling/Disabling Switch Off function

You can prevent that the handset from being switched off by a user.

1. Select Customization > Phone restrictions
2. In the Prevent switch off handset drop-down list, select one of the following:
   - Yes - The user will not be able to switch off the handset by pressing the On-hook key.
   - No - The switch off restriction is disabled.

Enabling/Disabling call list

You can disable the call list on handset to prevent an unauthorized person from viewing calls in the the call list.

1. Select Customization > Phone restrictions.
2. In the *Possible to enable call* list drop-down list, select one of the following:

- Yes - The handset will store the calls in the Call list.
- No - The handset will not store any calls in the Call list.

Note:

Old incoming and outgoing calls (if any) will not be deleted in the Call list when setting the parameter to No. It is recommended to clear all call lists (if any) to ensure that no old calls are stored.

Actions when telephone is placed in charger

In Charger action when not in call

The telephone can be configured to switch off, turn the sound off, or redirect calls when it is placed on a charger. The selected action is only performed when no call is established. When the telephone is removed from the charger, it returns to previous settings.

1. Select **Connections** > **In Charger**.
2. In the **In charger action** drop-down list, select one of the following:
   - No action - No action will be performed when telephone is placed on charger.[1]
   - Switch off - The telephone will be switched off when placed on charger.
   - Sound off - The telephone will be silenced when placed on charger (not available in Integral mode).

1. If the parameter "Possible to turn off sound" is set to "No", the device will not be muted when placed in charger.

- Redirect - The telephone will redirect all calls and messages when placed on charger. (not available in Integral mode).

  Note:The destination number must be programmed in the PBX to be able to redirect calls and messages.

- Change profile - the handset will change profile when placed in charger. In the Change to profile drop-down list, select the profile to be used. By default, only the profile Normal is selectable. If configured, additional profiles will be visible. See Profiles on page 237.
- Message absence - When an application/system sends a message to a handset, it will receive an indication that the handset is absent. If a handset is absent, the application/system determines if the message shall be sent to the handset or not, or redirected to another handset.

In Charger action when in call

The telephone can be configured to end a call or turn on the loudspeaker when it is placed on a charger during a call. If the telephone is removed from the charger during the call, it will not return to its previous settings.

1. Select **Connections** > **In Charger**.
2. In the **Call behaviour** drop-down list, select one of the following:
   - No action - No action will be performed when the telephone is placed on charger.
   - End - The telephone will disconnect calls when placed in charger.
   - Put on Loudspeaker - The telephone will activate the loudspeaker mode when placed on charger.

Clearing lists when inserted in charger

The telephone can be configured to clear lists when placed on a charger. The following lists will then be cleared:

- Inbox (for 3725, 3740, 3745, and 3749)
- Unsent (for 3725, 3740, 3745, and 3749)
- Sent (for 3725, 3740, 3745, and 3749)
- Call list
- Missed calls

Note:

Both call lists and message lists will be cleared. However, this option is not valid if the handset is in Integral mode.

Using the PDM/AIWS and the **Edit template** feature, the parameter can be found at **Connections** > **In_Charger** > **Clear_Lists_In_Charger** in a template or parameter definition file (.def).

The default setting for **Clear list in charger** is **Off**. The feature is activated by changing the parameter value to **On**. When the feature is enabled, the lists are cleared when the telephone is placed in the charger.

Disabling Homebase GAP registration

Note:

Do not activate this feature if the telephone is used in an Integral 5 system.

When the feature is enabled, it is not possible to register to a home base.

Using the **Edit template** feature in the PDM/AIWS, the parameter can be found at **Systems** > **Home_Base_Subscription**.

The parameter shall be set to **Enable** for registration of a new base station. The default value is **Disable**.

Making encrypted Base Station mandatory

The telephone can be configured to establish calls via encrypted base stations only. So the handset will prevent unencrypted calls. This setting can be used to avoid snooping in the telephony network. If the setting is active, the encryption needs to be enabled in the base station. See corresponding manual for the base station.

Using the "Edit template" feature in the PDM, the parameter can be found at **Systems** > **Encryption required**. When the parameter is set to **Yes**, it is only possible to establish calls via encrypted base stations. The default value is **No**.

Note:

In the IP-DECT R4 system, the air interface of all base stations is encrypted. For ISDN DECT, only RM627/RM637 supports encryption that needs to be enabled via the ISM/ISA tool. Do not set this parameter in installations with RM588, RM603, and RM617.

Early Encryption

Early encryption is used when DECT security is activated in the base station. This means that the radio link is encrypted early before data is transmitted.

To enable early encryption in the handset, the "Early encryption enable" parameter is set via the PDM in the following way:

1. From the PDM, select **Systems** > **System x** > **Early encryption enable**
2. From the **Value** column, select "**true**" from the pull-down menu.

Note:

Problems may be experienced with early encryption if the management and control frames passed from the handset MAC layer to the IP addressing layer are disturbed and lose their integrity. This can occur where RF propagation is disturbed, for example, if the handset is being used in an environment where highly reflected metallic surfaces are used in the construction of the locale.

If users experience connection problems when early encryption is turned on, the function may be turned off in the handset by reconfiguring the handset through the PDM and setting the value of the parameter to "**false**".

Out of range beep

The behavior of the handset when moving out of coverage area of the connected DECT system can be configured at **Settings** > **Sound and Alerts** > **Out of range alert**. The handset can either be silent when loosing the system or do a single beep or beep every minute for the next 30 minutes to alert the user that the system is out of range.

Handset idle roaming

It is recommended to set the new parameter **Location** > **Base station positioning** to **Off**. Otherwise there will be a strange roaming behavior in the handset that could cause some undefined side effects. Additionally, the battery standby time will be reduced if the parameter is set to **On**.

This parameter was introduced for the hotfix Version 2.8.30 in the 3725 Handset only to improve the idle roaming behavior in this load as a short-term fix. The handset will search every few seconds for the IPBS with the best signal strength. In later handset releases, a more optimized idle roaming behavior was introduced, which is always active (for 3720 as well) and has much less impact on the battery standby time. The parameter has to be kept in the parameter definition to be able to set it to **Off** in case of updating the handset from the hotfix release 2.8.30 to a later release where this parameter is not needed anymore.

Site survey tool

This feature is included in 3725, 3740, 3745, and 3749 phones. It is not available in the 3720 phones.

Protect registration from user deletion

You can configure the system to protect or unprotect a registration from deletion via the telephone menu by altering the parameter “Protected flag”. In a template/Number in PDM/AIWS, the parameter is found at **Systems > System X > Registration data**.

Emergency call number

This is a phone number for emergency calls. It is always possible to call this number, regardless of whether phone-lock or key-lock are active or not. The parameter is found in **Settings**.

Alarm ringing volume (Integral Systems)

The ringing volume for incoming Alarms for an Alarm server is configurable.

1. Select **Settings** > **Sound and Alerts**.
2. For the IMS call ringing volume, select:
   - Always loud - The handset will always ring with the maximum volume for an incoming alarm.
   - Ringing Volume - The handset will ring with the configured ringer volume of the handset on the I55 side.

Note:

If the handset supports the local ringing melodies in Integral mode, the ringing volume of the handset on the I55 side can be set by the following the programing sequence *Prog 5 Redial 2*. It is recommended to configure the sequence in the **Call Service** menu or in **My Favorites**.

Note:

It is not possible to set the ringer volume for the alarm to level 0 or to change to the silent mode for an incoming alarm.

Common alarm settings

Note:
This feature is applicable for Avaya 3749 telephone only.

The parameters described in this chapter are applicable for all alarm types: the Push-Button Alarm, the Man-Down Alarm, and No-Movement Alarm.

In a template or Number in PDM/AIWS, the parameters for activation are found at **Alarm** > **Common**.

Parameters in the current version are:

- Password protect ALS - Determines if a password is required to turn off the ALS.
- Number for automatic call after alarm - The number to be called after an alarm has been sent. The number can also be called without sending an alarm by pressing the push button. See Call Predefined Number without Sending Alarm on page

Push button alarm

Note:
This feature is applicable for 3749 only.

It is possible to configure how alarms shall be handled in a system. You can activate an alarm in two different ways:

- A single long press
- Multiple presses

The following alarm types are handled:

- Push-button alarm
- Test alarm

In a template or Number in PDM/AIWS, the parameters for activation are found at **Alarm** > **Alarm on long press** and **Alarm** > **Alarm on multiple press**.

Parameters in the current version are:

- **Alarm type for long press** - Test alarm, Push-button Alarm 1, Push-button Alarm 2, or Not used. If Not used is selected, it is still possible to dial a predefined number after alarm number without sending an alarm.
- **Alarm type for multiple press** - Test alarm, Push-button Alarm 1, Push-button Alarm 2, or Not used. If Not used is selected, it is still possible to dial a predefined number after alarm number without sending an alarm.
- **ALS** - Acoustic Location Signal enabled.

- **Mode for automatic call after alarm** - The call can be established in the following modes:
  - Off: No call will be established.
  - Normal: The call is established as an ordinary call.
  - Loudspeaking: The loudspeaker on the backside of the handset is turned on.

For additional parameter settings, see Common alarm settings on page 233.

Calling a predefined number without sending alarm

You can configure the Push-button to automatically dial a number after alarm number without sending an alarm. Example of configuration:

1. Select **Alarm** > **Common**.
2. In the **Number for automatic call after alarm** field, enter the number to be dialed.
3. Select **Alarm** > **Alarm on long press**.
4. In the **Alarm type for long press** drop-down list, select **Not used**.
5. In the **Mode for automatic call after alarm** drop-down list, select one of the following:
   - Normal: The call is established as an ordinary call.
   - Loudspeaking: The loudspeaker on the backside of the telephone is turned on.

This configuration makes it possible to long press the Push-button to dial the number without sending an alarm. However, the Push-button alarm can be configured to send an alarm by pressing it twice. See Alarm type for multiple press in Push button alarm on page 233.

Man-down alarm and No-Movement alarm

Note:
This feature is applicable for Avaya 3749 telephone only.

Man-down alarm	If the telephone is tilted 45º (default) or more for a preset time (default 7 seconds), the Man-down alarm[1] will be triggered.
No-movement alarm	If no movement is detected during a preset time (default 30 seconds), the No-movement alarm will be triggered.

1. The accuracy is +/- 10 %

In a template or Number in PDM/AIWS, the parameters for activation are found at **Alarm** > **Man-down and No-movement alarm**.

The alarms can also be activated in the telephone. For more information, see User Manuals for the corresponding telephones. Parameters in the current version are:

- **Man-down alarm** - Determines if the Man-down alarm shall be enabled or disabled.
- **Man-down detection time** - Determines when the warning phase will start after man-down is triggered.
- **No-movement alarm** - Determines whether the No-movement alarm shall be enabled or disabled.
- **No-movement detection time** - Determines when the warning phase will start after No-movement alarm is triggered.
- **Warning phase duration** - Determines the time before the warning phase is ended and the alarm is sent.
- ***ALS*** - Acoustic Location Signal enabled.
- **Mode for automatic call after alarm** - The call can be established in the following modes:
  - Off: No automatic call after alarm.
  - Normal: The call is established as an ordinary call.
  - Loudspeaking: The loudspeaker on the backside of the handset is turned on.

For additional parameter settings, see Common alarm settings on page 233.

Messaging settings

You can configure how incoming messages shall be indicated and displayed in telephone.

The parameters that can be found at **Settings** > **Sound and Alerts**:

- Vibrate alert - Determines if the telephone shall vibrate when receiving incoming calls and messages.
- Message alert - Determines the message sound for incoming messages.The parameters that can be found at **Settings** > **Messaging**:
- Message alert during a call- Determines the message sound for incoming messages. It is possible to select a predefined melody (Message 1 - Message 7) or a beep code that represents a certain sound.
- Text size - Size of the message text when viewing and writing messages.
- Message alert during call - Determines if a message alert should be played when receiving a message during a call.
- Message volume - Determines the message volume for incoming messages. By default, the message volume follows the ring volume, but another message volume can be set with this parameter.
- Vibrator for message during call - Determines if the handset shall vibrate when receiving messages during an ongoing call. The Vibrate alert parameter must also be enabled if the handset shall vibrate when receiving a message during the call.

Audio adjustment

You can configure the adjustment of the side tone level, i.e. how much of the speakers voice that is fed back to the speaker and the microphone sensitivity level. The parameters can be found at the following path, Audio > Normal.

- Normal side tone adjustment. The parameter affects the “normal” mode, i.e. not wired headset, not Bluetooth headset and not the handsfree/loudspeaking mode
- Normal mic adjustment - Determines the microphone sensitivity, that is, how much sound the microphone shall gain.

For configuration of headset audio see, Headset configuration on page 236.

Note:

Changing this parameter may result in lower sound quality and high sound level. Evaluate carefully before applying.

Headset configuration

A headset is recommended if you frequently use the telephone and/or want to have both hands free. The headset comes in two versions; microphone integrated in the cable, and microphone on a boom.

In order to achieve optimal audio quality with the different headset types, it is recommended to set the corresponding headset profile.

The default setting is "microphone on a boom," which means that the audio is optimized for using a headset with microphone on a boom. The headset profile can be changed in the telephone menu or in a template/Number via PDM/AIWS in:

Connections > Headset > Headset type

If the preconfigured headset profiles does not match the headset or the audio performance is bad, it is possible to configure a headset profile. In PDM/AIWS, this is done under:

Connections > Headset > Headset type > User headset profile

When a name has been configured for the profile it will be visible and selectable in the telephone menu.

The following parameters can be set:

- microphone gain
- speaker gain

Note:

Changing these parameters may result in a very high sound level which can cause hearing damage.

Note:

Changing these parameters may result in lower sound quality such as noise and echo. If audio problems occur, it is noticeable for the person listening on the conversation. Evaluate carefully before applying.

Owner identification in the idle display.

You can add owner identification in standby mode of the telephone. In a template or Number in PDM/AIWS, the parameter is found at:

Settings > Owner ID

Note:

You can configure the Owner ID using the telephone menu. See User Manuals for corresponding telephones.

Profiles

This feature is included in 3725, 3740, 3745, and 3749, but not in 3720.

You can set up an own profile for incoming calls, message alerts, vibrating alerts, key sound etc. This can be useful when there are many users on the same telephone, and they want different sound profiles. It can also be used for temporarily settings, for example while in a meeting, incoming calls should be silent.

Profiles are configured via parameters in the **Profiles** folder.

Note:

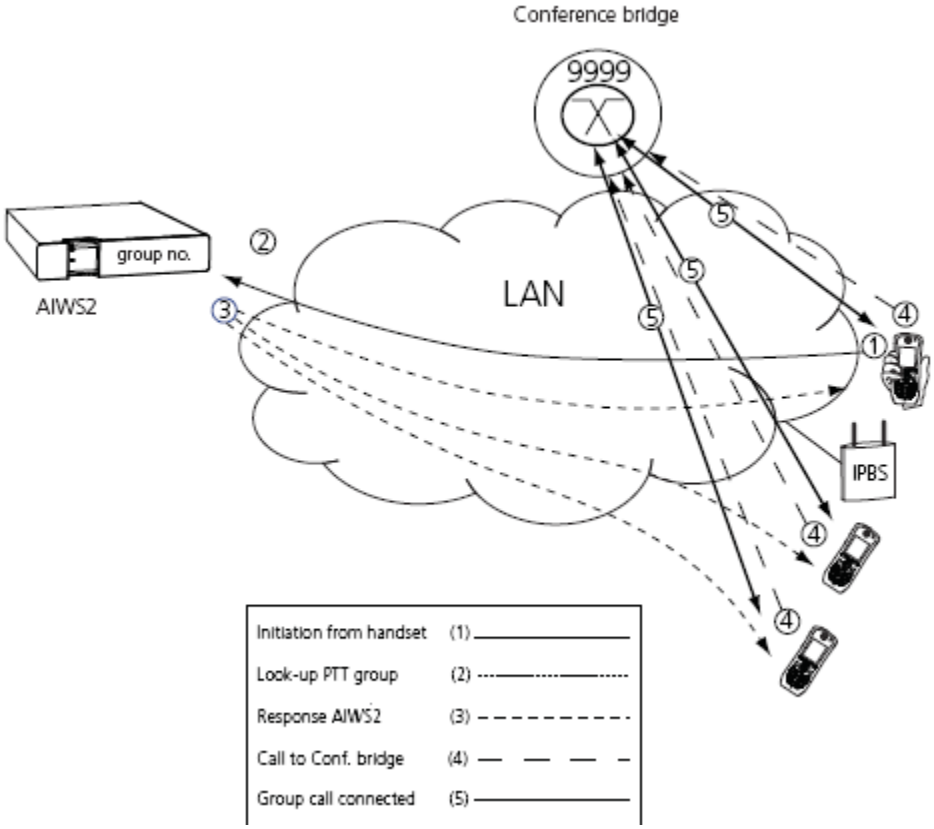
It is also possible to configure profiles using the telephone menu. See *User Manuals for Avaya 3725, 3740, 3745, and 3749 telephones*.

Push-to-Talk (PTT) group call

When the user initiates a PTT session on the handset by sending an invitation, the handset sends a message to the AIWS2 with the phone number to the conference bridge (in this example, the number is 9999). When the AIWS2 has found the PTT group, it forwards the message to all members in the group, including the initiator if the initiator is a member.

When the PTT session is accepted, either manually or automatically, the handset is connected to the number that handles the conference/group calls, and all handsets in the PTT group are connected.

Figure 56: PTT call initiation by handset



Note:

PTT sessions are by default configured to open in loudspeaking mode but can also be configured otherwise.

The message sent to the PTT group members can include the possibility to accept or decline the PTT session, or a demand that it is to be accepted automatically.The calls are made in half-duplex communication, which means that while one user is talking, the other users are listening.

Note:

You must define Messaging group(s) in the Unite module. See *Predefined Groups and Messages* on page 503.

To be able to call a PTT group, you must configure the properties for the PTT group. Using the PDM/Device Manager and the *Edit template* feature, and select **Push to Talk > PTT X** (where X represents the groups 1 to 10).

You can configure the following parameters:

- Group number – The Messaging group number that is defined in Unite module.
- Display text – This text appears in the display when the PTT group call is connected.

- Conference number – The phone number to the conference bridge (PTT server) that is provided by the system administrator.
- Answer mode – Determines if the PTT call shall be automatically or manually answered.
- Speaker mode – Determines if the PTT call shall be answered in loudspeaker mode.

For configuring PTT call using MX Exchange, see *Configuring PTT on Meeting Exchange* on page 705

Importing contacts

You can import a phonebook file (that is, local phonebook) to a telephone. The phonebook file is a tab-separated .txt file, and contains two items per row, number and name. The PDM is used to import the phonebook file to the handset.

See also Import Contacts on page 340 in the PDM section, and Importing contacts on page 416 in the AIWS section.

See also Central phonebook on page 219 and Company phonebook on page 219.

Shortcuts

This feature is included in 3725, 3740, 3745, and 3749, but not in 3720 DECT handset.

One click access to predefined functions can be configured for the Soft keys, Hot keys, Navigation keys, and the Multi-function button. For example, you can define the Soft key to make a call by selecting the Phone call function. Selecting the user sequence function provides an option to send, for example, FAC through shortcut. When configuring the function, the following values can be entered:

- Digits 0-9, #,*
- H: Hook
- P: Pause
- T: DTMF tone on
- t: DTMF tone off
- U: user input, the telephone prompts for user input with the possibility to enter and edit numerical characters or even select a number from the local contacts (procedure call).

Additional codes in stimulus mode:

- A: Prog
- B: List
- C: Redial
- D: Shift
- E: Speed dial

Shortcuts are configured via parameters in the **Shortcuts** folder.

Note:

The Multi-function button on 3749 is used as an alarm button and cannot be configured as a shortcut key.

Note:

When programming Soft keys, both name and function must be set.

Note:

You can configure shortcuts through the telephone menu. See *User Manuals for Avaya 3725, 3740, 3745, and 3749 telephones*.

Administration

Admin menu tree

The telephone has a hidden menu for system administrators. The Admin menu contains:

- Software and hardware information, IPDI and IPEI, User ID, Messaging ID1 and Device Management system
- DECT link and system information
- Centralized Management status
- Site survey tool (not included in 3720)
- Fault logging
- Enhanced system menu with ability to alter protection
- Factory reset option

To activate the Admin menu, enter **Settings > Device info > Software** and press the buttons containing **CRAFT#**, that is **27238#**.

Note:

Once the Admin menu was activated by "CRAFT" a new menu entry **Admin menu** will appear in the **Settings** menu. So you can easily enter the admin menu again without typing "CRAFT". The new menu entry can be deleted by a restart of the telephone.

Note:

Never enter **Craft#** in the **Settings >Admin menu > Device info >Software** menu to activate the admin menu again, even it is already active. The telephone can get stuck.

The following table shows the menu tree for the Admin menu in 3725, 3740, 3745, and 3749. Other menus are described in *User Manual, Avaya 3725 telephone*, *User Manual, Ayava 3720 telephone*, and *User Manual, Avaya 3740/3745/3749*.

Admin Menu

Device info	>	Software		
		Hardware		
		IPEI/IPDI		
		User ID		

Admin Menu (continued)

DECT info		Link		
		System		
		Encryption mode		
Centr. Management[1]				
Site survey tool		Link		
	>	HO & roam beep	>	On/Off
		Range beep	>	On/Off
		Error rate beep	>	On/Off
		Set range (-dbm)	>	<Value>
		Set error rate (f/s)	>	<Value>
		Show RFPs	>	All RFPs
				Selected RFPs
				All except selected
				Residential RFPs
Logging	>	No. of events		
		Restart reason		
System	>	Change system	>	Automatically
				<System>
				...
		Subscribe	>	• Next
		Unsubscribe	>	<System>
		Rename system	>	<System>
		Priority	>	<System>
		Protection	>	<System>
Frequency band (see important note)	>	Default EU US China (autodetect)		
		LA (Latin America)		

Admin Menu (continued)

		Brazil		
Factory Reset				

1. Centr. Management shows the status of the handset for the maintenance:
   DECT: over the air status
   Eth/USB: DC4/RC3 status
   Firmware download status
   Synch status

Important:

The Frequency Band selection is only available in a factory fresh handset or after a factory reset. **This setting can never be changed if it was done once. A wrong configuration will result that the handset will not operational anymore and needs to be sent back to the Avaya repair center.** The default setting is "EU US China" what will result in a auto detect mode for the different frequency bands. This setting needs only to be changed for users in Latin America and Brazil.

The currently used frequency band can be found on the **Device info** > **Hardware** page.

Quick access to the telephone information/SST menu

For quick access to device information, short codes can be used in the idle menu. To display this information, enter the following codes in the telephone.

Information	Code
Software version	*#34#
Hardware version	*#34#
IPEI	*#34# or *#06#
IPDI	*#34# or *#06#
User ID	*#34#
Open Site Survey tool menu	*#77#

LED indications

The following table shows the LED indications that are used for 3725/3720 and 3740/3745/3749.

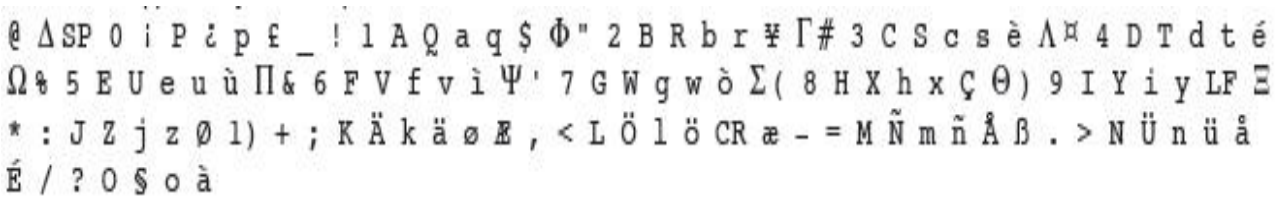
LED indication	Description
None	Switched off.
Green, fixed	Telephone fully charged and in charger.
Green, flashing	Switched on, but not in charger.
Orange, fixed	Charging.
Orange, flashing (1000 ms on, 1000 ms off)	Software download.
Orange, flashing (100 ms on, 800 ms off)	“Change phone” indication during Easy Replacement.
Red, fixed	Software error. Service needed.
Red, flashing (100 ms on, 800 ms off)	Error indication during Easy Replacement. Put back old portable in charger.
Red, flashing (800 ms on, 100 ms off)	Error during Easy Replacement. Service needed for *both* portables.

See also LED indications in Easy Replacement on page 211.

Characters for SMS

For SMS from handset to handset only the following characters will be supported by the SMS protocol:

Figure 57: SMS Characters



Troubleshooting

See Avaya 3720/3725 and 3740/3749 DECT Telephones on page 681.

Configuring Avaya Aura® Communication Manager

General usage and important notes

For releases before Avaya Aura® Communication Manager 6.0 the special application SA8567-PHS X-Station Mobility over IP is mandatory to be installed to enable the IP-DECT capability on Communication Manager. Since Communication Manager 6.0 IP DECT is part of the general Communication Manager features, hence SA8567 is not required any more.

The communication between the Communication Manager and the IP-DECT system is done via IP-Trunks using the H.323/X-Mobile protocol. One or more fixed IP trunk connections are required between an IPBS Master and Communication Manager. The Radio IPBS are controlled by the IPBS Master, they do not register to the Communication Manager system.

Several Master IPBS can be connected to the Communication Manager building one common IP-DECT system while one main Master IPBS holds the DECT user database. Users can roam between these IP-DECT masters using one single subscription with the system.

A separate IPBS Master needs to be configured for a site which has survivability for the Communication Manager system. The primary trunks of this IPBS master will be configured to the Communication Manager in the main location. Redundant trunks will be configured to the local LSP that will take over if the connection to the main location fails. This LSP can only take over if the main location uses PE (processor ethernet) for the trunk connection to the Master IPBS (This requires Communication Manager 5.2 or higher). The number of signaling and trunk groups strongly depends on the system architecture of the IP-DECT system in terms of number of users, number of locations and redundancy requirements. For more information, see Configuring trunks on page 156.

For DECT R4 users the same features are available as for DECT R2 and previous IP DECT users. The available features and feature operation is the same as for analog station users, but interactions with Multiple Locations feature set is limited. Roaming users have to follow the actual location rules for dialing and for feature activation/deactivation.

Since Communication Manager 4.0.3 and Communication Manager 5.1 the optional feature Location Based Routing for IP-Trunks was introduced which is important for Multi-Location configuration. For Communication Manager versions below Communication Manager 6.0 the SA field SA9004 - Location Based Routing for IP-Trunks on page 7 of the system-parameters special-applications form needs to be enabled. Since Communication Manager 6.0 Location Based Routing for IP-Trunks is part of the general Communication Manager features, hence SA9004 is not available any more.

The Avaya 3720/3725 and 3740/3749 telephone user should use feature access codes (FAC), programmed via PDM for in-call menu and/or call services menu in the phone for activating/ deactivating Communication Manager features if the station's COS has the Console Permission turned off (set to ’n’).

Communication Manager system administration

The configuration and administration for IP-DECT on Communication Manager 6.0 is now part of Communication Manager documentation. For more information, refer the following documents:

- Administering Avaya Aura® Communication Manager, DOC-ID 03-300509
- Avaya Aura® Communication Manager Feature Description and Implementation, DOC-ID 555-245-205
- Avaya Aura® Communication Manager Screen Reference, DOC-ID 03-602878

For previous versions of Avaya Communication Manager, such as Communication Manager 4, and Communication Manager 5, you can find the system administration described below.

The required settings for DECT R4 are highlighted in the screenshots. All other settings in the screenshots are only exemplary and dependent on the customer demands. Changing all of them to the screenshot values could cause some trouble.

The special application SA8567 and optional SA9004 needs to be enabled in the license file:

For Communication Manager 4 and Communication Manager 5

```
display system-parameters special-applications                  Page   4 of   7
                              SPECIAL APPLICATIONS

     (SA8481) - Replace Calling Party Number with ASAI ANI? n
                (SA8500) - Expanded UUI Display Information? n
                  (SA8506) - Altura Interoperability (FIPN)? n
                 (SA8507) - H245 Support With Other Vendors? n
                 (SA8508) - Multiple Emergency Access Codes? n
 (SA8510) - NTT Mapping of ISDN Called-Party Subaddress IE? n
                       (SA8517) - Authorization Code By COR? n
   (SA8518) - Automatic Callback with Called Party Queuing? n
           (SA8520) - Hoteling Application for IP Terminals? n
  (SA8558) - Increase Automatic MWI & VuStats (S8700 only)? n
             (SA8567) - PHS X-Station Mobility over IP? y
       (SA8569) - No Service Observing Tone Heard by Agent? n
                  (SA8573) - Call xfer via ASAI on CAS Main? n
           (SA8582) - PSA Location and Display Enhancements? n
                (SA8587) - Networked PSA via QSIG Diversion? n
                          (SA8589) - Background BSR Polling? n
     (SA8608) - Increase Crisis Alert Buttons (S8700 only)? n
                       (SA8621) - SCH Feature Enhancements? n
```

Since Communication Manager 4.0.3 and Communication Manager 5.1

```
Change system-parameters special-applications                    Page 7 of 7
                            SPECIAL APPLICATIONS

                      (SA8896) - IP Softphone Lamp Control? n
                  (SA8911) - Expanded Public Unknown Table? n
      (SA8917) - LSP Redirect using special coverage point? n
     (SA8928) - Display Names on Bridged Appearance Labels? n
            (SA8931) - Send IE with EC500 Extension Number? n
          (SA8944) - Multiple Logins for Single IP Address? n
  (SA9004) - Multi-Location Call Routing for IP-Trunk? n
```

Configure maximum number of DECT R4 X-Mobile stations

It's not possible to configure X-Mobile DECT stations if the max number is set to 0. If the special application SA8567 is not available the number of XMOBILE stations will remain 0.

For Communication Manager 4

```
display system-parameters customer-options                      Page   1 of  11
                              OPTIONAL FEATURES

     G3 Version: V14
       Location: 2                          RFA System ID (SID): 1
       Platform: 7                          RFA Module ID (MID): 1

                                                          USED
                              Platform Maximum Ports: 900   69
                                   Maximum Stations: 450   7
                         Maximum XMOBILE Stations: 100    18
                  Maximum Off-PBX Telephones - EC500: 0     0
                  Maximum Off-PBX Telephones -   OPS: 0     0
                  Maximum Off-PBX Telephones - PBFMC: 0     0
                  Maximum Off-PBX Telephones - PVFMC: 0     0
                  Maximum Off-PBX Telephones - SCCAN: 0     0




        (NOTE: You must logoff & login to effect the permission changes.)
```

Configure the node name and IP- address for the IP-DECT system

This is the name and IP-Address of the DECT R4 system (Master IPBS).

For Communication Manager 4 and Communication Manager 5

```
display node-names ip
                                    IP NODE NAMES
    Name                  IP Address
ACM2                   192.168.0.1
Master IPBS            192.168.0.104
default                0.0.0.0
procr                  192.168.0.200




( 4 of 4 administered node-names were displayed )
Use 'list node-names' command to see all the administered node-names
Use 'change node-names ip xxx' to change a node-name 'xxx' or add a node-name
```

Configure the codec used for the selected network region

A codec-set supported by IPBS and **Media Encryption**-**none** is required, the "Far-end Network Region" that has to be configured in the signaling-group will be linked to this codec.

IPBS codec support:

- G.711 A-law (64kbps) – 20 and 30 ms packets
- G.711 µ-law (64kbps) – 20 and 30 ms packets
- G.723.1 (5.3 kbps) – 30 and 60 ms (Not supported with Avaya G450 Gateway)
- G.729A (16 kbps) - 20, 30, 40, 50, and 60 ms

For Communication Manager 4 and Communication Manager 5

```
display ip-codec-set 1                                          Page   1 of   2

                         IP Codec Set

   Codec Set: 1

   Audio         Silence      Frames   Packet
   Codec         Suppression  Per Pkt  Size(ms)
 1: G.711MU         n           2         20
 2:
 3:
 4:
 5:
 6:
 7:


    Media Encryption
 1: none
 2:
 3:
```

```
display ip-network-region 1                                   Page   1 of  19
                              IP NETWORK REGION
  Region: 1
Location:         Authoritative Domain:
    Name:
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                        IP Audio Hairpinning? n
   UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS                  RTCP Reporting Enabled? y
 Call Control PHB Value: 46      RTCP MONITOR SERVER PARAMETERS
        Audio PHB Value: 46       Use Default Server Parameters? y
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                       RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

```
display ip-network-region 1                                   Page   3 of  19

                    Inter Network Region Connection Management

 src dst codec direct   WAN-BW-limits   Video                            Dyn
 rgn rgn  set   WAN  Units    Total Norm  Prio Shr Intervening-regions  CAC IGAR
 1   1    1
 1   2    1     y    NoLimit                                             n
 1   3
 1   4
 1   5
 1   6
 1   7
 1   8
 1   9
 1   10
 1   11
 1   12
 1   13
 1   14
 1   15
```

Configuring the dial plan

The TAC you enter on the **Trunk Group** screen must match the format you have administered for a DAC on the **Dial Plan Analysis Table.**

For Communication Manager 4 and Communication Manager 5

```
display dialplan analysis                                    Page   1 of  12
                          DIAL PLAN ANALYSIS TABLE
                                                          Percent Full:    0

      Dialed   Total  Call    Dialed   Total  Call     Dialed   Total  Call
      String   Length Type    String   Length Type     String   Length Type
       0          1   fac
       1          3   ext
       2          4   ext
       3          4   ext
       4          4   ext
       5          4   ext
       9          3   dac
       *          3   fac
       #          3   fac
```

Configuring the signaling group

The IP trunk's signaling group needs to have the node name of the Master IPBS as **Far-end Node Name**.

There is a strong linkage between the **signaling group** and the related **trunk group**. When creating the signaling group before the trunk group is available, the fields **Trunk Group for NCA TSC**, **Trunk Group for Channel Selection**, and **X-Mobility/Wireless Type** have to be left **blank**. After the trunk group is created change the **Trunk Group for NCA TSC**, **Trunk Group for Channel Selection** to the number of the new trunk group and **X-Mobility/Wireless Type** should be **DECT**.

The **Near-end Listen Port** needs to match the Master IPBS IP Trunk setting "CS Port". The **Far-end Listen Port** needs to match the Master IPBS Trunk setting "**Local Port**".

Note:

Do not use port 5022 as **Local Port** or **Far-end Listen Port**. It is already used internally on the Communication Manager side.

Max number of NCA TSC and **Max number of CA TSC** should be set to 1 or higher. The Enable Layer 3 Test should be set to "y" for IP trunk supervision.

For Communication Manager 4

```
display signaling-group 9                                    Page   1 of   5
                                SIGNALING GROUP

 Group Number: 9                 Group Type: h.323
                              Remote Office? n          Max number of NCA TSC: 1
                                        SBS? n           Max number of CA TSC: 1
          IP Video? n                                 Trunk Group for NCA TSC: 9
 Trunk Group for Channel Selection: 9               X-Mobility/Wireless Type: DECT
     TSC Supplementary Service Protocol: a             Network Call Transfer? 1
                           T303 Timer(sec): 10

   Near-end Node Name: procr                  Far-end Node Name: Master IPBS_110
Near-end Listen Port: 6000                          Far-end Listen Port: 6000
                                                  Far-end Network Region: 1
        LRQ Required? n                  Calls Share IP Signaling Connection? n
        RRQ Required? n
    Media Encryption? n                       Bypass If IP Threshold Exceeded? n
                                                      H.235 Annex H Required? n
        DTMF over IP: In-band               Direct IP-IP Audio Connections? y
Link Loss Delay Timer(sec): 90                        IP Audio Hairpinning? n
Enable Layer 3 Test? y                          Interworking Message: PROGress
                                             DCP/Analog Bearer Capability: 3.1kHz
```

Since Communication Manager 4.0.3 and Communication Manager 5.1

The **Location for Routing Incoming Calls** parameter is only visible when SA9004 field is ON and group type is H323. The setting for **Location Routing Inc Calls** provides the location from where the call is being initiated over the Signaling Group. If "Location Routing Inc Calls" field of Signaling Group is blank (default value), the location of CLAN's cabinet or the location of the Processor Ethernet (PE) is taken for routing the call, depending on whether CLAN or PE is being used to carry that H.323 signaling channel.

.

```
 Page   1 of   5
                              SIGNALING GROUP

 Group Number: 110            Group Type: h.323
                          Remote Office? n          Max number of NCA TSC: 5
                                   SBS? n           Max number of CA TSC: 5
         IP Video? n                             Trunk Group for NCA TSC: 110
Trunk Group for Channel Selection: 110     X-Mobility/Wireless Type: DECT
      TSC Supplementary Service Protocol: a
T303 Timer(sec): 10                          Location Routing Inc Calls? xxx
H.245 DTMF Signal Tone Duration(msec):
Near-end Node Name: aled-S85_CLAN_1       Far-end Node Name: Master IPBS
 Near-end Listen Port: 5210               Far-end Listen Port: 5210
                                       Far-end Network Region: 1
        LRQ Required? n               Calls Share IP Signaling Connection? n
        RRQ Required? n
    Media Encryption? n                     Bypass If IP Threshold Exceeded? n
                                                H.235 Annex H Required? n
        DTMF over IP: In-band           Direct IP-IP Audio Connections? y
 Link Loss Delay Timer(sec): 90                   IP Audio Hairpinning? n
 Enable Layer 3 Test? y                     Interworking Message: PROGress
                                     DCP/Analog Bearer Capability: 3.1kHz
```

Configuring the signaling group for LSP setup

After adding first page of the signaling group on the main server (as mentioned in the heading **Configuring the signaling group**), now go to the page-2 of the signaling group and configure the page as below.

Note:

Note: Below page will display only with Communication Manager 5.2 or later version and with PE configuration only.

```
change signaling-group 2                                        Page   2 of 6

                LIMIT SIGNALING GROUP USAGE
             Enable on the main Processor(s)? y
           Enable on Survivable Processors (ESS and LSP): all
```

Configuring the trunk group

Set for the **Signaling Group** the related **signaling group** number used for DECT R4 trunk or if the Member Assignment Method is manual, the related Signaling Group has to be set for each trunk group member.

Set the TAC (Trunk Access Code) according to the dialplan analysis table for a DAC (Dial Access Code), same first digits (dialed string) and same total length.

The Incoming Digit Handling for the IP trunk should support overlap:

Application note:

For the Signaling Group, set the related signaling group number used for DECT R4 trunk. Otherwise, if the Member Assignment Method is manual, the related Signaling Group has to be set for each trunk group member.

An extra trunk group and an appropriate signaling group needs to be configured for each trunk configured on IPBS Master and Standby Master as Primary or Redundant Trunk. Every signaling group shall have a dedicated trunk group and vice versa (it is not allowed to use the same trunk group by two signaling groups). A trunk group used by an IPBS Master or Standby Master cannot share port to several Signaling Groups.

Set the Trunk Access Code (TAC) according to the dial plan analysis table for a Dial Access Code (DAC), same first digits (dialed string) and same total length. The Incoming Digit Handling for the IP trunk should support overlap.

For Communication Manager 4 and Communication Manager 5

```
display trunk-group 9                                        Page   1 of  21
                              TRUNK GROUP

Group Number: 9                    Group Type: isdn          CDR Reports: y
  Group Name: IP_DECT_Trunk              COR: 1        TN: 1        TAC: 909
   Direction: two-way       Outgoing Display? n        Carrier Medium: H.323
 Dial Access? y             Busy Threshold: 255  Night Service:
Queue Length: 0
Service Type: tie                  Auth Code? n
                                           Member Assignment Method: auto
                                                     Signaling Group: 9
                                                   Number of Members: 10
```

```
display trunk-group 9                                          Page   2 of  21
      Group Type: isdn

TRUNK PARAMETERS
         Codeset to Send Display: 0   Codeset to Send National IEs: 6
                                    Charge Advice: none
Supplementary Service Protocol: a Digit Handling (in/out): overlap/enbloc
       Digit Treatment:                                      Digits:

                                                  Digital Loss Group: 18
Incoming Calling Number - Delete:     Insert:                 Format:

 Disconnect Supervision - In? y  Out? v
 Answer Supervision Timeout: 0
                                  CONNECT Reliable When Call Leaves ISDN? n
```

```
display trunk-group 9                                          Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                  Internal Alert? n        Maintenance Tests? y
                                Data Restriction? n     NCA-TSC Trunk Member: 1
                                      Send Name: n Send Calling Number: y
            Used for DCS? n                               Send EMU Visitor CPN? n
   Suppress # Outpulsing? y   Format: unk-pvt
                                          UUI IE Treatment: service-provider

                                             Replace Restricted Numbers? n
                                           Replace Unavailable Numbers? n
                                              Send Connected Number: y
Network Call Redirection: none               Hold/Unhold Notifications? n
             Send UUI IE? y                Modify Tandem Calling Number? n
               Send UCID? n
 Send Codeset 6/7 LAI IE? y
```

```
display trunk-group 9                                          Page   4 of  21
                       QSIG TRUNK GROUP OPTIONS









                                SBS? n
                  QSIG Value-Added? n
```

```
display trunk-group 9                                          Page   5 of  21
                                TRUNK GROUP
                                     Administered Members (min/max):   1/10
GROUP MEMBER ASSIGNMENTS                 Total Administered Members:  10

       Port              Name        Night
  1: T00051              IP_DECT_Tr
  2: T00052              IP_DECT_Tr
  3: T00053              IP_DECT_Tr
  4: T00054              IP_DECT_Tr
  5: T00055              IP_DECT_Tr
  6: T00056              IP_DECT_Tr
  7: T00057              IP_DECT_Tr
  8: T00058              IP_DECT_Tr
  9: T00059              IP_DECT_Tr
 10: T00060              IP_DECT_Tr
 11:
 12:
 13:
 14:
 15:
```

Configuring the station

The DECT station administration **Type** should be XMOBILE, the **XMOBILE Type** should be DECT and the **Configuration Set** should be blank. The Avaya 3720/3725 and 3740/3749 DECT sets support ICON Message Waiting, therefore **Message Lamp Ext** has to be set to the station number and **Length of Display** to 16x2. For the **Mobility Trunk Group** select the appropriate Trunk group. **Cell Phone Number** needs to be set to the station number and **Mapping Mode** to both.

Note:

If the feature "Redirect in charger" should be used, in Page 3 of 4, **No Reply For Internal/External Calls** has to be set to **Y**.

Application Note:

The DECT station administration **Type** should be XMOBILE, the **XMOBILE Type** should be DECT, and the **Configuration Set** should be blank. The Avaya 3720/3725 and 3740/3749 DECT sets support ICON Message Waiting, therefore **Message Lamp Ext** has to be set to the station number and **Length of Display** to **16x2**. **Cell Phone Number** needs to be set to the station number and **Mapping Mode** to both.

For the **Mobility Trunk Group**, select the appropriate trunk group. At least one of the Primary Trunks to the IPBS Master should be selected. The mobility trunk group will be updated automatically in the station form according to the currently used trunk. This will be achieved by sending a proprietary H.323 X-Mobile message for each station on the currently assigned trunk from the IPBS Master or Standby Master to the Communication Manager.

If the feature "Redirect in charger" should be used, **No Reply For Internal/External Calls** has to be set to **Y**.

For Communication Manager 4 and Communication Manager 5

```
display station 5012                                          Page   1 of   4
                                    STATION

Extension: 5012                       Lock Messages? n              BCC: 0
  Type: XMOBILE                     Security Code:                  TN: 1
                                   Coverage Path 1:                 COR: 1
     Name: IPDECT 5012             Coverage Path 2:                 COS: 1
                                   Hunt-to Station:
STATION OPTIONS
                                       Time of Day Lock Table:

  XMOBILE Type: DECT                        Message Lamp Ext: 5012
         Display Module? y                Message Waiting Type: ICON
       Display Language: english          Length of Display: 16x2
    Mobility Trunk Group: 9                     Calls Allowed: all
       Configuration Set:

 CELL PHONE NUMBER MAPPING
             Dial Prefix:
       Cell Phone Number: 5012
            Mapping Mode: both
```

```
display station 5012                                          Page   2 of   4
                                    STATION
FEATURE OPTIONS
           LWC Reception: spe
          LWC Activation? y
  LWC Log External Calls? n
              CDR Privacy? n                            Data Restriction? n
                                                  Call Waiting Indication: y
                                              Att. Call Waiting Indication: y
   Bridged Call Alerting? y                      Distinctive Audible Alert? y
        Switchhook Flash? y

                                    Per Station CPN - Send Calling Number?
       Service Link Mode: as-needed
         Multimedia Mode: basic                   Audible Message Waiting? y
    MWI Served User Type:
              AUDIX Name:
                                              Coverage After Forwarding? s
                                                Multimedia Early Answer? n

  Emergency Location Ext: 5012
```

```
display station 5012                                          Page   3 of   4
                                    STATION


Bridged Appearance Origination Restriction? n




                              ENHANCED CALL FORWARDING
                                      Forwarded Destination         Active
 Unconditional For Internal Calls To:                                  n
                   External Calls To:                                  n
          Busy For Internal Calls To:                                  n
                   External Calls To:                                  n
      No Reply For Internal Calls To:                                  n
                   External Calls To:                                  n
```

```
display station 5012                                          Page   4 of   4
                                    STATION

                                                       Headset? n
                                                       Speaker? n
                                                      Mounting: d
     Floor:                                          Cord Length: 0
   Building:                                           Set Color:




ABBREVIATED DIALING
     List1:                    List2:                    List3:

HOT LINE DESTINATION
         Abbreviated Dialing List Number (From above 1, 2 or 3):
                                                      Dial Code:

     Line Appearance: call-appr
```

SRTP Configuration

Verifying License Grant permissions for configuring SRTP

On the Communication Manager, view the installed license grants permisisons.

1. Use the SAT command as follows

   display-system parameters customer options.

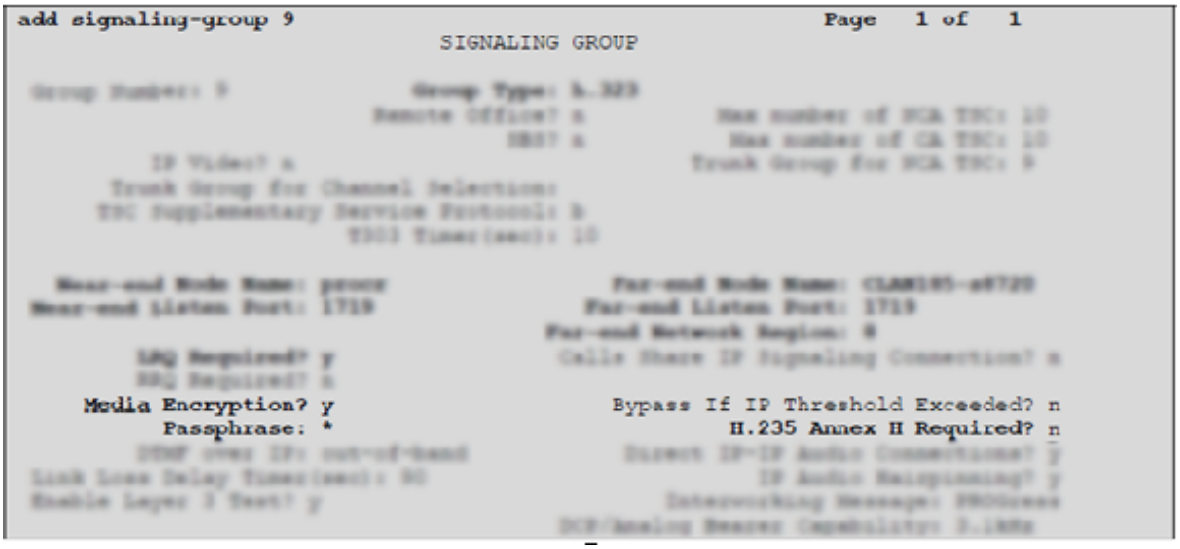
```
display system-parameters customer-options                    Page   2 of  10
                            OPTIONAL FEATURES
IP PORT CAPACITIES                                      USED
                  Maximum Administered H.323 Trunks: 50    48
            Maximum Concurrently Registered IP Stations: 10    3
```

```
display system-parameters customer-options                    Page   4 of  10
                            OPTIONAL FEATURES
   Emergency Access to Attendant? y                          IP Stations? y
            Enable 'dadmin' Login? y
            Enhanced Conferencing? y                      ISDN Feature Plus? n
                   Enhanced EC500? y          ISDN Network Call Redirection? n
    Enterprise Survivable Server? n                        ISDN-BRI Trunks? n
       Enterprise Wide Licensing? n                              ISDN-PRI? y
                  ESS Administration? n               Local Survivable Processor? n
          Extended Cvg/Fwd Admin? y                    Malicious Call Trace? y
       External Device Alarm Admin? n                Media Encryption Over IP? y
  Five Port Networks Max Per MCC? n     Mode Code for Centralized Voice Mail? n
                  Flexible Billing? n
    Forced Entry of Account Codes? n                 Multifrequency Signaling? y
       Global Call Classification? y          Multimedia Call Handling (Basic)? n
              Hospitality (Basic)? y       Multimedia Call Handling (Enhanced)? n
 Hospitality (G3V3 Enhancements)? n
                       IP Trunks? y
```

2. Verify whether sufficient H.323 trunk and IP station capacity are available.
3. Verify whether Media Encryption over IP is enabled.
4. Next, verify whether private networking is enabled.

```
display system-parameters customer-options                    Page   5 of  10
                            OPTIONAL FEATURES
                Multinational Locations? n                Station and Trunk MSP? y
 Multiple Level Precedence & Preemption? n          Station as Virtual Extension? n
                     Multiple Locations? y
                                                  System Management Data Transfer? y
          Personal Station Access (PSA)? y                   Tenant Partitioning? n
                       Posted Messages? y          Terminal Trans. Init. (TTI)? y
                       PNC Duplication? n                   Time of Day Routing? y
                  Port Network Support? n                  Uniform Dialing Plan? y
                                                 Usage Allocation Enhancements? y
              Processor and System MSP? y          TN2501 VAL Maximum Capacity? y
                    Private Networking? y
                    Processor Ethernet? y                    Wideband Switching? n
```

5. On the signaling group page, set Media Encryption =Y
6. Set H.235 Annex H Required = N



7. Enter Passphrase.

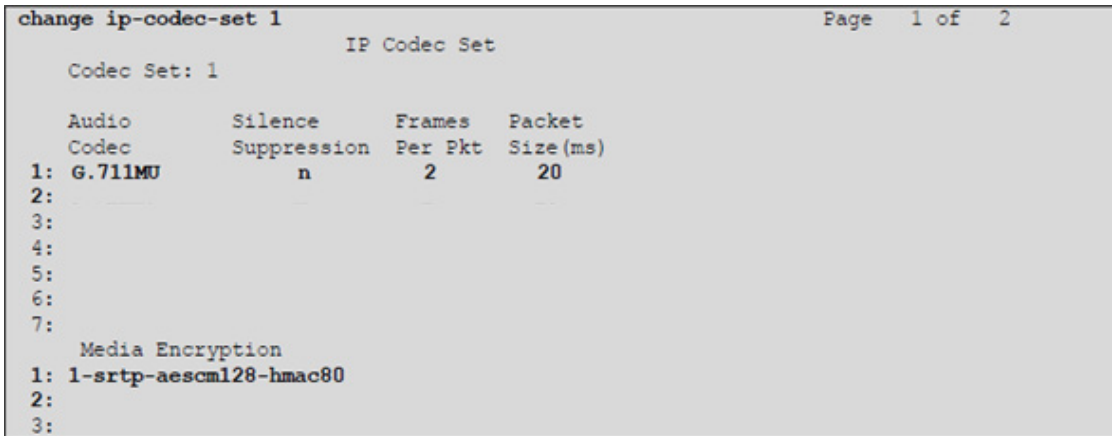
   The passphrase entered shall match the Passphrase entered in base station, since CM uses it to encrypt keys during key exchange.

8. On the Network region configuration page, set the H.323 profile to use "any-auth" to allow for the procedures relevant to the device. You can also use "pin-eke" (H.323 H SP1).

9. In IP CODEC set form ‘Media Encryption’ group specifies a priority listing of the three possible options for the negotiation of encryption. Communication Manager attempts to provide bearer encryption per this administered priority order. The selected option for an IP codec set applies to all codecs defined in that set.

Note:

Although it is possible to configure several codecs in the Communication Manager IP-Codec-SET page, ensure that the first entry in the list in the Code list and Media encryption list is equivalent to the **Coder** and the ***Secure RTP*** field value in the IPBL/IPBS system because the IPBS/IPBL supports only one protocol at a time.



```
change ip-codec-set 1                                          Page   1 of   2
                        IP Codec Set
    Codec Set: 1

    Audio          Silence      Frames   Packet
    Codec          Suppression  Per Pkt  Size(ms)
 1: G.711MU             n          2        20
 2:
 3:
 4:
 5:
 6:
 7:
     Media Encryption
 1: 1-srtp-aescm128-hmac80
 2:
 3:
```

For configuring SRTP on base station see, Enabling SRTP on the base stations. on page 166

Installing and operating the Advanced Charger

Introduction

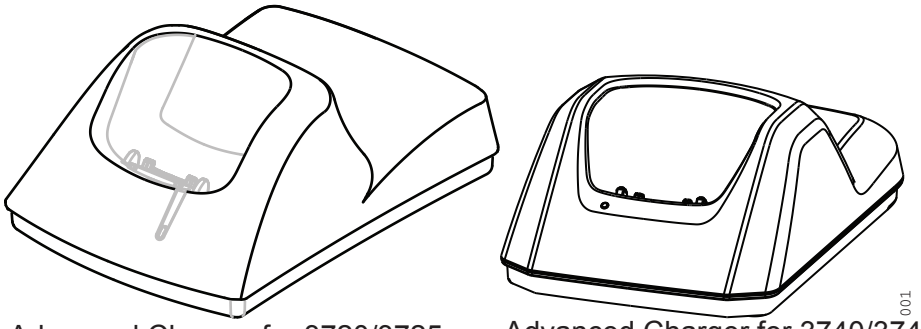
This chapter describes how to install, configure and operate the Advanced Charger. It is an advanced charger equipped with a USB port, making it possible to connect it directly to a PC for the purpose of upgrading or configuring the Advanced Charger itself or a cordless telephone placed in the charger. The Advanced Charger also has two Ethernet ports, enabling upgrading and configuring over a LAN of a cordless telephone placed in the charger.

The USB port is used to connect the Advanced Charger to a PC running the Portable Device Manager (PDM). This program can be used to upgrade the software and to configure parameters in the Advanced Charger as well as in a cordless telephone placed in the Advanced Charger.

The USB port is used when the Advanced Charger is connected to a PC running thePortable Device Manager (PDM). The PDM or the Avaya In-Building Wireless Server (AIWS) can be used to upgrade the software and to configure parameters in the Advanced Charger as well as in a telephone placed in the Advanced Charger.

The Advanced Charger supports easy replacement, that is replacement of a faulty telephone via the telephone display and does not involve PDM or AIWS.

Figure 58: Advanced Charger



Advanced Charger for 3720/3725 Advanced Charger for 3740/3749

The Ethernet ports makes it possible to connect several Advanced Chargers to the same LAN.

This chapter is intended as a guide for installation, maintenance, operation and troubleshooting purposes.

	Advanced Charger	Advanced Charger Adapter
Supply voltage	5 V DC	100 - 240 V AC, (50-60Hz)
Max current consumption when charging	2.0 A	0.4 A

Safety

The desktop charger adapter shall be connected to 100 - 240 V AC, 50 - 60 Hz. Therefore extra caution shall be taken during operation. The Advanced Charger itself is supplied with 5 V DC from the adapter.

Important:
Use only the power supply adapter delivered with the charger. Replacing with other power supply units means risk of battery explosion caused by too high input voltage or switched polarity. Supplying the charger with 5 V on opposite poles than intended is strongly forbidden.

Technical solution

The following functionality is provided by the Advanced Charger:

- Provide a means for software and parameter update of cordless telephones.
- Charging of the battery of the telephone.
- Easy replacement

The Advanced Charger has one USB connection and two Ethernet connections. When using Ethernet connection it is possible to connect several Advanced Charger serially to the LAN.

If the Advanced Charger is connected towards PDM via both USB and Ethernet, the USB connection overrides the Ethernet connection.

Each Advanced Charger needs an IP address.

See label for MAC address.

Requirements

Computer:

- USB port. USB 1.1 required, USB 2.0 supported.
- Ethernet port 10/100 Mbit/s.
- Windows XP® Professional including Service Pack 2 (SP2), Windows 7® Professional, Windows 7® Enterprise, or Windows 7® Ultimate.

Installation and configuration

Important:
Installation of the unit is NOT permitted in an hazardous area. Only an authorized personnel must install the unit.

Advanced Charger installation

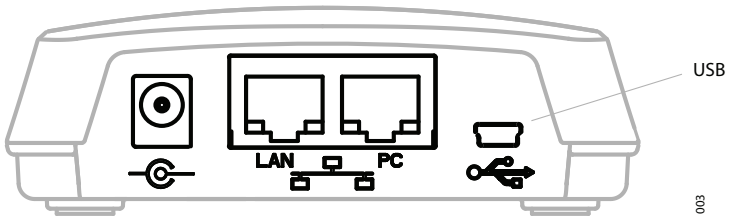
The chargers shall be placed in a dry environment with a temperature range from 5° C up to + 40° C.

Delivery includes:

- Advanced Charger
- Power Supply Cable (AC cord with corresponding wall plug)
- Power Supply adapter including DC cable
- USB cable

No tools are required.

Figure 59: Advanced Charger connections



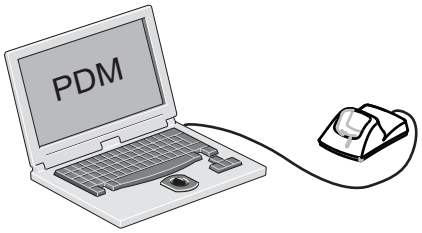
From left: DC power, Ethernet LAN, Ethernet PC and USB.

1. Connect the AC power supply cord to the adapter.
2. Connect the power supply cord to the wall socket.
3. Connect the DC cable to the charger. The charger LED indicates the status of the charger. See table in chapter Operation on page 277.
4. Connect the Advanced Charger to the pc with a USB or Ethernet cable.

One of the Ethernet connections is used for communication with a PC and the other can be used for LAN connection. Power over Ethernet is not supported.

The USB Interface supports USB 2.0 Full speed. One Mini-B Receptacle USB connector is used. The USB connection is used for communication with a PC. Power over USB is not supported.

Figure 60: Connection to PDM



Software installation

The charger is delivered with pre-installed software and it is possible to upgrade the charger software. Please see Software update on page 276.

Advanced Charger configuration

Each Advanced Charger need access to DHCP to receive an IP address automatically. If no DHCP is accessible it is possible to configure the IP address with PDM or AIWS.

If the Advanced Charger is configured to run DHCP, connect the network cable and the charger will automatically receive an IP address. If the charger is not configured to run DHCP the charger will use the setup IP addresses.

The following parameters exist for Advanced Charger and can be changed via PDM or AIWS:

Parameter	Description
Ethernet Bit rate[1]	auto (default)
Ethernet connector[1]	auto (default)
Ethernet duplex[1]	auto (default)
DHCP Enabled	Yes (default), No
Charger IP address[2]	192.168.0.101 (default)
Subnet mask	255.255.255.0 (default)
Default gateway IP address	192.168.0.1 (default)
DNS IP address	192.168.0.2 (default)

Charger IP port	12346 (default)
Service Discovery Enabled	Yes (default), No
Service Discovery Domain	Name of domain
DH IP address (one DH only)	192.168.0.3 (default)
DH IP port	10147 (default)

1. Currently only “auto” setting is available
2. The IP address is only valid if **DHCP Enabled** is set to "No".

Note:
It may be necessary to import the parameter definitions file that is included in the software package.

Follow this instruction to set Advanced Charger parameters:

1. Check that the Advanced Charger is connected to PDM/AIWS.
2. In PDM or the device manager in AIWS, click on the **Numbers** tab.
3. Select the Advanced Charger device that you want to change parameters for.
4. In the Number menu, click **Edit...**.
5. Edit the parameters you want to edit.
6. Click **OK**.

Advanced Charger does not appear in AIWS

If the Advanced Charger does not appear in the AIWS Device Manager, the Service Discovery might not be working in the customers network setup.

In this case connect the Advanced Charger to PDM and edit the following parameters:

- *Service Discovery Enabled:* No
- *DH IP address (one DH only)*: Enter AIWS IP-Address

Note:
Service Discovery might not work if the Advanced Charger is not in the same subnet as the AIWS.

Security

(information regarding software security)

N/A

Commissioning

Follow these instructions to verify that the charging works.

1. Connect the charger according to chapter Advanced Charger installation on page 272.
2. Place a telephone in the charging slot to start charging. The telephone indicates the charging progress, see respective user guide for details.

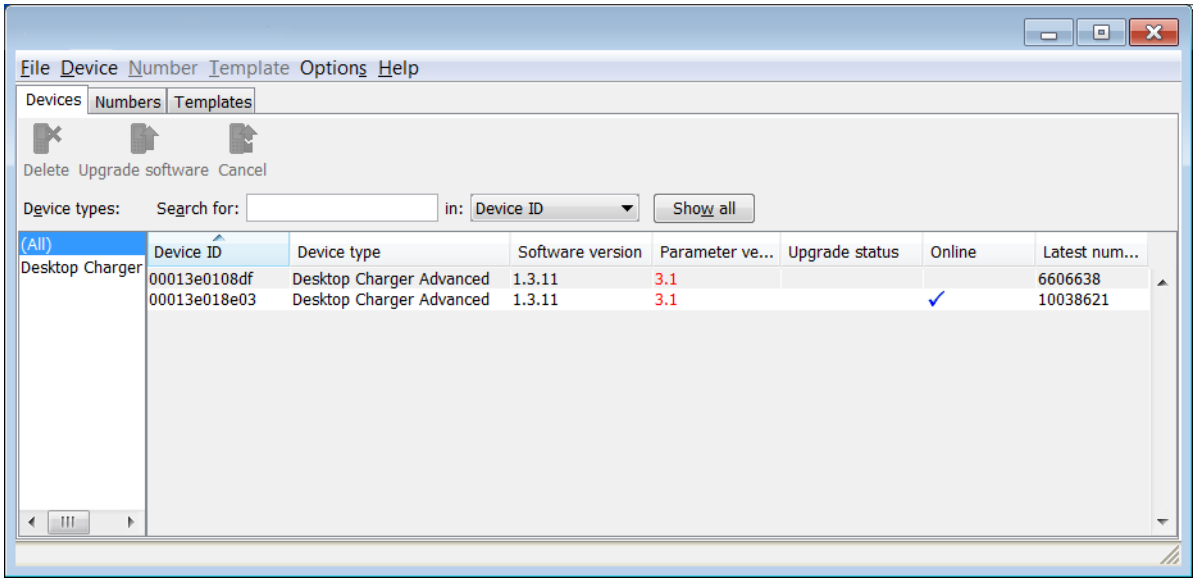
See figure 59 on page 272 to see the connections to the charger.

Follow these instructions to start PDM or AIWS.

In the case of Portable Device Manager (PDM):

1. Check that the charger is connected to your PC via USB.
2. Start PDM.
3. Go to the **Devices** tab and verify that the Advanced Charger is online.

Figure 61: Desktop Charger in PDM.



In the case of Avaya In-Building Wireless Server (AIWS):

1. Check that the charger is connected to the LAN.
2. Start AIWS.
3. Go to the **Devices** tab and verify that the Advanced Charger is online (it may take up to 15 s).

For instructions on how to verify that the charger parameter setting works, and for further instructions, please see Device Manager on page 397.

Maintenance

Software update

The charger software is pre-installed. Updates can be performed by using PDM or AIWS. For PDM details see Delete Imported Files for Devices on page 351, or for AIWS details see Upgrading a device with new software on page 433.

Operation

Charger operation

Operation when charger is connected to power supply

When the charger is connected to external power supply, the following normal operation can be done:

Telephone charging

1. Connect the charger to the AC power supply.
2. Place a telephone in the charging slot to start charging.

Telephone disconnection

1. First, tilt the telephone forwards.
2. Then, lift the telephone upwards.

Note:
Do not try to lift the telephone upwards before tilting it forwards.

Easy Replacement

The Advanced Charger supports the Easy Replacement feature. Easy replacement is performed via the telephone display and does not involve PDM or AIWS. The Advanced Charger only needs a power connection to support easy replacement. A connection to PDM/AIWS is not needed.
See the Configuration Manual for your cordless telephone for details.

Note:
The Advanced Charger software needs to be of version 1.3.7 or higher.

Operation when charger is connected to PDM/AIWS

When the charger is connected to a PDM/AIWS, the following additional operations can be done:

- Software upgrade (of charger or telephone)
- Parameter editing (of charger or telephone)
- Phonebook upload

- Language upload

See Installing and operating the Portable Device Manager (WinPDM) on page 315, or AIWS Device Manager on page 397 for details.

LED indications

The charger is equipped with a status LED. The following indications are used:

LED indication	Description
Green, fixed	Logged on to PDM/AIWS.
Orange, fixed	Not logged on to PDM/AIWS.
Orange, flashing (1000 ms on, 1000 ms off)	1. Software download. 2. File transfer during Easy Replacement
Orange, flashing (100 ms on, 800 ms off)	"Change phone" indication during Easy Replacement.
Red, fixed	Software error. Service needed.
Red flashing	Parameter error
Red, flashing (100 ms on, 800 ms off)	Error indication during Easy Replacement. Put back old telephone in charger. Charger returns to “Not logged in to PDM/AIWS” mode when telephone is removed.
Red, flashing (3 long flashes, 800 ms on, 100 ms off)	Parameter error in user parameters. Charger performs a factory reset and restarts.
Red, flashing (800 ms on, 100 ms off)	1. Parameter error in production parameters. Service needed for charger. 2. Error during Easy Replacement. Service needed for telephone.

LED indications are also described in troubleshooting Advanced Charger on page 687.

Troubleshooting

See Troubleshooting on page 675.

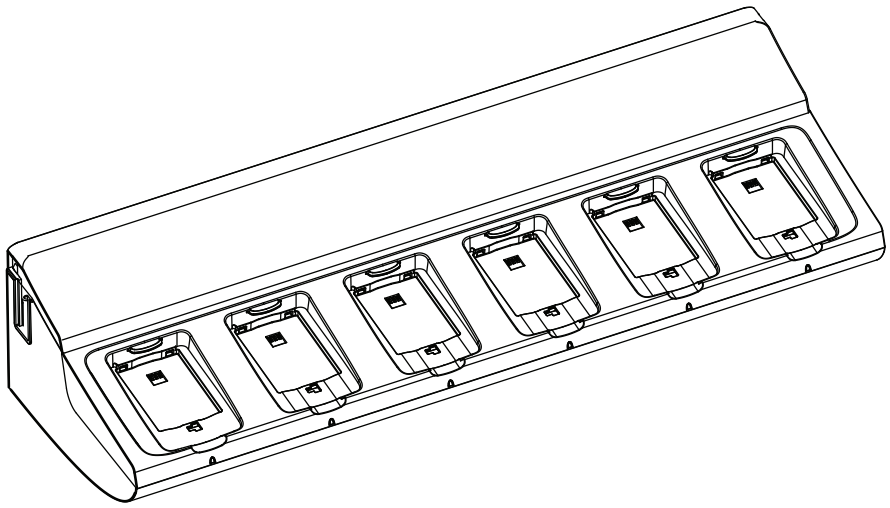
Installing Multiple Battery Charger

Introduction

This chapter describes how to install, configure and operate the Multiple Battery Charger. It charges batteries for the Avaya DECT Telephones.

Each Multiple Battery Charger charges six batteries simultaneously.

Figure 62: Multiple Battery Charger



Multiple Battery Charger can be serially connected with up to four Battery Pack Chargers connected to the same power source.

This chapter is intended as a guide for installation and troubleshooting purposes.

	Power Supply for Multiple Battery Charger
Supply voltage	100–240 VAC/0.7 A, 50/60 Hz
Building fuse for fixed installation	10 A

Installation alternatives

- The CR4 as delivered can be installed as a single unit. When installed as a single unit, the power cord with the C14 connector may be used with a suitable extension cord to be plugged into a wall outlet.

- If more than one CR4 is used in a serial configuration a fixed installation must be made. For safety reasons it is not allowed to supply more than one unit by the power cord with the C14 connector. When units are supplied in series, the installation must be made by an authorized electrician and the C14 connectors must be removed. Maximum five units may be connected in serial power supply.

In Sweden, Norway and Finland a connection to protective earth (safety grounding) must be provided.

Safety

The Battery Pack Charger CR4 shall be connected to 100-240VAC/0.7A 50/60 Hz.

For safety reasons:

- the safety covers on top of the supply voltage terminal blocks must be mounted to prevent hazardous situations, like electric shock.
- when servicing the units the mains power supply cable must be disconnected.

Note the following:

For PERMANENTLY CONNECTED EQUIPMENT, a readily accessible disconnect device shall be incorporated in the building installation wiring. The disconnect device shall disconnect both poles.

For PLUGGABLE EQUIPMENT, the socket-outlet shall be installed near the equipment and shall be easily accessible.

In Sweden, Norway and Finland the unit must be connected to a wall outlet with protective earth (safety grounding). For other countries it is recommended to use a protective earth connection.

- Suomi: Laite on liitettävä suojamaadoituskoskettimilla varustettuun pistorasiaan.
- Norge: Apparatet må tillkoples jordet stikkontakt.
- Sverige: Apparaten skall anslutas till jordat uttag.

Compliance

Regulatory Compliance Statements (EU/EFTA only)

Permission and Conformity

We, Avaya GmbH & Co. KG, declare that the product line Avaya Multiple Battery Charger concurs with the basic requirements and other relevant provisions of EU Directive 1999/5/EU concerning radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity.

Intended use

This equipment is intended for connection to radio interfaces (DECT) of Avaya PABX systems.

It is compliant with the essential requirements of the EU-Directive 1999/5/EU (Radio and Telecommunication Terminal Equipment, R&TTE).

Due to the differences of the individual public networks and network operators this compliance does not by itself give an unconditional assurance of successful operation at every network termination point. For the time being we are not aware of any network on which the equipment will not work due to its design.

In the event of problems, you should contact your equipment supplier or your Avaya service.

The conformity declaration can be accessed at the following Internet address:

www.avaya.de/gcm/emea/de/includedcontent/conformity.htm

or search the index using the key term "Conformity".

CE.

FCC compliance statements for USA

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.

IC Requirements for Canada

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la Classe B conforme á la norme NMB-003 du Canada.

Technical solution

The following functionality is provided by the Multiple Battery Charger:

- Charging of the Avaya DECT telephone battery.

Installation and Configuration

Multiple Battery Charger Installation

General

Important:
The unit shall be installed by authorized personnel only.

- The units shall be placed in a dry environment with a temperature range from +5° C up to + 40° C (41° F to 104° F).
- The units shall be mounted on a vertical wall.
- Avoid mounting the Multiple Battery Charger in a sunlit place. This can affect the charging capacity.
- The unit shall be mounted on concrete or plaster walls only.
- If the Multiple Battery Charger is connected to a power supply via an AC wall plug, serial power supply connection is not allowed.
- When using a fixed connection, up to five Multiple Battery Charger or Rackmount Charger can be serially connected to the same AC connection.
- If the Multiple Battery Charger is connected to a power supply via an AC wall plug, the socket-outlet shall be situated near the equipment and shall be easily accessible.
- If the Multiple Battery Charger is connected to a power supply via a fixed connection, a readily accessible disconnect device shall be incorporated in the building installation wiring.

Delivery includes:

- Battery Pack Charger
- Power supply cord including IEC C14 connector (male)
- Inlet accessory kit including cable support holders and screws

Note:
An extension cord IEC C13 AC connector (female IEC60320-C13) to wall socket has to be ordered separately. It shall be connected between the pre-installed IEC C14 AC connector (male) and the wall socket.

Required Tools etc.

- Screwdrivers
- Cutting pliers
- Multimeter
- Screws and wall plugs for wall mounting. Make sure the screws and wall plugs have the correct length for the type of wall used. See example below:

Wall material	Plug length	Screw diameter
Single plasterboard	Thorsman TP1	3.5 – 5 mm
Double plasterboard	Thorsman TP2	3.5 – 5 mm
Concrete	Thorsman TP2	3.5 – 5 mm

Examples of Ways to Mount the Battery Pack Chargers

The following picture shows different ways to mount Multiple Battery Charger. It is possible to set up different combinations of Multiple Battery Charger and Rack Chargers.

Installation steps

The installation is done in two steps:

1. Wall mounting.
2. Electrical installation.

Wall mounting

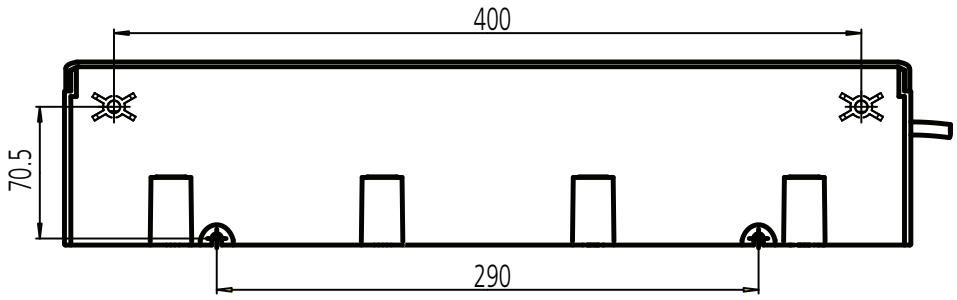
First, make an outline of how the battery pack chargers are to be placed.

Tip:
If several Multiple Battery Charger (or Rackmount Chargers) are to be mounted close to each other, mount them so that there is enough space between then to be able to disconnect the batteries or the telephones (vertical distance) and to be able to open the top cover (horizontal distance).

Tip:
When you are planning the location of the modules, start to mount them in a height that makes it easy to reach the batteries.

Measure and mark the drill holes by using the dimensions in figure 63. Drill and fasten the battery pack charger on the wall with four screws.

Figure 63: Mounting dimensions in mm

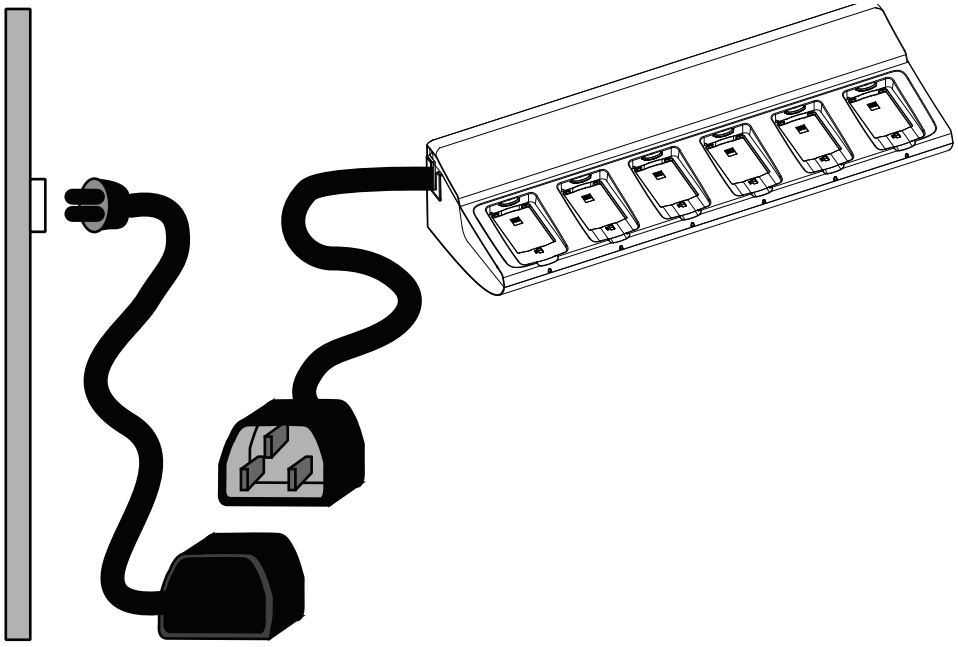


Multiple Battery Charger seen from the back

Electrical installation

The Multiple Battery Charger is delivered with a cord with a an IEC C14 connector (male). An extension cord IEC C13 AC connector (female IEC60320-C13) to wall socket has to be ordered separately. It shall be connected between the pre-installed AC connector (male) and the wall socket.

Figure 64: Multiple Battery Charger with IEC C14 connector and an extension cord with an IEC C13 connector



Installation test

1. Connect the mains power supply cord to the wall socket.

2. Place a battery in the charging slot.
3. A yellow LED indicates that charging starts while a green LED indicates a fully charged battery.

Power supply by fixed connection

Note:

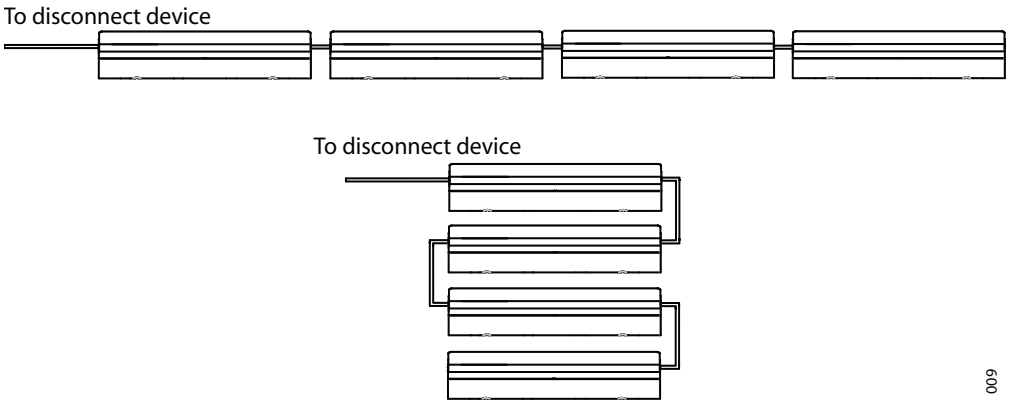
If the rack charger shall be connected with a fixed connection, the AC connection must be done by a authorized electrician.

Tip:

It is possible to use any one of the two AC terminal blocks for AC input. Consequently, the unused terminal block may be used to connect the next rack charger or battery pack charger.

The Power Supply module connects to 100-240VAC/0.7A 50/60 Hz. When working with the units, the main power supply cable must always be disconnected. The safety covers must be mounted on top of the power supply terminal blocks to prevent hazardous situations, like electric chock.

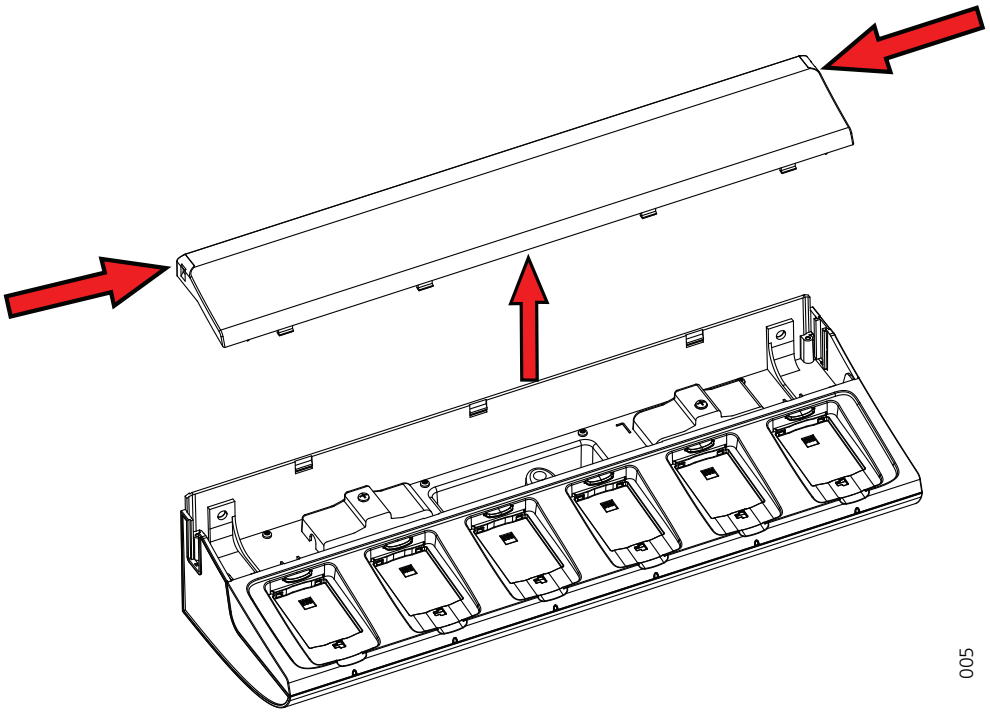
Figure 65: .Examples of how Multiple Battery Charger can be mounted and connected to a power source



Opening the top cover

Open the top cover by first pressing on the sides of the top cover, then lifting it upwards.

Figure 66: Opening the top cover of the Battery Pack Charger



Fixed installation in detail

Fixed installation of the first charger or single unit with fixed electrical installation.

1. Remove the C14 connector from the power cord. Measure cut and strip the power cord to be connected to the disconnect device.
2. Connect the mains power supply cord to the disconnect device.

The IEC color code is used in the power cord supplied.

	Colors			
IEC	US	Old *	Load	Also called
Brown	Black	Red	Active	Line, Hot
Blue	White	Black	Neutral	Return, Cold, Grounded connector
Gr/Ye **	Green	Green	Earth	Ground, Safety Earth, Earth Ground, Grounding conductor ***

* The "Old" standard was used in various countries (including Australia), and some wiring may still use these colors.

** Gr/Ye - Green with Yellow stripe - this is the standard world wide, although it is not common in the US or Canada at present.

*** There is an important distinction between "Grounding conductor" (safety earth) and "Grounded conductor" (Neutral). These are *US* terms for the conductors and they are ***not*** interchangeable, despite the similarity of the names !

Installation of additional units in a serial power configuration

Note:

Maximum five units may be connected in power series.

Important:

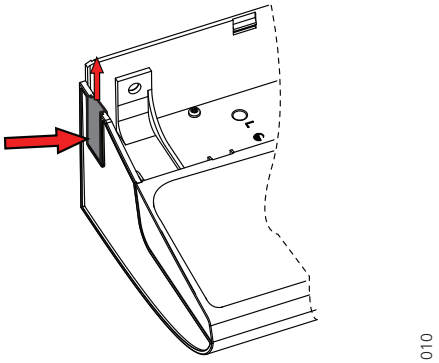
It is not allowed to connect additional Rack Chargers or Battery Pack chargers if the chargers are connected to the power supply via an AC plug.

Important:

Disconnect the power supply connection before working on the units.

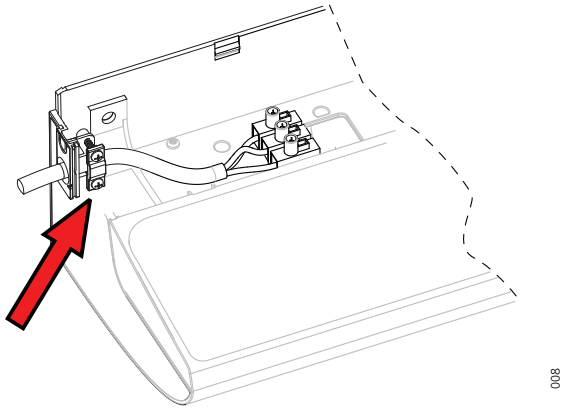
1. If the additional Rack Charger has not yet been mounted on the wall, do this according to figure 65 on page 288.
2. Open the top cover of the rack charger closer to the AC power source.
3. Remove the cover which protects the unused AC output terminal block of the charger closer to the AC power source.
4. Mount the cable support holder at the unused opening in the charger closer to the AC power source. The cable support holder is provided in the parts bag. See figure 67

Figure 67: The rectangular cover that shall be removed and exchanged with a cable support holder with a mains power supply cord run through it



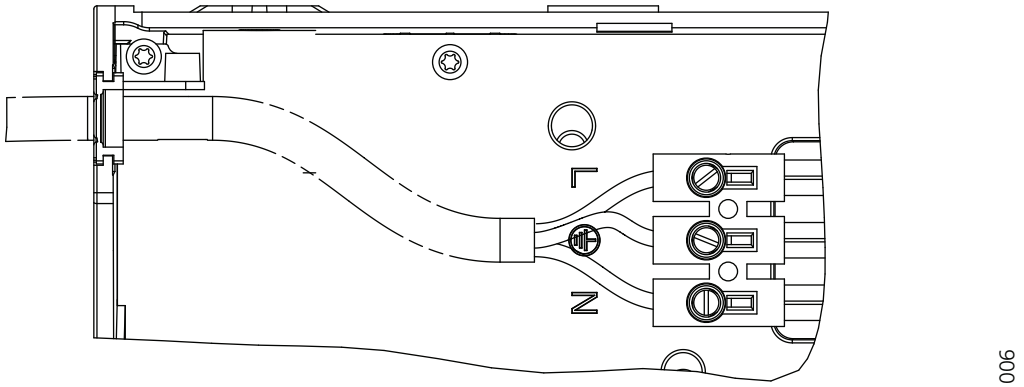
5. Remove the C14 connector from the additional charger. Cut and strip the mains power supply cord coming from the additional charger to the length required.
6. Run the power supply cord from the additional charger through the cable support holder of the previous charger, see figure 68

Figure 68: Securing the *mains power supply cable*



7. Connect the power supply cord from the additional charger to the unused terminal block in the charger closer to the AC power source. Note the embossed markings L, earth symbol and N, see figure 69.

Figure 69: The mains power supply connection



8. Mount the safety cover and fasten it with one screw.
9. Secure the mains power supply cable with two screws (2), which are provided in the parts bag, see figure 68.
10. Replace the top cover, see figure 66.
11. Fasten the power cord to the wall depending on local regulations.
12. If more rack chargers shall be connected, repeat the above steps 1-12 for the next unit.

Installation test

1. When the fixed installation is completed, apply AC power by switching on the disconnect device.
2. Place a battery in the charging slot.
3. A yellow LED indicates that charging starts while a green LED indicates a fully charged battery.

Commissioning

The commissioning includes the following:

- Installation test
- Charging

Installation test

For Installation test, see chapter Installation test on page 292 or 287.

Charging

To verify that the charging works, follow these instructions.

1. Place a battery in a charging slot.
2. A yellow LED indicates that the charging has started while a green LED indicates a fully charged battery.

Operation

When the charger is connected to external power supply, normal operation is done as follows:

charging

1. Connect the charger to the AC power supply.
2. Place a battery in the charging slot to start charging. Secure the battery by moving the lock switch.

Battery disconnection

1. Unlock the lock switch on the battery.
2. Remove the battery by lifting it.

Troubleshooting

See Troubleshooting on page 675.

Installing and operating the Rackmount Charger

Introduction

This chapter describes how to install, configure and operate the Rackmount Charger. The Rackmount Charger is a rack charger equipped with a USB port and two Ethernet ports, making it possible to connect it directly to a LAN or to a PC for the purpose of upgrading or configuring cordless telephones placed in the Rackmount Charger or the Rackmount Charger itself.

Note:

The Rackmount Charger is always intended to be connected to an Ethernet based local area network.

The Rackmount Charger is part of the Avaya IP-DECT systems. It charges the Avaya 3720, 3725, 3740, and 3749 DECT Telephones.

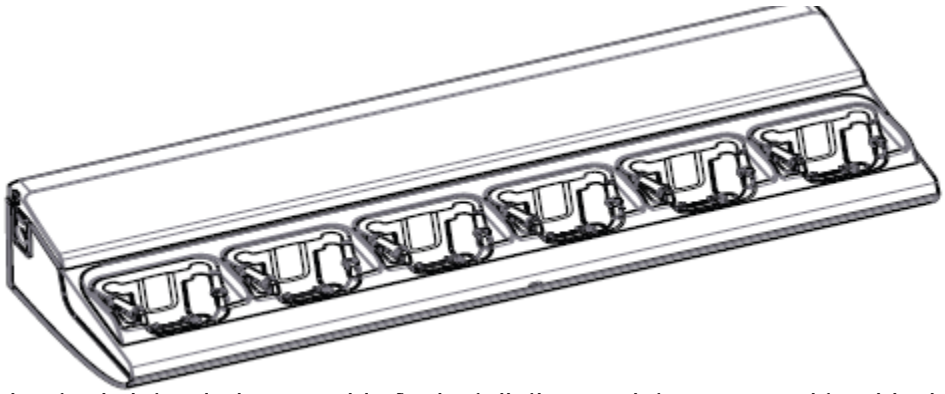
Important:

There are two different CR3 Rack Chargers: An older one for 3720/3725 handsets only and a newer one for both 372x and 374x. Do NOT force a 3740/3749 handset into a charging slot for 3720/3725.

Each Rackmount Charger charges six telephones simultaneously.

The USB port is used to connect the Rackmount Charger to a PC running the Portable Device Manager (PDM) or to the Avaya In-Building Wireless Server (AIWS). This program can be used to upgrade the software and to configure parameters in cordless telephones placed in the Rackmount Charger as well as the Rackmount Charger itself. The Ethernet ports makes it possible to connect up to four Rackmount Charger to one single LAN outlet.

Figure 70: Rackmount Charger



This chapter is intended as a guide for installation, maintenance and troubleshooting purposes.

	Power Supply for Rackmount Charger
Supply voltage	100–240 VAC/0.7 A, 50/60 Hz; Building fuse for fixed installation: 10 A maximum

Installation alternatives

- The Rackmount Charger as delivered can be installed as a single unit. When installed as a single unit, the power cord with the C14 connector may be used with a suitable extension cord to be plugged into a wall outlet. Up to four single units may be connected to one single LAN outlet.
- If more than one Rackmount Charger is used in a serial configuration a fixed installation must be made. For safety reasons you must not supply more than one unit by the power cord with the C14 connector. When units are supplied in series, the installation must be made by an authorized electrician and the C14 connectors must be removed. Maximum five units may be connected in serial power supply, but LAN serial connection is limited to four units.

In Sweden, Norway and Finland a connection to protective earth (safety grounding) must be provided.

In the USA and Canada the CR3 must only be installed as a single unit, serial configuration is not permitted.

Safety

The Rackmount Charger is connected to 100-240VAC/0.7A 50/60 Hz. For safety reasons:

- the safety covers on top of the supply voltage terminal blocks must be mounted to prevent hazardous situations, like electric shock.
- when servicing the units the mains power supply cable must be disconnected.

Note:

For PERMANENTLY CONNECTED EQUIPMENT, a readily accessible disconnect device shall be incorporated in the building installation wiring. The disconnect device shall disconnect both poles.

For PLUGGABLE EQUIPMENT, the socket-outlet shall be installed near the equipment and shall be easily accessible.

In Sweden, Norway and Finland the unit must be connected to a wall outlet with protective earth (safety grounding). For other countries it is recommended to use a protective earth connection.

- Suomi: Laite on liitettävä suojamaadoituskoskettimilla varustettuun pistorasiaan.
- Norge: Apparatet må tillkoples jordet stikkontakt.
- Sverige: Apparaten skall anslutas till jordat uttag.

Compliance

Regulatory Compliance Statements (EU/EFTA only)

Permission and Conformity

We, Avaya GmbH & Co. KG, declare that the product line Avaya Rackmount Charger concurs with the basic requirements and other relevant provisions of EU Directive 1999/5/EUand ErP Directive 2009/125/EC concerning radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity.

Intended use

This equipment is intended for connection to radio interfaces (DECT) of Avaya PABX systems.

It is compliant with the essential requirements of the EU-Directive 1999/5/EU (Radio and Telecommunication Terminal Equipment, R&TTE).

Due to the differences of the individual public networks and network operators this compliance does not by itself give an unconditional assurance of successful operation at every network termination point. For the time being we are not aware of any network on which the equipment will not work due to its design.

In the event of problems, you should contact your equipment supplier or your Avaya service.

The conformity declaration can be accessed at the following Internet address:

www.avaya.de/gcm/emea/de/includedcontent/conformity.htm

or search the index using the key term "Conformity".

CE.

FCC compliance statements for USA

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.

IC Requirements for Canada

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la Classe B conforme á la norme NMB-003 du Canada.

Technical Solution

The following functionality is provided by the Rackmount Charger:

- Provide a means for software and parameter update of telephones.
- Charging of the telephone battery.

The Rackmount Charger has one USB connection and two Ethernet connections. When using Ethernet connection it is possible to connect several Rackmount Chargers serially to the LAN.

If the Rackmount Charger is connected towards PDM via both USB and Ethernet, the USB connection has higher priority.

Note:
Each Rackmount Charger needs an IP address.

See label for MAC address.

The Rackmount Charger is equipped with a combined reset button and embedded LED on the front.

Requirements

Computer:

- Windows XP® Professional including Service Pack 2 (SP2), Windows 7® Professional, Windows 7® Enterprise, or Windows 7® Ultimate.

- Sun Java Runtime Environment (JRE) version 6 or higher.
- USB port. USB 1.1 required, USB 2.0 supported.
- Ethernet port 10/100 Mbit/s.

Installation and configuration

Important:
Installation of the unit is NOT permitted in a hazardous area. The unit must be installed by an authorized person only.

Rackmount Charger installation

General

Note:
The unit shall be installed by authorized personnel only.

- The units shall be placed in a dry environment with a temperature range from +5° C to + 40° C (41° F to 104° F).
- The units shall be mounted on a vertical wall.
- Avoid mounting the Rackmount Charger in a sunlit place. This can affect the charging capacity.
- Avoid mounting the Rackmount Charger where radio/network coverage is not sufficient. This can reduce the messaging capacity.
- The unit shall be mounted on concrete or plaster walls only.
- If the Rackmount Charger is connected to a power supply via an AC wall plug, serial power supply connection is not allowed.
- If the Rackmount Charger is connected to a power supply via an AC wall plug, the socket-outlet shall be situated near the equipment and shall be easily accessible.
- If the Rackmount Charger is connected to a power supply via a fixed connection, a readily accessible disconnect device shall be incorporated in the building installation wiring.

Delivery includes:

- Rackmount Charger
- Power supply cord including IEC C14 connector (male)

- Inlet accessory kit including cable support holders and screws

Note:

An extension cord IEC C14 AC connector (female IEC60320-C13) to wall socket (IEC60320-C14) has to be ordered separately. It shall be connected between the pre-installed IEC C14 AC connector (male) and the wall socket.

Required Tools etc.

- Screwdrivers
- Cutting pliers
- Multimeter
- Screws and wall plugs for wall mounting. Make sure the screws and wall plugs have the correct length for the type of wall used. See example below:

Wall material	Plug length	Screw diameter
Single plasterboard	Thorsman TP1	3.5 – 5 mm
Double plasterboard	Thorsman TP2	3.5 – 5 mm
Concrete	Thorsman TP2	3.5 – 5 mm

Examples of ways to mount the Rackmount Chargers

Different ways to mount CR3 Rack Chargers is shown in figure 73 on page 303. It is possible to set up different combinations of CR3 Rack Chargers and Battery Pack Chargers. A maximum of four CR3 Rack Chargers (or Battery Pack Chargers) can be serially connected to the same LAN source.

Installation steps

The installation is done in three steps:

1. Wall mounting.
2. Electrical installation.
3. Communication cable connection.

Wall mounting

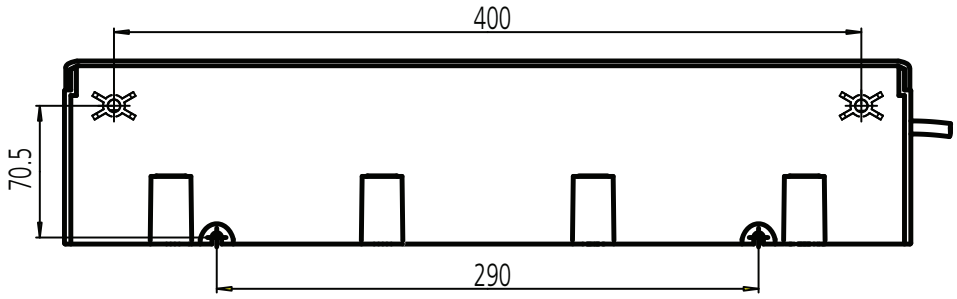
First, make an outline of how the Rackmount Chargers are to be placed.

Tip: If several Rackmount Chargers (or Multiple Battery Charger) are to be mounted close to each other, mount them so that there is enough space between them to be able to disconnect the telephones (vertical distance) and to be able to open the top cover (horizontal distance).

Tip: When you are planning the location of the modules, start to mount them in a height that makes it easy to reach the cordless telephones and to read the cordless telephones' display.

Measure and mark the drill holes by using the dimensions in figure 71. Drill and fasten the Rackmount Charger on the wall with four screws.

Figure 71: Mounting dimensions in mm



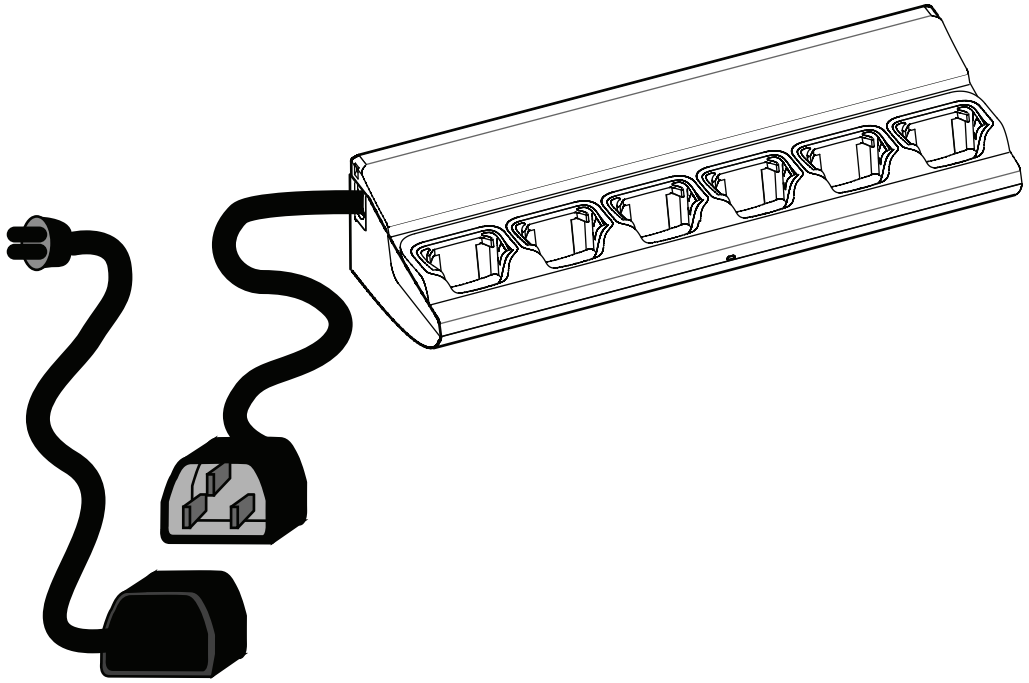
Rackmount Charger seen from the back

Electrical installation

Power supply by power cord to wall outlet

The Rackmount Charger is delivered with a cord with an IEC C14 connector (male). An extension cord IEC C13 AC connector (female, IEC60320-C13) to wall socket has to be ordered separately. It shall be connected between the pre-installed AC connector (male) and the wall socket.

Figure 72: CR3 with IEC C14 connector and an extension cord with an IEC C13 connector.



Proceed with the Communication cable connection when required.

Installation test

1. Connect the mains power supply cord to the wall socket.
2. The LED on the front of the charger shall now light up.

Power supply by fixed connection

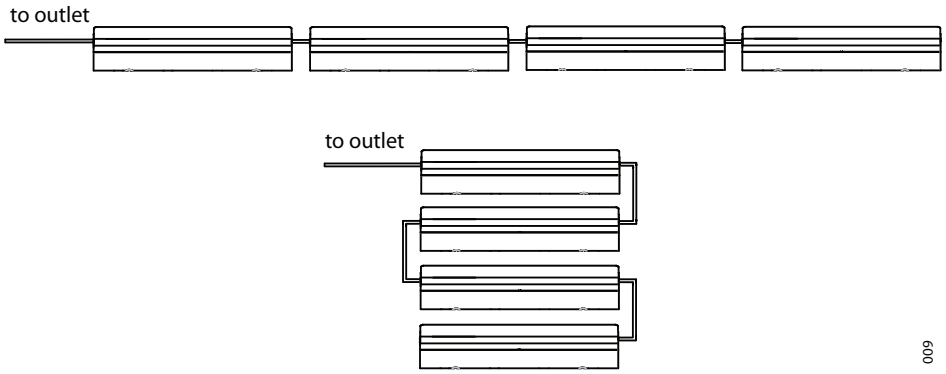
Note:

If the rack charger shall be connected with a fixed connection, the AC connection must be done by a authorized electrician.

Tip: It is possible to use any one of the two AC terminal blocks for AC input. Consequently, the unused terminal block may be used to connect the next rack charger or battery pack charger.

The Power Supply module connects to 100-240VAC/0.7A 50/60 Hz. When working with the units the mains power supply cable must always be disconnected. The safety covers must be mounted on top of the power supply terminal blocks to prevent hazardous situations, like electric chock.

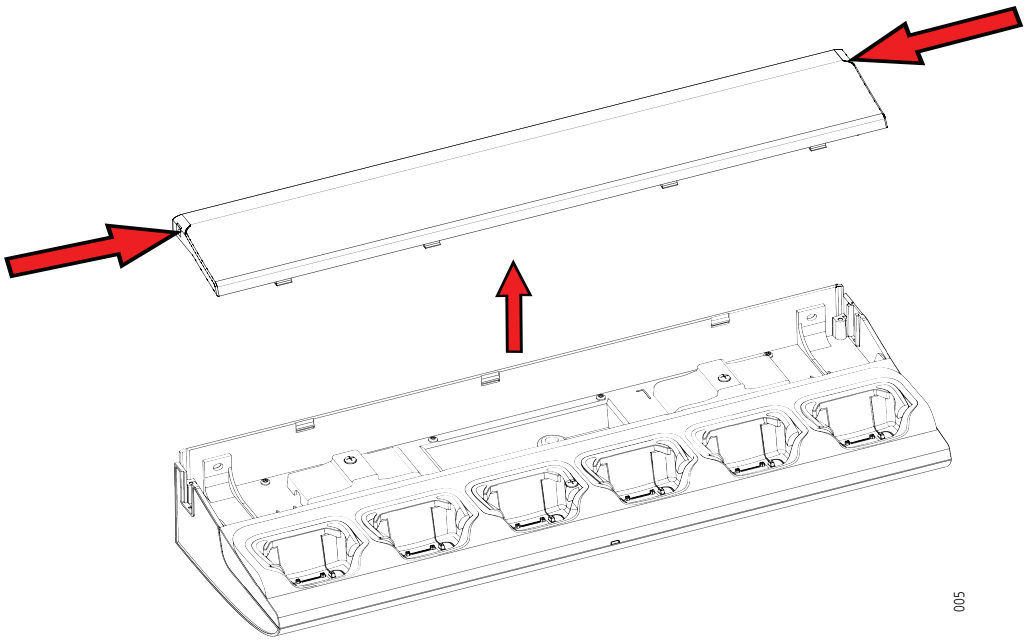
Figure 73: Examples of how Rackmount Chargers can be mounted and connected to a power source



Opening the top cover

1. Open the top cover by first pressing on the sides of the top cover, then lifting it upwards.

Figure 74: Opening the top cover of the Rackmount Charger



Fixed installation in detail

Fixed installation of the first charger or single unit with fixed electrical installation.

1. Remove the C14 connector from the power cord. Measure cut and strip the power cord to be connected to the disconnect device.

2. Connect the mains power supply cord to the disconnect device.

The IEC color code is used in the power cord supplied.

	Colors			
IEC	US	Old *	Load	Also called
Brown	Black	Red	Active	Line, Hot
Blue	White	Black	Neutral	Return, Cold, Grounded connector
Gr/Ye **	Green	Green	Earth	Ground, Safety Earth, Earth Ground, Grounding conductor ***

* The "Old" standard was used in various countries (including Australia), and some wiring may still use these colors.

** Gr/Ye - Green with Yellow stripe - this is the standard world wide, although it is not common in the US or Canada at present.

*** There is an important distinction between "Grounding conductor" (safety earth) and "Grounded conductor" (Neutral). These are *US* terms for the conductors and they are ***not*** interchangeable, despite the similarity of the names !

Installation of additional units in a serial power configuration

Note:
Maximum five units may be connected in power series.

Note:
Maximum four units may be connected in LAN series to one single LAN outlet.

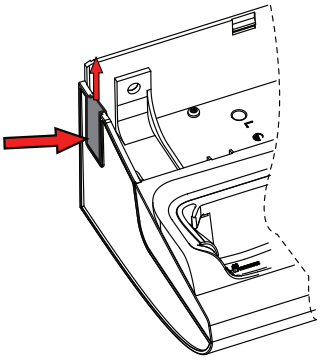
Important:
It is not allowed to connect additional Rack Chargers or Battery Pack chargers if the chargers are connected to the power supply via an AC plug.

Important:
Disconnect the power supply connection before working on the units.

1. If the additional Rack Charger has not yet been mounted on the wall, do this according to figure 73 on page 303.
2. Open the top cover of the rack charger closer to the AC power source.

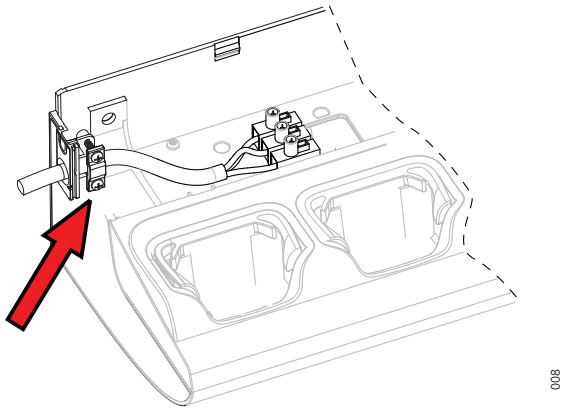
3. Remove the cover which protects the unused AC output terminal block of the charger closer to the AC power source.
4. Mount the cable support holder at the unused opening in the charger closer to the AC power source. The cable support holder is provided in the parts bag. See figure 75.

Figure 75: The rectangular cover that shall be removed and exchanged with a cable support holder with a mains power supply cord run through it



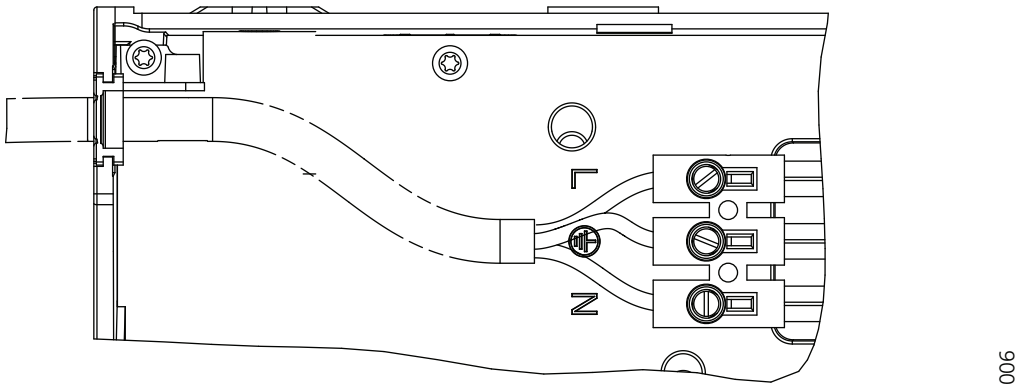
5. Remove the C14 connector from the additional charger. Cut and strip the mains power supply cord coming from the additional charger to the length required.
6. Run the power supply cord from the additional charger through the cable support holder of the previous charger, see figure 76

Figure 76: Securing the mains power supply cable



7. Connect the power supply cord from the additional charger to the unused terminal block in the charger closer to the AC power source. Note the embossed markings L, earth symbol and N, see figure 77.

Figure 77: The mains power supply connection



8. Mount the safety cover and fasten it with one screw.
9. Secure the mains power supply cable with two screws (2), which are provided in the parts bag, see figure 76.
10. Replace the top cover, see figure 74.
11. Fasten the power cord to the wall depending on local regulations.
12. If more rack chargers shall be connected, repeat the above steps 1-12 for the next unit.

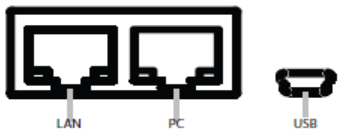
Installation test

1. When the fixed installation is completed, apply ,AC power by switching on the disconnect device.
2. The LED on the front of each charger shall now light up.

Communication cable connection

The communication cable connections are situated under the top cover of the Rackmount Charger.

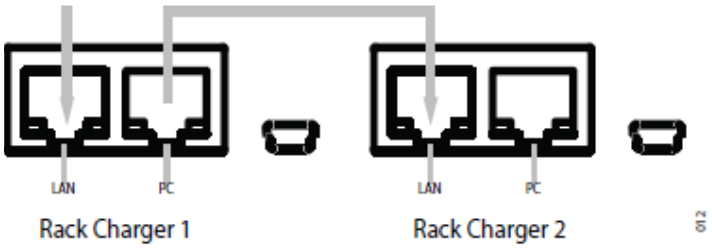
Figure 78: Communication connections inside the Rackmount Charger



Ethernet connections USB connection

When connecting several Rackmount Chargers over Ethernet, it is possible to connect them in series using the two Ethernet connections. Power over Ethernet is not supported.

Figure 79: Connecting Rack Chargers in series using Ethernet cables



1. Open the top cover, see figure 74 on page 303.
2. Connect the communication cable(s) to the connections shown in figure 78.
3. Let the communication cables run on top of the cable support holders, see figure 76 on page 305.
4. Close the top cover.

The USB Interface supports USB 2.0 Full speed. One Mini-B Receptacle USB connector is used. The USB connection is used for communication with a PC. Power over USB is not supported.

The USB connection is used for connecting the Rackmount Charger directly to a PC or to a LAN for the purpose of upgrading or configuring the Rackmount Charger itself or telephones placed in the charger.

Software installation

The charger software is pre-installed. Updates can be performed by using PDM or AIWS. For PDM details see Installing and operating the Portable Device Manager (WinPDM) on page 315, or for AIWS details see Upgrading a device with new software on page 433.

Rackmount Charger configuration

Each Rackmount Charger needs access to DHCP to receive an IP address automatically. If no DHCP is accessible it is possible to configure with PDM.

If the Rackmount Charger is configured to run DHCP, connect the network cable and the charger will automatically receive an IP address. If the charger is not configured to run DHCP the charger will use the setup IP addresses.

The following parameters exist for Rackmount Charger and can be changed via AIWS or PDM:

Parameter	Description
Ethernet Bit rate[1]	auto (default)

Ethernet connector[1]	auto (default)
Ethernet duplex[1]	auto (default)
DHCP Enabled	Yes (default), No
Charger IP address	192.168.0.101 (default)
Subnet mask	255.255.255.0 (default)
Default gateway IP address	192.168.0.1 (default)
DNS IP address	192.168.0.2 (default)
Charger IP port	12346 (default)
Service Discovery Enabled	Yes (default), No
Service Discovery Domain	Name of domain
DH IP address (one DH only)	192.168.0.3 (default)
DH IP port	10147 (default)

1. Currently only “auto” setting is available

Note:

It may be necessary to import the parameter definitions file that is included in the software package.
The package is provided by your supplier. The PDM/AIWS/AIWS2 used may differ from the version that is described here.

Follow these instructions to set Rackmount Charger parameters:

1. Check that the Rackmount Charger is connected to PDM/AIWS.
2. In PDM or the Device Manager in AIWS, click on the **Numbers** tab.
3. Select the Rackmount Charger device that you want to change parameters for.
4. In the **Number** menu, click **Edit.**. The **Edit parameters** window opens.
5. Edit the parameters you want to edit.
6. Click **OK**.

Rackmount Charger does not appear in AIWS

If the Rackmount Charger does not appear in the AIWS Device Manager, the Service Discovery might not be working in the customers network setup.

In this case connect the Rackmount Charger to PDM and edit the following parameters:

- *Service Discovery Enabled:* No
- *DH IP address (one DH only)*: Enter AIWS IP-Address

Note:

Service Discovery might not work if the Rackmount Charger is not in the same subnet as the AIWS.

Commissioning

The commissioning includes the following:

- Installation test
- Charging
- Communication with Avaya In-Building Wireless Server (AIWS) or Portable Device Manager (PDM)

Installation test

For Installation test, see chapter Installation test on page 302 or 309.

Charging

To verify that the charging works, follow these instructions:

1. Check that the LED on the front of the charger(s) is lit.
2. Place a telephone in a charging slot. Start of charging may be indicated differently depending on telephone model.

Communication with AIWS or PDM

See figure 78 on page 306 to see the communication connections to the charger.

Follow these instructions to start PDM or AIWS:

If you are using AIWS:

1. Check that the Rackmount Charger is connected.
2. Open a web browser and enter the URL to access the AIWS/AIWS2.
3. Click on **Device Manager**. The **Device Manager** window appears.

4. Go to the **Devices** tab and verify that the Rackmount Charger is online (it may take up to 15 sec).

If you are using PDM:

1. Check that the Rackmount Charger is connected to your PC.
2. Start PDM.
3. Go to the **Devices** tab and verify that the Rackmount Charger is online.

For instructions on how to verify that the charger parameter setting works, and for further instructions, please see Installing and operating the Portable Device Manager (WinPDM) on page 315, or Devices on page 417.

Operation

Charger operation

When the charger is connected to external power supply, normal operation is done as follows:

Telephone charging

1. Connect the charger to the AC power supply.
2. Place a telephone in the charging slot to start charging.

Telephone disconnection

1. First, tilt the telephone forwards.
2. Then, lift the telephone upwards.

Note:
Do not try to lift the telephone upwards before tilting it forwards.

If the charger is connected to PDM/AIWS, the following operations can be done:

- Software upgrade of charger or handset
- Parameter settings of charger or handset

  See Installing and operating the Portable Device Manager (WinPDM) on page 315, or Devices on page 417, for details.
- Easy Replacement of handset
- Phonebook upload (handset)

- Language upload (handset)

  The Rackmount Charger supports the Easy Replacement feature. See Configuring Avaya DECT phones on page 203 for details.

Refer the respective User Manual for more information on updating the telephones.

LED indications

The charger is equipped with a status LED. The following indications are used:

LED indication	Description
Green, fixed	Logged on to PDM/AIWS/AIWS2.
Orange, fixed	Not logged on to PDM/AIWS/AIWS2.
Orange, flashing (1000 ms on, 1000 ms off)	1. Software download. 2. File transfer during Easy Replacement
Orange, flashing (100 ms on, 800 ms off)	"Change phone" indication during Easy Replacement.
Red, fixed	Software error. Service needed.
Red, flashing (100 ms on, 800 ms off)	Error indication during Easy Replacement. Put back old portable in charger. Charger returns to “Not logged in to PDM/ AIWS/AIWS2” mode when portable is removed.
Red, flashing (3 long flashes, 800 ms on, 100 ms off)	Parameter error in user parameters. Charger performs a factory reset and restarts.
Red, flashing (800 ms on, 100 ms off)	1) Parameter error in production parameters. Service needed for charger. 2) Error during Easy Replacement. Service needed for both portables.

LED indications are also described in troubleshooting Rackmount Charger on page 689.

The reset button is used to reset the Rackmount Charger.

Maintenance

Software upgrade

The charger software is pre-installed. Updates can be performed by using PDM or AIWS. For PDM details see Installing and operating the Portable Device Manager (WinPDM) on page 315, or for AIWS details see Upgrading a device with new software on page 433.

Administration

Data backup

N/A

Troubleshooting

See Troubleshooting on page 675

Installing and operating the Portable Device Manager (WinPDM)

Introduction

The WinPDM provides a generic application for managing Cordless Telephones, Advanced Chargers and Rackmount Chargers on one or more sites.

The WinPDM makes it possible to edit parameters, update software in the devices and upload files. It can save parameters and software for individual sites in a database.

This chapter is intended as a guide for installation, maintenance and troubleshooting purposes and is relevant for:

- Installation and parameter setup.
- Device administration and WinPDM daily use.
  Handles devices on own site only.

The WinPDM provides a generic application for managing all devices (e.g. handsets and chargers) on one or more sites. The WinPDM makes it possible to edit parameters, update software in the devices and upload files. It can save parameters and software for individual sites in a database.

How to use this chapter

For a basic description on how to work with WinPDM, see Introduction on page 315.

Installation and configuration

These tasks are intended for installation and configuration.

In order to simplify, for example an installation on a site, use the following steps.

1. Install the PDM on your computer, see Software installation on page 320.
2. Open and configure the PDM, see Software configuration on page 320.
3. Create a template with settings common for all devices of a certain device type at the site, see Create a Parameter Template on page 344.

During system setup it is likely that the personnel doing the installation and configuration continues with the Administration tasks below to make the system fully functioning.

Administration

These tasks are intended for administration. This is the recommended order.

1. Create new Numbers, see Create New Numbers on page 336, and run the template on the Number(s), see Apply Template to set Parameter Values on page 338.
2. Make individual settings for each Number. See Edit Parameters on page 337.
3. If applicable, switch on the devices.
4. Connect the devices, one after the other, and associate them with the Numbers. Different devices have different ways of connecting. See Associate a Number with a Device on page 338.

Note:

The very first time a device is connected to the USB port, the **Found New Hardware** wizard displays (not for all computers). Do the following: Select **No, not this time** and click **Next** (twice).

More tasks are described in this document, such as how to import different types of files.

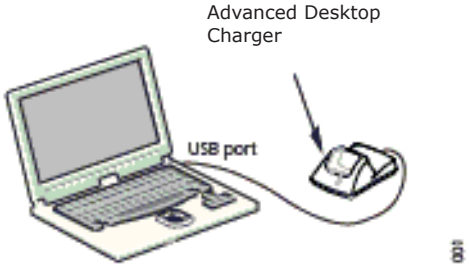
Technical solution

The WinPDM software is installed on a PC running Windows XP® or Windows 7® (32-bit or 64-bit). The charger is then connected to the PC running the PDM software through the USB port. The COM port is also supported by PDM but currently no Avaya device.

Note:

Only one charger at a time can be connected to PDM. A Rackmount Charger can hold one or more cordless telephones though.

Figure 80: Charger connection to the PDM



Parameters can be edited for a single device and then sent to the device, but if many devices are to be updated with new parameter settings it is also possible to create a parameter template and run the template on each Number.

Parameters can be uploaded from a connected device, edited and sent to the device again. If the PDM shall store parameter settings in the site database or not, is selectable.

When editing parameters there are help texts to assist in writing the correct parameter format.

Devices can be upgraded with new software. A text and a status bar indicates that the connected device is being updated with the new software.

Requirements

See the Data Sheet for WinPDM.

WinPDM description

WinPDM terminology

This section gives a brief description of the basic terminology in WinPDM.

Contacts	The name of the phonebook in a handset.
CSV file	Comma Separated Value: A file with data, where values in each row are separated by a delimiter, which can be a comma, a semicolon or a tab.
Device	can be a charger, a desktop programmer or a handset that can be connected to WinPDM.
GUI	Graphical User Interface.
JRE	Sun Java Runtime Environment
Language file	Language file for handset or WinPDM.
Number	Settings for the complete set of parameters of a single device, tied to a specific identity.
Template	general settings for a specific device type. A template can be applied to several Numbers of the same device type
Parameter definition file	a file including all possible settings for a certain device type. Templates are created from parameter definition files.
Package file	a file that can contain other files, such as parameter definition files, software files and template files.

PDM usage

This section gives a short description to give a basic understanding on how to use the WinPDM with devices. This description is intended to be used to get a basic understanding of the work flow and is not intended to be followed in work.

- Import a parameter definition file of the corresponding device type to WinPDM.
- Create a template from the parameter definition file.
- Add a device to WinPDM.

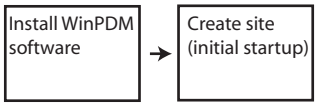
- Create a new Number for the corresponding device type.
- Associate the Number with the device.

Refer to the following chapters, mainly chapters Operation on page 328 and Administration on page 353, for a detailed description.

Installation and configuration

This section describes the basic settings required to getting started with the WinPDM. The basic settings and the sequence in which they should be completed are illustrated in figure 6.

Figure 6. Basic settings



Software installation

This section describes the installation procedure when installing from a CD.

Note:
Do not connect the hardware to the computer before installation.

1. Locate the software provided by your supplier.
2. Double-click on the **Setup.exe** file located in the **Avaya WinPDM x.x.x** folder, where x.x.x represents the software version of WinPDM.
3. Follow the instructions given by the Setup Wizard.

If an older version of WinPDM is installed, the setup wizard will uninstall the older version before installing the newer WinPDM version.

Software configuration

This chapter includes settings for:

- Initial startup
- Site setup
- Definition files
- Language

Initial startup

In the **Start** menu, select **All Programs > Avaya WinPDM > Avaya WinPDM**.

Note:

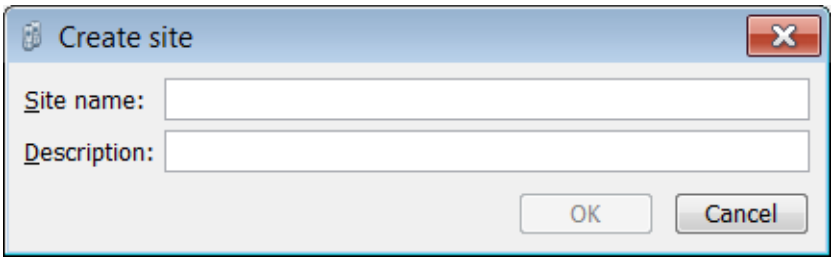
Windows Firewall may alert you of “PMServer” etc. You can ignore these security alerts, it will not affect the WinPDM, but then the alerts will appear every time the WinPDM is started. A better way is to select Continue blocking or Unblock.

Note:

The very first time the WinPDM is started, a Create site window appears.

The first time PDM is started, the **Create site** dialogue opens.

Figure 7. The Create site window.



1. In the **Site name** field, enter a site name.
2. In the **Description** field, enter a description of the site (optional).
3. Click the **OK** button.

Note:

Additional sites can also be created. See Site Management on page 334.

Initial Configuration of Devices

This section applies to new devices that shall be configured the very first time. The devices are delivered with factory settings from the manufacturer. The initial settings and the sequence in which they should be completed are illustrated in figure 8.

Figure 8. Initial configuration of devices



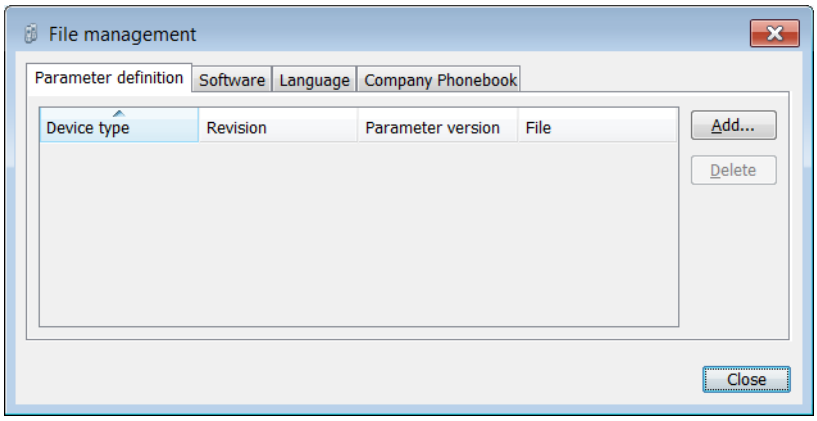
Import Package Files

The package files (.pkg) for your devices are distributed by your supplier. The package file includes the following:

- A software file (.bin) used for upgrading the device
- A parameter definition file (.def) including the parameters that can be configured in the device.
- Templates might also be included. The templates can for example include parameter settings for different exchange system.

NOTE: It is recommended to import the latest released package files for your devices.

1. From the **File** menu, select **File management**.

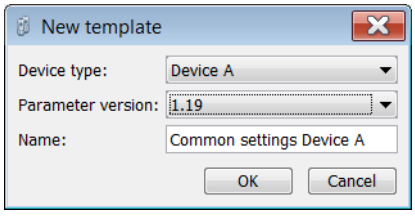


2. Click the **Parameter definition** tab and then click the **Add** button.
3. Select the package file (.pkg) to be imported and click the **Open** button.

Create Template with Common Settings

This section describes how to create a template including common settings that can be applied to the device's numbers later on.

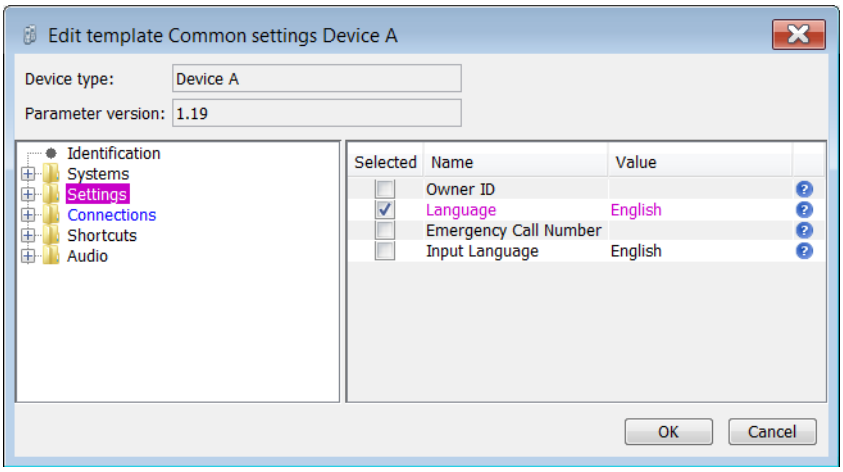
1. Click the **Templates** tab.
2. From the **Template** menu, select **New**.



- Select which device type the template should be applicable for
- Select which parameter version the template should be based on. The parameter version determines which parameter settings that are available for your device type. It is recommended to select the latest parameter version to obtain full compatibly with the device.
- Enter an appropriate name of the template

3. Click the **OK** button.
4. The **Edit template** dialog window opens showing parameters organized in a tree structure in the left pane, with the parameters in the current node in the right pane. Clicking the icon will give a short description of selected parameter. In addition, see also the manual for the device for more information about the parameter.

Select the parameters to be saved in the template by selecting the check box to the left o each parameter. Change the parameters to the desired values.



In the **Edit template** window, the following color coding is used:

Color	Description
Black	Normal
Dark blue	Parameter has been edited during the current session
Purple	The parameter is included in the template (checked)

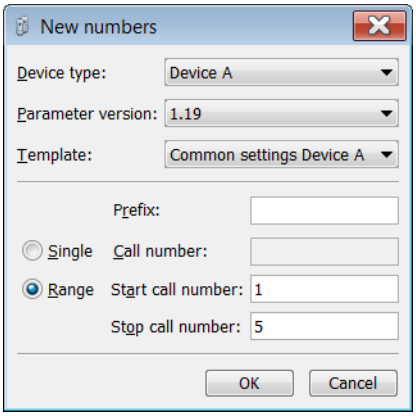
Red	Value not valid
Turquoise	The value differs from the default value

5. When all needed parameters have been configured, click the **OK** button to save the settings.

Create Numbers and Apply Template

This section describes how to create numbers to be associated with the devices later on. In addition, the common settings will also be applied to the numbers through the template you created earlier.

1. Click the **Numbers** tab.
2. From the **Number** menu, select **New**.



3. In the **Device type** drop-down list, select which device type the number(s) is created for.
4. In the **Parameter version** drop-down list, select the same parameter version used when you created the template for your device type.
5. In the **Template** drop-down list, select which template to be applied to the number(s).
6. In the **Prefix** field, enter the prefix (if needed) to be added to the number(s).
7. Select one of the following options:
   - To create a single number, select the **Single** option and enter the number.

Note:

To create a range of numbers, select the **Range** option. Enter the start number and end number.
NOTE: The maximum range that can be added at a time is 100 numbers.

8. Click the **OK** button.

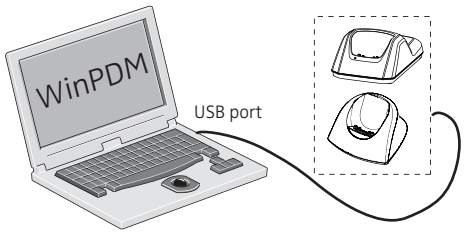
Connect Device to Computer

This section describes how to connect the devices to the computer running WinPDM.

The device is connected to the computer running the WinPDM via the USB port. The device must be set up to handle this connection according to the instructions in the manual for the device.

Example of connected devices are shown in figure 9.

Figure 9. Connection to the computer running WinPDM

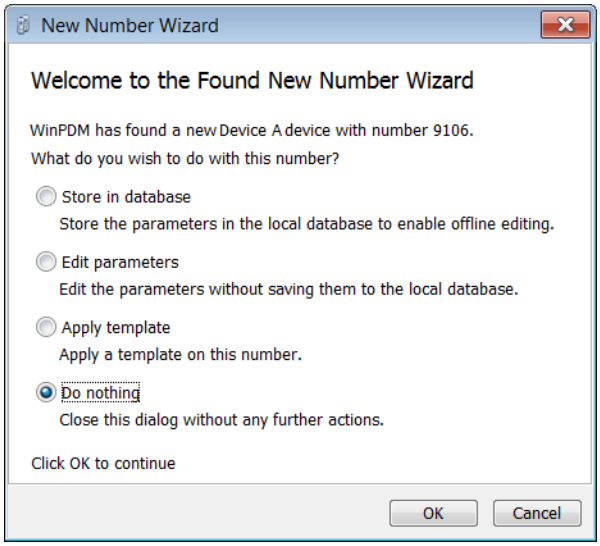


Depending on connected device, a **Device Wizard** window or a **New Number Wizard** window might be shown. In this case, click the **Do nothing** option and then click the **OK** button.

Figure 10. The Device wizard



Figure 11. The New Number wizard

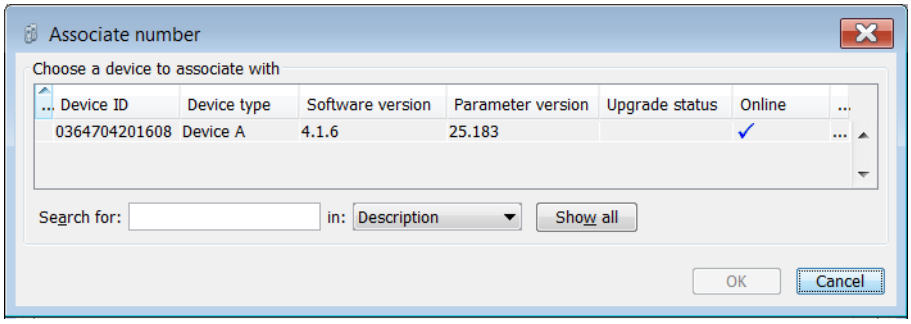


The device should now appear as online in WinPDM indicated by ✓ in the **Online** column.

Associate Number with Device

This section describes how to configure the connected device with the number you created earlier and also to apply the common settings for the device.

1. Click the **Numbers** tab.
2. Select the device to be associated with a number.
3. From the **Numbers** menu, select **Associate with device**.



4. Select the device to be configured with the selected number.
5. Click the **OK** button.

Note:

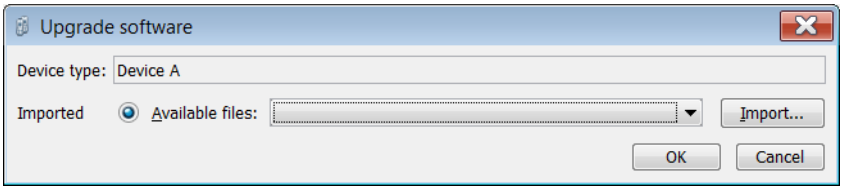
If you cannot find your device in the list, the device is not compatible with the parameter version used when you created the number. In this case, the device's software must first be updated and then you can associate the number with the device.

Upgrade a Device with New Software

This section describes how to upgrade the software in a device. To be able to associate a number with a device later on, the device's parameter version must be compatible with the number's parameter version. The compatible parameter version is applied to the device when upgrading the device's software.

Additionally, newer software versions might be available since the device was delivered from the manufacturer, and it is therefore recommended to upgrade the device with the latest released software version.

1. Click the **Devices** tab.
2. Select the device to be upgraded.
3. Form the **Device** menu, select **Upgrade software**.
4. In the **Available files** drop-down list, select the software to be uploaded.



5. Click the **OK** button.

The software will be downloaded to the device. A progress bar in the **Status** column for the device shows the progress of the download.

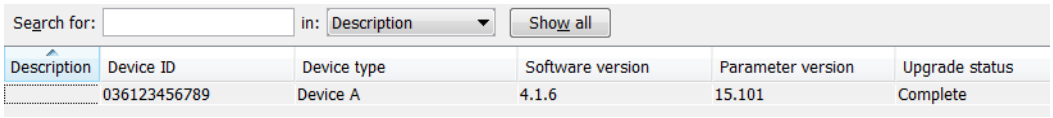
Note:

To cancel the upgrade, right-click the device in the list and select **Cancel current upload**.

The device will restart automatically after a successful download.

6. When the device has been upgraded; the upgrade status shows Complete, the new software version, and the new parameter version for the device are also shown.

Figure 12. Example of completed software upgrade



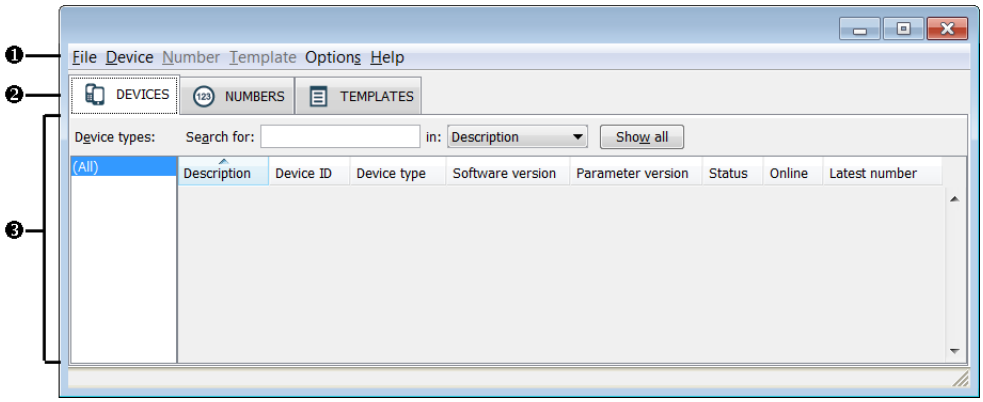
Operation

The WinPDM GUI

WinPDM Window

The WinPDM window has a menu bar (1), three tabs (2) and a work area (3). When a tab is selected the available device types will be shown in the left hand pane of the work area. The right pane of the work area shows devices, numbers, and templates already configured.

Figure 13. WinPDM overview



Search Field

In the upper part of the Work area there are search fields where different search criteria can be selected depending on which tab that is displayed. The search field is color coded green or red depending on if there are possible matches to the search criteria or not.

Sort the List

By default the lists are sorted by the first column. To sort the list by any other column, click the column heading. To reverse the sort order, click the column heading again. The sort order is indicated by an up or down arrow in the column heading.

Filter the List

By default the list in each tab shows all available Devices, Numbers or Templates. It is possible to filter the list by selecting a device type in left pane.

Color coding

General color coding

- If the version number is shown in red, WinPDM has found no parameter definition files supporting that device type.
- If the version number is shown in dark red, the parameter definition file is compatible, but does not have exactly the same version as the device.
- If the Number is shown in dark red, the WinPDM warns that the parameter settings will be applied to a particular device (its hardware) instead of a particular user id/number. This occurs when the extension number has been manually changed in the handset via its Login menu.

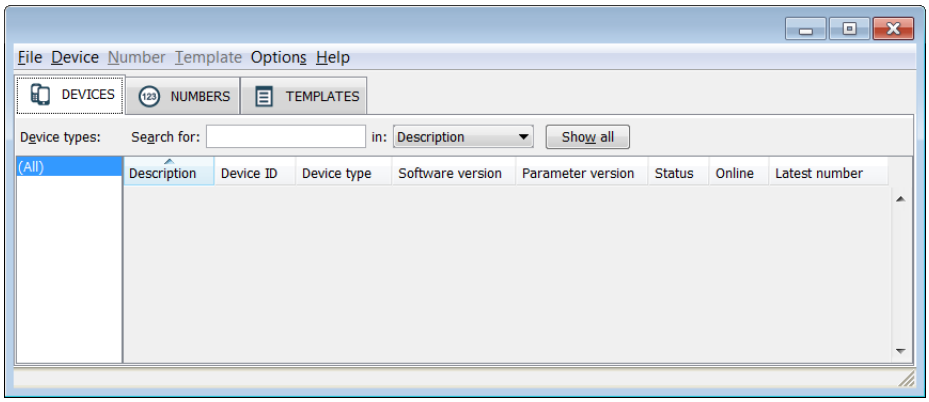
Color coding for parameter and template editing

In the parameter and template editing window, the following color coding is used:

Color	Context	Description
Black	General	Normal
Dark blue	For templates and parameter editing	Parameter has been edited during the current session
Purple	For templates	The parameter is included in the template (checked)
Red	For templates and parameter editing	Value not valid
Turquoise	For templates and parameter editing	The value differs from the default value

Tabs

Devices Tab



The view shows all devices configured at the site in a detailed list. The following information can be displayed:

- Description – optional information of a device that can be added by the WinPDM user. For example, the user of the device.
- Device ID – the unique identifier of the device.
- Device type – the device model.
- Software version – the version of the software in the device.
- Parameter version – the version of the parameters in the Number
- Status – might show one of the following symbols:

  – new software upgrade is in progress (a green arrow).
  It is also possible to see a progress bar when the device is being upgraded.

  – software upgrade Pending, Request sent, or Accepted.

  – Retrying

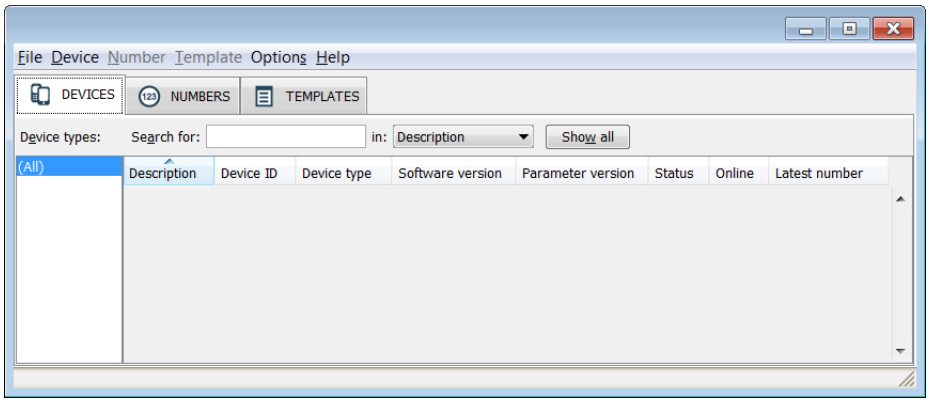
  – the last upgrade Failed or Aborted (a red broken arrow).

- Online – shows if the device is connected to the computer running WinPDM. When connecting a device to the WinPDM, it might take a while before the device goes online. The ✓ symbol indicates a device that has become connected/online.
- Latest number - shows the latest known Number for a device.

Numbers Tab

Figure 14. The Numbers tab

The view shows all Numbers configured at the site in a detailed list.

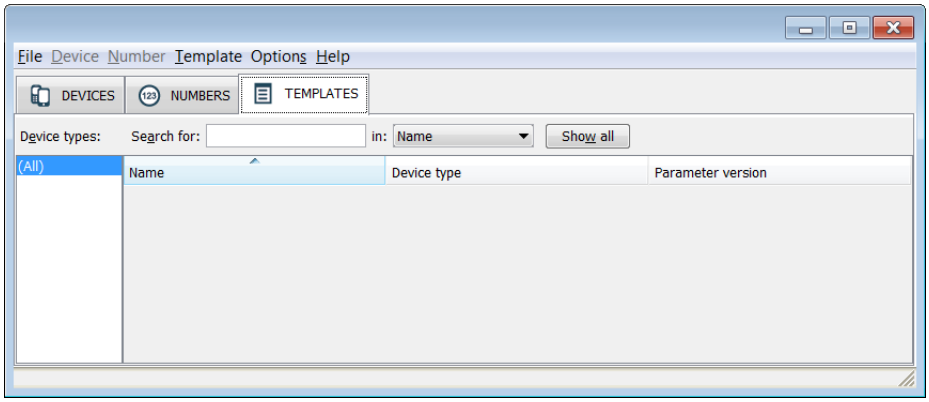


- The following information can be displayed:
- Description – optional information of a device that can be added by the WinPDM user. For example, the user of the number.
- Number – the unique identifier of the Number. The identifier is unique for that device type.
- Device type – the device model the Number is intended for.
- Parameter version – shows the version of the parameters in the Number.
- Device ID – the unique identifier of the device that the Number is associated to.
- Online – shows if the device the Number is uploaded to is connected to the computer running WinPDM. It might take a while before a connected device goes online in the WinPDM. The ✓ symbol indicates a device that is online/connected.
- Status – shows the parameter synchronization status. A Number can also be queued for synchronization. Several different indications are used, for example Synchronizing, Synchronized, etc. When the Number is offline, the status Synchronized or Not synched is shown.
- Saved – shows if the Number's parameters have been stored in the database. The ✓ symbol indicates that the parameters have been stored.
- Last login – shows the latest date and time the device was online in WinPDM/logged in to WinPDM.
- Last run template - indicates which template that was last run for that Number.

Templates Tab

The view shows all templates configured at the site in a detailed list. The following information can be displayed:

Figure 15. The Templates tab



- Name – the name of the template.
- Device type – the device model.
- Parameter version – shows the parameter version.

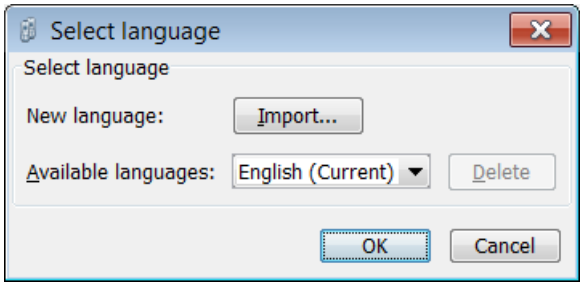
Language Settings for WinPDM GUI

It is possible to select the language to be used in the menus in WinPDM by importing a language file with the file extension *.xml.

The default language is english, and stored as a default translations file in your installation directory at installation:

C:\Program Files\Avaya\WinPDM\Client\default-translations.xml

This file can be copied and edited to create a new language and can then be imported as described below.

1. From the **Options** menu, select **Select language**.
2. 

3. Click the **Import** button.
4. Select the language file (.xml) to be imported and click the **Open** button.
5. In the **Available languages** drop-down list, select which language to use.
6. Click the **OK** button.

Tip:
For adding a new language to a device, see Import Language Files for Devices on page 350 and Delete Imported Files for Devices on page 351.

The Device Wizard

When a device without a number is connected to the WinPDM, the **Device Wizard** window appears.

Figure 16. The Found Device Wizard window.



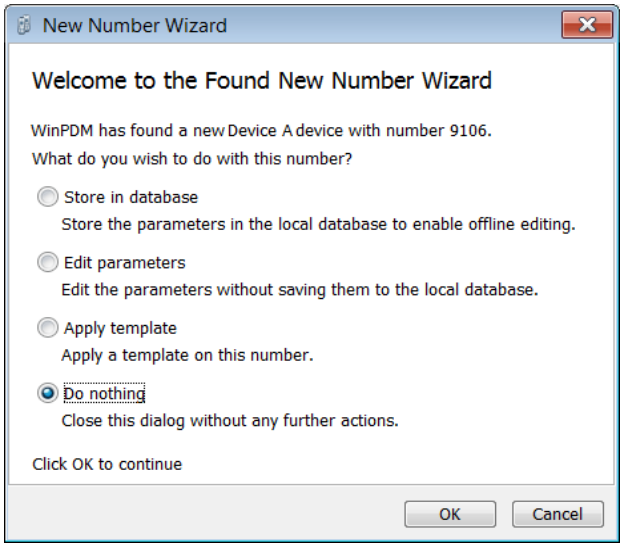
There are four choices in the wizard:

- Associate with number, see Associate a Number with a Device on page 338.
- Edit parameters, see also Edit Parameters on page 337.
- Apply template, see also Apply Template to set Parameter Values on page 338.
- Do nothing

The New Number Wizard

When a new device with an unsaved Number is connected, the **New Number Wizard** window appears.

Figure 17. The New Number Wizard window.



There are four choices in the wizard:

- Store in database
- Edit parameters, see also Edit Parameters on page 337.
- Apply template, see also Apply Template to set Parameter Values on page 338.
- Do nothing

Open the WinPDM

- From **Windows Start** menu, select **All Programs** > **Avaya WinPDM** > **Avaya WinPDM**.

The view of the last used Site opens. To open another site, see Open Site on page 335.

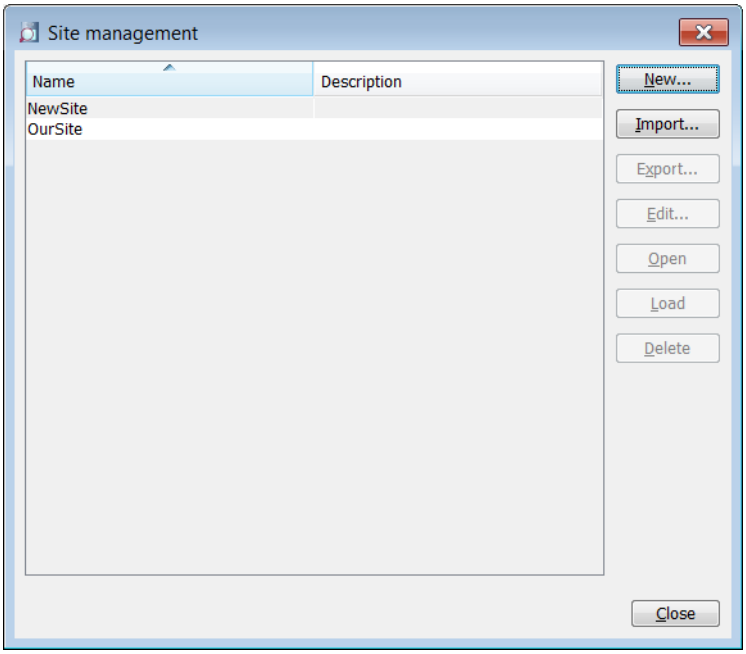
Site Management

By creating a Site for each customer installation, devices and software can be managed for that site. The settings are saved in a database.

Note:

There is a subtle but important difference between loading and opening a site. When a site is opened, the **Site management** dialog closes and it is possible to start working with the devices in the site. When a site is loaded, the **Site management** dialog stays open, making it possible to continue with site management tasks, such as creating and deleting sites.

Figure 18. The Site management window



Create New Site

1. From the **File** menu, select **Site management**.
2. Click the **New** button.
3. Enter a name for the site and a description (optional) and click the **OK** button.

Open Site

1. From the **File** menu, select **Site management**.
2. Select the site to be opened and click “Open”.

Load Site

1. From the **File** menu, select **Site management**.

2. Select the site to be loaded.
3. Click the **Load** button. The view in the main window changes to the newly opened site.

Delete Site

1. From the **File** menu, select **Site management**.
2. Make sure that the site to be deleted is not currently active. If it is active, load another site (see *Load Site*).
3. NOTE: If there is only one site remaining, it cannot be deleted.
4. Select the site to be deleted and click the **Delete** button.
5. Click the **Yes** button to confirm the deletion.

Import Site

When importing a site, numbers with parameters and devices are imported. Templates, software and definition files are not imported.

1. From the **File** menu, select **Site management**.
2. Click the **Import** button.
3. Select the Site file (.ste) to be imported and then click the **Open** button.
4. In the **Input** dialog, enter a name for the site and click the **OK** button.

Export Site

1. From the **File** menu, select **Site management**.
2. Select the site to be exported and click the **Export** button.
3. Select the location where the exported file should be saved.
4. Enter a file name of the site (.ste) and then click the **Save** button.

Numbers

Create New Numbers

1. Click the **Numbers** tab.
2. From the **Number** menu, select **New**.
3. In the **Device** type drop-down list, select device type.

4. In the **Parameter version** drop-down list, select the parameter version.
5. In the **Template** drop-down list, select which template to apply to the Number. This is optional and therefore “None” can be selected.
6. In the **Prefix** field, enter the Number’s prefix (if needed).
7. Select one of the following options:
   - To create a single Number, select the **Single** option and enter the call number.

   Note:
   To create a range of Numbers, select the **Range** option. Enter the start call number, end call number.

   NOTE: The maximum range that can be added at a time is 100 Numbers.
8. Click the **OK** button.

Save a Number to Database

The number of an online device can be saved to the database.

1. Click the **Numbers** tab.
2. Select the device which number to be saved.
3. From the **Number** menu, select **Save**.

Enter/Edit Description of a Number

It is possible to enter information of a Number using WinPDM. For example, the description can be used to describe a user of a number.

1. Click the **Numbers** tab.
2. Select the number which description to be edited.
3. From the **Number** menu, select **Enter description**.
4. Enter an appropriate description and then click the **OK** button.

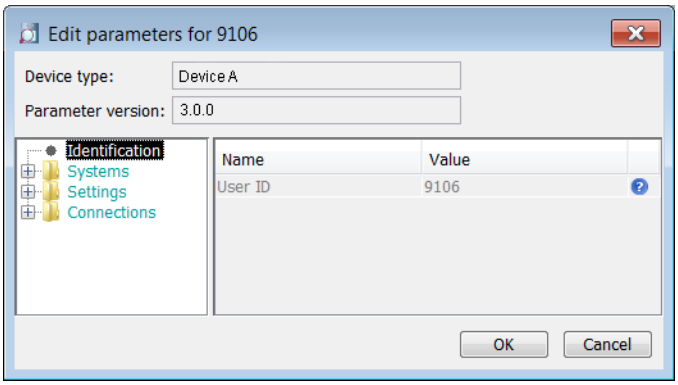
Edit Parameters

The **Edit Parameters** window shows the set of parameters for the Device/Number. The parameters are organized in a tree structure in the left pane, with the parameters in the current node in the right pane. Clicking the icon will give a short description of selected parameter.

Note:
If Edit parameters was selected in the Device Wizard window, or in the New Number Wizard window, continue from step 4.

1. Click the **Numbers** tab.

2. Select the device which parameters to be edited.
3. From the **Number** menu, select **Edit**.



4. In the left pane, select the parameters to be edited.
5. In the **Value** column, make your changes.

When a parameter has been edited, the node in the left pane changes to a blue color.

6. Click the **OK** button to save the changes, or click the **Cancel** button to undo all parameter changes. When saving the changes, the parameters are automatically sent to the device when it is online in WinPDM.

Apply Template to set Parameter Values

If a template has been created for a device type, it can be used to set the parameter values for a range of devices, or a single device.

Note:

If Apply template was selected in the Device Wizard dialog window, or in the New Number Wizard dialog window, continue from step 4.

1. Click the **Numbers** tab.
2. Select the device(s) you want to apply the template on.
3. From the **Number** menu, select **Apply template**.
4. Select the template to be used and click the **OK** button.

Associate a Number with a Device

Before being able to synchronize parameters between WinPDM and devices, it is necessary to associate a Number with a device. It is possible to enter several Device IDs in advance and to associate them with a Number at a later moment.

Note:

If Associate with number was selected in the Device Wizard window, continue from step 3.

1. Click the **Numbers** tab.
2. Select the number you want to associate with a device.
3. From the **Number** menu, select **Associate with device**.
4. Select the device you want to associate with in the list and click the **OK** button.

If the selected device is online, it will immediately be updated with the selected Number. If the selected device is not online, it will be updated the next time it is online.

It is possible to associate several Numbers with several devices simultaneously.

Delete a Number in the Site Database

1. Click the **Numbers** tab.
2. Select the device which number you want to delete.
3. From the **Number** menu, select **Delete**.
4. In the **Delete Numbers** window, click the **Yes** button.

Note:

If a device that is online is deleted, it will stay in the list as online but not saved.

Rename a Number

Note:

It is not possible to rename a number that is shown in dark red since the parameter settings no longer will be applied to the number. Instead, the parameter settings will be applied to a particular device using its IPDI. This occurs when the extension number has been manually changed in the handset via its Login menu.

1. Click the **Numbers** tab.
2. Select the device which Number you want to rename.
3. From the **Number** menu, select **Rename**.
4. In the **Rename number** window, enter a new prefix (optional) and a new Number and click the **OK** button.

Copy a Number

1. Click the **Numbers** tab.
2. Select the device which Number you want to copy.

3. From the **Number** menu, select **Copy**.
4. In the **Copy number** window, enter a new prefix (optional) and a new Number and click the **OK** button.

Import Contacts

Note:

The number for the device must be saved, see Save a Number to Database on page 337.

Import Contacts From File

A file containing contacts can be imported to WinPDM and synchronized with a device. This can for example be useful when you want to transfer contacts from legacy devices to newer devices.

When importing the file, the device's contacts (if any) are overwritten by the contacts in the file. Additionally, the import works only if the device can store all contacts included in the file. For example; if the file contains 100 contacts, the device must have support for storing at least 100 contacts.

If needed, the number of contacts in the file can be changed by using Excel or other compatible application.

1. Click the **Numbers** tab.
2. Select the number which the contacts should be imported to.
3. From the **Number** menu, select **Import contacts** > **From file**.
4. Select file containing contacts (.txt, .csv, or .skv). Click the **Open** button.

The contacts in the imported file are synchronized with the device.

Import Contacts From Number

You can make a copy of a device's contact list and paste it to another device's contact list directly. This means that the contact list do not need to be saved on for example your computer.

Note:

The import works only if the receiving device can store the entire contact list of the device you are importing from. For example; if the contact list contains 100 contacts, the receiving device must have support for storing at least 100 contacts. Additionally, the Company phonebook contacts included in the contact list are not transferred to the other device using this feature.

1. Click the **Numbers** tab.
2. Select the number which the contacts should be imported to.
3. From the **Number** menu, select **Import contacts** > **From number**.
4. Select the number which contacts to be copied.

5. Click the **OK** button.

The contacts are now imported to the handset.

Export Contacts

You can make a copy of a device's contact list that can be used as backup (.csv). The contact list can also be imported to another supporting device later on (seeImport Contacts From File on page 340).

1. Click the **Numbers** tab.
2. Select the device which contacts to be exported.
3. From the **Number** menu, select **Export contacts**.
4. Enter a descriptive file name and click the **Save** button.

Devices

All work with devices is performed from the **Devices** tab.

- Devices can be added to a site by connecting the device to the computer.
- It is possible to transfer the information for a device to another device.
- Devices can be reset to factory settings.
- Devices can be updated with new software.

Add Devices to a Site

Before connecting a device to the WinPDM, make sure the connection is set up according to the instructions in the device's manual (for example, Installation Guide or Configuration Manual).

If a range of new devices are to be added to a site, the easiest way is to:

1. Create a template with all common parameter settings for the site. See Create a Parameter Template on page 344.
2. Add a range of Numbers and run the template. See Create New Numbers on page 336 and Apply Template to set Parameter Values on page 338.
3. Edit the parameters and change individual settings. See Edit Parameters on page 337.
4. Connect the physical devices, one after the other, and associate them with the Numbers in the site database. See Associate a Number with a Device on page 338.

A single device can be added in the same way.

Synchronize a Device

When a device is connected, it is synchronized with the associated Number in the WinPDM.

When a device is being synchronized, parameters that have been changed in the device are uploaded to the WinPDM, and parameters that have been changed in the WinPDM are sent to the device. If a parameter has been changed in both the device and the WinPDM, the setting made in the WinPDM will take precedence.

1. Click the **Numbers** tab.
2. Connect a device to the computer running the WinPDM. If the Number is saved, and it has a parameter definition, the device is automatically synchronized.

Delete a Device in the Site Database

1. Click the **Devices** tab.
2. Select the device to be deleted.
3. From the **Device** menu, select **Delete**.
4. In the **Delete Device** window, click the **Yes** button.

Note:
It is not possible to delete a device that is online in WinPDM.

Replace a Device

If a device should be replaced with a new one, it is possible to transfer its associated Number to a new device. The new device must be of the same device type as the old one.

1. If the device to be replaced is still working, make sure that it is synchronized.
2. Connect the new device to the WinPDM.

Associate the new device to the Number associated to the old device as follows:

3. Click the **Numbers** tab.
4. From the **Number** menu, select **Associate with device**.
5. Select the device you want to associate with in the list and then click the **OK** button. The Number is no longer associated to the old device.

Create New Device

It is possible to enter several new Device IDs in advance into WinPDM for later association.

In order to simplify input when handling many devices, it is possible to use a bar code reader. The bar code reader should send a carriage return after each item, but it is not necessary. If carriage return is not sent, it is necessary to click **Create** after each read item.

1. Click the **Devices** tab.
2. From the **Device** menu, select **Add device**.
3. Select device type and parameter version.
4. Enter a Device ID for the device, manually or by using a bar code reader.
5. The **Continuous registration** check box can be used to select whether the **Create devices** dialog shall close after clicking **Create** or if it shall still be open.
6. Click the **Create** button.
7. Repeat 4 to 6 if more devices are to be created.

Assign a Number

It is possible to assign a Number to a device that has not yet been assigned a Number in WinPDM.

Note:
Assign should not be done on a device that already has a Number.

1. Click the **Devices** tab.
2. Select the device that should be assigned a Number.
3. From the **Devices** menu, select **Assign number**.
4. In the **Assign number to device** window, enter a new prefix (optional) and a new Number
5. Click the **OK** button.

Enter/Edit Description of a Device

1. It is possible to enter information of a device using WinPDM. For example, the description can be used to describe a location of a device.
2. Click the **Devices** tab.
3. Select the device which to edit the description for.
4. From the **Device** menu, select **Enter description**.
5. Enter an appropriate description and click the **OK** button to save the setting.

Factory Reset

Factory reset means that the device parameters will be set to factory default settings. The Number in the database that is associated with the device will not be affected.

Note:
The device must be online.

1. Click the **Devices** tab.
2. Select device(s) to be reset.
3. From the **Device** menu, select **Factory reset**.
4. Click the **Yes** button.

Device Properties

To get a summary of the properties of a device:

1. Click the **Devices** tab.
2. Select the device which properties you want to show.
3. From the **Device** menu, select **Properties**.

The following information is displayed:

- Description of the device (if entered by the WinPDM user)
- Device ID
- Device type
- Parameter version
- Software version
- Last known number
- Online status
- File upload information

Templates

Templates are a collection of user defined parameter values. These templates can be used to create common settings to be used on several devices of a certain device type.

Note:

Templates created in one site are also selectable in the other sites used in WinPDM.

Create a Parameter Template

1. Click the **Templates** tab.
2. From the **Template** menu, select **New**.
3. Select device type and parameter version, enter a name for the template, and click the **OK** button.

Note:

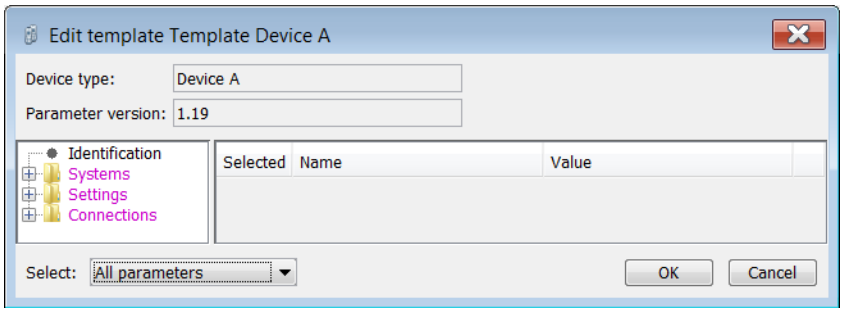
If the wanted device type and/or parameter version is not found in the list, WinPDM needs to be updated with new parameter definition files, see Import Parameter Definition Files on page 348.

4. In the **Edit Template** window, select the parameters to be saved in the template by selecting the check box to the left of each parameter. Change the parameters to the desired values.
5. Click the **OK** button.

Create a Parameter Template from a Number

It is also possible to create a template from a number in the WinPDM. This can be used to save settings in the template that later on can be applied to other numbers.

1. Click the **Numbers** tab.
2. Select the number which settings to be used as template.
3. From the **Template** menu, select **Use as template**.
4. Enter a name for the template.
5. Click the **OK** button.



When creating a template based on a number, a Select drop-down list is shown in the bottom left corner. This setting decides which parameters that shall be copied from the device. If All parameters is selected, the synchronization time will be longer.

6. Select the parameters to be saved in the template by selecting the check box to the left of each parameter. Change the parameters to the desired values

It is also possible to create a template from a device that is online but not stored in the database. The template will contain all parameters for the device except for those that are Number specific.

Rename a Template

1. Click the **Templates** tab.

2. Select the template to be renamed.
3. From the **Template** menu, select **Rename**.
4. In the **Rename template** window, enter a new name and then click the **OK** button.

Copy a Template

1. Click the **Templates** tab.
2. Select the template to be copied.
3. From the **Template** menu, select **Copy**.
4. In the **Copy template** window, enter a new name and then click the **OK** button.

Edit a Template

1. Click the **Templates** tab.
2. Select the template to be edited.
3. From the **Template** menu, select **Edit**.
4. In the **Edit template** window, edit the parameters and then click the **OK** button.

Delete a template

1. Click the **Templates** tab.
2. Select the template to be deleted.
3. From the **Template** menu, select **Delete**.
4. In the **Delete template** window, click the **Yes** button.

Upgrade a Template

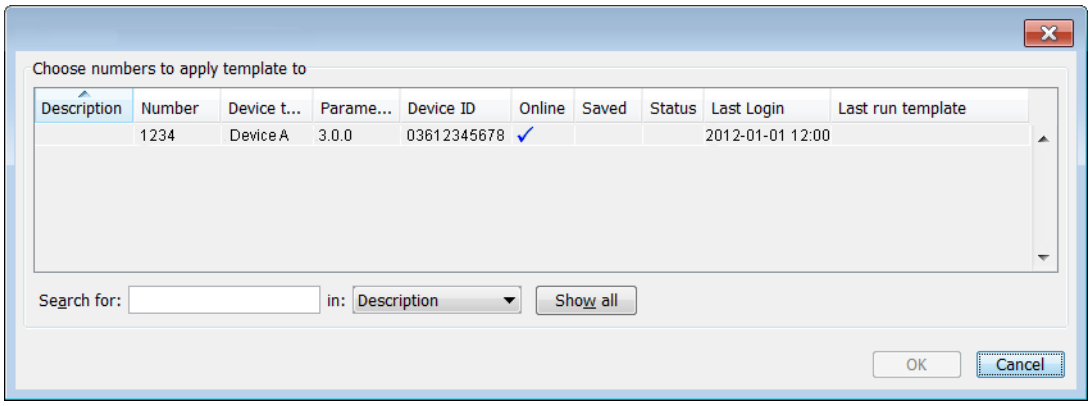
Note:

In order to upgrade a template, the new parameter version must have the same major version as the old parameter version. For example, upgrading from 25.8 to 25.9 works, but upgrading from 25.8 to 26.x does not work.

1. Click the **Templates** tab.
2. Select the template to be upgraded.
3. From the **Template** menu, select **Upgrade**.
4. Select the parameter version to upgrade to and then click the **OK** button.

Apply a Template

1. Click the **Templates** tab.
2. Select the template to be used.
3. From the **Template** menu, select **Apply to**.



Tip:
It is possible to search for a device in the list using the **Search** field.

4. Select device(s) to apply the template on and then click the **OK** button.

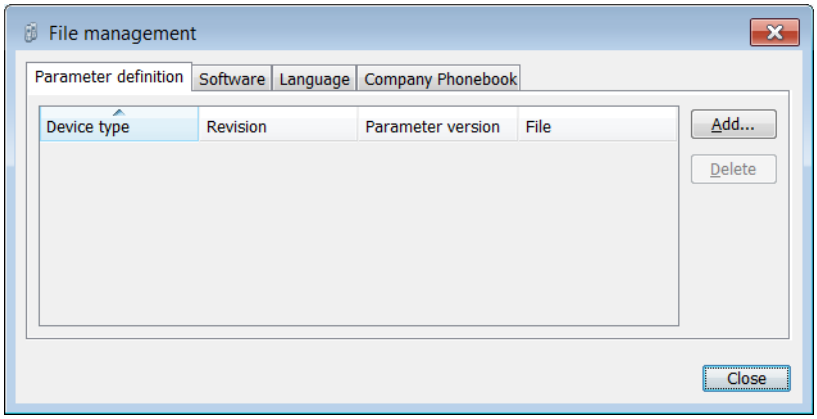
File Management

This chapter covers File management for parameter definition files, software files, language files (.lng) for devices, and company phonebook files.

Import and export of templates and numbers are described in Import and Export of Numbers and Templates on page 351. Import of language files (.xml) for the WinPDM menu are described in Language Settings for WinPDM GUI on page 332.

The parameter definition file holds the definitions of all parameters for a specific version of a Number's parameter set. Updated software and new parameter definition files for devices and Numbers can be added to the WinPDM, see Import Parameter Definition Files on page 348.

Figure 19. The File management window



Definition File Version – Parameter Version

Both definition files and device software include parameters and are indicated by a version number.

If a device associated to a Number is upgraded to a software supporting another parameter version than the stored Number, it does not always demand a new definition file. An old definition file can often be used, but if new parameters have been added in the new parameter version these parameters will not be editable. The release note will tell you if a new definition file is needed to match the new parameters. If the old definition file cannot be used, it will be highlighted with red.

Import a Package File

A package file may include different types of files, such as software files, parameter definition files and/or template files. If the package does not include a certain file, it can be imported separately. See Import Parameter Definition Files on page 348, Import New Software Files for Devices on page 349, and/or Import Templates on page 352.

1. From the **File** menu, select **File management**.
2. Select the **Parameter definition** tab or **Software** tab and click the **Add** button.
3. Select the package file (.pkg) to be imported and click the **Open** button.

The files included in the package are now imported.

Import Parameter Definition Files

Tip:
Parameter definition files (.def) are mainly included in package files (.pkg) distributed by your supplier, see Import a Package File on page 348.

1. From the **File** menu, select **File management**.
2. Select the **Parameter definition** tab and click the **Add** button.
3. Select the definition file (.def) to be imported and click the **Open** button.
4. Only files with a corresponding extension are shown, such as .def and .pkg.

Import New Software Files for Devices



Tip:
Software files (.bin) are mainly included in package files (.pkg) distributed by your supplier, see Import a Package File on page 348.

1. From the **File** menu, select **File management**.
2. Select the **Software** tab and click the **Add** button.
3. Select the software file to be imported and click the **Open** button.
4. Only files with a corresponding extension are shown, such as .bin and .pkg.

To apply the software for a device, continue with the instruction in *Upgrade a Device with New Software*.

Upgrade a Device with New Software

It is possible to upgrade the software in a device. The device must be online/logged in to WinPDM.

1. Click the **Devices** tab.
2. Select the device which should be upgraded. It is possible to select several devices, but only devices of the same device type can be selected.
3. From the **Device** menu, select **Upgrade**.
4. In the **Available files** drop-down list, select the software to be uploaded.
5. NOTE: If the software is not available, you can import it by clicking the **Import** button.
6. Click the **OK** button.

The software will be downloaded to the device. A progress bar in the Status column for the device shows the progress of the download. The device will restart automatically after a successful download.

To cancel the upgrade, select **Device** > **Cancel upgrade**.

Import Language Files for Devices

Note:

To select the language to be used in the WinPDM, see Language Settings for WinPDM GUI on page 332.

For adding a new language to a device, a language file (.lng) distributed by your supplier must be imported to the WinPDM and then uploaded to the device.

1. From the **File** menu, select **File management**.
2. Click the **Language** tab and then click the **Add** button.
3. Select the language files to be imported and click the **Open** button.
4. Only files with a corresponding extension are shown, such as .lng.

To apply the language for a device, continue with the instructions in *Upload a Language to Devices*.

Upload a Language to Devices

It is possible to upload a language to devices that support this feature.

1. Click the **Devices** tab.
2. Select the device(s) to upload a language to. It is possible to select several devices, but only devices of the same device type can be selected.
3. From the **Device** menu, select **Upload Language**.
4. In the **Available files** drop-down list, select which language to upload.
5. NOTE: If your language is not available in the drop-down list, the language file (.lng) can be imported by clicking the **Import** button.
6. Click the **OK** button.

Import Company Phonebook Files

It is possible to import a company phonebook file for later use.

1. From the **File** menu, select **File management**.
2. Click the **Company Phonebook** tab and click the **Add** button.
3. Select the company phonebook files (.cpb) to be imported and click the **Open** button.

To upload the company phonebook to a device, continue with the instructions in *Upload a Company Phonebook*.

Upload a Company Phonebook

It is possible to upload the company phonebook to a device that supports this feature. The company phonebook will appear in the device's Contacts list.

1. Click the **Devices** tab.
2. Select the device(s) to upload a company phonebook to. It is possible to select several devices, but only devices of the same device type can be selected.
3. From the **Device** menu, select **Upload company phonebook**.
4. In the **Available files** drop-down list, select which company phonebook to be uploaded.
5. NOTE: If your company phonebook is not available in the drop-down list, the company phonebook file (.cpb) can be imported by clicking the **Import** button.
6. Click the **OK** button.

Delete Imported Files for Devices

It is possible to delete parameter definition files, software files, language files (.lng) for devices, and company phonebook files.

1. From the **File** menu, select **File management**.
2. Select the applicable tab.
3. Select the file(s) to be deleted.
4. Click the **Delete** button.
5. In the **Delete files** window, click the **Yes** button.

Import and Export of Numbers and Templates

This section describes import and export of Numbers and templates.

- Import and additional file handling of parameter definition files, software files, language files and company phonebook files for devices are described in File Management on page 347.
- Import of language files for WinPDM are described in Language Settings for WinPDM GUI on page 332.

The purpose of exporting and importing Numbers and templates is to be able to move Numbers and templates to another site or to use at a later time.

The parameter configuration in Numbers can be exported to a file. This file can be used by the supplier to pre-program devices before delivery to the customer, and to share Numbers and templates with other PDMs.

Import Numbers

Updated Number files may be distributed by your supplier.

1. From the **File** menu, select **Import** > **Numbers**.
2. Select the Number file(s) to be imported (*.xcp) and click the **Open** button.

If there is a Number conflict when importing Numbers, the error message Number import failed: Number already exists is displayed.

Export Numbers to a File

It is possible to configure Numbers for a site and export the settings to a file. One or several Numbers can be selected. The exported file can then be used when producing new devices for the customer. Only Numbers stored in the database can be exported. There is no restriction on device type when exporting.

1. Click the **Numbers** tab.
2. Select the Number(s) to be exported
3. From the **Number** menu, select **Export**.
4. Enter a file name for the Numbers (.xcp) and where to save the file and click the **Save** button.

Import Templates

Updated template files may be distributed by your supplier.

1. From the **File** menu, select **Import** > **Templates**.
2. Select the template files to be imported (*.tpl) and click the **Open** button.

If there is a naming conflict when importing a template, the new template is imported and a digit within brackets is added after the name. The old template's name is not affected.

For example:
Template MyHandset (old template)
Template MyHandset (2) (new template)

Export Templates

It is possible to export template files. One or several templates can be exported.

1. Click the **Templates** tab.
2. Select the template (or templates) to be exported.
3. From the **Template** menu, select **Export**.

4. Enter a file name for the templates (.tpl) and where to save the file and click the **Save** button.

Administration

Data Backup

All settings in the WinPDM, such as the configuration, the sites and the templates are stored as database files. It is recommended to do backups on a regular basis. Device software, definition files, templates, devices and Numbers including parameters are included in the backup.

Backup WinPDM Database Files

1. Close the WinPDM.
2. The database files are saved in the **WinPDM** folder located in:
3. C:\USERS\<USER>\APPDATA\ROAMING\AVAYA\
4. Copy the **WinPDM** folder to, for example, a network drive.

Restore WinPDM Database Files

1. Close the WinPDM.
2. Retrieve the saved copy of the **WinPDM** folder.
3. Copy the **WinPDM** folder to:
4. C:\USERS\<USER>\APPDATA\ROAMING\AVAYA\

Uninstall the WinPDM

1. From the **Windows Start** menu, select your WinPDM application.
2. Select **Uninstall**. Follow the instructions in the wizard.

Troubleshooting

When troubleshooting the WinPDM, it is always a good idea to examine the log files, since they provide additional information that may prove useful. When reporting an error to your supplier, always include the appropriate log file.

Log files are stored under

C:\USERS\<USER>\APPDATA\ROAMING\AVAYA\WinPDM\log

The log files are rotated every 10 MB and are time-stamped with 1 ms resolution.

Fault	Action or comment
The WinPDM does not start or installation fails	To run the WinPDM, the computer must confirm to the requirements listed in Requirements on page 317. If you do not have the correct software versions installed, contact your system administrator. To install the WinPDM, you must have administrator rights on the computer. Contact your system administrator if you are not able to install the WinPDM.
Firewall alerts appear every time WinPDM is started.	Windows Firewall may alert you of “PMServer” etc. You can ignore these security alerts, it will not affect the WinPDM, but then the alerts will appear every time the WinPDM is started. A better way is to select “Continue blocking” or “Unblock”.

Connected device does not appear in WinPDM.	Make sure the device is properly connected, or try disconnecting and reconnecting the device. Make sure that the USB port is configured correctly as follows: - In Windows 7: Open **Windows Control Panel**. Select **System and Security** > **Hardware and Sound**. Under **Devices and Printers**, select **Device Manager**. If the device does not show up in the list (as an USB port controlled device depending on the handset model), check the connection and reinstall the drivers and/or software for the device.
A device's software is not recognized/ synchronization fails	A device might have software with a parameter set that is newer than the version recognized by the WinPDM. The WinPDM will then be unable to send parameters to the device. The symbol  in the **Status** column for the selected device indicates that the synchronization between the device and the WinPDM was not successful. If this is the case, the WinPDM should be updated with new software and definition files provided by your local supplier. See Import a Package File on page 348.
Upgrade of a device's software fails (aborted)	The device does not support the software version. Use another software version. Ask your supplier.

A Parameter conflict dialog window appears	If a device is detected and the same Number has been used by another device in the system there will be a parameter conflict. A dialog window appears, asking the user to decide whether to use the Number settings in WinPDM or the Number settings in the device. One typical situation when this parameter conflict will occur is if a device's hardware has been replaced. For example: A replacement device has first been registered with the same Number as the damaged device. When the replacement device is connected to the WinPDM, the WinPDM will warn for a parameter conflict. In this case, select "WinPDM" to transfer the phonebook of the damaged device (located in WinPDM) to the new device. If "Device" is chosen in this situation, the phonebook belonging to the damaged device and located in WinPDM will be deleted (and replaced with the empty phonebook in the replacement device). For more information about device replacement, see the User Manual or Configuration Manual for respective device.

WinPDM Keyboard Shortcuts

General

Shortcut	Description
Ctrl + H	Open the File management window.
Ctrl + Tab	Switch tab
Alt + F4	Close the application

Devices

Shortcut	Description
Ctrl + N	Add a new device
Enter	Upgrade the selected device(s)
Delete	Delete the selected device(s)
Ctrl + F	Find a device
Ctrl + Enter	Open the Properties window for the selected device

Numbers

Shortcut	Description
Ctrl + N	Add a new Number
Enter	Edit the selected Number
Ctrl + C	Copy the selected Number
F2	Rename the selected Number
Ctrl + S	Save the selected Number to the database
Delete	Delete the selected Number from the database
Ctrl + F	Find a Number

Templates

Shortcut	Description
Ctrl + N	Add a new template
Enter	Edit the selected template
Ctrl + C	Copy the selected template
F2	Rename the selected template
Delete	Delete the selected template
Ctrl + F	Find a template

File Types

In this appendix, the different file extensions that are used in WinPDM are explained. System files are not described.

File type	Extension	Description
Software file (devices)	bin	Software for devices
Company Phonebook file	cpb	Company Phonebook file for portable devices.
Parameter Definition file	def	Including all possible settings for a certain device type for a certain version.
Language file	lng, or xml	Language file for portable devices or WinPDM. Language file for WinPDM uses XML (eXtensible Markup Language.).
Package file	pkg	Archive that can include different file types such as parameter definition files (.def), software files (.bin) and template files (.tpl).
Site file	ste	Storage for site specific data. These files may not be edited manually.
Template file	tpl	Contains one or more exported templates.
Number file	xcp	Exported Numbers.

Installing and operating the AIWS and the AIWS2

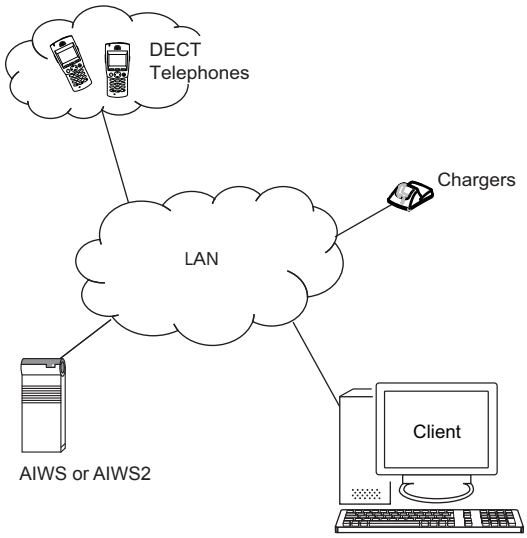
Introduction

The Avaya In-Building Wireless Server (AIWS) is a server for handling wireless services and messaging. It runs on a solid Elise 2 Server (AIWS) or on a Elise 3 Server (AIWS2) that is an updated hardware version in a new housing. You can combine any number of Elise 2 and Elise 3 servers in a multi AIWS/AIWS2 installation. However the AIWS2 includes some new features that are not available on the AIWS. This chapter describes both the AIWS and AIWS2. Features described for AIWS are common for AIWS2, too. Any differences in the configuration and the new features for AIWS2 only are highlighted accordingly.

This chapter describes the installation and configuration of AIWS plus operation of the system. The main functionality is:

- On-site and remote administration of cordless telephones and chargers
- Parameter configuration and software download to cordless telephones and chargers
- Supervision of chargers
- Central phonebook application for cordless telephones
- Text messaging between cordless telephones

Figure 81: AIWS in a system.



The AIWS2 can have different levels of functionality dependent on license. The Device Management application in AIWS2 is used for managing devices such as handsets, desktop chargers and charging racks, i.e. handle settings and software for the devices. It makes it possible to change settings and update software in the devices. All devices are updated remotely from AIWS2 and parameters and software for the devices are saved in a database. Administration of handsets and chargers can be done via a remote connection to a customer site.

Messaging features supported by AIWS2 include SMS between users in the system, sending instant or predefined text messages from a web browser. AIWS2 also includes a central phonebook which can be accessed from the handsets. The number of entries in the phonebook depends on whether the internal database or an external database is used as phonebook source

Note:

The software uses open-source components.

This chapter is intended as a guide for installation, maintenance and troubleshooting purposes and is relevant for:

- Installation and configuration, administrator rights
- Daily operation of the system, user rights

Licenses

Licenses for AIWS:

- WSM-MVB, AIWS Basic, including Elise 2, power supply and license
- WSM-MVS, AIWS Standard, including Elise 2, power supply and license
- WSM-MVP, AIWS OAP, including Elise 2, power supply and license
- WSM-MVE, AIWS Enterprise Management, including Elise 2, power supply and license

Licenses for AIWS2:

- FE3-EACAAC, Avaya AIWS2 Basic including hardware and SW license
- FE3-EBCAAC, Avaya AIWS2 Basic + including hardware and SW license
- FE3-ECCAAC, Avaya AIWS2 Standard including hardware and SW license
- FE3-EDCAAC, Avaya AIWS2 OAP including hardware and SW license
- FE3-EECAAC, Avaya AIWS2 Enterprise including hardware and SW license
- FE3-EACAAD, Avaya AIWS2 Basic, Argentina, including hardware and SW license
- FE3-ECCAAD, Avaya AIWS2 Standard, Argentina, including hardware and SW license

Note:

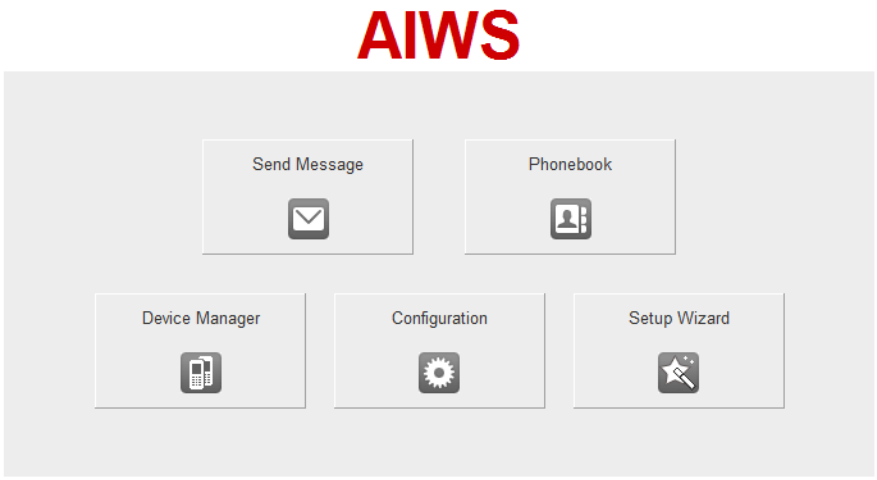
Not all functionality described in this document is available in all variants.

For details regarding items and technical specifications, refer to Avaya In-Building Wireless Server (AIWS) on page 656 and Avaya In-Building Wireless Server 2 (AIWS2 hardware) on page 659.

Overview

From the AIWS start page it is possible to select different functionality modules.

Figure 82: AIWS start page



- Send Message, see Operation on page 387.
- Phonebook, see Central phonebook administration on page 364.
  Describes how to handle phonebook entries.
- Device Manager, see Device Manager on page 397.
  Describes device management.
- Configuration, see Configuration Page on page 382.
  Setup page for the AIWS settings.
- Setup Wizard, see Configuration and AIWS setup Wizard on page 366.
  The first time and as long as AIWS is not configured, the setup wizard will start automatically.

How to use this chapter

This document is used for installation and configuration, for administration, maintenance and troubleshooting. These activities require good knowledge about functionality and limitations, both on module and system level, and also knowledge about how systems, modules and parameters interact.

The document also includes information about the daily operations of creating and sending messages, which can be done by any user in the system.

For example, in order to simplify an installation, use the following steps:

Installation and setup

- For installation and basic configuration, refer to chapters
  - Installation and configuration on page 365
  - Configuration and AIWS setup Wizard on page 366

Charger installation

Follow the instructions in the chapter for the charger.

Recommended work flow for telephone installation

The recommended work flow depends on what type of telephones that are used.

- DECT telephones when adding new telephones
- DECT telephones when telephone is up and running

Recommended work flow when adding new DECT telephones

1. Install and configure AIWS, see Installation and configuration on page 365.
2. Create a template with settings common for all devices at the site, see Creating a parameter template on page 405.
3. Add a range of Numbers to the site, see Creating new numbers on page 410. Run the template.
4. Connect the telephone to AIWS. The telephone is shown as Online (✓) in the Devices view.
5. In the Numbers view, right click and associate the Number, see Associating a number with a device on page 414.
6. Register the telephone in the PBX

Recommended work flow for DECT telephones that are up and running

1. Install and configure AIWS, see Installation and configuration on page 365.
2. Connect the telephones to the AIWS. When connected, the Numbers are shown as Online (✓) in the Device Manager.
3. Right click on the entries and Save.

Central phonebook administration

- For administration of the central phonebook, refer to chapter Phonebook Administration on page 390.

Daily operation

- For the daily operation i.e. creating and sending messages, refer to chapter Operation on page 387.

Included in the delivery

- Elise 2 (AIWS Hardware) or Elise 3 Server (AIWS2 Hardware)
- Safety and security leaflet
- Ordinary RJ45 (straight through pinouts) network cable for connection to the LAN
- License certificate

Technical solution

AIWS consists of a server and a client part. The server runs on the Elise 2 (AIWS Hardware) or Elise 3 Server (AIWS2 Hardware) and is configured from a web interface. The Java based client is run on a PC connected to the Local Area Network (LAN) and is loaded from the server (Device Manager).

Requirements

Refer to Avaya In-Building Wireless Server (AIWS) on page 656 and Avaya In-Building Wireless Server 2 (AIWS2 hardware) on page 659.

Installation and configuration

After installing the AIWS, the basic configuration is easily done with the help of a setup wizard. The wizard includes all basic settings needed to get the AIWS up and running.

Required information

Make sure the following information is available:

Information required for the installation

- MAC address – found on the license certificate enclosed in delivery
- An IP address is needed, see Getting Started with the AIWS on page 505 and Getting started with AIWS2 on page 509

Information required for the configuration

- License number – found on the license certificate enclosed in delivery
- Network parameters – ask your network administrator
- Type of connected wireless phone system
- IP address to connected system (if connected via IP)
- Other messaging systems to send messages to (optional)
- LDAP properties if an LDAP server is used for Central Phonebook requests (optional)

Hardware installation and configuration

For information on installation and configuration Elise 2 Server (AIWS Hardware), see Installing Elise 2 Server (AIWS Hardware) on page 523.

Note:

Attach the ferrite bead on the power supply cable. Follow the enclosed assembly card for EMC protection, M0271500.

For information on installation and configuration of the Elise 3 Server (AIWS2 Hardware), see Installing the Elise 3 Server (AIWS2 Hardware) on page 570.

Software installation

AIWS

For information on the software installation, see Maintenance information for the AIWS on page 550.

See also Getting Started with the AIWS on page 505.

AIWS2

For information on the software installation, see Maintenance information for the AIWS2 on page 590.

See also Getting started with AIWS2 on page 509.

Configuration and AIWS setup Wizard

Accessing AIWS

When accessing AIWS the first time, follow the instructions in Getting Started with the AIWS on page 505 and Getting started with AIWS2 on page 509.

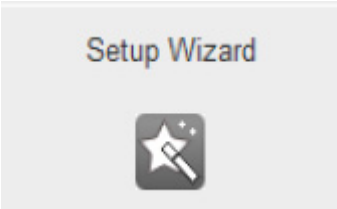
Note:

The IP address must not change during operation because renew of IP address via DHCP is not handled. Other equipment connected to this product also expects a fixed IP address in some cases. If the IP plan is changed, this product must be restarted to update the IP address. Otherwise there is a risk for IP address collision.

For information about Power Down and Restart, see Powering down and restarting the Elise 2 Server (AIWS Hardware) on page 527 and Powering down and restarting the Elise 3 Server (AIWS2 Hardware) on page 564.

Basic configuration steps

Figure 83: Setup Wizard button on AIWS start page



The first time and as long as the AIWS is not configured, the setup wizard will start automatically when logging on from a web browser. Requires "**admin**" or "**sysadmin**" password, refer to Authentication Levels and Default Passwords on page 378.

1. Log on to AIWS.

   The setup wizard will open and help you with the basic configuration. The setup wizard includes the following settings:

   - Network setup – can be set manually or via DHCP
   - License number – the type of license determines the functionality
   - DECT IP address – IP address to the DECT exchange
   - Date and time properties/settings – for time stamps on activities
   - Central Phonebook properties – database to use when searching (internal, external or LDAP server)
   - LDAP properties (only visible if LDAP is selected in the Central Phonebook Properties)
   - TFTP properties – IP address and port number to use (only visible if TFTP is selected in the Central Phonebook Properties)
   - Passwords – change from default to site specific passwords

2. Configure the phonebook (but only if an LDAP server or TFTP is **not** used), refer to Central Phonebook Configuration on page 443.
3. Create a backup of the configuration.

   We recommend you to create a backup of all settings (to facilitate the configuration in case of a software upgrade). Refer to Backing up the configuration on page 460.

Optional settings

Some of the optional settings in AIWS are included in the basic license, other require an additional optional license. Refer to How to use this chapter on page 362.

- Set Language – it is possible to translate the user interface language, refer to chapter Customizing the language on page 477.
- Customize the Start page and NetPage GUI – the Start page and the NetPage user interface can be customized to suit the individual customer requirements concerning functionality. Refer to chapter Customizing the user interface (GUI) on page 482.
- Open Access Protocol (OAP) – makes it possible to communicate with other systems that is connected to the AIWS. Refer to chapter Open Access Protocol (OAP) on page 504.

Digit Treatment – makes it possible to set the way telephone numbers are converted in telephone number lists. Refer to Digit treatment for IP regions on page 449.

Adding device software to the Device Manager

1. Log in to AIWS (http://xxx.xxx.xxx.xxx) and click on **Device Manager**.
2. Upload definition files. The definition files are usually included in a package file. See Importing a package File on page 426 for more information. A package file contains a definition file (.def). It may also contain software for the devices (.bin) and a template (.tpl). You may have to contact your supplier for the latest updates.

   If the definition file shall be imported as a separate file, see Importing parameter definition files on page 427for more information.You may have to contact your supplier for the latest updates.

How to work with Numbers is described in chapter Numbers on page 410.

Updating AIWS for Elise 2 Server (AIWS Hardware)

Update of software is done via the web interface.

There are two choices, **Install software** and **Install image**.

If new software is installed by doing an update of AIWS, using an .eas file, information stored in the database will not be overwritten.

If a new image file is installed, using an .img file, the database information is deleted, and software and definition files are removed.

For instructions on how to upgrade, both .eas and .img files, see Updating application software on page 550. It is recommended to do a backup before upgrading.

Make sure no Device Manager client is open during an update of the AIWS. It is also important that no ftp client is logged in to the AIWS. If the Microsoft Internet Explorer is used as ftp client, close it before upgrade.

Note:

Customized NetPage GUI will be overwritten when upgrading. See also Updating the user interface after a new AIWS Release on page 493

Updating Elise 3 Server (AIWS2 Hardware):

On the Elise 3 hardware, the software update is done with a software package (.pkg file) only. Software upgrade is started from the AIWS application. See Software administration on the AIWS2 on page 507.

Besides the software administration via the configuration page, it is also possible to administer the software via the module's Boot Mode GUI. See Installation of software on page 590. The Boot Mode GUI is typically used if no software is installed on the module or if it is impossible to access the software.

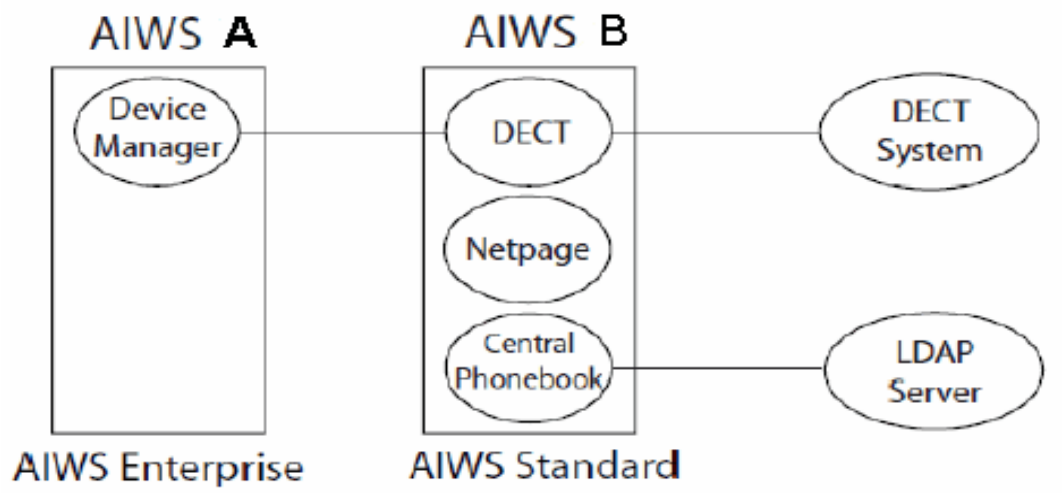
Multiple AIWS configuration

For some situations, there is a need to configure more than one AIWS in a system. This chapter presents examples for multiple AIWS configuration. Examples of functionality distributed on different AIWS's are Device Management, Central Phonebook and Netpage Messaging.

Functionality distributed on two AIWS modules

A system configuration with two AIWS's is required when there are more than 120 cordless telephones simultaneously in the system, and Central Phonebook with LDAP/TFTP or NetPage Advanced is used.

Figure 84: Example of a multiple AIWS solution with Device Handling on one AIWS and DECT interface on another AIWS



Basic configuration for the setup

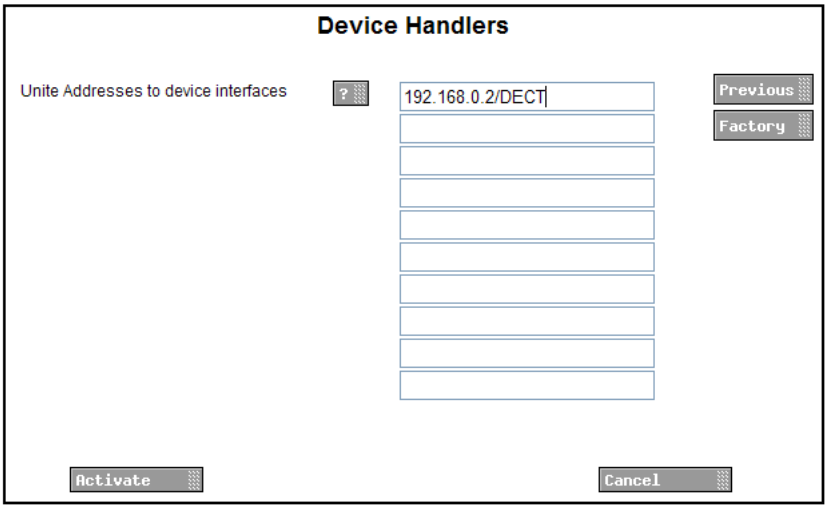
The basic configuration for this setup is described below.

- AIWS A (Enterprise)
  This setting is done in the **Configuration** page, not in the Setup Wizard.
  - In **Configuration > Other Settings > Advanced Configuration > Device Management**:
    Replace the address `127.0.0.1/DECT` with `<IP address of AIWS B>/DECT`, that is, if AIWSB has the IP address `192.168.0.2`, change to `192.168.0.2/DECT`.

- Set forwarding for NetPage:
  In **Configuration > Other Settings > Advanced Configuration > Other > UNS > Operating mode**:

  Operating Mode shall be set to Forwarding. **IP address of forward destination UNS** shall be set to the IP address of the AIWS with the DECT connection (here AIWSB: 192.168.0.2). Click **Activate**
- Disable the DECT interface on the AIWS A because it's not used. If the DECT interface is disabled the AIWS will not show any error logs, because of an non connected DECT interface. Select **advanced configuration > general settings > view advanced parameters.** Set DECT interface to **disable**.

Figure 85: Setting the IP address



- AIWS B (Standard)
  - DECT and Central Phonebook connection are configured in the AIWS Setup Wizard.
  - In **Configuration > Other Settings > Advanced Configuration > Device Management**:
    Remove all IP addresses.

Migration to a double AIWS solution

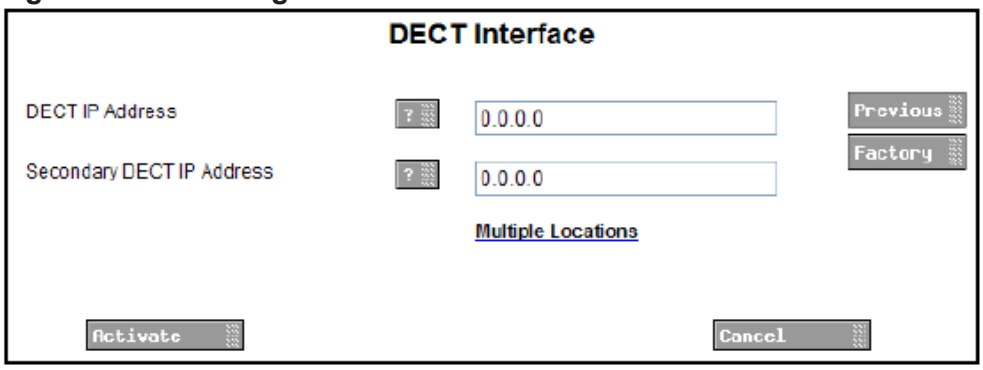
This example assumes that the original system uses one AIWS Enterprise and this single AIWS handles both Device Management and the connection to DECT. An additional module, AIWS Standard shall now be added to the system.

One reason for this migration is to configure the more business critical applications such as NetPage and Central Phonebook on one AIWS and the less critical application Device Management on another.

Change the following settings in the original AIWS:

- AIWS Enterprise (AIWS A, original AIWS)
  - In **Configuration > Other Settings > Advanced Configuration > Device Management**:
    Replace the address `127.0.0.1/DECT` with the IP address of AIWS B plus `/DECT`, that is, if AIWS B has the IP address `192.168.0.2`, change to `192.168.0.2/DECT`.
    Click **Activate**.
  - In **Configuration > Other Settings > Advanced Configuration > DECT Interface > IP-DECT**:
    Click "Factory" to remove IP addresses. Click **Activate**.

Figure 86: Removing DECT IP addresses.



For settings in the added AIWS, see above.

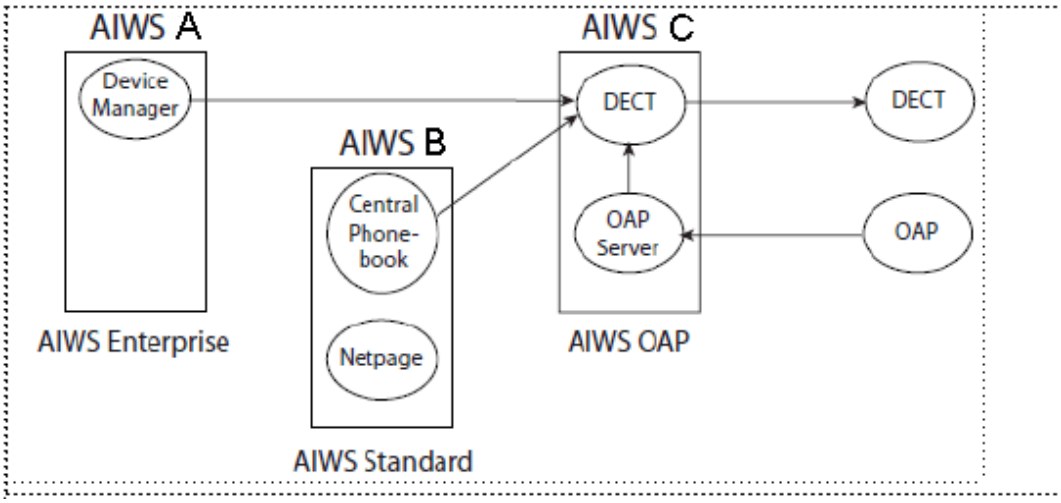
Functionality distributed on three AIWS modules

A system configuration with three AIWS's is required when the following three conditions exist:

- there are more than 120 cordless telephones simultaneously in the system
- an external application is connected, for example using OAP
- Central Phonebook with LDAP/TFTP or NetPage Advanced is used

An example presenting a distributed solution is shown in figure 87.

Figure 87: Example of a multiple AIWS solution with functionality distributed on three AIWS's



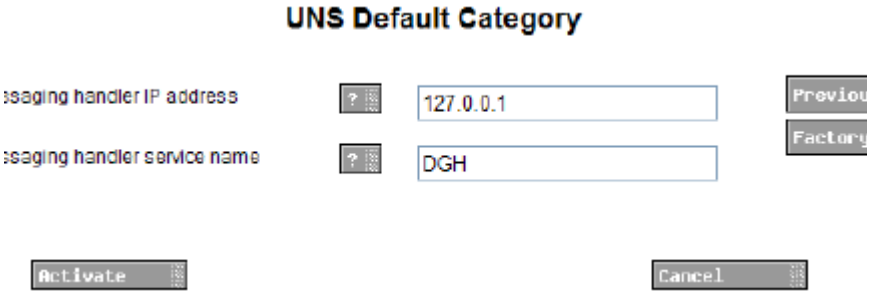
Basic configuration for the setup

The basic configuration for this setup is described below.

- AIWS A (Enterprise)
  - In **Configuration > Other Settings > Advanced Configuration > Device Management**:
    Replace the address of AIWS B `192.168.0.2/DECT` with the IP address of AIWS C plus `/DECT`, that is, if AIWS C has the address `192.168.0.3`, change to `192.168.0.3/DECT`.
  - Set UNS Default Category for messaging to function:
    In **Configuration > Other Settings > Advanced Configuration > Other > UNS > Default category**:
    Enter the IP address and name of the messaging handler, here "192.168.0.3" and "DECT".
    Click **Activate**.
  - Disable the DECT interface on the AIWS A because it's not used. If the DECT interface is disabled the AIWS will not show any error logs, because of an non connected DECT interface. Select advanced configuration - general settings -view advanced parameters. Set DECT interface to **disable**.
- AIWS B (Standard)
  - In **Configuration > Other Settings > Advanced Configuration > Device Management**:
    Remove all IP addresses.

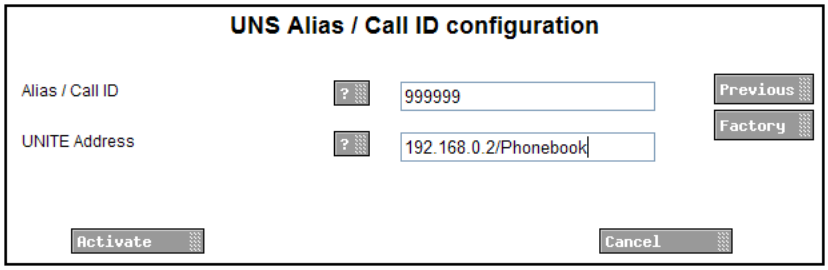
- Set UNS Default Category for messaging to function:
  In **Configuration > Other Settings > Advanced Configuration > Other > UNS > Default category**:
  Enter the IP address and name of the messaging handler, here "192.168.0.3" and "DECT".
  Click **Activate**.
- Disable the DECT interface on the AIWS B because it's not used. If the DECT interface is disabled the AIWS will not show any error logs, because of an non connected DECT interface. Select advanced configuration - general settings -view advanced parameters. Set DECT interface to **disable**.

Figure 88: Setting UNS Default Category



- AIWS C (OAP)
  - The DECT connection is configured in the AIWS Setup Wizard.
  - In **Configuration > Other Settings > Advanced Configuration > Device Management**:
    Remove all IP addresses.
  - In **Configuration > Other Settings > Advanced Configuration > Other > UNS > Alias / Call ID > 999999**:
    In the **UNITE Address** field, set to the IP address of AIWS B plus **/Phonebook**, that is, if AIWS B has the address **192.168.0.2**, set to **192.168.0.2/Phonebook**.

Figure 89: Setting Unite IP address



Migration to a triple AIWS solution

This example assumes that the original system uses one AIWS Enterprise and one AIWS Standard as in Functionality distributed on two AIWS modules on page 369. The AIWS Enterprise (AIWS A) handles Device Management. The AIWS Standard (AIWS B) handles NetPage and the connection to DECT. An additional module, AIWS OAP shall now be added to the system.

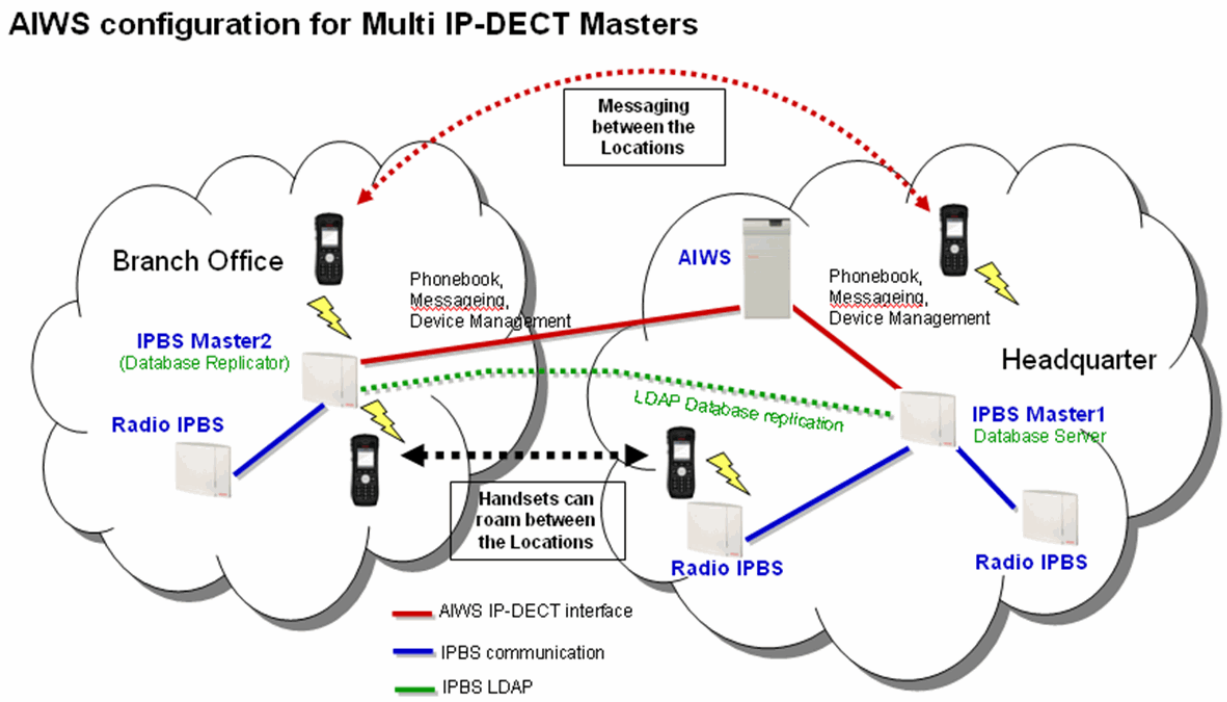
One reason for this migration is to configure the external application which here is considered to be the most business critical application on one AIWS and the less critical applications NetPage, Phonebook and Device Management on the another two AIWSs.

Change the following settings in the original AIWSs:

- AIWS Enterprise (AIWS A):
  - In **Configuration > Other Settings > Advanced Configuration > DECT Interface > IP-DECT**:
    Click **Factory** to remove IP addresses. Click **Activate**.
- AIWS Standard (AIWS B):
  - In **Configuration > Other Settings > Advanced Configuration > DECT Interface > IP-DECT**:
    Set the IP addresses for **DECT IP Address** and **Secondary DECT IP Address** to `0.0.0.0`
  - In **Configuration > Other Settings > Advanced Configuration > Other > UNS > Default category**:
    Enter the IP address and name of the messaging handler, here **192.168.0.3** and **DECT**. Click **"Activate"**
  - In **Configuration > Other Settings > Advanced Configuration > Device Management**:
    Remove all IP addresses.

For settings in the added AIWS, see above.

AIWS configuration for Multi Base Station Masters



The AIWS is able to support multiple Base Station Masters. This configuration offers

- Messaging from AIWS web page to handsets independently from the connected Base Station Masters
- Messaging from handset to handsets independently from the connected Base Station Masters
- A central phonebook can be used in all offices. Digit manipulation for Phonebook queries will be supported according to the location of the connected master (in first step this will only be supported for the LDAP phonebook).
- Centralized device management for all connected devices on different Master Base stations

Beside other basic configuration of the AIWS and IPBS Master and Standby Master the following steps are recommended to support a multiple Base Station Masters configuration.

On the AIWS:
(If a multi AIWS configuration is used this needs to be done on the device running the IP-DECT interface):

- Open the advanced configuration page: On the AIWS start page, select **Configuration**. The **AIWS Configuration** page opens. Select **Other Settings** > **Advanced Configuration**. The **AIWS Advanced Configuration** page opens.

- In IP **-DECT** under **DECT Interface** remove the entries (or just configure to 0.0.0.0) for **IP-DECT IP address** and **Secondary IP-DECT IP Address**. Set multiple Locations (former IP-Regions) to **Yes**
- In **Phonebook** select **Location settings** (former IP-Region settings). Set Digit Treatment to enable. Now configure the digit treatment settings. For each Location with different digit treatment rules an own entry using the appropriate Location ID (former IP-Region ID) needs to be created. Each IPBS Master needs to refer to one of these Location IDs. IPBS Masters and Standby Masters in the same Location area can refer to the same Location ID. It’s recommended to use the same Location IDs as used on the Communication Manager side (IP Region page).
- In **UNS** under **Other** select **Default Category**. Make sure the **Messaging handler service name** is set to **DGH** (Device Group Handler).

On AIWS device manager:

- Make sure that the following two entries are identical:
  - The entry in the **Number** field of a handset device configured in the **Numbers** tab and
  - the **Number** (extension number) of the handset assigned in the IPBS Master **Users** tab.

  Otherwise the messaging and centralized phonebook access won't work. This restriction only exists in systems using multi IPBS Masters on one AIWS.

On each Base Station Master and Standby master:

- In **UNITE** > **SMS**, you will need to configure the Location ID (former IP-Region ID) according to the digit treatment rules for the corresponding Location configured on the AIWS.

Note:

Note: In the Standby Master it’s recommended to use the same Location ID as its Master Base Station is configured.

Administration

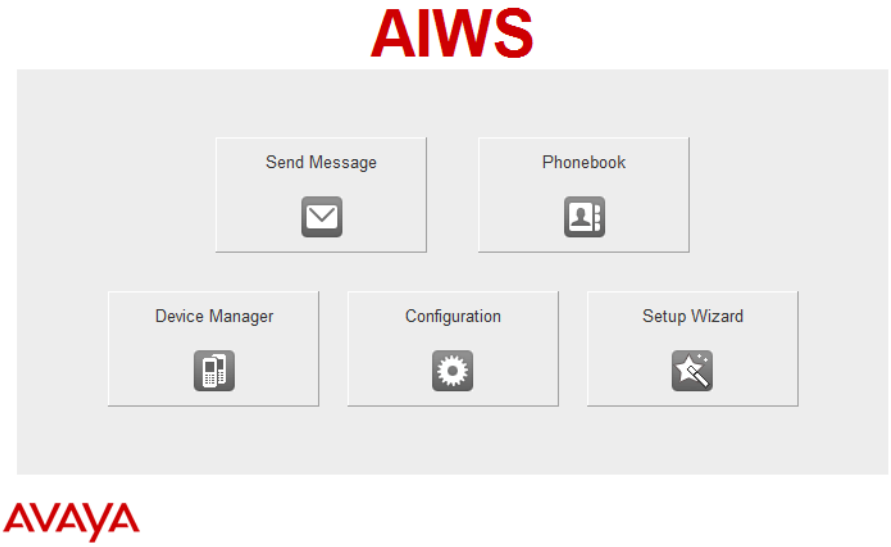
Data backup

All settings in AIWS are stored as database files. Ensure that you backup these files on a regular basis, see Backing up the configuration on page 460.

AIWS Overview

Authentication Levels and Default Passwords

Figure 90: AIWS start page



AIWS has different authentication levels:

- Using the *Send Message* function, i.e. creating and sending messages can be done by default by any user in the system and requires no password.
- *User* rights are required for the administration of the phonebook and opening the device manager. Default user name and password are “user” and “password”.
- *Administrator* rights is required for the setup, the configuration and administration, simple troubleshooting and changing passwords (except for the sysadmin password). Default user name and password are “admin” and “changeme”.
- *System Administrator* rights is used for advanced troubleshooting, gives access to all administration pages and the permission to change all passwords. Default user name and password are “sysadmin” and “setmeup”.
- Auditor rights gives basically the same access as Administrator rights, but without permission to alter values. There is no access to the Setup Wizard or the Device Manager. Default user name and password is "auditor" and "readonly".

For information about password protection of NetPage, see Password Protected Access to NetPage on page 492.

Different levels of password policy can be set in AIWS, see Password policy on page 380.

Functionality matrix

The following matrix shows which functionality that can be used by the different authentication levels.

	anonymous	user	admin	sysadmin	auditor
Send messages	Yes	Yes	Yes	Yes	Yes
Phonebook administration	No	Yes	Yes	Yes	No
View configuration settings	No	No	Yes	Yes	Yes
AIWS configuration Access to the Setup Wizard .	No	No	Yes	Yes	No
Access to the Device Manager	No	Yes	Yes	Yes	No
Change passwords	No	No	Yes **Note**: admin cannot set password for syadmin	Yes	No

Setting passwords

The default passwords for the various types of users such as sysadmin, admin and others, can be changed and it is also possible to specify the password complexity, such as length and number of character types. Passwords can be changed in both the Setup Wizard and on the Advanced Configuration page, but the password complexity (password policy) can only be changed on the Advanced Configuration page.

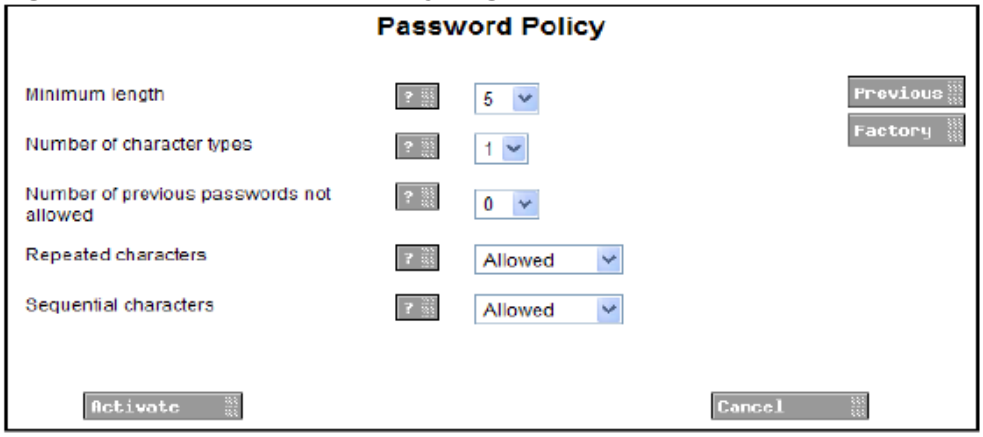
1. Click **Configuration** on the start page. The **Configuration** page appears.
2. Select Other **Settings > Advanced Configuration** in the left menu in the **AIWS Configuration** page. The **Advanced Configuration** page appears.
3. Under **Security**, click **Change Passwords**. The **Change Passwords** page appears.
4. Click the user to change password for.
5. Enter your user name and password. Enter new password and confirm the password.
6. Click **Ch. Passwd**.

Password policy

The required password complexity can be set in AIWS, follow this instruction:

1. Login to AIWS.
2. Click on **Configuration**.
3. In the left pane, select **Other Settings** > **Advanced Configuration**.
4. Under Security, select **Password policy**. The **Password Policy** page opens

Figure 91: The Password Policy page



5. Select password policy.
6. Click **Activate**.

It is also possible to select previous or factory settings.

Web access security settings

When secure mode is enabled (recommended), only secure access via HTTPS and FTPES is allowed. HTTP is automatically redirected to HTTPS and FTP access is not allowed.

The web access security level can be set as follows:

1. Login to AIWS.
2. Click on **Configuration**.
3. In the left pane, select **Other Settings** > **Advanced Configuration**.
4. Under Security, select **Web access**. The *Web* **Access Security** page opens

Figure 92: The Web Access Security page



5. Select if *Secure Mode* shall be enabled or not.
6. Click on **Activate**

It is also possible to select previous or factory settings.

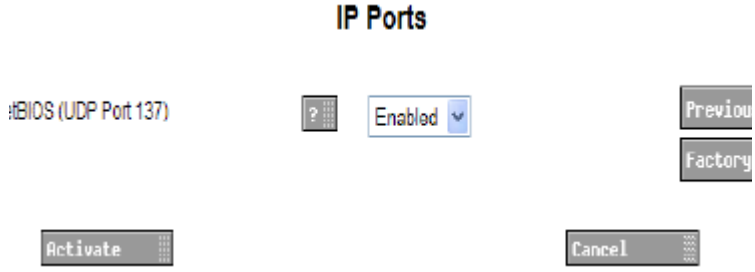
Note:
AIWS2 supports SSLv3.0 and TLS 1.0 for secured connections.

Disabling the NetBIOS Service

The NETBIOS Service makes it possible to access the module with the NetBIOS name "elise-XXXXXXXX", where XXXXXXXX is the module key number.

1. The NetBIOS port is enabled by default, but can be disabled if needed for security reasons.
2. Click "**Configuration**" on the start page.
3. Select **Other Settings > Advanced Configuration** in the menu on the Configuration page.
4. Select **IP Ports** in the menu on the Advanced Configuration page.

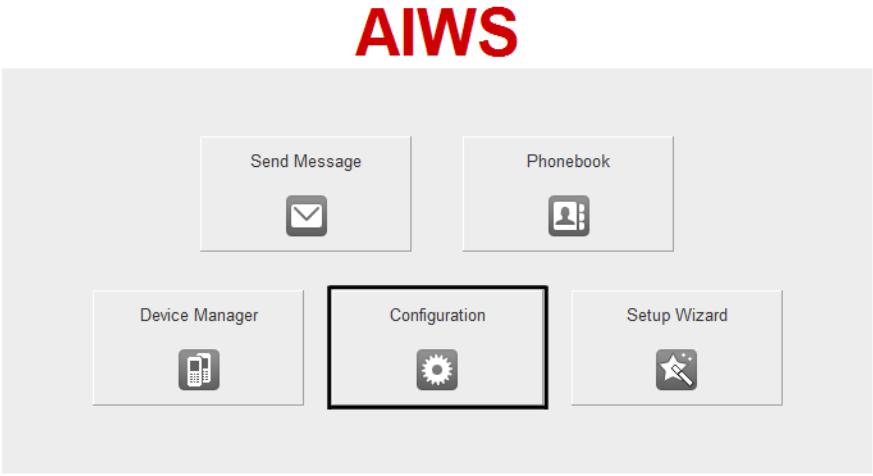
Figure 93: IP Ports setting on Advanced configuration page



5. Select "**Disabled**" int the drop down list.
6. Click "**Activate**".

Configuration Page

Figure 94: AIWS Configuration from AIWS start page.



In order to reach the AIWS Configuration page, click on Configuration on the AIWS start page.

Figure 95: AIWS Configuration page.



With system administrator or administrator rights you will be able to access the complete AIWS configuration page from the *Configuration*, and *Phonebook* buttons on the start page.

Use the symbol if you want to return to the start page without logging out. Using the “Log out” link will also send you back to the start page but you will be logged out as well.On the *Configuration* page, system information is shown, for example:

- Host Name
- IP Address
- MAC Address
- Module Key
- License Number
- Software Version
- Number of Active Faults

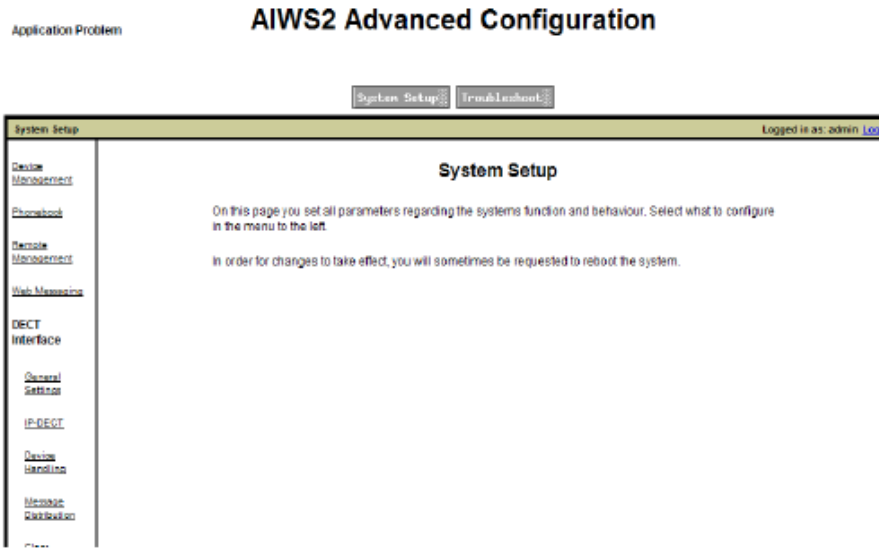
On AIWS2 Elise 3 Server (AIWS2 Hardware) the following information will additionally be available:

- Current status,
- NTP server address
- the current time
- uptime

Advanced Configuration page

The **Advanced Configuration** page is reached from the **Configuration** page (under Other Settings).

Figure 96: The AIWS2 Advanced Configuration page



Icons

On the AIWS pages the following icons might be shown:



Click on this icon if you want to return to the start page without logging out. Using the “Log out” link will also send you back to the start page but you will be logged out as well..



Click on this icon to return to the *AIWS Configuration* top page.



Click on this icon to create a shortcut in your Internet Browser.

Certificates

Certificates are used to increase security by encryption. A self-signed digital certificate is created during the first start-up of AIWS. This certificate is issued to the MAC address of the module. It is possible to import a certificate or to create one in the AIWS.

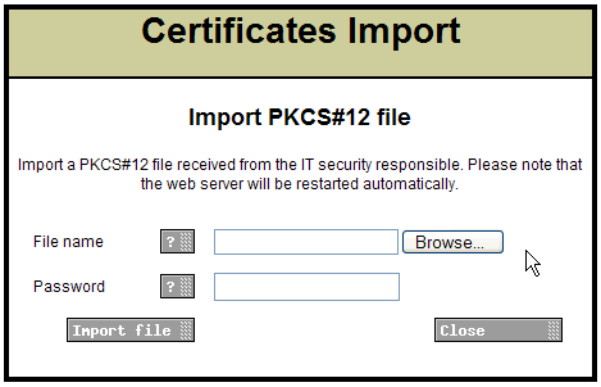
Importing certificates

It is possible to import certificates to AIWS. These certificates may be created by a system administrator with IT security responsibility. AIWS uses PKCS#12 files, which include keys and certificates.

For instructions on how to import a PKCS#12 file, follow this instruction:

1. On the **AIWS start page**, click on **Configuration**. The **AIWS Configuration** page opens.
2. In the left pane, click **Other settings** > **Advanced configuration**. The **AIWS Advanced Configuration** page opens.
3. In the left pane, under **Certificates**, click on **Import**. The **Certificates Import** page opens.

Figure 97: The Certificates Import page.



4. On the **Certificates Import** page, you can locate a certificate file. Enter file name and a valid password. The certificate is tied to a specific password which should be delivered with the file.
5. Click **Import file**. The file is imported to AIWS.
6. Click **Close**.

You may have to ask the network administrator for PKCS#12 files.

When starting, there may be a warning about the security certificate. This warning can be ignored.

Creating a certificate

It is possible to create certificates in AIWS. For instructions on how to create a PKCS#12 file, follow this instruction:

1. On the **AIWS start page**, click on **Configuration**. The **AIWS Configuration** page opens.
2. In the left pane, click **Other settings** > **Advanced configuration**. The **AIWS Advanced Configuration** page opens.
3. In the left pane, under **Certificates**, click on **Create**. The **Create Self Signed Certificate** page opens.

Figure 98: The Create Self Signed Certificate page.



4. On the **Create Self Signed Certificate** page, enter valid parameters for your certificate file. **Validity** and **Common name** are mandatory.

   Due to security reasons, some characters in the ASCII-table are not allowed to use in the fields **Common Name**, **Organization Unit**, **Organization**, **Locality**, **State or Province** and **Country** when creating a certificate.
   Among these are: [,], (,), {, }, $, &, \, |, *, ", `, ', ?, ~, >, <, ^, \n, \r.

5. Click on **Create Certificate**. A certificate file is saved and the web server is restarted.

Demonstration Mode

Demonstration Mode makes it possible to run the product for two hours with almost full functionality of the application.

The Demonstration Mode can be set from the application's Configuration page or manually by using the Mode button. The module will automatically return to previous licence and parameters (without restart) after 2 hours.

The Demonstration Mode is indicated by the Status LED with yellow slow flashing light. If any application encounters problems during Demonstration Mode, the Status LED will however show red slow flashing light instead. The Mode button LED shows blue fixed light.

From the application's Configuration page:

1 Click "**Configuration**" on the start page.

2 Select **Other Settings > Demonstration Mode** in the menu on the Configuration page.

3 Click "**Activate**".

4 Exiting before the 2 hours have passed, is done by clicking "**Deactivate**".

Using the Mode button:

1 Press and hold the Mode button for 10 seconds.

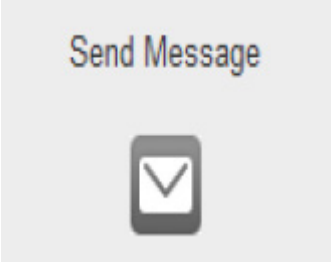
Operation

Messaging

Creating and sending messages requires no password and can be done by any user in the system. Depending on the license, the following tools for messaging are displayed:

- Messaging tool - included if license does not include NetPage
- NetPage - included in Avaya AIWS2 Standard license

Figure 99: Messaging button on AIWS start page

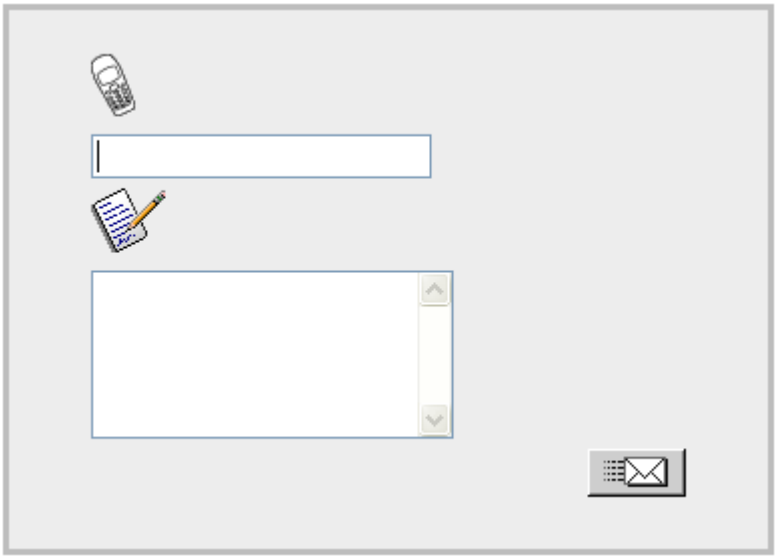


For configuration of the Messaging Tool, see Operation on page 387.

Messaging Tool

The Messaging Tool GUI is displayed on AIWSs without additional license.

Figure 100: Messaging Tool GUI

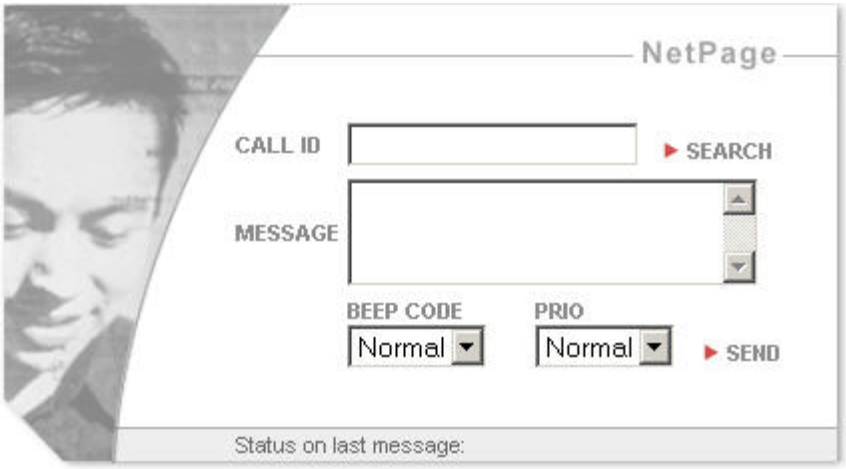


In order to send a message, do as follows:

1. On the AIWS start page, click on **Send Message**, the Messaging Tool window appears.
2. Enter phone number in the top text field.
3. Enter message in the bottom text field.
4. Click on the send button. The message is sent to the receiver and the result is dispayed by the appropriate icon.

NetPage

The NetPage messaging tool is shown for user with a license including NetPage.



Creating and sending messages

You can sent a message with priority **Normal**, **Low** and **High**. The higher the priority the faster the message will be delivered. An additional priority code Alarm can also be made available by customizing the NetPage html files. Messages send with priority Alarm will be opened immediately independent from the active screen on the handset site (even if the handset is in a call).

In the combo box **Beep Code** you can select, how the message should be signalled on the called telephone.

Note:

Selecting **Beep Code *x beeps*** will only work, if on the called phone the setting **Sound & Alerts > Message alerts** is set to **Beep**.

1. Click **Send Message** on the start page. The **NetPage** opens.
2. Click either on the **Search** button to search a number from the Users list, or enter number in the **Call ID** field. It is possible to enter several Call ID's separated by semicolon.
3. Enter message text in the **Message** *text* field. All possible characters are shown in Characters for SMS on page 245.
4. Select ***Beep code*** and ***Prio***.
5. Click **Send**.

Phonebook Administration

The phonebook administration in this chapter requires authentication on *user* level. For further configuration, see Central Phonebook Configuration on page 443.

Figure 101: Phonebook button on AIWS start page



The phonebook makes it possible for users to search and find phonebook entries from a telephone in the system.

If a local phonebook is used the entries must be added, either by creating them manually, refer to Adding entries to the phonebook on page 390, or importing them from a CSV file, see Importing entries to the phonebook from a CSV File on page 393.

Phonebook editing

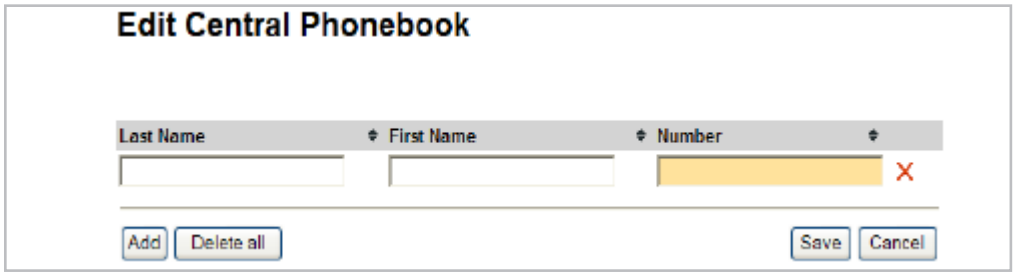
Adding entries to the phonebook

The entries in the phonebook can be filled in manually.

1. Click **Phonebook** on the start page.
2. Enter ***User name*** and ***Password*** and click **OK. The Edit Phonebook page appears.**
3. Click **Add** button and enter the information needed in the text fields as described in Adding entry manually below,

Adding entry manually

Figure 102: The Edit Phonebook page



1. Enter the following settings in the text fields:

Setting	Description
Last Name:	The family name. If the family name is a double-name, it is possible to add blank(s) between the names.
First Name:	The first (given) name. If the first name is a double-name, it is possible to add blank(s) between the names.
Number:	The phone number

Note:

If first names and/or last names include spaces, ensure that you enable the **Central Phonebook Allows Space** parameter in the telephone. See the corresponding Configuration Manual for the telephone. This makes it possible to search for contacts that include spaces.

2. To add several rows click **Add** again.
3. Click **Save**.

Sorting of phonebook

The entries in the phonebook can be sorted on Last Name, First Name or Number.

1. On the start page, click **Phonebook**.
2. Enter User name and Password and click **OK**. The **Edit phonebook** page appears.
3. To sort the entries, click on the arrows in the list's title bar.

Deleting a single entry

Entries in the phonebook can be deleted in the following way:

1. On the start page, click **Phonebook**.
2. Enter User name and Password and click **OK**. The **Edit Phonebook** page appears.
3. In the **Edit Phonebook** page, locate the entry to be deleted. Click the button in the same row.
4. Click **Save**. The entry is deleted.

Deleting All

All entries in the phonebook can be deleted by clicking the **Delete All** button.

1. On the start page, click **Phonebook**.
2. Enter User name and Password and click **OK**.The "Edit phonebook" page appears.
3. In the **Edit Phonebook** page, click **Delete All**. It is now possible to mark entries not to be deleted by clicking on the blue arrow, ( ). If the blue arrow icon is clicked, it disappears and a red is displayed.
4. Click **Save**. All entries marked with a blue arrow are deleted. The entries that are marked are kept.

Operation

The user accesses the phonebook by sending a message from the telephone. The message includes a search query containing part of the first name and/or the family name, or phone number, see below.

You want to search for:	Text to be entered:
First name or Family name	<Part of name>
First and Family name	<Part of first name><space><Part of family name>
First name only	<Part of first name><space>
Family name only	<space><Part of family name>
Telephone number	<Part of number>

Some telephones have separate fields for these entries.

By part of name means the first characters of the name and by part of number means the last digits of the number. If no message text is entered the AIWS will return a failure.

1. Enter the text and send it to the phonebook with the specified address (number).

   The search result is sent back to the telephone as an message. If more than one number that matches the query is found, the result is displayed as a list of names.

   Note:

   A central phonebook search will only show the first 25 entries (if more matches available) in the cordless telephone. User needs to narrow down the search string to get not displayed entries.

2. Select a name and press the Call key to dial the number. See also the documentation for the telephone that is used.

Searching examples

You want to search for:	Text to be entered:	Search result:
First name or Family name	S M	All names that start with *Sm*, both first names and family names.
First and Family name	L ␣ B	All entries where the first name starts with L and the family name starts with B.
First name only	A N ␣	All first names that starts with *An.*
Family name only	␣ A N	All family names that start with *An*.
Telephone number	2 0 0	All telephone numbers that end with 200.

Note:

The ␣ character indicates a space.

Importing and exporting a phonebook

Importing entries to the phonebook from a CSV File

The CSV file to be imported to the phonebook shall have the following format using a semicolon, a comma or a TAB as a delimiter, i.e.:

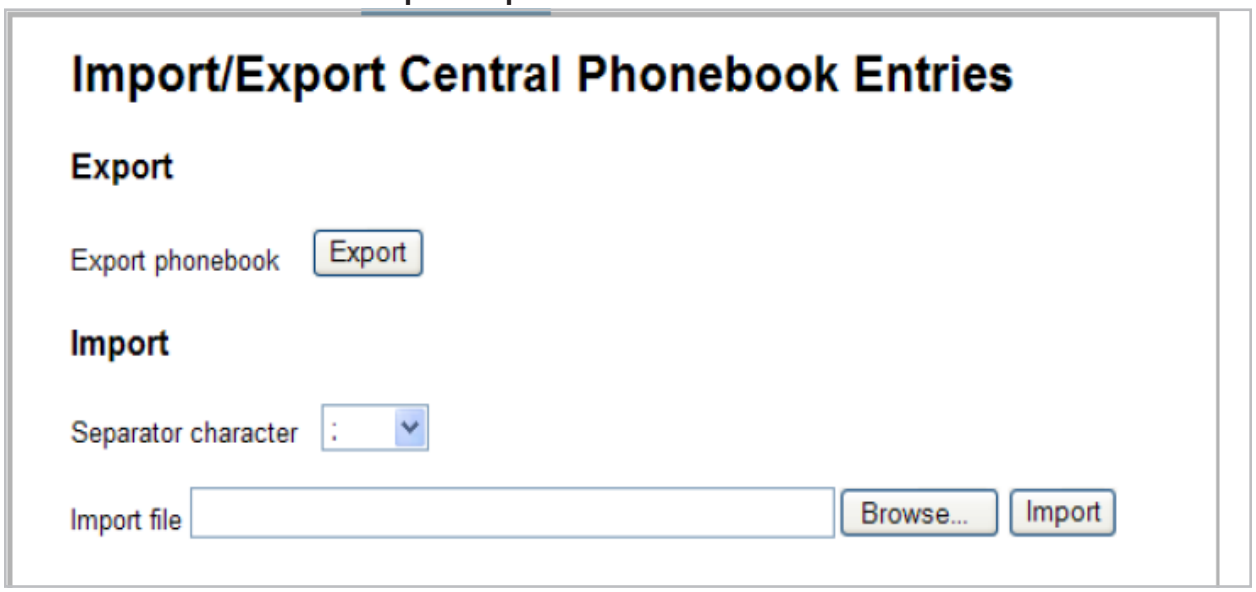
```
First name 1;Last name 1;Phone number 1
First name 2;Last name 2;Phone number 2
```

Note:

If the Central phonebook contains first names and/or last names that include spaces, Avaya recommends enabling the **Central Phonebook Allows Space** parameter for the handset in WinPDM or Device Manager in AIWS. See the corresponding Configuration Manual for the telephone. This makes it possible to search for contacts that include spaces.

WARNING:
When importing a phonebook file in CSV format, existing entries are deleted.

1. Click **Phonebook** on the start page.
2. Enter ***User name*** and ***Password*** and click **OK**. The **Edit Phonebook** page appears.
3. Select **Phonebook > Import/Export** in the left menu.



4. Click **Browse** to locate the CSV file in the system.
5. Select the delimiter (TAB, comma or semicolon) used in the CSV file.
6. Click **Import**.

Exporting the phonebook to a CSV File

The complete phonebook can be exported to a CSV file for example for editing or backup reasons.

1. Click **Phonebook** on the start page.
2. Enter ***User name*** and ***Password*** and click **OK**. The **Edit Phonebook** page appears.
3. Select **Phonebook > Import/Export** in the left menu.
4. Click **Export**.

5. Click **Save** in the dialogue window that appears.
6. Enter a ***name*** of the file and select in which ***folder*** the file should be saved.
7. Click **Save**.

Device Management

Device management in the AIWS/AIWS2 can be done through the chargers. The charger is by default configured to connect to the network using DHCP. If DHCP is not used in the network, a static IP address has to be configured.

Device management in network not using DHCP

1. Connect each charger via USB to a PDM Windows Version.
2. In the PDM Windows Version, click the "Number" tab.
3. Select charger in the Device types column.
4. Double-click in the Number column.
5. Select Network > IP > Charger IP Address.
6. Click the Value field for changing the IP address.
7. Disconnect the USB port(s) and connect the desktop charger(s) (DC4) or the rack charger (CR3) via the Ethernet port(s) to the network.
8. Start the Device Manager in AIWS2.
9. Place the telephone in a charger that is connected to the AIWS2. The telephone can either be turned off or turned on when placing it in the charger. A telephone that is turned off will start up automatically and the battery charging symbol will be displayed.

Device management in network using DHCP

1. Connect a desktop charger (DC4) or a rack charger (CR3) via the Ethernet port to the network.
2. Open a web browser and enter the URL to access the AIWS2.
3. Place the telephone in a charger that is connected to the AIWS2. The telephone can either be turned off or turned on when placing it in the charger. A telephone that is turned off will start up automatically and the battery charging symbol will be displayed.

Device management over-the-air via IP-DECT

There is no external equipment needed besides AIWS2 and IP-DECT.

Device Management in Multiple Systems

When using a device in multiple systems, it is possible to determine in which system the device shall be synchronized with the Device Manager in AIWS2. This means that software upgrade and configuration of the telephone only will be applied when it is present in the system where the telephone shall synchronize with the Device Manager.

The default setting depends on two conditions:

- If a telephone has a valid subscription and is upgraded to software version 3.3.x or greater, the default setting will be that the telephone synchronizing with the Device Manager in all systems.
- If a telephone has no subscriptions and you subscribe it towards the first system, the default setting will be that the telephone synchronizing with the Device Manager in that system (that is System A).

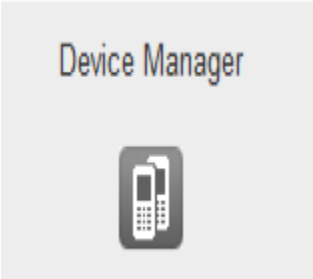
Note:

When changing the "Device Management system" parameter to another system, the handset will lose the connection to the IP-DECT system for a few seconds.

1. In the PDM Windows Version or Device Manager in AIWS2, select the **Number** tab.
2. Select the device to be configured.
3. In the Number menu, select **Edit parameters**. A dialog window opens.
4. Select **Systems**.
5. In the Device Management System drop-down list, select the system to be used for device management.

Device Manager

Figure 103: Device Manager button on AIWS start page



Device Management is the general term of managing devices. Centralized Management implies that devices are managed from a central application. The Centralized Management concept gives several advantages when administrating devices.

Centralized Management makes it possible to handle parameters and software for devices on-site on a central workstation or remotely.

The Device Manager can manage large sets of devices and contains a solution for:

- Centralized software upgrade on a set of devices
- Centralized configuration of devices
- Central database storage for all device settings
- No need to collect all devices when upgrading software or changing settings

This section gives a description of the Device Manager in AIWS and how it is intended to be used.

In the Device Manager much of the work is done with Devices, Numbers and Templates. A Device can be a telephone, a charger etc. A Number consists of the parameters belonging to a certain device. A Template can be used to set parameters that are common for several devices of a certain device type. The template can later be applied to a certain Number.

Ensure that the Device Manager is configured to communicate with the interface (for example IP-DECT) the devices are connected to. If not, the devices will not appear in the Device Manager. See Device Management setup on page 461

Device Manager description

Device Manager terminology

This section gives a brief description of the core terminology in the Device Manager.

- Device; can be a charger, a handset, or a fixed device (such as IP-DECT base station) that can be connected to the module..
- Number; the complete settings for a single device.
- Template; general settings for a specific device type. A template can be applied to several Numbers of the same device type.
- Tabs; in the Device Manager there are three different views, or tabs. In these tabs, the information for devices, Numbers and templates are shown. Some information is shown in two tabs.
- Parameter definition file; a file including all possible settings for a certain device type. Templates are created from parameter definition files.
- Software; is the software used in devices. The device software can be updated via AIWS.
- Version; parameter definition files and device software are indicated by versions.
- Package file; a file that can contain other files, such as parameter definition files, software files and template files.
- Importing; different types of files can be imported. Note that if a software file should be imported, it may have been delivered in a package file.
- Associate; before being able to synchronize parameters between AIWS and devices, it is necessary to associate a Number with the device. Association includes all parameters. If it exists on that device type, it also includes Contacts.
- Assign; it is possible to assign a Number to a device that has not yet been assigned a Number in the Device Manager. Assign includes only the parameters defining the Number.

Device Manager usage

This section gives a short description to give a basic understanding on how to use the Device Manager with devices.

This description is intended to be used to get a basic understanding of the work flow and is not intended to be followed in work.

- Import a parameter definition file of the corresponding device type to AIWS.
- Create a template from the parameter definition file.
- Add a device to Device Manager[1].

1. Not applicable for fixed devices.

- Create a new Number for the corresponding device type[1].
- Associate the Number with the device.

Refer to the following chapters for a description.[1]

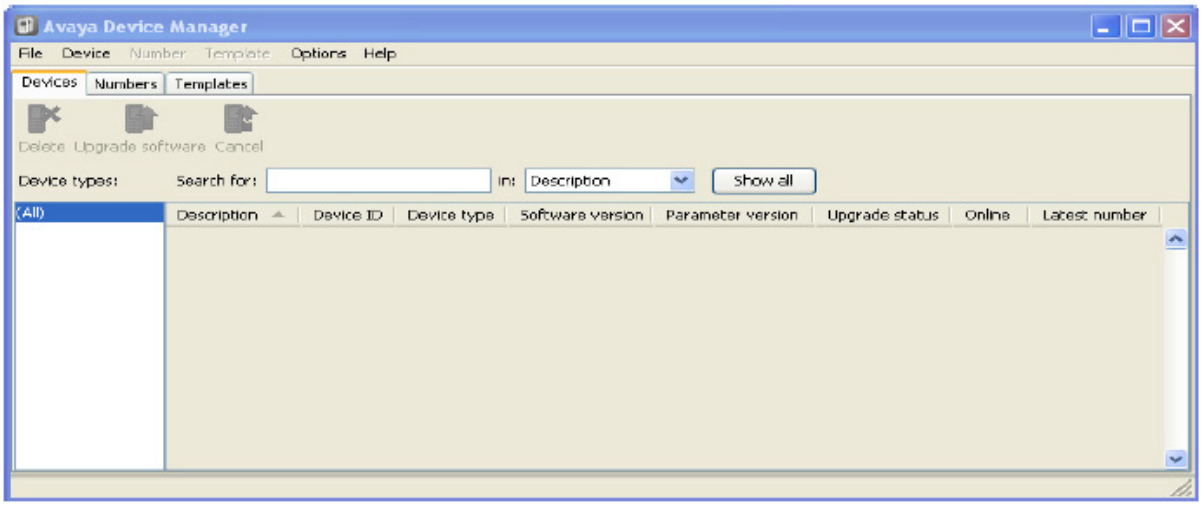
The Device Manager

AIWS is opened in a web browser by typing the IP address of AIWS in the address bar. Then click **Device Manager** to reach the Device Manager GUI.

The **Device Manager** window consists of three areas: **Menu**, **Toolbar** and **Work Area**. The Toolbar has three tabs: **Devices**, **Numbers** and **Templates**. When one of these tabs is selected the available devices types will be shown in the left hand pane of the work area. The right hand pane shows the devices, numbers or templates which have already been configured.

In the upper part of the Work area there are search fields where different search criteria can be selected depending on which tab that is displayed.

Figure 104: Device Manager window areas



Sorting the list

By default the lists in **Devices**, **Numbers**, and **Templates** are sorted by Device ID, Number ID, and Name respectively. To sort the list by any other column, click on the appropriate column heading. To reverse the sort order, click on the column heading again. The sorting order is indicated by an up or down arrow in the column heading.

Filtering the list

By default the list in each tab shows all available Devices, Numbers, or Templates. It is possible to filter the list by selecting the desired device type in the **Device types***:* column in the left pane.

Color coding

General color coding

This color coding is valid for the lists under the tabs:

- If the version number is shown in red, the Device Manager has found no parameter definition files supporting that device type.
- If the version number is shown in dark red, the parameter definition file is compatible, but does not have exactly the same version as the device.

Color coding for parameter and template editing

In the parameter and template editing windows, the following color coding is used:

Color	Context	Description
Black	General	Normal
Dark blue	For templates and parameter editing	Parameter has been edited during the current session
Purple	For templates	The parameter is included in the template (checked)
Red	For templates and parameter editing	Value not valid
Turquoise	For templates and parameter editing	The value differs from the default value

Navigation

For keyboard shortcuts, see Device Manager Keyboard Shortcuts on page 516.

Tabs

The information in AIWS is shown in different views, or tabs:

- Devices tab
- Numbers tab
- Templates tab

In each of these tabs, specific information is shown in lists about devices, Numbers, or templates. Some of the information overlaps, for example Device ID, which is tied to both a specific device and to a specific Number.

The operations that can be done in the Device Manager are done from these tabs and from the menu. Different menus are accessible in the different tabs.

Devices tab

Select the **Devices** tab. The view shows all devices configured at the site in a detailed list. The following columns are displayed on each row:

- *Description – (AIWS2 only) individual description of the device valid for the device tab only that can be added by the administrator.*
- *Device ID* – the unique identifier of the device
- *Device type* – the device model
- *Software version* – shows the version of the software in the device
- *Parameter version* – shows the version of the parameters in the device
- *Upgrade status* – show one of the following icons

  software upgrade in progress.
  
  It is also possible to see a progress bar when the device is being upgraded.

  
  software upgrade Pending, Request sent, or Accepted (a green arrow).

  
  software upgrade Scheduled or Retrying.

  
  - the last upgrade Failed or Aborted (a red broken arrow).
  - device busy, operation cannot be executed because handset is not in idle state. Please bring handset back to idle state to start the operation. Sometimes a restart of the PDM application is needed to get the proper status update for this handset.

  "Completed", no icon is shown

Note:

A software upgrade from AIWS should be done on one device to start with. If successful, the remaining devices can be updated in one operation.

- *Online* – shows if the device is connected to the Device Manager. The ✓ icon indicates a connected device.
- *Latest Number* - shows the Number ID that the device had during its last login.

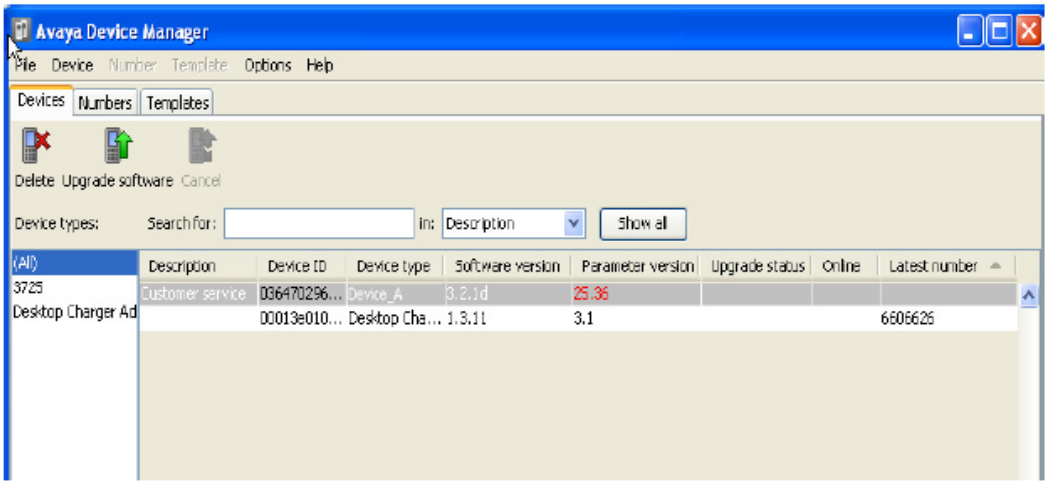
Note:

A handset can be online when connected over the air or plugged into an advanced charger.

Advanced Chargers and Rackmount Chargers will be online when connected to the Ethernet

There is a certain time out of a view hours, so it's not mandatory that the device is still online.

Figure 105: The Devices tab showing a list of devices in a system

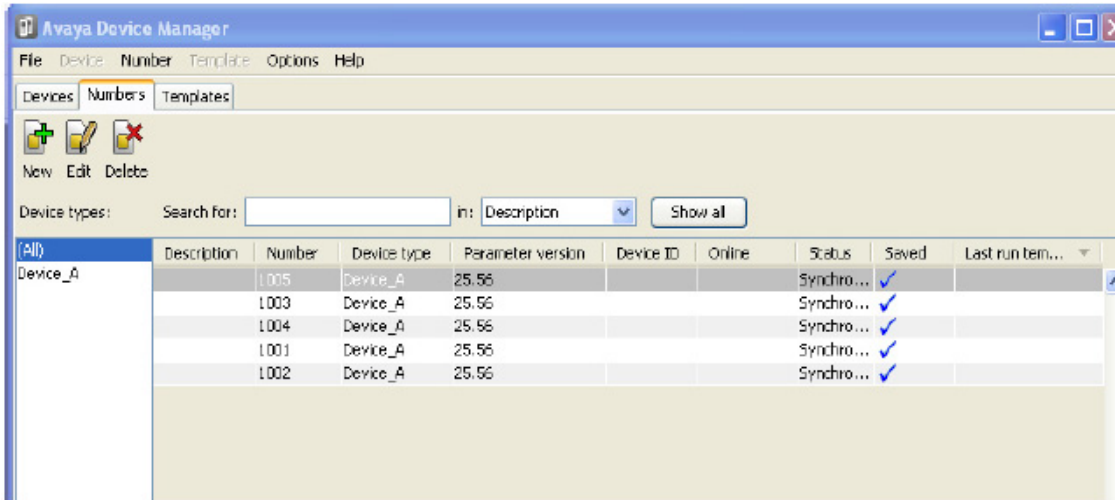


Numbers tab

Select the **Numbers** tab. The view shows all Numbers configured at the site in a detailed list. The following columns are displayed on each row:

- *Description – (AIWS2 only) individual description of the device valid for the numbers tab only that can be added by the administrator.*
- *Number* – the unique identifier of the Number. The identifier is unique for that device type.
- *Device type* – the device model the Number is intended for
- *Parameter version* – shows the version of the parameters in the Number
- *Device ID* – the unique identifier of the device that the Number is associated to
- *Online* – shows if the device the Number is associated to is online. The ✓ icon indicates an online device
- *Status* – shows the parameter synchronization status. A Number can also be queued for synchronization. Several different indications are used, for example Synchronizing, Sync queued, Save queued, Synchronized, etc.
  When the Number is offline, the database status is shown; Synchronized or Not synched.
- *Saved* – shows if the Number's parameters have been stored in the database. The ✓ icon indicates that the parameters have been stored.
- *Last run template* - indicates which template that was last run for that Number

Figure 106: The Numbers tab showing a list of Numbers in a system



Templates tab

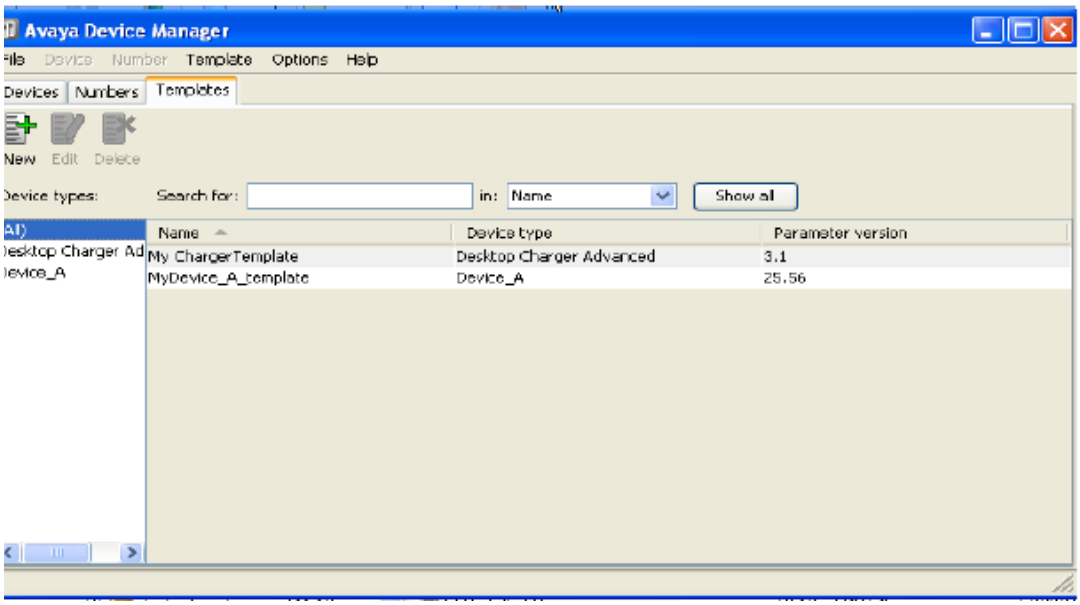
Note:

This tab is not applicable for fixed devices.

Select the **Templates** tab. The view shows all templates in a detailed list. The following columns are displayed on each row:

- *Name* – the name of the template
- *Device type* – the device model the template is intended for
- *Parameter Version* – shows the parameter version

Figure 107: The Templates tab in the Device Manager



Logging on to the Device Manager

Note:

When an attempt is made to start AIWS Device Manager, a popup window is displayed with a warning that the program's digital signature that cannot be verified. The text is displayed in the language used in the computer's operating system. Click **Run** (or the equivalent term in the operating system language).

Note:

Three clients can be logged in at the same time, but to avoid conflicts make sure that only one at a time is updating Numbers.

1. Start a Web Browser. Type the IP address for AIWS.
2. Click on **Device Manager**.
3. Select User ID and enter password, see Authentication Levels and Default Passwords on page 378.
4. Click **OK**. The Device Manager starts.

Closing the Device Manager

In the **File** menu, click "**Exit**". The Device Manager shuts down.

Templates in Device Manager

By using a template, the same configuration can easily be applied to many handsets simultaneously. Templates are also an efficient way to give good control over which changes that are applied to each handset.

Templates enable configuration of all aspects of a handset from sound volume to keypad shortcuts.

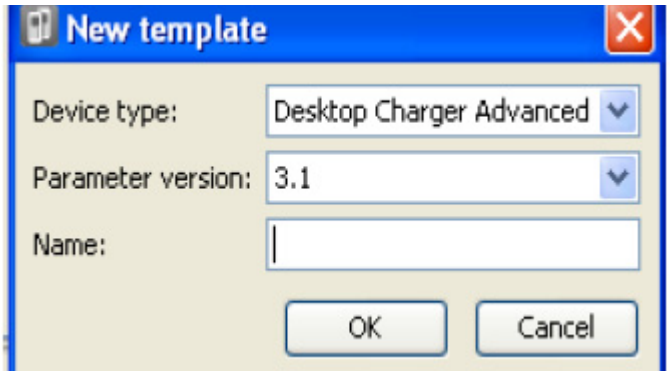
The handset will have full functionality towards the PBX even without such a template. By using such a template, though, the handset will be customized for that PBX with menu options for PBX specific functions such as Callback, call diversion etc.

Creating a parameter template

It is usually desirable to create a customized parameter template that can be applied to all devices of a certain device type.

1. Select the **Templates** tab.
2. In the **Template** menu, click **New**. The **Create Template** dialogue appears.

Figure 108: Create Template dialogue

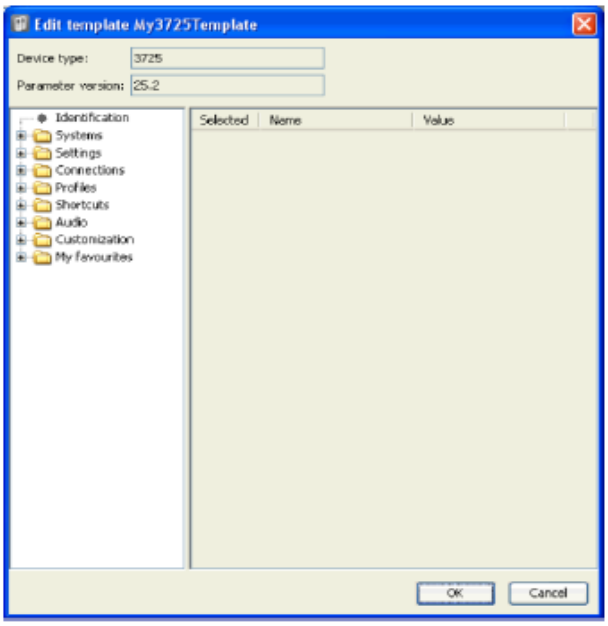


3. Select ***device type*** and ***parameter version***, type in a ***name*** for the template, and click **OK**. The view switches to the **Edit Template** parameter view.

Note:

If you cannot find your device type and/or parameter version in the list, the Device Manager needs to be updated with new parameter definition files, see Importing parameter definition files on page 427

Figure 109: Edit Template parameter view



4. Select the parameters you want to be saved in the template by selecting the check box to the left of each parameter.
5. Change the parameters to the desired values.
6. Click **OK**.

Creating a parameter template from a number

It is also possible to create a template from a Number in the Device Manager.

1. Select the **Numbers** tab.
2. Mark the ***Number*** you want to use.
3. Right click on the ***Number*** and select **Use as template...**
   The **Enter template name** dialogue opens.
4. Enter a ***name*** for the template.
5. Click **OK**.
6. The **Edit template** dialogue opens. Continue with 4 to 6 in Creating a parameter template on page 405.

Note:

When the **Edit template** window is opened from the **Use as template** command, an extra drop-down list, **Select** is shown in the bottom left corner. This setting decides which parameters that shall be copied from the Number. If **All parameters** is selected, the synchronization time will be longer.

It is also possible to create a template from a portable that is online but not stored in the database. The template will contain all parameters for the device except for those that are Number specific.

Saving a device configuration as a template

It is possible to use an already configured device and save it as a template. The template will contain configuration data and will not include contacts and other personal data if it is a handset.

This template can be used as a backup if you later want to restore the configuration of the device, or as a template to be applied on a number of devices.

1. Some parameters are user specific. If you want to apply this type of template to several handsets, Avaya recommends you to exclude the following parameters:
   - **Owner ID** - A text string specified in standby mode. The parameter is located directly Under "**Settings**".
   - **Phone lock PIN code** - The security code used to unlock the keypad. The parameter is located under under **Settings > Locks**.
2. Open the **Device Manager**.
3. Select the Numbers tab and select the handset you want to save as a template.
4. Right-click and select "**Use as a template...**". Enter a descriptive name for the template.
5. The **Edit template** window is opened. By default, all parameters are selected and are saved when clicking "**OK**". If one or more parameters should be excluded, remove them by clearing the checkbox next to the parameter.
6. Click "**OK**".

Note:

When the Edit template window is opened from the "Use as template" command, an extra drop-down list is shown in the bottom left corner. This setting decides which parameters that shall be copied from the Number. If "All parameters" is selected, the synchronization time will be longer. It is also possible to create a template from a handset that is online but not stored in the database. The template will contain all parameters for the device except for those that are Number specific.

Renaming a template

1. Select the **Templates** tab.
2. Select the template you want to rename. The selected row is highlighted.
3. In the **Template** menu, select **Rename...** or right click and select **Rename...**. The **Rename template** dialogue opens.

4. In the **Rename template** dialogue, enter a new name in the **New name** text field.
5. Click **OK**. The **Rename template** dialogue closes and the new name appears in the list in the **Templates** tab.

Copying a template

1. Select the **Templates** tab.
2. Select the template you want to copy. The selected row is highlighted.
3. In the **Template** menu, select **Copy...** or right click and select **Copy...**. The **Copy template** dialogue opens.
4. In the **Copy template** dialogue, enter a new name in the **New name** text field.
5. Click **OK**. The **Copy template** dialogue closes and the new template appears in the list in the **Templates** tab.

Editing a template

1. Select the **Templates** tab.
2. Select the template you want to edit. The selected row is highlighted.
3. In the **Template** menu, select **Edit...** or right click and select **Edit...**. The **Edit template** window opens.
4. In the **Edit template** window, edit the parameters that shall be edited.
5. Click **OK**. The **Edit template** window closes.

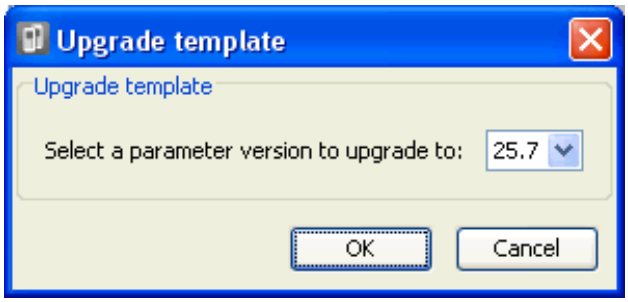
Deleting a template

1. Select the **Templates** tab.
2. Select the template you want to delete. The selected row is highlighted.
3. In the **Template** menu, select **Delete**, or right click and select **Delete**, or press the Delete button. The **Delete template** dialogue opens.
4. Click **Yes**. The **Delete template** dialogue closes and the template is deleted.

Upgrading a template

1. Select the **Templates** tab.
2. Select the template you want to upgrade. The selected row is highlighted.
3. In the **Template** menu, select **Upgrade...** or right-click and select **Upgrade...**. The **Upgrade template** dialogue appears.

Figure 110: The Upgrade template dialogue.

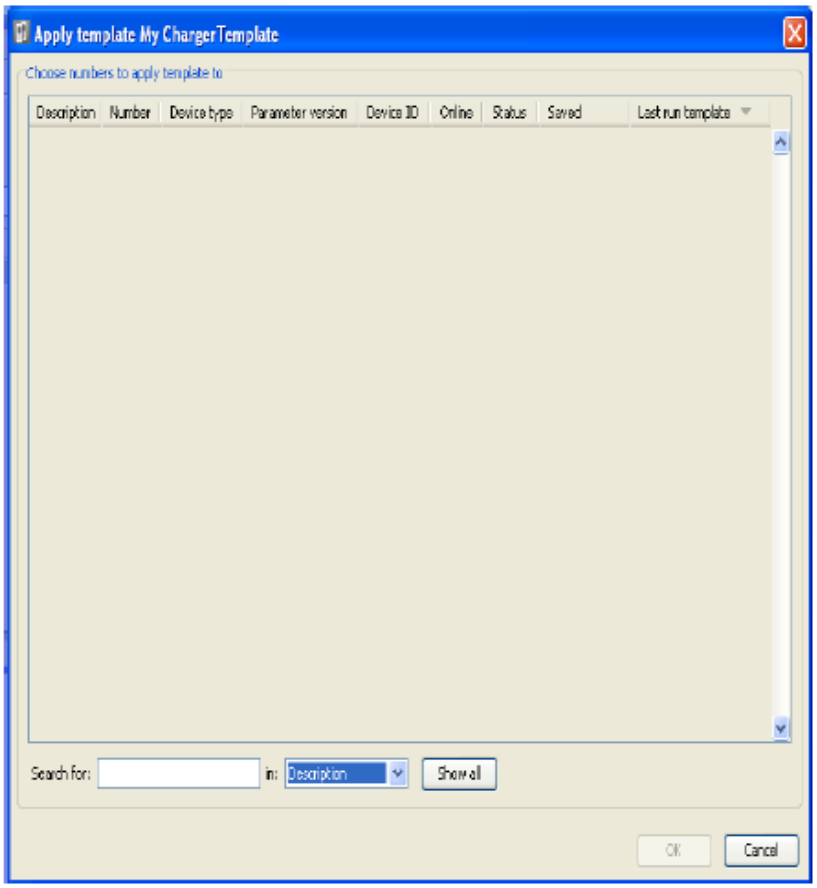


4. Select the parameter version to upgrade to.
5. Click **OK**. The template is upgraded and the dialogue closes.

Applying a template

1. Select the **Templates** tab.
2. Select the template you want to use. The selected row is highlighted.
3. In the **Template** menu, select **Apply to...** or right-click and select **Apply to...**. The **Apply template** window appears.

Figure 111: The Apply template window.



4. If needed, select search parameters or click **Show all**.
5. Select Number(s) to apply the template on.
6. Click **OK**.The template is applied and the window closes.

Numbers

Note:
Templates are not applicable for fixed devices.

Creating new numbers

1. Select the **Numbers** tab.
2. From the Number menu, click **New...**. Alternatively, right-click in the **Numbers** list and select **New...**. The **New Numbers** dialogue opens.

3. Select device type in the **Device type** list.
4. Select the parameter version in the **Parameter version** list. All parameters except Number specific parameters will be set to their default values.
5. Select which template to run on the Number. This is optional at this stage and therefore **None** can be selected.
6. If you want to create a single Number, select the **Single** option and enter the call number in the **Call number** text box. It is recommended to use the telephone extension of the handset as the number in the AIWS.
7. If you want to add a range of Numbers, select the **Range** option. Enter the start call number in the **Start call no.** text box, and the end call number in the **End call no.** text box.

   Note: The maximum range that can be added at a time, is 100 Numbers.
8. Click **OK**. The dialogue closes and the new Numbers show up the list in the Numbers view.

Note:

If you try to add more numbers than allowed, the following dialogue window appears, see below.

Figure 112: Dialogue window, maximum numbers allowed (example)



Saving a number to Database

An online device can be saved to the database.

1. Select the **Numbers** tab.
2. Select the Number.
3. In the **Number** menu, select **Save**. Alternatively, right-click the Number and select **Save**.

Note:

An online device can automatically be enabled and saved (default), see Automatically enabling new devices settings on page 438 for more information.

Parameter transfer between a device and the Device Manager

When a device is connected, it is synchronized with the associated Number in the Device Manager, see Synchronizing a device on page 418.

Note:

When parameters have been edited and the device is synchronized, only the edited parameters will be sent to the device.

Editing Parameters

The **Edit Parameters popup** window shows the set of parameters relevant to the Number that is being edited. The parameter groups are organized in a tree structure in the left pane, with the parameters in the current node in the right pane. The parameter list has one column with the parameter name, and another column gives the parameter value. This can be for example a numerical value, a boolean value, or text. Clicking in the column will give a short description of the selected parameter.

1. Select the **Numbers** tab. The **Number** view appears.
2. Select the Number. The selected row is highlighted.
3. Click **Edit** in the **Number** menu. Alternatively, right-click and choose **Edit**, or double-click on the Number.

   The **Edit Parameters for <Number>** window opens, where <Number> is the ID of the current Number.
4. Select parameter in the left pane.
5. Make your changes on the **Value** row.

   When a parameter has been edited, the name of the node to which the parameter belongs changes to a blue color.

   (Click **Cancel** if you want to undo all parameters edited since your last save and return to the main window.)
6. Click **OK** to save your changes.

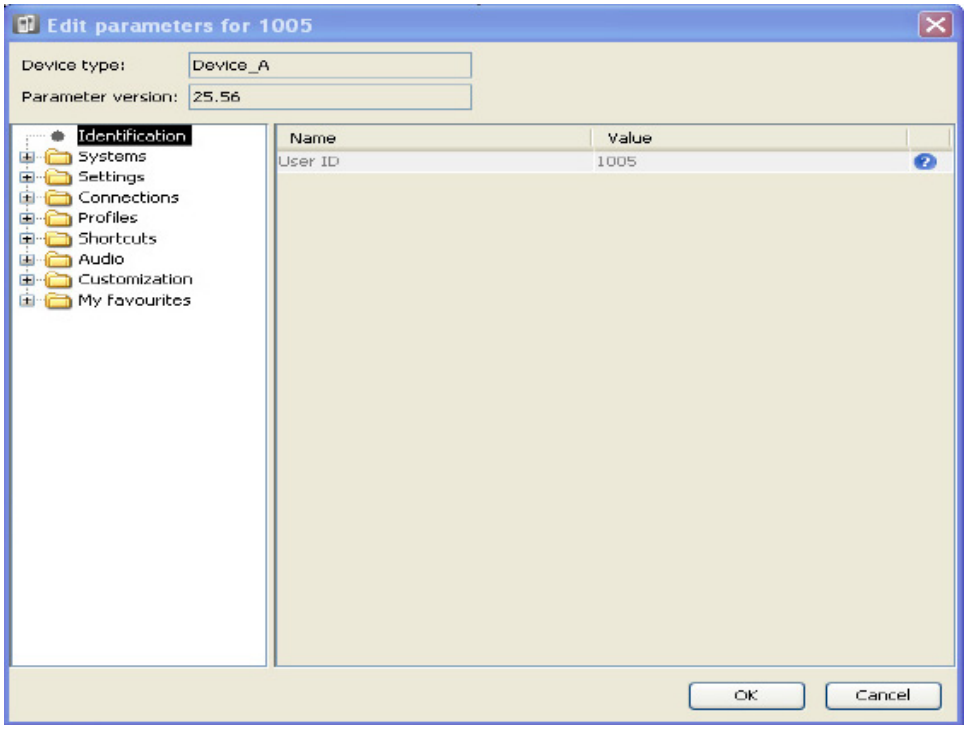
Note:

If the Handset is used on an Integral system only the sound and alert settings for:

- - Vibrating alert: on, off
- - key sound: click, tone, silent
- - ring type: normal short silent

will be valid. Other settings are ignored. This is also valid when configuring profiles.

Figure 113: Editing parameters in AIWS GUI



Note:

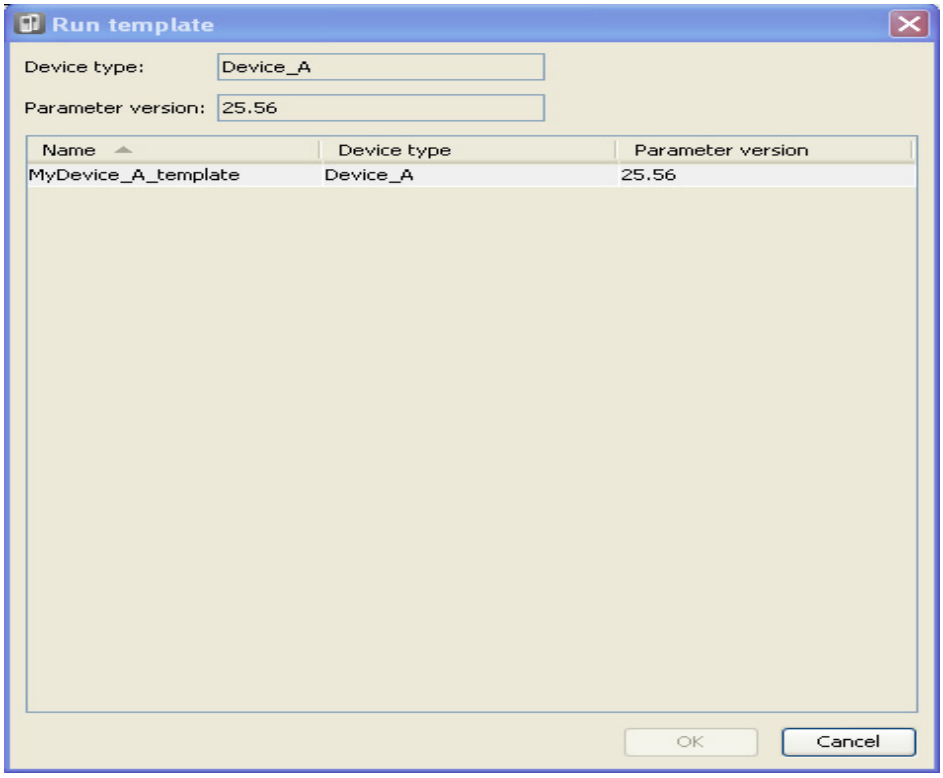
When you save the parameters, they are automatically sent to the device if it is online.

Running a template to set parameter values

If a template has been created for a device type, it can be used to set the parameter values for a range of devices, or a single device. The command to use is Run template.

1. Select the **Numbers** tab. The **Number** view opens.
2. Select the Number(s) you wish to run the template on.
3. In the Number menu, click **Run template...**. Alternatively, right-click on the Number in the **Number** list and select **Run template...** from the menu that appears. The **Run template** window appears.

Figure 114: Selected template to run on one or several Numbers



4. Select a template from the **Template** list.

   Note:
   If multiple templates are selected only one of them will be executed.

5. Click **OK**.

   If the parameters in the database have been edited but not yet sent to the device it is indicated with **Not synched** or **Updated queued**.

If the Number has not been associated with a device, it is now possible to do so. Connect a device and associate it with a Number in the database. The parameters will automatically be sent from the Device Manager to the device. See Associating a number with a device on page 414.

Associating a number with a device

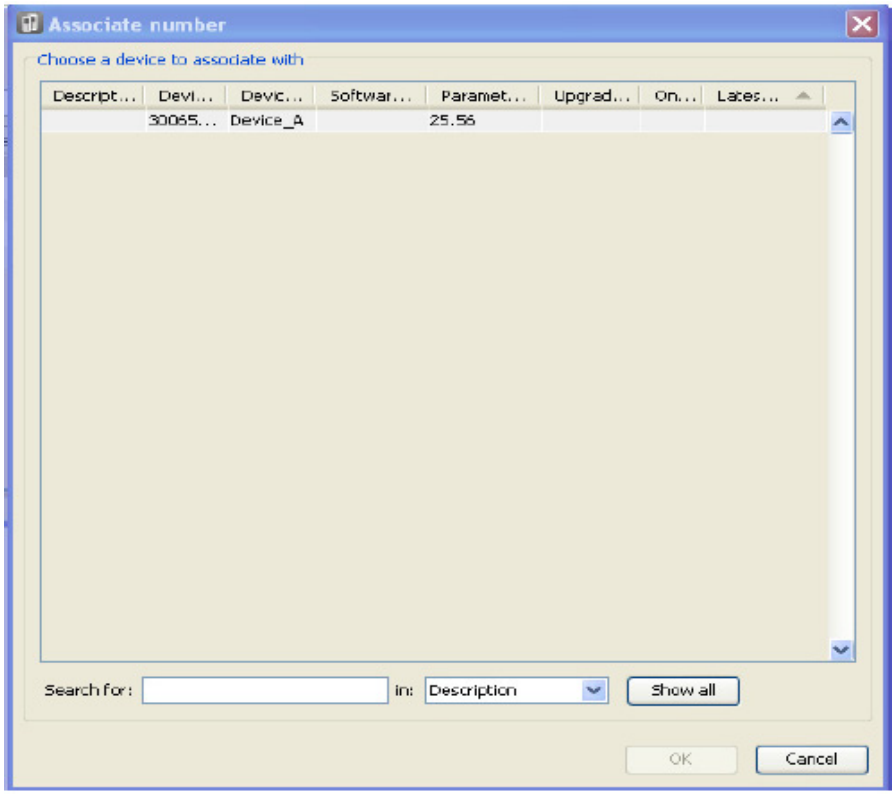
Before being able to synchronize parameters between AIWS and devices, it is necessary to associate a Number with the device. It is possible to enter several Device ID's in advance and to associate them with a Number at a later moment.

See also Assigning a number to a device on page 420 and Adding a new device on page 419.

1. Select the **Numbers** tab.

2. In the **Number** menu, select **Associate with device...**. The **Associate Number** dialogue opens.

Figure 115: Associate number dialogue



3. Select the device you want to associate with in the list and click **OK**.
4. Click **OK**.

If the selected device is online, it will immediately be updated with the selected Number. If the selected device is not online, it will be updated the next time it is online.

It is possible to associate several Numbers with several devices simultaneously.

Deleting a number in the site database

1. Select the **Numbers** tab.
2. Select the Number you want to delete. The selected row is highlighted.
3. In the **Number** menu, select **Delete** or right click and select **Delete**.
4. Click **Yes** in the **Delete Number** dialogue.

The dialogue closes and the Number is deleted from the list.

Renaming a number

1. Select the **Numbers** tab.
2. Select the Number you want to rename. The selected row is highlighted.
3. In the **Number** menu, select **Rename...** or right click and select **Rename...**. The **Rename number** dialogue opens.
4. In the **Rename number** dialogue, enter a new Number in the **New number** text field.
5. Click **OK**. The **Rename number** dialogue closes and the new Number appears in the list in the **Numbers** tab.

Copying a number

1. Select the **Numbers** tab.
2. Select the Number you want to copy. The selected row is highlighted.
3. In the **Number** menu, select **Copy...** or right click and select **Copy...**. The **Copy Number** dialogue opens.
4. In the **Copy number** dialogue, enter a new Number in the **New number** text field.
5. Click **OK**. The **Copy number** dialogue closes and the new Number appears in the list in the **Numbers** tab.

Importing contacts

Note:
The number for the handset must be saved, see Saving a number to Database on page 411.

Import contacts from file

A file containing contacts can be imported to AIWS and synchronized with a handset. This feature enables transfer of contacts from older types of handsets. The file is created using the Local_Phonebook_Tool.xls tool.

Important:
When importing a local phonebook file, the local phonebook entries (if any) in the cordless telephone will be deleted and replaced by the entries in the file.

1. In the Device Manager, select the **Numbers** tab.
2. Select a number.
3. In the **Number** menu, select **Import contacts** > **From file**. Alternatively, right-click the Number in the Number list and select **Import contacts** > **From file** from the menu that appears.

4. Find and select a file containing contacts and click **Open**.

The contacts in the imported file are synchronized with the cordless telephone.

Import contacts From number

This feature enables transfer of contacts from one handset to another handset that has been saved in the Device Manager.

Important:
When importing number, the local phonebook entries (if any) in the cordless telephone will be replaced by the imported numbers.

Note:
Company phonebook contacts included in the Call contact list are not transferred to the other cordless telephone using this feature. To upload the Company phonebook, see Uploading a company phonebook on page 433.

1. In the Device Manager, select the **Numbers** tab.
2. Select a number.
3. In the **Number** menu, select **Import contacts** > **From number**. Alternatively, right-click the Number in the Number list and select **Import contacts** > **From number** from the menu that appears.
4. Select a number.
5. Click **OK**. The contacts are now imported to the handset.

Devices

A device can be a DECT telephone, a Rackmount Charger or an Advanced Charger developed to work together with the Device Manager. See the user manual for respective portable.

All work with devices is performed from the **Devices** view.

- Devices can be added by connecting the device to the system. or use the **Add device** function.
- It is possible to transfer the information for a Number from one device to a new device.
- Devices can be reset to factory settings.
- Devices can be updated with new software.

Adding devices

Note:

Before connecting a device to the Device Manager, make sure the connection is set up according to the instructions in the device´s *User Manual*.

If a range of new devices are to be added, the easiest way is to:

1. Create a template with all common parameter settings. See Creating a parameter template on page 405.
2. Add a range of Numbers and run the template. See Creating new numbers on page 410 and *Running a template to set parameter values*.
3. Edit the parameters and change individual settings. See Editing Parameters on page 412.
4. Connect the devices and associate them with the Numbers in the database. See Associating a number with a device on page 414.

A single device can be added in the same way.

Note:

It is not possible to change model of a device already added to the site. Instead, a new device of the desired model must be added to the site and the parameters set to the correct values.

Synchronizing a device

Note:

This feature is not applicable for fixed devices.

When parameters have been changed in a device, the device is synchronized with the Number saved in the database. When a device is being synchronized, parameters that have been changed in the device are uploaded to the Device Manager, and parameters that have been changed in the Device Manager are sent to the device. If a parameter has been changed in both the device and the Device Manager, the setting made in the Device Manager will take precedence.

1. When a device is connected to the system running the Device Manager, and if the Number is saved, and it has a parameter definition, the device is automatically synchronized.

   While synchronizing, a progress bar and a text is shown in the Numbers view.

Note:

Due to hardware limitations in the 3720 telephone the device might be busy for parameter synchronisation, e.g. during a call.

Deleting a device

1. Select the **Devices** tab.

2. Select the device you want to delete. The selected row is highlighted.
3. In the Devices menu, select **Delete** or right click and select **Delete**.
4. Click **Yes** in the **Delete Device** dialogue.

The dialogue closes and the device is deleted from the list.

Note:
You cannot delete a device that is online.

Replacing a device

Note:
This feature is not applicable for fixed devices.

If a device shall be replaced with a new device, it is possible to transfer its associated Number including settings to a new device. The new device must be of the same device type as the old one.

1. If the device to be replaced is still working, make sure that it is synchronized.
2. Shut off the old device or make a factory reset.
3. Connect the new device to the Device Manager.
4. Associate the new device to the Number associated to the old device according to the instructions in Associating a number with a device on page 414. The Number will no longer be associated with the old device.

Note:
The subscription data will not be copied by this mechanism, so a handset needs to be subscribed to the IP-DECT system additionally.

Adding a new device

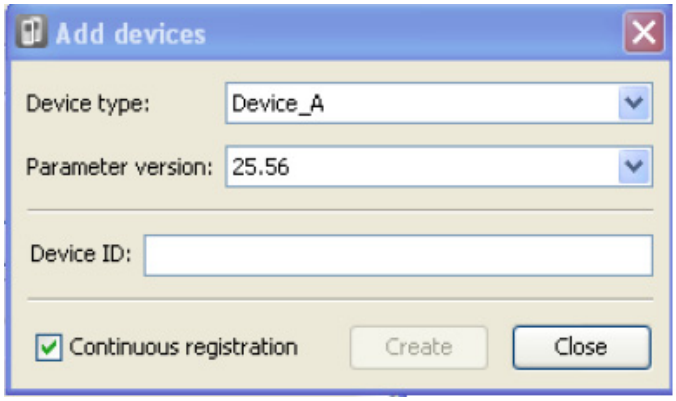
Note:
This feature is not applicable for fixed devices.

It is possible to enter several new Device ID's in advance into Device Manager for later association.

In order to simplify input when handling many devices, it is possible to use a bar code reader. The bar code reader should send a carriage return after each item, but it is not necessary. If carriage return is not sent, it is necessary to click **Create** after each read item.

1. Select the **Devices** tab.
2. In the **Device** menu, select **Add device**. The **Create devices** dialogue opens.

Figure 116: The Create devices dialogue

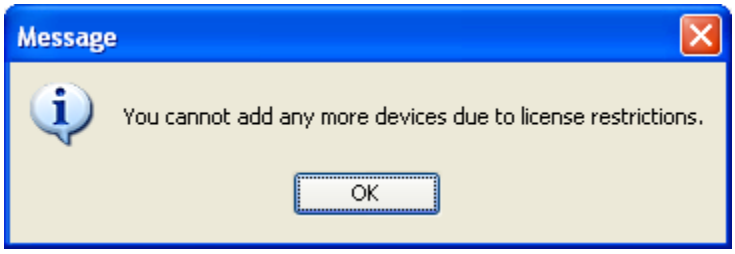


3. Select device type and parameter version.
4. Enter a Device ID for the device manually or by usng a bar code reader.
5. To keep the **Create devices** dialogue open after clicking **Create**, select the **Continuous registration** check box.
6. If the bar code reader does not send carriage return, click **Create**.

Note:

If you try to add more devices than allowed, the following dialogue window appears, see below. For more information, see License restrictions for device handling on page 422.

Figure 117: Dialogue window



7. Repeat 4 to 6 if more devices are to be created, otherwise click **Close**.

Assigning a number to a device

Note:

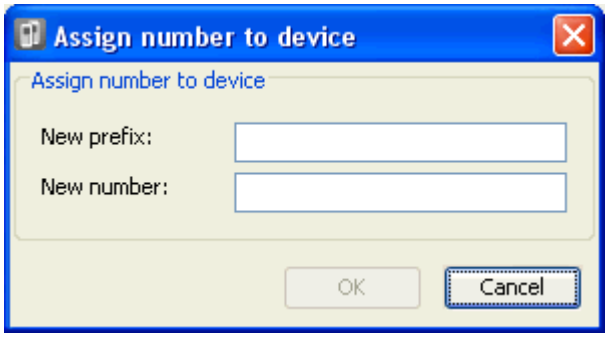
This feature is not applicable for fixed devices.

It is possible to assign a Number to a device that has not yet been assigned a Number in the Device Manager. This feature can be used if parameters have been changed on the device prior to connection to the Device Manager.

Assign a Number to a device shall not be done on a device that already has a number.

1. Select the **Devices** tab.
2. Select the device you want to assign a Number for.
3. In the **Devices** menu, select **Assign number**. The **Assign number to device** dialogue opens.

Figure 118: The Assign number to device dialogue



4. Enter a new number in the **New number** field. Click **OK**.

Note:
The prefix is not used in Avaya systems.

5. The new Number appears in the list in the **Numbers** tab.

Note:
Some devices need to be restarted for the new numbers to be shown.

Factory reset

Note:
This feature is not applicable for fixed devices.

Factory reset means that the device parameters will be reset to factory settings. The Number in the database that is associated with the device will not be affected.

Note:
The device must be online.

1. Select the **Devices** tab.
2. Select the device(s) to be reset.

3. Click **Factory reset** in the **Device** menu. Alternatively, right-click on the device and select **Factory reset**.
4. A message saying **Do you want to reset the selected device(s) to factory defaults?** will appear.
5. Click **Yes**.

License restrictions for device handling

The license for AIWS determines how many devices and numbers that can be added to the Device Manager. See the following scenarios for more information.

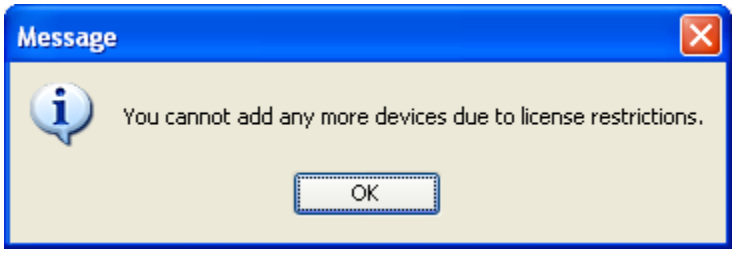
Scenario 1

The AIWS has the license WSM-MVS, AIWS Standard that allows to add 120 devices and 300 numbers.

Allowed Devices and Numbers	Added Devices and Numbers	Remaining Devices and Numbers
120 Devices	110 Devices	10 Devices
300 Numbers	250 Numbers	50 Numbers

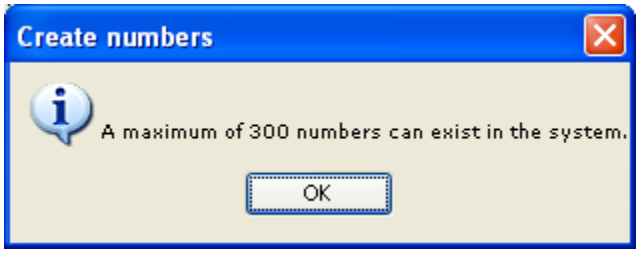
The administrator wants to add 20 devices according to Adding a new device on page 419. When trying to add more devices than allowed, the following dialogue window (see figure 119) appears.

Figure 119: Additional devices cannot be added



The administrator wants to add 60 numbers according to Creating new numbers on page 410. When trying to add more numbers than allowed, the following dialogue window (see figure 120) appears.

Figure 120: Maximum numbers allowed



This issue can be resolved by doing one of the following:

- Adding a license for AIWS that supports additional devices/numbers, see Licenses on page 361.
- Deleting added devices or numbers

Scenario 2

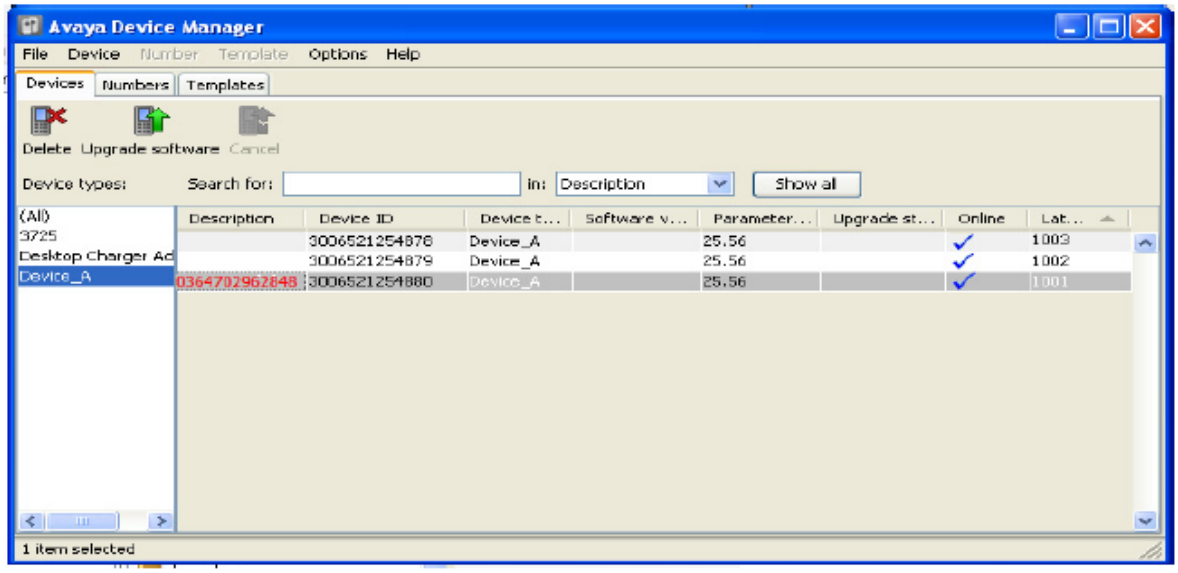
The AIWS has the license WSM-MVS, AIWS Standard that allows to add 120 devices and 300 numbers.

Allowed Devices and Numbers	Added Devices and Numbers	Remaining Devices and Numbers
120 Devices	120 Devices	0 Devices
300 Numbers	300 Numbers	0 Numbers

The number of allowed devices/numbers have been added in the Device Manager. An additional device is registered in the Device Manager by placing it in an advanced charger or using Over-the-Air. This device will automatically be disabled.

In the **Devices** tab, the Device ID of the disabled device is highlighted with red color, see figure 121 on page 424.

Figure 121: Example of an disabled device indicated by a red highlighted Device ID

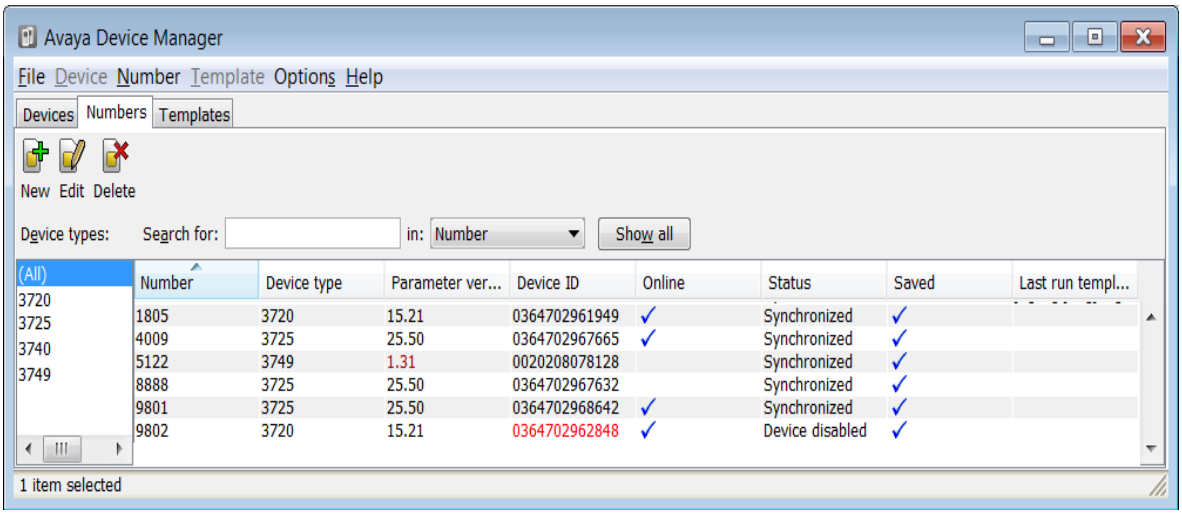


In the **Numbers** tab, the red highlighted Device ID of the disabled device is also displayed. In addition, the status of the device is indicated as Device disabled. See figure 122.

Note:

A device is only visible in the **Numbers** tab if it has a number.

Figure 122: Example of an disabled device indicated by a red highlighted Device ID and the status Device disabled

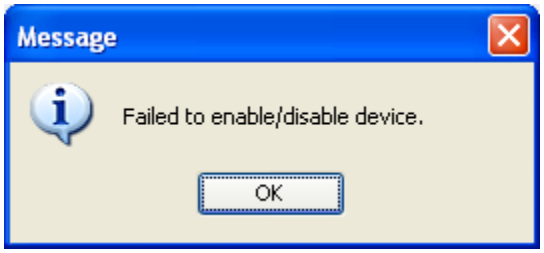


A device that is disabled cannot be configured such as edit parameters, associate with device, import contacts etc. To enable the device, another device must first be disabled or deleted. For more information, see Disabling and enabling devices on page 425 or Deleting and enabling devices on page 425.

Disabling and enabling devices

It is only possible to disable one device at the time, and then enable another device at the time. If you trying to disable two devices after each other, a dialogue window appears (see figure 123 on page 425).

Figure 123: Failed to enable/disable device



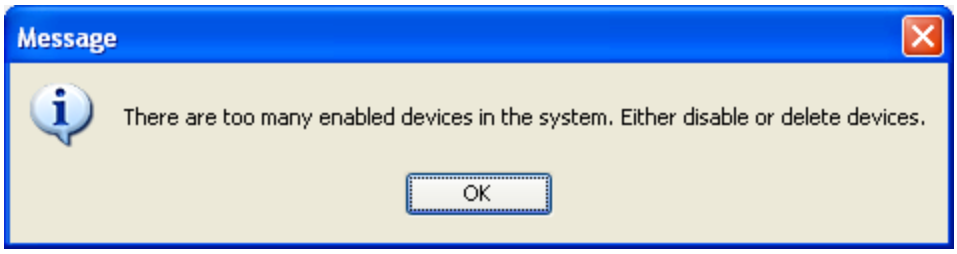
1. In the **Devices** tab, right-click a device to be disabled.
2. Select **Disable device**.

   The Device ID of the disabled device is now highlighted with red color.
3. Right-click a device to be enabled.
4. Select **Enable devices**. The Device ID of the enabled device is then highlighted with black color.
5. Repeat step 2 - 4 to disable/enable additional devices.

Deleting and enabling devices

It is possible to delete devices that are not online, and then enable another devices until maximum allowed devices are reached. If you trying to enable several devices than allowed, the following dialogue window appears (see figure 124).

Figure 124: Too many devices enabled



1. In the **Devices** tab, select the device(s) to be deleted.
2. Right-click and select **Delete**.
3. Select the device(s) to be enabled.

4. Right-click and select **Enable devices**.The Device ID(s) of the enabled device(s) are highlighted with black color.
5. Repeat step 2 - 4 to disable/enable additional devices.

File management

This chapters covers the File management for parameter definition files, software files, language files and phonebook file. Import and export of templates and numbers is described in Importing/Exporting Numbers and Templates on page 437.

Import of translation files is described in Importing translation files on page 481.

The parameter definition file holds the definitions of all parameters for a specific version of a Number's parameter set. Updated software and new parameter definition files for devices and Numbers can be added to the Device Manager, see Importing parameter definition files on page 427 and Importing new software for devices on page 428.

If there is a naming conflict when importing, a warning message is displayed.

Definition File Version – Parameter Version

Both definition files and device software include parameters and are indicated by a version number.

Note:

The version of the definition file matches the version of the device software.

If a device is updated with a new parameter version it does not always demand a new definition file. An old definition file can often be used but if new parameters have been added in the new parameter version, these parameters will not be editable. The release note will tell you if a new definition file is needed to match the new parameters.

There are different parameter versions for different device types.

Example

If a parameter version for a Number is 2.5, then a parameter definition file with a version between 2.0 and 2.5 is required.

Importing a package File

IA package file may include different types of files, such as software files, parameter definition files and/or template files. If the package does not include a certain file, it can be imported seperately. See Importing parameter definition files on page 427, Importing new software for devices on page 428 and/or Importing templates on page 438.

1. In the **File** menu, select "**File management**".

2. Select the **Parameter definition** tab or **Software** tab and click “**Add**”.
3. Select the package file (.pkg) to be imported and click “**Open**”.The files included in the package are now imported. If needed, select the **Parameter definition** tab or **Software** tab to view the corresponding imported files (if any).If template(s) has been imported, it can be viewed by clicking “**Close**“ and then selecting the **Template** tab.
4. Click “**Close**”.

Note:
Parameter definition files (.def) and software files (.bin) may be included in package files (.pkg) or delivered as separate files.

Importing parameter definition files

Updated parameter definition files are distributed by your supplier.

Note:
Parameter definition files (.def) may be included in package files (.pkg).

1. In the File menu, click **File management**. The **File management** window opens.
2. Select the **Parameter definition** tab.
3. Click **Add...**. The **Import files** dialogue opens.
4. Select the definition files to be imported.

   Only files with a corresponding extension are shown, such as .def and .pkg.
5. Click **Open**.
6. Check that the newly imported definition files appear in the list.
7. Click **Close**.

If a definition file for a certain device type already exists in the database and an attempt is made to import a definition file with the same parameter version and with a *lower* revision, the file will not be imported.

If a definition file for a certain device type already exists in the database and a new definition file with the same parameter version and with a *higher* revision is imported, the old file will be replaced with the imported file.

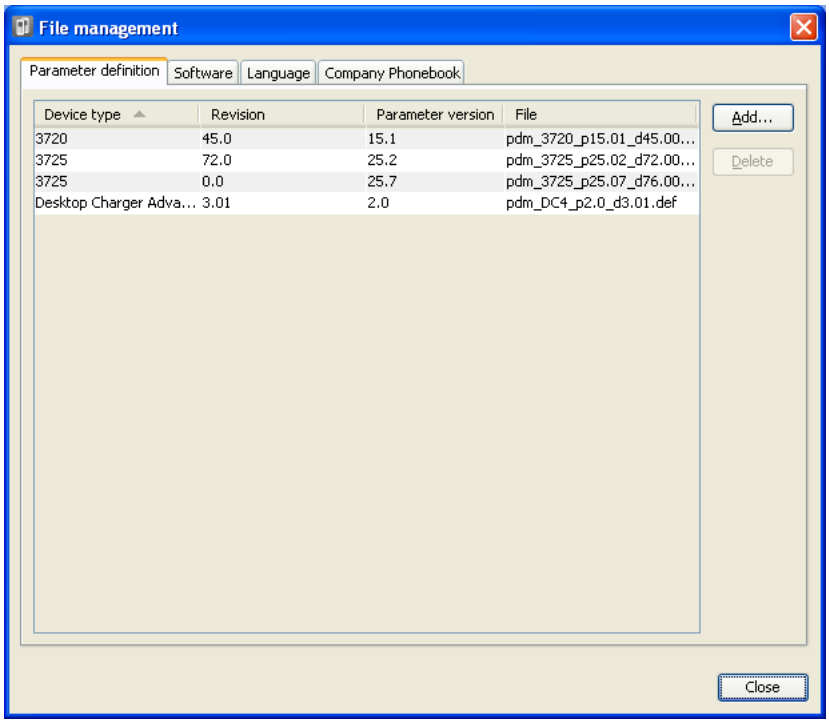
For each update of a parameter definition file, the revision is increased. An update does not necessarily affect the parameter version.

The following columns are displayed:

- *Device type* – the device model.
- *Revision* – the revision number of the definition file. Used to determine which definition file is the most recent.
- *Parameter version* – shows the version of the parameters in the definition file. Used to determine compatibility with device software.

- *File* – the name of the imported definition file

Figure 125: File management window, Parameter definitions tab

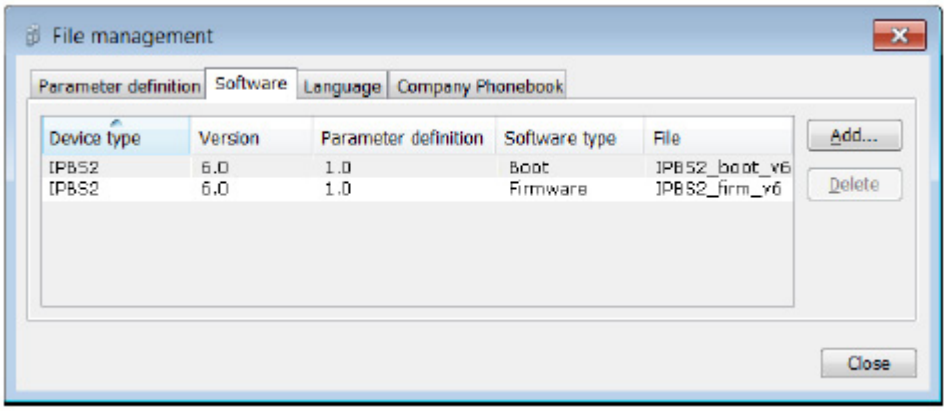


Importing new software for devices

Updated software files are distributed by your supplier.

Note:
Software files (.bin) may be included in package files (.pkg).

1. In the **File** menu, click **File management**. The **File management** window appears.
2. Click on the **Software** tab.



The following columns are displayed:

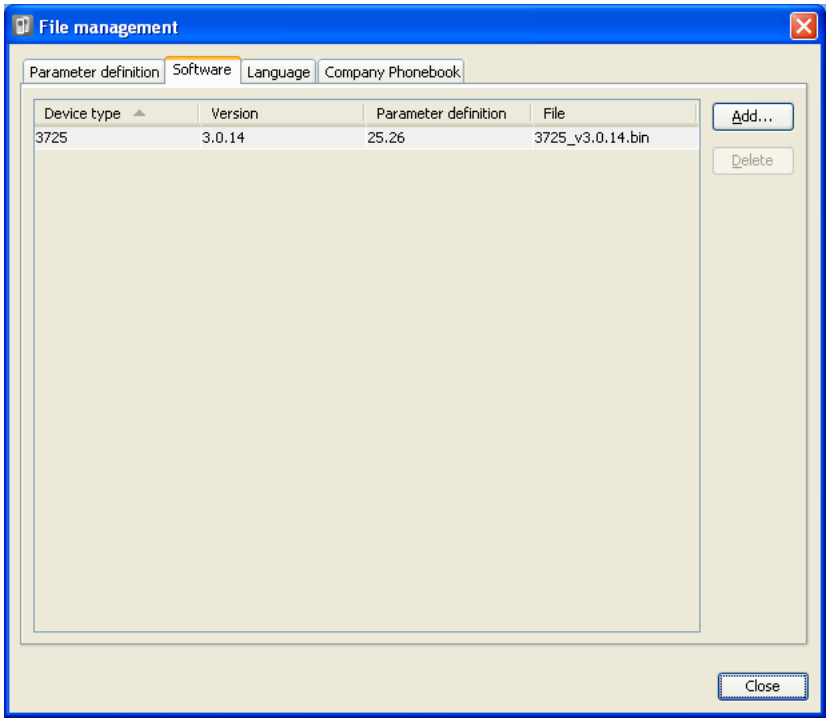
- Device type – the device model.
- Version – the version number of the software file. Used to determine which software file is the most recent.
- Parameter version – shows the version of the parameters in the definition file.
- Used to determine compatibility with device software.
- Software type – shows if the software type is a boot software[1] or a firmware.
- File – the name of the imported software file.

3. Click **Add**. The **Import files** dialogue opens.
4. Select the software files to be imported.

   Only files with a corresponding extension are shown, such as .bin and .pkg.
5. Click **Open**.
6. Check that the newly imported software files appear in the list.
7. Click **Close**.

1. Currently, boot software is only applicable for fixed devices.

Figure 126: File management window, Software tab



Importing language files for devices

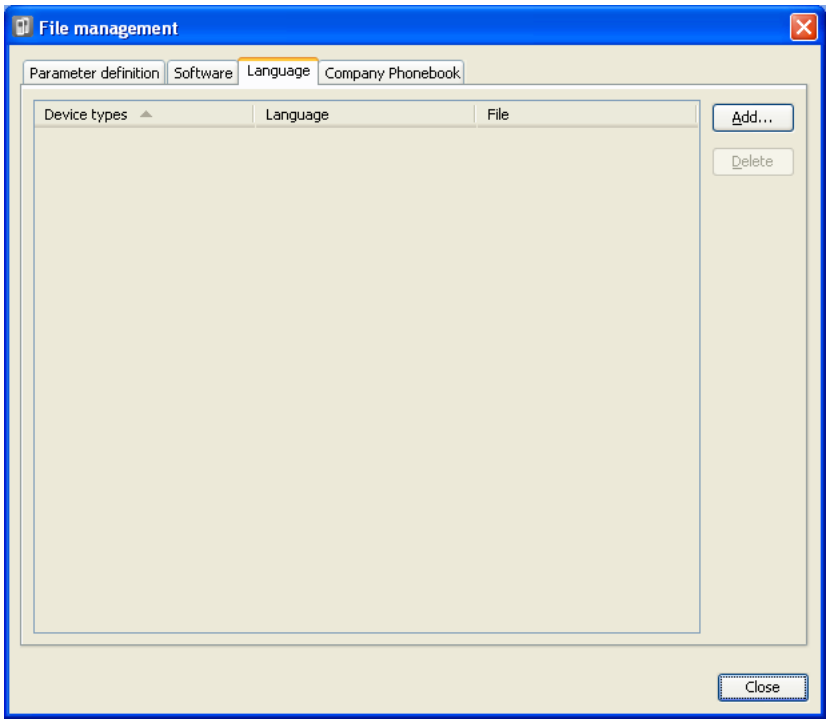
Note:

There is a difference between *Language files* (.lng) for devices described in this section and *Translation files* (.xml) for the AIWS interface that are described in Customizing the language on page 477. Import of translation files are done via the **AIWS Configuration** page.

Language files for an appropriate device type and software version are usually provided with the software package of the device.

1. In the **File** menu, click **File management**. The **File management** window appears.
2. Click on the **Language** tab.
3. Click **Add**. The **Import files** dialogue opens.
4. Select the language files to be imported.
5. Click **Open**.
6. Check that the newly imported language files appear in the list.

7. Click **Close**.

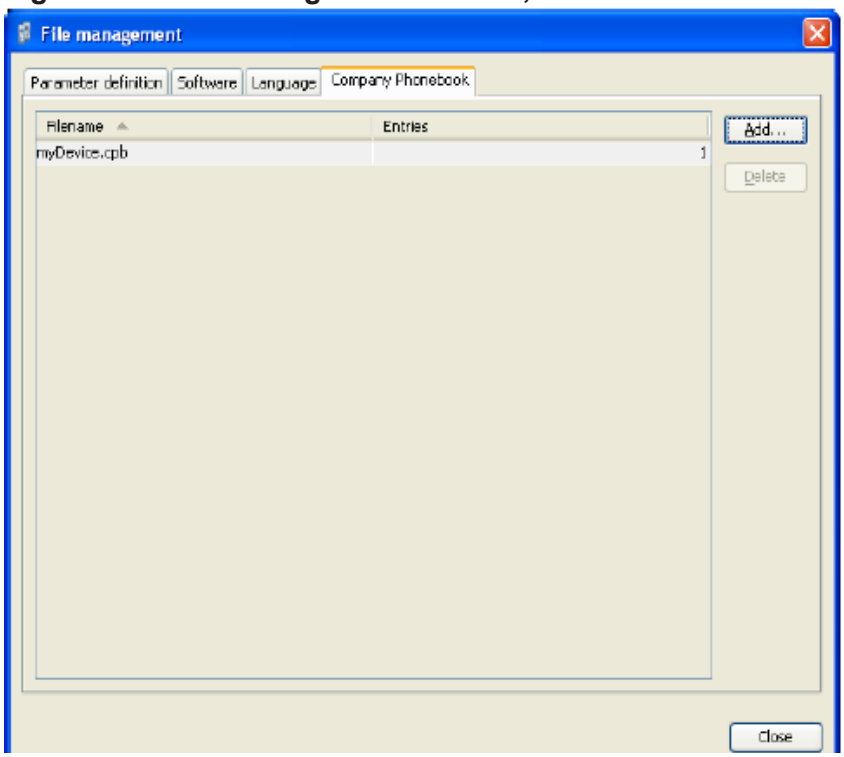


Importing company phonebook files

It is possible to import a phonebook file for later use (see Company phonebook on page 219).

1. In the **File** menu, click **File management**. The **File management** window opens.
2. Click on the **Phonebook** tab.
3. Click **Add**. The **Import files** dialogue opens.
4. Select the phonebook files to be imported.
5. Click **Open**.
6. Check that the newly imported phonebook files appear in the list.
7. Click **Close**.

Figure 127: File management window, Phonebook tab



Uploading a language to a device

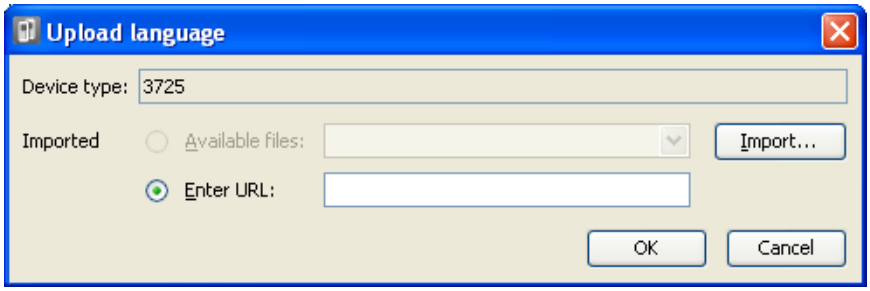
It is possible to upload a language to portable devices that support Language Upload.

Upload of languages is not available in unlicensed mode.

This feature requires a license valid for file upload.

1. Select the **Devices** tab.
2. Select the device(s) to upload a language to. It is possible to select several devices, but only devices of the same Device Type can be selected.
3. In the Device Menu, select **Upload Language...**. The **Upload Language** dialogue opens.

Figure 128: Upload Language dialogue



4. Do one of the following:
   - If needed, import the language file (.lng) to be used by clicking **Import...**, locating the file, and then clicking **OK**. In the **Available files** drop-down list, select which language to upload.
   - Enter the URL where the language file is located.
5. Click **OK**. The language is uploaded to the device.

Uploading a company phonebook

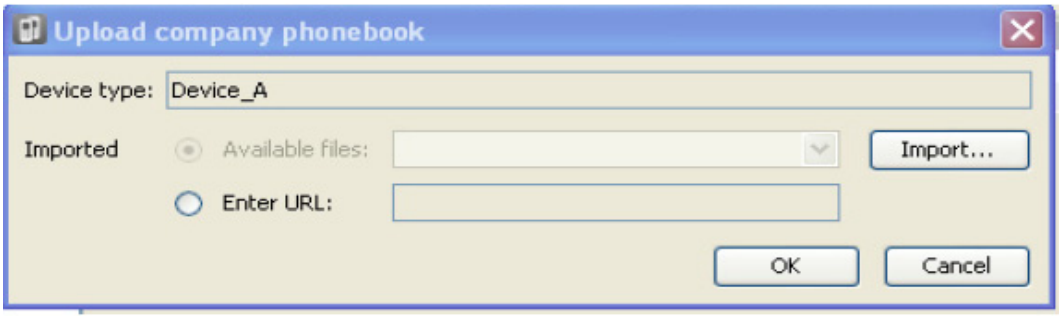
It is possible to upload a phonebook to portable devices that support this feature.

Upload of Company Phonebook is not available in unlicensed mode.

This feature requires a license valid for file upload.

1. Select the **Devices** tab.
2. Select the device(s) to upload a company phonebook to. It is possible to select several devices, but only devices of the same Device Type can be selected.
3. In the Device Menu, select **Upload Company Phonebook...**. The **Upload Company Phonebook** dialogue opens.

Figure 129: Upload Company Phonebook dialogue



4. Select which phonebook to upload.
5. Click **OK**. The phonebook is uploaded to the device.

Upgrading a device with new software

It is possible to upgrade the software in a device.

Upgrade of device software is not available in demonstration mode.

1. Connect a device to the system.
2. Select the **Devices** tab.

3. Select from the list the device(s) that are to be upgraded. The selected row is highlighted. It is possible to select several devices, but only devices of the same Device Type can be selected.

Note:

A software upgrade from AIWS should be done on one device to start with. If successful, the remaining devices can be updated in one operation.

Tip:

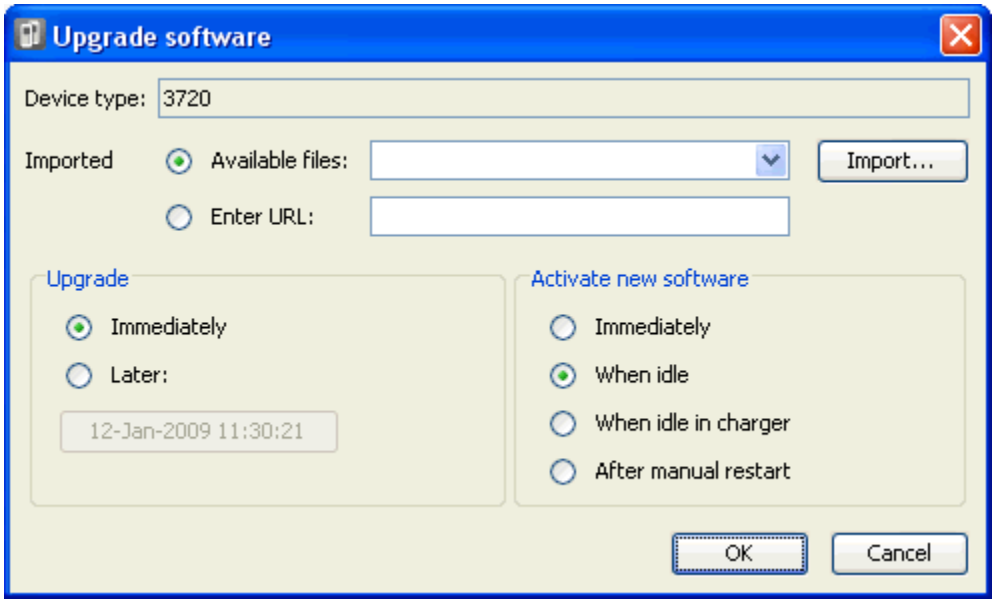
By using Ctrl and/or Shift it is possible to select several devices simultaneously.

4. Click **Upgrade** in the **Device** menu.

   Alternatively, right-click and choose **Upgrade**, double-click on the desired device, or click the **Upgrade** button in the toolbar.

5. The view changes to the **Upgrade software** dialogue.

Figure 130: The Upgrade software dialogue



In the **Upgrade software** dialogue the following fields are shown:

- **Device type** – shows the model of your device.

Note:

Imported
– The **Available files:** box contains previously imported software files (see Importing new software for devices on page 428); the latest used software file is selected by default.
– The **Enter URL:** box gives a possibility to enter a path to a URL.
– **Import...** is used to import new software.
When upgrading devices with imported software, up to 10 devices can be upgraded simultaneously. When upgrading devices with software obtained through a URL, up to 20 devices can be upgraded simultaneously.

- **Upgrade**
  – **Immediately** is used to start upgrade immediately
  – **Later**: enter a date and time for a scheduled upgrade. Upgrades can be scheduled about 4 month ahead.
- **Activate new software** – mark **Immediately**, **When idle**, **When idle in charger** or **After manual restart**. depending on when new software shall be activated.

6. If the software to be used for software upgrade is not available, it needs to be imported. If so, click **Import...**. The **Import software** dialogue opens. Locate the file and click **Open**. The software file is imported to the Device Manager.

   It is recommended to use *Enter URL:* if the software is stored on an external server and should not be imported to the Device Manager.

   Note:

   It is recommended to open a web browser and enter the URL (for example http://myserver/kathy_v1.5.7.bin). Make sure that the web browser asks you to save or open the correct file. Copy the URL and paste it in the Upgrade software dialogue

7. Select software to be used in the upgrade in the **Available software:** text box.
8. Click **OK**. The **Upgrade software** window closes.
9. The software will be downloaded to the device. For some device types, a progress bar in the Status column for the device shows the progress of the download.

   To cancel the upgrade, click **Cancel upgrade** in the **Device** menu. Alternatively, right-click on the device in the device list and select **Cancel upgrade**. Cancelling the upgrade lets you restart the handset.

   The device will restart automatically after a successful download and when the handset is idle.

Note:

The Handset will not restart if a missed call popup or a new message popup is active on the handset. This is not considered as an idle state.

A switched off device is upgraded when restarted.

Telephones that are not in the coverage area will be upgraded when they come online.

It is not possible to upload phonebook, language file and software to 3720 telephone while it is on a call.

Deleting parameter definition files

1. In the File menu, click **File management**. The **File management** window opens.
2. Click on the **Parameter definition** tab.
3. Select the definition file(s) to be deleted.
4. Click **Delete**.
5. In the **Delete files** dialogue, click **Yes**.
6. Click **Close**.

Deleting Software

1. In the File menu, click **File management**. The **File management** window opens.
2. Click on the **Software** tab.
3. Select the software to be deleted.
4. Click **Delete**.
5. In the **Delete files** dialogue, click **Yes**.
6. Click **Close**.

Deleting a language

Note:

This applies to language files (.lng). Translation files (.xml) are not deleted.

1. In the File menu, click **File management**. The **File management** window opens.
2. Click on the **Language** tab.
3. Select the Language to be deleted.
4. Click **Delete**.
5. In the **Delete files** dialogue, click **Yes**.
6. Click **Close**.

Deleting company phonebook File

1. In the **File** menu, click **File management**. The **File management** window opens.
2. Click the **Company Phonebook** tab.
3. Select the company phonebook to be deleted.
4. Click **Delete**.
5. In the **Delete files** dialogue, click **Yes**.
6. Click **Close**.

Importing/Exporting Numbers and Templates

This section describes import and export of Numbers and templates.

The purpose of exporting and importing Numbers and Templates is to be able to move Numbers and Templates to another site or to use at a later time. It is also possible to move between PDM Windows Version and AIWS.

The parameter configuration in Numbers can be exported to a file. This file can be used by the supplier to pre-program devices before delivery to the customer.

If there is a naming conflict when importing a template, the new template is imported and the old template is deleted. If there is a Number conflict when importing Numbers, an error message is displayed.

Exporting numbers to a file

It is possible to configure Numbers for a site and export the settings to a file. One or several Numbers can be selected.

The exported file can then be used when producing new devices for the customer.

1. Select the **Numbers** tab. The **Numbers** view appears.
2. Select the Number (or Numbers).
3. In the Number menu, click **Export**.

   The **Export Numbers** dialog appears. By default the file will be saved in the ***My documents*** directory with the name ***[EliseSite].xcp***. You can select another name and directory.
4. Click **Save**.

Exporting templates to a file

It is possible to export templates to a file. One or several templates can be selected.

1. Select the **Templates** tab. The **Templates** view appears.
2. Select the template (or templates).
3. In the Template menu, click **Export**.

   The **Export Templates** dialog appears. By default the file will be saved in the ***My documents*** directory with the name Templates.tpl. You can select another name and directory.
4. Click **Save**.

Importing numbers

1. In the **File** menu, click **Import > Numbers...**. A File Browser window appears.
2. Select the Number files to be imported (*.xcp).
3. Click **Open**.
4. The Number(s) will be imported.

Importing templates

A template may be imported from another system. Updated Template files may be distributed by your supplier.

1. In the **File** menu, click **Import > Templates...**. A File Browser window appears.
2. Select the Template files to be imported (*.tpl).
3. Click **Open**.
4. The Template(s) will be imported.

Other settings

Automatically enabling new devices settings

By default, when a device logs in, it is automatically saved in the AIWS database and this is the default setting.

Note:

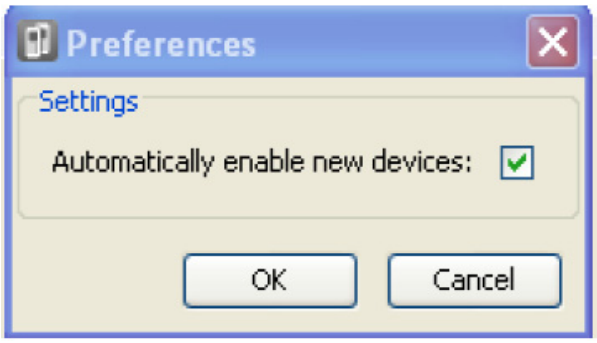
The AIWS license determines the number of devices that can be enabled simultaneously in the Device Manager. If logging in more devices than allowed, they will be disabled in the Device Manager. The devices must be enabled in order to configure them.

When a single AIWS is used, the *Automatically enable new devices* function should normally be enabled. When Device Management is distributed over multiple AIWS in a system, the function shall be disabled. If the function is enabled, devices will be enabled and saved on all AIWS running device management. This will cause synchronization problems and the logged in devices will consume license positions on each AIWS. See also Multiple AIWS configuration on page 369.

To disable automatic saving of new numbers:

1. In the **Options** menu, click **Preferences**. The Preferences window appears.

Figure 131: The Preferences window.



2. In the **Preferences** window, clear the **Automatically enable new devices** check box.
3. Click **OK**.

Closing the Device Manager

In the **File** menu, click **Exit**. The Device Manager shuts down.

DECT Interface

Cordless telephone system

IP-DECT Single Master

Ensure that you configure the interface to the IPDECT Master and IPDECT Standby Masters from the Wizard. This can also be done from the Advanced Configuration page.

This chapter describes configuration from the Advanced Configuration page, for some carrier systems. It does not include all supported carrier systems.

Figure 132: Redundancy achieved by connecting AIWS to two IP-DECT base stations



AIWS can communicate with the IP-DECT system over a LAN. For configuration of the IP-DECT system, see Installing and operating the IPBS and IPBL on page 63.

You can also set an address to a secondary IP-DECT Standby Master which is used as a redundancy backup. The secondary IP Address is used if the connection to the primary IP Address is lost. If the secondary IP Address is lost, AIWS will try to use the primary IP Address.

To enter IP-DECT IP address settings, do as follows:

1. On the AIWS Start page, click on **Setup Wizard**. The **Setup Wizard** opens.
2. Click **Next** until you reach **DECT IP Address**.
3. Enter settings in the fields for **DECT IP Address** and **Secondary DECT IP Address**.
4. Set multiple Locations (former IP regions) to **no**.

IP-DECT multi Master Base Station configuration

For an IP-DECT system with multiple Master Base Stations connected to a single AIWS the IP-DECT interface settings needs to be changed. In this configuration one IP-DECT interface on the AIWS is communication with multiple Master Base Stations on the same or different locations:

1. On the AIWS Start page, click **Setup Wizard**. The **Setup Wizard** opens.

2. Click **Next** until you reach **DECT IP Address**.
3. Set multiple Locations (former IP regions) to **yes**.
4. Do not enter any IP address or remove the entries for the DECT IP-Address and for the secondary DECT IP-Address

Note:

Of course a multi AIWS configuration with splitting services of the AIWS to several Elise hardware units is supported in the same manner, see Multiple AIWS configuration on page 369.

DECT Interface settings

The DECT Interface controls the messaging flow between the Cordless Telephone System and the AIWS services.

General Settings

To find DECT General Settings, do as follows:

1. On the AIWS start page, select **Configuration**. The **AIWS Configuration** page opens.
2. Select Other Settings > Advanced Configuration. The **AIWS Advanced Configuration** page opens.
3. On the **AIWS Advanced Configuration** page, select **General Settings** under **DECT Interface**.

- *Call Diversion Display Text*
  When this parameter is enabled, the text specified is added to the display message when a call diversion takes place. The original Call ID can be included in the parameter text by writing a % character where the Call ID shall be inserted.

Advanced parameters include:

- Extended Activity Log
  N/A
- Broadcast
  Specifies whether broadcast messaging is allowed or not. Only IP-DECT systems can handle broadcast, all other systems will ignore the parameter.
- *Set time in DECT*
  N/A
- Priority conversion
  Used to convert messaging priorities; Alarm, High, Normal and Low. This conversion is normally only used for compatibility with some PWT telephones and should never be enabled unless you are absolutely sure.

- DECT Interface
  This parameter makes it possible to disable the DECT Interface on AIWS. When the DECT interface is disabled, messaging is not supported and lost link to DECT system will not be indicated.

  Note:

  In multiple AIWS configurations, there is only one AIWS with an active DECT interface talking to the IPBS Masters. On the other AIWS, the DECT interface should be disabled using the DECT interface of the dedicated AIWS to talk to the IPBS Masters.

- IM update status handling
- No of included 9dLD locations
  Only valid in combination with Avaya messaging system.

Message Distribution

The DECT Interface has distribution lists that define where incoming data from telephones, for example alarms and user data, should be sent. The following information is supported:

To find settings for DECT Message Distribution, do as follows:

1. On the AIWS start page, select **Configuration**. The AIWS Configuration page opens.
2. Select **Other Settings > Advanced Configuration**. The AIWS Advanced Configuration page opens.
3. On the AIWS Advanced Configuration page, select **Messaging Distribution** under DECT Interface.

- Alarm

  Personal alarms from cordless telephones in the Cordless Telephone System.

- Mobile Data - Not used.
- Location - Not used.
- Availability - Not used.

SMS Character set

This setting determines which characters that can be displayed in the handsets when they receive messages. Additionally, the setting also determines which characters that can be entered in the handsets when the users write messages.

Note:

The number of characters that can be entered in the handset when writing a message depends on which SMS character set that is used.

1. Click **Configuration** on the **Start** page.
2. Select **Other Settings > Advanced Configuration** in the menu on the **Configuration** page.
3. Select **SMS Character Set** under DECT Interface in the menu on the **Advanced Configuration** page.
4. Select one of the following:
   - Standard SMS - (Compatibility Mode): Standard SMS works with all handsets but some special characters may not be correct.
   - Latin -1:Used for later generation of handsets.
   - UTF-8:Used for later generation of handsets. Use UTF-8 to include characters that is not included in the Latin-1 character set.

   Tip:
   Russian requires UTF-8 character set.

   Note:
   The UTF-8 character set requires an Avaya IP-DECT system with version 3.0 or later.
5. Click **Activate**.

Basic Configuration

The basic configuration requires *system administrator* or *administrator* rights. With *user* rights you will only be able to access and configure the *Phonebook*. Refer to Authentication Levels and Default Passwords on page 378.

Central Phonebook Configuration

This chapter describes the configuration of the AIWS Central Phonebook.

The AIWS Central Phonebook gives the possibility to search for phone numbers in a local database or in an LDAP server.

If the search is to be forwarded to an LDAP server, the LDAP parameters need to be configured as described in LDAP Parameter Setup on page 446.

For information on phonebook administration, see Phonebook Administration on page 390.

Note:

If an LDAP connection to a central phonebook is used, all settings needed is done in the setup wizard.

Technical Specification

The local database has defined limitations while most of the limitations for the LDAP server depends on the LDAP server used, see table below.

	Local Database	LDAP Server
Max. No. of phonebook entries:	500/2000	Server dependent
Max. No. of characters in family name:	20	Server dependent
Max. No. of characters in first name:	20	Server dependent
Max. No. of digits in phone number:	20	Server dependent
Max. No. of returned entries / request:	25	25
telephones that can access the phonebook[1]	Depends on telephone type	

1. See also documentation for the telephone

Phonebook address

When the Unite Name Server (UNS) is set to forwarding mode, the phonebook Call ID must exist in the module that the requests are sent to. Any change of the Call ID and/or IP address must be made in that module. If the default address is used, no changes are needed. When the UNS is set to stand-alone mode, do as follows to change the address:

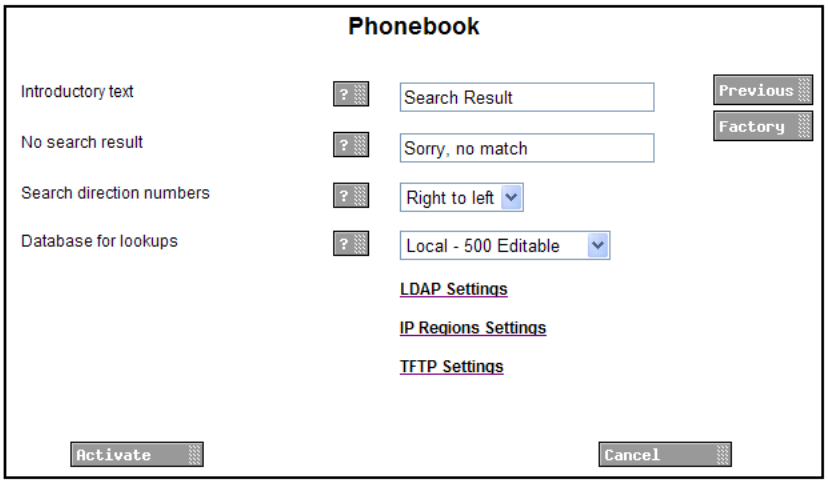
The default Call ID is 999999 for phonebook access.

1. On the **AIWS start page**, click on **Configuration**. The **AIWS Configuration** page opens.
2. In the left pane, click **Other settings > Advanced configuration**. The **AIWS Advanced Configuration** page opens.
3. In the left pane, under **Other**, click **UNS**
4. Click on **Alias / Call ID**.
5. Click **999999** in the list.
6. Enter the new Call ID for the phonebook, i.e. the Call ID the telephones are using to access the phonebook. Check that the Call ID does not conflict with any of the telephones in the system.
7. If the phonebook is located on another module, enter the IP address to that module.

1.

Phonebook setup

Figure 133: AIWS Phonebook Setup



Entering search result texts

When a request is sent to the phonebook, a text is included in the response that is sent to the telephone. These texts can be customized, for example translated.

1. On the AIWS start page, click on **Configuration**. The **AIWS Configuration** page appears.
2. In the left pane, click **Other settings > Advanced Configuration**. The AIWS Advanced Configuration page appears.
3. In the left pane, click **Phonebook**.The **Phonebook** page appears.

   Search direction **Right to left** means that the Central Phonebook returns entries that ends with the entered search criteria.

   Note:

   If the LDAP phone book is selected, the search direction will always be left to right. So the direction setting will not be valid in this case.
4. Enter the texts that should be included in the search result, see table below for more information about the different texts and when they are used.

Default text	Description
Search result	Included in a successful request before the entries that matched the request
Sorry, no match	Sent when there were no match for the sent request.

Note:
This setting does not affect all handset types.

5. Click **Activate**.

Selecting Central phonebook database

Select which database to use for phone numbers; **Local - 500 Editable**, **Local - 2000 View only**, **TFTP** or **LDAP**.

- If the default local database is selected, continue below in chapter Importing entries to the phonebook from a CSV File on page 393, Exporting the phonebook to a CSV File on page 394 and Adding entries to the phonebook on page 390.
- If LDAP server is selected, continue in chapter LDAP Parameter Setup on page 446.
- If TFTP is selected, continue in chapter TFTP parameter setup on page 448

Note:
Import of central phonebook over TFTP is supported only for IP Office.

Select database to use for the Central Phonebook.

1. On the AIWS start page, click **Configuration**. The **AIWS Configuration** window opens.
2. In the left pane, click **Other settings > Advanced Configuration**. The **AIWS Advanced Configuration** page opens.
3. In the left pane, click **Phonebook**. In the **Database for lookups** field, choose between **Local - 500 Editable**, **Local - 2000 View only**, **LDAP** and **TFTP**.

If **Local - 2000 View only** is chosen, the **Add** and **Delete all** buttons are not visible in the Edit Phonebook pages.

LDAP Parameter Setup

Note:
This feature requires FE3-EECAAC, Avaya AIWS2 Enterprise variant.

The Lightweight Directory Access Protocol (LDAP) is an application protocol for querying and modifying directory services running over TCP/IP. The AIWS starts an LDAP session by connecting to an LDAP server. The AIWS then sends operation requests to the server, and the server sends responses in return.

An LDAP directory is a tree of directory entries and follows the structure below:

- An entry consists of a set of attributes.
- An attribute has a name and one or more values.

An entry can look like this:

dn: cn=John Ericson,dc=company,dc=com

cn: John Ericson

givenName: John

sn: Ericson

telephoneNumber: +1 888 555 6789

dn is the name of the entry; it is not an attribute nor part of the entry. "cn=John Ericson" is the entry's RDN, and "dc=company, dc=com" is the DN of the parent entry. The other lines show the attributes in the entry. Attribute names are typically mnemonic strings, like **cn** for common name, **dc** for domain component, **mail** for e-mail address and **sn** for surname. See Examples of settings on page 448.

1. On the **AIWS start page**, click on Configuration. The **AIWS Configuration** page opens.
2. Click on **Other settings > Advanced Configuration**. The **AIWS Advanced Configuration** page appears.
3. In the left pane, click on Phonebook. The **Phonebook** page appears.
4. Click the **LDAP Settings** link.
5. Enter the IP or DNS address to the LDAP server in the **LDAP Server Address** field.
6. Enter the port number used by the LDAP server in the **Port Number** field.
7. Select how to authenticate to the LDAP server in the **Authentication Method** drop down list.

Note:

If the authentication method "SASL/DIGEST-MD5" is selected, the IP address for primary DNS server must be entered in the DNS server field on the Network setup page. Otherwise it is not possible to authenticate with the LDAP directory Microsoft Active Directory 2003.

8. Enter the user name used for logging on to the LDAP server in the **User name** field. It is a good idea to create a new user in the domain with access for the LDAP server.
9. Enter the password used for logging on to the LDAP server in the **Password** field.
10. Enter the user entries' parent DN in the **Search Base DN** field.
(The distinguished name for all users common entry.)
11. Enter the name of the attribute that holds the phone numbers in the **Number attribute** field.
12. Select the appropriate option in the **Type of Name Attribute(s)** drop down list.

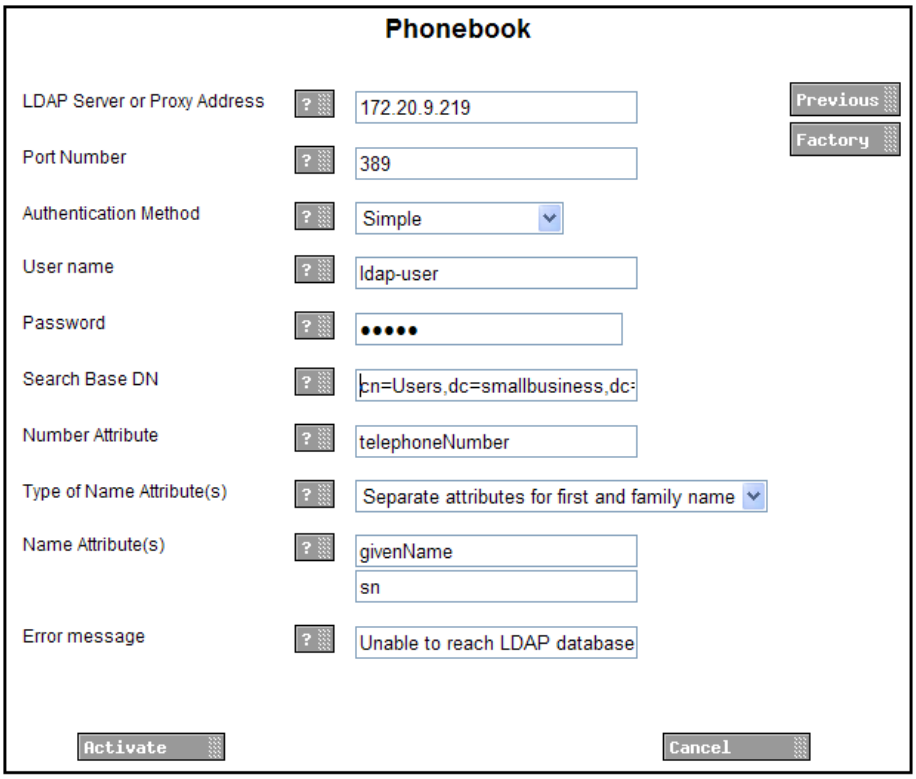
    The option depends on if the name is stored in a single attribute or if it is split into two different attributes.

13. Enter name(s) of the attribute(s) containing first name and family name in the **Name Attribute(s)** field. If two attributes are used, enter the first name on the first line and the family name on the second line.
14. Enter an error message to be sent as an answer to a phonebook query that was unsuccessful, due to no answer from the server, in the **Error message** field.

Examples of settings

- Active directory 2003

Figure 134: Settings for Active directory 2003



TFTP parameter setup

If TFTP is selected, it means that phonebook searches will return entries from the Avaya PBX through TFTP.

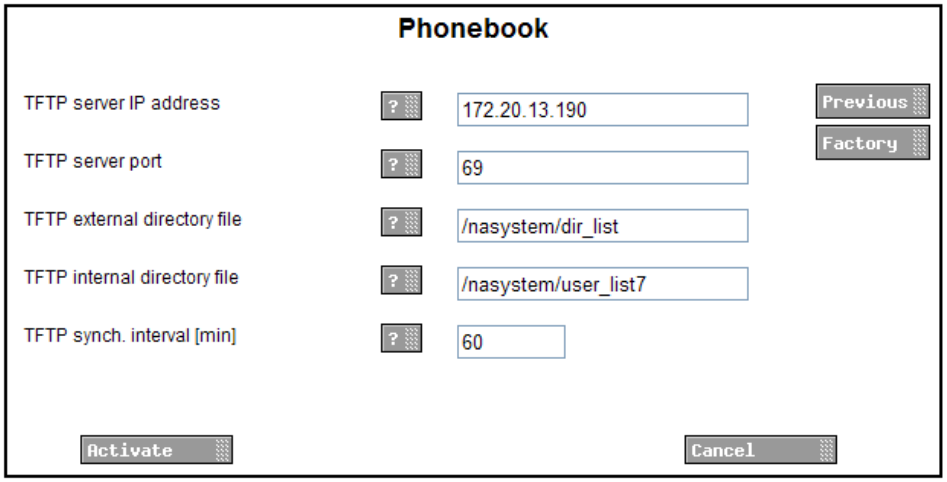
Note:

Import of central phonebook over TFTP is supported only for IP Office.

To do settings for TFTP, do as follows:

1. On the **AIWS start page**, click on Configuration. The **AIWS Configuration** page opens.
2. Click on **Other settings > Advanced Configuration**. The **AIWS Advanced Configuration** page appears.
3. In the left pane, click on Phonebook. The **Phonebook** page appears.
4. Click the **TFTP settings** link.
5. Enter the IP address to the TFTP server in the **TFTP server IP address** field.
6. Enter the port number used by the TFTP server in the **TFTP server port** field.
7. Enter the external directory file path in the **TFTP external directory file** field.
8. Enter the internal directory file path in the **TFTP internal directory file** field.
9. Enter the TFTP synchronization interval in minutes in the **TFTP synch. interval** field.
10. Click **Activate**.

Figure 135: Example of TFTP settings



Digit treatment for IP regions

When importing telephone numbers it is sometimes necessary to automatically change the way a number is written according to preset conditions.

Depending on where a number is situated, the AIWS can alter the number that is returned in a phonebook query. If, for example, the queried number is situated within the same local exchange, the telephone number is considered to be an internal number and the number is stripped from superfluous international prefixes, etc.

This feature is only used if LDAP is selected as database.

Telephone number standards

There are several standardized ways of writing telephone numbers.

The following formats are currently supported:

Format	Comment
+4631559300	E.164 international standard, and E.123
(031)-559300	E.123 local number
+46(031)559300	National prefix + national destination code in parentheses
+46(0)31559300	National prefix in parentheses
+46(31)559300	Canonical address format
4631551234	Digits only. Conversion is controlled by setting maximum lengths of internal and global numbers.

Examples

The following figure shows the elements of a telephone number, +46(31)551234 (in canonical format), used in the parameter descriptions below.

Figure 136: Example of how a telephone number is built up from different prefixes and extensions.

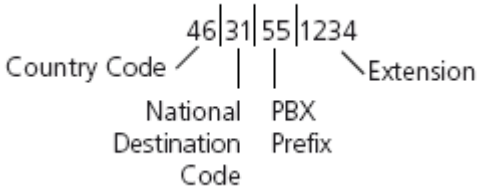
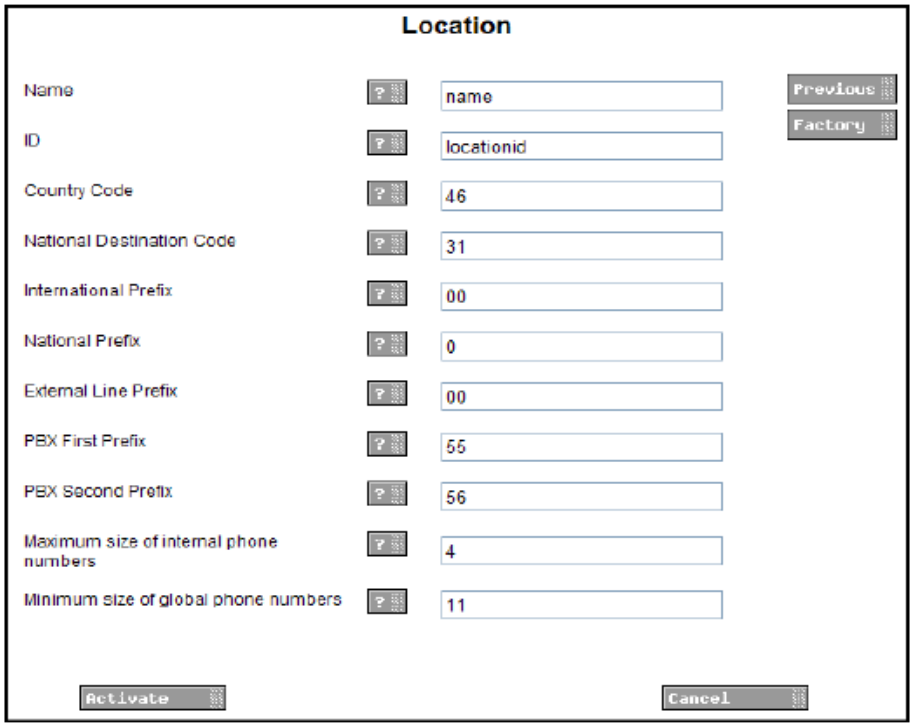


Figure 137: Example of a digit treatment setting for location (former IP region)



The following examples illustrates how digit treatment works in different queries. The queries are considered to be done from within +463155xxxx (local exchange), see also figure 137 above.

- Example 1: The query is within the same local exchange.

  Queried number: 551234

  Digit treatment identifies 55 as the local exchange prefix and strips 55 from the number.

  Resulting number: 1234

- Example 2: The query is within the same city (area code), but outside the local exchange.

  Queried number: 031612500

  Digit treatment identifies 0 as National Prefix and 31 as National Destination Code, strips 031from the number and adds 00 for external line.

  Resulting number: 00612500

- Example 3: The query is within the same country, but not in the same city.

  Queried number: 035158115

  Digit treatment identifies 0 as National Prefix and 35 as National Destination Code and adds 00 for external line.

  Resulting number: 00035158115

- Example 4: The query is within another country.

  Queried number: +4781530555

  Digit treatment identifies "+47" as an international call, skips the "+", and adds 00 for external line prefix and 00 for international prefix.

  Resulting number: 00004781530555

- Example 5: Size of internal number.

  Queried number: 1234

  Digit treatment identifies that the number of digits in the telephone number is equal to the number of digits entered as "maximum size of internal phone numbers".

  Resulting number: 1234

- Example 6: Size of global number.

  Queried number: 47815305555

  Digit treatment identifies that the number of digits in the telephone number is equal to the number of digits entered as "minimum size of global phone numbers", then adds 00 for external line prefix and 00 for international prefix.

  Resulting number: 000047815305555

Digit treatment settings

The parameters for digit treatment is set via the AIWS **Configuration** page:

Digit treatment can be enabled and disabled. When enabled, digit treatment is defined per Location (former IP region).

1. On **AIWS Start Page**, select Configuration.
2. In the left pane, select **Other Settings** > **Advanced Configuration**. The **AIWS Advanced Configuration** page appears.
3. Select Phonebook. The **Phonebook** page appears.
4. Click **Location Settings**.
5. Select Digit Treatment to be Enabled or Disabled.
6. Click **Activate**.
7. For each Location (former IP region) to be used, enter the **Location** (former **IP region**) page.

8. Enter settings for Location (former IP region) and digit treatment.
9. Click **Activate**.

The following parameters can be configured for digit treatment:

- Digit Treatment (Enabled or Disabled)

  The digit treatment function can be enabled and disabled. If the function is enabled, the parameters below apply, otherwise they do not apply.

- Name
  A textual description of the current Location (former IP region).

- ID
  An identifier for the Location (former IP region) represented by a numerical value between 1-250. The Location ID (former region ID) set in the IPBS Master or Standby Master needs to correspond to one of the configured Location ID (former Region IDs) in the AIWS. The digit treatment for a central phonebook query in the handsets will be done according to the defined rules for the Location (former IP region) of the IPBS Master and Standby Master the handset is connected to. Multiple IPBS Masters and Standby Masters in an IP DECT system can use the same Location ID (former Region ID), so they will use the same digit treatment rules.

- Country Code

  The Country Code is the prefix to be used when dialling to a particular country from another country. The country code is what follows after the + in a telephone number.

  The value is used to identify the country code in the number and remove it when it is not needed.

- National Destination Code

  The National Destination Code (NDC) is what follows after the country code in a telephone number.

  The value is used to identify the NDC in the telephone number and remove it when it is not needed.

- International Prefix

  The International Prefix is used to dial a call from a particular country to another country. This is followed by the country code for the destination country.

  This value is used to replace the + character when an international call is made.

- National Prefix

  National Prefix is used to make a call within a country from one city to another. The national prefix is followed by the national destination code for the destination of the call.

  This value is used for two purposes:

  – To identify the national prefix in the number and remove it when it is not needed.

  - To change a number when the destination is another city.
- External Line Prefix

  External Line Prefix is what needs to be dialled before the number to reach the public network.

  The value is used to change the telephone number if it is identified as an external number.
- PBX First Prefix

  PBX First Prefix is what precedes an internal number to create an external number.

  This value is used to compare with the phonebook number to decide whether the number is internal or external.
- PBX Second Prefix

  Points out an additional prefix to be handled in the same way as “PBX First prefix”.
- Maximum size of internal telephone numbers

  Used for numbers that starts with a digit instead of “+” or “(“. If the number is longer than this value, it is considered to be an external number.
- Minimum size of global telephone numbers

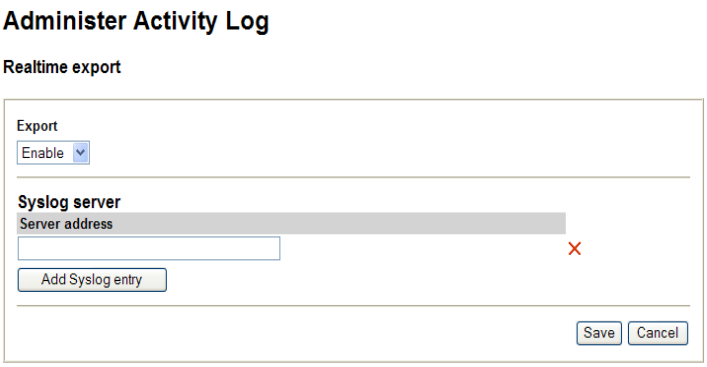
  Used for numbers that starts with a digit instead of “+” or “(“. If the number is equal to or longer than this value, it is considered to be a global number.

Export activity logs to a Syslog server

Activities in the module are logged and can be exported to a Syslog Server where the logs can be managed and analyzed. Messages are sent to the syslog server every time an activity occur in the module.

Example of activities are: An SMS has been sent to a handset, an alarm has been received from a handset, an error has occured in the module etc.

Syslog is a simple protocol (SYStem LOG protocol) for transmitting event messages and alerts text across an IP network. The activities are sent as text messages from the module to the Syslog Server. The IP address to the Syslog Server must be set in the module, DNS is supported so entering the servername will work as well. The activities can be exported to 5 syslog servers in parallel.



1. Click **Configuration** on the **Start** page.
2. Select **Activity Log > Log Export** in the menu on the **Configuration** page.
3. Select **Enable** in the drop-down list.
4. Click the **Add Syslog entry** button.
5. Enter the Syslog Server's IP address in the text field.
6. Click **Save**.

Status

On these pages, information on active faults or stored faults can be shown.

Active faults

The last 100 received active fault logs are listed on the *Active Faults* page. For more information about the fault log, refer to Fault log on page 457.

1. Click **Configuration** on the start page.
2. Select **Status** > **Active Faults** in the left menu on the **AIWS Configuration** page to open the page.

The following information is shown for each fault:

- Time when the fault occurred
- Level of the fault:
  - Critical error
  - Error
  - Warning

- Description of the fault, as defined in the module
- Type of module
- IP address and host name of the module that generated the fault

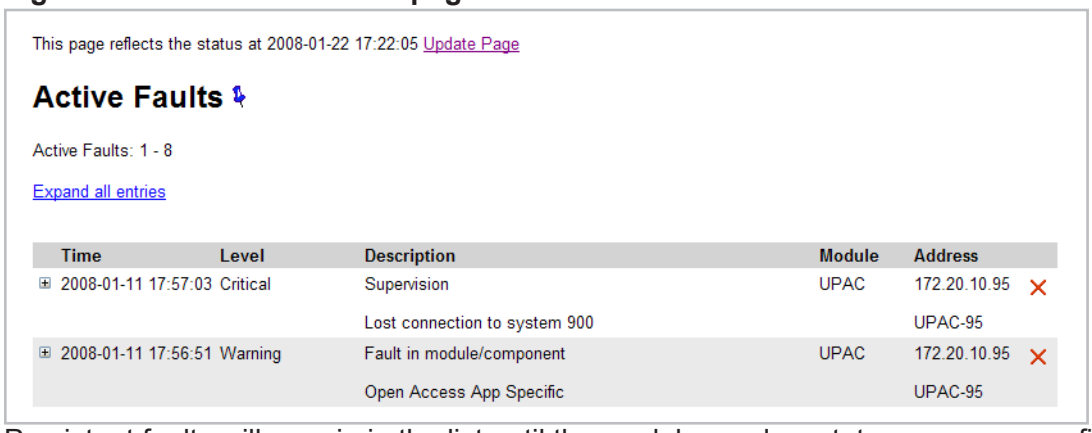
By expanding the fault in the list, additional information about the fault is shown containing:

- Fault ID

  This is used to reference a persistent fault when it later is reset
- Fault code
- Description of the fault code
- Extended address information showing the system, bus type and module address

  In the figure below the system is 00, the bus type is 1 and the module address is 0A.

Figure 138: The Active faults page



Persistent faults will remain in the list until the module sends a status message confirming that the module is working properly again. It is also possible to delete the fault in the list by clicking the delete symbol.

Note:

If the IP address or license is changed in AIWS, the faults reported for the previous IP address/license will remain since no confirmation can be received. These faults must be manually deleted.

The active faults list page has to be manually updated by clicking the **Update Page** link uppermost on the page. See Function Indicator and Error Relay Output on page 519 and Installing Elise 2 Server (AIWS Hardware) on page 523.

Resetting the error relay

The error relay can be reset manually from the Active Faults page.

1. Click **Configuration** on the start page.
2. Select **Status > Active Faults** in the menu on the **Configuration** page.

3. Click the **Reset** button.

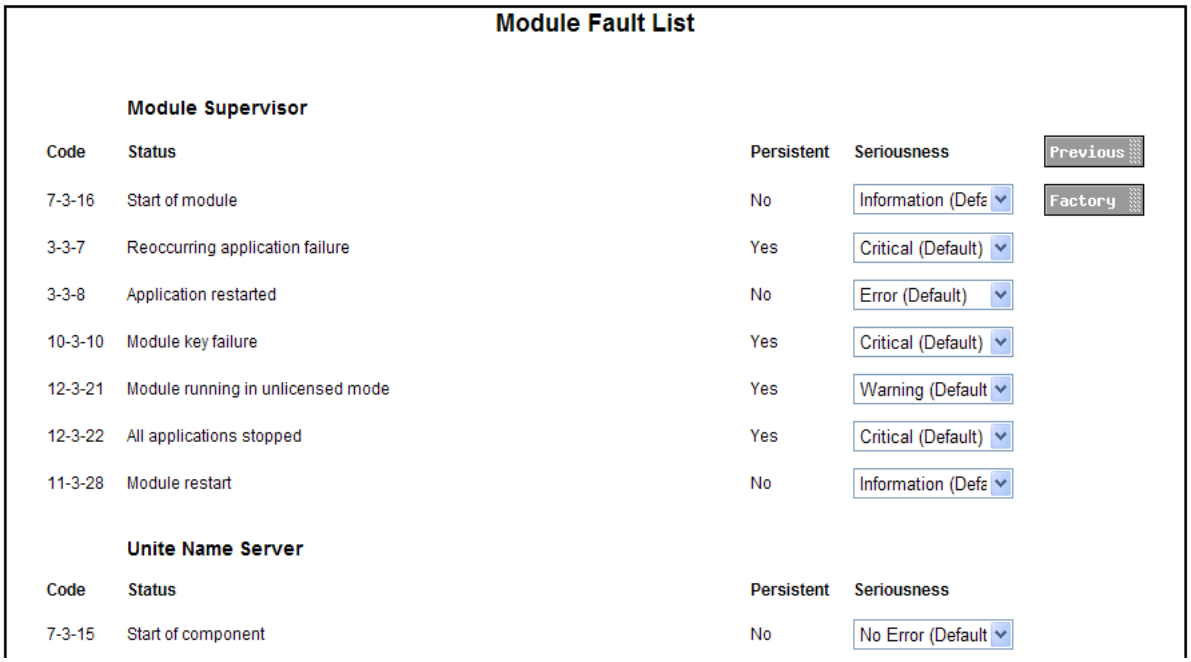
See also Function Indicator and Error Relay Output on page 519 and Installing Elise 2 Server (AIWS Hardware) on page 523.

Level of Seriousness for different Fault Types (Module Fault List)

The level of seriousness can be changed for different fault types in the logs. There is a list of all possible module faults, which shows codes and statuses etc. for AIWS.

1. Click **Configuration** on the start page.
2. Select **Other Settings** > **Advanced Configuration** in the left menu on the **AIWS Configuration** page.
3. Click the **Troubleshoot** button and select **Module Fault List** in the left menu to open the list.
4. Select level of seriousness in the drop-down list for the code(s) for which you want to change level.

Figure 139: Part of the Module Fault list page.



Fault log

The AIWS fault log is a centralised log file and shows a complete log of the faults in the system. Every time a fault message is generated in the system, information about the fault is written to the log file. The maximum number of entries in the log file is 1050. When the log file is full, the 50 oldest entries are removed.

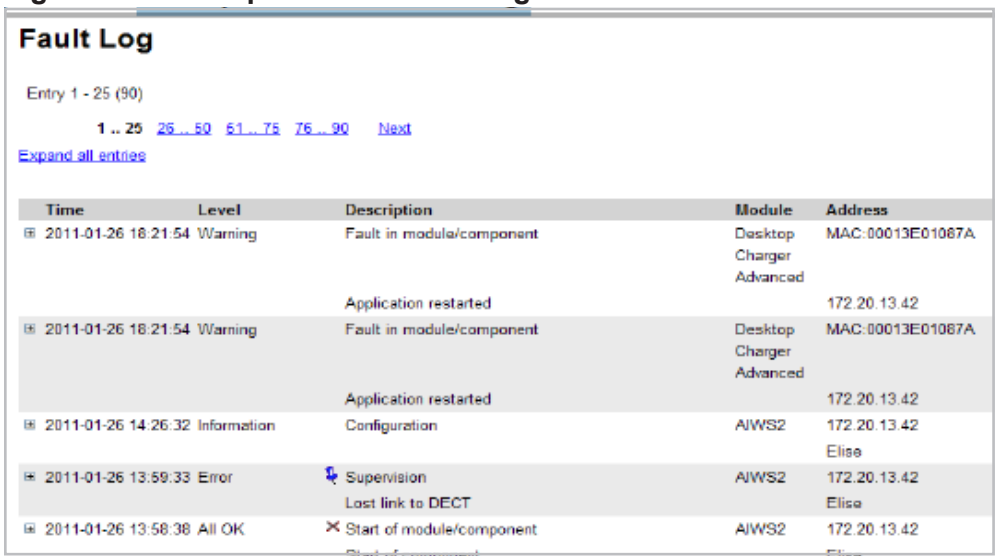
1. Select **Status** > **Fault log** in the left menu on the **AIWS Configuration** page to open the page.

The first 25 log entries are shown. To get the following 25 log entries, click the **Next** link.

The following fault levels exist in the log:

- Information
- Individual reset
- All OK
- Critical error
- Error
- Warning

Figure 140: Example of AIWS fault log.



Symbols used in the Fault Log

Symbol	Description
	Active persistent fault
	Persistent fault that has been handled
	Reset message, no fault exists

To get more detailed information about the events, it is possible to expand the log entries by clicking the **Expand all entries** link. Single log entries can be expanded by clicking the individual plus symbol.

Note:

When the persistent fault is recovered, it takes a while before the persistent fault is cleared.

Administering fault log

In the **Administer Fault Log** page, it is possible to export the log file to CSV (Comma Separated Values) file format, and to clear the status log file from non-active faults.

1. Click **Configuration** on the start page.
2. Select **Other Settings** > **Administer Fault Log** in the left menu on the **AIWS Configuration** page to open the page.

Exporting a fault Log

Click to export the fault log. The log will be exported in csv format.

1. Click **Export**.
2. Click **Save** in the dialogue window and enter the file name (default name statuslog.csv) and the file path.

Clearing fault

This functionality removes all non-active faults from the fault log.

1. Click **Clear**.
2. Click **Yes** in the dialogue window to remove all non-active faults from the status log file.

Timeout

Repeated faults can be blocked, i.e. the fault will be discarded and no actions will be taken. The incoming fault will be handled when first received and blocked during the set timeout.

1. Enter the timeout in minutes (0-1000 minutes), the default value is 10 minutes.

   If no Status Logs should be blocked, set the timeout to 0.

2. Click **Set timeout** to save the setting.

An incoming fault will now be handled the first time it is received and then blocked during the set timeout.

Backing up the configuration

This instruction is used to backup the Device Manager database and Elise 2 configuration. The backup file is saved in a proprietary file format and cannot be edited. Save it in a place where you can easily find it for a restore.

1. On the **AIWS Start page**, click on **Configuration** and log in.
2. Click on **Other Settings** in the left menu.
3. Click on **Backup/Restore**. The **Backup / Restore** view appears.

Figure 141: Parameter Backup / Restore



4. To make a backup file of the current configuration, click **Backup** in the **Backup/Restore** window. The File Download popup appears.
5. Click **Save**. The **Save As** popup appears.
6. Select a location and enter a file name, then save the file.

Note:

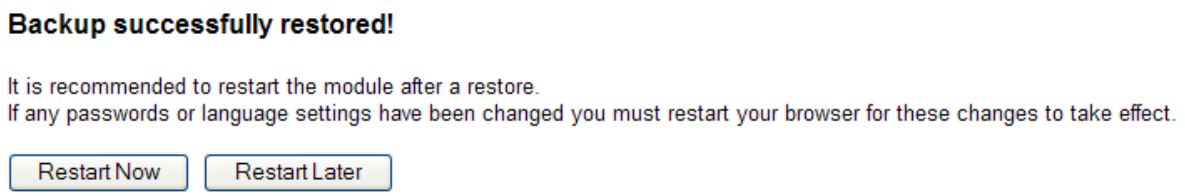
The backup does not include customized GUIs (including NetPage files), software files (.bin files) and certificates.
Since AIWS Edition 3 version 2.7x, the backup file includes the NetPage section on the ftp side, the loaded software, and packet files as well as the user data including local contacts. So the size of a backup file could increase significantly.

Restoring the configuration

Note:
When the AIWS is restored, all changes that have been made since the last backup will be discarded.

1. Click **Configuration** on the start page.
2. Select **Other Settings > Backup/Restore**. The **Backup / Restore** view appears.
3. Click **Browse...** and select the backup file.
4. Click the **Restore** button. An information window will open and inform you when the restore is ready.
5. Click "**Restart Now**" to reboot, else click "**Restart Later**". If the IP address or DECT interface has been changed the module needs to be restarted for the settings to take effect.

A restart will take a couple of minutes and during that time the module cannot be reached. When the restart is completed, the window will refresh to the Configuration page overview.



Since the .bin files are not restored, this has to be done manually. See Importing new software for devices on page 428 or Importing new software for devices on page 428.

Restore of NetPage files is described in Files for Translation/Editing on page 482.

Important:
A backup file taken on the Elise 2 (AIWS Hardware) can be reused to restore the configuration on the Elise 3 (AIWS2 hardware).

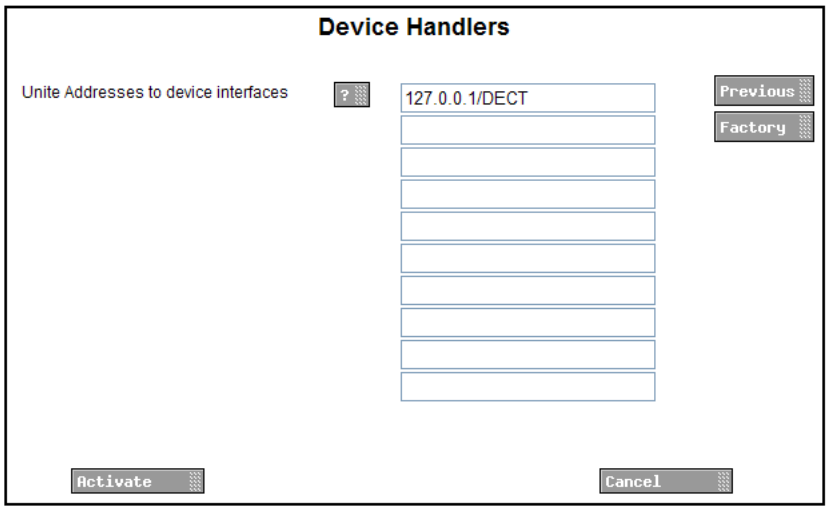
Device configuration

Device Management setup

This setup page is used to set addresses to theUnite modules that have the Device manager enabled. Additionally a service dedicated to the interface (for example the IP-DECT)T devices that are connected is also added to the address. The specified interfaces then inform the Device Manager about all devices that are logged in.

1. On the AIWS Start page, click **Configuration**. The **Configuration** page opens.
2. In the left pane, select **Other Settings** > **Advanced Configuration**. The **AIWS Advanced Configuration** page appears.
3. Click **Device Management**. The **Device Handlers** page appears.

Figure 142: The Device Handlers page.



4. Enter the address to the Unite module that is handling the Device Manager, followed by the appropriate service.

- If IP-DECT handset is to be managed in the Device Manager, enter <Unite IP address>/DECT
- If IP-DECT Base Station is to be managed in the Device Manager, enter <Unite IP address>/IPDECT

5. Click **Activate**.

Device handling configuration

IP-DECT Handsets and Chargers

It is possible to set the types of devices that can login to AIWS. This enables a possibility for example, to enable portable devices log in to one device manager and to enable chargers to log in to another device manager.

1. Login to AIWS.
2. Click on **Configuration**.
3. In the left pane, select **Other Settings > Advanced Configuration**.
4. Under DECT Interface, select **Device Handling**.

5. Select the ***device type*** to enable/disable login from
6. Change ***Status*** to desired value
7. Click **Activate.**

IP-DECT Base Stations

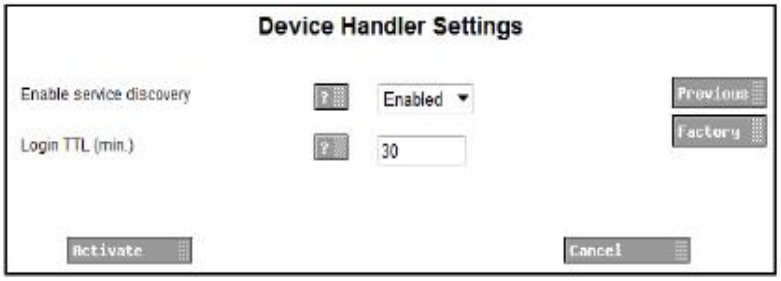
If your system having multiple Device Managers, it is possible to set which Device Manager the IP-DECT base station (IPBS) should logon to. This can be used to logon the IPBS to one Device Manager while another Device Manager for example can be used for handsets.

The IPBS can use either the Unite module's IP-address or the Service Discovery Domain ID to logon to the wanted Device Manager. This chapter is only applicable when Service Discovery Domain ID is to be used.

For example:

In the IPBS, the Service Discovery is enabled with Domain ID set to "UniteModule1", and the Domain ID in your Unite module is also set to "UniteModule1". For more information see Service discovery on page 465. In this case, enable the service discovery in your Unite module in order to logon the IPBS to the Device Manager that matches the Domain ID.

1. Click **Configuration** on the start page.
2. Select **Other Settings > Advanced Configuration** on the Configuration page.
3. Under IP-DECT Interface, click **Device Handling** in the menu on the Advanced Configuration page



4. In the Enable service discovery drop-down list, select **Enable** if the IP-DECT base station uses service discovery to find the Device Manager.
5. Click **Activate**.

On-line status report time for chargers

You can configure how often a device type must "log in" in order to be considered on-line. This is called "On-line Status Report Time". To enable moving a charger without being logged out, it is possible to set a "Status Log Delay Time".

If the device has not logged in again within the On-line Status Report Time, the Status Log Delay Time starts ticking. If the device does not log in again within that time a Status Report is sent to the Fault Log.

1. Login to AIWS
2. Click **Configuration**.
3. In the left pane, select **Other Settings > Advanced Configuration**.
4. In the left pane, select **Device Handling**.
5. Click on the ***device type*** to change settings for.
6. Enter **On-line Status Report Time** in minutes.
7. To set the margin, enter **Status Log Delay Time** in minutes.
8. Click **Activate**.

On-line Status report time for portable devices in a charging unit

You can configure how often a portable device type placed in a charging unit must "log in" in order to be considered online. This is called "On-line Status Report Time".

If the device has not logged in again within the On-line Status Report Time, it will be considered off-line.

1. Login to AIWS
2. Click **Configuration**.
3. In the left pane, select **Other Settings > Advanced Configuration**.
4. In the left pane, select **Device Handling**.
5. Click on the ***device type*** to change settings for.
6. Enter **On-line Status Report Time** in minutes.
7. Click **Activate**.

IP-DECT Base Stations

Relogin Time for IP-DECT Base Stations (Time to Live)

You can now configure how often an IP-DECT base station (IPBS) must “log on” to the Device Manager in order to be considered online. If the IPBS has not logged in again within the relogin time, it will be considered as logged out.

1. Click **Configuration** on the start page.
2. Select **Other Settings > Advanced Configuration** on the Configuration page.

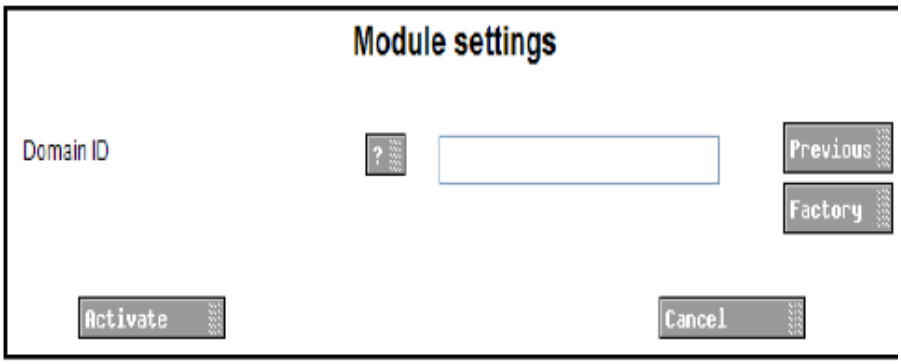
3. Under IP-DECT Interface, click **Device Handling** in the menu on the Advanced Configuration page.
4. In the Login TTL text field, select the maximum time (10 - 1440 minutes) the IPBS has to relogin before it will be considered logged out.
5. Click **Activate**.

Service discovery

Service Discovery allows automatic detection of devices and services on a network without prior configuration. AIWS2 and the devices that shall belong to that AIWS2 have to be set to the same Domain ID.

1. Click **Configuration** on the start page.
2. Select **Other Settings** > **Advanced Configuration** on the **Configuration** page.
3. Under **Other**, click **Service Discovery** in the menu on the **Advanced Configuration** page.
4. In the Domain ID field, enter the Service Discovery Domain ID.
5. Click **Activate**.

Figure 143: Module settings page



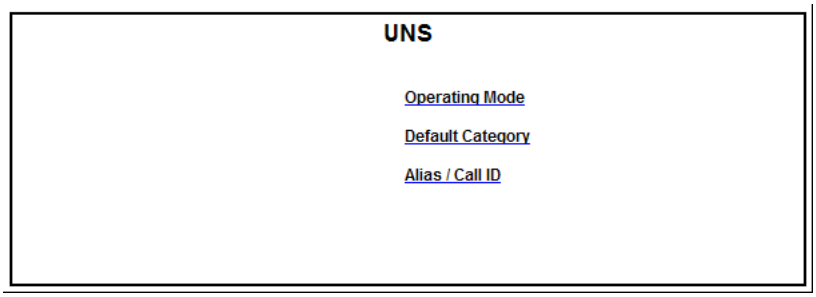
Additional System settings

Unite Name Server (UNS)

The UNS is used to resolve addresses into complete destinations. The AIWS can be configured to send all requests to the local UNS (stand-alone mode) or to forward all requests to a centralized UNS (forwarding mode). In forwarding mode, the local UNS will only be used if the centralized UNS cannot resolve the address.

1. Click **Configuration** on the start page. The **Configuration** page appears.
2. Select **Other Settings** > **Advanced Configuration** in the left menu in the **AIWS Configuration** page. The **Advanced Configuration** page appears.
3. Under Other, click **UNS**. The UNS page appears.

Figure 144: The UNS page.

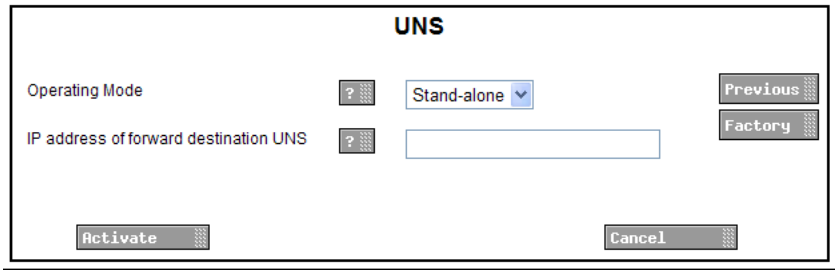


Operating mode

Operating mode is changed in systems with an Unite CM (Connectivity Manager) only.

1. To set Operating mode, click **Operating mode**. The **UNS Operating Mode** page appears.

Figure 145: The UNS Operating Mode page.



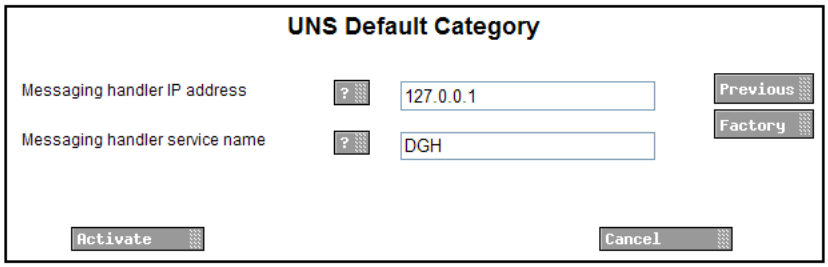
2. In a system with a Unite CM, set operating mode to Forwarding and enter the Unite CM IP address.
3. Click **Activate**.

Default category

The UNS Default Category is used to decide where messages from the AIWS shall be sent. The messaging handler is default set to localhost (127.0.0.1) which is the internal message group handler in the module. This can be changed if you want to use a messaging handler in another module. This parameter is changed when the IP-DECT system is connected to another module.

1. To set Default Category, click **Default Category**. The **UNS Default Category** page appears.

Figure 146: The UNS Default Category page.



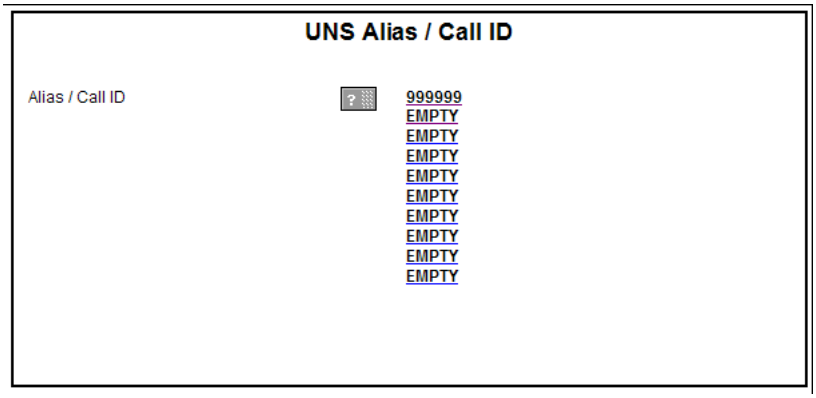
2. Enter the IP address of the module with the IP-DECT system connected. Set messaging handler to DGH.
3. Click **Activate**.

Alias / Call ID

Alias can be used when there are numbers that do not belong to the default category.

1. To set Alias / Call ID, click **Alias / Call ID**. The **UNS Alias / Call ID** page appears.

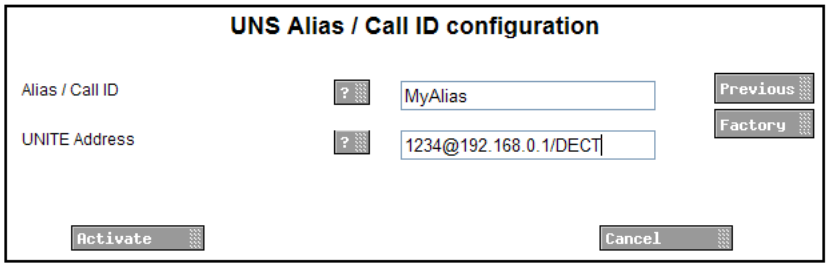
Figure 147: The UNS Alias / Call ID page.



999999 is a preset alias used for phonebook queries. It shall normally not be changed.

2. Click one of the links. The **UNS Alias / Call ID configuration** page appears.

Figure 148: The UNS Alias / Call ID configuration page.



3. Enter settings for UNS Alias / Call ID.

   In this example, a message that is addressed to **MyAlias** will be sent to the handset with telephone number 1234 in the IP-DECT system that is connected to the AIWS with the address 192.168.0.1.

4. Click **Activate**.

Logging

Status information can be stored locally, but can also be sent to a central log. The System Activity Log can store **activities** such as messages, alarms, faults, input/output activities, etc. Activity logging is useful for troubleshooting. The default status and system activity logs are stored locally but they can also be sent to another Unite module.

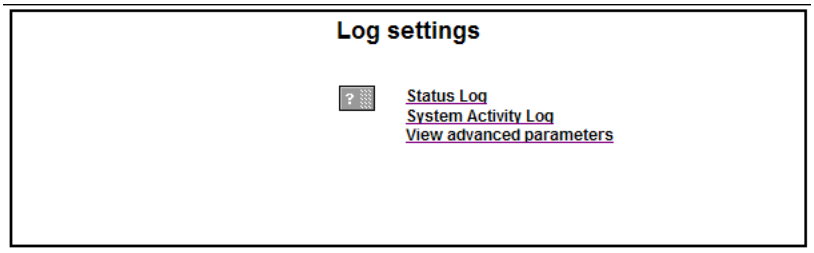
A Unite CM is needed for Activity Logging.

Note:

See Export activity logs to a Syslog server on page 454.

1. Click **Configuration** on the start page. The **Configuration** page appears.
2. Select **Other Settings** > **Advanced Configuration** in the left menu in the **AIWS Configuration** page. The **Advanced Configuration** page appears.
3. Under Other, click **Logging** The **Log settings** page appears.

Figure 149: The Log settings page.



4. Click **Status Log**, **System Activity Log** or **View Advanced parameters**.

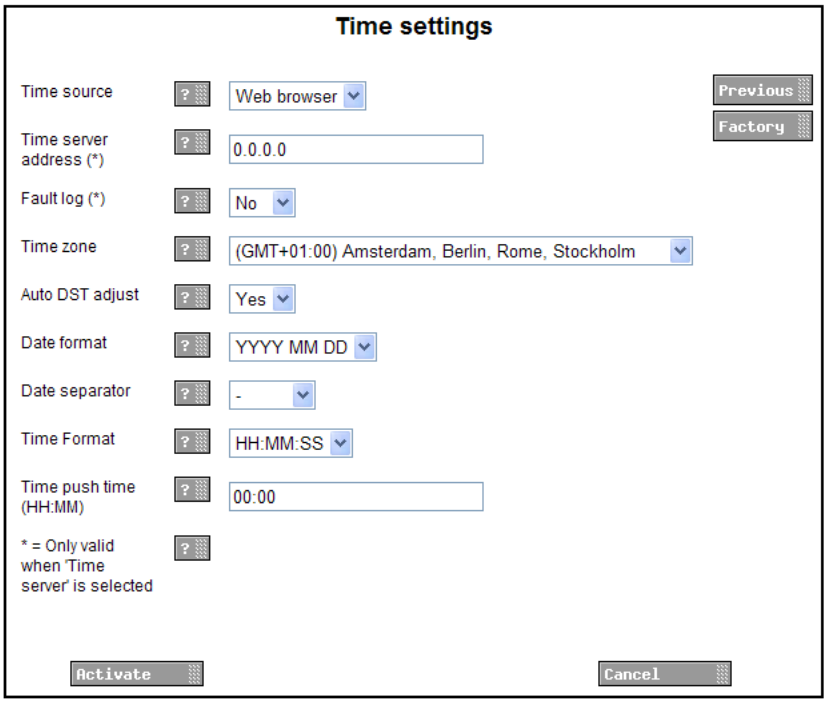
5. In the selected log page, enter settings. Click **Activate**.

Time Settings

It is possible to select where to fetch the time from, such as a web browser or a time server.

1. Click **Configuration** on the start page. The **Configuration** page appears.
2. Select **Other Settings** > **Advanced Configuration** in the left menu in the **AIWS Configuration** page. The **Advanced Configuration** page appears.
3. Under Time, click **Settings** The **Time settings** page appears.

Figure 150: The Time Settings page.



4. Enter time settings.
5. Click **Activate**.

The following parameters can be set via the Advanced Configuration page. Some of these parameters can also be set in the Setup wizard.

- Time source
- Time server address
- Fault log
- Time zone

- Auto DST adjust
- Date format
- Date separator
- Time Format
- Time push time

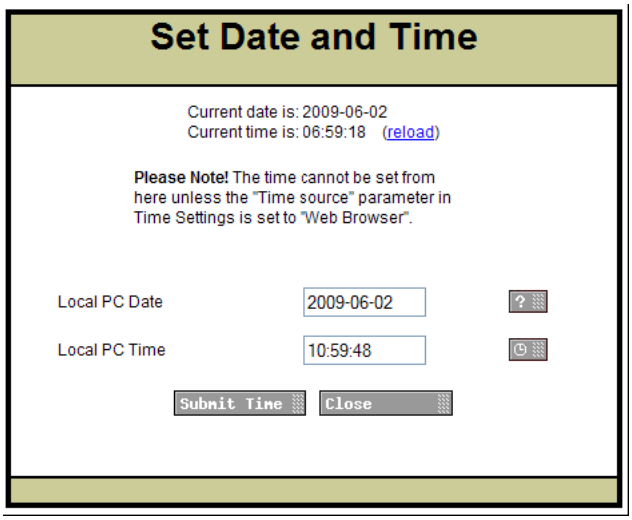
For additional information, see also Installing Elise 2 Server (AIWS Hardware) on page 523.

Setting time

If Web browser has been selected as time source, the time must be set manually. Otherwise this setting shall not be done.

1. Under Time, click **Set time** The **Set Date and Time** page appears.
2. Stop time counting by clicking on the approriate button on the right side.

Figure 151: The Set Date and Time page.



3. Enter date and time. Click **Submit time**.

Date and time can also be set in the Setup wizard.

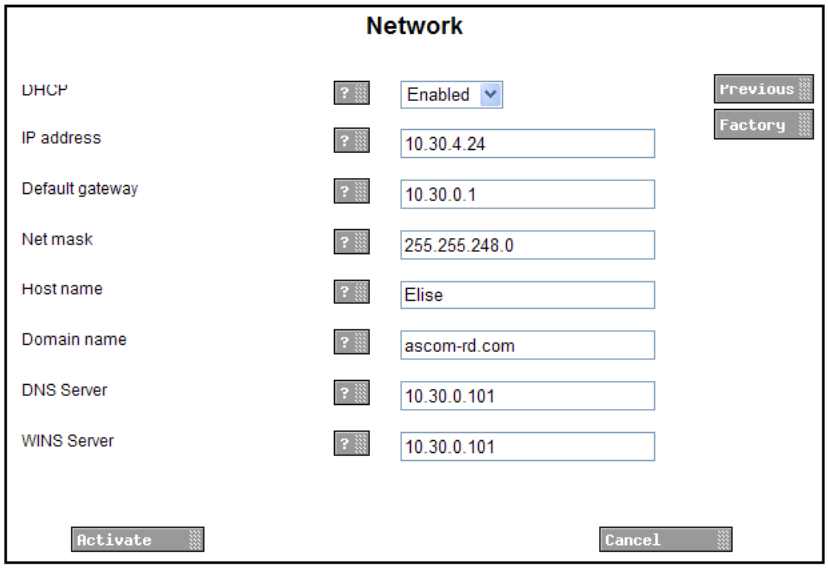
Changing power supply parameter

This chapter is for AIWS2 only, please refer to chapter Changing power supply parameters on page 577.

Configuring network settings

1. Click **Configuration** on the start page. The **Configuration** page appears.
2. Select **Other Settings** > **Advanced Configuration** in the left menu on **AIWS Configuration** page. The **Advanced Configuration** page appears.
3. Under Common, click **Network** The **Network** page appears.

Figure 152: The Network page.



The following parameters can be set via the Advanced Configuration page. Some of these parameters can also be set in the Setup wizard.

- DHCP
- IP address
- Default gateway
- Net mask
- Host name
- Domain name
- DNS Server
- WINS Server

For additional information, see also Installing Elise 2 Server (AIWS Hardware) on page 523.

4. Click **Activate**.

Setting license Number

It is possible to enter the license number via the **Advanced Configuration** page and the Setup Wizard. To set via the **Advanced Configuration** page

1. Click **Configuration** on the start page. The **Configuration** page appears.
2. Select **Other Settings** > **Advanced Configuration** in the left menu in the **AIWS Configuration** page. The **Advanced Configuration** page appears.
3. Under Common, click **License** The **License** page appears.
4. Enter License number.
5. Click **Activate**.
6. Reboot the AIWS.

Rebooting the phones

It is possible to reboot the AIWS via the **Advanced Configuration** page.

1. Click **Configuration** on the start page. The **Configuration** page appears.
2. Select **Other Settings** > **Advanced Configuration** in the left menu in the **AIWS Configuration** page. The **Advanced Configuration** page appears.
3. Under Common, click **Reboot.** The **Reboot** page appears.
4. To reboot the AIWS, click **Reboot**.

Note:

If the Reboot page is reloaded, another reboot is triggered.

Call Diversion

You can configure user friendly call diversion menus in the telephone using PDM/ AIWS2. These menus can then be selected in the handset by selecting Calls > Call services > Divert calls.

Note:
Beside the default call diversion menus, it is possible to define 10 extra system specific services codes.

1. Select Systems > System X (where X represents A - H).
2. Select PBX Settings > Diversion.
3. Select "Internal", "External", "On No Reply", "On Busy", and/or "All Calls"; enter the following:

- Prefix - the system specific prefix code to be used (if required by the PBX used)
- Suffix - the system specific code required to activate the diversion (for example "*21*")
- Cancel - the system specific code required to deactivate the diversion (for example "#23#").

The user can now enter the diversion number in the handset.

Absence Handling

Note:

The Absence List feature is not supported by the Avaya IP-DECT system.

You can configure user friendly absence menus in the handset using PDM/AIWS2. These menus can then be selected in the handset by selecting Calls > Call services > Absence. This menu is used to set the reason why a call cannot be answered, for example when you are in a meeting. The caller will be notified about the absence reason when he/she calling.

Beside the default absence menus, it is possible to define 10 extra system specific services codes. See Call services on page 220.

1. Select Systems > System X (where X represents A - H).
2. Select PBX Settings > Absence.
3. Select "Common codes", enter the following:

- Activation prefix - the system specific activation prefix code required to activate the absence (for example *23*)
- Activation suffix - the system specific activation suffix code required to activate the absence (for example #)
- Deactivation - the system specific code required to deactivate the absence (for example "#23#").

4. Select "Lunch", "Meeting", "Trip", "Vacation", "Out" and/or "General absence X"; enter the following:

- Activation code - the system specific code for an absence reason, for example "0*".
- Name - enter name of absence reason (only for General absence). The name will be visible in handset.
- User input - specifies if time or date is required for the absence reason (only for General absence). See Call services on page 220.

Remote Management

Through the AIWS, you can establish a remote connection to a customer site to configure and maintain sites, independent of the distance.

To be able to connect remotely, the remote management server in the AIWS has to be configured. The helptext buttons in the GUI will give more information about each parameter setting.

1. Click **Configuration** on the start page.
2. Select **Other Settings** > **Advanced Configuration** in the left menu on **AIWS Configuration** page.
3. Select **Remote Management** in the left menu. The **Remote Management Server** configuration page is opened.

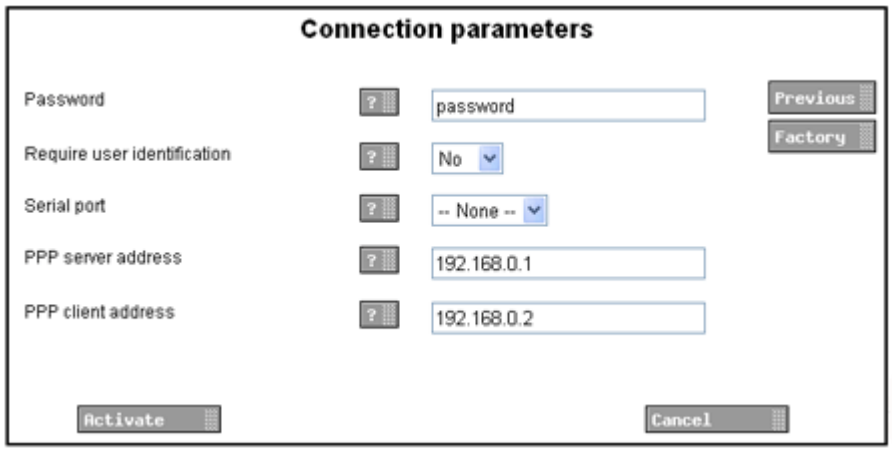


Remote connection

1. Click **Edit** for Remote Connection, to set up the connection parameters.

   Parameter notes:

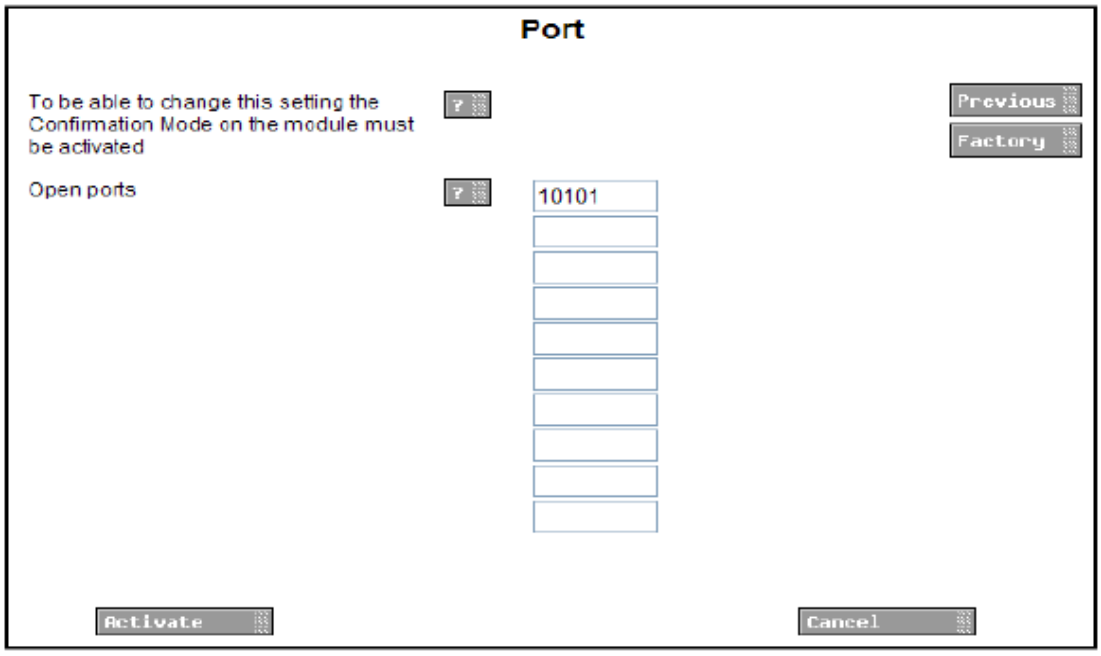
   Require user identification shall be set to **No**.



2. Set up the connection parameters and click **Activate**.

Setting open ports

1. Click **Edit** for Open Ports to open any additional ports that are needed for configuration tools. This is a secured setting and before it can be activated it must be manually confirmed by pressing the Mode button on the module. For TCP and Rs 232, port 10101 must be left open..



2. Set up the port parameters and click **Activate**. The system prompts you to confirm the change by pressing the Mode button.
3. Press the Mode button on the module.
4. Click **Activate** to save the changes.
5. Click the mode button to return to normal mode immediately or wait 10 minutes for the module to return automatically. Any secured setting can be activated within the 10 minutes period.

The module must be restarted for the changes to take effect.

Serial port channel

Not applicable.

Administration of language and user interface

All text shown in the user interface is by default in English but a copy of the language can be translated and imported to AIWS. Several languages can be added. The default English language is not possible to edit or remove. The supplied user interface can also be modified to suit the individual customer requirements concerning functionality.

Basic changes that can be made are:

- Translate or adapt text (refer to Translating/Editing the language on page 478).
- Hide unused functionality (refer to Changing the NetPage user interface functionality on page 487).
- Modify the user interface to suit the customer's image (refer to Customizing the user interface (GUI) on page 482).
  - Limit the number of characters included in the message text.
  - Add company logo and/or modify the GUI to suit the customer's image.

Note:

The AIWS user interface only supports the Latin-1 character set.

For the best screen appearance

Windows standard screen settings, using normal font size, are recommended. The recommended screen resolution is 1024 x 768.

How to edit

The code is thoroughly commented to make it easy to understand, and can be edited with a simple text or HTML editor. Basic HTML, Java Script, and CSS knowledge is recommended.

Note:

Do not use an intelligent html editor like Frontpage or Dreamweaver, as it might corrupt the html code.

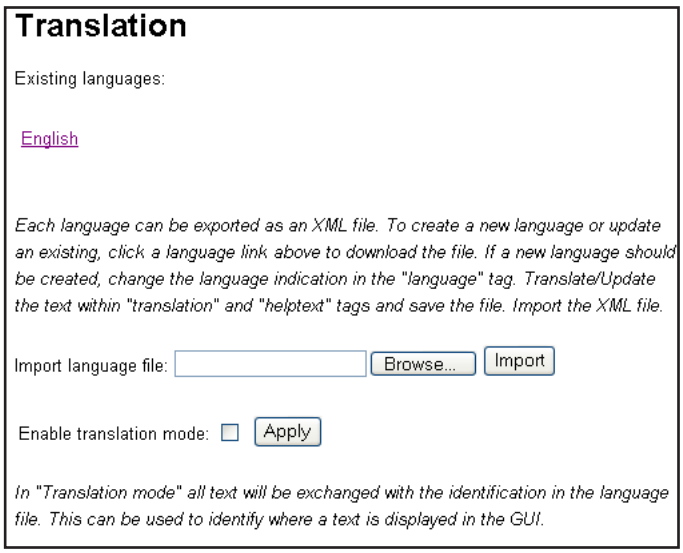
Customizing the language

Note:

There is a difference between *Translation files* (.xml) described in this section and *Language files* (.lng). Translation files are used to change the language to be used in the AIWS. The Language files (.lng) are files that may be imported and uploaded to a device, see description in Importing language files for devices on page 430.

Exporting a language for Translation/Editing

1. Click **Configuration** on the start page.
2. Enter ***User name*** and ***Password*** and click **OK**
3. Select **Other Settings > Set language** in the left menu on the **AIWS Configuration** page. The **Set language** page opens.
4. Click the **Import/Export Language** button. The **Translation** page opens.



5. Click an existing language link to create or update languages. An XML file is generated from the AIWS and a **File download** window opens.
6. Save the file for translation or editing purposes. The file can be saved in any name during the translation.

Translating/Editing the language

In the downloaded language file, there are numerous tags, but only the translation of two tags and one attribute are mandatory:

- <language id=”English”>
  The “id” attribute is the text that appears in the drop-down list. Change **English** to the name of your translated language here.
- <translation>
  Text displayed in menus, on buttons, tabs etc. Translated text can be added inside the tags.
- <helptext>
  On-line help text. Translated text can be added inside the tags

Below is an example of a language file (just showing two buttons with helptext, for simplicity).

Figure 153: Example of a translation file

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<translations>
 <language id="English" type="complete">
  <app id="Alarm Manager">
   <text id="ACTION_TYPE_SELECTOR">
    <translation>Action Type</translation>
    <helptext>Select which type of action to take.</helptext>
   </text>
   <text id="ACTIVATE_EHCONF_OK">
    <translation>Activation of configuration OK.</translation>
   </text>
   <text id="ALARM_TYPE_SELECTOR">
    <translation>Alarm Type</translation>
    <helptext>The alarm type that should be triggered. </helptext>
   </text
  </app>
 </language>
</translations>
```

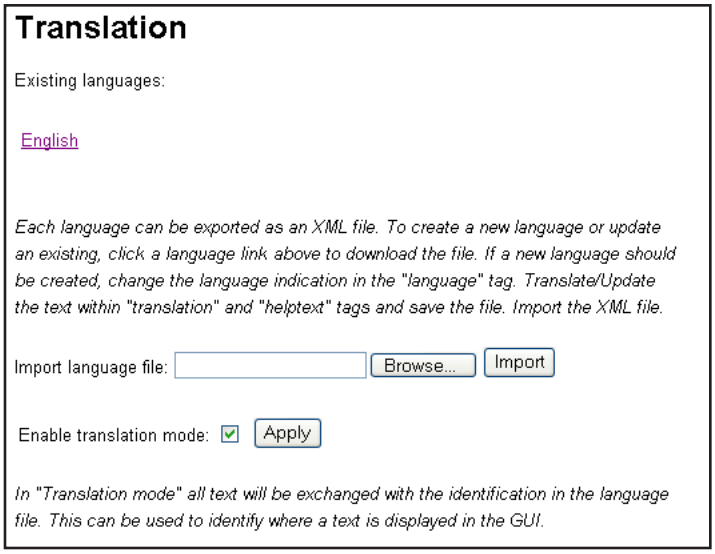
079

Showing pages in translation mode

All texts, buttons, menus etc. are identified with labels (for example TEXT_TRANSLATION_TITLE). With the translation mode function it is possible to view the label for each button, menu etc. This can be helpful when translating the language file. For not losing one´s bearings during the translation it is a help to open two windows and view one of them in translation mode and the other in normal mode.

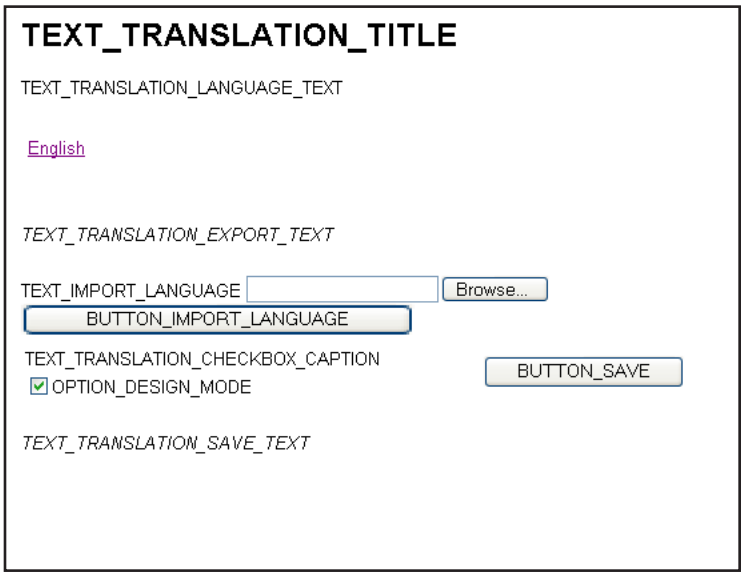
1. Select the **Enable translation mode** check box in the **Import/Export Language** page, and click **Apply**.

Figure 154: Translation page in normal view



All the labels on the pages are shown, see example below.

Figure 155: Translation page in translation mode



To return to standard view:

2. Clear the **OPTION_DESIGN_MODE** box.
3. Click **BUTTON_SAVE**.

Importing translation files

When the file is translated, it must be imported to the AIWS.

1. On the **AIWS start page**, click on **Configuration**. The **AIWS Configuration** page opens.
2. In the left pane select **Other settings > Set language**. The **Set language** page opens.
3. Click on the **Import/Export Language** button. The **Translation** page opens.
4. Click **Browse** to locate the translated file and click the **Import** button.

The name of the translated language (the language **id** attribute) will appear as a link in the Existing Language list and can be downloaded for editing purposes.

Deleting language

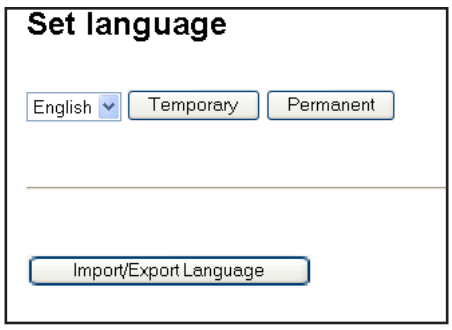
On the **Translation** page, click the **Delete** symbol to the right of the language you want to remove, see below. Note that it is not possible to remove the default language.



Selecting language

Translated languages (the language **id** attribute) are shown together with the default language **English** in the language drop-down list in the **Set Language** page.

1. Click **Configuration** on the start page.
2. Enter ***User name*** and ***Password*** and click **OK**
3. Select **Other Settings > Set language** in the left menu on the **AIWS Configuration** page.



4. Select language in the drop-down list and click **Permanent**.

   To change language for this session only, i.e. for this browser window until closed, click **Temporary**.

Customizing the user interface (GUI)

AIWS has 5 Mb disk space on the FTP area and about 1.6 Mb is dedicated for the user interfaces. The free space can be used for storing files and folders, for example, a customized user interface for sending messages.

The AIWS 2 has an FTP area with default 50 MB disk space. The disk space can be set in the interval 5 MB up to 150 MB.

About 1.6 Mb of the disk space on the FTP area is dedicated for the NetPage user interfaces. The free space can be used for storing files and folders, for example, a customized user interface for sending messages.

Changing the size of the FTP Area (AIWS2 only)

This is a secured setting and before it can be activated it must manually be confirmed by pressing the mode button on the module.

1. Click “**Configuration**” on the start page.
2. Select **Other Settings > Advanced Configuration** in the menu on the **Configuration** page.
3. Select **FTP area** under **Common** in the menu on the **Advanced Configuration** page.
4. Fill in required size between 5 – 150 MB and click **Activate**.
5. Press the **Mode** button on the module. This is a secured setting so you will be prompt to confirm the change by pressing the mode button.
6. Click **Activate** to save the changes.
7. Click the **Mode** button to return to normal mode immediately or wait 10 minutes for the module to return automatically. Any secured setting can be activated within the 10 minutes period.
8. The module needs to be restarted for the changes to take effect.

Note:

Changing the size of the FTP area without pressing the **Mode** button to switch to confimation mode results in a misleading error message as follows: "‘One or more of the parameters are not valid. Please review your changes and try again."

Files for Translation/Editing

1. Log on to the module via an FTP client. The log on process can be different for FTP clients. The Internet Explorer is not an FTP client; it can be used for viewing but not for transferring files.

2. Log on with default username as “ftpuser” and default password as “changemetoo”. The hostname is xxx.xxx.xxx.xxx.

   Examples:

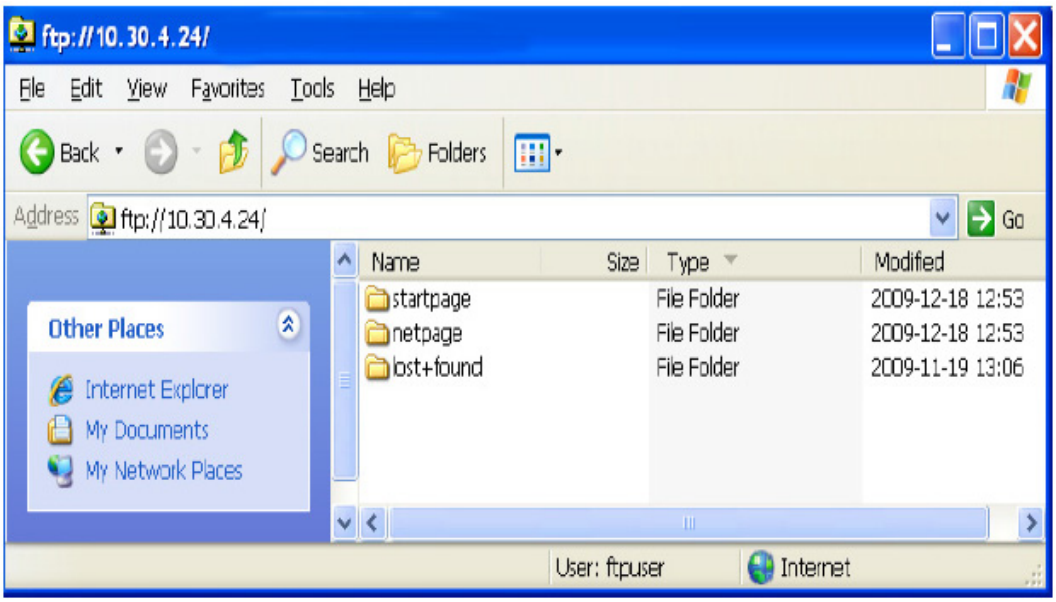
   • Windows Explorer: fill in “ftp://username:password@xxx.xxx.xxx.xxx” in the

   address field.

   • Firefox: fill in “ftp://xxx.xxx.xxx.xxx” in the address field and log on with “username” and “password”.

   The files located in the Start page and NetPage folders, including GIFs and CSS, can be downloaded/copied to a folder on your hard disc.

Figure 156: Folders on the FTP area



When restoring NetPage files, the files shall be placed in the same folder.

When secure mode is enabled, see Web access security settings on page 380, only secure access via HTTPS and FTPES is allowed. HTTP is automatically redirected to HTTPS and FTP access is not allowed. The FileZilla Client freeware (not included) supports FTPES.

Default User Interfaces

Default start page GUI

Figure 157: Start page default user interface (index_template)

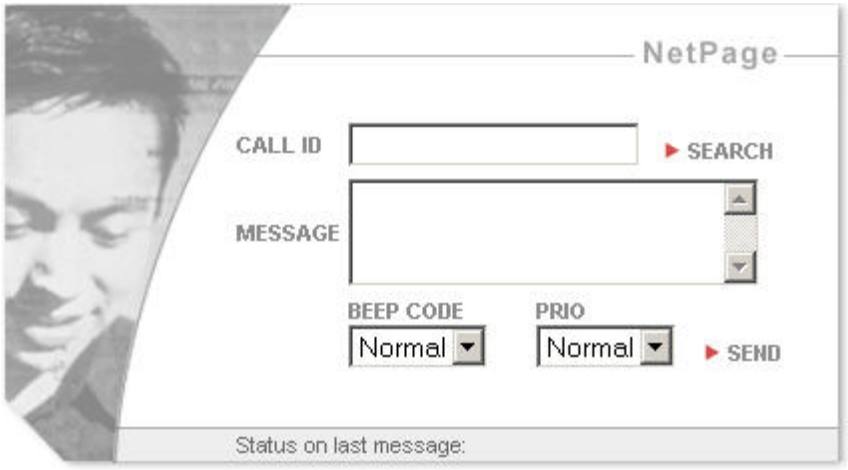


A copy of the default AIWS Start page, see figure 157 above, is stored in the start page folder on the AIWS FTP area. The start page copy *index_template,* is an html file which can be copied and edited. It is also possible to replace the start page with a completely new user interface.

When the edited or new html file is saved as **`index.html`** and placed in the Start page folder on the AIWS FTP area, it will replace the default start page.

Default Send Message GUI

Figure 158: NetPage default user interface (index3)



The default NetPage user interface is index.html located on the AIWS FTP area and is opened from the start page by clicking **Send Message**. See figure 158 above.

Note:

On AIWS2, this is only valid if you select "Custom" for the default GUI on the Advanced configuration - Web messaging page.

In the NetPage folder on the AIWS FTP area there are four examples of the NetPage user interface, *index1*, *index2*, *index3* and *index4*. Index3 is a copy of the default NetPage user interface.

All NetPage functionality is included in the default user interface, but all parameters that can be configured in the example user interfaces index1, index2 and index3, are not shown. The necessary code for viewing and configuring the hidden parameters is included, but they are marked as comments to prevent the browser from interpreting them, see figure 160 and figure 161 on page 488.

The default user interface can be exchanged with one of the example user interfaces, shown in figure 159 on page 486, by saving the html file as **`index.html`** and replacing the existing **`index.html`** file. *index4* is shown in figure 162 on page 490.

Note:

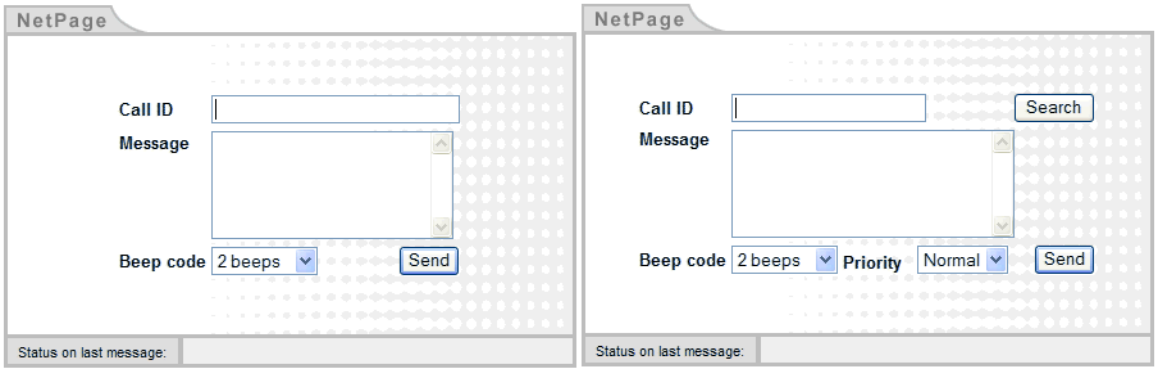
When changing the index.html or changing the setting for the default GUI on the Advanced configuration - Web messaging a reload of the new page is needed in your web browser. Press refresh (F5) on the netpage window to force the reload..

Selecting a predefined message (when using the index4.html interface) will replace the already typed message in the message text.

Do not modify the Javascript code and the applets as they are used to interpret and display responses from the messaging system. Modifying the code may result in loss of Message History functionality.

No server side scripts are allowed in the FTP area.

Figure 159: NetPage user interface examples; index1 and index2



Priority and Beep Codes in the default NetPage User Interface

GUI Description	Priority Code
Low	9
Normal	7
High	3
Alarm[1]	1

1. Marked as hidden in the html page (index.html). To make the alarm priority option available, remove the comment and save the file in the ftp area. When using index4.html, these changes need to be done in several files, see Changing the NetPage user interface functionality on page 487.

GUI Description	Beep Code
Silent	0
1 beep	1
2 beeps	2
3 beeps	3
4 beeps	4
5 beeps	5
10 beeps	6
Siren	7

Note:

The system does not distinguish between the number of beep codes. Beep codes 0 (Silent), 2 (Normal) and 7 (Siren) are supported by default. To make the other beep codes available, the html page (index.html) has to be modified.

Changing the NetPage user interface functionality

As a help for locating comments/hidden text in the html code, the comment marks " <!--" and "-->" are used, see the example in figure 160. The comment marks are also used to hide functionality in the user interface. Text written, or functionality, framed by the comment marks is not interpreted by the web browser.

Figure 160: Example of how to mark html text as comments, i.e. hide it

```
<TD valign="top" style="height:25">
  <!-- This is the button that opens the NetPage phonebook.
  If the phonebook is not used, remove the complete script and
  the    line (mark it as comments to be able to
  include it again later on) -->
```

880

For comments included in the JavaScript code, the comment mark "//" is used, see figure 161. Text written after the comment mark (in the same line) is not interpreted by the web browser.

Figure 161: Example on comments in a JavaScript

```
function sendform() {
  addCallNo(document.testform.callno.value, '');
  // If the user forgot to press 'add'
  tmplist = document.testform.callnolist;
```

689

Buttons, for example the **To** button that opens the phonebook, can also be hidden directly in the code. To do this, insert "hidden" (double quotation marks both before and after "hidden") as input type as follows:

document.write('<input type="button" value="...

will become

document.write('<input type="hidden" value="...

Note:
To change the user interface (index4) it is necessary to open and change one or more of the files: **send.html**", **receive.html**" and **admin.html**".

Note:
If changes to the phonebook access (**To** button), beep codes or priority settings are made, it is also necessary to change the files **editpagtext.html** and **leditpagtext.html**, to get a consistent user interface.

Note:
In order to be able to restore the default GUI, make a backup before changes. See Backing up and restoring NetPage files on page 502.

Translation of the user interfaces

The texts presented in the user interfaces can be translated. The translation is entered differently depending on the example user interface that is used. The HTML files *index_template* and *index1, index2* and *index3* are translated in the HTML code. The NetPage user interface (index4) on the other hand is translated in the **language.js** and **receive.html** file, where receive.html includes the NetPage message history applet. See figure 162 on page 490 for an overview of where the different files are used.

Start Page

1. Download/copy the file and included image from the FTP area, refer to Files for Translation/Editing on page 482.
2. Open the file in a text or HTML editor and translate all words.
3. Save the file.
4. Upload/paste the file to the FTP area, refer to Uploading the files to the AIWS FTP Area on page 491.
5. Check that the user interface looks all right.

Example User Interfaces index1, index2 or index3

1. Download/copy the file and included images from the FTP area, refer to Files for Translation/Editing on page 482.
2. Open the file in a text or HTML editor and translate all words and "immediate status" texts. For existing "immediate status" texts, see table below.
3. Save the file.
4. Upload/paste the file to the FTP area, refer to Uploading the files to the AIWS FTP Area on page 491.
5. Check that the user interface looks all right.

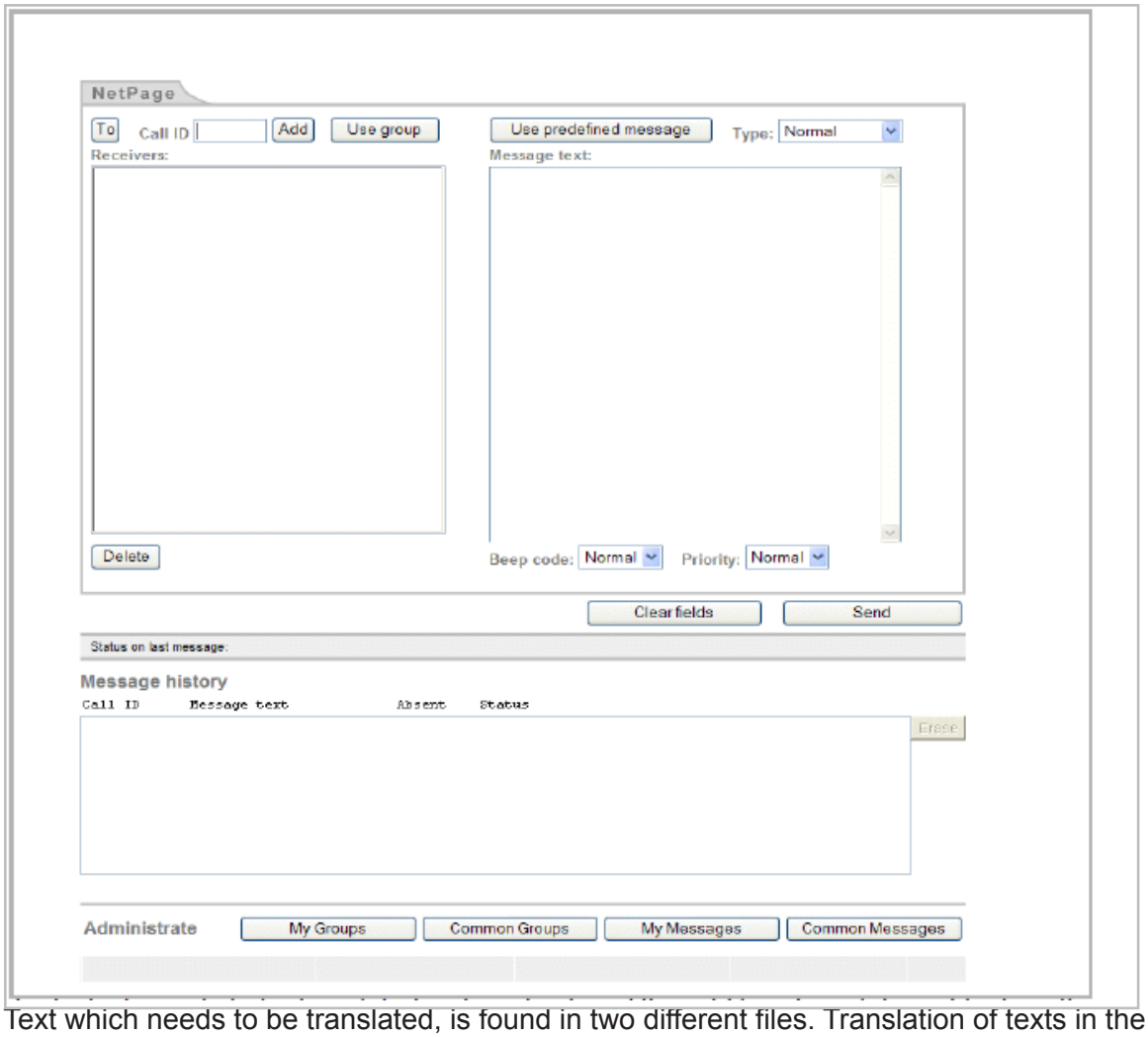
The following "immediate status" texts must be translated. Exchange the English text with your translation. Keep the code (20, 30 etc.) unchanged.

20	Message accepted
30	Memory full in message service
31	Message deleted due to time-out
40	Message not sent, invalid Call ID
nst	Message not sent
nlc	Message canceled, no license
sto	Status time-out from message service
sns	Can’t receive status

nan	Message canceled, no Call ID
oor	Call ID(s) out of number range
	Unknown returncode, confused!

Example GUI index4

Figure 162: Files used for translation of the user interface (index4)



Text which needs to be translated, is found in two different files. Translation of texts in the user interface (including text in Administrate pages, but excluding text in the Java Applet) are found in the **`language.js`** file. Translation of the Java Applet (Message history field) is found in the **`receive.html`** file.

1. Download/copy the files **language.js** and **receive.html** from the FTP area, refer to Files for Translation/Editing on page 482.
2. Open the **language.js** file in a text editor, for example Wordpad.
   a. Add the translation inside the quotation marks after the English text, see example below:

      `"Add Group", " "` will become `"Add Group", "Your translation".`

   b. Save the file.
3. Open the **receive.html** file in a text editor, for example Wordpad.
   a. Add the translation inside the quotation marks after the English text, see example below:

      `PARAM NAME="English text" VALUE="Your translation".`

   b. Save the file.
4. Upload/paste the files to the FTP area, refer to Uploading the files to the AIWS FTP Area on page 491.
5. Refresh the page and check the result. All buttons except the Administration buttons will expand/decrease when the text is translated. The width of the Administration buttons is fixed but can be altered in the HTML file **admin.html**.

Uploading the files to the AIWS FTP Area

Upload/paste all updated AIWS files (including GIFs and CSS) to the AIWS FTP area.

When secure mode is enabled, see Web access security settings on page 380, only secure access via HTTPS and FTPES is allowed. HTTP is automatically redirected to HTTPS and FTP access is not allowed. The FileZilla Client freeware (not included) supports FTPES.

1. Log on with an FTP client. Note that how to log on can differ between different FTP clients. Note that Internet Explorer is not an FTP client; it can be used for viewing but not for transferring files. Default username is “ftpuser” and default password is “changemetoo”. xxx.xxx.xxx.xxx is the host name.
   Examples:

- For Windows Explorer, fill in “ftp://username:password@xxx.xxx.xxx.xxx” in the address field.
- For Firefox browser, fill in “ftp://xxx.xxx.xxx.xxx” in the address field and log on with “username” and “password”.

2. Copy the files and paste them into the FTP area.

Inserting a company logo

In the default GUI, a company logo can be inserted, for example, in a separate table above the NetPage application.

In the examples index1, index2 and index3, the company logotype can be inserted in any of the empty table cells of the NetPage application.

Password Protected Access to NetPage

For AIWS

If access to NetPage has to be password protected, do as follows:

1. Log on to AIWS with an FTP client. When secure mode is enabled, see Web access security settings on page 380, only secure access via HTTPS and FTPES is allowed. HTTP is automatically redirected to HTTPS and FTP access is not allowed. The FileZilla Client freeware (not included) supports FTPES. Log on with "**ftpuser**". The default password is "**changemetoo**".

Examples:

- Windows Explorer: fill in “ftp://username:password@xxx.xxx.xxx.xxx” in the address field.
- Firefox (AIWS2 only): fill in “ftp://xxx.xxx.xxx.xxx” in the address field and log on with “username” and “password”.

2. Change the name of the file **`htaccess`** to **`.htaccess`** (a point is added in front of the name).

With this modification, one has to log on with the user name "**user**" to get access to NetPage. The default password is "**password**".

When secure mode is enabled, see Web access security settings on page 380, only secure access via HTTPS and FTPES is allowed. HTTP is automatically redirected to HTTPS and FTP access is not allowed. The FileZilla Client freeware (not included) supports FTPES.

For AIWS2

See NetPage configuration on page 494.

Accessing NetPage from a Cordless Unit with WAP

NetPage can be accessed from a cordless unit that supports WAP. Two WML pages for this purpose are included in NetPage. The page that is accessed is called **`send.wml`** and the response is shown on **`receive.wml`**.

The included WAP application enables specifying a Call ID and a message text. When the message has been sent the receive page is opened and the send status is shown. The send application is accessible from the receive page in case another message should be sent.

Note:

If the cordless unit uses WAP version earlier than 2.0 it has to be stated that the message is UTF8 encoded. See *UTF8 encoded* on page 493 for more information.

UTF8 encoded

When NetPage is accessed from a cordless unit that uses WAP version earlier than 2.0, the message that is sent will be UTF8 encoded. The parameter "utf8" then has to be included to indicate this for the CGI script in NetPage. The parameter "utf8" has to be given a value but the value has no meaning, i.e. it can be any value.

Testing the new user interface

It is recommended to test the customized user interface as follows, for example:

- If a company logotype is added, check that it looks all right and that AIWS opens quickly. If AIWS opens slowly, minimize the picture file size and save it as "interlaced" to decrease wait time for the image.
- Check that all text is correctly translated.
- Check that the phonebook opens and that the entries are correct.
- Send a message.
- Check that the **message history status** is received and displayed.

Updating the user interface after a new AIWS Release

When a new version of the AIWS is released, there might be changes in the user interface that need to be translated.

1. Import your old translated file to the new AIWS software version. New text and buttons in the user interface are shown in English.
2. Click the language file link and save it.
3. Open the file. All tags that are not translated are marked with the comment:
   <!-- The text identifier below couldn't be translated -->
4. Translate the new text and import the translated file again.

Messaging

Depending on AIWS item (see Licenses on page 361), different tools for messaging are displayed:

- Messaging Tool - for AIWSs without NetPage
- NetPage - for AIWSs with NetPage

Operation of the Messaging Tool is described in Operation on page 387.

Messaging Tool configuration

It is possible to change the title of the Messaging Tool webpage.

1. Click “**Configuration**” on the start page. The **AIWS Configuration** page appears.
2. Select **Other Settings** > **Advanced Configuration** in the left menu on **AIWS Configuration** page. The **AIWS Advanced Configuration** page appears.
3. In the left pane, click **Messaging Tool**. The **Messaging Tool** page appears.

Figure 163: The Messaging Tool page.



4. Enter text to be shown as the title. Click **Activate**.

NetPage configuration

Configuring NetPage messaging

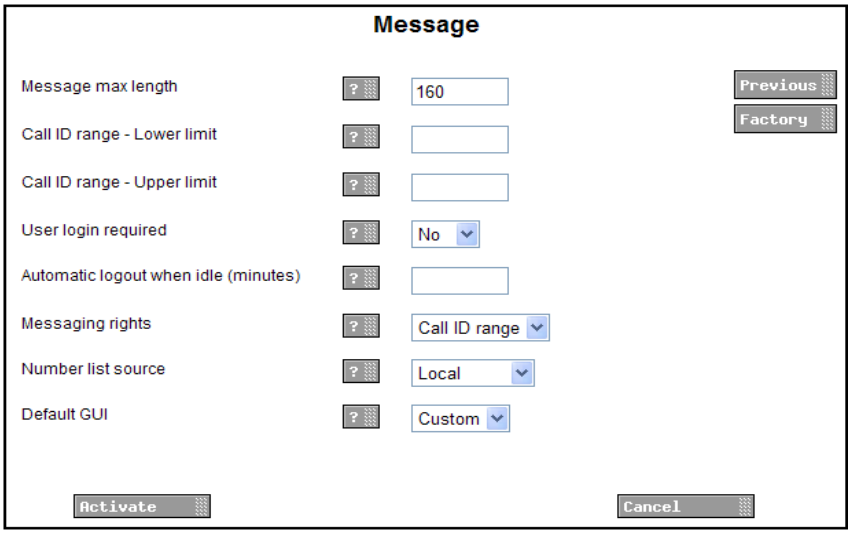
The following settings are applicable for NetPage web messaging.

For AIWS2 (only): Besides the settings for NetPage web messaging it is also possible to select which GUI to use as default for NetPage.

To set messaging properties:

1. Click **Configuration** on the start page. The **AIWS Configuration** page appears.
2. Select **Other Settings** > **Advanced Configuration** in the left menu on **AIWS Configuration** page. The **AIWS Advanced Configuration** page appears.
3. Select **Web Messaging** in the left menu. The **Message** page appears.

Figure 164: The Message configuration page.



Note:
The setting for the Default GUI is available in AIWS2 only.

4. Enter values for messaging.
5. Click **Activate**.

The following parameter can be set:

- Message max length.
  Sets the maximum number of characters that can be forwarded to a unit. Messages longer than the set value are truncated.
- Call ID range - Lower limit
  Sets the lower limit of a Call ID range. Messages sent to Call IDs out of this range are canceled. If a group of Call IDs partly consists of Call IDs out of this range, the message will only be sent to the Call IDs within the range. An empty field means no lower limit.
- Call ID range - Upper limit
  Sets the upper limit of a Call ID range. Messages sent to Call IDs out of this range are canceled. If a group of Call IDs partly consists of Call IDs out of this range, the message will only be sent to the Call IDs within the range. An empty field means no upper limit.

Note:

If an upper and/or lower limit for the Call ID range is set messages using an Alias / Call ID will not be sent anymore. The Alias value will not pass the limit check in this case.

- User login required (No or Yes)
  Sets whether a login is required for NetPage. If a Unite CM module is used as "User Server", users configured in the Unite CM can also log in. This parameter shall be set to no for the default GUI (index3). If index4 is used, the Message History section must be included. Refer to Customizing the user interface (GUI) on page 482.
- Automatic logout when idle (minutes)
  Sets how long a user can be idle before being logged out. To prevent automatic logout, leave this field empty. If the parameter **User login required** is set to **No**, leave this field empty.
- Messaging rights. Choose between Call ID range and User rights to determine how NetPage shall verify Call IDs.
  Call ID range means that Call IDs are verified according to the Call ID range limit settings. This setting shall always be used for systems without theUnite CM module.
  User rights means that Call IDs are verified according to the settings in the Unite CM module. This requires that the parameter **User login required** is set to **Yes**.
- Number list source. Choose between Local and Unite CM users.
  This is the Number list that is used in NetPage. In systems without an Unite CM, this parameter shall always be set to **Local**.
- Default GUI (Applicable to the AIWS2 only). Select which GUI to use as start page for NetPage. Choose between Index 1, Index 2, Index 3, Index 4 that are hard coded page layouts and the "Custom" which refers to the index.html in the ftp netpage area.
  See Customizing the user interface (GUI) on page 482 for more information on the different GUIs.

Note:

Changing the setting of the defaul GUI requires a refresh (F5) of the netpage in your browser.

Creating or updating the number list

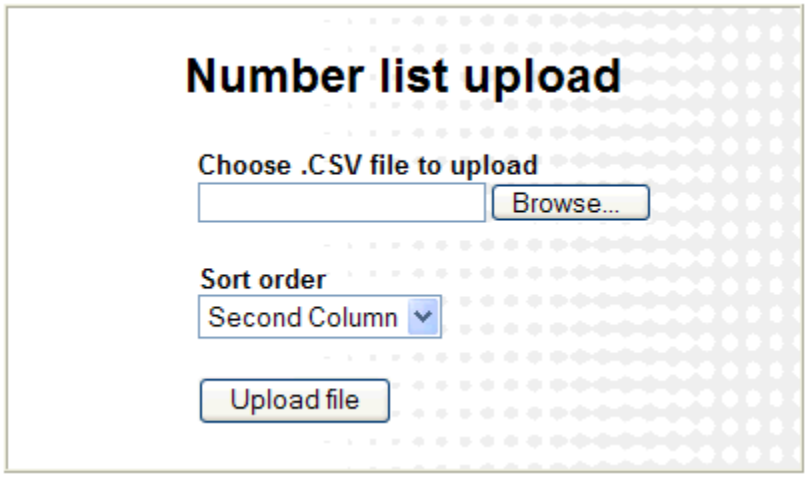
In the NetPage default GUI (index.html), a number list can be accessed by clicking the **Search** button. Before the number list can be used, the entries have to be added.

The number list entries can be created from any CSV file, using Microsoft Excel or any leading spreadsheet or relational database application.

For AIWS2 it is possible to import maximum 3000 entries via the CSV file.

The CSV file is uploaded/pasted with the **Number list upload** program (included in NetPage) as described below.

Figure 165: The page for uploading a new or updated CSV file.



1. Create a CSV file with the following format:

   First name 1;Surname 1;Phone number 1

   First name 2;Surname 2;Phone number 2

2. Open the page: http://xxx.xxx.xxx.xxx/admin/user/uploadnrlist.html.
   Log on with "user**"**. The default password is "password".
   The application shown in figure 165 will appear.

3. Browse to find the CSV file. Choose the sort order. Click on **Upload file**.

   When the CSV file is uploaded, it will be converted and saved as **`uploadednrlist.js`**. The file is a text file with the following format:

   nr_array=[[“First name 1”,”Surname 1”,”Phone number 1”],[“First name 2”, ”Surname 2”,”Phone number 2”]];

   If you later want to edit the number list, the **`uploadednrlist.js`** file is accessible with the ftp client and can also be modified manually.

4. Test that the number list works as desired.

5. Make a backup of the **`uploadednrlist.js`** file, see further in Backing up and restoring NetPage files on page 502.

Note:

When the number list has been updated, be sure to clean the cache memory on the web browser.

Predefined groups

Note:

My Groups are created from the NetPage and are not to be mistaken for the groups created from the Configuration page in AIWS. This functionality is only accessible from index4, see figure 162 on page 490.

Common groups

Common Groups can be used by all NetPage users. It is possible to create up to 30 predefined **Common Groups** with up to 50 Call IDs in each. These groups are stored on the FTP area.

My groups

My Groups are stored locally and can only be accessed or changed from the PC where they are stored.

There is a limited storage area. This means that, for groups with approximately 20 characters (name and Call ID), the following applies:

Amount of Groups	Group Members
10	19
15	7
20	2

Creating groups in My Groups

1. Click the **Common Groups** or **My Groups** button in NetPage. For **Common Groups** enter the user name "user" and the password "password".
2. Click **Add group**.
3. Enter a name for the group in the **Name** text field.
4. Click the **To** button and select users (from the phonebook) to be members of this group or enter number in the Call ID text field and click **Add**.
5. Click **Save**.
6. Click **Close** to exit the administration.

Editing Groups

1. Click the **Common Groups** or **My Groups** button in NetPage. For **Common Groups** enter the user name "user" and the password "password".

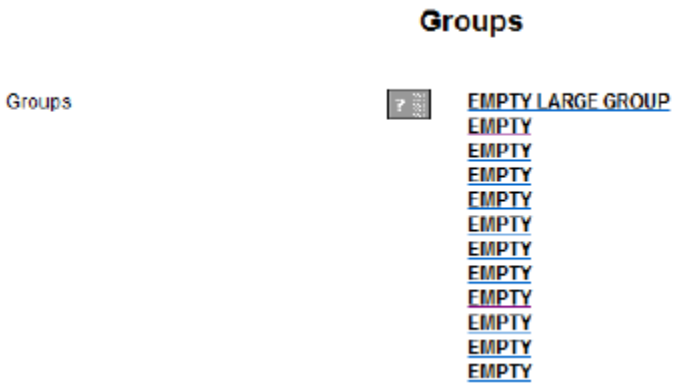
2. Select the groups that should be changed and the administration field will open.
3. Make changes and click **Save**.
4. Click **Close** to exit the administration.

Creating messaging groups

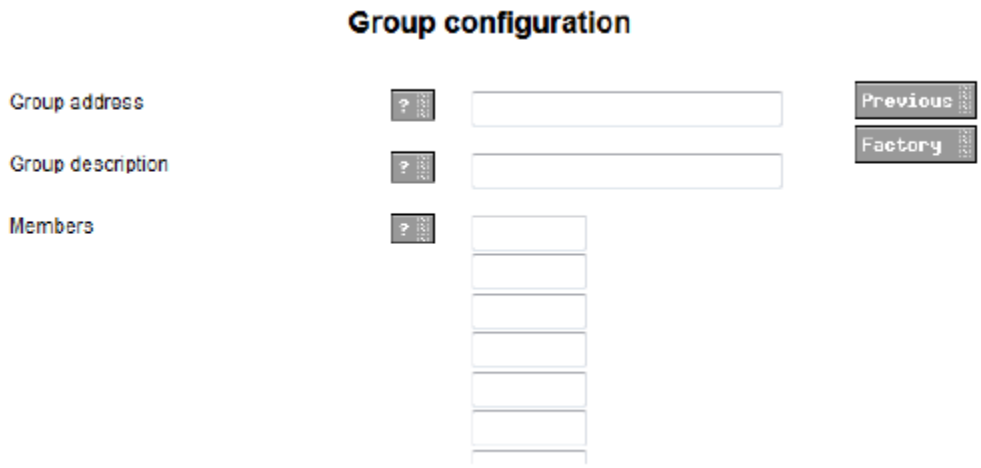
Messaging Groups in the Unite module makes it possible to send one message to several handsets. 30 groups with 15 handsets in each group, and one group with 50 handsets can be created. These groups can also be used to initiate a PT call.

Each group is given an address, either a name or a number, and a description. Then the addresses of the handsets, that should be included in the group, are added.

1. Click *Configuration* on the Start page.
2. Select Messaging Groups > Edit in the menu on the Configuration page.



3. Open the group to be configured by clicking on its name (default EMPTY).



4. Enter the following settings:

Setting	Description
Group Address	ID for the group can be name[1] or a number
Group Description	Description of the group
Members	Add members/handset to the group

1. If it is possible to send messages from a handset in the Cordless Telephone System, the address must be a number.

5. Click **Activate**.

Predefined messages

Note:

This feature can only be reached from *index4*.

The predefined messages include message text, beep characteristics, priority and message type. There are two types of messages: “Common Messages” and “My Messages”.

Note:

The maximum message length differs depending on which system or telephone the message is sent to and the amount of special characters included in the message.

Common Messages

Common Messages can be used by all NetPage users. Up to 30 “Common Messages” can be created. These messages are stored on AIWS and can only be changed by authorized persons.

My Messages

Up to 30 predefined “My Messages” with 120 characters per message can be created. It is also possible to have fewer “My Messages” containing more characters. These messages are stored locally and can only be accessed or changed from that PC.

Creating a predefined message

1. Click the **Common Messages** or **My Messages** button in **NetPage**. For **Common Messages** enter the user name “user” and the password “password”.
2. Click **Add message**.
3. Enter the name of the message and add a message text of maximum 250 characters.
4. Set the message type, beep code and priority.
5. Click **Save**.
6. Click **Close** to exit the administration.

Editing a predefined message

1. Click the **Common Messages** or **My Messages** button in **NetPage**. For **Common Messages** enter the user name “user” and the password “password”.
2. Select the messages that shall be changed and the administration field will open.
3. Make the changes and click **Save**.
4. Click **Close** to exit the administration.

Message history status

Status on the last sent message:

Status	Description
Message accepted	The message is accepted by NetPage and will be transmitted.
Message completed	The Messaging System has completed the transmission of the message.

In the user interface (index4), other **message history statuses** can appear such as:

- Absence
- Call Diversion
- Manual Acknowledge
- Delivery Receipt

Backing up and restoring NetPage files

Ensure that you make a backup of all NetPage files, the phonebook and predefined groups and messages. This is useful, for example, when recovering a customized GUI in case of software or hardware replacements. Even after a software update, the NetPage files need to be restored.

Since AIWS Edition 3 (version 2.7x and later) and AIWS2, the NetPage area is included in the backup file.

NetPage Files

NetPage files are the phonebook, the GUI files including image files and the Common Groups and the Common Messages files.

Backup

Copy and save all NetPage directory files in the NetPage ftp area, see Files for Translation/Editing on page 482.

Restore

1. Put copies of all of the backup NetPage directory files in the NetPage ftp area, see Files for Translation/Editing on page 482.
2. Test that NetPage is functioning properly, see Testing the new user interface on page 493.

Predefined Groups and Messages

Note:

This functionality can only be reached from index4, see figure 162 on page 490.

Backing up

1. Open NetPage. In the Administrate field, select the **My Groups** button. Click on the **Backup/ Restore** button. The **Backup/ Restore** view is opened. Click **Backup** > **Save**. Choose the file name and save.
2. If not already done, repeat the same process as above in point 1) but for **Common Groups**. (Log on with "user" and password "password".)
3. Repeat the same process as above in point 1) but for **My Messages**
4. If not already done, repeat the same process as above in point 1) but for **Common Messages**. (Log on with "user" and password "password".)

Restoring

1. Open NetPage. In the Administrate field select the **My Groups** button. Click on the **Backup/ Restore** button. In the **Backup/ Restore** view click **Browse...** and browse to the once backed-up file. Click **Open** > **Restore**.
2. If not already done, repeat the same process as above in point 1) but for **Common Groups**. (Log on with "user" and password "password".)
3. Repeat the same process as above in point 1) but for **My Messages**
4. If not already done, repeat the same process as above in point 1) but for **Common Messages**. (Log on with "user" and password "password".)
5. Test that NetPage is functioning properly, see Testing the new user interface on page 493.

Open Access Protocol (OAP)

OAP is a protocol that applications can use to communicate with other connected systems, for example the Cordless Telephone System. The client communicates with an OAP Server. The protocol is XML based and is sent to the OAP Server over the LAN using a TCP connection.

This feature requires an additional licence, see Licenses on page 361.

For more information, such as a Function Description, please contact your system administrator.

Configuration

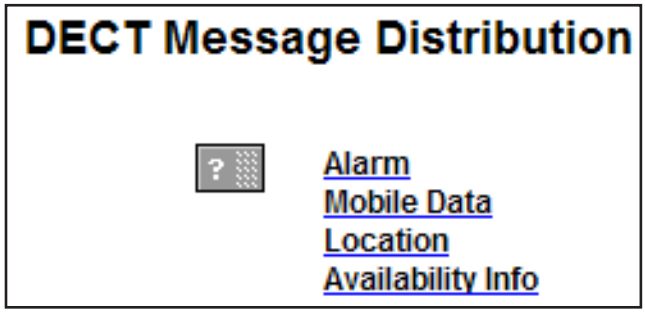
The Message Distribution lists for the different interfaces have to be configured to send the information to the OAP Server, in order to give the client access to the information. The address of the OAP Server is xxx.xxx.xxx.xxx/OAP.

Configuration example

The DECT Interface should be configured to send User Data to the OAP Server.

1. Open the AIWS Configuration pages and select **Other Settings > Advanced Configuration**. Under DECT Interface, select **Message Distribution**.
2. Click on **Alarm**, see figure 166 on page 504.

Figure 166: Setting up the Message Distribution list for the DECT Interface to send information to the OAP Server



3. Enter the address xxx.xxx.xxx.xxx/OAP in one of the address fields. Click on the **Activate** button.

Software administration on the AIWS

For software administration on Elise2 (AIWS hardware) refer Maintenance information for the AIWS on page 550.

Getting Started with the AIWS

These instructions will help you getting started and to access this product. Once logged in, a setup wizard will help you with the basic configuration.

Supply voltage:	12 – 24 VDC ±10%
Current consumption:	max 0.4 A at 12 V max 0.2 A at 24 V

Note: Refer to reverse side for figures and information about connections, cables, switches, etc.

Accessing the Product

The web browser Internet Explorer 6.0™ or later is used for accessing the product's user interface. The product can be assigned an IP address from a DHCP server but the IP address can also be set manually.

Network with a DHCP Server

It is required that this product always gets the same IP address, to prevent it from losing contact with other equipment after a restart. Inform the network administrator about the MAC address and ask him to reserve a fixed IP address via DHCP for this product.

1 Set all sections on switches SW2 and SW3 to OFF, refer to *Figure 4*.

2 Connect this product to the LAN **and** to the power supply as shown in *Figure 1*.

Wait until the function indicator shows the status *License error* (refer to *Figure 2*).

3 Open the web browser and enter the address "elise-xxxxx", where xxxxx is the module key number (starting zeros in the number can be excluded). The module key number can be found on the enclosed licence certificate. The number can also be found on the circuit board, refer to *Figure 3*.

Network without a DHCP Server

1 Set section one (1) on switch SW3 to ON (all other sections to OFF) and all sections on switch SW2 to OFF, refer to *Figure 4*.

2 Connect the Ethernet connector (shown in *Figure 1*) to the PC or LAN with appropriate cable.

- Cross-over cable if connected directly to the PC
- Ordinary cable (straight through pinouts) if connected over the LAN

3 Connect the power supply to this product as shown in *Figure 1*.

4 When the function indicator shows the status *Network Setup mode*, set all sections on switch SW3 to OFF. Refer to *Figure 2* and *3*.

The configuration IP address "192.5.36.229" must be added to the PC's routing table to be able to access this product (requires administrator rights on the PC). Follow the instructions in steps 5 and 6 below.

5 Open a command prompt.

Note: In Windows Vista, you need to run the command prompt as PC administrator to be authorized to change the routing table.

6 Enter the following command: "**route ADD 192.5.36.229 MASK 255.255.255.255 xxx.xxx.xxx.xxx**", where xxx.xxx.xxx.xxx is the PC's IP address.

7 Open the web browser and enter the address "192.5.36.229/config".

Configuration

The setup wizard will start automatically when this product is accessed from the web browser.

1 Enter user name "admin" and the password "changeme".

2 Run the wizard.

(If the IP address has not been assigned by an DHCP server, it must be set manually in the wizard).

Connections

Figure 1 shows the placement of the connectors used for the startup of the product.

J5 Connection of supply voltage.

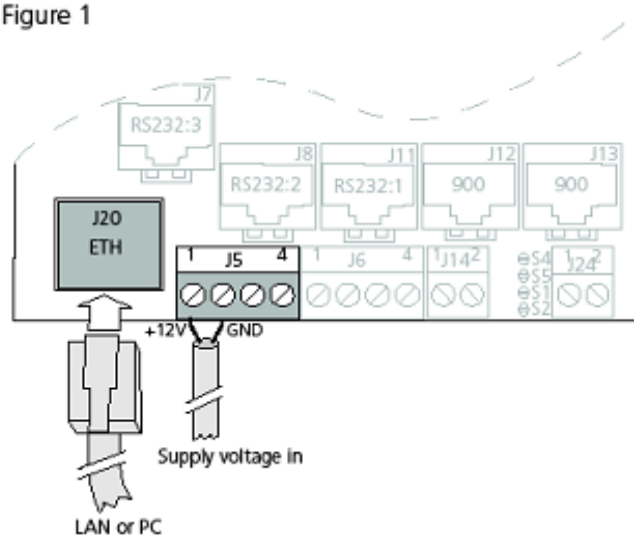
J20 For connection of 10baseT or 100baseT Ethernet TCP/IP network.

Cables

Ethernet cable:

- Use a cross-over cable if connected directly to a PC
- Use an ordinary cable (straight through pinouts) if connected to the LAN

Figure 1

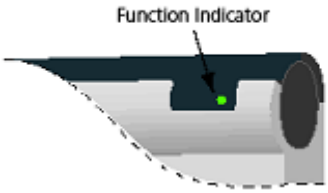


Function indicator

Figure 2 shows the function indicator and different status.

Note: If a DECT Exchange is selected in the wizard as wireless phone system but not yet connected, the *Starting up* status will be indicated until connected.

Figure 2



Colour	*LED Indication*	*Status*
Green		OK. Running
Orange		Network setup mode
Orange		Starting up[1]
Orange		Power up Restart
Red		Licence error
	Each segment = 100 ms	

[1] Starting up mode is indicated during start of applications or if an application has lost connection to a required resource, for example DECT Exchange

Module key number

Figure 3 shows where to find the module key number on IC24.

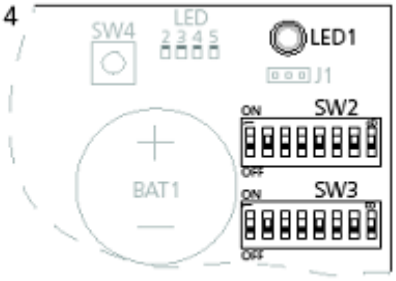
Figure 3



Operation switches SW2 and SW3

Figure 4 shows the placement of SW2 and SW3 and ON/OFF positions.

Figure 4



Software administration on the AIWS2

On AIWS2 there are 2 partitions available to manage and install the module software via web interface on the configuration page.

In addition to the software administration through the configuration page on the AIWS2, you can also administer the software via the module's Boot Mode GUI.
See Installing software in boot mode on page 592. The Boot Mode GUI is typically used if no software is installed on the module or if it is impossible to access the software.

Software information

All information about the installed software is shown in this view. Two software versions can be installed on the module.

1. Click **Configuration** on the start page.
2. Select **Software > Information** in the menu on the **Configuration** page.The software name, versions, the date they were installed and also which version that currently is running are shown.

Toggling with software

If two software versions are installed on the module you can switch between them.

1. Click "**Configuration**" on the start page.
2. Select **Software > Switch** in the menu on the **Configuration** page.
3. Select settings, either "**Copy current setting**" or "**Use factory default settings**".

Current settings means that you copy the configuration from the software you are currently using.

4. Click "**Switch**".

Installing new software

Note:

It is not recommended to use the module's Management port when installing software. Ensure that no Device Manager client is open and it is also important that no ftp client is logged in to the module.The information stored in the database will not be overwritten when new software is installed. Files in the netpage folder in the ftp area that are new or changed are kept when updating.

1. Click "**Configuration**" on the start page.
2. Select **Software > Installation** in the menu on the **Configuration** page.
3. Select software (.pkg) to upload. The software will replace the not running software.
4. Select "**Switch immediately**" if you want to run the new software.
5. Select "**Copy current settings**" if you want the new software to inherit the settings currently used.
6. Click the "**Start Installation**" button.

Creating a software backup

It is recommended to now and then create a backup of the software configuration.

1. Click "**Configuration**" on the start page.
2. Select **Software > Installation** in the menu on the **Configuration** page.
3. Click the "**Backup**" button.

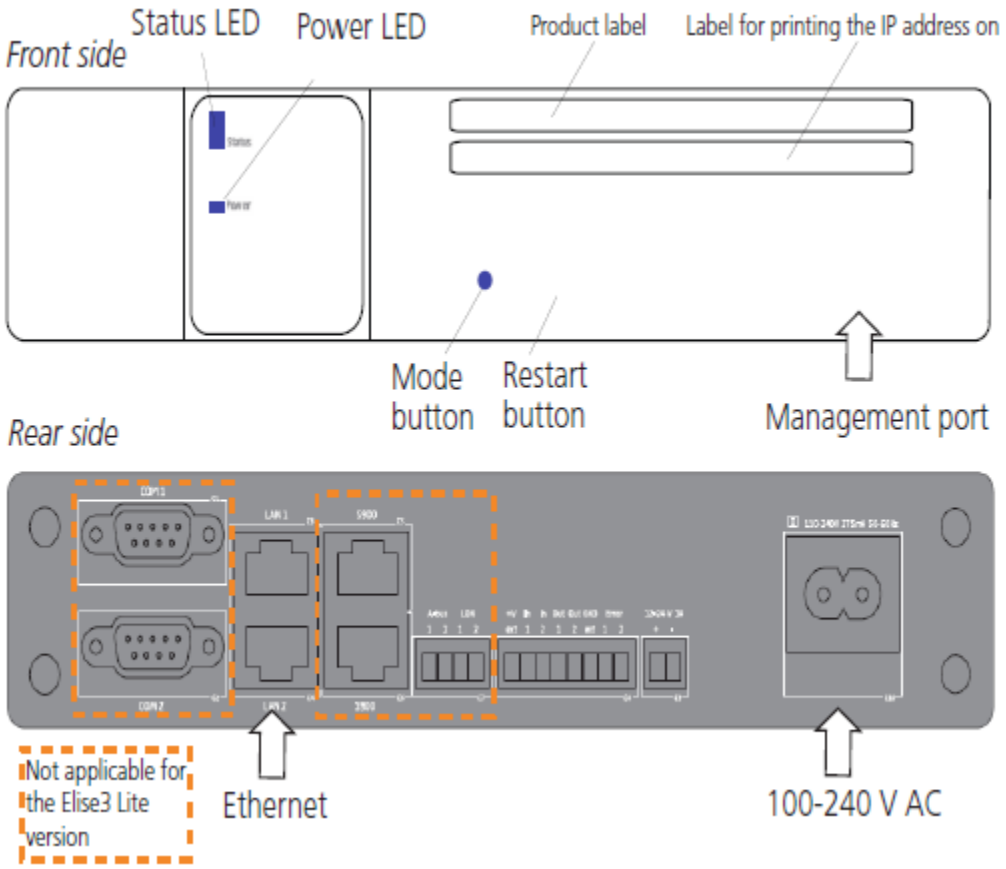
Note that the backup will contain configuration for the running software only.

Upgrading the boot software

For instructions on upgrading the Elise 3 hardware with new Boot software (autoupdate.bin) refer to Performing a field upgrade of the boot software on page 591.Troubleshooting

See Avaya In-Building Wireless Server (AIWS) on page 693.

Getting started with AIWS2



LEDs

		Status LED	Power LED		Mode LED
Status and power OK	Blue				
Starting up/ shutting down	Blue				
Error/fault	Red				
Warning	Red				
Mass storage mode				Blue	

Fixed light indicates normal state
Slow flashing light indicates medium attention
Quick flashing light indicates high attention

Accessing the Product

This product can be accessed either via an IP network or directly via the management port (mini-USB). The web browser Internet Explorer 8.0 or later is recommended for accessing the product's web interface.

Access via a Network with a DHCP Server

It is recommended that this product always gets the same IP address if it communicates with other equipment, in order to prevent it from losing contact with the equipment after a restart. Inform the network administrator about the MAC address (found on a label on the products rear side) and ask to reserve a fixed IP address in the DHCP server.

1. Connect the module to the LAN.
2. Connect the power supply. Starting up is indicated on the status LED with fast flashing blue light.
3. When the starting up indication has stopped, open a web browser on your computer and enter the address elise-XXXXXXXX, where XXXXXXXX is the module key number (starting zeros can be excluded). The module key number can be found on a label on the products rear side, and also in the separately ordered license certificate.

Access via the Management port

Note:

A port driver needs to be installed on your computer the first time it is used for accessing the product via the management port. The port driver is located on the product.

Note:

The installation of the port driver differs depending on the computer's operating system, see either Install the Port Driver on Windows XP/Vista on page 511 or Install the Port Driver on Windows 7 on page 512.

1. Connect the power supply. Starting up is indicated on the status LED with fast flashing blue light.
2. Connect a mini-USB type B cable between the USB port on your computer and the management port on the module.
3. If the required port driver is not installed on the computer, install it now. See port driver installation.

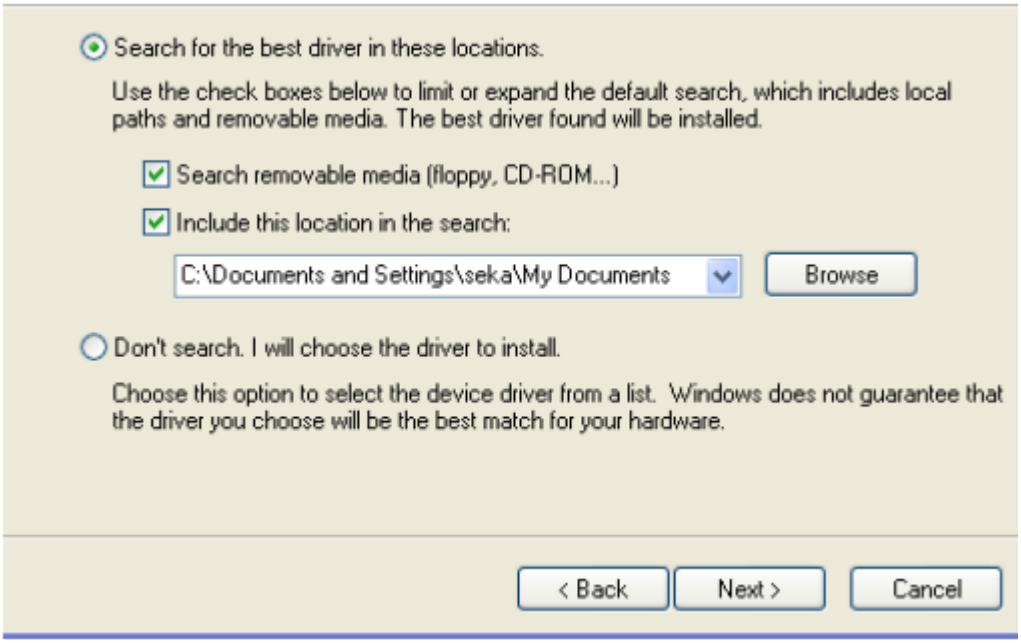
4. When the starting up indication has stopped, open a web browser on your computer and enter the IP address “192.5.36.229” in the address field to access the products web interface.
5. Continue the Configuration on page 513.

Install the Port Driver on Windows XP/Vista

Note:

When switching between mass storage mode and network mode, it takes about 30 seconds before the module can be accessed with the 192.5.36.229 address.

1. Connect a mini-USB type B cable between the USB port on your computer and the management port on the module. The *Found new hardware* wizard opens but at this stage a valid USB port driver is not available, so close the wizard and continue to install the driver.
2. Press the Mode button twice to change the mode to mass storage. The module will now turn up as a mass storage device on your computer. This is indicated by slow flashing blue light on the Mode button LED.
3. Locate the required “elise3.inf” driver and save it on your computer.
4. Press the Mode button twice again to change the USB mode to network access. The *Found new hardware* dialog box opens.
5. Select No, not this time and click “Next”.
6. Select Install from a list or specific location (Advanced) and click “Next”.
7. Select Search for the best driver in these locations.
8. Check the Search removable media (floppy, CD-ROM...) check box.
9. Check the Include this location in the search: check box.
10. Browse to the folder where the port driver is saved.



11. Click “Next”. The installation of the port driver begins.
12. If a message opens, saying the software has not passed Windows Logo testing, click “Continue Anyway”.
13. Click “Finish”. A dialogue box will open and inform you that new hardware is installed.

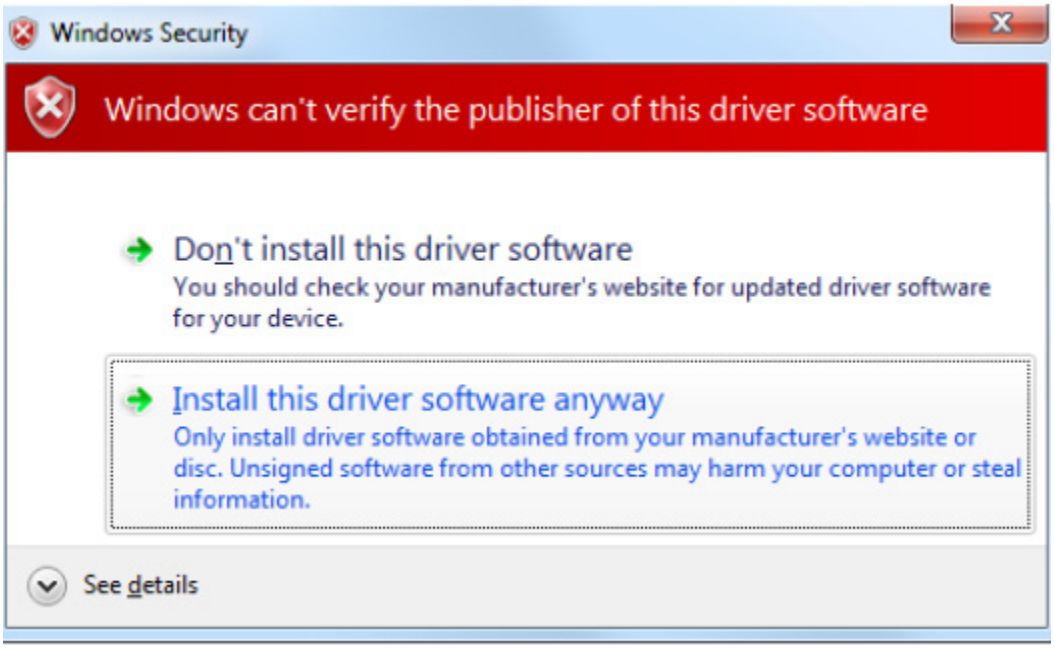
Install the Port Driver on Windows 7

Note:

When switching between mass storage mode and network mode, it takes about 30 seconds before the module can be accessed with the 192.5.36.229 address.

1. Connect a mini-USB type B cable between the USB port on your computer and the management port on the module.
2. Press the Mode button twice to change the USB mode to mass storage. The module will now turn up as a mass storage device on your computer. This is indicated by slow flashing blue light on the Mode button LED.
3. Locate the required “elise3.inf” driver and save it on your computer.
4. Press the Mode button twice again to change the USB mode to network access.
5. Select Control Panel > Hardware and Sound.
6. Select “Device Manager” under Devices and Printers.

7. Right click “RNDIS/Ethernet gadget” and select “Update driver software”. A new window opens.
8. Click “Browse my computer for driver software”.
9. Browse to the folder where the port driver is saved and click “Next”. A Windows Security window opens.



10. Click “Install this driver software anyway”. The installation begins.
11. Click “Close” when the installation has finished. The port driver “Linux USB Ethernet/ RNDIS Gadget” is now installed in Control Panel > Hardware and Sound > Devices and Printers > Device manager > Network adapters.

Configuration

The product needs to be configured with basic settings. Some products settings can be set in an installation Setup Wizard accessible from the web interface. The Setup Wizard will start automatically the first time the module is accessed from the web browser and every time until the configuration has been saved. If the product has not got a Setup Wizard all settings are set from the products configuration pages, see Setup from the Advanced Configuration Page on page 514.

Note:

For extended configuration, refer to the Installation and Operation Manual for this product.

Setup via the Setup Wizard

1. Access the module either via the network or via the management port.
2. Enter user name “admin” and the password “changeme”.
3. Complete the Setup Wizard. (If the module’s network IP address has not been assigned by a DHCP server, it must be set manually in the wizard).
4. Select “Restart now” when the setup wizard has finished. The module will restart with the new configuration.

Setup from the Advanced Configuration Page

1. Access the module either via the network or via the management port, but add “/admin” after the address in the address bar as in “xxx.xxx.xxx.xxx/admin”, where xxx.xxx.xxx.xxx is the modules IP address.
2. Enter user name “admin” and the password “changeme”.
3. Click “System Setup” and navigate to “Network”.
4. Set the network parameters. Use the on-line help if any problems occur.
5. Click “License” and enter the license number.
6. Click “Settings” and select time source.
7. Change the default passwords for all users. If the passwords are not changed, anyone with knowledge of the default passwords can access the module and change any parameter.
8. Reboot the module by navigating to “Reboot”.
9. When the module has been restarted, enter “xxx.xxx.xxx.xxx/admin” in your browser (xxx.xxx.xxx.xxx is the IP address that was given to the module during network setup) to see that it has started up correctly.

Safety and Regulatory Instructions for Elise3

Safety Instructions

For safe and efficient operation of the equipment, observe the guidelines given in this manual and in the Installation Guide, and all necessary safety precautions when using the equipment. Follow the operating instructions and adhere to all warnings and safety precautions located on the product, and in the product manuals.

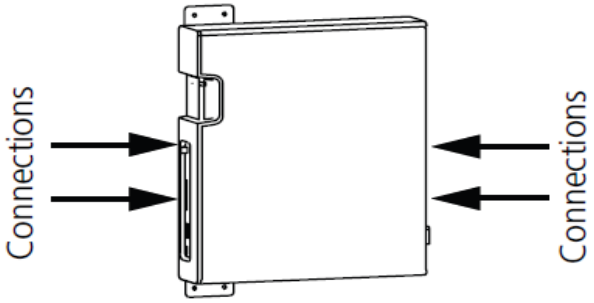
Precautions

- Save this manual. It includes important safety information and operating instructions. Save all instructions for future reference.
- Install all wiring according to local, state, and federal electrical code requirements.
- Connect AC (power supply) only to designated power sources as marked on the product.

WARNING:
DANGER: Never alter the AC cord or plug. If the plug will not fit into the outlet, have a proper outlet installed by a qualified electrician. Improper connection increases the risk of electric shock.

WARNING:
Ensure the AC receptacle is installed near the equipment and easily accessible. Position the electrical cord to the AC power supply where it is least likely to be subjected to damage or stress.

Important:
IMPORTANT: When mounting the device on a wall the device should (to fulfill the fire classification) be mounted so the position of the connectors is in a vertical plane, i.e. on the right and left side, see picture. Use fasteners supplied with the system.



Four screws size 3,5×40 together with four wall plugs, and four screws size M3×6, are delivered with the product. The M3×6 screws are used for attaching the assembly brackets to the module. Use the 3,5×40 screws for walls made of wood. For walls made of concrete and bricks use them together with the wall plugs. For other types of walls use suitable screws and plugs according to wall material.

For detailed mounting instructions refer to Installation Guide Elise3.

Device Manager Keyboard Shortcuts

The following table shows the shortcuts that can be used in the Device Manager.

General

Shortcut	Description
Ctrl + H	Open the File handling dialogue.
Ctrl + Tab	Switch tab
Alt + F4	Close the application

Devices

Shortcut	Description
Ctrl + N	Add a new device
Enter	Upgrade the selected device(s)
Delete	Delete the selected device(s)
Ctrl + F	Find a device
CTtrl + Enter	Open the Properties window for the selected device

Numbers

Shortcut	Description
Ctrl + N	Add a new Number
Enter	Edit the selected Number
Ctrl + C	Copy the selected Number
F2	Rename the selected Number
Ctrl + S	Save the selected Number to the database
Delete	Delete the selected Number from the database
Ctrl + F	Find a Number

Templates

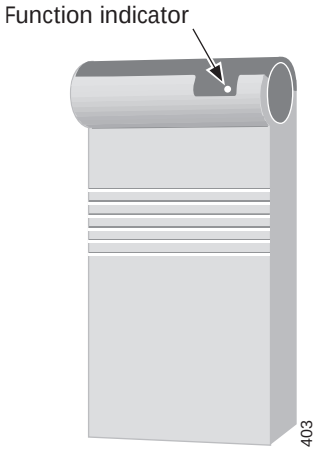
Shortcut	Description
Ctrl + N	Add a new template
Enter	Edit the selected template
Ctrl + C	Copy the selected template

F2	Rename the selected template
Delete	Delete the selected template
Ctrl + F	Find a template

Function Indicator and Error Relay Output

For Elise 2 (AIWS Hardware)

Figure 167: The function indicator that indicates the status of the AIWS



The function indicator and the error relay indicate the status of the AIWS. The indication is dependent of whether the AIWS is connected to the A-bus or not and also whether there is a Central Unit connected to the A-bus. Which mode the AIWS uses is set on the AIWS administration pages. The function indicator and error relay indications are described below.

AIWS connected to A-bus with Central Unit

Status	Function Indicator	Error Relay
Communication with the Cordless Telephone System and the Central Unit.	Green	Operates
Communication with the Cordless Telephone System but not with the Central Unit. or Communication with the Central Unit but not with the Cordless Telephone System.	Flashing orange (100ms ON/100 ms OFF)	Released
Shut down	Flashing red (1000ms ON/3000 ms OFF)	Released
Restart or reboot	Flashing orange (100ms ON/800 ms OFF)	Released

AIWS connected to A-bus without Central Unit or A-bus not connected

Status	Function Indicator	Error Relay
Communication with the Cordless Telephone System. A-bus connection does not change the indication.	Green	Operates
No communication with the Cordless Telephone System.		
Shut down	Flashing red (1000ms ON/3000 ms OFF)	Released
Restart or reboot	Flashing orange (100ms ON/800 ms OFF)	Released

For information about other LED indications, see Installing Elise 2 Server (AIWS Hardware) on page 523.

For Elise 3 (AIWS2 hardware)

For Elise 3 (AIWS2 hardware), refer to chapter Status LED indicators on page 566 of the Installing Elise 3 Server (AIWS2 Hardware) section.

File types

In this appendix, the different file extensions that are used in PDM and AIWS are explained. System files are not described.

File type	Extension	Description
Software file (devices)	bin	Software for devices
Phonebook file	cpb	Company Phonebook file for portable devices. Not used by PDM.
Parameter Definition file	def	Including all possible settings for a certain device type for a certain version.
Software file (AIWS)	eas	Used for package upgrade of AIWS(Elise 2 only). Not used by PDM.
AIWS2 software package	pkg	Software image for AIWS2 (Elise 3 only)
Image file	img	Used for complete (image) upgrade of AIWS(Elise 2 only). Not used by PDM.
Language file	lng	Language file for portable devices.
Package file	pkg	Archive that can include different file types such as parameter definition files (.def), software files (.bin) and template files (.tpl).
Site file	ste	Storage for site specific data. These files may not be edited manually. Used only by PDM.
Template file	tpl	Contains one or more exported templates.
Number file	xcp	Exported Numbers.
Translation file	xml	eXtensible Markup Language. Language file for PDM and AIWS

Installing Elise 2 Server (AIWS Hardware)

Introduction

The Elise 2 Server (AIWS Hardware) (AIW hardware) can be used as a platform for a wide range of applications. It can be used as an interface between systems, for example a TCP/IP network and the System 900.

The license is application dependent and therefore described in the application documentation.

The parameter setup for the Elise 2 Server (AIWS Hardware) is done with a web browser.

Supply voltage:	12 – 24 V/DC ±10%
Current consumption:	max 0.4 A at 12 V max 0.2 A at 24 V
Delivery includes:	Elise 2 Server (AIWS Hardware)
	System Bus Cabling
	Ethernet cable
Tools etc. required:	Screwdriver
	Cutting pliers
	Screws for installation
	Multimeter
	Power supply
	PC with Microsoft Internet Explorer 5.5 or later
	Software "Route to ELISE". (Available from the distributor)

FCC Compliance Statements for Class A Digital Device

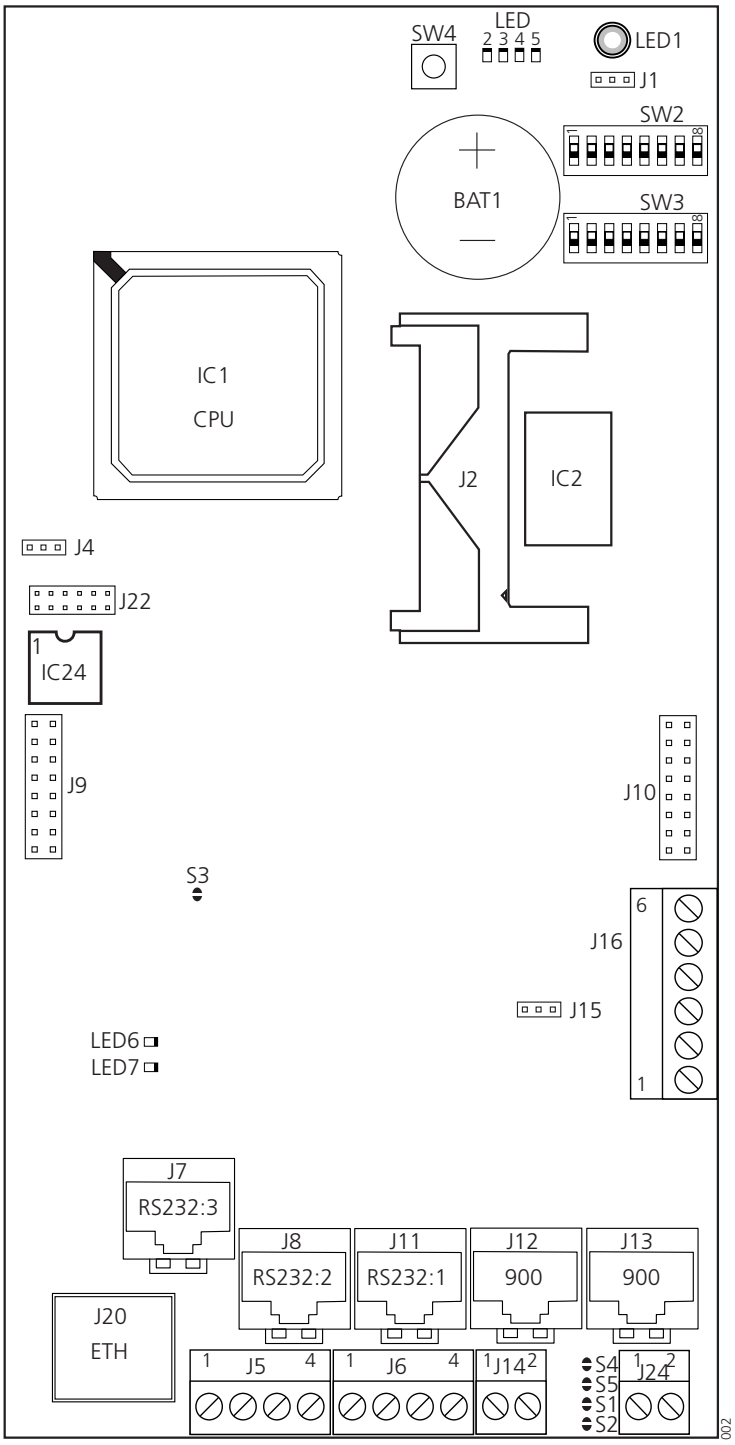
This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

EU Compliance statements for Class A device

This is a limit-class A device. This device can cause radio interference in residential areas, in which case the owner may be required to undertake appropriate countermeasures.

Board description

Figure 168: The Elise 2 Server (AIWS Hardware) circuit board.



Connectors

J2	Connector for the Compact Flash
J5	Connection of supply voltage
J6	For connection of RS422 communication
J7	Modular jack (RJ45) for connection of RS232 communication. RS232:3
J8	Modular jack (RJ45) for connection of RS232 communication. RS232:2
J9, J10	LON/GP Interface Connector
J11	Modular jack (RJ45) for connection of RS232 communication. RS232:1
J12, J13	Modular jacks (RJ45) for connection of System 900 bus cabling
J14	Connector where an error relay output is available.
J16	Connects AUX Input and AUX Output
J20	For connection of 10baseT or 100baseT Ethernet TCP/IP network
J22	For internal use only
J24	For connection of A or B-bus from System 900 when modular system bus cable is not used.

Jumper points and push buttons

J1	Jumper that activates the backup battery. (Jumper pin 2-3 to activate).
J4	For grounding and production test
J15	Jumper that determines if the Error relay output should be active when the relay operates or is released. Normally set to 1-2 to select operating.
S1, S2	Jumper points for selection of A or B-bus
S3	For internal use only
S4, S5	Jumper points used when Elise 2 Server (AIWS Hardware) controls the communication on the A/B-bus.
SW4	Reset button for CPU

Switches

SW2	Module address selector switch for A or B-bus. If the setting of SW2 is changed, the Elise 2 Server (AIWS Hardware) detects this automatically and will reconnect to the System 900 with the new address (it takes approximately 30 s).
SW3	Selector switch for operating mode

Module key and Backup battery

IC1	CPU

IC2	On-board flash memory (used for software reboot)
IC24	Module key
BAT1	Backup battery
LEDs	
LED1	Function indicator with green, orange and red indication
LED2-LED5	Application dependent functionality. See documentation on the application for description.
LED6	Communication on the Ethernet
LED7	Ethernet speed indicator. ON 100 MBit/s, OFF 10 MBit/s

General information

License

All Elise 2 Server (AIWS Hardware) units must have a valid software license.

The license can be found on the administration web page, under the section System Setup > Common > License.

Important:
Changing this field may seriously affect the functionality.

If no valid license is present, the unit will not start and the Function Indicator (see figure 170) will indicate license error with a slow flashing red light. The unit can be started in unlicensed mode, see Unlicensed Mode on page 529 and Selecting operating mode on page 529 for more information. Unlicensed mode is indicated by the Function Indicator with an orange light (3000 ms ON/100 ms OFF), see also Function indicator on page 530.

Powering down and restarting the Elise 2 Server (AIWS Hardware)

Power Down

1. Remove the cover from the Elise 2 Server (AIWS Hardware).
2. Press the push button SW4 to perform a shut down of the processor.
3. Wait until the Function Indicator is flashing orange.

4. Remove the power cable. The power must be removed within 10 minutes or Elise 2 Server (AIWS Hardware) will restart. If Elise 2 Server (AIWS Hardware) restarts, wait until the Function Indicator is not indicating starting up (flashing orange) before pressing SW4 again.

Restart

There are two ways to restart an Elise 2 Server (AIWS Hardware):

- following the power down instruction above, and then apply the power again, or
- initiate a restart from the administration web page.

Operating Modes

There are five different operating modes; normal, network setup, fail-safe, image installation and unlicensed.

Network Setup Mode

To be able to contact the Elise 2 Server (AIWS Hardware), a valid and unique IP address is necessary. In this mode, the IP address is set to 192.5.36.229, which is reserved for installation of Elise 2 Server (AIWS Hardware). Network Setup Mode should only be used when Elise 2 Server (AIWS Hardware) has not got any IP address or when the IP address has to be changed, i.e. if Elise 2 Server (AIWS Hardware) has been moved from one network to another.

Fail-safe Mode

This mode can be used when it is impossible to contact the Elise 2 Server (AIWS Hardware). When started in Fail-safe Mode, no applications are started. It is possible to return to factory settings or a backup copy of parameters from the web page xxx.xxx.xxx.xxx/admin (xxx.xxx.xxx.xxx is the IP address given to the Elise 2 Server (AIWS Hardware)). If there is a problem accessing this page, it is possible to access xxx.xxx.xxx.xxx/system, where it is possible to change network parameters or install new software.

Image Installation Mode

The Compact Flash includes the Elise 2 Server (AIWS Hardware) operating system and application software. If all information (operating system and application software) needs to be updated, then the complete Compact Flash image must to be replaced. The Elise 2 Server (AIWS Hardware) is normally set in image installation mode from the administration pages but it can also be set by the operating mode switch. See Replacing an image on the Compact Flash on page 551 or Installing an image on an empty Compact Flash on page 552.

If the Compact Flash needs to be partly updated with new application software, the image installation mode should *not* be used. For more information, see Updating application software on page 550.

Unlicensed Mode

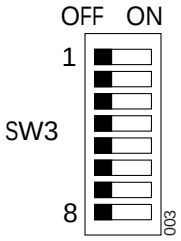
It is possible to run the Elise 2 Server (AIWS Hardware), with full functionality for two hours, without a license. Exact functionality is application dependent. For more information about the functionality during unlicensed mode, see the application documentation.

In unlicensed mode, it is possible to enter a license that does not match the current hardware. This makes it possible to configure a Compact Flash on one hardware and move the Compact Flash to another hardware without changing the license.

Selecting operating mode

All 8 sections of SW3 are set to OFF for normal operating mode.

Figure 169: Switch for selection of operating mode.



Section 1: **Network setup mode**

Section 2: **Fail-safe mode**

Section 3: Not used, must be set to OFF

Section 4: **Image Installation mode**

Section 5: **Unlicensed mode**

Section 6: Not used, must be set to OFF

Section 7: Not used, must be set to OFF

Section 8: Not used, must be set to OFF

Changing Operating Mode

1. Set the section that corresponds to the operating mode to ON.
2. Open the administration web page and press "Reboot" or follow the instructions in Powering down and restarting the Elise 2 Server (AIWS Hardware) on page 527.

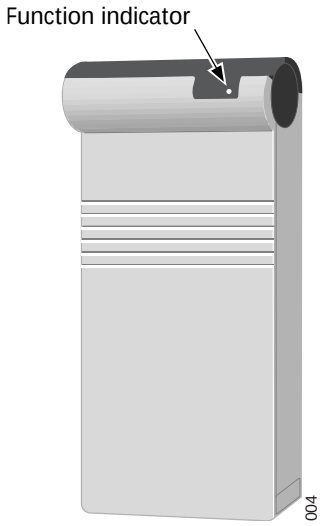
Starting the unit in Normal Mode

1. Set all sections on SW3 to OFF.

2. Open the page System Setup > General on the administration web page and check that the correct license is entered.
3. Press "Reboot".

Function indicator

Figure 170: Status is indicated by the Function Indicator according to the list below.



Colour	LED Indication	Status
Green		OK. Running
Orange		Fail-safe mode[1] Network setup mode[2]
Orange		Image installation mode
Orange		Starting up[3]
Orange		Power up Restart
Orange		Halted (auto. restart after 10 min.)
Orange		Unlicensed mode
Red		Low voltage
Red		Licence error
Red		Watch-dog reset
Red		Shut-down
Red		Memory error (3 s ON / 3 s OFF)
Red		Network error (IP interface initiation error) Module key error (Module key not found)
	Each segment = 100 ms	

005

[1] Fail safe mode is indicated, even if SW3 pin 2 is not set to ON, if the application on Elise 2 Server (AIWS Hardware) is not completely installed or when the application part of the Compact Flash is erased.

[2] When Elise 2 Server (AIWS Hardware) is in Network setup mode, this will always be indicated and override LED indications of other simultaneously activated modes, for example Image installation mode.

[3] Starting up mode is indicated during start of applications or if an application has lost connection to a required resource, for example A-bus or connected IPBS Master or NTP server.

Administration and authentication

Administration on Elise 2 Server (AIWS Hardware) is done from a web browser. In order to access the administration pages a user name and password have to be given.

Important:
The default passwords have to be changed, else anyone with knowledge of a password and the IP address can access the administration web pages and make changes.

Authentication

There are two different users in all Elise 2 Server (AIWS Hardware) products; admin and sysadmin.

The user *admin* has the default password "changeme" and is used for administration and simple troubleshooting of the product. The admin has permission to change all passwords except the sysadmin password.

The user *sysadmin* has the default password "setmeup" and is used for advanced troubleshooting. The user also has access to all administration pages. The sysadmin has permission to change passwords for all users in the product.

In addition, there are two other users in some Elise 2 Server (AIWS Hardware) products. One is called *user* and the default password is "password". This user is product dependent and what it is used for is described in corresponding product documentation. This user does not have access to the administration pages where passwords normally are changed. The user can change its own password on the following page; http://xxx.xxx.xxx.xxx/admin/public/user_chpass.shtml. The password can also be changed by the users admin and sysadmin.

The other user is called *ftpuser* and the default password is "changemetoo". The user is available in products with a FTP area. The user can change its own password on the following page; http://xxx.xxx.xxx.xxx/admin/public/ftpuser_chpass.shtml.

Administration

To access the web pages below, the user *admin* is used.

The web page "xxx.xxx.xxx.xxx/admin" is used in most occasions, for example:

- System setup, for example System 900 configuration

- Troubleshooting information
- Changing passwords

On the following occasions, the web page "xxx.xxx.xxx.xxx/system" must be used.

- Current software installation has to be replaced.
- No software is installed on Elise 2 Server (AIWS Hardware).
- Compact Flash image update or installation

The system page can also be used when configuring network parameters.

Installation

Elise 2 Server (AIWS Hardware) should be placed in a dry environment with a temperature range of 0 to +40°C.

The Elise 2 Server (AIWS Hardware) can be connected via system bus cabling, or via twisted-pairs together with other units in the System 900. The Elise 2 Server (AIWS Hardware)s can communicate with each other via the TCP/IP network.

Important:
The Elise 2 Server (AIWS Hardware) must be mounted in a vertical position to ensure sufficient cooling for the electrical components.

Important:
Always follow the instructions in Powering down and restarting the Elise 2 Server (AIWS Hardware) on page 527 when disconnecting the power to the Elise 2 Server (AIWS Hardware).

Note:
Only install one Elise 2 Server (AIWS Hardware) at a time, otherwise problems might occur during IP addressing.

Installation Procedure

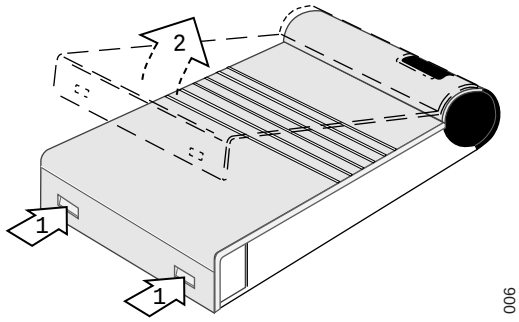
1. Read chapters 4.1 and 4.2 before starting the installation.
2. At delivery Elise 2 Server (AIWS Hardware) is configured for system communication on the A-bus. If modular system bus cabling is used and the B-bus shall be used for system communication, follow the instructions in Selection of A or B-bus on page 534.
3. At delivery, the Elise 2 Server (AIWS Hardware) is configured to be connected to a Central Unit on the A/B-bus. If the Elise 2 Server (AIWS Hardware) should control the communication on the A/B-bus, follow instructions in Elise 2 Server (AIWS Hardware) controlling the communication on the A/B-bus on page 535.

4. Mount Elise 2 Server (AIWS Hardware) on the wall, follow instructions in *Mounting* on page 537 and Mounting together with other units on page 537.
5. Set the system bus address, follow instructions in System 900 addressing on page 538.
6. Connect the system bus, follow instructions in Connection of system bus on page 538 and Connection of supply voltage on page 540.
7. Optionally connect outputs and inputs described in Additional connections on page 540.
8. Activate the battery, follow instructions in Activation of battery on page 543.
9. Perform a network parameter setup of Elise 2 Server (AIWS Hardware), follow instructions in Setup of network parameters on page 545.
10. Connect Ethernet connector to the Local Area Network, follow instructions in Connection of ethernet on page 544.
11. Perform a test of the installation, follow the instructions in Installation test procedure on page 546.
12. Continue with additional parameter setup for the unit according to chapter - and respective software application documentation.
13. Make a backup copy of all parameters.

Opening the housing

Use a screwdriver or similar to release the cover by applying a light pressure to the two snap catches (1) and remove the cover (2).

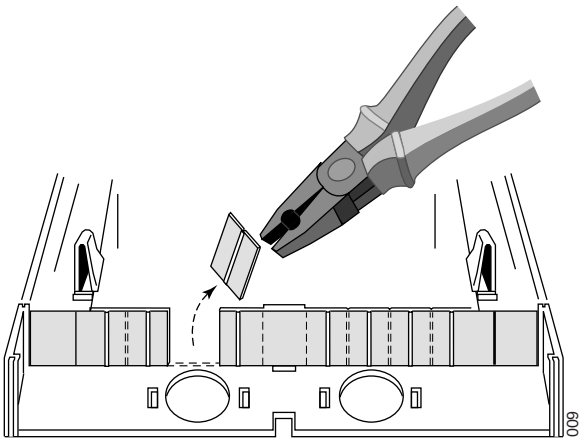
Figure 171: Opening the Elise 2 Server (AIWS Hardware) housing.



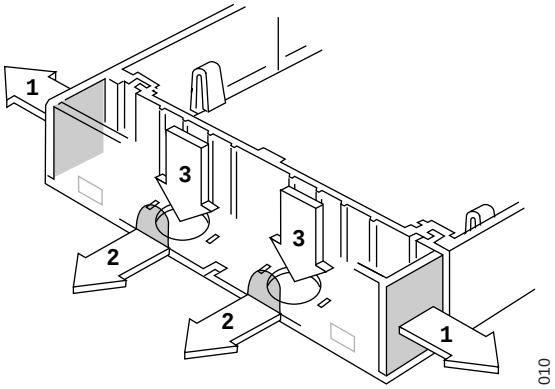
Wiring runs

The plastic partition is scored to facilitate breaking at convenient intervals.

1. Use pliers to break off a suitable section.



- Run the wiring out through the partition. Wiring can be run three ways from the Elise 2 Server (AIWS Hardware):Remove the rectangular covers and run the cabling out



through the side (1).

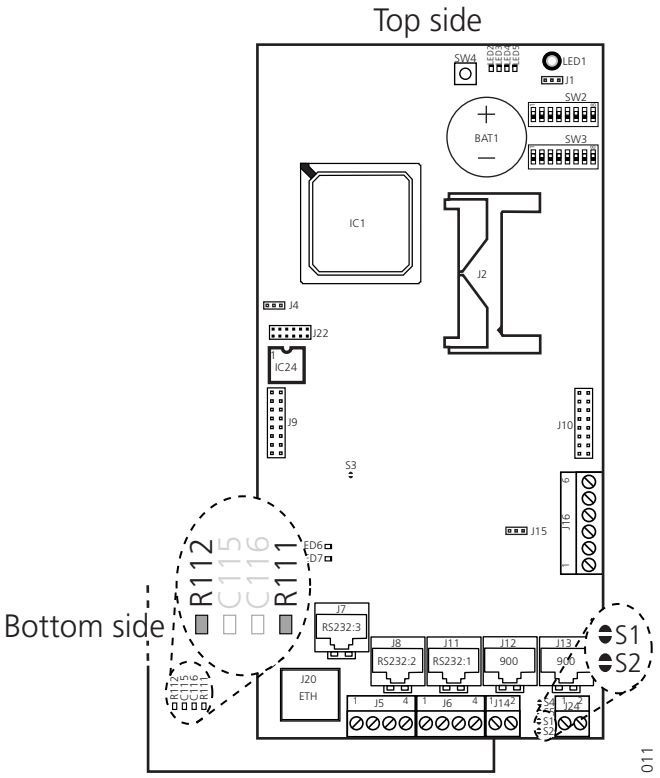
- Break off sections at short side of case and run the cabling downwards (2).
- Run the cabling through the round holes at the bottom of the case (3).

2. Secure the wiring with cable straps.

Selection of A or B-bus

When modular bus cabling is used for connection of the System 900 bus the A-bus is used default. To use the B-bus, remove the 0 ohm resistors R111 and R112 from the circuit board and solder jumper points S1 and S2 (R111 and R112 are situated on the bottom side of the circuit board). See figure 172 on page 535.

Figure 172: Jumper points for adjusting the Elise 2 Server (AIWS Hardware) unit to use the System 900 B-bus instead of the A-bus.



Elise 2 Server (AIWS Hardware) controlling the communication on the A/B-bus

Depending on the software application on the Elise 2 Server (AIWS Hardware), it can be used to control the communication on the A-bus, i.e. the Central Unit is not used for communication control. This can be useful when System 900 is not used for messaging but only to communicate with, for example, an Alarm Module or Output Module.

The same information that can be received when the Elise 2 Server (AIWS Hardware) is connected to an A-bus with Central Unit, can also be received when it is controlling the communication. Examples of information is input activity and pagings from the Alarm Modules (see respective software application documentation for more information about the possibilities). Alarms and Mobile data from cordless telephones can be transferred from the Elise 2 Server (AIWS Hardware) to modules connected to the A-bus. The Elise 2 Server (AIWS Hardware) does not have any other of the Central Unit functionality, for example the possibility to address Pocket Units over the A-bus or handle absence information received from Charging Racks.

System Installation

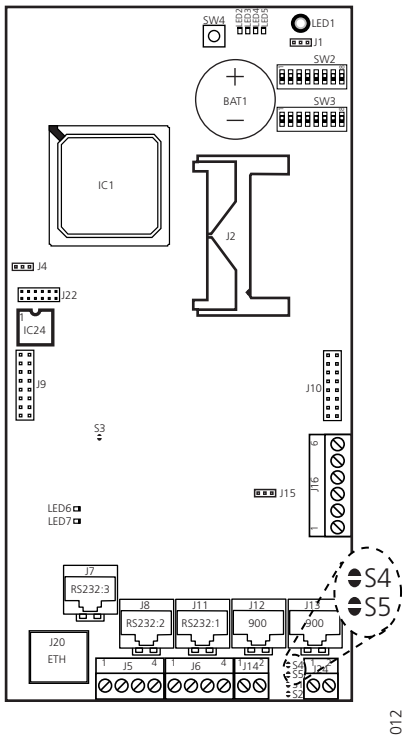
When the Elise 2 Server (AIWS Hardware) controls the communication on the A-bus, a maximum of 15 modules can be connected to the A-bus. The Elise 2 Server (AIWS Hardware) should have the address 00 and other modules that are connected to the A-bus must have addresses in the range 01-0F.

See also Message distribution on page 548 and documentation for the System 900.

Required Hardware Modifications

When Elise 2 Server (AIWS Hardware) shall control the communication on the A/B-bus, jumper points S4 and S5 has to be soldered, see figure 173 below.

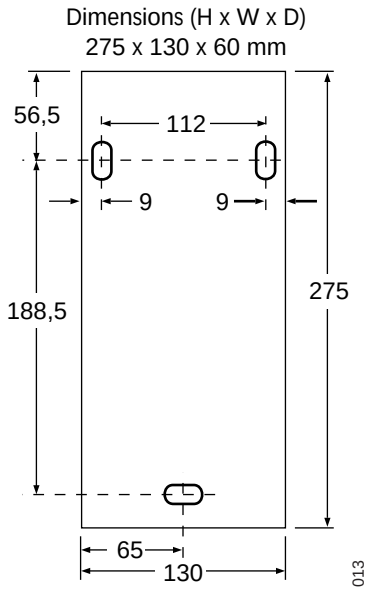
Figure 173: Jumper points for configuring the Elise 2 Server (AIWS Hardware) unit to be a communication controller on A/B-bus.



Mounting

Note:

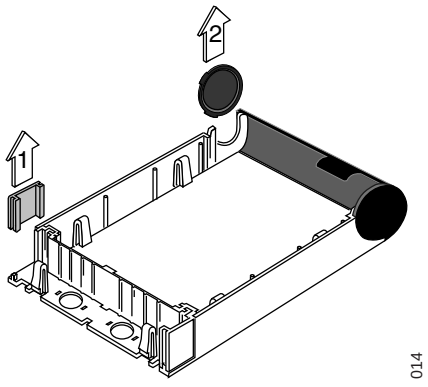
Dimensions for installation of the Elise 2 Server (AIWS Hardware).To facilitate



service after the unit is installed, we recommend a free space of about 150 mm above and 50 mm below the unit.

Mounting together with other units

1. Remove the rectangular (1) and circular (2) covers.

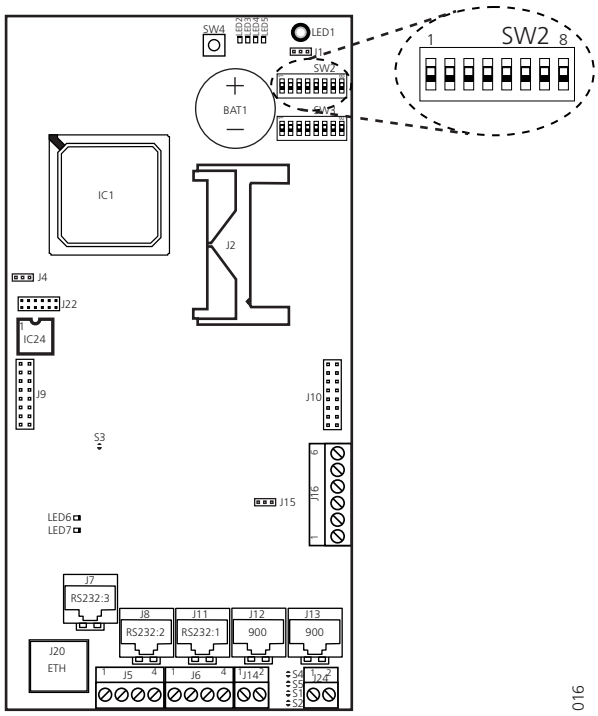


2. The rectangular covers are used to fasten units to each other (3 and 4)Fasten the unit with three screws, see the illustration in Mounting on page 537.

System 900 addressing

The System 900 address consists of two hexadecimal digits that are selected by the eight sections of the address switch, SW2. Sections 5-8 of the switch select the first (most significant) digit and section 1-4 select the second (least significant) digit. The address must not be the same as any other System 900 unit address (see document *System Installation, On-site Paging System, TD 90227GB* for more information*).*

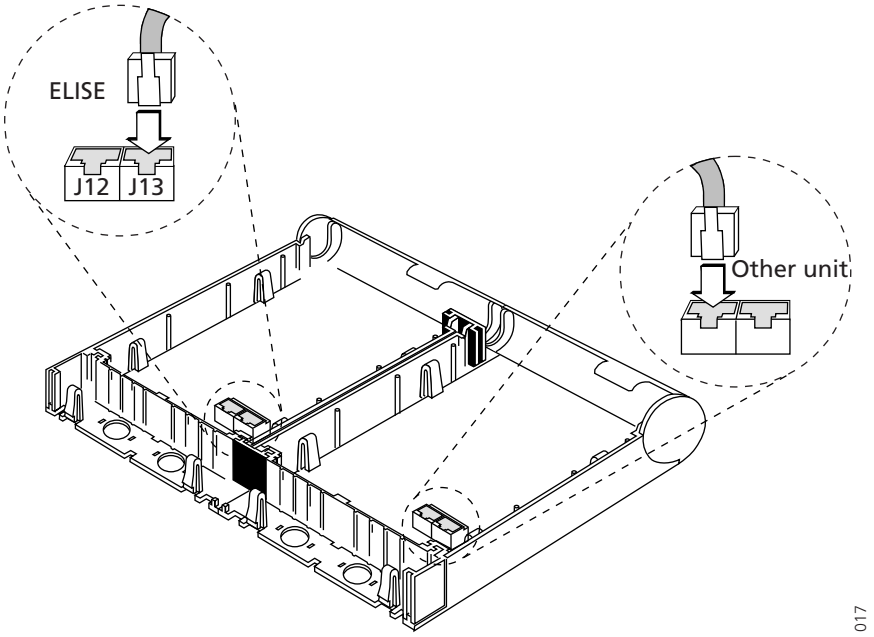
Figure 174: The Elise 2 Server (AIWS Hardware) addressing switch.



Connection of system bus

The Elise 2 Server (AIWS Hardware) can be installed together with other System 900 units, either via modular system bus cabling or via twisted-pair lines.

1. **Bus Connection to Modular Jacks**The illustration above shows an Elise 2 Server



(AIWS Hardware) placed to the left of another System 900 unit. Connect the bus cable as shown, from connector J12/J13 on the Elise 2 Server (AIWS Hardware) to the bus connector on the other unit.

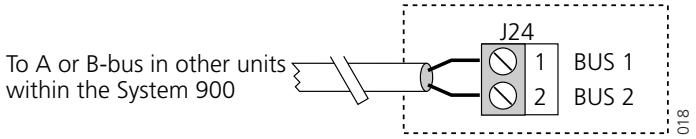
Note:

Make sure connectors are correctly inserted!

Bus Connection to Screw Terminals

If system bus cable is not used, connections are made with twisted pairs to screw connector J24.

Figure 175: Connection of System 900 bus.



Other System 900 units are connected to A or B-bus, pin 1 and 2 at screw connector J24.

Note:

Observe polarity. Use only twisted pairs for two-wire connections.

Connection of supply voltage

A separate power supply is connected to screw connector J5, pin1 and 2. The current through J5 must not exceed 3A.

Note:

External power supply must incorporate an insulating transformer. Output current must be inherently limited to max. 8 A.

Note:

The external power supply must comply with EN IEC 60950-1 requirements.

Note:

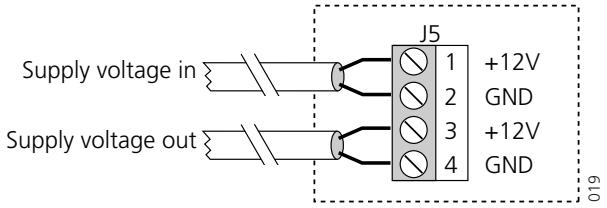
For US and Canada: The Elise 2 Server (AIWS Hardware) shall only be connected with the following power supply: AWS 1166, SA60, Sino American Electronic Co. Ltd. Switching Adapter.

1. Connect the power supply cable to J5:1-2.

Note:

+12 V wire is marked with white stripes
GND wire has a text printing of the cable characteristics

Figure 176: Connection of supply voltage



Additional connections

Error Relay Output

Figure 177: A relay output on connector J14 is used to indicate Elise 2 Server (AIWS Hardware) malfunction and can also be used to indicate other errors. **Jumpering that decides when the error relay output is active, either when the relay operates or is released.**

The jumpering J15 decides if the output shall be active when the relay is operating or released. 1-2 selects operating and 2-3 selects released. In figure 177, the relay is released and as the jumpering is set to 1-2 the circuit is open and the error relay output is inactive.

At power-up or restart of the Elise 2 Server (AIWS Hardware), the relay is released until the applications are working properly. If the relay is released longer, Elise 2 Server (AIWS Hardware) is malfunctioning.

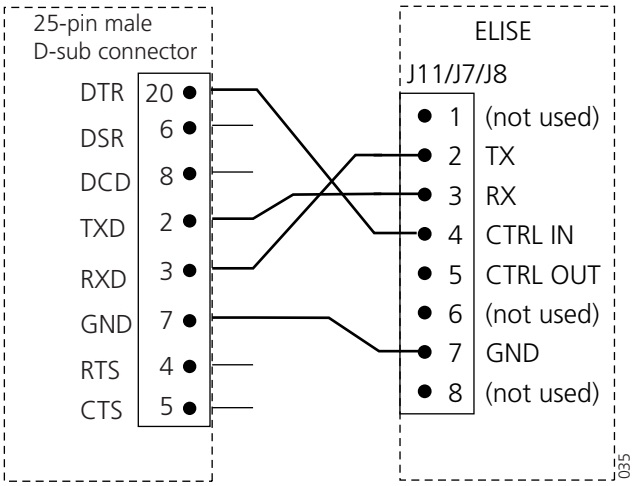
RS232 Communication with external unit

Figure 178: The Elise 2 Server (AIWS Hardware) has three identical RS232 connectors; J7, J8 and J11. Depending on software application the RS232 ports can be used or not. How to connect external equipment to the Elise 2 Server (AIWS Hardware) is described in the documentation of the software application. In figure 178, the RS232 connectors on the Elise 2 Server (AIWS Hardware) is described.**Description of the Elise 2 Server (AIWS Hardware) RS232 ports.**

Connections for Serial Line Printer

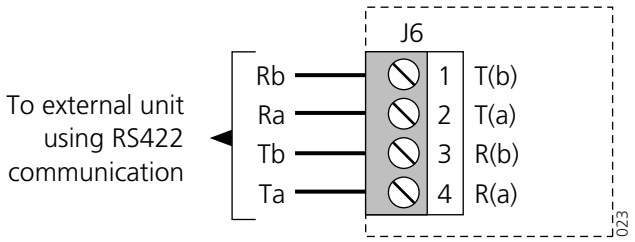
To connect the serial line printer, see figure 179 for the pin-layout and wiring run.

Figure 179: Connections for serial line printing.



RS422 Communication with external unit

Figure 180: Depending on software application the RS422 port is used or not. If it is used, the connector J6 is connected to the external unit as shown in the figure below.**Connection of external unit via the RS422 port.**



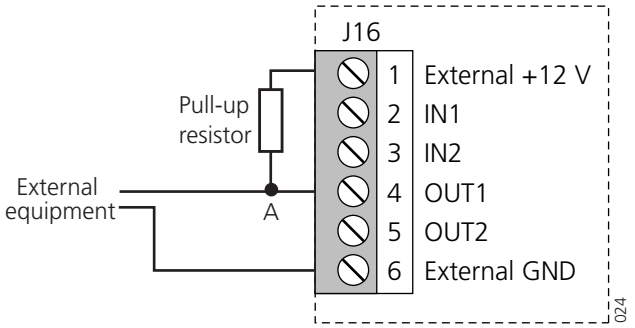
Connection of AUX inputs and AUX outputs

The application of the inputs and outputs are software dependent.

Two digital inputs and two digital outputs can be connected via J16. The outputs are of open-collector type and the output signals are dimensioned for 100 mA at max 12 V.
A pull-up resistor should be connected to the output as shown in figure 181.

Galvanic isolation of the inputs and outputs is provided by using a separate power supply. When galvanic isolation is not needed, supply voltage can be taken from the Elise 2 Server (AIWS Hardware) circuit board by connecting J16-1 to J5-3 and J16-6 to J5-4.

Figure 181: Connection of inputs and outputs.

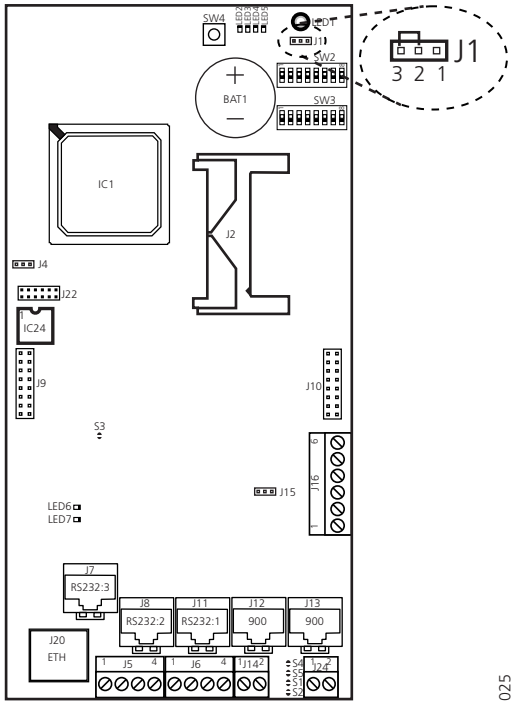


The inputs IN1 and IN2 are active when they are connected to 12 V. When the output OUT1 is active, the potential in point A in figure 181 will be close to 0 V. The same applies for a similar connection for OUT2.

Activation of battery

Activate the real-time clock backup battery by closing jumper J1 on the circuit board. (Jumper pin 2-3 to activate).

Figure 182: Battery placement.



The backup battery is a 3V lithium battery. At any interruption in the ordinary power supply, the real-time clock will be supplied by the battery.

Battery Data

Current consumption, real-time clock:

	Typical	Maximum
3V battery	3 µA	40 µA

Battery life (battery connected):

	Typical	Minimum
Power not connected	6 years	0.5 years
Power connected		10 years

Battery life (battery not connected):

Minimum 10 years.

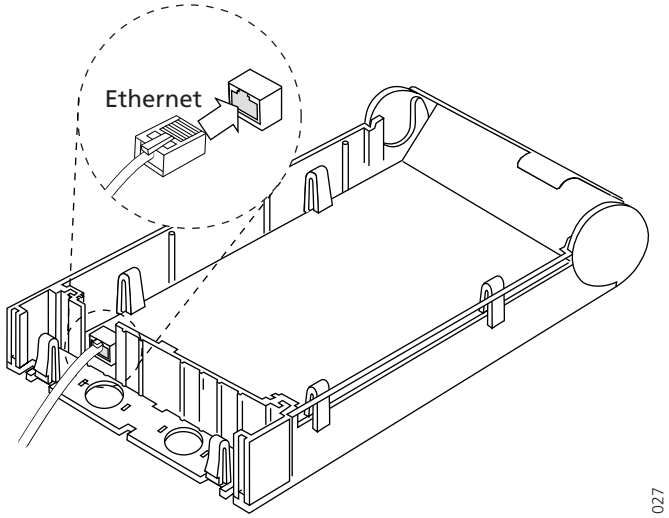
Connection of ethernet

If Elise 2 Server (AIWS Hardware) is connected directly to a PC, a crossover cable has to be used. If Elise 2 Server (AIWS Hardware) is connected to a HUB, an ordinary (straight through pinouts) cable has to be used. The cable supplied is an ordinary cable.

Connect the Ethernet cable to connector J20, see figure 183 below.

It is recommended to break off a suitable section before inserting the Ethernet cable, see Wiring runs on page 533.

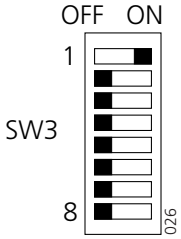
Figure 183: Connection of Ethernet cable



Setup of network parameters

1. Set section one in SW3 to ON to set Elise 2 Server (AIWS Hardware) in "Network setup mode". The remaining sections should be set to OFF.

Figure 184: Setting the Elise 2 Server (AIWS Hardware) in Network setup mode.



2. Connect Elise 2 Server (AIWS Hardware) Ethernet connector J20 either
   - with crossover cable directly to a PC or
   - with ordinary (straight through pinouts) cable via a HUB on the LAN to the PC. Observe that it has to be the same LAN, i.e. same Ethernet Broadcast Domain.
3. Connect the power cable and wait until the Function Indicator indicates with steadily orange light. Elise 2 Server (AIWS Hardware) now has the network setup IP address 192.5.36.229.

   If the function indicator is red, check that supply voltage is 12.5 Vdc ±10%.

4. To be able to access Elise 2 Server (AIWS Hardware) from a PC, the PC has to belong to the same network as Elise 2 Server (AIWS Hardware) or Elise 2 Server (AIWS Hardware)’s IP address has to be found in the PC’s route table. To facilitate this, the program "Route to ELISE" is provided.

   Start the program "Route to ELISE". Press "Attach" to add the Elise 2 Server (AIWS Hardware) network setup IP address to the route table.
5. Press "Launch config". This will open the page "192.5.36.229/system" in your browser. The user ID is "admin" and the default password is "changeme".
6. Press "System Setup" and navigate to "Network". Set the network parameters. Use the on-line help if any problems occur.
7. Navigate to "System 900" and select the bus operating mode for the module. The modes are described in the on-line help.
8. Change the default passwords for **all** users. If the passwords are not changed, anyone with knowledge of the default passwords can access your Elise 2 Server (AIWS Hardware) and change any parameter.
9. Set all sections in SW3 to OFF. Reboot Elise 2 Server (AIWS Hardware) by navigating to "Reboot".
10. Return to the program "Route to ELISE" and press "Detach" to remove the Elise 2 Server (AIWS Hardware) network setup IP address from the route table. Close the program.
11. When Elise 2 Server (AIWS Hardware) has been restarted, enter the URL xxx.xxx.xxx.xxx/admin in your browser (xxx.xxx.xxx.xxx is the IP address that was given to Elise 2 Server (AIWS Hardware) during network setup) and see that it has started up correctly.
12. If an entry is added in the DNS, it will be easier to connect to Elise 2 Server (AIWS Hardware).

Installation test procedure

1. If the Elise 2 Server (AIWS Hardware) is connected to a Central Unit, the indicator will light steadily green within 90 seconds.

   If the indicator continues to flash orange, check:

   - Connections on Elise 2 Server (AIWS Hardware)
   - Elise 2 Server (AIWS Hardware) has a correct System 900 address
   - Check in the AIWS advanced configuration > system information of all applications are running.
     Check if the following are connected: Time synchronizer, DECT interface, SMS center.
     Check at the DECT DH (Device handler) whether the Nr. of DM (Device Managers) is more than 0.

Note:

Check also the application documentation for trouble-shooting information.

If the indicator starts to blink red, check:

- IP address
- Network connections
- License
- Module key

If everything seems to be OK but the function indicator still flashes, the fault is probably located outside the Elise 2 Server (AIWS Hardware):

Check the other System 900 units according to document *System Installation, On-site Paging System, TD 90227GB,* or contact your dealer.

2. Open the administrator page in a browser and navigate to "Troubleshoot". Use the information log and tools given to test that Elise 2 Server (AIWS Hardware) is functioning properly.
3. Replace the cover.
4. When all other units are installed, perform the system test described in *System Installation, On-site Paging System, TD 90227GB*.

Clock synchronisation and time settings

The clock in different Elise 2 Server (AIWS Hardware)s can be set from the web browser, A-bus (i.e. Central Unit in System 900) or a time server. To be able to synchronize the clocks in different Elise 2 Server (AIWS Hardware)s a time server has to be used. Depending on software application and license, an Elise 2 Server (AIWS Hardware) can be used as time server. An external time server supporting the Network Time Protocol (NTP) can also be used. Normally the Elise 2 Server (AIWS Hardware) that is used as time server synchronizes with an external time server, and then all other Elise 2 Server (AIWS Hardware) use that Elise 2 Server (AIWS Hardware) as the time server.

To select time source do as follows:

1. Open the administration pages of the Elise 2 Server (AIWS Hardware) by entering "xxx.xxx.xxx.xxx/admin" in the address field in the web browser.
2. Click on "Settings" in the left menu.
3. Select time source; Web browser, A-bus or Time server.

Note:

Not all system’s Central Unit can provide the time.

Independent of time source the Elise 2 Server (AIWS Hardware) can handle different time zones and adjust the clock according to daylight saving time.

The date and time format controls the appearance of date and time in log views and application specific pages. The administration pages that are common to all Elise 2 Server (AIWS Hardware) will display date and time in the following format: YYYY-MM-DD, HH:MM:SS (for example 2000-01-31 13:30:00). This format for date and time will also be used in exported log files.

An Elise 2 Server (AIWS Hardware) can also set the time in connected systems, for example System 900. In this case, the Elise 2 Server (AIWS Hardware) will send its time to the connected system once every 24-hour period and when the time is updated.

To set the time in System 900 from the Elise 2 Server (AIWS Hardware) do as follows:

4. On the time settings page, enter when the Elise 2 Server (AIWS Hardware) should send its time to System 900 in the "Time push time" field.
5. Click "Setup System 900 time".
6. Select "Yes" in the "Set time in System 900".

Setting time in other carrier systems is done similarly. If several carrier systems are available, the time will be sent at the same time to all systems.

Time Synchronization

It can take a few seconds to synchronize the date and time during start up. It also takes a few seconds if the server parameters changes to another server.

When the time is changed in the time server it takes different long time to synchronize the time, depending on how the modules are set up and how they are connected together. If a module does not have a time server license, it takes about 15 minutes to update its clock. A module with a time server license takes about 30 minutes to update.

Message distribution

In the administration pages, there are distribution lists that are used to distribute incoming information to other modules. If a module is to be connected to several carrier systems, for example both System 900 and a Cordless Telephone System, distribution of incoming data from the different systems has to be configured independently. The distribution of "Status Logs" and "Activity Logs" are configured separately. Advanced activity settings for activity logs are described in the *Function Description, Activity Logging in Unite, TD 92341GB.*

The addressing is described in the examples below:

Addressing a module on the System 900 A-bus

When a specific module on the A-bus is addressed, the data will be transferred directly to that module. It is however not necessary to address a specific module on the A-bus as the Central Unit in the System 900 can distribute the data to a module. Note that this requires configuration of the Central Unit.

- *No module addressing*

  127.0.0.1/S900

  The data is sent to the System 900 interface in the Elise 2 Server (AIWS Hardware), which sends the data on the A-bus without the module address defined. The Central Unit in the system has to be configured to distribute the data to a module. It is also possible to address the System 900 interface on another module by entering its IP address instead of 127.0.0.1 (localhost).

- *Module addressing*

  127.0.0.1/S900?03

The data is sent to the System 900 interface (127.0.0.1/S900) in the Elise 2 Server (AIWS Hardware) and is then sent to the module with address 03 in the system. It is also possible to address the System 900 interface on another module by entering its IP address instead of 127.0.0.1 (localhost).

Addressing another Unite compliant module on the LAN

The addressing includes the IP address that the data should be distributed to and also which service on that address that should take care of it. How a unit is addressed is described in each units documentation.

- *Addressing of another Unite compliant module*

  xxx.xxx.xxx.xxx/Service

  First the IP address of the module is defined. After the “/”, the application service that should take care of the data is specified.

The following example describes how to distribute data from an Elise 2 Server (AIWS Hardware) software application to an Alarm Management Server.

- *Addressing of an Alarm Management Server*

  xxx.xxx.xxx.xxx/EventHandler

  First the Alarm Management Server IP address is defined. After the “/”, the application service EventHandler is specified.

  Note:

  For AMS version 3.00 and 3.10 the service cannot be used. Instead the correct port on the AMS, port number 10010, has to be used for addressing, i.e. xxx.xxx.xxx.xxx/:10010.

Unite Name Server (UNS)

The UNS is used to resolve addresses into complete Unite destinations. The Elise 2 Server (AIWS Hardware) can be configured to send all requests to the local UNS (stand-alone mode) or to forward all requests to a centralised UNS (forwarding mode). In forwarding mode, the local UNS will only be used if the centralised UNS cannot resolve the address.

Maintenance information for the AIWS

Replacement of the Compact Flash

Note:
Only Compact Flashes can be used.

1. Remove the cover, see Opening the housing on page 533.
2. Perform a power down of the unit, see Powering down and restarting the Elise 2 Server (AIWS Hardware) on page 527.
3. Remove the circuit board, see Circuit board replacement on page 553.
4. Replace the Compact Flash.
5. Put the circuit board back into the cabinet.
6. If the Compact Flash is not preprogrammed with a valid IP address follow the instructions in Setup of network parameters on page 545 else connect the power cable.
7. Replace the cover.

Updating application software

The application software on the Compact Flash can be updated, for example if new functionality for the application has been released. The version of the application software has to be compatible with the Elise 2 Server (AIWS Hardware) operating system version. See *Replacing an image on the Compact Flash* below for information about how to upgrade the operating system.

The AIWS device manager needs to be closed before the software update can be started. Otherwise, the software upgrade will not start until the AIWS device manager will be closed. There is no additional indication or warning text that the AIWS Device manager is still open.

Important:
When updating the application software, the customized configuration of the NetPage will be overridden and needs to be restored afterwards. Therefore it's recommended to take a backup of all NetPage files as well. Refer to Backing up and restoring NetPage files on page 502.

1. Open the page xxx.xxx.xxx.xxx/system.
2. Press "Software". The current software versions for the application and Elise 2 Server (AIWS Hardware) are shown.
3. Navigate to "Install software" and follow instructions.

Note:
The .eas files must be used to update the application software.

It is possible to update the software over a remote connection. However, note that it is not possible to update software on the Elise 2 Server (AIWS Hardware) that handles the remote connection.

Replacing an image on the Compact Flash

The complete Compact Flash image has to be replaced if the Elise 2 Server (AIWS Hardware) operating system has been updated.

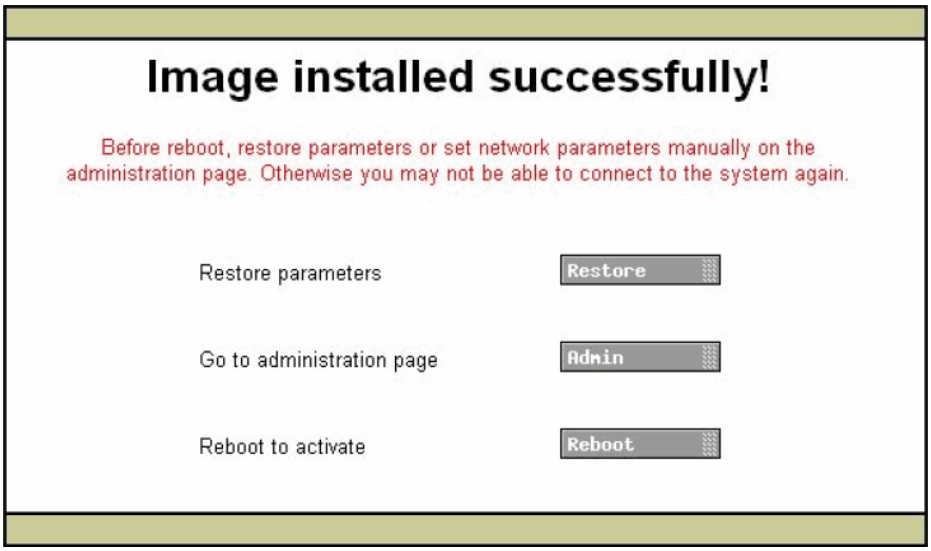
Important:
When a new image is installed, all information on the Compact Flash will be replaced (this includes **all** IP settings). It is strongly recommended to take a backup of the parameters before the image is installed in order to be able to recover the unit to original setup. Refer to Backing up and restoring NetPage files on page 502.

1. Open the page xxx.xxx.xxx.xxx/system.
2. Press "Software". Navigate to "Install Image". Follow the instructions on the page.
3. Select parameter backup and take a backup of the current configuration incl. network setup and license key.
4. Select start installation. The AIWS will reboot in image installation mode. If the automatic redirect fails after the reboot press the back button in your browser. If this fails either open the page http://xxx.xxx.xxx.xxx/install manually. Refer to Avaya In-Building Wireless Server (AIWS) on page 693 to get further information.
5. Select the image file and press writ e to flash to start the installation. It will take some time to install the new image. The time is dependent of the size of the image and the type of connection to the Elise 2 Server (AIWS Hardware).

Note:

The .img file must be used to update the complete image on the Compact Flash.

6. Restore the old AIWS configuration from the backup that was taken before. Without restoring all parameters especially the network setup and license key will get lost after reboot.



7. Press reboot to start the AIWS with the new software image

It is possible to replace the image over a remote connection. However, note that it is not possible to replace the image on the Elise 2 Server (AIWS Hardware) that handles the remote connection.

Installing an image on an empty Compact Flash

An image can also be installed on an empty Compact Flash.

1. Set section one and four in SW3 to ON, to set the Elise 2 Server (AIWS Hardware) in "Network setup mode" and "Image installation mode".
2. Perform a power down of the unit and then restart it, see Powering down and restarting the Elise 2 Server (AIWS Hardware) on page 527.
3. Use the program "Route to ELISE" to connect to the Elise 2 Server (AIWS Hardware). A web page where a new image can be installed will open.
4. Select the image to install. Note that it will take some time to install the new image. The time is dependent of the size of the image and the type of connection to the Elise 2 Server (AIWS Hardware).

Note:

The .img file must be used to update the complete image on the Compact Flash.

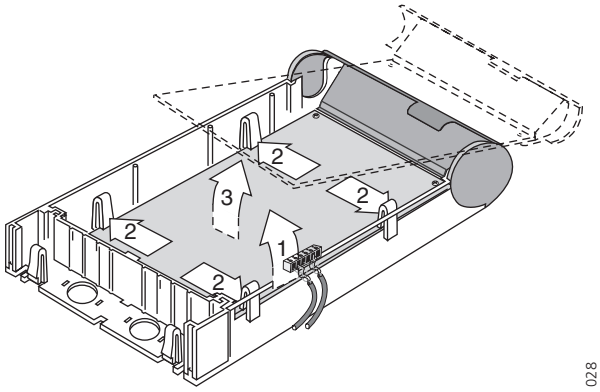
5. Set section four in SW3 to OFF and press "Reboot" on the displayed web page, to leave "Image installation mode".
6. Setup the parameters according to instructions in Setup of network parameters on page 545 or recover parameters from a backup file.

Updating the software license

1. Open the page xxx.xxx.xxx.xxx/admin and press "General".
2. Enter the new license, and press "Activate".

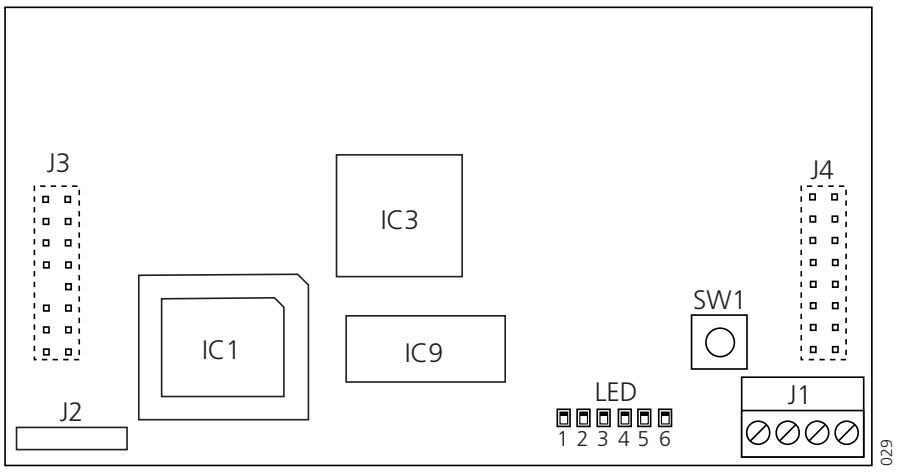
Circuit board replacement

Figure 185: Replacing the Elise 2 Server (AIWS Hardware) circuit board.



1. Perform a power down of the unit.
2. Remove the cover, see Opening the housing on page 533.
3. Lift off the screw connectors from the circuit board. (1)
4. Press the four holding clips to release the circuit board (2).
5. Remove the circuit board (3).
6. Install the new circuit board in the case and make sure the circuit board clicks into position.
7. Set all switches and jumpers as they were on the original circuit board and replace the screw connectors.
8. Check installation according to Installation test procedure on page 546.

LON Piggy Back Circuit Board (LPB)



Connectors and Jumper Points

J1	Connection for the teleCARE M LON (only use terminals 1 and 2)
J2	Connector for In System Programming (ISP) of the flash micro controller
J3	Male connector to be put on J9 on Elise 2 Server (AIWS Hardware) circuit board. Pin 12 cut off
J4	Male connector to be put on J10 on Elise 2 Server (AIWS Hardware) circuit board

Push button

SW1	For service

Micro Controllers and others

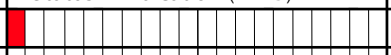
IC1	Flash memory
IC3	Neuron micro controller
IC9	PIC flash micro controller

LEDs

LED1	LON Rx
LED2	LON Tx
LED3	See table for LED3 in Status indication of LPB on page 555
LED4	Rx data transfer
LED5	Tx data transfer
LED6	See table for LED6 in Status indication of LPB on page 555

Status indication of LPB

LED3

Sequence	Status 1 Indication (LED3)	Function
1		Power up (On momentarily)
2		Normal operation (Off continously)
3		Watch-dog reset
4		Unconfigured (Neuron uC)
5		No application (no Neuron firmware)
	Each segment = 100 ms	

030

LED6

Sequence	Status 2 Indication (LED6)	Function
1		Searching for baudrate. No connection with NSS/ISC main board
2		Normal operation. Connection with NSS/ISC main board (LON Protocol running)
	Each segment = 250 ms	

031

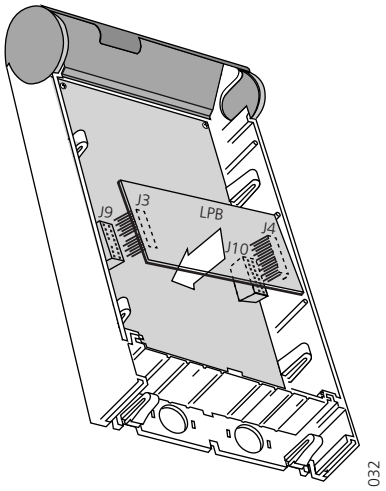
Installation of LPB

Important:
Always follow the instructions in Powering down and restarting the Elise 2 Server (AIWS Hardware) on page 527 when disconnecting the power to the Elise 2 Server (AIWS Hardware).

1. Remove the cover from the Elise 2 Server (AIWS Hardware), see Opening the housing on page 533
2. Perform a power down of the Elise 2 Server (AIWS Hardware), see Power Down on page 527
3. Lift off the screw connector J1 from the LPB

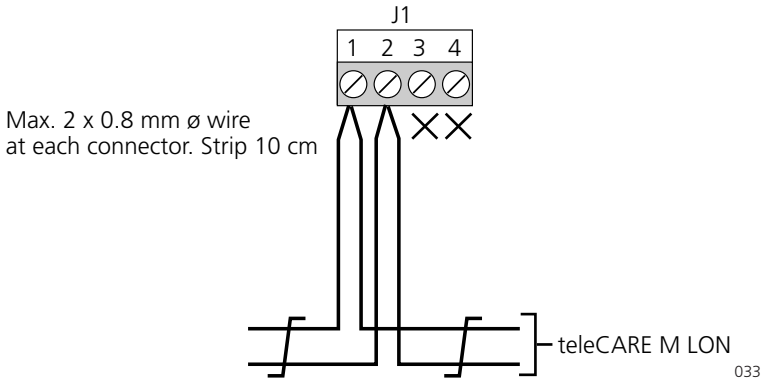
4. Attach the LPB on the Elise 2 Server (AIWS Hardware) circuit board. Carefully line up the male connector pins of the LPB with the female connector of the Elise 2 Server (AIWS Hardware), then press the LPB down firmly. (To avoid misalignment, the pin 12 on the J3 connector of the LPB is cut off and the corresponding hole on the J9 connector of Elise 2 Server (AIWS Hardware) plugged). See figure 186 below.

Figure 186: Mounting of LPB on Elise 2 Server (AIWS Hardware) circuit board



5. Connect cables to the screw connector J1. Use max. 2 x 0.8 mm wires per connector. Strip the outer sheath of the cables to a length of about 10 Communication Manager. Only use pins 1 and 2 for connection of the LON bus in/out. (Pins 3 and 4 can be used for connection of other LON devices, for example SLA). See figure 187 below.

Figure 187: Cabling of screw connector J1



6. Replace all removed connectors
7. Close the cover and restart Elise 2 Server (AIWS Hardware), see Powering down and restarting the Elise 2 Server (AIWS Hardware) on page 527.

Installing Elise 3 Server (AIWS2 Hardware)

Introduction

The Elise 3 Server (AIWS2 Hardware) is an embedded Linux based hardware platform for applications such as messaging, alarm handling, administration and device management. The module can be used independently but also works in combination with other modules or systems.

The Elise 3 is available in several hardware variants. The Avaya IP-DECT R4 system uses the Elise 3 Lite variant.

The Elise 3 Lite is intended for connections via IP only. It has two LAN connections, two USB 2.0 ports for communication with external devices, one mini-USB port for easy management and is equipped with two galvanically isolated physical inputs and outputs. The inputs can be used for trigger conditions which in turn can use the outputs for actions.

Figure 188: Elise 3 Server (AIWS2 Hardware)



Specifications

The license and supported features are application dependent and therefore described in the application documentation and the datasheet.

Parameter	Value
Supply voltage:	12 – 24 V/DC ±10%
Current consumption:	Max 275 mA at 100 V AC input Max 1 A at 12 V DC input

Delivery includes:	Elise 3 Server (AIWS2 Hardware)[1]
	Two assembly brackets
	Four screws size 3.5×40 together with four wall plugs
	Four MFT screws size M3×6 for fastening the assembly brackets
	Power cable
	• Avaya Safety leaflet for AIWS2 • Getting started document: Elise 3, Embedded Linux Server including safety and security instructions
Tools etc. required:	• Philips screwdriver (Ph No. 2) for the wall screws size 3.5×40 • Torx (T10) for the MFT screws size M3×6 • Screwdriver 0.40 x 2.5 mm for screw connectors on the rear side
	Cutting pliers
	Ethernet cable
	Screws for installation
	Multimeter
	Power supply
	PC with Microsoft Internet Explorer 8.0 and 9.0, Mozilla Firefox 3.6 up to 12.0 Sun™ Java™ Runtime JRE 6
	Software "Route to Elise". (Available from the distributor)

1. Separately ordered license certificate

Memory	Capacity
SDRAM	256 MB
NAND Flash	1 GB for software application
Serial data flash	8 MB for booting purposes
SD card(currently not supported- for future use only)	1 slot for 1 GB SD card

FCC Compliance statements for Class B Digital device

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Re-orient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio or television technician for help.

Information to user

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- this device may not cause harmful interference, and this device must accept any
- interference received, including interference that may cause undesired operation.

Modifications

Changes or modifications to the equipment not expressly approved by the party responsible for compliance could void the user’s authority to operate the equipment.

IC Requirements for Canada

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la Classe B conforme á la norme NMB-003 du Canada.

EU Compliance Statements for Class A Device

This is a limit-class A device. This device can cause radio interference in residential areas, in which case the owner may be required to undertake appropriate countermeasures.

AIWS2 Overview

Connectors, LEDs and buttons

The Elise 3 Server (AIWS2 Hardware) front panel has various status indicators and is used for maintenance. The LEDs indicates the status of the module and the management port makes it possible to have direct connection to the module. It also has an SD card slot and two USB ports for external temporary devices.

The rear panel is used for connecting supply voltage, communication to external systems and for connecting inputs and outputs. It has two LAN connections, two com ports for communication with external devices, one mini-USB port for easy management and is equipped with two galvanically isolated physical inputs and outputs. The inputs can be used for trigger conditions which in turn can use the outputs for actions. It also has the A bus connector, the LON connector, AUX input and outputs, and a error relay output conection on the rear panel. The rear side also houses the connections for the external battery and AC power supplies.

Figure 189: Elise 3 Server (AIWS2 Hardware) front and rear panels

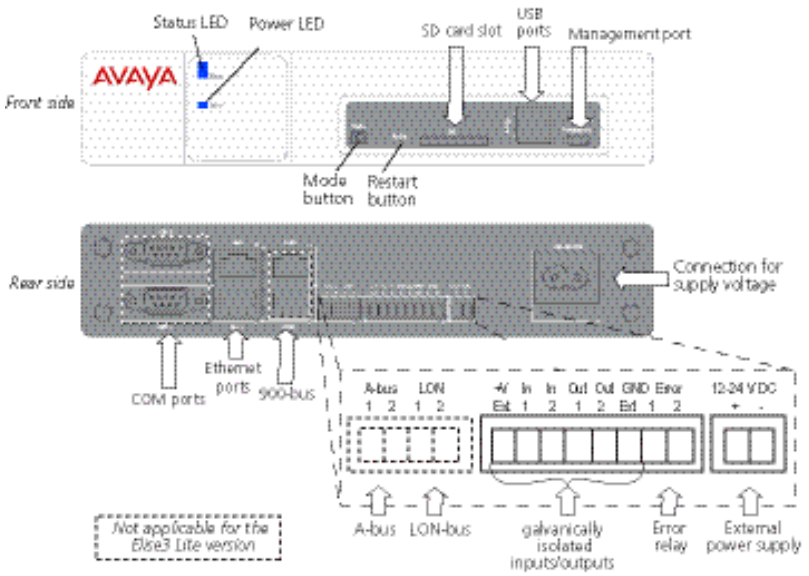


Table 1: Connections, buttons and LEDs on the Elise 3 Server (AIWS2 Hardware) Front panel

Restart button	The Restart button is a hole button that requires a paper clip (or similar) to be able to push. Used for performing controlled restart and forced restart, See Powering down and restarting the Elise 3 Server (AIWS2 Hardware) on page 564
Power LED	Indicates the Power status

Table 1: Connections, buttons and LEDs on the Elise 3 Server (AIWS2 Hardware) Front panel

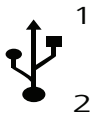
	USB Port 1 USB Port 2
Management	Mini-USB port for device management See Accessing the Elise 3 Server (AIWS2 Hardware) through the management port (USB) on page 581
Mode button	A temporary push button with a blue LED. Used to place the module into specific modes using different push patterns. See Powering down and restarting the Elise 3 Server (AIWS2 Hardware) on page 564
SD Card slot	Currently not used

Table 2: Connections, buttons and LEDs on the Elise 3 Server (AIWS2 Hardware) Rear panel

LAN1	Modular jacks (RJ45) for connection of 10baseT or 100baseT Ethernet. See Ethernet ports on page 578
LAN2	Currently not used (for future releases)
S900/S900	Modular jacks (RJ45) for connection of A-bus from System 900 with modular system bus cabling, see A-bus connection to System 900 on page 578 Not applicable for the Elise 3 Lite version.
A-bus	Screw connector for connection of A-bus from System 900 when modular system bus cable is not used, see A-bus connection to System 900 on page 578 Not applicable for the Elise 3 Lite version
LON	Screw connector for connection of the LON bus, see LON Bus on page 579 Applicable for the Elise 3 LON version only
V+ Ext/GND	Ext External 12 V power supply to provide galvanic isolation of the inputs and outputs, see below.

Table 2: Connections, buttons and LEDs on the Elise 3 Server (AIWS2 Hardware) Rear panel

In1/In2 and Out1 Out2	Connects AUX inputs and AUX outputs, see Connection of AUX inputs and AUX outputs on page 580
COM1/COM2	COM ports for connection of RS232 communication, see COM Ports (RS232 communication with external equipment) on page 578 Not applicable for the Elise 3 Lite version

License

All Elise 3 Server (AIWS2 Hardware) units must have a valid software license. The license document is included in the AIWS2 package.

You can find the license on the administration web page, under the section System Setup > Common > License.

Important:
Changing this field may seriously affect the functionality.

If no valid license is present, the unit can be started in unlicensed mode, see Unlicensed mode on page 565 and Operating modes on page 564 for more information.

Note:
Licenses can be moved from Elise 2 to Elise 3 server, refer to Moving a license from Elise 2 Server (AIWS Hardware) to the Elise 3 Server (AIWS2 Hardware) on page 595.

Mac address

The MAC address can be found on a label on the products rear side, in the application's GUI in the Setup Wizard, on the Configuration page (the first view) and on the Advanced Configuration page in Troubleshoot > System Information. It is also found in the Boot Mode GUI under System > Information.

Powering down and restarting the Elise 3 Server (AIWS2 Hardware)

Powering down

1. Press the Restart button using a paper clip and release within 4 seconds.The Status LED indicates shutting down with quick flashing blue light.
2. Wait until module shuts down, then remove the power cable. If power to the device is not disconnected the Elise 3 Server (AIWS2 Hardware) restarts in about a minute. Before starting up again, the Status LED will indicate “waiting” for one minute with fixed yellow light. You can remove the power cable within this period. If the power cable is not detached the system restarts and the Status LED indicates starting up with quick flashing blue light.

Performing a controlled restart

There are two ways to restart an Elise 3 Server (AIWS2 Hardware):

- following the power down instruction above, and then apply the power again, or
- initiate a restart from the administration web page.

Note:

When a controlled restart is performed via the Restart button, all ongoing jobs on the module end in a controlled way and everything is logged.

Performing a forced restart

1. Use a paper clip or similar and press the Restart button for at least 5 seconds. The power LED will turn off for a short time (3 seconds) and when it turns on again the Status LED indicates starting up with quick flashing blue light.

Note:

Forced restart is used as a last resort when the module does not respond at all. When a Forced restart is performed, ongoing jobs are not finished (as in a controlled restart). During startup, there is a delay for three seconds in which you can start the module in Boot Mode.

Operating modes

Apart from the normal mode, there are three different operating modes; Boot mode, Demonstration Mode (unlicensed), and Troubleshoot Mode.

Normal mode

All configuration and settings for the application, maintenance such as backups, software upgrade and troubleshooting, are performed in the application GUI and is described in the separate application documentation. The application GUI is the web user interface for the software application running on Elise 3 Server (AIWS2 Hardware).

Boot mode

The Boot Mode can be used for installing new software, viewing settings, performing factory reset, troubleshooting and also starting up in normal operation again. If the module detects several major errors (for example restart loop), the module can set itself in Boot Mode.

When the application running on Elise 3 Server (AIWS2 Hardware) cannot be accessed, the module can be set in Boot Mode. From the Web Interface or the GUI it is possible to install new software, start Troubleshoot Mode, view settings and to reset the module back to factory default settings. Placing the module in Boot Mode is performed manually by the user but if the module detects several major errors the module can place itself in Boot Mode.

See Starting in boot mode on page 565

Troubleshoot mode

Troubleshoot Mode makes it possible to troubleshoot the system and access log files when it is impossible to access and troubleshoot in the application running on Elise 3 Server (AIWS2 Hardware). No application is started in the Troubleshoot Mode.

Unlicensed mode

It is possible to run the Elise 3 Server (AIWS2 Hardware), with full functionality for two hours, without a license. Exact functionality is application dependent. For more information about the functionality during unlicensed mode, see the application documentation.The Unlicensed Mode can be set when the module is running in normal operation, either via the application's web interface or manually by using the Mode button.

See Starting in unlicensed or demonstration mode on page 566

Selection of operating mode

Starting in boot mode

1. Press the Restart button and release within four seconds. The Status LED indicates quick shutting down with a quick flashing blue light and then ’waiting’ with fixed yellow light.

2. Wait for one minute until the status LED indicates starting up with quick flashing blue light , then press the Mode button.The Mode button LED will lit and show fixed blue light
3. Wait untill the Status LED changes to quick flashing yellow light which indicates that the module has started in Boot Mode(After approximately one minute).
4. Open the web browser and enter the modules IP address to log on.

Starting in unlicensed or demonstration mode

1. Press and hold the Mode button for 10 seconds.The unlicensed or Demonstration Mode is indicated by the Status LED with slow flashing yellow light and by the Mode button LED with fixed blue light .
2. To exit the module within the limit of two hours, access the application’s web interface.

The module will automatically return to the previous license and parameters (without restart) after 2 hours. You can also restart the Demonstration Mode after exiting, from the application's web interface after a delay of 10 minutes. In case you want an immediate restart you can use the Mode button.

Status LED indicators

Figure 190: Status is indicated by the Status LEDs according to the list below.

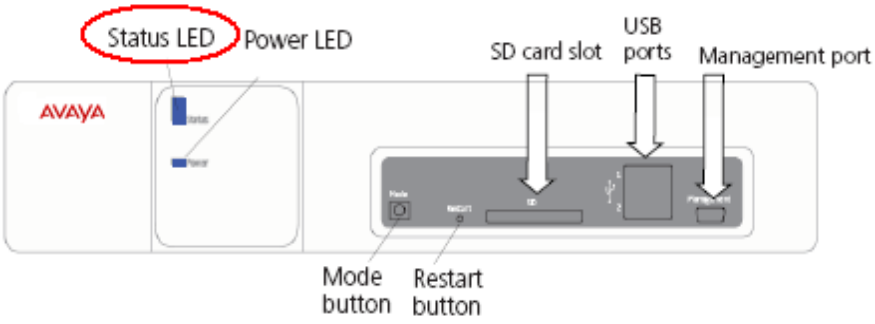
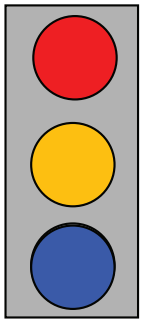


Figure 191: LED Indications

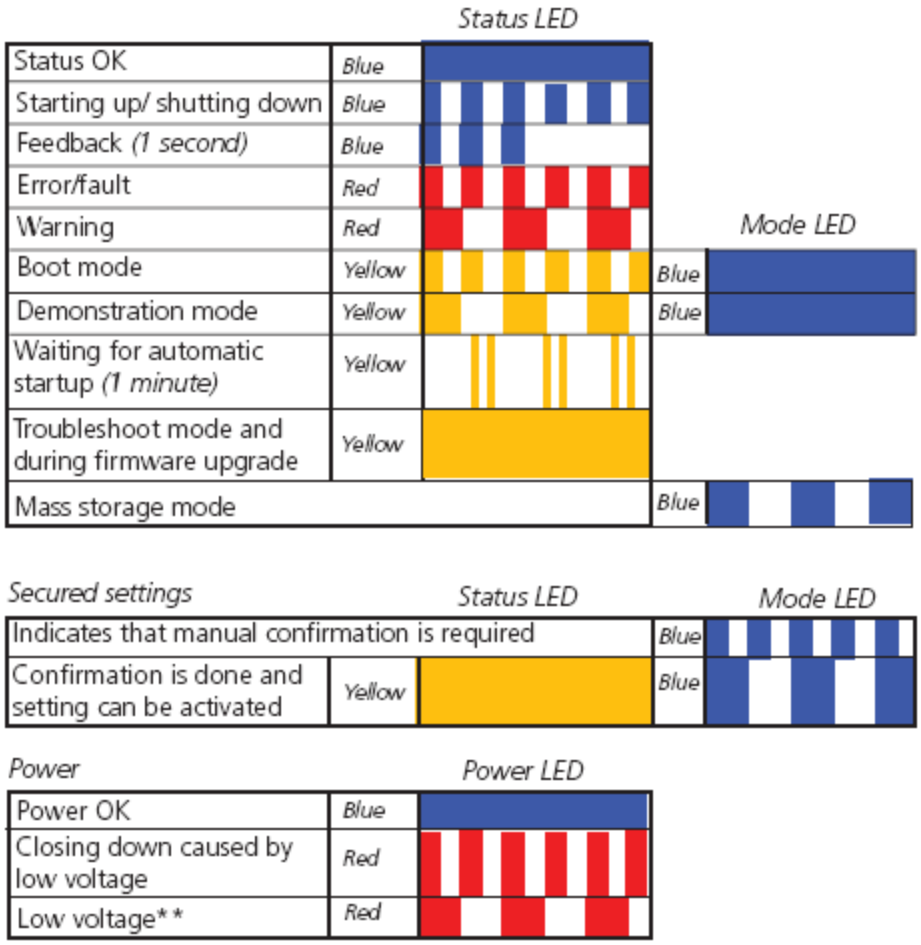


The LEDs show different colours to determine the type of information and have different flashing modes for showing the priority..

Color	Indication
Red	Fault
Yellow	Mode
Blue	Normal

- Fixed light incates normal state
- Slow flashing light indicates medium attention
- Quick flashing light indicates high attention

Figure 192: LED Status Indicators



** also used if the Power parameter conflicts with the actual setup.

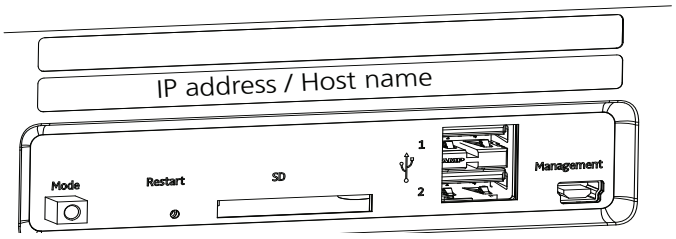
Label for IP address/Host name

To facilitate future support and access to the module, the module's IP address or Host name can be printed on a blank label and attached to the module as shown in the figure below.

The blank label is found on the back side of the Getting started and Safety document:

"Elise 3 – EMBEDDED LINUX SERVER INCLUDING SAFETY INSTRUCTIONS", included in the delivery.

Figure 193: Label for IP Address/Host name



Authentication and administration

Administration on Elise 3 Server (AIWS2 Hardware) is done from a web browser. You need a user name and password in order to access the administration pages.

Important:
The default passwords must be changed to prevent unauthorized access.

Authentication

There are two different users in all Elise 3 Server (AIWS2 Hardware) products; admin and sysadmin.

The user *admin* has the default password "changeme" and is used for administration and simple troubleshooting of the product. The admin has permission to change all passwords except the sysadmin password.

The user *sysadmin* has the default password "setmeup" and is used for advanced troubleshooting. The user also has access to all administration pages. The sysadmin has permission to change passwords for all users in the product.

In addition, there are two other users in some Elise 3 Server (AIWS2 Hardware) products. One is called *user* and the default password is "password". This user is product dependent and its usage is described in corresponding product documentation. This user does not have access to the administration pages where passwords normally are changed. The user can change its own password on the following page; http://xxx.xxx.xxx.xxx/admin/public/user_chpass.shtml. The password can also be changed by the users admin and sysadmin.

The other user is called *ftpuser* and the default password is "changemetoo". The user is available for products with a FTP area. The user can change its own password on the following page; http://xxx.xxx.xxx.xxx/admin/public/ftpuser_chpass.shtml.

Administration

To access the web pages below, the user *admin* is used.

You can access the web page on "xxx.xxx.xxx.xxx/admin", where xxx.xxx.xxx.xxx is the modules IP address. For applications having a start page, You can also press the “Configuration” button on the start page and then select Other Settings > Advanced Configuration.

You can be set and change all configurations through the Advanced Configuration page, such as system setup, changing passwords, etc. This page also contains troubleshooting and detailed configuration, for example Messaging interfaces.

As an admin user you can perform the following tasks:

- System setup, for example System 900 configuration
- Troubleshooting information
- Changing passwords

You must use the "xxx.xxx.xxx.xxx/system" page when:

- Replacing current software installation.
- No software is installed on Elise 3 Server (AIWS2 Hardware).
- Updating or installing Compact Flash image

The system page can also be used when configuring network parameters.

Installing the Elise 3 Server (AIWS2 Hardware)

The Elise 3 Server (AIWS2 Hardware) should be placed in a dry environment within a temperature range of 0 to +40°C. The Elise 3 Server (AIWS2 Hardware) can be mounted vertically on a wall or be placed horizontally on a 19" rack. It must be fixed by screws or other fixtures to the wall or rack, and must not be easily movable.

The Elise 3 Server (AIWS2 Hardware) can be connected via system bus cabling, or via twisted-pairs together with other units in the System 900. The Elise 3 Server (AIWS2 Hardware)s can communicate with each other via the TCP/IP network.

Important:
Always follow the instructions in Powering down and restarting the Elise 3 Server (AIWS2 Hardware) on page 564 when disconnecting the power to the Elise 3 Server (AIWS2 Hardware).

Note:
Install only one Elise 3 Server (AIWS2 Hardware) at a time, otherwise IP address conflict might occur.

Installation procedure

1. Read chapters 4.1 and 4.2 before starting the installation.
2. Mount the device, see Mounting on page 571.
3. Connect the suppy voltage, see Supply voltage on page 576.
4. Access the module through the web interface, see Accessing the Elise 3 Server (AIWS2 Hardware) on page 580.
5. Fill in the required data, see Basic configuration on page 586.
6. Connect to the equipment as required, see Connectors, LEDs and buttons on page 560.

Mounting

You can mount the Elise 3 Server (AIWS2 Hardware) horizantally or vertically on a 19 " wall mounting or a rack mounting. You can also mount the module side-by-side or back to front in the rack,

Wall mounting

Note:

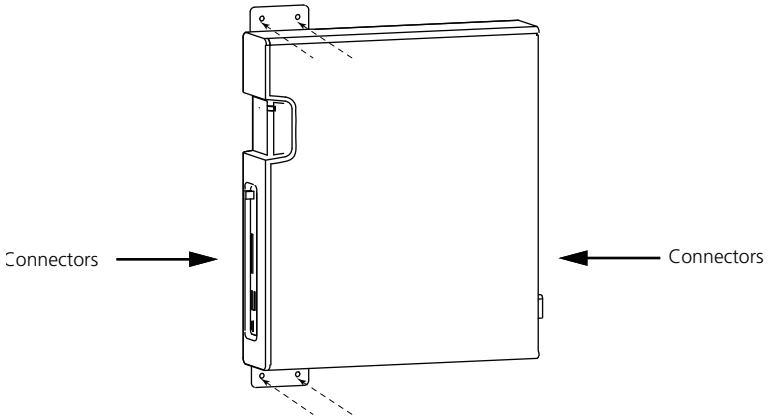
Four screws size 3,5×40 together with four wall plugs and four screws size M3×6, are delivered with the product. The M3×6 screws are used for attaching the assembly brackets to the module. Use the 3,5×40 screws for walls made of wood. For walls made of concrete and bricks use them together with the wall plugs. For other types of walls use suitable screws and plugs according to wall material.

Important:

When mounted on a wall, ensure that the connections are located in a vertical plane to fulfil the fire classification requirements.

1. Fasten the supplied assembly brackets on the bottom side of the module.
2. Use the supplied screws and wall plugs (or other suitable screws and plugs dependent on wall material) and mount the module as shown in the picture below.

Figure 194: Mounting on a wall



Rack mounting

The Elise 3 Server (AIWS2 Hardware) can either be front mounted or reverse mounted in a 19´´ rack.

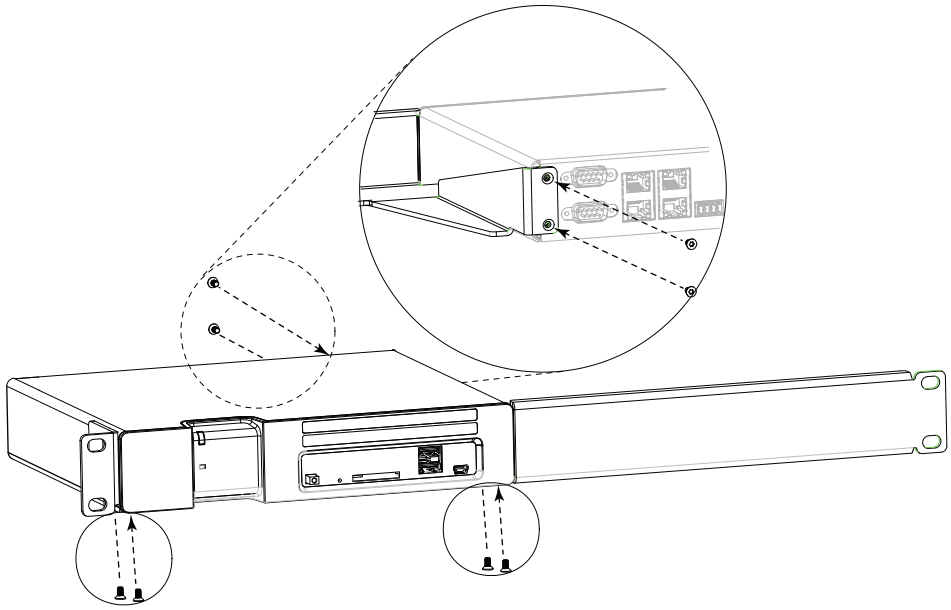
Accessories required for mounting in a rack (To be ordered separately):

Standard 19" rack kit	Small left/right brackets for two front mounted Elise 3 modules and one big bracket for one front mounted Elise 3 module.
Reverse 19 " rack kit	Small left/right brackets for two front mounted Elise 3 modules and one big bracket for one reverese mounted Elise 3 module

Front mounting single (requires the standard 19´´rack kit)

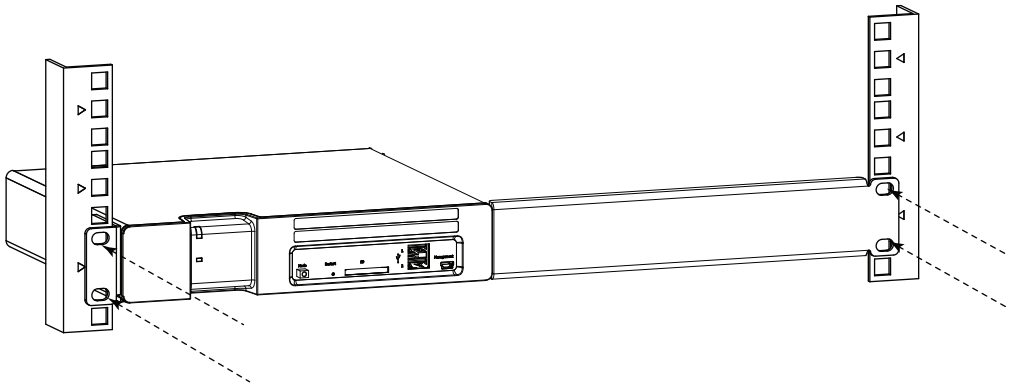
1. Fasten the big assembly bracket on the right side of the module and the small ssembly bracket on the left side as shown in the figure below.

Figure 195: Front Mounting single rack 1



2. Fasten the assembly brackets in the rack.

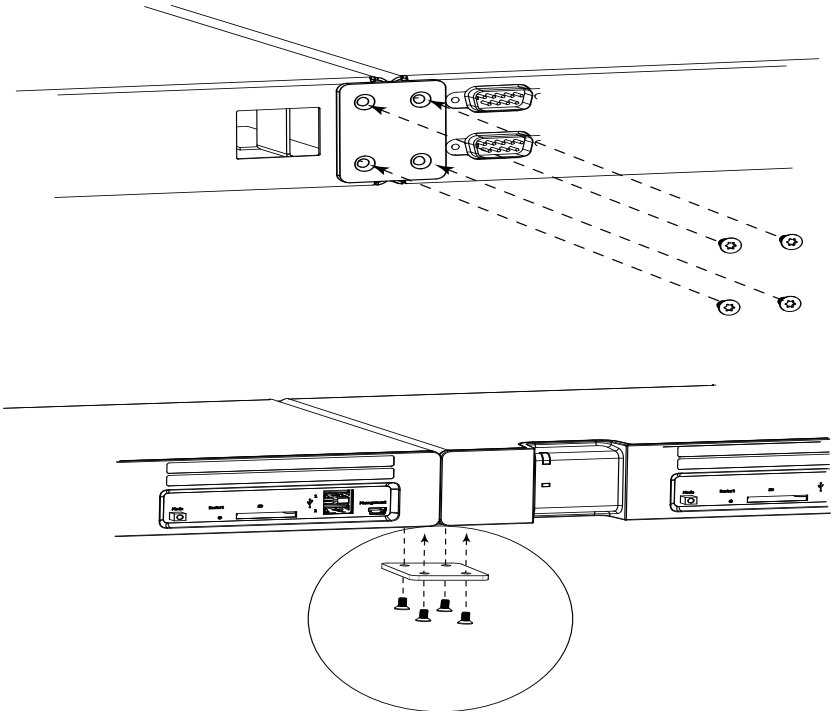
Figure 196: Front mounting single rack 2



Front mounted double (requires the Standard 19" rack kit)

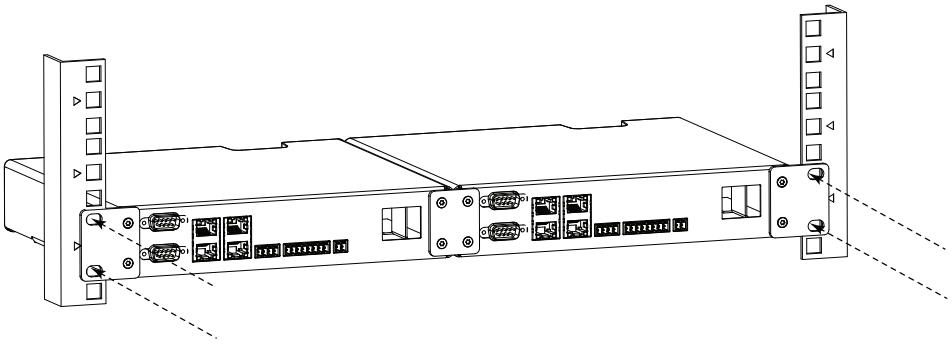
1. Use the supplied assembly brackets and fasten the two modules together, both on the rear side and on the bottom side, as shown in the two figures below:

Figure 197: Front mounted double rack 1



2. Use the two small standard assembly brackets and fasten one on the right front side and the other on the left front side.
3. Fasten the assembly brackets in the rack, see figure below (screws not included).

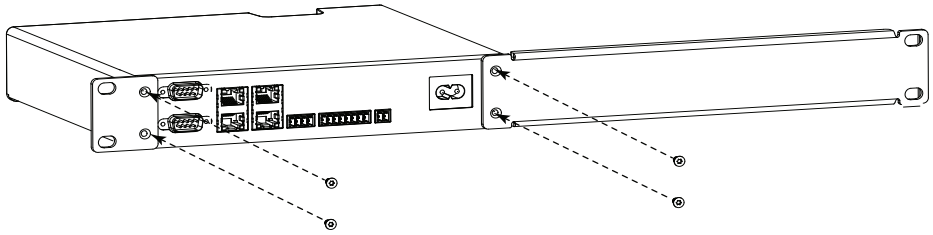
Figure 198: Front mounted double rack 2



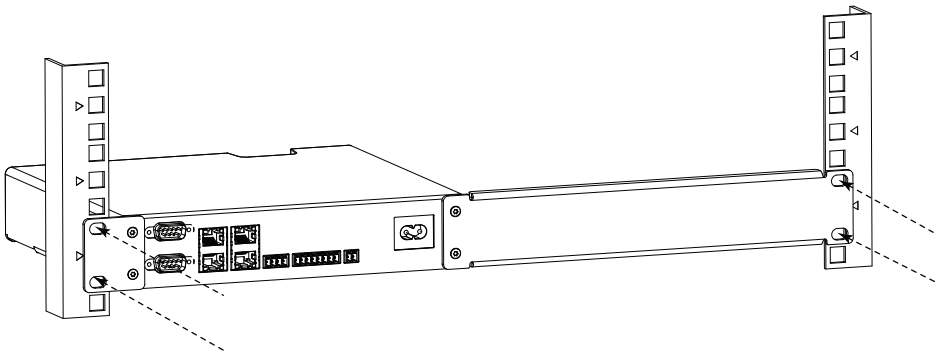
Rear mounted single (requires reverse 19 " rack")

1. Fasten the big assembly bracket on the right side of the module and the small assembly brackets on the left side, as shown in the figure below.

Figure 199: Rear Mounted single 1



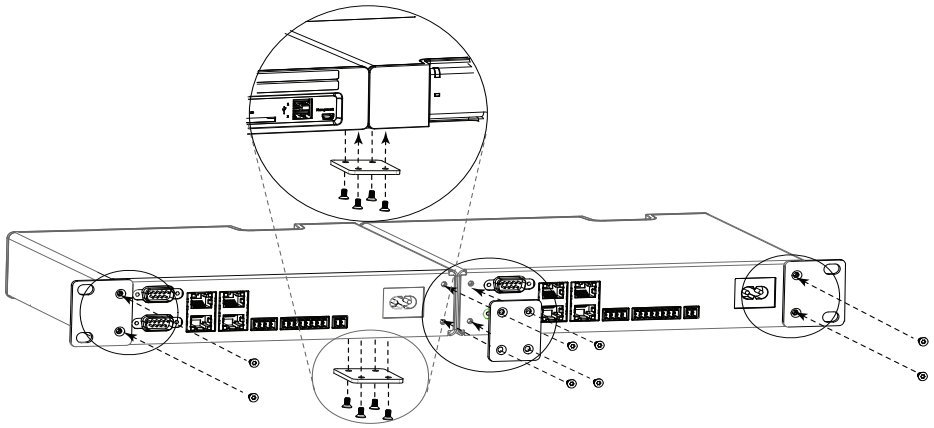
2. Fasten the assembly brackets in the rack, see below (screws not included)



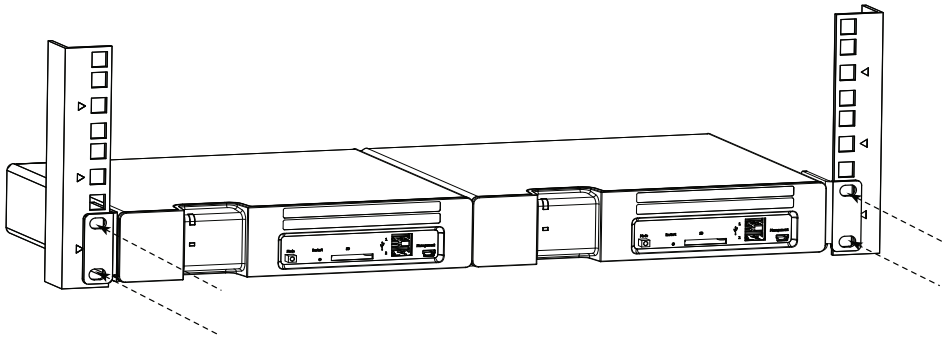
Rear mounted double (requires the reverse 19" kit)

1. Use the supplied assembly brackets and mount the two modules together, both on the rear side and on the bottom side, see figure below.
2. Use the two small reverse assembly brackets and fasten one on the right rear side and the other on the left rear side.

Figure 200: Rear Mounted double



3. Fasten the assembly brackets in the rack, see below (screws not included).



Supply voltage

The Elise 3 Server (AIWS2 Hardware) can be connected to an external power supply (12-24 V DC battery or power source) as a complement to the primary power supply (100-240 V AC). If the primary power supply fails it switches over to the external power supply automatically, without any negative influence on the running application.

Note:

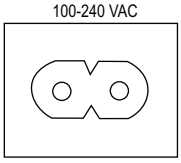
A 24 hours backup requires a 12V battery with at least 4.8 Ah.

Important:
For installation on ships the 12 - 24 V DC input should be used to meet the regulatory requirements for safety and EMC. (To meet the regulatory requirements for EMC alone, the 12 - 24 V DC input should be used on deck, bridge and in special power distribution zones while 100 - 240 V AC input can be used in general power distribution zones).

Primary power supply 100-240 V AC

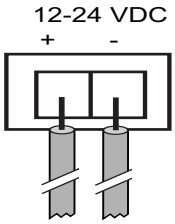
Connect supply voltage to the 100-240 V AC jack as shown in figure:

Figure 201: 100-240 V AC



Connect the external power supply to the 12-24 V DC screw connector.

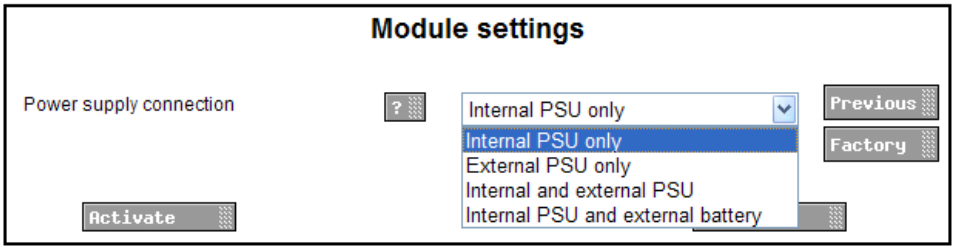
Figure 202: 12-24 V DC connection to external supply



Changing power supply parameters

By default, the Elise 3 Server (AIWS2 Hardware) is configured to use the primary power supply (100-240 V AC). If you connect the module to an external battery, you must configure accordingly from the Advanced Configuration page. If the parameter setting conflicts with the actual setup, the Power LED will indicate with slow flashing red light.

1. Select Other Settings > Advanced Configuration in the menu on the Configuration page.
2. Select Power supply in the menu on the Advanced Configuration.



3. Select setting in the drop-down list (Internal PSU only, External PSU only, Internal and external PSU or Internal PSU and external battery).
4. Click "Activate".

Connections

COM Ports (RS232 communication with external equipment)

Note:
(Applicable only to the Elise 3 Standard or LON variant).

Utilization of the RS232 ports depends on the application software. The Elise 3 Server (AIWS2 Hardware) has two identical RS 232 connectors; COM1 and COM2.

Ethernet ports

The Elise 3 Server (AIWS2 Hardware) has two 10baseT/100baseT Ethernet modular jacks (RJ45) but only the jack marked 1 is currently in use (the jack marked 2 is intended for future releases).

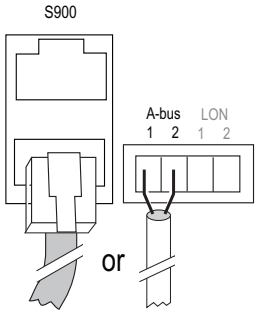
Important:
Shielded ethernet cables should be used for installation on trains to meet the regulatory requirements for railway equipment.

A-bus connection to System 900

Note:
Not applicable for the Elise 3 Lite version.

The Elise 3 Server (AIWS2 Hardware) module can be installed together with System 900 modules, either via modular system bus cabling or via twisted-pair lines to 1 and 2 on screw connector A-bus.

Figure 203: Modular jacks for system bus and screw connectors for twisted pairs



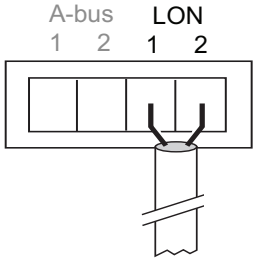
LON Bus

Note:

Requires the Elise 3 LON variant.

The Elise 3 Server (AIWS2 Hardware) module can be installed together with teleCare M modules. Connections are made with twisted pairs to 1 and 2 on screw connector LON.

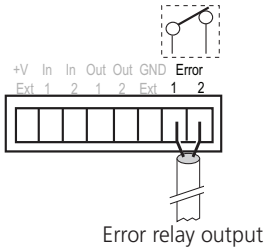
Figure 204: LON connector



Error relay output

A relay output is used to indicate Elise 3 Server (AIWS2 Hardware) module malfunction and can also be used to indicate other errors. See the application documentation for more information about functionality. Connections are made with twisted pairs to 1 and 2 on screw connector.

Figure 205: Error Relay



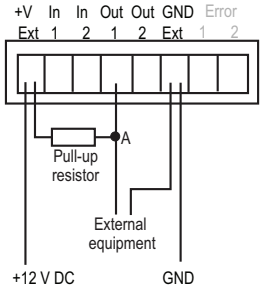
When the Elise 3 Server (AIWS2 Hardware) is running the relay is closed, i.e. the error relay output is activated when the relay releases, for example if the power is dropped. At power up or restart the relay is released until the applications are working properly. If the relay is released longer the Elise 3 Server (AIWS2 Hardware) is malfunctioning.

Connection of AUX inputs and AUX outputs

Note:

The application of the inputs and outputs is software dependent.

Figure 206: AUX input and outputs



Two digital inputs and two digital outputs can be connected. The outputs are of open collector type and the output signals are dimensioned for 100 mA at max 12 V. A pull-up resistor should be connected to the output as shown in figure above. Galvanic isolation of the inputs and outputs is provided by using a separate power supply. If galvanic isolation is not needed and the Elise 3 Server (AIWS2 Hardware) is supplied by an external 12 V power source, the supply voltage can be taken from the 12-24 V DC screw connector by connecting +V Ext to “+” and GND Ext to “-”. The inputs In 1 and In 2 are active when they are connected to 12 V. When the output Out 1 is active, the potential in point A in above figure will be close to 0 V. The same applies for a similar connection for Out 2.

Accessing the Elise 3 Server (AIWS2 Hardware)

The Elise 3 Server (AIWS2 Hardware) can be accessed either via an IP network or directly via the management port (mini-USB). You can access the product´s web interface using browsers Internet Explorer 8.0™, Mozilla Firefox 3.6 or later.

Accessing the Elise 3 Server (AIWS2 Hardware) through the network

Avaya recommends that the Elise 3 Server (AIWS2 Hardware) module should always be assigned the same IP address if it communicates with other equipment, to prevent it from losing contact with the equipment after a restart. You can inform the network administrator about the MAC address and reserve a fixed IP address for the Elise 3 Server (AIWS2 Hardware) through the DHCP server.

Write the IP address on the blank label, found on the back side of the Getting Started and Safety document and attach the label on the front side to facilitate future access.

See Label for IP address/Host name on page 568

Note:

If NetBIOS is enabled in the network, the address elise-XXXXXXXX can be used when accessing the module via the network, where XXXXXXXX is the module key number. The module key number can be found on the license certificate or on the label on the back of the module.

Browser requirements to access Elise 3

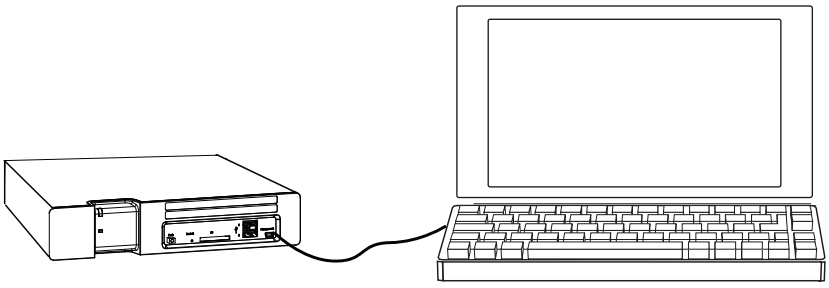
- Windows® Internet Explorer® (versions: 8.0 or 9.0)
- Mozilla Firefox® (versions: 3.6 up to 12.0)
- Java applets have to be enabled for messaging status and Device Management.

1. Connect the module to the LAN.
2. Open the web browser and enter the modules IP address or elise-XXXXXXXX, where XXXXXXXX is the module key number (leading zeros can be excluded). The module key number can be found on the license certificate or on the label on the back of the module.
3. Continue with the basic configuration steps, See Basic configuration on page 586.

Accessing the Elise 3 Server (AIWS2 Hardware) through the management port (USB)

The management port can be used when Elise 3 Server (AIWS2 Hardware) does not have a valid and unique IP address, when the IP address has changed or the Elise 3 Server (AIWS2 Hardware) is moved from one network to another. The management port gives access to the module without having access to the customer’s network.

Figure 207: Connection through the Management port



Note:

The reserved IP address for accessing the Elise 3 Server (AIWS2 Hardware) through the management port is “192.5.36.229”.

Note:

A port driver must be installed on your PC to get access through the management port.

The default mode for the management port is **Network access** but the **Mass storage** mode is used to get the required driver for the module. When set to **Mass storage**, the module will automatically change to the **Network access** mode within 10 minutes. By pressing the **Mode** button twice, the Management port toggles from **Network access** to **Mass storage** mode and the other way around.

The **Mass storage** mode is only used when the driver, required for accessing the module through the management port, shall be installed. This mode is utilized only when the PC is used for the first time.

1. Connect a mini-USB type B cable between the USB port on your PC and the management port on the module.

Note:

If the required port driver is not installed on the PC, install it now. The installation differs and is dependent on the operating system. See either Installing the port driver on Windows XP/Vista on page 582 below or Installing the port driver on Windows 7 on page 584.

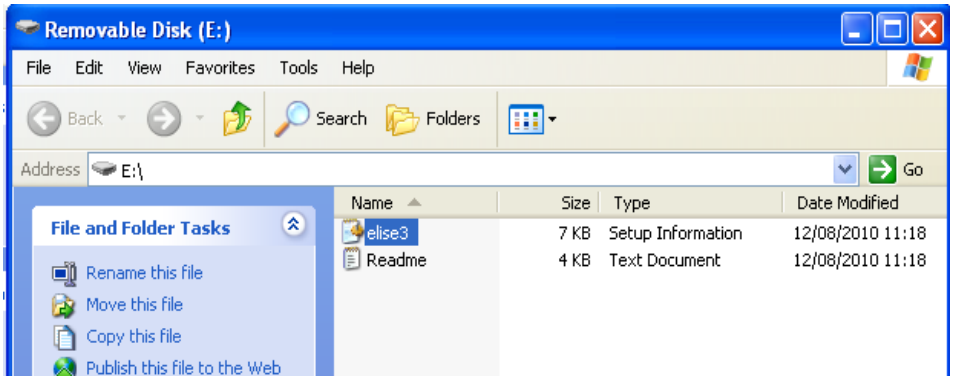
2. Open a web browser on your PC and enter the IP address “192.5.36.229" in the address field to access the products web interface.
3. Continue the basic configuration steps. See Basic configuration on page 586.

Installing the port driver on Windows XP/Vista

Note:

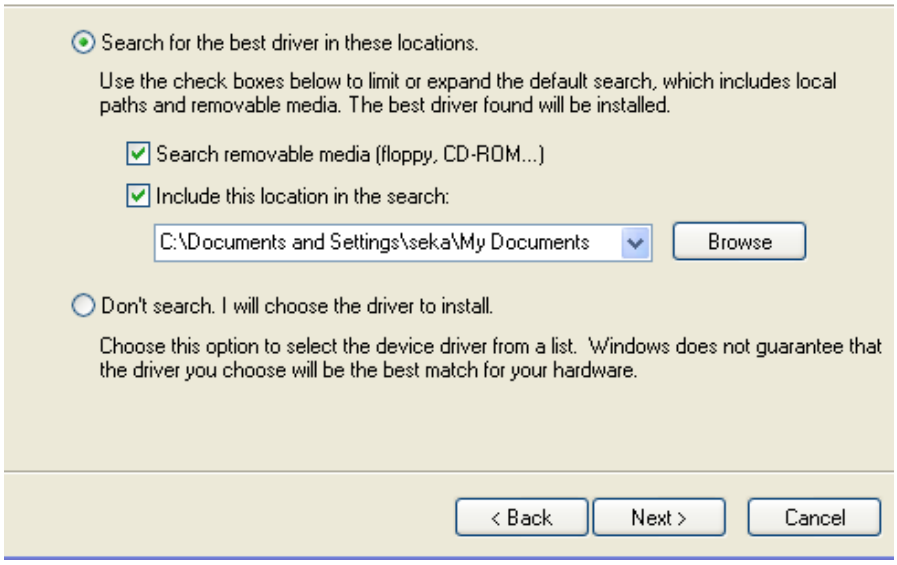
When switching between **Mass storage** mode and **network** mode, it takes about 30 seconds before the module can be accessed with the 192.5.36.229 address.

1. Connect a mini-USB type B cable between the USB port on your PC and the management port on the module. The **Found new hardware** wizard opens but at this stage the valid port driver is not present, so close the wizard and continue to install the driver.
2. Press the **Mode** button twice to change the mode to mass storage.The module will now turn up as a mass storage device on your computer. This is indicated by slow flashing blue light on the Mode button LED.
3. Locate the required “elise3.inf” driver and save it on your PC.



4. Press the Mode button twice again to change the mode to network access[1]. The Found new hardware.... dialogue box opens.
5. Select No, not this time and click “Next”.
6. Select Install from a list or specific location (Advanced) and click “Next”.
7. Select Search for the best driver in these locations.
8. Select the Include this location in the search: check box.
9. Browse to the folder where the port driver is saved.

1. If not pressed within 10 minutes, the module will automatically change to Network access (default mode).



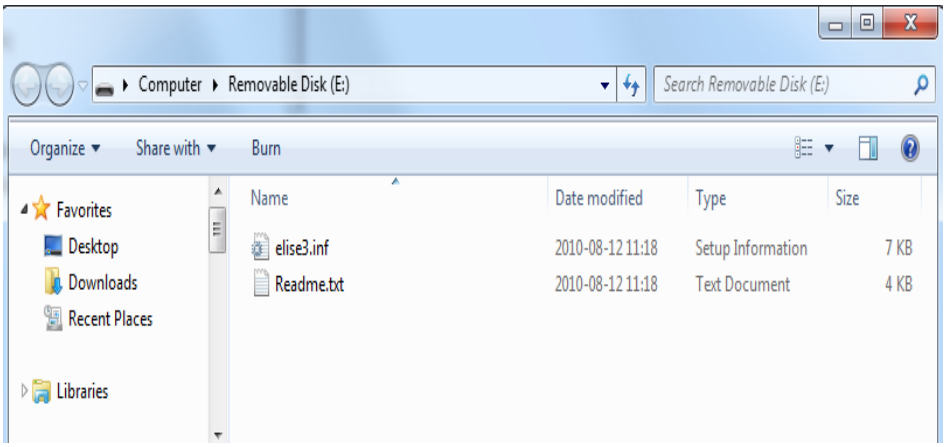
10. Click “Next”. The installation of the port driver begins. If a message opens, saying the software has not passed Windows Logo testing, click “Continue Anyway”.
11. Click “Finish”. A dialogue box will open and inform you that new hardware is installed.

Installing the port driver on Windows 7

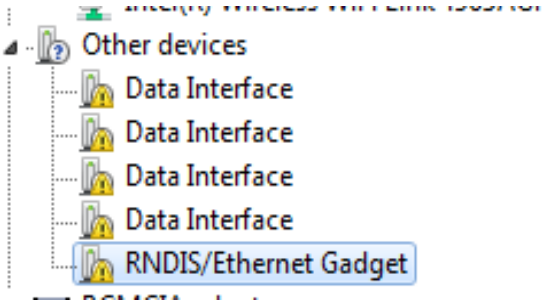
Note:

When switching between mass storage mode and network mode, it takes about 30 seconds before the module can be accessed with the 192.5.36.229 address.

1. Connect a mini-USB type B cable between the USB port on your PC and the management port on the module. The Found new hardward wizard opens but at this stage there is no valid port driver so close the wizard and continue to install the driver.
2. Press the Mode button twice to change the mode to mass storage.The module will now turn up as a mass storage device on your computer. This is indicated by slow flashing blue light on the Mode button LED.
3. Locate the required “elise3.inf” driver and save it on your PC.

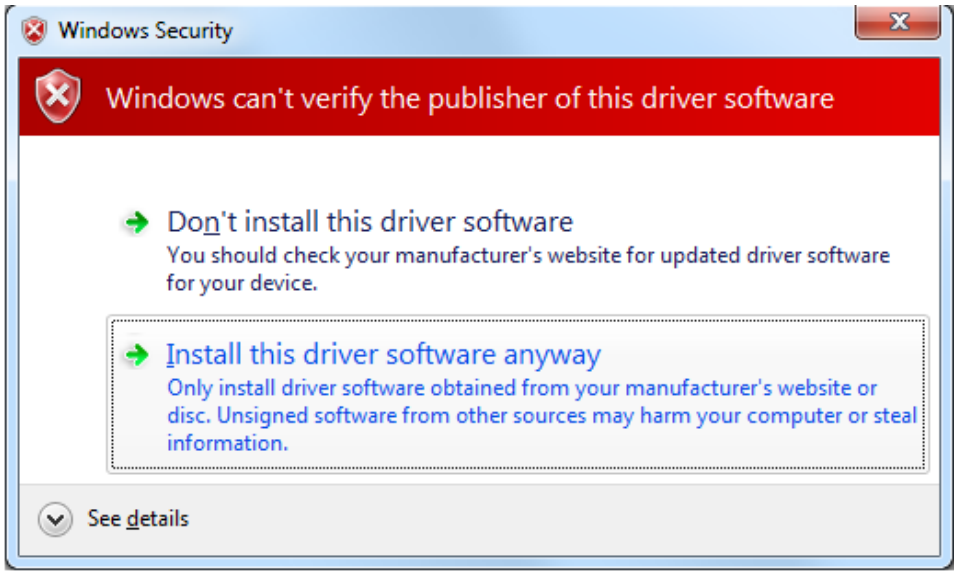


4. Press the Mode button twice again to change the mode to network access[1].
5. Select Control Panel > Hardware and Sound.
6. Select “Device Manager” under Devices and Printers.

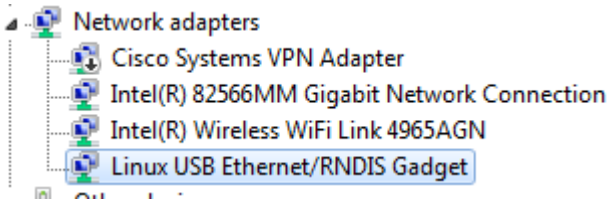


7. Right click “RNDIS/Ethernet gadget” and select “Update driver software”. A new window opens.
8. Click “Browse my computer for driver software”.
9. Browse to the folder where the port driver is saved and click “Next”. A Windows security window opens.

1. If not pressed within 10 minutes, the module will automatically change to Network access (default mode).



10. Click “Install this driver software anyway”. The installation of the port driver begins.



11. Click “Close” when the installation has finished. The port driver “Linux USB Ethernet/ RNDIS Gadget” is now installed in Control Panel > Hardware and Sound > Devices and Printers > Device manager > Network adapters.

Basic configuration

Elise 3 Server (AIWS2 Hardware) needs to be configured with basic settings. Some products settings can be set in an installation Setup Wizard accessible from the web interface. The Setup Wizard will start automatically the first time the module is accessed from the web browser and every time until the configuration is saved. Follow the wizard and fill in the required data (IP address, NTP server, license etc.). After it is saved the wizard can always be opened from the start page. Other settings are set from the application’s configuration pages and are described in the application’s Installation and Operation Manual.

For products not having a Setup Wizard, all settings are configured from the product’s Advanced Configuration page, see Setup using the Advanced configuration page on page 587.

Setup using the Setup Wizard

1. Access the module either via the network or via the management port, see Accessing the Elise 3 Server (AIWS2 Hardware) on page 580
2. Enter user name “admin” and the password “changeme”.
3. Complete the Setup Wizard (If the module’s network IP address has not been assigned by an DHCP server, it must be set manually in the wizard).
4. Select “Restart immediately” when the setup wizard has finished.The module will restart with the new configuration.

Setup using the Advanced configuration page

1. Access the module either via the network or via the management port, see Accessing the Elise 3 Server (AIWS2 Hardware) on page 580.
2. Enter user name “admin” and the password “changeme.”
3. Click “System Setup” and navigate to “Network”. Set the network parameters.Use the online help if any problems occur.
4. Click “License” and enter the license number.
5. Set the time, see Clock synchronisation and time Settings on page 588.
6. Change the default passwords for all users. If the passwords are not changed, anyone with knowledge of the default passwords can access the module and change any parameter.
7. Restart Elise 3 Server (AIWS2 Hardware) Select “Reboot” in the menu and click the “Reboot” button.
8. When the Elise 3 Server (AIWS2 Hardware) restarts, enter the URL xxx.xxx.xxx.xxx/admin in your browser (xxx.xxx.xxx.xxx is the IP address that was given to the Elise 3 Server (AIWS2 Hardware) during network setup) to see that it has started up correctly.

Changing secured settings

To be able to activate some security settings it is required that someone physically confirms the changes on the module. This is a security feature due to the remote access (LAN or VPN) ability on the Elise 3 module. An Elise 3 module is often locked in some kind of secured area that only approved users have access to (such as the server room).

When you click the “Activate” button for a secured setting, the web user interface prompts the user to confirm the secured change by pressing the Mode button on the module. The module’s Mode button LED indicates that a confirmation is needed with a quick flashing blue light.



1. Push the Mode button. The Mode button LED stops flashing and indicates that confirmation has been done with fixed yellow light on the status LED and slow flashing blue light on the mode button.



2. Click the “Activate” button to save the secured setting. The possibility to save secured settings is open for 10 minutes after the Mode button has been pressed or until the user manually exits the mode by clicking the Mode button once more.

Clock synchronisation and time Settings

The clock in different Elise 3 Server (AIWS2 Hardware)s can be set from the web browser, A-bus (i.e. Central Unit in System 900) or a time server. To be able to synchronize the clocks in different Elise 3 Server (AIWS2 Hardware)s a time server has to be used. Depending on software application and license, an Elise 3 Server (AIWS2 Hardware) can be used as time server. An external time server supporting the Network Time Protocol (NTP) can also be used. Normally the Elise 3 Server (AIWS2 Hardware) that is used as time server synchronizes with an external time server, and then all other Elise 3 Server (AIWS2 Hardware) use that Elise 3 Server (AIWS2 Hardware) as the time server.

To select time source do as follows:

1. Open the administration pages of the Elise 3 Server (AIWS2 Hardware) by entering "xxx.xxx.xxx.xxx/admin" in the address field in the web browser.
2. Click on "Settings" in the left menu.
3. Select time source; Web browser, A-bus or Time server.

Note:

Not all system’s Central Unit can provide the time.

Independent of time source the Elise 3 Server (AIWS2 Hardware) can handle different time zones and adjust the clock according to daylight saving time.

The date and time format controls the appearance of date and time in log views and application specific pages. The administration pages that are common to all Elise 2 Server (AIWS Hardware) will display date and time in the following format: YYYY-MM-DD, HH:MM:SS (for example 2000-01-31 13:30:00). This format for date and time will also be used in exported log files.

An Elise 3 Server (AIWS2 Hardware) can also set the time in connected systems, for example System 900. In this case, the Elise 3 Server (AIWS2 Hardware) will send its time to the connected system once every 24-hour period and when the time is updated.

To set the time in System 900 from the Elise 3 Server (AIWS2 Hardware) do as follows:

4. On the time settings page, enter when the Elise 3 Server (AIWS2 Hardware) should send its time to System 900 in the "Time push time" field.
5. Click "Setup System 900 time".
6. Select "Yes" in the "Set time in System 900".

Setting time in other carrier systems is done similarly. If several carrier systems are available, the time will be sent at the same time to all systems.

Time Synchronization

It can take a few seconds to synchronize the date and time during start up or if the IP address to the time server has been changed.

When the time is changed in the time server, it can take up to 30 minutes to synchronize the time, depending on how the modules are set up and how they are connected together.

Message distribution

In the administration pages, there are distribution lists that are used to distribute incoming information to other modules. If a module is to be connected to several carrier systems, for example both System 900 and a Cordless Telephone System, distribution of incoming data from the different systems has to be configured independently. The distribution of "Status Logs" and "Activity Logs" are configured separately. Advanced activity settings for activity logs are described in the *Function Description, Activity Logging in Unite,TD 92341GB.*

The addressing is described in the examples below:

Addressing a module on the System 900 A-bus

When a specific module on the A-bus is addressed, the data will be transferred directly to that module. It is however not necessary to address a specific module on the A-bus as the Central Unit in the System 900 can distribute the data to a module. Note that this requires configuration of the Central Unit.

- *No module addressing*

  127.0.0.1/S900

  The data is sent to the System 900 interface in the Elise 2 Server (AIWS Hardware), which sends the data on the A-bus without the module address defined. The Central Unit in the system has to be configured to distribute the data to a module. It is also possible to address the System 900 interface on another module by entering its IP address instead of 127.0.0.1 (localhost).

- *Module addressing*

  127.0.0.1/S900?03

The data is sent to the System 900 interface (127.0.0.1/S900) in the Elise 2 Server (AIWS Hardware) and is then sent to the module with address 03 in the system. It is also possible to address the System 900 interface on another module by entering its IP address instead of 127.0.0.1(localhost)

.Addressing another Unite compliant module on the LAN

The addressing includes the IP address that the data should be distributed to and also which service on that address that should take care of it. How a unit is addressed is described in each units documentation.

- *Addressing of another Unite compliant module*

  xxx.xxx.xxx.xxx/Service

  First the IP address of the module is defined. After the “/”, the application service that should take care of the data is specified.

Below is an example that describes how to distribute data from an Elise 2 Server (AIWS Hardware) software application to an Alarm Management Server.

- *Addressing of an Alarm Management Server*

  xxx.xxx.xxx.xxx/EventHandler

  First the Alarm Management Server IP address is defined. After the “/”, the application service EventHandler is specified.

Note:

For AMS version 3.00 and 3.10 the service cannot be used. Instead the correct port on the AMS, port number 10010, has to be used for addressing, i.e. xxx.xxx.xxx.xxx/:10010.

Maintenance information for the AIWS2

Software management -

Installation of software

Normally the installation of software is done from the application’s web interface but it can also be done in Boot Mode, see Installing software in boot mode on page 592. See also Software administration on the AIWS2 on page 507.

Creating a backup of the software settings

Normally the backup is done from the application's web interface but it can also be done in Boot Mode.

1. Put the module in Boot Mode, see Starting in boot mode on page 565.
2. Select Software > Install software.
3. Click the "Backup" button. All settings for last run software will be saved.
4. Click "Save" in the File Download window.
5. Select where to save the file and click "Save" again.

Performing a field upgrade of the boot software

By using a USB memory stick with a Boot software (autoupdate.bin), the module can be upgraded on the field.

1. Insert the USB memory stick in the upper USB connector marked.
2. Perform a controlled restart via the Restart button, by pressing the button and releasing it within 4 seconds.The Status LED indicates shutting down with quick flashing blue light. Before starting up again, the Status LED will indicate "waiting" for one minute with fixed yellow light.
3. When the Status LED indicates starting up with quick flashing blue light, press the Mode button within 3 seconds. The Mode button should indicate by showing fixed blue light .

The module now detects the memory stick and begins the upgrade process which is indicated by the Status LED with fixed yellow light . The upgrading process takes 7-8 minutes.

After the upgrade process has finished, the module will continue and start up the last used application software. The complete operation can take up to 10 minutes.

To verify a successful upgrade, you can put the USB stick back in your PC and open the file autoupdate.log. In the end of that file, you should then see the text "Upgrade finished successfully".

Note:

If the USB memory stick contains faulty Boot software, the module will start up in Boot Mode.

Resetting back to factory default settings

Resetting the module's application software back to factory default settings can be done from the application's web interface on the Configuration page under Software. Either by switching software or reinstalling software and selecting factory default settings.

Factory default settings can also be chosen from the Boot Mode's web interface when new software is installed or when returning to Normal Operation from Boot Mode, see Installing software in boot mode on page 592.

Note:

Network settings (IP address, Host name, etc.) will not be changed.

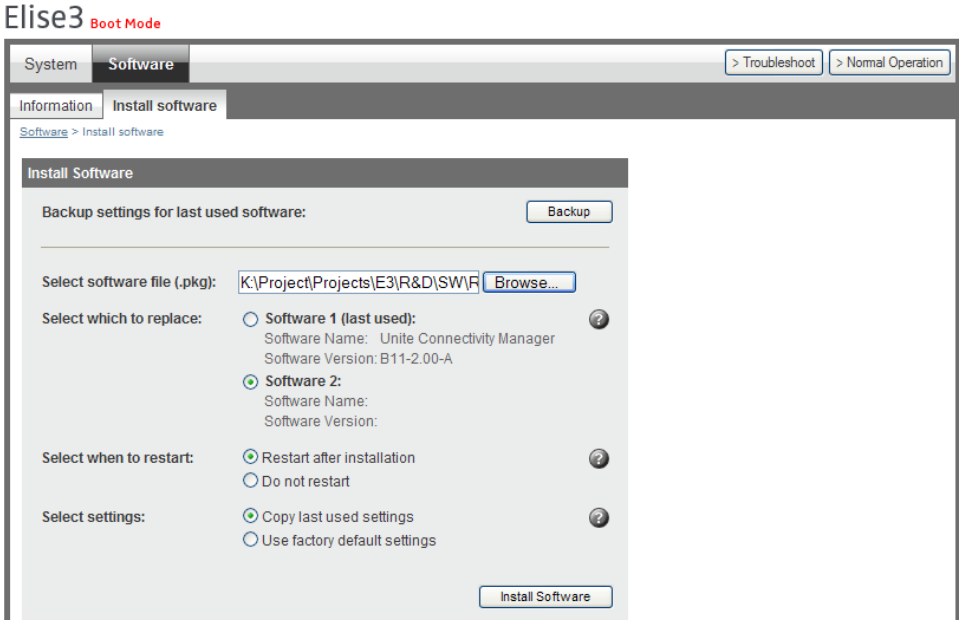
Installing software in boot mode

Installing new software is normally done from the application's web interface, refer to the application documentation. But if the application's web interface cannot be reached it is possible to put Elise 3 Server (AIWS2 Hardware) in Boot Mode, access the modules web interface and install new software from there.

Note:

It is not recommended to use the module's Management port when installing software.

Two software versions can be installed on the module. One software version is active and the other inactive in normal operation.



1. Put the module in Boot Mode, see Starting in boot mode on page 565.
2. Select Software > Install software.
3. Click the "Browse..." button and locate the software (.pkg) file to install.
4. Select where to save the software. If two versions of the software already have been installed on the module choose which software to replace.

5. Select if the module shall be restarted after the installation or not.
6. If “Restart after installation” is selected, choose if the last used settings or the factory default settings shall be applied on the new software. If you choose “Do not restart”, you can later, when returning to normal operation, choose and apply settings to software that is installed but not yet started.

Note:

If current parameters cannot be used, i.e. if software of another type has been installed, factory default parameters will always be used.

7. Click the “Install Software” button.
8. If “Do not restart” is selected a dialogue box is shown. Click “OK”.

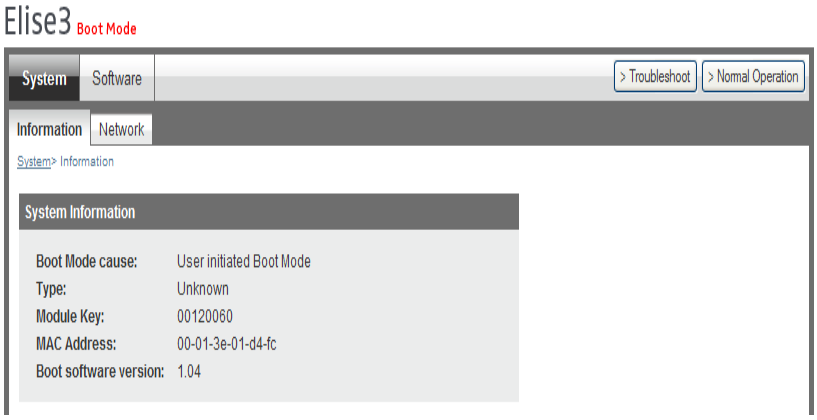
Returning to normal operation

1. Click the Normal Operation button in the Boot Mode GUI’s upper right corner. The Normal Operation dialogue box opens.
2. Select which software to start and click “OK”.
3. Select which settings to use for the software and click “OK”. The module will restart and return to normal operation.

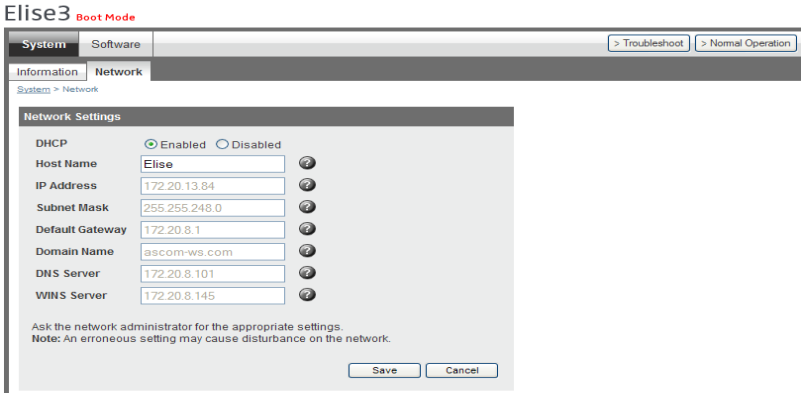
Working in boot mode

When the Elise 3 Server (AIWS2 Hardware) is started in Boot mode, you can view the system information, the network settings and the software information that helps you troubleshoot the system

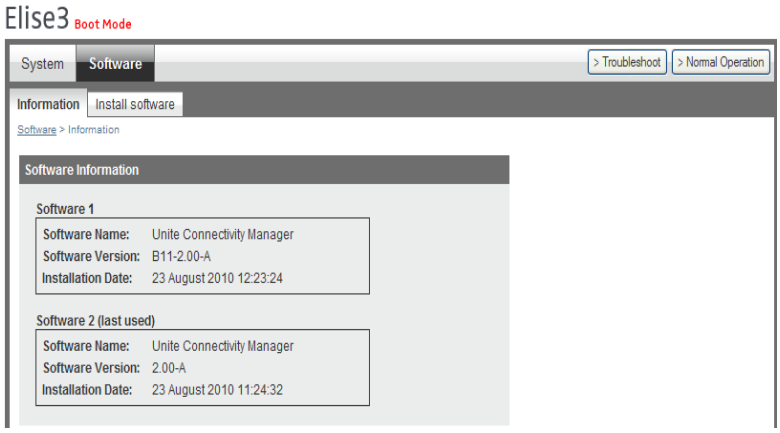
You can find the Module key number, MAC address, and Boot software version, Under System > Information in the Boot mode.



Under System > Network you can view the network settings. All network settings can be edited in this view if DHCP is disabled, but only the Host name if DHCP is enabled.



You can view the installed software name, version and installation date Under Software > Information. If two versions have been installed, information about both versions and also which version that was last used by the module is shown. The format of the installation date is dependent on the PC's language settings.



Replacing an existing Elise 2 module with Elise 3

For a hardware replacement of an Elise 2 module with an Elise 3 module follow the steps:

1. Create a backup of your configuration on the Elise 2 module.
2. Restore the backup of the configuration on the Elise 3 module.

3. Change the license key (of the Elise 2) restored on the Elise 3 with the licenses key that needs to be used for Elise 3 module. If the License type of the Elise 3 is not the same as used on Elise 2 you can move the license by exchanging the module key of the modules,

Refer Moving a license from Elise 2 Server (AIWS Hardware) to the Elise 3 Server (AIWS2 Hardware) on page 595.

Moving a license from Elise 2 Server (AIWS Hardware) to the Elise 3 Server (AIWS2 Hardware)

A license for a product on Elise 2 server can, if the license is compatible with Elise 3, be moved to the EliSE 3 by moving the Module key from the Elise 2 module to the Elise 3 module.

For example, the UniteCM and Mobile Monitoring Gateway (MMG) are compatible products.To make it easier to differ between the Module Keys, the marking “2M” is added on the label on a Module Key from Elise 3.

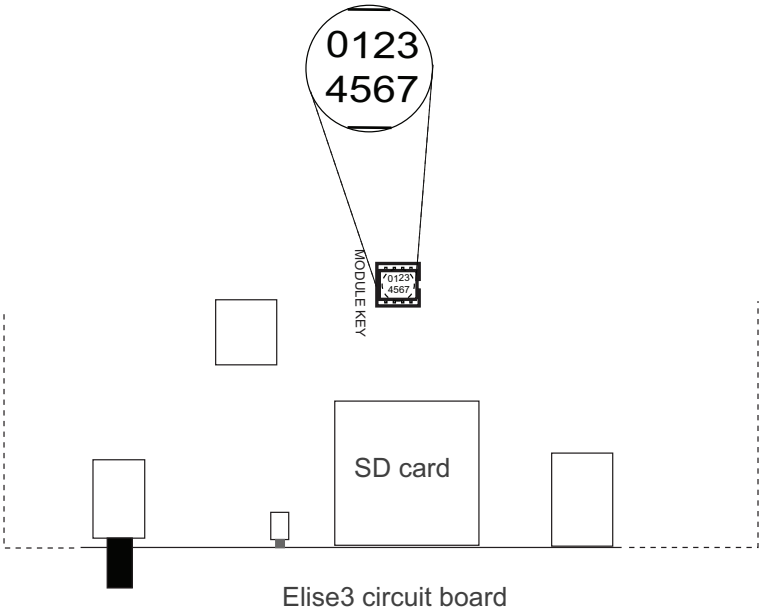
Note:

All functions will be the same as they were in Elise 2. Only one ethernet port (LAN1) can be used.

1. Create a backup of your configuration on the Elise 2 module.
2. Remove the four screws on the back side of the Elise 3 module.
3. Slide the metal cover backwards.
4. Remove the Module Key from the Elise 2 module.
5. Replace the Module Key on the Elise 3 with the one from Elise 2.

See figure below.

Figure 208: Elise 3 circuit board



6. Slide the metal cover back to the front.
7. Replace the four screws.
8. Restore the configuration.

Datasheet for the Elise 3 hardware (AIWS2)

Table 3: Physical Specifications

Dimensions (h × w × d)	44 × 220 × 199 mm
Weight	1465 g for Elise 3 Lite
Material	Sheet metal/plastic
Colour	Grey/white

Table 4: Functional Specifications

Supply voltage	100 - 240 V AC ±20% 12 - 24 V DC (-25% and +20%) (Under normal conditions a 12V battery with 10 Ah will guarantee 24 hours backup)
Current consumption	Max. 275 mA at AC input (100 - 240 V AC) Max. 1A at DC input (12V)

Table 5: Environmental Specifications

Operating temperature	0°C to +40°C
Storage temperature	-25°C to +55°C
Relative humidity	30-85% (non condensing)
Enclosure protection	IP30
Immunity to electromagnetic fields	10 V/m
Immunity to ESD	6 kV contact discharge and 8 kV air discharge

Table 6: Memory

SDRAM	256 MB
NAND flash	1 GB (for the SW application)
Serial data flash	8 MB (for booting purposes)
SD card Currently not software supported (for future use)	1 × slot for 1 GB SD card (Secure Digital non-volatile memory)

Table 7: Accessories

Standard 19” rack kit for Elise 3	Small left/right brackets for two front mounted Elise 3 and one big bracket for one front mounted Elise 3
Reverse 19” rack kit for Elise 3	Small bracket for two reverse mounted Elise 3 and one big bracket for one reverse mounted Elise 3

Table 8: Variants

FE3-AAAAAA	Elise 3 Lite, EU/EFTA
FE3-AAAAAB	Elise 3 Lite, UK, NA, AU/NZ
FE3-AAABAA	Elise 3 Standard, EU/EFTA
FE3-AAABAB	Elise 3 Standard, UK, NA, AU/NZ
FE3-AAACAA	Elise 3 NSS/LON[1], EU/EFTA
FE3-AAADAA	Elise 3 ISC/LON[2], EU/EFTA

1. Elise 3 Standard with LON piggyback
2. Elise 3 Standard with LON piggyback

Table 9: IO Input Output

Feature	Elise 3 Lite
Serial ports: 2 × RS232 (D-sub-9 male connectors), used for external interfaces ESPA, Line protocol, TAP, etc.	-
2 × modular jacks (RJ45) used for System 900 A-bus	-
1 × screw terminal used for System 900 A-bus	-
1 × screw terminal used for LON bus	-
LAN: 2 (One for future use, not yet software supported) × 10baseT or 100baseT Ethernet (Modular jack, RJ45)	Yes
USB ports 2 × USB Host port 2.0 full speed	Yes
1 × Mini-USB_B Device port 2.0 full speed	Yes
Error relay output: Configurable solid state relay – make/break operation, used for fault actions and error indications, 100 mA, 30 V DC	Yes
AUX outputs: 2 × galvanically isolated open collector outputs, 100 mA, 30 V DC	Yes
AUX inputs: 2 × digital inputs	Yes
Power supply: 1 × screw terminal for a 12-24 V DC external power supply, or 12 V DC lead battery max. 10 Ah	Yes

Technical Data

Introduction

This chapter shows you technical specifications for the following IP-DECT equipment and accessories:

- IP-DECT Base Station (IPBS1)
- IP-DECT Base Station (IPBS2)
- TDM-DECT Base Station (DB1)
- Base Station RM627 (BS330)
- Base Station RM637 (BS340)
- Avaya 3725 DECT Telephone
- Avaya 3720 DECT Telephone
- Avaya 3740 DECT Telephone
- Avaya 3745 DECT Telephone
- Avaya 3749 DECT telephone
- Advanced Charger
- Basic Charger
- Multiple Battery Charger
- Rackmount Charger
- Portable Device Manager (WinPDM)
- Avaya In-Building Wireless Server (AIWS)
- Avaya In-Building Wireless Server (AIWS2)
- Omnidirectional single antenna
- Directional dual antenna
- Directional single antenna
- Outdoor housing DECT base stations

IP-DECT Base Station (IPBS1)

Versions	
IPBS1 with internal antenna	
IPBS1 with external antenna	
DECT frequencies	
IPBS1 Standard for use with DECT in the 1880-1900 MHz frequencies	
IPBS1 LA (Latin America) for use with DECT in the 1910-1930 MHz frequencies	
IPBS1 Brazil for use with DECT in the 1910-1920 MHz frequencies	
IPBS1 US (North America) for use with DECT in the 1920-1930 MHz frequencies	
Physical	
Dimensions (l × w × d):	165 × 200 × 56 mm (including mounting bracket)
Weight:	450g
Material:	ABS moulded plastic
Color:	Beige
External connectors	2 × RJ45
Power	
Power over Ethernet IEEE 802.3af or local power supply	
Operating voltage:	21 to 56 Vdc
Power consumption:	typical 4W, maximum 5W
Network	
Ethernet:	10/100baseT
Voice over IP	
Voice over IP:	H.323 XMobile incl. H.450
Voice Encoding:	G.711 A-law / µ-law (64kbps) G.723.1 (5.3 kbps) G.729A and AB (16 kbps) G.726 (32 kbps)

Radio	
RF output power (e.r.p.), EU:	Between 23 dBm and 28 dBm (with internal antenna) Between 20 dBm and 25 dBm (with external antenna)
RF output power (e.r.p.), US:	Between 17 dBm and 21,6 dBm (with internal antenna)
Environmental	
Operating temperature:	-10°C to +55°C
Storage temperature:	-40°C to +70°C
Relative operating humidity:	15 to 90%, non condensing
Relative storage humidity:	5 to 95%, non condensing
Immunity to electromagnetic fields:	3V/m (EN61000-4-3)
Immunity to ESD:	4 kV contact discharge and 8 kV air discharge (EN61000-4-2)
Supported Handsets	3720, 3725 and 3740/3745/ 3749
Compliance to European regulations and standards	
EU directives:	1999/5/EC (R&TTE)
Radio:	EN 301406, TBR22
Safety:	EN 60950-1
EMC:	EN 301 489-6
Product marking:	CE
EC Declaration of Conformity can be found at: http://support.avaya.com/DoC	
Compliance to US and Canadian regulations and standards	
Safety:	CSA/UL 60950-1
EMC/Radio:	FCC part 15 (Class B) and RSS-213 ans ICES-003
Product marking:	FCC ID: BXZIPBS1, IC:3724B-IPBS1
Compliance to Australian regulations and standards	
Radio:	ACA TS028
Safety:	IEC 60950 3Ed
Product marking:	

IP DECT Base Station (IPBS2)

Versions	
IPBS2-C3A/1A	
IPBS2-C4A/1A e	
IPBS2-Z3A/1A	
DECT	
DECT Security	Enhanced DECT Security (ETSI TS 102 841, GAP.N.35)
	Supports NTP Protocol version 4
	Can handle 8 simultaneous calls
DECT Frequencies	
IPBS2 Standard (Europe, Africa, Middle East, Australia, New Zealand and parts of Asia) for use with DECT in the 1880-1900 MHz frequencies	
IPBS2 LA (South America) for use with DECT in the 1910-1930 MHz frequencies	
IPBS2 US (North America) for use with DECT in the 1920-1930 MHz frequencies	
IPBS2 Brazil for use with DECT in the 1910 – 1920 MHz frequencies	(Brazil is a POE only solution)
Physical	
Dimensions (l × w × d):	170 × 170 × 38 mm (including mounting bracket)
Weight:	400g
Material:	ABS moulded plastic
Color:	White (NCS S 0502-B)
External connectors	2 × MCX connectors for external antenna
Power	
Power over Ethernet IEEE 802.3af or local power supply. **Note:** Brazil is a POE only solution.	
Operating voltage:	21 to 56 Vdc

Power consumption:	typical 4W, maximum 5W
Network	
Ethernet:	10/100baseT
Voice over IP	
Voice over IP:	H.323 version 4 incl. H.225, H.235, H.245 H.450 with H.450.1, H.450.2, H.450.3, H.450.4, H.450.6, H.450.7, H.450.8 and H.450.9
Voice Encoding:	G.711 A-law / µ-law (64kbps) G.723.1 (5.3 kbps) G.729A and AB (16 kbps)
Radio	
RF output power (e.r.p.), EU:	Between 23 dBm and 28 dBm (with internal antenna)
RF output power (e.r.p.), US:	Between 17 dBm and 21.6 dBm (with internal antenna)
RF output power (e.r.p.), LA:	Between 20 dBm and 25 dBm (with internal antenna)
RF output power, Brazil:	20, 25 dBm
Environmental	
Operating temperature:	-10°C to +55°C
Storage temperature:	-25°C to +70°C
Relative operating humidity:	15 to 90%, non condensing
Relative storage humidity:	5 to 95%, non condensing
Immunity to electromagnetic fields:	10V/m (EN61000-4-3)
Immunity to ESD:	6 kV contact discharge and 8 kV air discharge (EN61000-4-2)
Supported Handsets	3720, 3725 and 3740/3745/ 3749
Compliance to European regulations and standards	
EU directives:	1999/5/EC (R&TTE), 2011/65/EU (RoHS)
Radio:	EN 301406
Safety:	EN 60950-1
EMC:	EN 301 489-6,EN 301 489-1,EN 60945
Product marking:	CE

EC Declaration of Conformity can be found at: http://support.avaya.com/DoC	
Compliance to US and Canadian regulations and standards	
Safety:	CSA/UL 60950-1
EMC/Radio:	FCC part 15 (Class B) and RSS-213 ans ICES-003
Product marking:	FCC ID: BXZIPBS2R2A, IC:3724B-IPBS2R2A
Compliance to Australian regulations and standards	
Radio:	Radiocommunications (Digital Cordless Communications Devices — DECT Devices) Standard 2007
Safety:	AS/NZS 60950-1
Product marking:	

TDM-DECT Base Station (DB1)

Versions	
DB1 with internal antenna	
DB1 with external antennas	
DECT	
DECT Security	Enhanced DECT Security (ETSI TS 102 841, GAP.N.35)
	Supports NTP Protocol version 4
	Can handle 8 simultaneous calls
DECT Frequencies	
1880-1900 MHz (Europe, Africa, Middle East, Australia, New Zealand and parts of Asia)	
1910-1930 MHz (South America)	
1920-1930 MHz (North America)	
Physical	
Dimensions (l × w × d):	170 × 170 × 38 mm (including mounting bracket)
Weight:	400g
Material:	ABS moulded plastic
Color:	White (NCS S 0502-B)
External connectors	2 × MCX connectors for external antenna
Power	
Power over Ethernet IEEE 802.3af or local power supply	
Operating voltage:	21 to 56 Vdc
Power consumption:	1.3 W to 2.0 W depending on number of slots currently in use.
Radio	
RF output power (e.r.p.), EU:	Between 23 dBm and 28 dBm (with internal antenna)
RF output power (e.r.p.), US:	Between 17 dBm and 21.6 dBm (with internal antenna)

Environmental	
Operating temperature:	-10°C to +55°C
Storage temperature:	-25°C to +70°C
Relative operating humidity:	15 to 90%, non condensing
Relative storage humidity:	5 to 95%, non condensing
Immunity to electromagnetic fields:	10V/m (EN61000-4-3)
Immunity to ESD:	6 kV contact discharge and 8 kV air discharge (EN61000-4-2)
Supported Handsets	3720, 3725 and 3740/3745/3749
Compliance to European regulations and standards	
EU directives:	1999/5/EC (R&TTE)
Radio:	EN 301406
Safety:	EN 60950-1
EMC:	EN 301 489-6,EN 301 489-1,EN 60945
Product marking:	CE
EC Declaration of Conformity can be found at: http://support.avaya.com/DoC	
Compliance to US and Canadian regulations and standards	
Safety:	AS/NZS 60950-1
EMC/Radio:	FCC part 15 (Class B) and RSS-213 ans ICES-003
Product marking:	FCC ID: BXZIPBS2, IC:3724B-IPBS2
Compliance to Australian regulations and standards	
Radio:	Radiocommunications (Digital Cordless Communications Devices — DECT Devices) Standard 2007
Safety:	AS/NZS 60950-1
Product marking:	

IP DECT Gateway (IPBL)

Salient Features	
• Connection to IP-PBX via Ethernet • Gateway between DECT and VoIP (H.323) • Connection of up to 16 TDM-DECT base stations (communication and power supply) • Synchronization between IP-DECT Base Stations and IP-DECT Gateways • Can handle 40 simultaneous calls • Supports NTP Protocol version 4 • Supports Enhanced DECT Security (ETSI TS 102 841, GAP.N.35) • Web based management • Easy to install in a standard 19” rack (height: 1u)	
Technical Specification	
Physical	
Dimensions (l × w × d):	436 × 483 × 352 mm (including mounting bracket)
Weight:	4.7 Kg
Material:	Steel
Color:	Beige
External connectors	2 × RJ45, 10BASE-T/100BASE-T Ethernet interface 2 × RJ45, Sync Ring I/O interface 2 × RJ45, Reference Sync I/O interface 16 × RJ45, ISDN UPN DECT base stations interface
Power	
Operating voltage:	110/230 VAC (100 - 240 VAC)
Power consumption:	Max 210 W (VAC) Max 250 W (VDC)
Power dissipation	Approx 15 W
Network	
Ethernet:	2 X 10/100baseT

DECT BASE STATION	Maximum distance between the IPBL and a DECT Base Station is 1500 m.
Supported DECT base station:	BS330-9131 BS330-9134 BS340-9131
Voice	
Voice over IP:	H.323 version 4 incl. H.225, H.235, H.245 H.450 with H.450.1, H.450.2, H.450.3, H.450.4, H.450.6, H.450.7, H.450.8 and H.450.9
Voice Encoding:	G.711 A-law / µ-law (64kbps) G.723.1 (5.3 kbps) G.729A and AB (8 kbps) G.726 (32 kbps)
Environmental	
Operating temperature:	0°C to +55°C
Storage temperature:	-40°C to +85°C
Relative operating humidity:	15 to 90%, non condensing
Relative storage humidity:	5 to 95%, non condensing
Immunity to electromagnetic fields:	10V/m (EN61000-4-3)
Immunity to ESD:	6 kV contact discharge and 8 kV air discharge (EN61000-4-2)
Compliance to European regulations and standards	
EU directives:	1999/5/EC (R&TTE)
Safety:	EN 60950-1
EMC:	EN 301489-1,EN 301 489-6,
Product marking:	CE
EC Declaration of Conformity can be found at: http://support.avaya.com/DoC	
Compliance to US and Canadian regulations and standards	
Safety:	CSA/UL 60950-1
EMC	FCC part 15 (Class B) and ICES-003
Product marking:	FCC ID:XXXXXXXX, IC:XXXXXXXXXXX

Compliance to Australian regulations and standards	
Safety:	IEC-60950-1
Product marking:	

Base Station RM627 (BS330)

Physical	
Dimension:	200 (w) x 165 (d) x 56 (h) mm
Weight:	470 g
Material:	ABS moulded plastic
Color:	light gray
Connectors:	two RJ45 connectors for Upn/power, one RJ12 connector for factory testing purposes.
Environmental	
Operating temperature:	-10°C to +55°C
Storage temperature:[1]	-40°C to +70°C
Relative operating humidity:	15 to 90%, non condensing
Relative storage humidity:	5 to 95%, non condensing
Enclosure protection:	IP20, IEC EN60529
Power	Locally, or centrally via 2 data pairs (UTP) and 1 optional pair
Operating voltage:	21 to 56 Vdc
Power consumption:	Between 1.3 W and 2.0 W (depending on the number of calls active)
RF output power (e.r.p.):	between 23 dBm and 28 dBm (depends on direction due to internal antenna characteristics)
Receiver sensitivity:	at least -86 dBm at B.E.R. = 10-3
Compliance to European regulations and standards	
CE regulation:	1999/5/EEC, Radio & Telecommunications Terminal Equipment (R&TTE) Directive and 2009/125/EC/(ErP).
Conformity marking:	CE
DECT standard:	EN 301 406:2001 (DECT) EN 300 444:2001 (TBR22 GAP)
Safety standard:	EN 60950-1:2006+A11:2009 and EN 60945
EMC standard:	EN301489- 6:2002

Base Station RM637 (BS340)

Physical	
Dimension:	200 (w) x 165 (d) x 56 (h) mm
Weight:	496 grams (incl. Standard external antennas)
Material:	ABS moulded plastic
Color:	light grey
Connectors:	two RJ45 connectors for Upn/power, one RJ12 connector for factory testing purposes.
Size standard antenna:	107 (l) x 8.5 (d) mm
Antenna connectors (Base Station):	MCX SMT type female receptacle from Amphenol (KJMCX625100-002-3GT30G-50; gold plated)
Antenna connectors (Antenna):	MCX straight crimp male plug from Amphenol (919-101P-51S1X; gold plated
Material:	ABS moulded plastic
Environmental	
Operating temperature:	-10°C to +55°C
Storage temperature:[1]	-40°C to +70°C
Relative operating humidity:	15 to 90%, non condensing
Relative storage humidity:	5 to 95%, non condensing
Enclosure protection:	IP20, IEC EN60529
Functional	
Operating voltage:	21 to 56 Vdc
Power consumption:	between 1.2 W and 2.0 W (depending on the number of calls active)
RF output power (e.r.p.):	between 20 dBm and 25 dBm (depends on direction due to external antenna characteristics)
Receiver sensitivity:	at least -86 dBm at B.E.R. = 10-3

Compliance to regulations and standards	
CE regulation:	1999/5/EC, Radio & Telecommunications Terminal Equipment (R&TTE) Directive 89/336/EC Electromagnetic Compatibility Directive (EMC) 73/23/EC Low Voltage Directive (LVD).
Conformity marking:	CE
DECT standard:	EN 301 406:2001 (DECT) EN 300 444:2001 (TBR22 GAP)
Safety standard:	EN60950-1:2001
EMC standard:	EN301489- 6:2002
Accessories	
Directional single antenna Directional dual antenna Omnidirectional single antenna Outdoor housing	

Avaya 3725 DECT Telephone

Physical	
Dimensions (l × w × d):	134 × 53 × 26 mm
Weight:	130 g (battery and clip included)
Material:	Case: PC/ABS, Key pad: PC, Clip: PPA
Color:	Grey
Display (w × h):	28 x 35 mm, CSTN display
Clip:	Hinge-type (standard) or swivel type
Battery	
Type:	Li-polymer
Speech time:	20 h under optimal conditions 13 h with Bluetooth headset in use under optimal conditions
Stand-by time:	120 h[1] under optimal conditions
Charge time:	< 4 hours
Discharge/charge cycles:	>=80% capacity left after 400 full charge/discharge cycles.
[1] The stand-by time is without activated screensaver	
Connectors	
Multi-purpose connector:	For battery charging, software download, and configuration
Headset connector:	Standard 2.5 mm
User interface	
Display (w × h):	Multiple colors with high resolution, more than 65k individual colors. 128 × 160 pixel LCD with white LED back-light
Indicator:	LED on top/front for visual indication of incoming call, message. The LED may also be used for visual indication of normal function.
Vibrator:	Incoming call/message

Keypad:	• Soft keys (3) • Hook off • On hook and Power On/Off (Symbol) on the same key • Five way navigation key (“OK” in the centre of key) • Numerical keys • Volume up/down • Multifunction button
Audio	
Ring signal:	Adjustable in 8 steps
Earpiece:	Adjustable in 8 steps of 3dB each
Maximum sound ring signal level:	88 dBA @ 10 cm
Loudspeaker:	Duplex loud speaking function
Settings	
Languages:	19 (Czech, Danish, Dutch, English, Finnish, French, German, Greek, Hungarian, Italian, Norwegian, Polish, Portuguese (Brazilian), Portuguese, Russian, Slovakian, Spanish, Swedish, and Turkish) and one downloadable language.
Security	Enhanced DECT security (SRTP encryption) GAP/CAP compliant DECT handset
Central Phonebook	
Maximum name and number length:	40 characters in a name and 20 digits in a number
Company Phonebook	
Maximum name and number length:	24 characters in a name and 24 digits in a number (1 number per name).
Entries:	1000
Local Phonebook	
Storage of contacts:	• 250 contacts • 48 character name • 24 digit work number • 24 digit mobile phone number • 24 digit other number • A selectable ring tone
Telephony	

Indication:	14 ring signals, flashing LED and vibrator.
Answer call:	Button press or auto answer
Call list storage capacity:	25 received, dialled and missed calls with time stamp
Messaging	
Maximum message length:	140 characters from handset. Message length to handset is system dependent.
Storage capacity:	30 received/sent messages (> 20 000 characters)
Character Encoding	SMS Standard Latin-1
Radio	
Receiver sensitivity:	-93 dBm
Automatic DECT protocol detection:	Automatic detection and configuration for US DECT and EU DECT at first registration.
Frequency range: • EU: • US: • LA: • BR:	 1880-1900 MHz 1920-1930 MHz 1910-1930 MHz 1910-1920 MHz
Modulation:	GFSK
Channel spacing:	1.728 MHz
Antenna:	Integral
Sensitivity:	-93 dBm
Radiated power:	EU: 250 mW US: 100 mW
Environmental	
Operating temperature:	0°C to +40°C
Storage temperature:[2]	-20°C to +60°C
Enclosure protection:	IP44, IEC EN60529
Immunity to electromagnetic fields:	3V/m EN61000-4-3
Immunity to ESD:	4 kV contact discharge and 8 kV air discharge (EN61000-4-2)

Free fall test, standard product:	IEC 60068-2-32, procedure 1, dropped 12 times from 1 metre. Avaya approves 12 drops from 1.5 metre.
Option	
Bluetooth radio: Radio spectrum:	add-on from factory ISM 2.4000-2.4835 MHz
Accessories	
• Leather case • Swivel type clip • Security chain • Basic charger • Advanced Charger • Multiple Battery Charger • Rackmount Charger • Avaya In-Building Wireless Server (AIWS) • Portable Device Manager (WinPDM)	• Verified Bluetooth Headset Nokia BH-804 Nokia BH-904 Plantronics Explorer 240/390/395 Plantronics Voyager 835/PRO/PRO+ Plantronics Voyager PRO Plantronics Discovery 925 Plantronics M20/M25/M50/M55/M1100 Plantronics Marque 2 Backseat GO Jabra BT530 Jabra GO 660/6430/6470 Jabra Supreme SonyEricsson HBH-GV435 SonyEricsson HBH-PV740 Peltor M2RX7-WS4
[2] Note that storing Li-Ion batteries at high temperature dramatically reduces its capacity. For example storage around maximum temperature reduces capacity with 20% in less than a month, permanently.	
Compliance to European regulations and standards	
EU directives:	1999/5/EC (R&TTE) & 2011/65/EU/ROHS
Product marking:	For models production date until March 2010: CE QD ID: B014317 For models since production date April 2010: CE QD ID: B016451
Radio:	EN 301 406, TBR22
Bluetooth:	EN 300 328-2, EN 301489-17
SAR (Specific Absorption Rate):	EN50360 and EN62209-1, 0.074 W/kg (10 gram)
Safety:	EN60950-1
EMC:	EN301489- 6, EN 301 489-1

Compliance to US regulations and standards	
Product marking:	FCC ID: BXZDH4BL For models production date until March 2010: QD ID: B014317 For models since production date April 2010: QD ID: B016451 US: 9FVW4NANDH4 HAC
SAR (Specific Absorption Rate):	FCC/OET Bulletin 65 Supplement C and IEEE Std. 1528 / ANSI/IEEE Std. C95.1 Normal operation 0.104 W/kg (1 gram) Body worn operation 0.029 W/kg (1 gram)
Safety:	UL 60950-1
EMC/Radio:	FCC Part 15 D, and FCC Part 15 C (Bluetooth)
Hearing Aid:	47 CFR Part 68, Subpart D and TIA-968-A
Compliance to Canadian regulations and standards	
Product marking:	IC:3724B-DH4BL For models production date until March 2010: QD ID: B014317 For models since production date April 2010: QD ID: B016451
EMC/Radio:	RSS-213 and RSS-210 (Bluetooth), ICES-03
SAR (Specific Absorption Rate):	IEEE Std C95.3 Normal operation 0.104 W/kg (1 gram) Body worn operation 0.029 W/kg (1 gram)
Safety:	CSA 60950-1
Hearing aid:	CS-03
Compliance to Australian regulations and standards	
Product marking:	For models production date until March 2010: QD ID: B014317 For models since production date April 2010: QD ID: B016451
Radio:	EN301406

Bluetooth:	EN 300 328-2, EN 301489-17, AUS/NZS-4771
SAR (Specific Absorption Rate):	EN 50360 and EN62209-1, 0.074 W/kg (10 gram)
Safety:	AUS/NZS 60950-1
EMC:	EN301489- 6, EN 301 489-1
DECT:	AS/ACIF 5004, TS028

Avaya 3720 DECT Telephone

Physical	
Dimension (l × w × d):	133 × 53 × 24 mm
Weight:	115 g (battery and clip included)
Material:	Case: PC/ABS, Key pad: Silicone, Clip: PC
Color:	Grey
Display (w × h):	28 x 35 mm, FSTN B/W
Clip:	Hinge type (standard) or swivel type
Battery and charging	
Type:	600 mAh (Li-Ion)
Speech time:	16 h during optimal condition
Stand-by time:	180 h during optimal condition
Charge time:	< 4 h
Discharge/charge cycles:	≥ 65% capacity left after 500 full charge/discharge cycles.
Connectors	
Multi-purpose connector:	For battery charging, software download, and configuration
Headset connector:	Standard 2.5 mm
User interface	
Display (w × h):	112 x 115 pixels, with white LED back-light.
Indicator:	LED on top/front for visual indication of incoming call. The LED may also be used for visual indication of normal function.
Vibrator:	Incoming call
Keypad:	• Soft keys • Hook off • On hook and Power On/Off on the same key • Four way navigation key • Numerical keys
Audio	

Ring signal:	Adjustable in 8 steps
Earpiece:	Adjustable in 8 steps of 3dB each
Maximum sound pressure level:	88 dBA @ 10 cm
Loudspeaker:	Duplex loud speaking function
Settings	
Languages:	4 (English, French, German, Spanish) and 1 downloadable language
Security	Enhanced DECT security
Central Phonebook	
Maximum name and number length:	40 characters in a name and 20 digits in a number
Company Phonebook	
Maximum name and number length:	24 characters in a name and 24 digits in a number (1 number per name).
Entries:	1000
Local Phonebook	
Storage of contacts:	• 250 contacts • 48 character name • 24 digit work number • 24 digit mobile phone number • 24 digit other numbers
Telephony	
Indication:	14 ring signals, flashing LED and vibrator.
Answer call options:	Button press or auto answer
Call list storage capacity:	25 received, dialled and missed calls with time stamp
Radio	
Automatic DECT protocol detection:	Automatic detection and configuration for US DECT and EU DECT at first registration.

Frequency range: • EU: • US: • LA: • BR	 1880-1900 MHz 1920-1930 MHz 1910-1930 MHz 1910-1920 MHz
Modulation:	GFSK
Channel spacing:	1.728 MHz
Antenna:	Integral
Sensitivity:	-93 dBm
Radiated power:	EU: 250 mW US: 100 mW
Environmental	
Operating temperature:	0°C to +40°C
Storage temperature:[1]	-20°C to +60°C
Enclosure protection:	IP40, IEC EN60529
Immunity to electromagnetic fields:	3 V/m EN61000-4-3
Immunity to ESD:	4 kV contact discharge and 8 kV air discharge (EN61000-4-2)
Free fall test, standard product:	IEC 60068-2-32, procedure 1, dropped 12 times from 1 metre.
Accessories	
• Leather case • Hinge type clip • Basic charger • Advanced Charger • Rackmount Charger • Telephone lanyard • Avaya In-Building Wireless Server (AIWS) • Portable Device Manager (WinPDM)	
[1] Note that storing Li-Ion batteries at high temperature dramatically reduces its capacity. For example storage around maximum temperature reduces capacity with 20% in less than a month, permanently.	
Compliance to European regulations and standards	

EU directives:	1999/5/EC (R&TTE)
Product marking:	CE
DECT Radio:	EN 301 406, TBR22
SAR (Specific Absorption Rate):	EN50360 and EN62209-1, 0.075 W/kg (10 gram)
Safety:	EN60950-1
EMC:	EN301489- 6, EN 301 489-1
Compliance to US regulations and standards	
Product marking:	FCC ID: BXZDH3 US: 9FVW4NANDH3 HAC
SAR (Specific Absorption Rate):	FCC/OET Bulletin 65 Supplement C and IEEE Std. 1528 / ANSI/IEEE Std. C95.1 Normal operation 0.043 W/kg (1 gram) Body worn operation 0.037 W/kg (1 gram)
Safety:	UL 60950-1
EMC/Radio:	FCC Part 15 D
Hearing aid:	47 CFR Part 68, Subpart D and TIA-968-A
Compliance to Canadian regulations and standards	
Product marking:	IC:3724B-DH3
SAR (Specific Absorption Rate):	IEEE Std C95.3 Normal operation 0.043 W/kg (1 gram) Body worn operation 0.037 W/kg (1 gram)
Safety:	CSA 60950-1
EMC/Radio:	RSS 213, ICES-03
Hearing aid:	CS-03
Compliance to Australian regulations and standards	
Product marking:	
Radio:	EN301 406
SAR (Specific Absorption Rate):	EN50360 and EN62209-1, 0.075 W/kg (10 gram)

Safety:	AS/NZS 60950
EMC:	EN301 489-1 and EN301 489-6
DECT:	AS/ACIF S004

Avaya 3740 DECT Telephone

Physical	
Dimensions (l × w × d):	142 × 56 × 25 mm
Weight:	170 g (battery and clip included)
Material:	Case: PC/ABS, Key pad: PC, Clip: PA
Color:	Telephone: Grey
Display (w × h):	28 x 35 mm, FSTN B/W
Clip:	Hinge-type (standard) or swivel-type
Battery	
Type:	Li-Ion
Speech time:	18 h
Stand-by time:	150 h without activated screensaver
Charge time:	< 2 hours - 10% charged; 3 hours - fully charged.
Discharge/charge cycles:	>=80% capacity left after 400 full charge/discharge cycles.
Connectors	
Multi-purpose connector:	For battery charging, software download, connection of headset, and configuration.
User interface	
Display (w × h):	128 × 160 pixel LCD with white LED backlighting.
Indicator:	LED on top for visual indication of incoming call/ message. The LED may also be used for visual indication of normal function.

Vibrator:	Incoming call/message
Buttons/Keypad:	- Soft keys (3) - Hook off key - On-hook and Power On/Off on the same key - Four-way navigation key - Numerical keys - Volume up/down buttons - Sound off key/Mute button - Multifunction button
Audio	
Ring signal:	Adjustable in 8 steps
Earpiece:	Adjustable in 8 steps
Maximum sound ring signal level:	100 dBspl @ 10 cm
Loudspeaker:	Duplex loud speaking function
Settings	
Languages:	19 languages. "Ceština" (Czech), "Dansk" (Danish), "Deutsch" (German), "Ελληνικά" (Greek), "English", "Español" (Spanish), "Français" (French), "Italiano" (Italian), "Magyar", "Nederlands" (Dutch), "Norsk" (Norwegian), "Polski" (Polish), "Português" (Brazilian Portuguese), "Português" (Portuguese), "Русский"(Russian), "Slovencina" (Slovakian), "Soumi" (Finish), "Svenska" (Swedish), "Türkçe" (Turkish), and one downloadable language.
Security	Enhanced DECT Security (SRTP encryption)
Central Phonebook	
Maximum name and number length:	40 characters in a name and 20 digits in a number
Company Phonebook	
Maximum name and number length:	24 characters in a name and 24 digits in a number (1 number per name).
Entries:	1000

Local Phonebook	
Storage of contacts:	- 250 contacts - 48 character name - 24 digit work number - 24 digit mobile phone number - 24 digit other number - A selectable ring tone
Telephony	
Indication:	14 ring signals, flashing LED and vibrator
Answer call:	Button press or auto answer
Call list storage capacity:	25 calls (received, dialled and missed) with time stamp
Messaging	
Maximum message length:	140 characters from handset. Message length to handset is system dependent.
Storage capacity:	30 received/sent messages (> 20 000 characters)
Message Encoding	SMS Standard Latin -1
Radio	
Receiver sensitivity:	-93 dBm
Automatic DECT protocol detection:	Automatic detection and configuration for US DECT and EU DECT at first registration.
Frequency range: EU: US: LA: BR:	 1880-1900 MHz 1920-1930 MHz 1910-1930 MHz 1910-1920 MHz
Modulation:	GFSK
Channel spacing:	1.728 MHz
Antenna:	Integral
Radiated power:	EU: 250 mW US: 100 mW LA: 250 mW BR: 250 mW

Dynamic output power	EU/LA/BR: 10 mW (maximum averaga power) US: 4 mW (maximum average power)
Environmental	
Operating temperature:	-10°C to +55°C
Storage temperature:	-20°C to +60°C
Enclosure protection:	IP65, IEC EN60529
Immunity to electromagnetic fields:	3V/m EN61000-4-3
Immunity to ESD:	8 kV contact discharge and 16 kV air discharge (EN61000-4-2)
Accelerated Life Testing	
Climate stress	Telephone exposed for quick temperature changes (-40° C to 75° C) 25 times. Telephone dwelt on each temperature during 40 minutes.
Drop test	Telephone dropped 30 times from 1,2 metres
Vibration test	Telephone exposed for vibrations during 2,5 hours
Chemical stress	Telephone exposed for Oleic Acid
Keypad actuation test	Keys pressed 15 000 times with a force of 13N
Squeeze test	Telephone squeezed 1 000 times with a force of 130N.
Free fall test, standard product	IEC 60068-2-32, procedure 1, dropped 12 times, specification extended to 2 metres. IEC 68-2-32, procedure 2, dropped 1 000 times from 0,5 metre.
Chemical resistance test	3% Hydrochloric Acid M-alcohol (85% methylated ethanol) 60% Chlorhexidin 0.5mg/ml
Keypad Abrasion test	20 NB 0500-B
Accessories	
Leather case Hinge-type/Swivel-type clip Desktop charger, Basic Desktop charger, Advanced Separate battery pack charger Charging rack	Avaya In-Building Wireless Server (AIWS) Portable Device Manager (WinPDM) Headset with microphone on boom[1] Headset adapter for Mic on boom Peltor hearing protection headset Headset adapter for standard Peltor headset (ATEX classified)

Compliance to European regulations and standards	
EU directives:	2006/95/EC(LVD), 2004/108/EC(EMC), 1999/5/EC (R&TTE) & 2011/65/EU/RoHS
Product marking:	CE 
Radio:	EN 301 406, TBR22
SAR (Specific Absorption Rate):	EN50360 and EN62209-1, 0.137 W/kg (10 gram)
Safety:	EN60950-1
EMC:	EN301489- 6, EN 301 489-1
Compliance to Australian regulations and standards	
Product marking:	
Radio:	EN301406
SAR (Specific Absorption Rate):	EN 50360 and EN62209-1, 0.137 W/kg (10 gram)
Safety:	AUS/NZS 60950-1
EMC:	EN301489- 6, EN 301 489-1
DECT:	AS/ACIF S004
Compliance to US regulations and standards	
Product marking:	FCC ID: BXZDH5 US: 9FVW4NANDH5 HAC
SAR (Specific Absorption Rate):	FCC/OET Bulletin 65 Supplement C and IEEE Std. 1528 / ANSI/IEEE Std. C95.1 Normal operation 0.008 W/kg (1 gram) Body worn operation 0.011 W/kg (1 gram)
Safety:	UL 60950-1
EMC/Radio:	FCC Part 15 D
Hearing Aid:	47 CFR Part 68, Subpart D and TIA-968-A
Compliance to Canadian regulations and standards	
Product marking:	IC: 3724B-DH5
EMC/Radio:	RSS-213 and ICES-003

SAR (Specific Absorption Rate):	IEEE Std C95.3 Normal operation 0.008 W/kg (1 gram) Body worn operation 0.011 W/kg (1 gram)
Safety:	CSA 60950-1
Hearing aid:	CS-03

1. Requires the headset adapter for Mic on boom, that is ordered separately.

Avaya 3745 DECT Telephone

Physical	
Dimensions (l × w × d):	142 x 56 x 25 mm
Weight:	175 g (battery and clip included)
Material:	Case: PC/ABS, Key pad: PC, Clip:PA
Color:	Grey
Display (w x h):	28 x 35 mm, CSTN display
Clip:	Hinge-type (standard) or swivel type
Battery	
Type:	Li-Ion
Speech time:	10 h with Bluetooth headset in use 12 h without Bluetooth enabled
Stand-by time:	90 h with black screen saver activated
Charge time:	2 hours - 90% charged; 3 hours - fully charged.
Discharge/charge cycles:	>=80% capacity left after 400 full charge/discharge cycles.
Connectors	
Multi-purpose connector:	For battery charging, software download, connection of headset, and configuration.
User interface	
Display (w × h):	Multiple colors with high resolution, 65k individual colors. 128 × 160 pixel LCD with white LED backlight
Indicator:	LED on top for visual indication of incoming call or message. The LED may also be used for visual indication of normal function.

Keypad/Buttons:	- Soft keys (3) - Off-hook key - On-hook and Power On/Off (Symbol) on the same key - Four way navigation key - Numerical keys - Volume up/down buttons - Alarm button - Sound off key/Mute button
Audio	
Ring signal:	Adjustable in 8 steps
Earpiece:	Adjustable in 8 steps
Maximum sound pressure level:	90 dBspl @ 10 cm
Loudspeaker:	Duplex loud speaking function
Settings	
Languages:	19 languages. "Ceština" (Czech), "Dansk" (Danish), "Deutsch" (German), "Ελληνικά" (Greek), "English", "Español" (Spanish), "Français" (French), "Italiano" (Italian), "Magyar", "Nederlands" (Dutch), "Norsk" (Norwegian), "Polski" (Polish), "Português" (Brazilian Portuguese), "Português" (Portuguese), "Русский"(Russian), "Slovencina" (Slovakian), "Soumi" (Finish), "Svenska" (Swedish), and "Türkçe" (Turkish).
Central Phonebook	
Maximum name and number length:	40 characters in a name and 20 digits in a number
Company Phonebook	
Maximum name and number length:	24 characters in a name and 24 digits in a number (1 number per name).
Entries:	1000

Local Phonebook	
Storage of contacts:	- 250 contacts - 48 character name - 24 digit work number - 24 digit mobile phone number - 24 digit other number - A selectable ring tone per contact
Telephony	
Indication:	14 ring signals, flashing LED and vibrator.
Answer call:	Key/button press, or auto answer
Call list storage capacity:	25 received, dialled and missed calls with time stamp
Messaging	
Message length:	Up to 140 characters from handset, depending on language and system settings
Storage capacity:	30 received/sent messages (totally max. 20 000 characters)
Message character encoding:	SMS Standard Latin-1
Radio	
Receiver sensitivity:	-93 dBm
Frequency range:	
EU: US: LA: BR:	1880-1900 MHz 1920-1930 MHz 1910-1920 MHz 1910-1920 MHz
Modulation:	GFSK
Channel spacing:	1.728 MHz
Antenna:	Integral
Dynamic output power:	EU/LA: 10 mW (maximum average power) BR: 120mW US: 4 mW (maximum average power)
Bluetooth radio:	Radio spectrum: ISM 2.4000-2.4835 MHz
Environmental	
Operating temperature:	-10°C to +40°C
Storage temperature[1]:	-20°C to +60°C

Enclosure protection:	IP65, IEC EN60529
Immunity to electromagnetic fields:	3V/m EN61000-4-3
Immunity to ESD:	8 kV contact discharge and 16 kV air discharge (EN61000-4-2)

1. Note that storing Li-Ion batteries at high temperature dramatically reduces its capacity. For example, storage around maximum temperature reduces the capacity with 20% in less than a month, permanently.

Accelerated Life Testing

Climate stress	Handset exposed for quick temperature changes (-40° C to 75° C) 25 times. Handset dwelt on each temperature during 40 minutes.
Drop test	Handset dropped 30 times from 1,2 metres
Vibration test	Handset exposed for vibrations during 2,5 hours
Chemical stress	Handset exposed for Oleic Acid
Keypad actuation test	Keys pressed 15 000 times with a force of 13N
Squeeze test	Handset squeezed 1 000 times with a force of 130N.

Other Tests

Free fall test	IEC 68-2-32, procedure 1, dropped 12 times from 1 meter, specification extended to 2 meters.
Chemical Resistance Test	3% Hydrochloric Acid M-alcohol (85% methylated ethanol) 60% Chlorhexidin 0.5mg/ml
Keypad Abrasion Test	20 NB 0500-B

Accessories

- Hinge-type/Swivel-type clip
- Desktop charger, Basic
- Desktop charger, Advanced
- Charging Rack
- Battery pack opener

Verified Bluetooth Headsets

- 3M Peltor WS XP
- Jabra EVOLVE 65
- Jabra MOTION
- Jabra STEALTH
- Jabra SUPREME
- Plantronics BlackBeat GO 2
- Plantronics Blackwire 710
- Plantronics M70
- Plantronics M90
- Plantronics ML20
- Plantronics Voyager Edge
- Plantronics Voyager Legend

Compliance to European regulations and standards

EU directives:	2006/95/EC(LVD), 2004/108/EC(EMC), 1999/5/EC (R&TTE) and 2011/65/EU (RoHS)
Product marking:	CE BT QD: B016451
Radio:	EN 301 406, TBR22
Bluetooth:	EN 300 328-2, EN 301489-17
SAR (Specific Absorption Rate):	EN 50360 and EN 62209-1, 0.137 W/kg (10 gram)
EMC:	EN 301489- 6, EN 301 489-1
Safety:	EN60950-1

Compliance to US Regulations and Standards

Product marking:	FCC ID: BXZDH5BL, BT QD: B016451 US: 9FVW4NANDH5 HAC
SAR (Specific Absorption Rate):	FCC/OET Bulletin 65 Supplement C and IEEE Std. 1528 / ANSI/IEEE Std. C95.1 Normal operation 0.013 W/kg (1 gram) Body worn operation 0.016 W/kg (1 gram)
Safety:	UL 60950-1
EMC/Radio:	FCC Part 15 D, and FCC Part 15 C (Bluetooth)
Hearing Aid:	47 CFR Part 68, Subpart D and TIA-968-A

Compliance to Canadian regulations and standards

Product marking:	IC: 3724B-DH5BL, BT QD: B016451
EMC/Radio:	RSS-213 and RSS-210 (Bluetooth), ICES-003
SAR (Specific Absorption Rate):	IEEE Std C95.3 Normal operation 0.013 W/kg (1 gram) Body worn operation 0.016 W/kg (1 gram)
Safety:	CSA 60950-1
Hearing aid:	CS-03

Compliance to Australian regulations and standards

Product marking:	BT QD: B016451
Radio:	EN301406
Bluetooth:	EN 300 328-2, EN 301489-17, AUS/NZS-4771
Safety:	AUS/NZ 60950-1
EMC:	EN301489- 6, EN 301 489-1
SAR (Specific Absorption Rate):	EN 50360 and EN 62209-1, 0.137 W/kg (10 gram)
DECT:	AS/ACIF S004

Avaya 3749 DECT Telephone

Physical	
Dimensions (l × w × d):	142 x 56 x 25 mm
Weight:	175 g (battery and clip included)
Material:	Case: PC/ABS, Key pad: PC, Clip:PA
Color:	Grey
Display (w x h):	28 x 35 mm, CSTN display
Clip:	Hinge-type (standard) or swivel type
Battery	
Type:	Li-Ion
Speech time:	10 h with Bluetooth headset in use 12 h without Bluetooth enabled
Stand-by time:	90 h with black screen saver activated
Charge time:	2 hours - 90% charged; 3 hours - fully charged.
Discharge/charge cycles:	>=80% capacity left after 400 full charge/discharge cycles.
Connectors	
Multi-purpose connector:	For battery charging, software download, connection of headset, and configuration.
User interface	
Display (w × h):	Multiple colors with high resolution, 65k individual colors. 128 × 160 pixel LCD with white LED backlight
Indicator:	LED on top for visual indication of incoming call or message. The LED may also be used for visual indication of normal function.
Vibrator:	Incoming call/message

Keypad/Buttons:	- Soft keys (3) - Off-hook key - On-hook and Power On/Off (Symbol) on the same key - Four way navigation key - Numerical keys - Volume up/down buttons - Alarm button - Sound off key/Mute button
Audio	
Ring signal:	Adjustable in 8 steps
Earpiece:	Adjustable in 8 steps
Maximum sound pressure level:	90 dBspl @ 10 cm
Loudspeaker:	Duplex loud speaking function
Settings	
Languages:	19 languages. "Ceština" (Czech), "Dansk" (Danish), "Deutsch" (German), "Ελληνικά" (Greek), "English", "Español" (Spanish), "Français" (French), "Italiano" (Italian), "Magyar", "Nederlands" (Dutch), "Norsk" (Norwegian), "Polski" (Polish), "Português" (Brazilian Portuguese), "Português" (Portuguese), "Русский"(Russian), "Slovencina" (Slovakian), "Soumi" (Finish), "Svenska" (Swedish), "Türkçe" (Turkish), and one downloadable language.
Security	Enhanced DECT security (SRTP encryption)
Central Phonebook	
Maximum name and number length:	40 characters in a name and 20 digits in a number
Company Phonebook	
Maximum name and number length:	24 characters in a name and 24 digits in a number (1 number per name).
Entries:	1000
Local Phonebook	

Storage of contacts:	- 250 contacts - 48 character name - 24 digit work number - 24 digit mobile phone number - 24 digit other number - A selectable ringtone per contact
Telephony	
Indication:	14 ring signals, flashing LED and vibrator.
Answer call:	Key/button press, or auto answer
Call list storage capacity:	25 received, dialled and missed calls with time stamp
Messaging	
Message length:	160 characters from telephone. Message length to telephone is system dependent.
Storage capacity:	30 received and sent messages (totally max. 20 000 characters)
Character Encoding	SMS Standard Latin-1
Radio	
Receiver sensitivity:	-93 dBm
Frequency range: EU: US: LA: BR:	 1880-1900 MHz 1920-1930 MHz 1910-1930 MHz 1910-1920 MHz
Modulation:	GFSK
Channel spacing:	1.728 MHz
Antenna:	Integral
Dynamic Output power:	EU/LA/BR: 10 mW (maximum average power) US: 4 mW (maximum average power)
Bluetooth radio:	Radio spectrum: ISM 2.4000-2.4835 MHz
Environmental	
Operating temperature:	-10°C to +40°C

Storage temperature[1]:	-20°C to +60°C
Enclosure protection:	IP65[2], IEC EN60529
Immunity to electromagnetic fields:	3V/m EN61000-4-3
Immunity to ESD:	8 kV contact discharge and 16 kV air discharge (EN61000-4-2)
Accelerated Life Testing	
Climate stress	Handset exposed for quick temperature changes (-40 °C to 75 °C) 25 times. Handset dwelt on each temperature during 40 minutes.
Drop test	Handset dropped 30 times from 1,2 metres
Vibration test	Handset exposed for vibrations during 2,5 hours
Chemical stress	Handset exposed for Oleic Acid
Keypad actuation test	Keys pressed 15 000 times with a force of 13N
Squeeze test	Handset squeezed 1000 times with a force of 130N.
Free fall test, ATEX/IECEx product	IEC 68-2-32, procedure 1, dropped 12 times from 1 metre, specification extended to 2 metres.
Accessories[3]	
Hinge-type/Swivel-type clip Desktop charger, Basic Desktop charger, Advanced Battery pack opener Charging Rack	ATEX/IECEx-classified headset adaptor for standard Peltor headset and ATEX/IECEx-classified Peltor headset.
Verified Bluetooth Headsets[3]	
Nokia BH-201/804/904 SonyEricsson HBH-GV435 SonyEricsson HBH-PV740 Jabra BT530 Jabra GO 660/6430/6470 Jabra Supreme	Plantronics Voyager 510/520/835/PRO/PRO+ Plantronics Discovery 925/975 Plantronics Explorer 240/390/395 Plantronics M20/M25/M50/M55/M1100 Plantronics Marque 2 Backseat GO Peltor M2RX7-WS4

1. Note that storing Li-Ion batteries at high temperature dramatically reduces its capacity. For example, storage around maximum temperature reduces the capacity with 20% in less than a month, permanently.

2. Sira has tested the enclosure to IP64. IPX5 marking is based on Avaya tests and is not validated by Sira.

3. In hazardous areas; it is only permitted to use EX classified accessories/Bluetooth headsets.

Intrinsically safe classification	
CE 0470 Ex SIRA 10ATEX2072 IECEx SIR 10.0038 II 2G, II 2D Ex ib IIC T4 Gb Ex ib IIIC T55°C Db IP65, Tamb = -10 °C to +40°C	
НАНИО ЦСВЭ РОСС SE.ГБ05.В03353 Ex ib IIC T4 Gb X IP65 Ex ib IIIC T55°C Db XIP65 -10°C = Ta = +40 °C	
SP C US 2011 2368858 I.S. for Class I, Zone 1,IP64 AEx ib IIC T4 Tamb= -10° C to +40° C	
Compliance to European regulations and standards	
EU directives:	1999/5/EC (R&TTE) and 94/9/EC (ATEX)
Product marking:	CE WEEE Ex BT QD: B016451
Radio:	EN 301 406, TBR22
Bluetooth:	EN 300 328-2, EN 301489-17
SAR (Specific Absorption Rate):	EN50360 and EN62209-1, 0.137 W/kg (10 gram)
EMC:	EN301489- 6, EN 301 489-1
ATEX:	EN 60079-0:2004, EN 60079-11, and EN 61241-11
Compliance to International regulations and standards	
IECEx Scheme:	IEC 60079-0, IEC 60079-11, IEC 61241- 11
EC Type Examination Certificate, IECEx Certificate of Conformity, EC Declaration of Conformity and following supplements can be found at http://support.avaya.com/DoC	

Compliance to Russian regulations and standards	
Product Marking	SP C US BT QD: B016451

Telecom/Radio	Corresponds to "Rules for the use of terminal equipment connected to the two-wire analogue interface of the general purpose telephone communication network", supplemented by Russian Ministry of Infocommunications regulation of 29.08.2005 in No. 102 (registered by Russian Ministry of Justice 02.09.2005, registration no. 6982).
Bluetooth	EN 300 328-2, EN 301489-17
Safety	GOST R IEC 60950-1:2005
Sanatory	MSanPin 001-96 "Sanitary norms of permissible levels for physical factors during use of domestic articles"; GN (Hygienic Norms) 2.1.6.1338-03 "Maximum Allowable Concentrations (MACs) of Pollutants in the Air of Residential Settings", SanPin 2.1.8/2.2.4/ 1190-03 "Hygiene requirements on the installation and implementation of terrestrial mobile radio communication systems".
EMC:	EN301489- 6, EN 301 489-1
SAR:(Specific Absorption Rate):	EN50360 and EN62209-1, 0.0.15 W/kg (10 gram)
EX:	GOST R IEC 60079 -0:2007, GOST R 52350.11-2005 (IEC 60079-11:2006), GOST R IEC 61241-11:2009
Non Incendive use[1,2]	
2011 2368858 IP 64 Non-Incendive for Class I, Div 2, Groups A, B, C, D, T4 Tamb= -10° C to +40° C	
Compliance to Australian regulations and standards	
Product marking:	BT QD: B016451
Radio:	According to EN 301406
Bluetooth:	EN 300 328-2, EN 301489-17, AUS/NZS-4771
Safety:	AUS/NZS 60950-1
EMC:	EN301489- 6, EN 301 489-1
SAR (Specific Absorption Rate):	EN 50360 and EN 62209-1, 0.137 W/kg (10 gram)
DECT:	AS/ACIF S004

1. Disclaimer: Explosive atmosphere; The approvals are valid exclusively for surface industry. Avaya explosion protected telephone 3749 shall therefore not be used in mining (underground) location. Avaya does not support or take responsibility for any change in the product or its designation.
2. Battery charging or replacement of battery is NOT permitted in hazardous area.

Advanced Charger for 3720 and 3725 DECT Telephones

Physical	
Dimensions (l × w × h):	130 × 98 × 55 mm
Weight:	160 g (excl. power adapter)
Material:	Case: PC/ABS Rubber feet
Color:	Charcoal grey
Functional	
Supply voltage:	100 - 240 V, 50 - 60 Hz AC (adapter), 5 V DC (charger)
Charge current:	0.65 A
Interfaces	
USB:	USB specification 2.0 full speed
Ethernet:	Support data transfer rates up to 100Mbps (IEEE802.3 standard)
Environmental	
Operating temperature:	+5°C to +40°C
Storage temperature:	-20°C to +65°C
Enclosure protection:	IP30, IEC EN60529
Immunity to electromagnetic fields:	3 V/m EN61000-4-3
Immunity to ESD:	4 kV contact discharge and 8 kV air discharge (EN61000-4-2)
Compliance to European regulations and standards	
EU directives:	2004/108/EC(EMC)
Product marking:	CE

Safety:	EN60950-1
EMC:	EN 55022 (class B), EN61000-4-3
Compliance to US regulations and standards	
Product marking:	
Safety:	UL 60950-1
EMC:	FCC CFR 47 Part 15
Compliance to Canadian regulations and standards	
Product marking:	
Safety:	CSA 60950-1
EMC:	FCC CFR 47 Part 15
Compliance to Australian regulations and standards	
Product marking:	
Safety:	IEC 60950-1
EMC:	EN 55022 (class B), EN61000-4-3

Advanced Charger for 3740, 3745, and 3749 Telephones

Physical	
Dimensions (l × w × h):	134 x 95 x 58 mm
Weight:	160 g (excl. power adapter)
Material:	Case: PC/ABS Rubber feet
Color:	Dark grey
Functional	
Supply voltage:	100 - 240 V, 50 - 60 Hz AC (adapter), 5 V DC (charger)
Charge current:	0.65 A
Interfaces	
USB:	USB specification 2.0 full speed
Ethernet:	Support data transfer rates up to 100Mbps (IEEE802.3 standard)
Environmental	
Operating temperature:	+5°C to +40°C
Storage temperature:	-20°C to +65°C
Enclosure protection:	IP30, IEC EN60529
Immunity to electromagnetic fields:	3 V/m EN61000-4-3
Immunity to ESD:	4 kV contact discharge and 8 kV air discharge (EN61000-4-2)
Compliance to European regulations and standards	
EU directives:	2004/108/EC(EMC)
Product marking:	CE
Safety:	EN60950-1
EMC:	EN 55022 (class B), EN61000-4-3
Compliance to US regulations and standards	
Product marking:	c SP us

Safety:	UL 60950-1
EMC:	FCC CFR 47 Part 15
Compliance to Canadian regulations and standards	
Product marking:	
Safety:	CSA 60950-1
EMC:	FCC CFR 47 Part 15
Compliance to Australian regulations and standards	
Product marking:	
Safety:	IEC 60950-1
EMC:	EN 55022 (class B), EN61000-4-3

Basic Charger for 3720 and 3725 DECT Telephones

Physical	
Dimensions (l × w × h):	95 × 95 × 55 mm
Weight:	170 g (excl. power adapter)
Material:	Case: PC/ABS Rubber feet
Color:	Charcoal grey
Functional	
Supply voltage:	100 - 240 V, 50 - 60 Hz AC (adapter), 5 V DC (charger)
Charge current:	0.65 A
Environmental	
Operating temperature:	+5°C to +40°C
Storage temperature:	-20°C to +65°C
Enclosure protection:	IP30, IEC EN60529
Immunity to electromagnetic fields:	3 V/m EN61000-4-3
Immunity to ESD:	4 kV contact discharge and 8 kV air discharge (EN61000-4-2)
Compliance to European regulations and standards	
EU directives:	2004/108/EC(EMC)
Product marking:	CE
Safety:	EN60950-1
EMC:	EN 55022 (class B), EN61000-4-3
Compliance to US regulations and standards	
Product marking:	c SP us
Safety:	UL 60950-1
EMC:	FCC CFR 47 Part 15
Compliance to Canadian regulations and standards	
Product marking:	c SP us

Safety:	CSA 60950-1
EMC:	FCC CFR 47 Part 15
Compliance to Australian regulations and standards	
Product marking:	
Safety:	IEC 60950-1
EMC:	EN 55022 (class B), EN61000-4-3

Basic Charger for 3740, 3745, and 3749 Telephones

Physical	
Dimensions (l × w × h):	108 x 95 x 58 mm
Weight:	181 g (excl. power adapter)
Material:	Case: PC/ABS Rubber feet
Color:	Dark grey
Functional	
Supply voltage:	100 - 240 V, 50 - 60 Hz AC (adapter), 5 V DC (charger)
Charge current:	0.65 A
Environmental	
Operating temperature:	+5°C to +40°C
Storage temperature:	-20°C to +65°C
Enclosure protection:	IP30, IEC EN 60529
Immunity to electromagnetic fields:	3 V/m EN 61000-4-3
Immunity to ESD:	4 kV contact discharge and 8 kV air discharge (EN 61000-4-2)
Compliance to European regulations and standards	
EU directives:	2004/108/EC(EMC)
Product marking:	CE
Safety:	EN 60950-1
EMC:	EN 55022 (class B), EN 61000-4-3
Compliance to US regulations and standards	
Product marking:	c SP us
Safety:	UL 60950-1
EMC:	FCC CFR 47 Part 15
Compliance to Canadian regulations and standards	

Product marking:	
Safety:	CSA 60950-1
EMC:	FCC CFR 47 Part 15
Compliance to Australian regulations and standards	
Product marking:	
Safety:	IEC 60950-1
EMC:	EN 55022 (class B), EN61000-4-3

Multiple Battery Charger

Physical	
Dimensions (l × w × h):	453 × 156 × 98 mm
Weight:	1,4 kg
Material:	Case: PC/ABS
Color:	Light grey
Functional	
Supply voltage:	100 - 240 VAC/0,7 A, 50/60 Hz
Charge current:	0.65 A
Environmental	
Operating temperature:	+5°C to +40°C
Storage temperature:	-20°C to +65°C
Enclosure protection:	IP30, IEC EN60529
Immunity to electromagnetic fields:	3 V/m EN61000-4-3
Immunity to ESD:	4 kV contact discharge and 8 kV air discharge (EN61000-4-2)
Recommended cables	
(not supplied by Avaya)	Power cord with IEC C13 connector
Compliance to European regulations and standards	
EU directives:	2004/108/EC(EMC)
Product marking:	CE
Safety:	EN60950-1
EMC:	EN 55022 (class B), EN61000-4-3
Compliance to US regulations and standards	
Product marking:	c SP us

Safety:	UL 60950-1
EMC:	FCC CFR 47 Part 15
Compliance to Canadian regulations and standards	
Product marking:	
Safety:	CSA 60950-1
EMC:	FCC CFR 47 Part 15
Compliance to Australian regulations and standards	
Product marking:	
Safety:	IEC 60950-1
EMC:	EN 55022 (class B), EN61000-4-3

Rackmount Charger

There are two kinds of Rackmount charger, one for the Avaya 3720/3725 DECT telephones and another for the Avaya 3740/3749 DECT Telephones. Both chargers are with the same hardware and housing but with a slightly different holder for the different handset types.

Physical	
Dimensions (l × w × h):	453 × 156 × 98 mm
Weight:	1,6 kg
Material:	Case: PC/ABS
Color:	Light grey
Functional	
Supply voltage:	100 - 240 VAC/0,7 A, 50/60 Hz
Charge current:	0.65 A
Interfaces	
Ethernet:	Support data transfer rates up to 100 Mbps (IEEE 802.3y standard)
USB:	USB specification 2.0 full speed
Recommended cables	
(not supplied by Avaya)	Power cord with IEC C13 connector
Environmental	
Operating temperature:	+5°C to +40°C
Storage temperature:	-20°C to +65°C
Enclosure protection:	IP30, IEC EN60529
Immunity to electromagnetic fields:	3 V/m EN61000-4-3
Immunity to ESD:	4 kV contact discharge and 8 kV air discharge (EN 301 489-6, EN61000-4-2)
Compliance to European regulations and standards	
EU directives:	R&TTE - 1999/5/EC and ErP 2009/125/EC
Product marking:	CE

Safety:	EN60950-1
EMC:	EN 55022 (class B), EN 301 489-6
Compliance to US regulations and standards	
Product marking:	
Safety:	UL 60950-1
EMC:	FCC CFR 47 Part 15
Compliance to Canadian regulations and standards	
Product marking:	
Safety:	CSA 60950-1
EMC:	FCC CFR 47 Part 15
Compliance to Australian regulations and standards	
Product marking:	
Safety:	IEC 60950-1
EMC:	EN 55022 (class B), EN 301 489-6
Compliance to Russia regulations and standards	
Product marking	
Safety	GOST R IEC 60950-1

Portable Device Manager (WinPDM)

PC Requirements	
Portable Device Manager (WinPDM) Installation and operation:	• Windows 7® Professional (32-bit/64-bit) • Windows 7® Enterprise (32-bit/64-bit), or • Windows 7® Ultimate (32-bit/64-bit) • Sun Java Runtime Environment (JRE) 7 or 8 **Note:** Windows 7 (64-bit) requires both JRE 32-bit and JRE 64-bit.
Available hard disk space:	200 MB (recommended)
Language	
Installation GUI	English only
Operational GUI:	English as standard, additional languages can be added.
Accessories	
Advanced Desktop Charger, DC4	Used for programming 372x and 374x. Requires USB port.
Rack Charger, CR3	Used for programming 372x and 374x. Requires USB port.

Avaya In-Building Wireless Server (AIWS)

Hardware Requirements	
Elise 2 Server (AIWS Hardware) / 64 MB RAM / 1 GB FLASH	
PC Requirements	
Installation and administration:	Microsoft Internet Explorer 6.0™ or later Sun Java Runtime Environment (JRE) 6 or later.
Screen resolution:	1024 x 768 pixels
Languages	
Installation GUI:	English only
Operational GUI:	English as standard, translations can be added
Items	
WSM-MVB	AIWS Basic, including Elise 2 Server (AIWS Hardware), power supply and licence
WSM-MVC	AIWS Basic+, including Elise 2 Server (AIWS Hardware), power supply and licence
WSM-MVS	AIWS Standard, including Elise 2 Server (AIWS Hardware), power supply and licence
WSM-MVP	AIWS OAP, including Elise 2 Server (AIWS Hardware), power supply and licence
WSM-MVE	AIWS Enterprise Management, including Elise 2 Server (AIWS Hardware), power supply and licence
Included accessories	
Power Supply	AC cord for EU, UK, US, Australia
Build-inCentral Phonebook	
Number of entries:	500 (editable) or 2000 (view only), csv format import and export
External Central Phonebook	
Supported protocols:	LDAP

Supported LDAP servers:	Active Directory® in Windows 2000 Server Active Directory® in Windows Server 2003 Cisco Call Manager 4.2
Time Synchronisation	
Time server ability:	Yes
Automatic daylight saving adjustment:	Yes
Date and time format:	Adjustable to commonly used formats
Time sources:	NTP server (NTPv4 compatible with NTPv2 and NTPv3) Other Unite module with time server ability Manual setting
Messaging	
IP-DECT	Max capacity: 4 000 messages / hour
Supported special characters:	Swedish, Norwegian, Danish, Finnish and German language
Supported Telephone Systems	
DECT	IP-DECT

Variants

You can combine AIWS Basic+, Standard, OAP and Enterprise Management in the same system. However, you can configure only one of them to have connection to the IP-DECT system. The others must be configured to connect through this AIWS.

Avaya AIWS Basic	
Build-in Central Phonebook	
SMS Handset to Handset	
Basic Web Messaging	
Telephone configuration via Advanced Charger or Rackmount Charger or OTA [1] => max 32 devices	
This licence cannot be used in a multi AIWS configuration.	
Avaya AIWS Basic+[2]	
Build-in Central Phonebook	
SMS Handset to Handset	
Basic Web Messaging	
Software download via Advanced Charger or Rackmount Charger or OTA => max 32 devices	
Telephone configuration via Advanced Charger or Rackmount Charger or OTA => max 32 devices	
Avaya AIWS Standard[3]	
Build-in Central Phonebook	
Access to Corporate LDAP Directories for phonebook enquiries	
SMS Handset to Handset	
Advanced Web Messaging	
Max. No. of predefined messages:	30 common messages, max. 20 kB in total 30 local messages, max. 4 kB in total[4]
Software download via Advanced Charger or Rackmount Charger or OTA	Max. 120 devices

Telephone configuration via Advanced Charger or Rackmount Charger or OTA	Max. 120 devices
Avaya AIWS OAP[3]	
Build-in Central Phonebook	
SMS Handset to Handset	
Basic Web Messaging	
Messaging protocols	OAP
Avaya AIWS Enterprise Management[3]	
Build-in Central Phonebook	
SMS Handset to Handset	
Basic Web Messaging	
Software download via Advanced Charger or Rackmount Charger or OTA	Max. 1 000 devices
Telephone configuration via Advanced Charger or Rackmount Charger or OTA	Max. 1 000 devices

1. only with AIWS SW release above 2.32
2. multi AIWS configuration supported (same as in Avaya AIWS Standard)
3. AIWS Standard, OAP and Enterprise Management can be combined in the same system
4. Cookies have to be enabled.

Avaya In-Building Wireless Server 2 (AIWS2 hardware)

Hardware Requirement	
Elise3 Server	For information on Elise 3 server hardware, refer Installing the Elise 3 Server (AIWS2 Hardware) on page 570 and Datasheet for the Elise 3 hardware (AIWS2) on page 597.
Technical Specifications	
Physical	
Dimensions (h × w × d)	44 × 220 × 199 mm

Weight:	1465 g
Material:	Sheet metal/plastic
Color:	Gray/Black
Functional:	
Supply voltage	100 - 240 V AC ±20% 12 - 24 V DC (-25% and +20%) (Under normal conditions a 12V battery with 10 Ah will guarantee 24 hours backup)
Current consumption:	Max 275 mA at 100 Vac input Max 1 A at 12 Vdc input Max 500 mA at 24 Vdc input
Environmental:	
Operating temperature:	0°C to +40°C
Storage temperature:	-25°C to +55°C
Relative humidity:	30-85% (non condensing)
Enclosure protection:	IP30
Immunity to electromagnetic fields:	10 V/m
Memory:	
SDRAM:	256 MB
NAND flash:	1 GB (for the SW application)
Serial data flash:	8 MB (for booting purposes)
SD-card:	Not used
Connections	
LAN:	2 (One is not used) × 10baseT or 100baseT Ethernet (Modular jack, RJ45)
USB:	2 × USB Host port 2.0 full speed 1 × Mini-USB_B Device port 2.0 full speed
Error relay output:	Solid state relay used for error indications, 100 mA, 30 V DC
AUX outputs:	Not used
PC Requirements	
Installation and administration:	Windows Internet Explorer® 8.0 through 9 Mozilla Firefox® 3.6 through 12 Sun™ Java™ Runtime Environment (JRE) 7 or 8

User interface (GUI) modification	Any HTML or text editor
Client browser	Windows® Internet Explorer® 8.0 or later Mozilla Firefox® 3.6 or later Java applets have to be enabled for messaging status and Device Management
Screen resolution	Minimum 1024 x 768 pixels
Language	
Installation GUI	English only
Operational GUI	English as standard, customized localization can be added Storage Capacity on FTP area
Storage Capacity on FTP area	
FTP area	150 MB Default 50 MB but can be set in the interval from 5 MB up to 150 MB
Items	
FE3-EACAAC[1]	AIWS2 Basic including hardware and license with Central Phonebook, SMS Handset to Handset, Basic Web Messaging, and Handset configuration for maximum 32 handsets.
FE3-EBCAAC[1]	AIWS2 Basic+ including hardware and license with Central Phonebook, SMS Handset to Handset, Basic Web Messaging, and Centralized device management for maximum 32 devices. Expandable with additional FE3-EBCAAC or with FE3-ECCAAC, FE3-EDCAAC and FE3-EECAAC
FE3-ECCAAC[1]	AIWS2 Standard including hardware and license with Central Phonebook, SMS Handset to Handset, Advanced Web Messaging, Group Handler, and Centralized device management for maximum 120 devices. Expandable with additional FE3-EBCAAC or with FE3-ECCAAC, FE3-EDCAAC and FE3-EECAAC
FE3-EDCAAC[1]	AIWS2 OAP including hardware and license with. Central Phonebook, SMS Handset to Handset, Basic Web Messaging, and OAP Messaging protocol. Expandable with additional FE3-EBCAAC or with FE3-ECCAAC, FE3-EDCAAC and FE3-EECAAC

FE3-EECAAC[1]	AIWS2 Enterprise including hardware and license with Central Phonebook, SMS Handset to Handset, Basic Web Messaging, Group Handler, and Centralized device management for maximum 1 000 devices. Expandable with additional FE3-EBCAAC or with FE3-ECCAAC, FE3-EDCAAC and FE3-EECAAC
For Argentina	
FE3-EACAAD[2]	AIWS2 Basic including hardware and license, for details see FE3-EACAAC.
FE3-ECCAAD[2]	AIWS2 Standard including hardware and license, for details see FE3-ECCAAC.
1. Includes Elise3 Lite, Getting Started leaflet and Safety Instructions, brackets for wall mounting and power cord for EU, UK, USA and Australia 2. Includes Elise3 Lite, Getting Started leaflet and Safety Instructions, brackets for wall mounting and power cord for Argentina	
Accessories (not included)	
DECT AIWS2 FRONT MNTNG KIT 660324	Mounting kit for 19¨, front mounting, single mounting or two modules side-by-side.
DECT AIWS2 REVERSE MNTNG KIT 660325	Mounting kit for 19¨, reverse mounting, single mounting or two modules side-by-side.
Secure Digital Memory card	All Industrial Grade 1 GB capacity or greater are supported. Used to store configuration/data of the Unite module with redundancy activated.
Central Phonebook	
Build in phonebook	500 (editable) or 2000 (view only), csv format import and export. Import from only IP Office is supported through TFTP.
Phonebook source	Internal database External database via LDAPv3 connection (Requires AIWS2 Standard or AIWS2 Enterprise)
External phonebook	LDAP protocol
Supported LDAP servers	Active Directory® in Windows 2000 Server Active Directory® in Windows Server 2003
Time Synchronisation	
Time server ability	Yes, can act as NTP server

Automatic daylight saving adjustment	Yes
Date and time format	Adjustable to commonly used formats
Time sources	NTP server, Local clock
Messaging	
IP-DECT system	Max. 12000 messages / hour
Supported special characters	Swedish, Norwegian, Danish, Finnish, and German language
Supported character encoding	SMS standard Latin -1
Web Message Tool functionality	Sending one-way messages to single handsets
Group Capacity	
Max. No. of groups:	30 with up to 15 users and 1 with up to 50 users
Advanced Web Messaging	
Common groups	30 common groups with 50 call numbers each, max. 60 kB in total.
Common messages	30 messages, max. 20 kB in total
My groups	Only accessible from the users own PC. Requires cookies to be enabled. Approx. 10 groups per user
Fault Handling	
Fault logging	Centralized system fault log with the latest 1000 entries
Activity Logging	
Exported log data format	Text messages to Syslog Server
Carrier System Interface	
Supported IP-DECT system	IP-DECT R4 connected via Ethernet
Open Access Protocol (OAP) includes	Messaging to handsets and alarm from handsets
Supported OAP protocol:	OAP version 3 OAP version 4

Includes:	• One-way messaging • Manual Acknowledge • Interactive Messaging • User Data • Alarm • Availability (OAP version 4 only) • Location (OAP version 4 only) • Poll Location (OAP version 4 only) • Device Property (OAP version 4 only) • Call Setup (OAP version 4 only) • Status log (OAP version 4 only)
Devices	
Max. No. of devices	Depends on license. Both handsets and network connected chargers are counted in the maximum number of devices for centralized management. Centralized device management can be configured to only handle selected device types.
IP-DECT R4	Device management “over the air”
Other DECT systems support	Via network connected desktop chargers or charging rack
Features	• Overview of all devices • Configuration of handsets • Configuration of chargers (connected via network) • Software application for managing devices such as handsets, chargers, and fixed IP DECT devices • Push to talk (PTT) • Web access • Templates for common settings for several or all devices • Software upgrade (can be scheduled to specific date and time). • Backup of individual settings, including contact list • Download of company phonebook and contact list to handset • Download of language file to handset (for additional handset languages) • Simultaneous handling of multiple devices

Variants

You can combine AIWS Basic+, Standard, OAP and Enterprise Management in the same system. However, you can configure only one of them to have connection to the IP-DECT system. The others must be configured to connect through this AIWS.

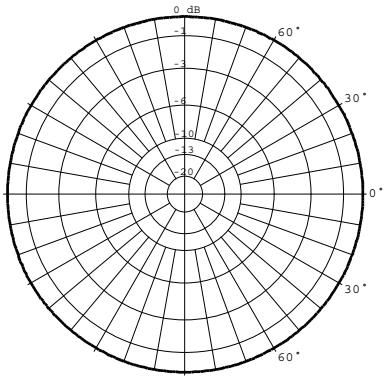
AIWS2 Basic	
	Built-in Central Phonebook Directory SMS Handset to Handset, Basic Web Messaging Handset configuration for maximum 32 handsets All AIWS2 variants except AIWS2 Basic can be combined in the same system. However only one can be configured to have connection to the IP-DECT system. AIWS2 Basic is not expandable.
AIWS2 Basic+	
	Built-in Central Phonebook Directory SMS Handset to Handset Basic Web Messaging Centralized device management for maximum 32 devices.
AIWS2 Standard	
	Built-in Central Phonebook Directory External Central Phonebook Directory SMS Handset to Handset Advanced Web Messaging Centralized device management for maximum 120 devices
AIWS2 OAP	

	Built-in Central Phonebook SMS Handset to Handset Basic Web Messaging OAP Messaging protocol
AIWS2 Enterprise	
	Built-in Central Phonebook Directory SMS Handset to Handset Basic Web Messaging Centralized device management for maximum 1000 devices.

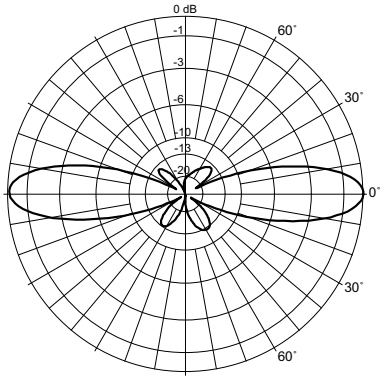
Omnidirectional single antenna

General	
Manufacturer:	MAT Equipment
Product code manufacturer:	MA430X14
Physical	
Height:	375 mm (above wall mounting bracket
Weight:	≈ 0.2 kg (excl. pole mounting bracked of 70 grams)
Mounting stand-off:	71 mm (wall to back of antenna)
Weight	≈ 0.82 kg
Material/color:	shroud: glass fiber, greyupper cap: plastic, black base: plastic, blackwall bracket: glass fiber, greypole mounting clamp: stainless steel
Environmental	
Operating temperature:	-33 to +55 °C:
Functional Specs	
Frequency	range 1880 to 1920 MHz
Nominal impedance:	50 ohms
VSWR:	≤ 1.7
Polarization:	linear, vertical
Gain (at connector level):	4.8 dBi ± 0.3 dBi
Radiation in horizontal plane:	omnidirectional within ± 0.3 dB
Radiation in vertical plane:	beam width (E-plane) at -3 dB: ≈ 24°
Maximum power:	10 watts
Connector:	MCX male connector at the end of a 1 m
	RG316 coaxial cable (minimum bending radius: 20 mm)

Radiation pattern



Typical radiation in horizontal plane

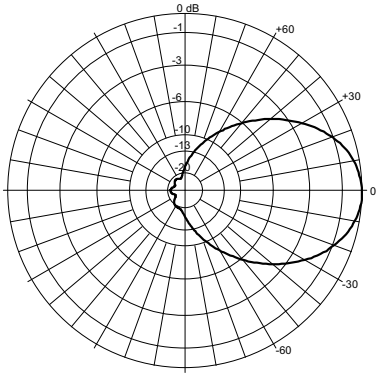


Typical radiation in vertical plane

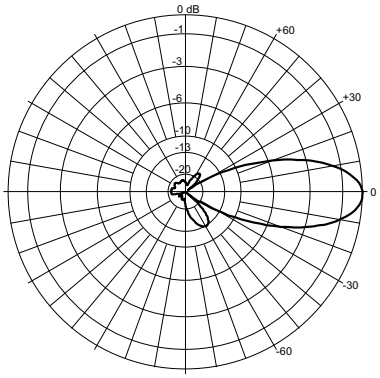
Directional dual antenna

General	
Manufacturer:	Huber+Suhner
Product code manufacturer:	SPA 1900/85/8/0/DS
Physical	
Size:	101(h) × 95(w) × 32(d) mm
Weight:	0.11 kg
Material/color:	housing: ASA and aluminium,
	light grey RAL 7035
	radome: ASA, dark grey RAL7042
Environmental	
Operating and storage temperature:	-40 to +80 °C
Functional Specs	
Frequency range:	1850 to 1990 MHz
Nominal impedance:	50 ohms
VSWR:	1.5
Polarization:	dual linear, ± 45° slant
Gain:	8 dBi
Radiation in horizontal plane:	beam width (H-plane) at -3 dB: 85°
Radiation in vertical plane:	beam width (E-plane) at -3 dB: 75°
Down tilt:	0°
Front to back ratio:	12 dB
Isolation between ports:	30 dB
Maximum power:	75 watts (CW) at 25 °C
Connector:	MCX male connector at the end of a 1 m
	ENVIROFLEX 316D coaxial cable

Radiation pattern



Typical radiation in horizontal plane



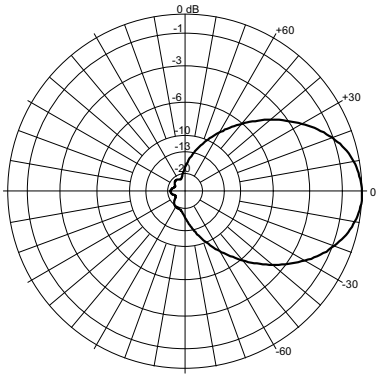
Typical radiation in vertical plane

Directional single antenna

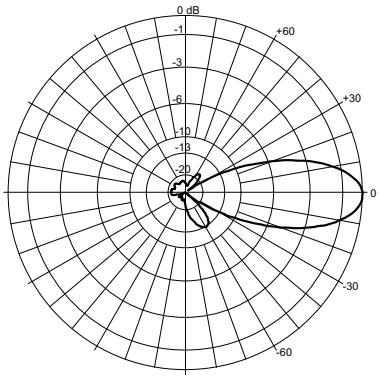
General	
Manufacturer:	MAT Equipment
Product code manufacturer:	MA420X44
Physical	
Size (h × w × th):	270(w) × 140(h) × 35 mm (panel thickness)
Mounting stand-off:	71 mm (wall to back of antenna)
Weight	≈ 0.82 kg
Material/color:	
	shroud: UV-resistant plastic, grey RAL 7035
	bracket: aluminium and zamak
Environmental	
Operating temperature:	-33 to +55 °C
Functional Specs	
Frequency	range 1880 to 1920 MHz
Nominal impedance:	50 ohms
VSWR:	≤ 1.6
Polarization:	linear, vertical
Gain (at connector level):	9.5 dBi ± 0.3 dBi
Radiation in horizontal plane:	beam width (H-plane) at -3 dB: ≈ 69°
Radiation in vertical plane:	beam width (E-plane) at -3 dB: ≈ 31°
Maximum power:	10 watts
Connector:	MCX male connector at the end of a 1 m
	RG316 coaxial cable (minimum bending radius: 20 mm)

Orientation capability:	± 45° in azimuth (horizontal plane)± 15° in
	elevation (vertical plane)

Radiation pattern



Typical radiation in horizontal plane



Typical radiation in vertical plane

TDM DECT Base Station

Physical	
Dimension:	170 × 170 × 38 mm (including mounting bracket)
Weight:	400 gms approximately
Material:	ABS molded plastic
Color:	White (NCS S 0502-B)
External connector	2 × MCX connectors for external antenna
PowerI	
Power	Locally, or centrally via 2 data pairs (UTP) and 1 optional pair
Operating voltage	21 to 56 Vdc
Power consumption	1.3 W to 2.0 W depending on number of slots currently in use.

Radio	
RF output power (e.r.p.) EU	Between 23 dBm and 28 dBm (with internal antenna)
RF output power (e.r.p.) US	Between 17 dBm and 21,6 dBm (with internal antenna)
Frequencies	
DB1 LA (Latin America) for use with DECT in the 1910-1930 MHz frequencies	
DB1 US (North America) for use with DECT in the 1920-1930 MHz frequencies	
Environmental	
Operating temperature	-10°C to +55°C
Storage temperature	-25°C to +70°C
Relative operating humidity	15 to 90%, non condensing
Immunity to electromagnetic fields	10V/m (EN61000-4-3)
Immunity to ESD	6 kV contact discharge and 8 kV air discharge (EN61000-4-2)
Compliance to European regulations and standards	
EU directives	1999/5/EC (R&TTE)
Radio	EN 301406
Safety	EN 60950-1
EMC	EN 301 489-6, EN 301 489-1, EN 60945
Product marking	CE
Compliance to US and Canadian regulations and standards	
Safety	CSA/UL 60950-1
EMC/Radio	FCC part 15 (Class B), RSS-213 and ICES-003
Product marking	FCC ID: BXZDB1, IC:3724B-DB1
Compliance to Australian regulations and standards	
Radio	Radiocommunications (Digital Cordless Communications Devices — DECT Devices) Standard 2007
Safety	AS/NZS 60950-1
Product marking	

Outdoor housing DECT base stations

Physical	
Dimension:	389 (w) x 170 (d) x 440 (h) mm
Weight:	5 kilogram (base station not included)
Material:	glass fibre reinforced polyester
Color:	grey (RAL 7036)
Environmental	
Check the environmental conditions of the base station to be used. Follow these conditions.	
Branding	Not branded
Compliance to regulations and standards	
Electrical safety:	IP66 according to IEC 529
Approvals: UL, CSA and Australian	UL, CSA and Australian
Optional Pole mounting set (can be ordered separately)	
Dimension:	The flexible mounting strip enables mounting on a pole with a circumference up to 750 mm.
Material:	stainless steel, aluminium and zinc plated metal
Weight:	ca. 1.5 kilogram

Troubleshooting

Introduction

This chapter provides steps to follow in the event of a failure of one of the following devices:

- IP-DECT Base Station (IPBS)
- Avaya 3720/3725 and 3740/3749 DECT Telephones
- Advanced Charger
- Multiple Battery Charger
- Rackmount Charger
- Portable Device Manager (PDM)
- Avaya In-Building Wireless Server (AIWS)

IP-DECT Base Station (IPBS)

The IPBS is unreachable by web GUI

If the firmware is corrupt, for example if firmware download is interrupted the IPBS could become unreachable by the web GUI. It will not be possible to load new firmware or to start correctly. If this occurs, the IPBS/IPBL runs on the bootcode and the Gwload tool (a tftp-style client used to repair a broken firmware) can be used to upload firmware.

1. Download the Gwload software from the IP-DECT system provider.
2. Set the IPBS/IPBL in TFTP-mode by performing a medium (~3 sec) hardware reset, see Reset using the reset button on page 191.
3. Start a command window.

   To update with new firmware, execute the following command from the folder where the **gwload.exe** file is located:

   IPBS:
   gwload /setip /i *<ipaddress>* /gwtype 1201 /prot *<..path/firmwarefilename>* /go
4. If there is more than one IPBS/IPBL in TFTP mode, select the unit to update and press enter.

Issues by using VLANs for connecting IPBS to the network

In an IP-DECT system all IPBS/IPBL (using the same Master) need to be in the same VLAN and need to use the same VLAN-ID. Check for LAN > VLAN configuration in the IPBS/IPBL web interface.

The switches the IPBS are connected to need to have the VLAN tagging mode enabled (e.g. dot1q) for the used ports.

Roaming between different IPBS masters of same IP DECT system not working

The coverage areas of the IPBS masters must not overlap. Otherwise roaming will not work properly. Due to the effects of overlap, the handset may sometimes not receive SMS. Also over the air, administration will sometimes not work. Finally, the handset sometimes cannot receive calls or make calls.

Fault Code Descriptions

This section lists the possible fault codes and their descriptions.

Description	Code
Interface down (Gateway)	0x00010001
Registration down (Gateway)	0x00010002

Description	Code
Protocol error (Gateway)	0x00010003
Standby Master is active	0x00030001
User registration failure	0x00030002
Emergency registration down (Master)	0x00030003
Connection to Radio lost (from Master)	0x00030204
Connection to Mobility Master lost (from MM)	0x00030301
Cannot establish connection to Mobility Master	0x00030302
Connection to Master lost (from MM)	0x00030303
Standby Mobility Master is active	0x00030304
No Media Data received (RTP)	0x00050001
Excessive loss of data (RTP)	0x00050002
Wrong Payload Type received (RTP)	0x00050003
Stun failed (RTP)	0x00050004
SRTP authentication failed (RTP)	0x00050005
SRTCP authentication failed (RTP)	0x00050006
Unexpected Message (H323)	0x00060001
Status Inquiry (H323)	0x00060002
NAT discovery failed (SIP)	0x00070001
Overload (SIP)	0x00070003
Coder selection failed (SIP)	0x00070004
Media configuration failed (SIP)	0x00070005
Unexpected restart (watchdog/reset/power on)	0x000b0001
Certificate validation is disabled until system time is set	0x000c1000
RFP disconnected	0x000e0001
RFP malfunctioning	0x000e0002
RFP disabled	0x000e0003
RFP software download failed	0x000e0004

Description	Code
RFP unsynchronized	0x000e0005
Synchronization to reference system lost	0x000e0006
Synchronization to alien system lost	0x000e0006
Backup synchronization master active	0x000e0007
Other DECT system with same sysid detected	0x000e0008
Sync master failed to resynchronize to reference	0x000e0009
Interface down	0x00110000
Interface not configured	0x00110001
DHCP server not responding	0x00110002
Invalid UDP-RTP port base/range	0x00110019
Invalid UDP-NAT port base/range	0x0011001a
Invalid NAT port base/range	0x0011001b
Checksum error	0x00110040
ARP poisoning detected	0x00110041
Out of TCP/NAT ports	0x00110046
Out of TCP ports	0x00110047
TCP checksum error	0x00110048
TCP bind error	0x00110049
Out of UDP/RTP ports	0x00110050
Out of UDP ports	0x00110051
UDP checksum error	0x00110052
UDP bind error	0x00110053
No route to destination	0x0011005a
No route to destination, if down	0x0011005b
No route to destination, if unknown	0x0011005c
No route to destination, if unconfigured	0x0011005d
No route to destination, no gateway	0x0011005e

Description	Code
No route to destination, loop	0x0011005f
Memory low (90%)	0x00120001

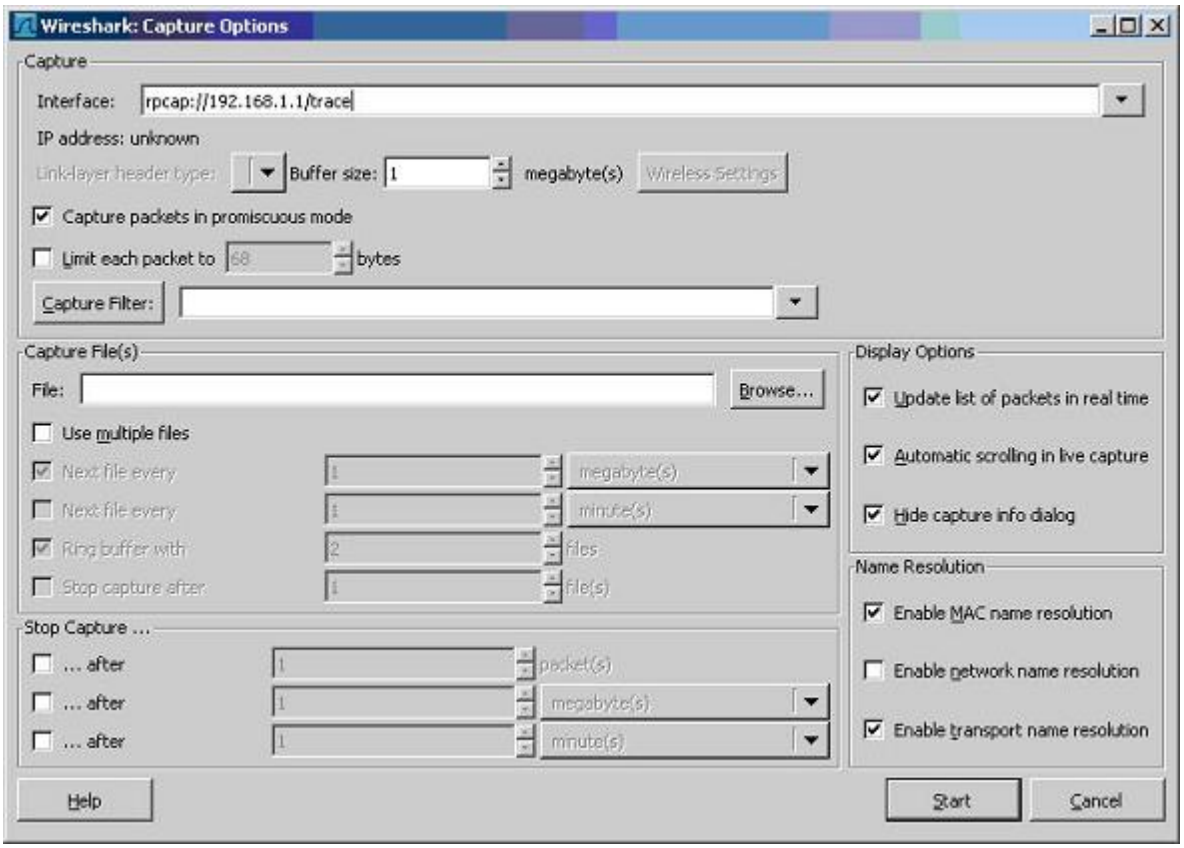
Remote LAN sniffer traces

The IPBS offers the ability to do remote LAN sniffer traces. The IPBS offers a PCAP interface that can be connected by LAN sniffer tools like Wireshark.

1. Go to **Diagnostics** > **Traces**.
2. In the **IP** section, select the **TCP/UDP Traffic** check box.
3. In the **Remote PCAP** section, select the **Enable** check box to enable the Remote PCAP interface.

Now the Remote PCAP interface “rpcap://xxx.xxx.xxx.xxx/trace” can be used in your wireshark tool to connect to the IP interface.

Figure 209: Remote LAN sniffer traces



Avaya 3720/3725 and 3740/3749 DECT Telephones

This section contains information on how to solve common operational problems, and warnings you may receive.

Go through the following lists if you encounter any problems.

Fault symptoms

If any of the following Fault Symptoms occur, follow the instructions below.

Fault	Probable cause	Action or comment
The display stays dark	Low battery level or faulty telephone.	Charge the battery. If the telephone does not work after charging it is defective.
There is no ring signal	**Sound off** or **Ring volume silent** icon is on, or faulty telephone.	Press and hold the Mute key, or increase volume (**Settings** > **Sound & Alerts** > **Volume**).
The handset does not log in to the Device Manager in AIWS/AIWS2	The handset is configure to log on a Device Manager in another system.	Change the "**Device Management System**" parameter to correct system
The Call list entries of the 3720 are deleted.	The battery was changed.	No fault. Normal behavior of 3720 after battery change.
Time stamp of Call log entries is wrong	*On DECT R4 systems:* Date and time info was not sent by IPBS. *On ADMM systems:* Date and time are not (correctly) set	Switch telephone off and on again. Set date/time manually in menu **Settings** > **Time/Date**.
Some menu items are not shown in the set language	Locally configured menu items are made in another language.	No fault. Locally by the administrator configured entries will not be translated when the language is changed.
Handset does not show the name from the local contacts for the calling number (Integral systems only)	Parameter Stimuli call phonebook look up is set on the handset	Parameter configuration needs to be changed by WinPDM or AIWS DM

While on charger, the telephone will shut down again immediately when it is switched on.	Switch off while in charger is activated.	Change setting in menu **Connections** > **In charger**.
Handset takes long time until it comes online in WinPDM or AIWS after it has been connected to the charger	If the handset has many local contacts or a big local company phonebook, it takes some time until the contacts are available after restart. The handset will come online after the contacts have been loaded.	need to wait after handset is switched on or a system change.
Not possible to mute the telephone by long pressing the **Sound off** key or the **Mute** button. Not possible to set the ring signal to Silent. Telephone, with the **In Charger** > **Sound off** parameter activated, is not muted when placed in charger.	The parameter **Possible to turn off sound** is disabled..	Enable the parameter. See *Configuration Manual, Cordless Telephones 3740/ 3725 for Avaya, TD 92617GB*.
Not possible to change ring signals in the telephone menu.	The telephone is configured to use the system-provided ring signals instead of the local ring signals.	Disable the **Force stimuli ringing** parameter. See Enabling/Disabling System ring signals (Stimuli) on page 227.

Phone cannot make or receive calls

- Check trunk configuration in IPBS master and Communication Manager (IP-Addresses and ports need to match).
- Check status station on Communication Manager if already in off hook state. Make a call to the station and check status station on Communication Manager again. I this does not work, remove station on Communication Manager and configure again.

Feature access codes do not work

It might be that feature access codes do not work even if they are sent manually or preprogrammed in the **In call** menu, **Call service** menu or **My favorites**. One option is to enter the R-key before sending the feature access code, e.g. "*05". If it is preprogrammed, you need to add the "R" in the value field for the feature, e.g. "R*05".

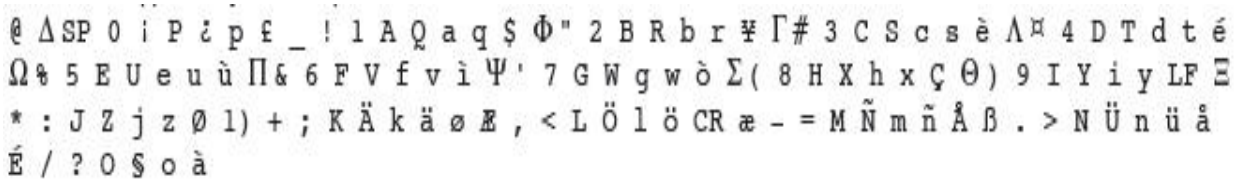
Handset cannot receive SMS and Centralized Phonebook access to LDAP directory does not work

In the IP DECT system, the user ID of the handset, **Menu** > **Settings** > **device info** > **User ID**, needs to be the extension number of the handset. The user ID can be configured by AIWS Device Manager or WinPDM. Navigate to the **Numbers** tab, select the device, and select **number - rename**. Change the number to the extension number of the handset.

Some characters will not be sent via SMS or the Send option does not work at the handset

For SMS, only the following characters will be supported by the SMS protocol:

Figure 210: SMS Characters



Handset restarts continuously when the handset moved away from the connected system

This is currently a limitation in the software. The problem occurs if the handset is subscribed to IP-DECT/other (GAP) *and* Integral Enterprise or Integral 5 systems at the same time and **Change system** is set to **Automatically**.

Workaround: After a restart the handset will start to search for a system. Go immediately to menu **Connections > System > Change system**. Select one of the systems in the list that you currently like to use. Make sure **Automatically** is *not* selected.

Centralized phone book search fails when using LDAP

It was observed when entering a blank in between the first name or the last name input field that there was no or faulty search results. Unfortunately a blank in the search string is internally used as a delimiter between first name and last name. E.g. if "Klaus Dieter" is entered as the first name and "Müller" as last name the LDAP request will search for "Klaus" as first name and "Dieter" as last name.

Handset shows “no access” but calls are possible

This issue could occur if the IPBS, with which the handset is currently connected, is disconnected from power and the IP network. In such situation, the handset roams to another IPBS of the same IP-DECT system, but the roaming to the new base station is incomplete from the IP-DECT system point of view (because the "old" IPBS doesn't answer anymore). The new IPBS will block the location registration for about 5 to10 minutes. So the handset will show “no access” for this time period. However, calls will be possible on this handset even if the location registration was not accepted by the new IPBS.

Display information

The following error messages can be shown in the telephone display:

Display shows	Probable cause	Action or comment
No access	The telephone is in range, but has no access rights.	Switch off the telephone and then switch it on again. If this does not work, the subscription data for this extension in the IPBS Master might be deleted.
No System. The telephone beeps once a minute with a low tone followed by a high tone (during max 30 minutes). If the vibrator is enabled, it vibrates after the last beep.	The telephone is out of coverage, or faulty telephone.	The beeps can be stopped with the mute button. **Note**: When re-entering the coverage area it can take a couple of minutes before the telephone automatically has registered into the system.
Name and number information of the other party not correctly shown in the display during a call	Wrong display format configured in Communication Manager.	Go to Communication Manager station form and check if "length of display" is configured to "16x2".
System busy	The IPBS you are connected to has reached its limited number of active calls.	Change place to get connected to the next available IPBS.
SERVICE NEEDED Parameters corrupt **Note:** This display message is only shown in English.	Faulty telephone.	Select the reset option on the middle soft key if available. Upgrade the telephone’s software to version 3.0.0 or greater If the problem persists send the telephone for service.

Display shows	Probable cause	Action or comment
PBX out of service	1. Handset can't do calls. Trunk configuration in IPBS Master is faulty or configured trunk on Communication Manager is down	1. Change trunk configuration on IPBS Master > DECT > trunk, use same ports on IPBS Master and Communication Manager side (both directions). Make sure that the port on the Communication Manager side is exclusively used by this signaling group.
	2. Handset can do calls and trunk IPBS Master is active, check on IPBS Master > Dect > trunk	2. Busy out the configured signaling group on the Communication Manager side, wait until trunk in IPBS Master is down, release signaling group on Communication Manager side, trunk on IPBS Master comes back to active, "PBX out of service" disappears on handset display.
Enter PIN code	Phone lock is activated.	Enter the required PIN code. If the PIN code has been lost, enter a new PIN code via PDM/AIWS.
Battery low, charge now	The battery level is low.	3725 and 3740: Charge the telephone, or replace or charge the battery. 3720 and 3749: Charge the battery while the battery is inserted in the telephone, or replace the battery.
Central phonebook is not available at the moment.	The Central phonebook does not respond or is not activated.	Verify Central phonebook configuration in the AIWS.

Display shows	Probable cause	Action or comment
Voice mail number not defined	There is no Voice mail number defined in the telephone.	Define a Voice mail number via the PDM/AIWS: Systems >System A > PBX Settings > Numbers.
Could not encrypt connection	The parameter "Encryption Required" is enabled in the telephone in combination with: 1. Unencrypted base station(s); and/or, 2. Unsupported base station(s).	1. Disable the "Encryption Required" parameter in telephone; and/or, 2. Enable the encryption in the base station(s); and/or, **Note:** If Avaya's base station(s) is used, the software version must be 3.1.x or greater. 3. Use supported base station(s). Ask your supplier.

LED error indications

See chapter LED indications on page 245.

LED is flashing red, quick flash, (100 ms on, 800 ms off)

- If a third telephone, that is an other telephone than the "old" and "new" telephone mentioned in Definitions on page 210, is inserted into the charger during Easy Replacement, this error indication appears. Change to the correct telephone.
- The charger has found that Easy Replacement does not work. Change back to the "new" telephone.

LED is flashing red, long flash (800 ms on, 100 ms off)

Error during Easy Replacement. *Both* telephones need to be sent for service.

Advanced Charger

For general LED indications, see also LED indications on page 278.

Status LED on the charger is not lit.

Check that power is supplied.

If power is supplied and the status LED is still not lit, the probable cause is a software error. Send charger for service.

Status LED on the charger is fixed red.

Send charger for service. Connect charger to PDM via USB and check if charger goes online. If yes check software version of the charger.

Status LED is flashing red for 3s, then green

A factory reset has been performed. It may be necessary to set parameters from PDM/AIWS.

Status LED is flashing red (100 ms on, 800 ms off) for more than 3s

An error occurred during Easy Replacement. Remove portable from charger.

Status LED is flashing red (800 ms on, 100 ms off) for more than 3s

If the error occurred during Easy Replacement, remove the portable from the charger. The charger should return to normal operation.

Otherwise send charger for service.

Charging does not start

Check that the telephone is properly inserted in the charger.

Advanced Charger does not appear in PDM/AIWS

Check that the communication cable (USB or Ethernet) is connected.

If charger doesn't appear in the AIWS device manager when connected via Ethernet you might have to configure the AIWS IP-address with the PDM tool (refer to Advanced Charger does not appear in AIWS on page 274).

Easy replacement does not start

Check that the handsets are of the same device type.

Check the handset software version. (refer to the configuration manual for details)

Check that the Advanced Charger software version is at least 1.3.7, see Software update on page 276.

Multiple Battery Charger

Charging does not start

Check that the battery is properly inserted in the charger.

Check the AC power supply connection.

Rackmount Charger

For general LED indications, see also LED indications on page 312.

Status LED on the charger is not lit.

Check that power is supplied.

If power is supplied and the status LED is still not lit, the probable cause is a software error. Connect charger to PDM via USB and check if charger goes online. If yes check software version of the charger. Send charger for service.

Status LED on the charger is fixed red.

Connect charger to PDM via USB and check if charger goes online. If yes check software version of the charger. Send charger for service.

Status LED is flashing red for 3s, then green

A factory reset has been performed. It may be necessary to set parameters from PDM/AIWS.

Status LED is flashing red (100 ms on, 800 ms off) for more than 3s

An error occurred during Easy Replacement. Remove portable from charger.

Status LED is flashing red (100 ms on, 800 ms off) for more than 3s

If the error occurred during Easy Replacement, remove the portable from the charger. The charger should return to normal operation.

Otherwise send charger for service.

Charging does not start

Check that the telephone is properly inserted in the charger.

Rackmount Charger does not appear in PDM/AIWS.

Check that the communication cable (USB or Ethernet) is connected.

If charger doesn't appear in the AIWS device manager when connected via Ethernet you might have to configure the AIWS IP-address with the PDM tool (refer to Advanced Charger does not appear in AIWS on page 274).

Easy Handset Replacement doesn't start at the Rackmount Charger

Easy handset replacement is only supported in the first slot (most left) of the Rackmount Charger.

Rackmount Charger doesn't go online in the Device manager or Easy handset replacement doesn't start

Try a software reset.To reset the Rackmount Charger, press the embedded LED on the front of the charger, for example with a pen or a screw driver.

Portable Device Manager (PDM)

When troubleshooting the PDM, it is always a good idea to examine the log files, since they provide additional information that may prove useful. When reporting an error to your supplier, always include the appropriate log file.

Log files are stored under
C:\Documents and Settings*<user name>*\Application Data\Avaya\WinPDM\log.
The log files are rotated every 10 MB and are time-stamped with 1 ms resolution.

The PDM does not Start / Installation fails

To run the PDM, the computer must fulfill the requirements listed in Portable Device Manager (WinPDM) on page 655. If you do not have the correct software versions installed, contact your system administrator.

For Windows 7 (64-bit machine), a Java 64-bit installation is required to run WinPDM. Java 32-bit and Java 64-bit can be installed in parallel on the same machine without problem.

To install the PDM, you must have administrator rights on the computer. Contact your system administrator if you are not able to install the PDM.

Firewall issues

Windows Firewall may alert you of **PMServer**, **CuspCsi**, **UspCsi, CuspSerialCSI** and **MwpCsi**. These alerts will not affect the PDM but you can select **Continue blocking** or **Unblock** to avoid further alerts.

No Indication of connected Device

If a device does not show up in PDM, make sure the device is properly connected, or try disconnecting and reconnecting the device.

If a connected Advanced Charger or Rackmount Charger does not show up as connected in the **Devices** view, the USB port may not be configured correctly.

Open Windows **Control Panel > System**. Select the **Hardware** tab and then select **Device Manager**. If the device does not show up in the list (as a USB port), check the connection and reinstall the drivers and/or software for the device (see Software installation on page 320).

The USB driver can also be installed separately and can be found on the PDM installation in the USB driver folder.

Connected device does not come to online

If the handset has many local contacts or a big local company phonebook, it takes some time until the contacts are available after restart. The handset will come online after the contacts have been loaded, which could take some minutes.

Software in Device Not Recognized/Synchronization Fails

A device might have software with a parameter set that is newer than the version recognized by the PDM. The PDM will then be unable to send parameters to the device. The icon (a red broken arrow) in the **Parameters** column for the selected device indicates that the synchronization between the device and the PDM was not successful.

If this is the case, the PDM should be updated with new software and definition files provided by your local supplier. See Import Parameter Definition Files on page 348.

Software Upgrade Fails

Verify device is still online. Handset needs to be plugged into the Advanced Charger or Rackmount Charger. Chargers need to be connected via USB to the PC. If device is still online try to restart the software upgrade again.

Avaya In-Building Wireless Server (AIWS)

General troubleshooting

Log files

When troubleshooting AIWS, it is always a good idea to examine the log files, since they provide additional information that may prove useful. When reporting an error to your supplier, always include the appropriate log file.

To find logs,

1. On the AIWS start page, click on **Configuration**. The **AIWS Configuration** page opens.
2. In the left pane, click on **Other settings** > **Advanced Configuration**. The **AIWS Advanced Configuration** page opens.
3. Click on **Troubleshoot**.
4. Click on **View Info Log**, **View complete Log** or **View Error Log**.

AIWS Device Manager does Not Start

To use the AIWS GUI, the computer must fulfill the requirements listed in Avaya In-Building Wireless Server (AIWS) on page 656. For the AIWS2 see the requirements listed in Avaya In-Building Wireless Server 2 (AIWS2 hardware) on page 659. If you do not have the correct software versions (Java runtime environment) installed, contact your system administrator.

AIWS Device Manager does Not Start with Firefox Browser

If you are using Firefox as your default browser, you will not be able to open AIWS Device Manager. You have to set the proxy settings in the Java Control Panel manually.

1. Open the Java Control Panel.
2. Select the **General** tab.
3. Click **Network settings**.
4. Select the **Use Proxyserver** option or the check box **Direct connection**.

   Your browser's proxy settings will be automatically copied in the text fields **Address** and **Port**.
5. Save the settings with **OK** button.

Firewall issues, or No Indication of Connected Device

If there is a firewall between AIWS and any devices, the firewall may need some configuration to allow communication.

Unable to Access FTP Area

Make sure the client is set in active mode.

Example for Internet Explorer:

In the menu, select **Tools -> Internet Options**... -> **Advanced**. Under “**Browsing**”, uncheck the “**Use Passive FTP** (for firewall and DSL modem compatibility)” checkbox.

When secure mode is enabled, see Web access security settings on page 380, only secure access via HTTPS and FTPES is allowed. HTTP is automatically redirected to HTTPS and FTP access is not allowed. The FileZilla Client freeware (not included) supports FTPES.

Get stuck while installing a new software image

After booting AIWS in image installation mode the browser is not redirected to the next page, there is a Network Error (tcp_errror) and the page was not found because the web server is not running. This is mostly observed once after a power on cycle when the internal battery of the AIWS is not activated by jumper J1, please refer to Activation of battery on page 543.

- Press back on your browser to boot the AIWS in the image installation mode again. Now you should get redirected to the next page even if the battery is not active.
- Sometimes the browser try to use a secured connection to https://xxx.xxx.xxx.xxx/install what is not supported. Connect manually to **`http://xxx.xxx.xx.xx/install`** to continue the update.

Installation of the new AIWS software is not successful

While installing a new software using the eas file, the installation is canceled and an error message like “Installation NOT successful, please use the complete image to upgrade the software” is displayed. In such a case, the software update needs to be restarted using the "image upgrade" option and the img file, for example, while upgrading from Edition 2 v2.4x to Edition 3 v2.7x.

Centralized phonebook via LDAP to Active Directory

When doing LDAP queries against MS AD it sometimes returns referrals. This will cause the LDAP query to not return the expected results. This is because OpenLDAP that Elise modules are using follows referals anonymously this is something that is not allowed in MS AD.

Referals will usually be returned when the Search Base DN is set to "wide". In order to avoid referrals in most cases it's enough to specify at least one OU in addition to the the DCs in the DN. This is dependent on the AD implementation though so it's not sure this will completely stop the referrals. This method also requires all the users that should be searchable to be placed in the OU that is specified or in sub containers. This is not always the case.

A more general approach to get the LDAP queries to work with MS AD is to use AD Global Catalog (GC). The GC is a role that an AD server can get. Instead of using the LDAP port 389 you use GC port 3286 for the AD server that have the GC role. The GC have to be configured to synchronize all attributes that is needed for the users in the phonebook.

NetPage troubleshooting

My Groups and My Messages don’t work

Check that cookies are enabled in your web browser.

Number list, Common Groups, or Common Messages are unsatisfactorily updated

Refresh the cache memory on the web browser. If they still are unsatisfactory, refresh caching proxy (if any). In, for example Microsoft Internet Explorer, this can be achieved by pressing CTRL+F5.

Entire Message history including column headings doesn’t appear

The Java Virtual Machine may be missing on your PC. Contact your IT department for assistance.

Message history is not running, although messages are sent and column headings are visible.

There might be a firewall preventing you from receiving data from the NetPage server. Contact your IT department to open port number 5891 in the firewall, in the direction from the web client to the NetPage server.

Reboot after image installation w/o restoring the parameters

When installing a new image file it is recommended to take a parameter backup in advanced and restore the backup afterwards. If reboot was selected w/o restoring the parameters all configuration including the IP-Network parameters is lost. However is a fixed IP address is used you can connect to the AIWS web interface by using this fixed IP address. When connecting to the AIWS the setup wizard will start automatically as usual after a factory reset. If a backup file is available you can select cancel for the setup wizard, go to configuration - other settings - backup/restore. Restore the old setting by choosing your backup file and select restore. Finally a reboot is needed to activate the old parameter settings.

Troubleshooting the Elise 3 Server (AIWS2 Hardware)

Troubleshooting Guide

Troubleshooting is normally done by accessing the application's web interface to see logs, statistics etc. But if for some reason the application's web interface cannot be reached, it is possible to get access to the information by placing the module in Troubleshoot mode. See Troubleshooting in boot mode on page 697

Fault	Probable Cause	Action or Comment
Several functions of the software application on Elise 3 Server (AIWS2 Hardware) do not start.	No valid license is present. The module has been running for more than two hours in the Demonstration mode.	Check if the functions start in Demonstration mode, if iyes, enter a valid license and restart the module.
The module has put itself in Boot Mode.	No software is installed or the installed software is malfunctioning.	Install new software
A LED shows slow or quick flashing red light		See Status LED indicators on page 566
The module cannot be accessed through the management port.	The required port driver is not installed on the PC or for the USB port you have connected to (or not correctly installed).	Note: The installation differs between Windows XP/Vista and Windows 7. See Accessing the Elise 3 Server (AIWS2 Hardware) through the management port (USB) on page 581.
	The PC has not been given enough time to obtain an IP address from the DHCP server.	When switching between mass storage mode and network mode, it takes about 30 seconds before an IP address is obtained from the DHCP server.

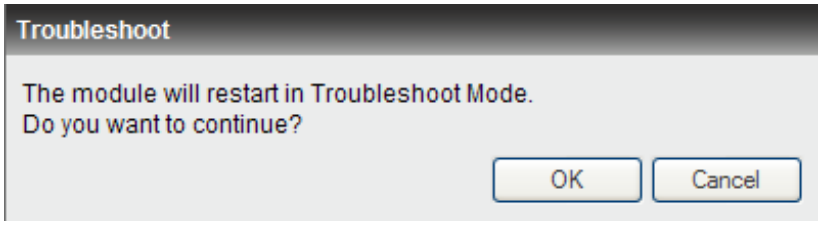
Fault	Probable Cause	Action or Comment
The installation of the USB port driver has been successful, but you still cannot connect to your Elise3 through the USB network.		Try the following command. Open the Command Prompt and type: route DELETE 192.5.36.229 arp -d 192.5.36.229
An external battery is connected but the Power LED shows slow flashing red light and in System status (under System Information in Troubleshoot Mode) the “Charge external supply” shows “off” even if the external battery voltage is shown in “External power supply”.	Elise3 does not charge the external battery.	The Elise3 module does not charge the external battery if the battery voltage is below 8.0 V or if the internal power supply voltage is less than 13.8 V.

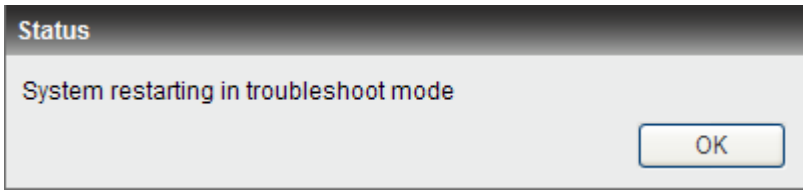
Troubleshooting in boot mode

You can access the applications through the Troubleshoot button in the web interface. (Boot Mode GUI), At this time no applications are running and you can see logs and other information. The log files provide additional information that may prove useful while troubleshooting.

When reporting an error to your supplier, always include the appropriate log file.

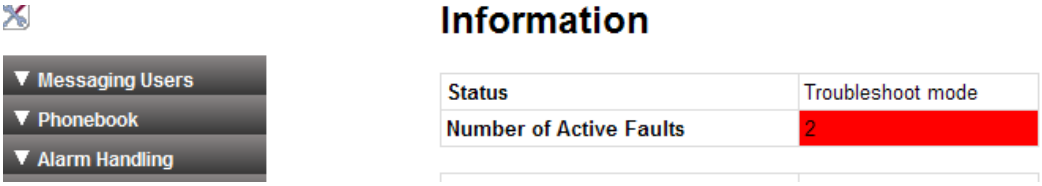
1. Enter Boot Mode, see Starting in boot mode on page 565.
2. Click the Troubleshoot button.
3. Click “OK” in the Troubleshoot dialogue window.





The system will restart in troubleshoot mode within approximately 5 minutes. The browser refreshes to the application's GUI automatically.

4. Access the application’s Configuration page.



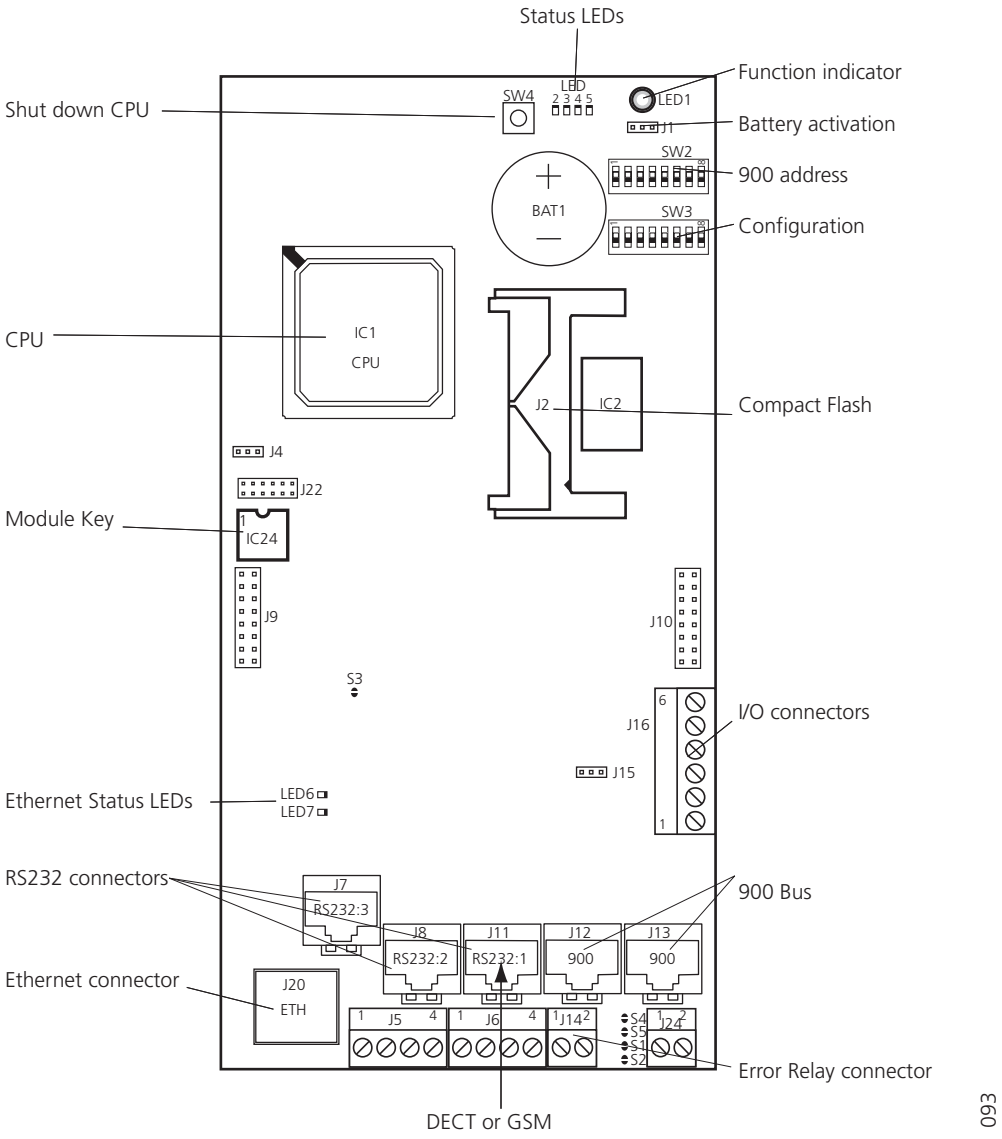
Select Other Settings > Advanced Configuration. You will now be able to perform troubleshooting actions and view system information, logs etc.

Built-in tools in AIWS

For Elise 2 Server (AIWS Hardware)

The AIWS hardware has different LEDs to indicate the status and besides that the possibility to show active faults and logging the faults.

Figure 211: AIWS Circuit board



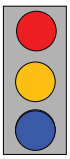
Tools	Description
Function Indicator	Refer to the table Function indicator on page 530 or Getting Started with the AIWS on page 505.
LED6	ON: Communication on Ethernet

LED7	ON: 100MBit/s OFF: 10MBit/s
Unlicensed mode	Unlicensed mode is activated by SW3, section 5 (pin 5), refer to Selecting operating mode on page 529, and a restart. AIWS will run with full functionality for 2 hours, then it stops! If it works in unlicensed mode and not in normal mode you probably have a licence problem. Refer to License on page 527 to install the valid license. Variants on page 658 describes which features are supported by which kind of licenses. **Note:** Do not forget to switch back to normal mode and restart the module.

Built-in tools in AIWS2

The hardware has different LEDs to indicate the status and besides that the possibility to show active faults and logging the faults through the GUI.

Table 10: Tools in the Elise 3 server

Tools	Description	
LEDs 	The LEDs show different colours to determine type of information and have different flashing frequency for showing the priority.	
	Color	**Indication**
	Red	Fault indication
	Yellow	Mode indication
	Blue	Normal operation
	Flashing frequency	**Indication**
	Fixed light	Indicates normal state
	Slow flashing light	indicates medium attention
	Quick flashing	Indicates high attention
Demonstration mode	Demonstration Mode is activated by pressing the Mode button for 10 seconds. The module will then run with full functionality for 2 hours, it then returns to the configured license! If it works in Demonstration Mode and not in normal operation you probably have a license problem.	
Active Faults	The Active faults page lists the last 100 received active persistent fault logs.	
Fault logging	The fault log is a centralized log file and shows a complete log of the faults in the system. Every time a fault message is generated in the system, information about the fault is written to the log file. The maximum number of entries in the log file is 1050. When the log file is full, the 50 oldest entries are removed.	
System Information	You can view the snapshots of logs or complete logs on the Advanced configuration page. Access to the Advanced configuration page requires administrator privileges.	

Advanced troubleshooting

AIWS Advanced Configuration page (requires administrator or system administrator rights) includes pages for advanced troubleshooting.

1. Click **Configuration** on the start page. The **AIWS Configuration** page appears.
2. Select **Other Settings** > **Advanced Configuration** in the left menu. The **AIWS Advanced Configuration** page appears.
3. Click the **Troubleshoot** button. The **Troubleshoot** page appears.
4. In the left menu in the *Troubleshoot* page there are links to pages where it is possible to view logs and find detailed information about the system.

- View Info Log
  Information saved in a volatile memory.
- View Error Log
  Errors and notifications saved in a permanent memory.
- View Complete Log
  (requires sysadmin rights)
  The Complete Log includes Info Log, Error Log and additional debug information.

  Note:
  This page shall only be used when information is requested by Technical Support.
- System Information
  - Information about module status.
  - Debug settings can be made. Standard debug is set by default but it can be extended to show more details.
- Send Test Message
  Possibility to send a test message to an entered Call ID.
- IP Statistics
  Information about the number of sent Unite messages and retransmissions for entered IP destinations can be viewed.
  The syntax of the listed IP addresses in the IP Statistics page is:
  <IP address> (<No. of sent messages>)[- !] where " - !" indicates that retransmissions have been made.
- Disk Status
  Status of the partitioned Compact Flash used by AIWS.
- Module Fault List
  Level of seriousness for different kinds of log events can be set. These events can appear in the Status Log (further described in chapter Status on page 455).

AIWS factory reset

There is no general factory reset procedure available on the AIWS. You manually need to go to the AIWS advanced configuration (AIWS start page - configuration - other settings - advanced configuration), check all the settings and press the "factory" button if available to reset the setting to default.

- Device management
- Phone book
- remote management (remote connection, open ports and serial port channels)
- general settings
- IP-Dect
- device handling (portable devices, desktop chargers, advanced chargers)
- message distribution (Alarm, Mobile Data, Location and Availability info)
- UNS (operating mode)
- User server
- logging (status log, system activity log, advanced parameters)
- Time settings
- Security web access
- password policy
- passwords needs to be changed/reset manually (sysadmin user/password needs to be known)
- network
- license

A work around is to install the image again on the AIWS flash card, see Replacement of the Compact Flash on page 550. This will clear all settings to default including the license key and network parameters. Of course you should not restore a AIWS backup file afterwards.

What to consider when replacing a module

Refer to Installing Elise 2 Server, General information on page 527 and Installation on page 532 to find information about:

- Address
- Jumpers
- Switches

- Cable connections
- Battery

Licences are defined in the Module key. The type of information that is located on the Compact Flash is software, configuration settings, fault logs, templates, etc.

When replacing a faulty Elise 2 hardware module, the Module Key and Compact Flash can be moved from the faulty Elise 2 module to the new Elise 2. By doing this, the licenses and the settings can be used directly on the new Elise 2.

See Getting Started with the AIWS on page 505 and Installation on page 532 for a detailed description on how to work with the Elise 2 hardware.

Configuring PTT on Meeting Exchange

Introduction

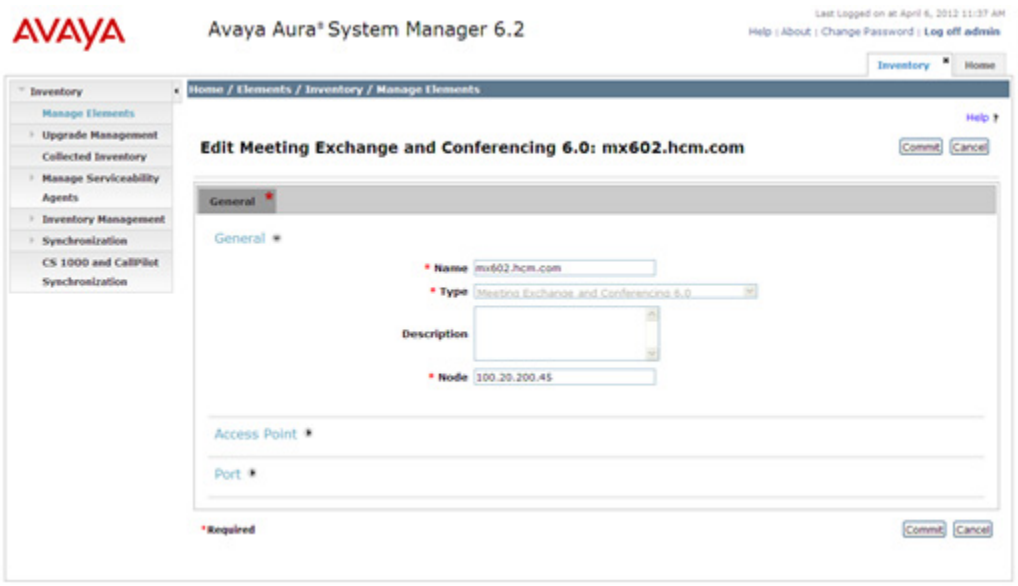
This chapter describes how to configure PTT for use on the DECT system.

Creating a DDI on the SMGR (Session Manager)

If you want to configure the direct conference for PTT calls, then you must create DDI aon SMGR and boot the conference using the Avaya Bridge Talk software.

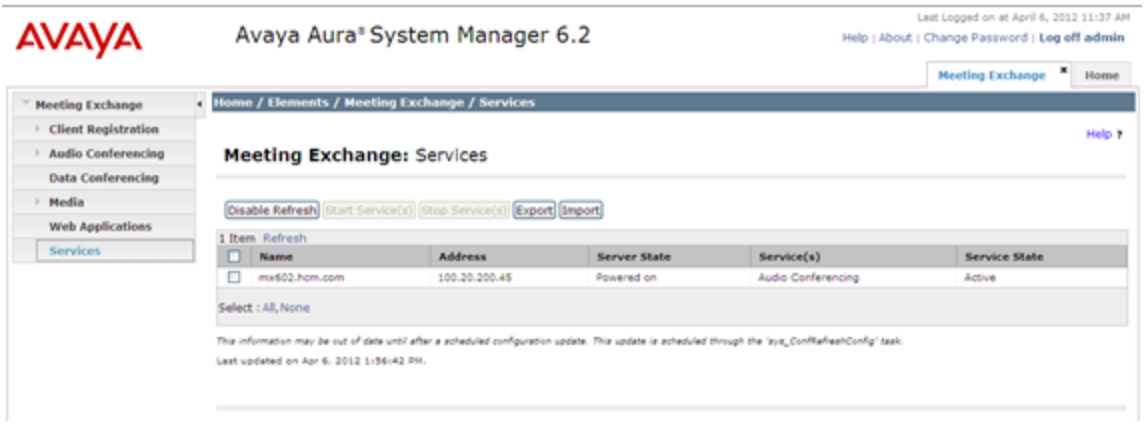
On the SMGR

1. Access the SMGR page.
2. Go to Element > Inventory.
3. Click on New.
4. Add the Meeting Exchange information as shown below:

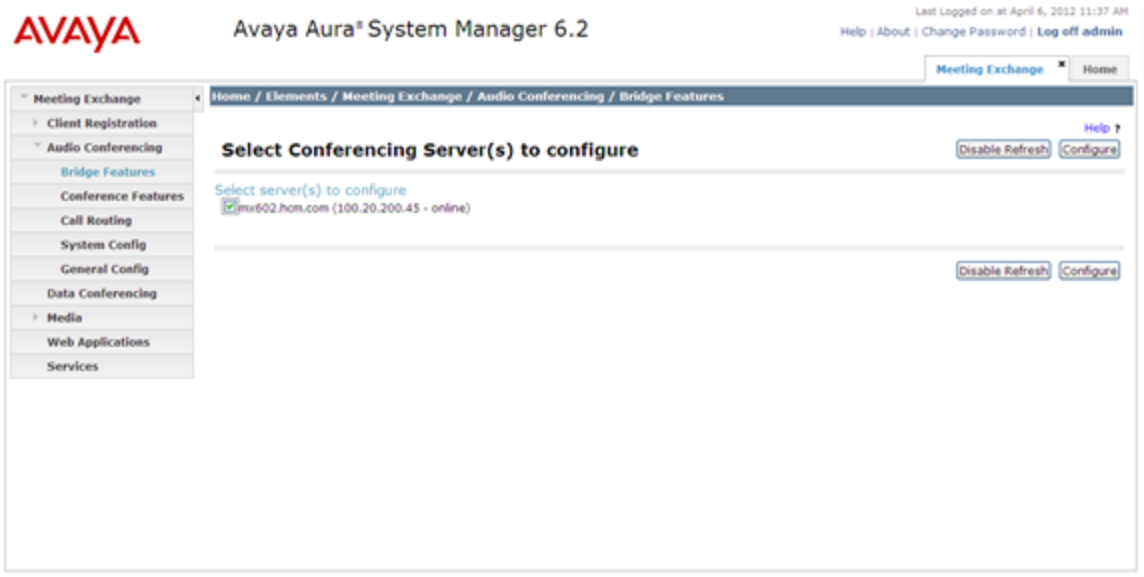


5. Go to the SMGR page > Element > Meeting Exchange
6. Go to Meeting Exchange > Services

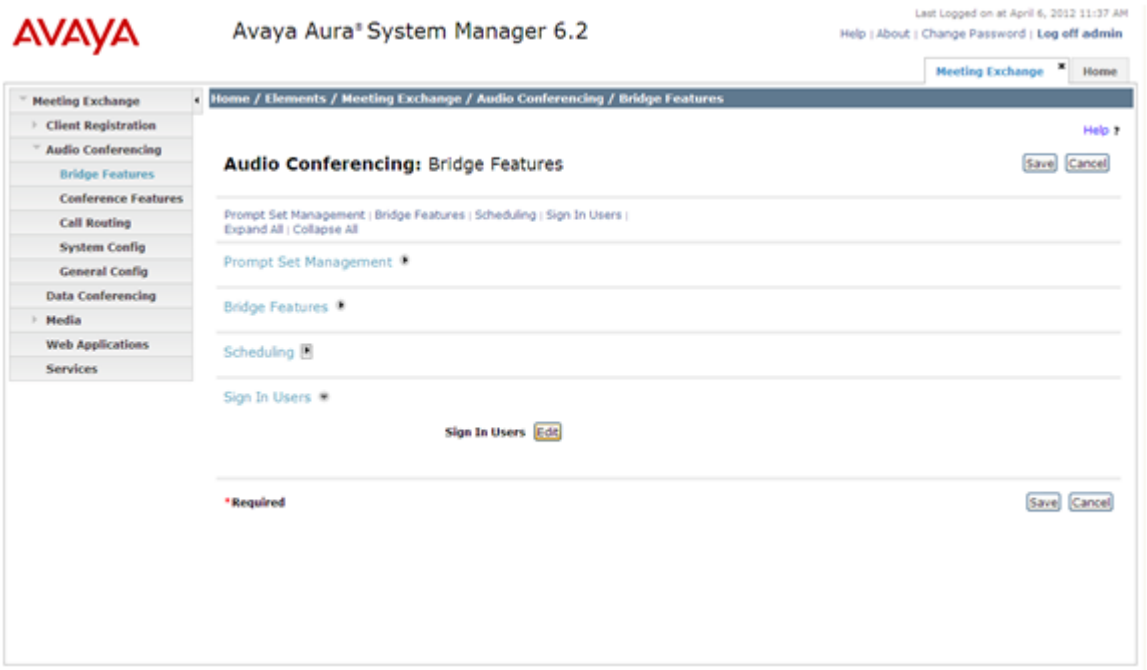
7. Verify the status of MX Server. If service is established it shows as active.



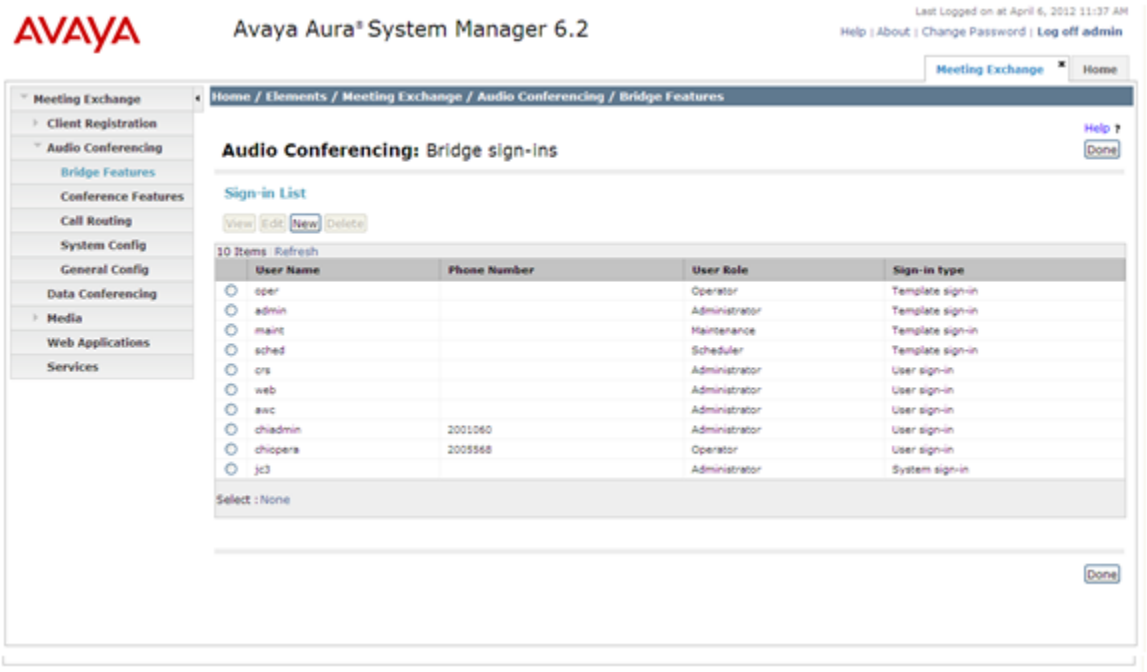
8. Go to Meeting Exchange / Audio Conferencing / Bridge feature.
9. Click on checkbox of Meeting exchange server and click “Configure” button.



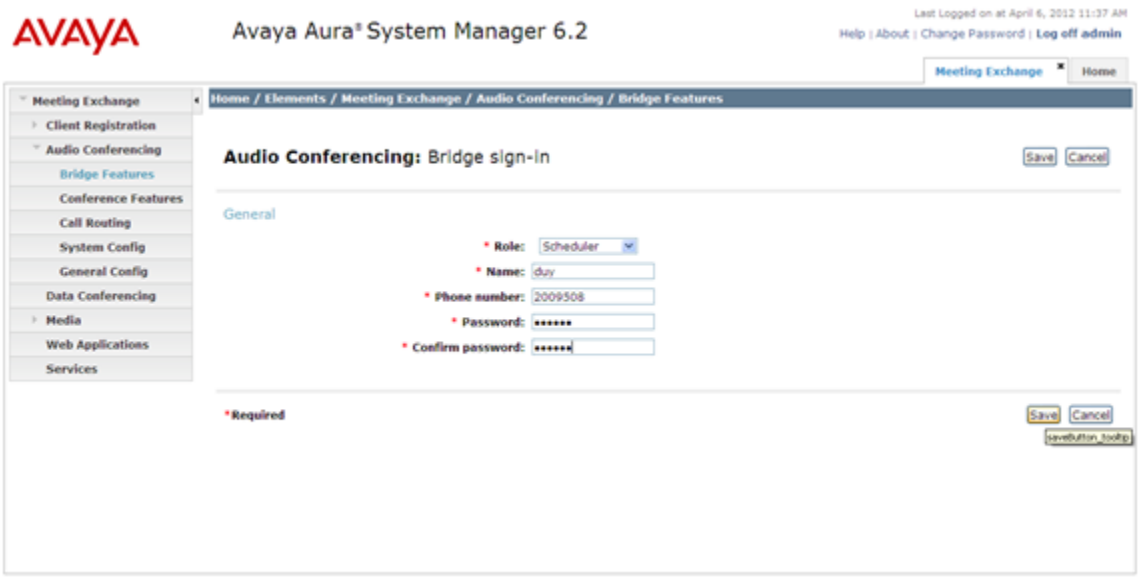
10. Go to Meeting Exchange / Audio Conferencing / Bridge feature /Sign In Users.
11. Click Edit button.



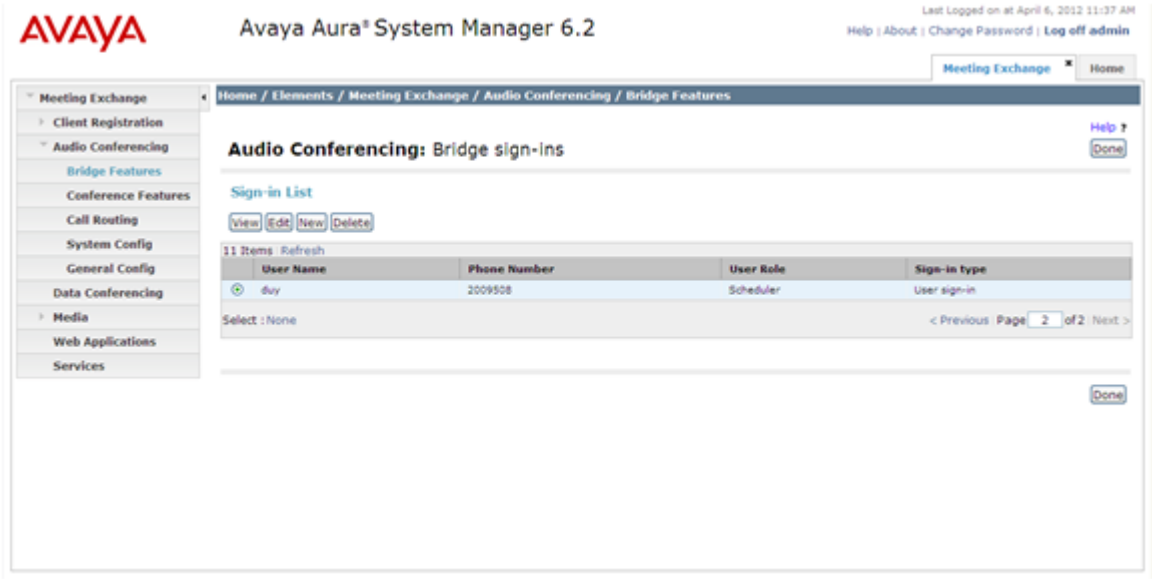
List of Sign-in users is displayed.



12. Sign in as the Operator/Maintenance/Scheduler



The screen displays the Bridge Sign-ins and roles.

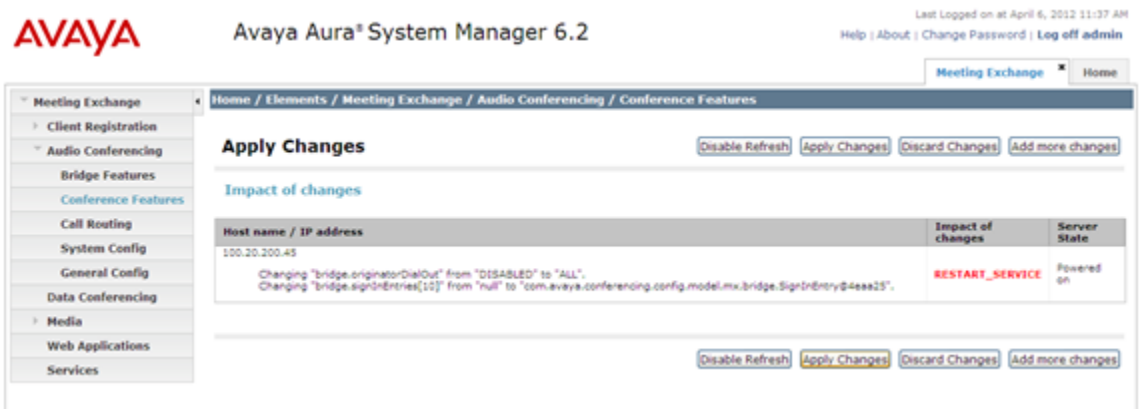


13. Go to Meeting Exchange / Audio Conferencing / Conferencing features / Conference Settings.

14. Enable “Original Dial Out” to All.



15. Apply change.

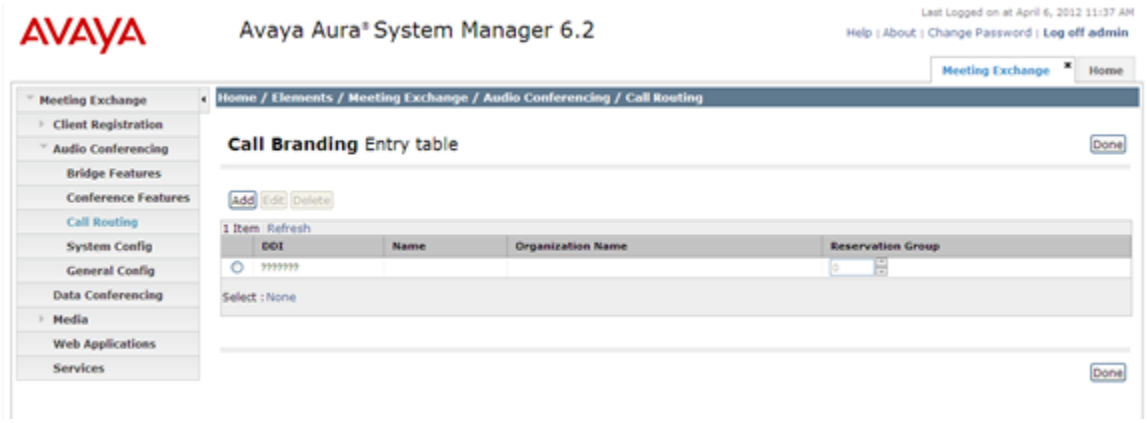


Adding a call branding entry

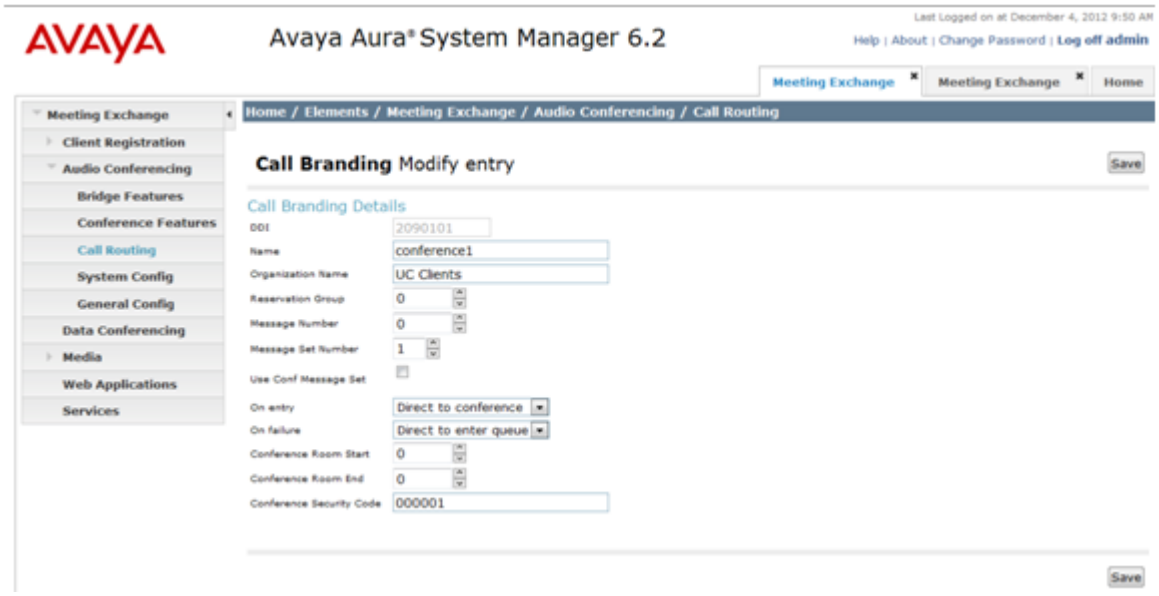
The purpose of this task is to create an association between a particular DDI and a Meeting Exchange call flow.

Procedure on SMGR

1. Navigate to Elements > Meeting Exchange > Audio Conferencing.
2. If necessary, select the IP address of the application server and click Configure.
3. Click Call Routing.
4. Click Call Branding to display the Call Branding Entry table and click Add.
5. Enter a call branding entry using a DDI from your deployment.
6. Click Save.



7. Click on Add.
   Note: Select Direct to Conference.



Tel num to URI

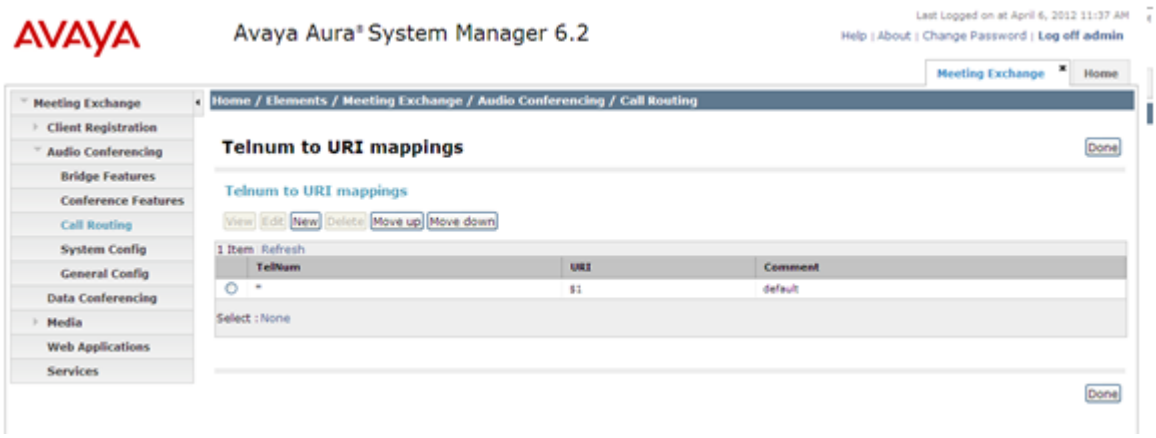
The TelnumToUri.tab file is stored in the /usr/ipcb/config directory.

Configuring patterns for dialing out

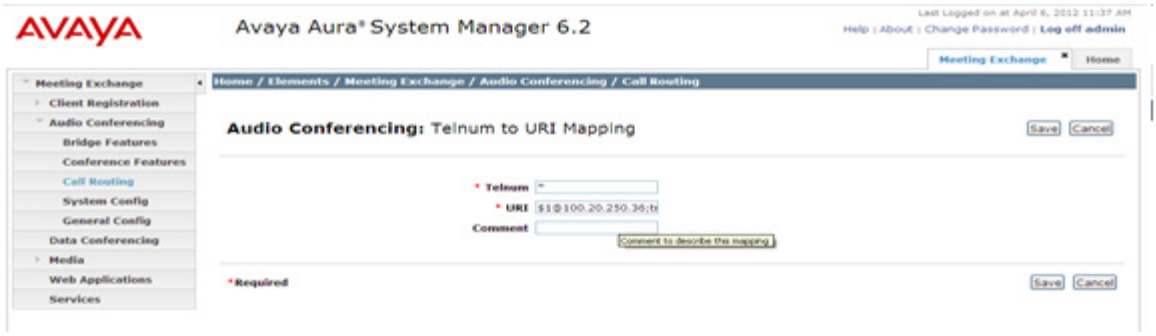
The purpose of this task is to create a pattern to enable conference moderators to dial out to other potential participants. As an aside, you can choose to disable this feature in your deployment.

Procedure

1. Navigate to Elements > Meeting Exchange > Audio Conferencing.
2. If necessary, select the IP address of the application server and click Configure.
3. Click Call Routing.
4. Click Edit at the Telnum to URI field.

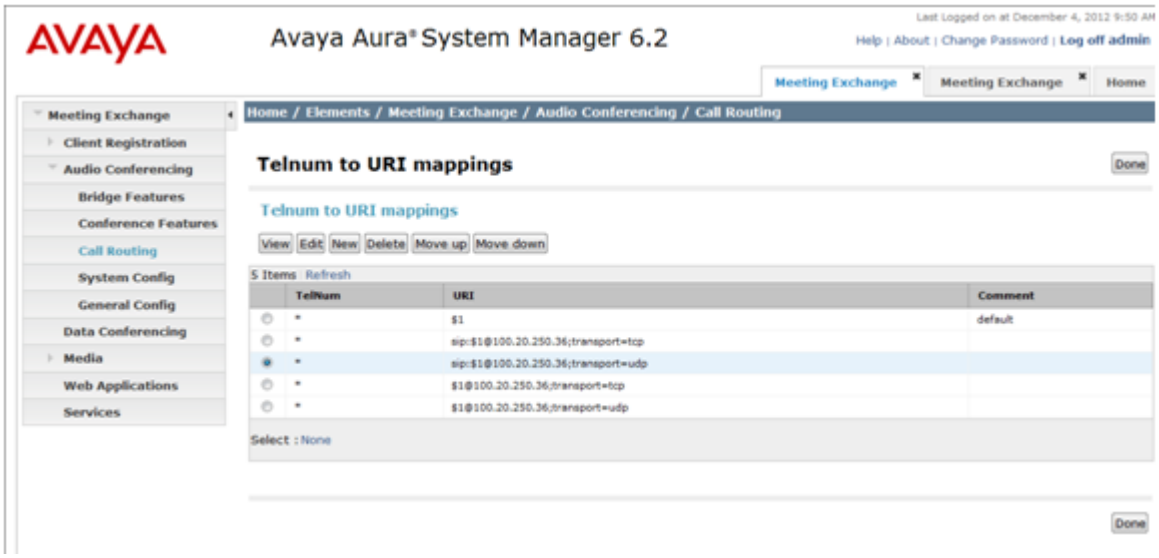


5. Click Add to display a new empty row.
6. Enter the pattern details that you require. Meeting Exchange adds the pattern to the Telnum to URI file.



TelnumPattern	TelnumConversion	comment Default
*	sip:$1@100.20.250.36;transport=tcp	SM address
*	sip:$1@100.20.250.36;transport=udp	

7. Click Save.



URI to tel num

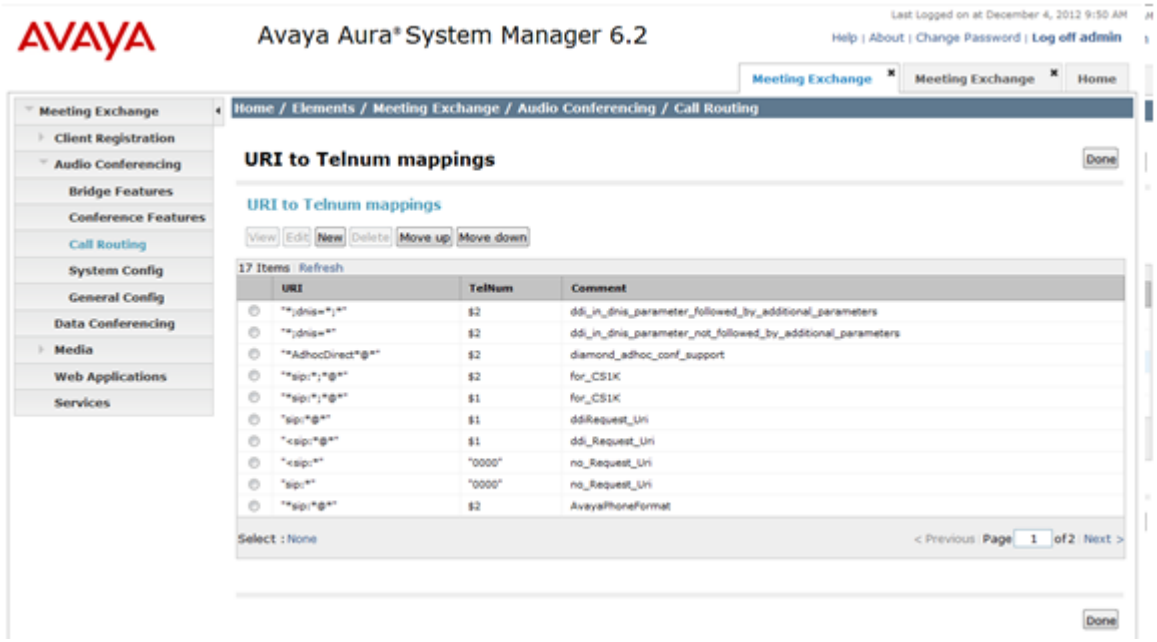
Uri To Telnum maps work in tandem with call branding to brand the customer experience for callers who dial into a conference or who dial a conference recording.

The UriToTelNum.tab file states that the Meeting Exchange application server should recognize a given URI and identify this URI's corresponding DNIS.
The UriToTelNum.tab file is stored in the /usr/ipcb/config directory.

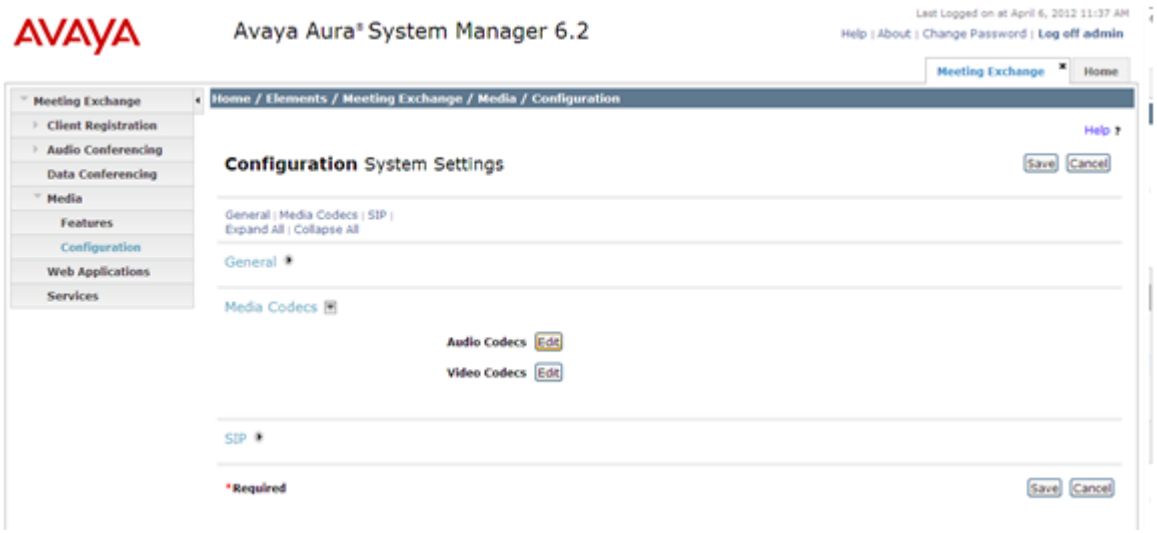
Configuring patterns for dialing in

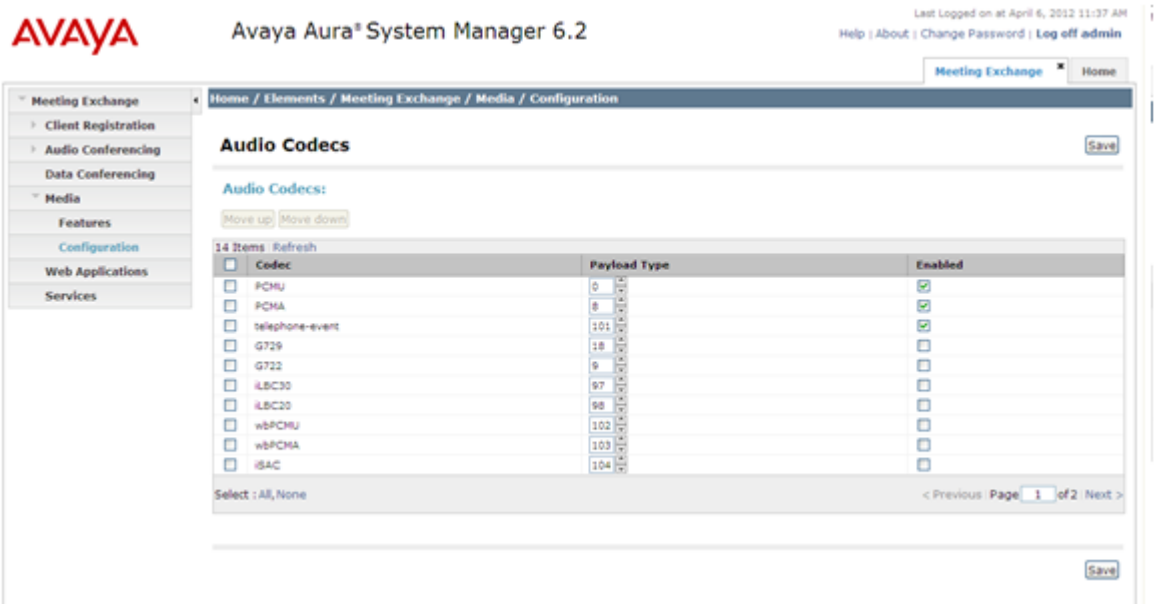
The purpose of this task is to create a pattern to enable Meeting Exchange to recognize a URI.

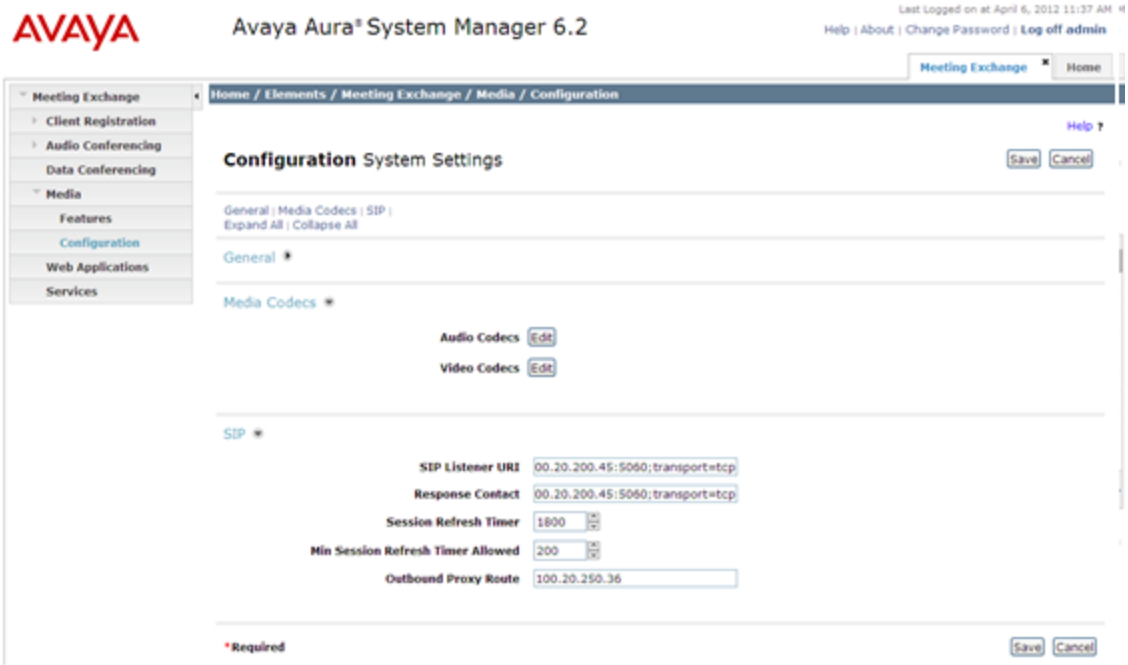
1. Navigate to Elements > Meeting Exchange > Audio Conferencing.
2. If necessary, select the IP address of the application server and click Configure.
3. Click Call Routing.
4. Click Edit at the URI to Telnum field.
5. Click Add to display a new empty row.
6. Enter the pattern details that you require. Meeting Exchange adds the pattern to the URI to Telnum file.



7. Check the Audio codecs.



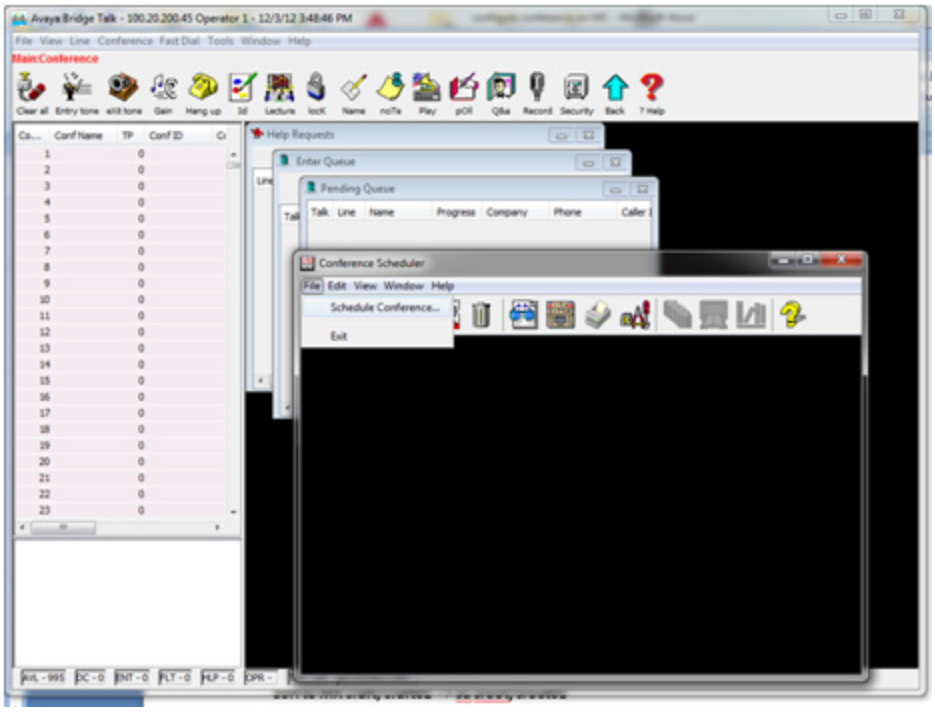




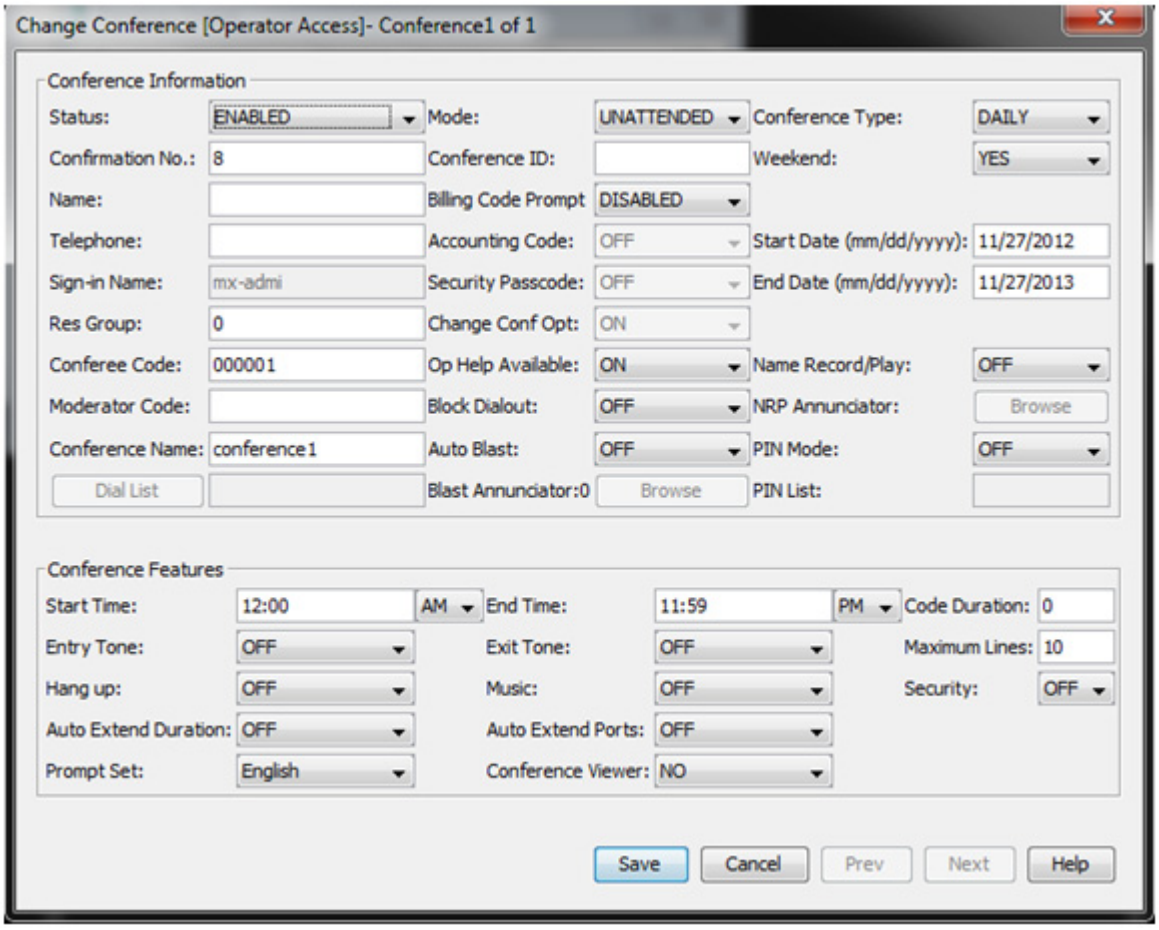
On the Avaya Bridge Talk

1. Use the user id that we configured earlier to login.
2. View > conference scheduler

3. File > Schedule conference



4. Fill out the parameters for the conference.



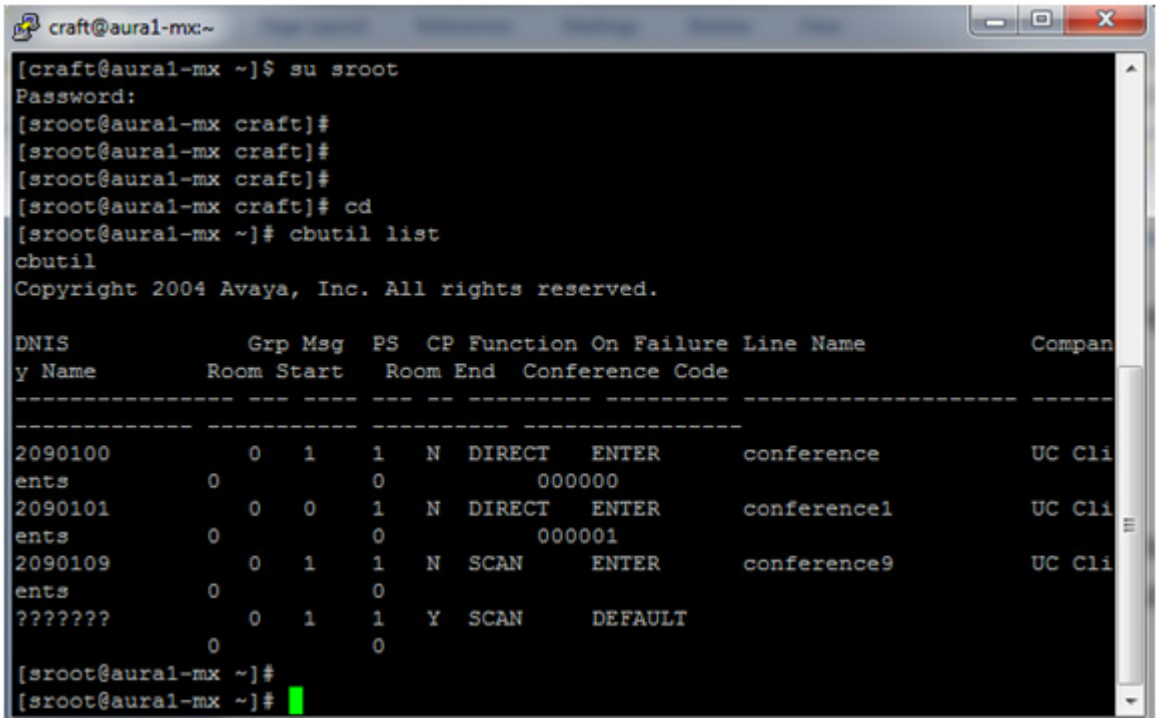
5. Save the settings.

Note:

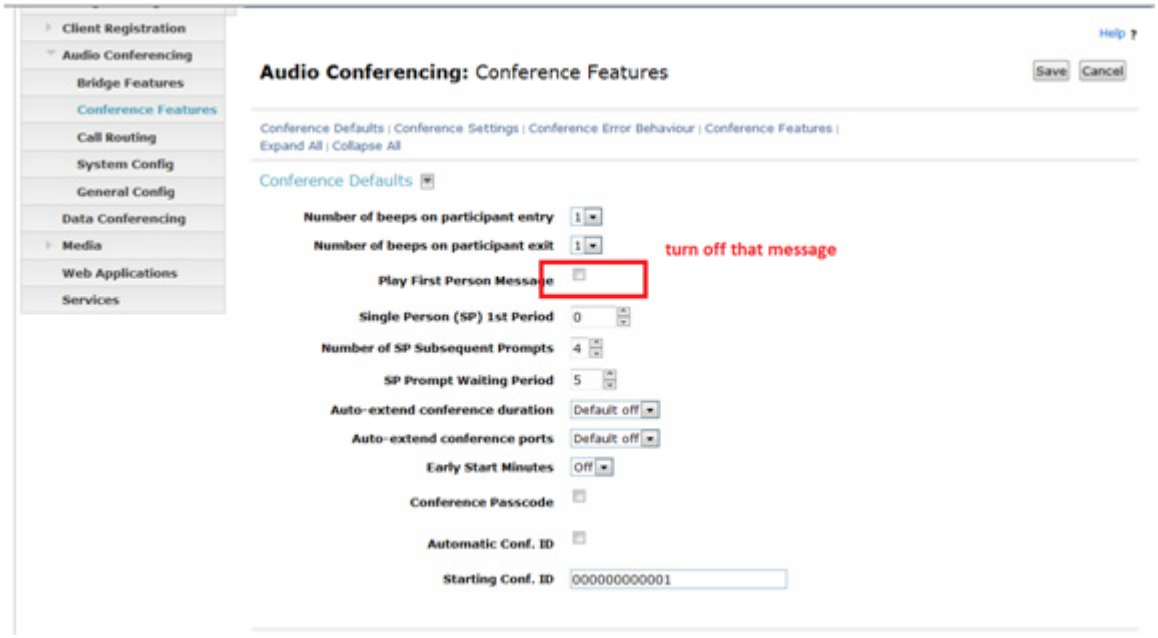
In the present scenario, TMA lab is using conference number 2090101. When using MX to run PTT call, you will require to disable branding when calling to conference

```
SSH to MX craft/craft01 --> su sroot/sroot01

cbutil list
```



cbutil update 2090101 -m 0 (to turn off Avaya branding when call to 2090101)



Glossary

A

ACM	Avaya Communication Manager an Avaya PBX
AIWS	Avaya In-Building Wireless Server Module that enables wireless services to and from the portable devices.
AIWS2	An application running on an ELISE3 module, that enables wireless services to and from portable devices and chargers. In this document, Unite application refers to AIWS2.

B

BPC	Battery Pack Charger

C

Central Phonebook	A Phonebook stored in a database in the control module or reached from the control module.
CM	Communication Manager an Avaya PBX, synonymous for Avaya Communication Manager
Company Phonebook	A Phonebook that is configured in and uploaded to a telephone from the Device Manager. The entries are locked for editing.
Contacts	The name of the phonebook in a cordless telephone.
CSV	Comma Separated Value: A file containing data separated by commas.

D

DECT	Digital Enhanced Cordless Telecommunications: A global standard for cordless telecommunication.
Device Manager	PDM System version running on an AIWS2, for management of portable devices, charging racks, etc.
DGH	Device Group Handler
DH	Device handler
DHCP	Dynamic Host Configuration Protocol a protocol for automating the configuration of computers that use TCP/IP
DTMF	Dual Tone Multiple-Frequency

E

Elise 2 Server	Embedded LInux SErver: A hardware platform used for AIW.

F

FER	Frame Error Rate
FTP	File Transfer Protocol

G

GAP	Generic Access Profile: communication protocol standard within DECT, that guarantees compatibility of systems and components
GoS	Grade of Service
GUI	Graphical User Interface

I

IP	Internet Protocol:
IPBL	IP-DECT (Blade) Gateway
IPBS	IP-DECT Base Station
IPDI	International Portable DAM Identity (DECT Authentication Module) for the DECT registration, where DAM stands for (DECT Authentication Module). IPDI is exchanged between handsets during the Easy replacement procedure.
IPEI	International Portable part Equipment Identity: The unique global GAP identity number for the handset. This code is needed for the system administrator to enable network subscription.
IPO	IP Office an Avaya PBX
ISDN	Integrated Services Digital Network

J

JRE	Sun Java Runtime Environment

L

LAN	Local Area Network: a group of computers and associated devices that share a common communication line.
LDAP	Lightweight Directory Access Protocol

N

Number	*PDM, AIS:* Settings for the complete set of parameters of a single device, tied to a specific identity.
NTP	Network Time Protocol a standard for synchronization of clocks via packet-based communication networks.

O

OAP	Open Access Protocol: XML based protocol used to create customized applications for Unite access.
OTA	Over The Air

P

PBX	Private Branch Exchange: telephone system within an enterprise that switches calls between local lines and allows all users to share a certain number of external lines.
PDM	Portable Device Manager
PKCS#12	A cryptography standard, defining a file format used to store keys and certificates.
PoE	Power over Ethernet
Portable, Portable device	In this document a portable device or portable means cordless telephone.
PSTN	Public Switched Telephone Network
PSCN	Primary receiver Scan Carrier Number: defines the RF carrier on which one receiver will be listening on the next frame.

Q

QoS	Quality of Service
QSIG	Q-signalling: a set of standards defined by ECMA, ESTI and ISO for connection PBX to PBX in networks.

R

RFP	Radio Fixed Part. DECT base-station part of the DECT Infrastructure.
RFPI	Radio Fixed Part Identity.
RSSI	Radio Signal Strength Information
RS232	Industry standard serial communication protocol
RTP	Real-Time Transport Protocol

S

SIP	Session Initiation Protocol
Site	Contains information of devices and Numbers
SMS	Short Message Service: global protocol for sending messages between cordless telephones.
SST	Site Survey Tool

T

ToS	Type of Service

U

UNS	Unite Name Server
USB	Universal Serial Bus a serial bus standard to interface devices, for example connect computer peripherals such as mice, keyboards, scanners etc.
User ID	User ID identifies the set of user parameters possible to save and administrate via PDM. It can be moved together with user parameters between telephones. It is normally set automatically at DECT subscription to be equal to call number.

V

VoIP	Voice over IP
VoWiFi	Voice over Wireless Fidelity: is a wireless version of VoIP and refers to IEEE 802.11a, 802.11b or 802.11g network.

W

WiFi	WiFi stands for Wireless Fidelity and is a term developed by the Wi-Fi Alliance® to describe wireless local area network (WLAN) products that are based on the Institute of Electrical and Electronics Engineers' (IEEE) 802.11 standards. Today, most people use WiFi as a reference to wireless connectivity.
WSM	see *AIWS*

Related documents

User Manual, Avaya 3725 DECT Telephone	21-603358
User Manual, Avaya 3720 DECT Telephone	21-603360
Function Description, IP-DECT System for Avaya	21-603368
User Manual, Avaya 3740, 3745, and 3749 DECT Telephones	21-603690
Avaya DECT System Description	21-604149

Index

A

Absence Handling 474
Assign a Number 343, 420
Associate a Number 338, 414
Audio adjustment 236
Authentication Levels 378

C

Characters for SMS 245
Charging 293
Clear lists 229
colour coding 329
Communication cable connection 306
Communication Manager 39
Company Phonebook 219
Compliance 283, 297
Configuration 366
Configuring PTT 705
Customize GUI 226

D

database 315
DECT Frequency Band configuration 151
Default Category 466
description of selected parameter 323, 337, 412
Device Manager 397
Devices 401
DHCP 307
Digit manipulation 449
Disk Status 702

E

Easy Replacement 211, 277
Easy replacement 269
Emergency Call Number 232
error 354, 691
Error Relay 519
EU Compliance,Elise 2 Server 524, 560
Export Contacts 341

F

Factory reset 210, 343
FCC Compliance,Elise 2 Server 524, 559
File management 347
File types 521
Firewall 693
firewall 691
Function Indicator 519

G

Glossary 719

H

Headset configuration 236

I

Import Contacts 340
Installation 285, 299
Installing 88
IP Statistics 702
IPBL 38
IPBS 38
IPDI 244
IPEI 244

L

Languages 350
LDAP Parameter Setup 446
LED 278, 312
LED indications 245
Licence 472
License 383
Log 702
Logging 468

M

MAC Address 383
Module Fault List 702
Module Key 383
Mounting 286, 300
Multiple frequency support 151
Multiple WSM 369
My Groups 498

N

Netpage 494
Network Settings 471
Number list 496
Numbers 402

O

Open Access Protocol 504
Operating mode 466
Own Line Settings 225
Owner identification 237

P

parameter definition file 347
parameters 307, 317
Phonebook 350
Phonebook Administration 390
Power Down 366
Powering 87
Profiles 237
Properties 344
Protect registration 232
PTT 237

R

Reboot 472
Remote Management 474
replace a device 419
reset 312, 690
Restart 366
RSTP 142
Run template 413

S

Send Test Message 702
Set time 470
Shortcuts 240
site database 317, 334, 341, 353
Site Survey tool menu 244
software . 327, 330, 331, 349, 401, 402, 433, 692
Software Version 383
System Information 702

T

Tabs 400
Telephone charging 310
Telephone disconnection 310
Templates 403
Time Settings 469
Tools 286, 300
Troubleshooting 293

U

UNS 465
Upgrade a telephone 210
USB port 316, 325, 691
User ID 244

W

web messaging 494