Making Innovation Thrive™

Dialogic® Diva® SIPcontrol™ Software 2.1.2

Reference Guide

April 2010 206-477-09

www.dialogic.com

Copyright and Legal Notice

Copyright © 2007-2010 Dialogic Corporation. All Rights Reserved. You may not reproduce this document in whole or in part without permission in writing from Dialogic Corporation at the address provided below.

All contents of this document are furnished for informational use only and are subject to change without notice and do not represent a commitment on the part of Dialogic Corporation or its subsidiaries ("Dialogic"). Reasonable effort is made to ensure the accuracy of the information contained in the document. However, Dialogic does not warrant the accuracy of this information and cannot accept responsibility for errors, inaccuracies or omissions that may be contained in this document.

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH DIALOGIC® PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN A SIGNED AGREEMENT BETWEEN YOU AND DIALOGIC, DIALOGIC ASSUMES NO LIABILITY WHATSOEVER, AND DIALOGIC DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF DIALOGIC PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY INTELLECTUAL PROPERTY RIGHT OF A THIRD PARTY.

Dialogic products are not intended for use in medical, life saving, life sustaining, critical control or safety systems, or in nuclear facility applications.

Due to differing national regulations and approval requirements, certain Dialogic products may be suitable for use only in specific countries, and thus may not function properly in other countries. You are responsible for ensuring that your use of such products occurs only in the countries where such use is suitable. For information on specific products, contact Dialogic Corporation at the address indicated below or on the web at www.dialogic.com.

It is possible that the use or implementation of any one of the concepts, applications, or ideas described in this document, in marketing collateral produced by or on web pages maintained by Dialogic may infringe one or more patents or other intellectual property rights owned by third parties. Dialogic does not provide any intellectual property licenses with the sale of Dialogic products other than a license to use such product in accordance with intellectual property owned or validly licensed by Dialogic and no such licenses are provided except pursuant to a signed agreement with Dialogic. More detailed information about such intellectual property is available from Dialogic's legal department at 9800 Cavendish Blvd., 5th Floor, Montreal, Quebec, Canada H4M 2V9. **Dialogic encourages all users of its products to procure all necessary intellectual property licenses required to implement any concepts or applications and does not condone or encourage any intellectual property infringement and disclaims any responsibility related thereto. These intellectual property licenses may differ from country to country and it is the responsibility of those who develop the concepts or applications to be aware of and comply with different national license requirements.**

Dialogic, Dialogic Pro, Brooktrout, Cantata, SnowShore, Eicon, Eicon Networks, Eiconcard, Diva, SIPcontrol, Diva ISDN, TruFax, Realblocs, Realcomm 100, NetAccess, Instant ISDN, TRXStream, Exnet, Exnet Connect, EXS, ExchangePlus VSE, Switchkit, N20, Powering The Service-Ready Network, Vantage, Making Innovation Thrive, Connecting People to Information, Connecting to Growth and Shiva, among others as well as related logos, are either registered trademarks or trademarks of Dialogic. Dialogic's trademarks may be used publicly only with permission from Dialogic. Such permission may only be granted by Dialogic's legal department at 9800 Cavendish Blvd., 5th Floor, Montreal, Quebec, Canada H4M 2V9. Any authorized use of Dialogic's trademarks will be subject to full respect of the trademark guidelines published by Dialogic from time to time and any use of Dialogic's trademarks requires proper acknowledgement.

Internet Explorer, Microsoft, Windows, Windows Server, and Windows Vista are registered trademarks of Microsoft Corporation in the United States and/or other countries. Other names of actual companies and products mentioned herein are the trademarks of their respective owners.

This document discusses one or more open source products, systems and/or releases. Dialogic is not responsible for your decision to use open source in connection with Dialogic products (including without limitation those referred to herein), nor is Dialogic responsible for any present or future effects such usage might have, including without limitation effects on your products, your business, or your intellectual property rights.

Software License Agreement

This Software License Agreement ("Agreement") is a legal Agreement for the conditional use of the software provided herein ("Program") between you, the end-user, whether an individual or a company and all of its authorized users of the Program ("You"), and Dialogic Corporation ("Dialogic"). By downloading, copying or otherwise using the Program, You agree to be bound by the terms of the foregoing license.

YOU ASSUME RESPONSIBILITY FOR THE SELECTION OF THE PROGRAM TO ACHIEVE YOUR INTENDED RESULTS, AND FOR THE INSTALLATION, USE, AND RESULTS OBTAINED FROM THE PROGRAM.

The Program may contain certain software applications and portions of applications which are provided to You under terms and conditions which are different from this Agreement (such as open source or community source), or which require Dialogic to provide Customer and its Subsidiaries with certain notices and/or information (“Excluded Code”). Dialogic will identify such Excluded Code in a text file or about box or in a file or files referenced thereby (and shall include any associated license agreement, notices and other related information therein), or the Excluded Code will contain or be accompanied by its own license agreement. Your use of the Excluded Code will be subject to the terms and conditions of such other license agreement solely to the extent such terms and conditions are inconsistent with the terms and conditions of this Agreement or are required by such other license agreement. By using or not uninstalling such Excluded Code after the initial installation of the Excluded Code You acknowledge and agree to all such license agreements, notices and information.

License

Under the terms and conditions of this Agreement:

- You may install and use one copy of the Program on a single-user computer, file server, or on a workstation of a local area network.
- Some or all functions of the Program may be available solely if the Program is used with one or more legally acquired Dialogic Activation Key(s).
- To obtain an Activation Key You must first purchase a Proof of Purchase Code (PPC). A PPC may be included in Your software or hardware package or You may have to purchase it separately.
- You will receive Your Activation Key upon registering the Proof of Purchase Code as directed in the PPC document.
- It may be possible to install multiple Activation Keys into the Program; in such a case, the total functionality provided by the Program will be the sum of the licensed functionalities controlled by the installed Activation Keys as long as the maximum capabilities of the Program are not exceeded and the functionalities are compatible.
- Your Activation Key(s) will restrict Your use of the Program. At least one of the following restriction schemes will be available to You when You register each PPC and request an Activation Key.
  - The Activation Key may be associated with a specific Dialogic hardware device. In this case, the licensed functionality controlled by the Activation Key will be available solely if the same Dialogic hardware is present in the computer. You can move the Program to another computer solely if You move the specified Dialogic hardware to the new computer.
  - The Activation Key may be associated with a specific Dialogic-supplied software protection device (‘dongle’). In this case, the licensed functionality controlled by the Activation Key will be available solely if the same dongle is present in the computer. You can move the Program to another computer solely if You also move the dongle to the new computer.
  - The Activation Key may be associated with Your specific computer hardware platform. In this case, the licensed functionality controlled by the Activation Key will be available solely if no significant change is made to the hardware installed in the computer. Replacement Activation Keys may be issued at the discretion of Dialogic solely if Dialogic can determine that You have not moved the Program to another computer. Sufficient information must be provided to Dialogic to allow it to make that determination.
- In addition to the above restrictions, each Activation Key may have a specific term of use commencing from the date of PPC registration. In this case, the licensed functionality controlled by the Activation Key will not be available after the Activation Key has expired.
- The Activation process requires that You enter the following information into the web-based system to obtain an Activation Key:
  - PPC
  - The Device ID provided to You by the "Activation" function in the Program
  - Your email address so that the Activation Key can be delivered to You by email
- Dialogic will retain the information above for the following purposes:
  - Validation of future requests from You for replacement Activation Keys
  - Sending renewal reminders to You in the case of limited time licenses.
- If the Dialogic hardware device that Activation Keys are associated with is judged to be defective by Dialogic following its standard practices, Dialogic's Support department will issue to You replacement Activation Keys associated with the replacement device upon receipt of the faulty device by Dialogic. Replacement of the faulty device is subject to the terms

of Dialogic's standard Hardware product Warranty in effect at the time You purchased the hardware product concerned ("Hardware Warranty"). If a valid Advance Replacement Insurance policy contract is in place for the Dialogic hardware product concerned, Dialogic will endeavor to expedite provision of Activation Keys associated with the replacement device.

- If the Dialogic-supplied software protection device (a "dongle" or "USB-stick") that Activation Keys are associated with is judged to be defective by Dialogic following its standard practices, Dialogic Support will issue to You replacement Activation Keys associated with the replacement device upon receipt by Dialogic of the failed device. Replacement of the faulty device is subject to the terms of Dialogic's Hardware Warranty.
- You may copy the Program into any machine readable or printed form for backup in support of Your use of one copy of the Program;
- You may make one copy of Dialogic's documentation provided that all copyright notices contained within the documentation are retained;
- You may transfer the Program, documentation and the license to another eligible party within Your Company if the other party agrees to accept the terms and conditions of this Agreement. If You transfer the Program and documentation You must at the same time either transfer all copies whether in printed or machine readable form to the same party or destroy any copies not transferred;
- You may not rent or lease the Program. You may not reverse engineer, decompile or disassemble the Program. You may not use, copy, modify or transfer the Program and documentation, or any copy, modification or merged portion, in whole or in part, except as expressly provided for in this Agreement;
- You may not modify the Program in order to circumvent or subvert the protection mechanisms inherent in the program or attempt to use a time-limited Activation Key after it has expired;
- If You transfer possession of any copy, modification or merged portion of the Program or documentation to another party in any way other than as expressly permitted in this Agreement, this license is automatically terminated.

Term

The license is effective until terminated. You may terminate it at any time by destroying the Program and documentation together with all copies, modifications and merged portions in any form.

It will also terminate upon conditions set forth elsewhere in this Agreement or if You fail to comply with any terms or conditions of this Agreement at any time. You agree upon such termination to destroy the Program and documentation together with all copies, modifications and merged portions in any form.

Limited Warranty

The only warranty Dialogic makes, beyond the replacement of Activation Keys under the terms set out above, is that the medium on which the Program is recorded will be replaced without charge if Dialogic, in good faith, determines that it was defective in materials or workmanship and if returned to Your supplier with a copy of Your receipt within ninety (90) days from the date You received it. Dialogic offers no warranty for Your reproduction of the Program. This Limited Warranty is void if failure of the Program has resulted from accident, misuse, abuse or misapplication.

Customer Remedies

Dialogic's entire liability and Your and Your Authorized Users exclusive remedy shall be, at Dialogic's option, either (a) return of the price paid or (b) repair or replacement of the Program that does not meet the above Limited Warranty. Any replacement Program will be warranted for the remainder of the original Warranty period.

No Other Warranties

Dialogic disclaims all other warranties, either express or implied, including but not limited to implied warranties or merchantability and fitness for a particular purpose and the warranty against latent defects, with respect to the Program and the accompanying documentation. This limited warranty gives You specific legal rights. You may have others, which may vary from jurisdiction to jurisdiction.

No Liability for Consequential Damage

In no event shall Dialogic, its affiliates or its suppliers or their officers, directors or employees be liable for any damages whatsoever (including without limitation, damages for loss of business profits, business interruption, loss of information, or other pecuniary loss and indirect, consequential, incidental, economic or punitive damages) arising out of this Agreement or the use of or inability to use this Program, even if Dialogic has been advised of the possibility of such damages. As some jurisdictions do not allow the exclusion or limitation for certain damages, some of the above limitations may not apply to You or Your Authorized Users.

Limit of Liability

Dialogic's entire aggregate liability under any provision of this Agreement shall be limited to the amount actually paid by You for the affected Program.

Right to Audit

If this Program is licensed for use in a Company, Your Company agrees to keep all usual and proper records and books of accounts and all usual proper entries relating to each installation of the Program during the term of this Agreement and for a period of three (3) years thereafter. During this period, Dialogic may cause an audit to be made of the applicable records and of the installations of the Program in order to verify Your compliance with this Agreement and prompt adjustment shall be made to compensate for any errors or omissions disclosed by such audit. Any such audit shall be conducted by an independent certified public accountant selected by Dialogic and shall be conducted during the regular business hours at Your offices and in such a manner as not to interfere with Your normal business activities. Any such audit shall be paid for by Dialogic unless material discrepancies are disclosed.

For such purposes, 'material discrepancies' shall mean the Company exceeding by three percent (3%) or more the number of licensed channels for any function of the Program or the Company exceeding the licensed number of Authorized Users by three percent (3%) or more. If material discrepancies are disclosed, Your Company agrees to pay Dialogic for the costs associated with the audit as well as the license fees for the additional licensed channels or additional Authorized Users. In no event shall audits be made more frequently than semi-annually unless the immediately preceding audit disclosed a material discrepancy.

Supplementary Software

Any Supplementary Software provided with the Dialogic Program referred to in this License Agreement is provided "as is" with no warranty of any kind.

U.S. Government Restricted Rights

The Program and documentation are provided with RESTRICTED RIGHTS. Use, duplication or disclosure by the U.S. Governments is subject to restrictions as set forth in subparagraph c) 1) ii) of The Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 or subparagraph c) 1) and 2) of the Commercial Computer Software-Restricted Rights at 48 CFR52.227-19, as applicable.

Governing Law

This Agreement shall be construed and controlled by the laws in force in the Province of Quebec, Canada with the exception of its conflict of laws rules. The United Nations Convention on Contracts for the Sale of Goods does not apply to this Agreement.

Miscellaneous

All rights and remedies, whether conferred hereunder or by any other instrument or law, will be cumulative and may be exercised singularly or concurrently. Failure by either Dialogic or You to enforce any term will not be deemed a waiver of future enforcement of that or any other term. The terms and conditions stated herein are declared to be severable. Should any term(s) or condition(s) of this Agreement be held to be invalid or unenforceable the validity, construction and enforceability of the remaining terms and conditions of this Agreement shall not be affected. You may not assign any rights, duties or obligations hereunder without the prior written approval of Dialogic and any attempt to assign any rights, duties or obligations hereunder without Dialogic's written consent will be void. It is expressly agreed that Dialogic and You are acting as independent contractors. These terms and conditions constitute the entire agreement between Dialogic and You with respect to the subject matter hereof. These terms and conditions will prevail notwithstanding any different, conflicting or additional terms and conditions that may appear on any other agreement between Dialogic and You. Deviations from these terms and conditions are not valid unless agreed to in writing in advance by an authorized representative of Dialogic. Any notice to Dialogic under this Agreement must be sent by courier or registered mail to the attention of Dialogic's legal department at the address below.

Contractor/ manufacturer is:

DIALOGIC CORPORATION.

9800 Cavendish Blvd., Montreal, Quebec, Canada H4M 2V9

This Agreement has been drafted in English at the express wish of the parties. Ce contrat a été rédigé en anglais à la demande expresse des parties.

Contents

About This Publication

How to use this online guide

- To view a section, click the corresponding bookmark located on the left.
- To view a topic that contains further information, click the corresponding blue underlined phrase.
- You may wish to print out the pages required for installing the drivers.

Structure of this guide

This guide is structured as follows:

Section	Contents
About the Dialogic® Diva® SIPcontrol™ Software	General information about the Diva SIPcontrol software, general features, supported Dialogic® Diva® Media Boards, and supported operating systems
Software Installation	Installation of the Diva SIPcontrol software with the setup wizard
License Activation	Activation of the license on the Dialogic activation web site
Dialogic® Diva® SIPcontrol™ Software Configuration	Overview of configuration parameters
How Calls Are Processed	Description of the processing of calls
How Call Addresses Are Processed	Description of the processing of call addresses
How Address Maps Are Processed	Description of the processing of address maps
How Numbers Are Processed	Description of the number normalization with the Diva SIPcontrol software
Software Uninstallation	Uninstallation of the Diva SIPcontrol software
Cause Code Mapping	Description of Cause Code mappings, Error codes, and Routing Examples
Event Logging	Overview of events written into the system event log
Use Case Examples	Description of the Diva SIPcontrol software configuration with the Dialogic Host Media Processing (HMP) software
Customer Service	Information on how to get technical support for Dialogic® Diva® products

CHAPTER 1

About the Dialogic® Diva® SIPcontrol™ Software

The Diva SIPcontrol software is a gateway that translates call control information from the PSTN into SIP messages and vice versa. The Diva SIPcontrol software is installed on top of a Dialogic® Diva® Media Board, allowing the Diva board to be used as a SIP gateway within the computer or server that hosts the media server platform. The Diva SIPcontrol software is delivered with a default license for the simultaneous use of two channels.

Feature Overview

New features in Dialogic® Diva® SIPcontrol™ Software version 2.1.2:

- Support for Dialogic® Diva® V-8PRI PCIe FS Media Boards

General features

- Support for Microsoft® Office Communications Server 2007 Release 2
- Noise suppression support
- Echo cancellation selectable via GUI
- Forward the display name from SIP to Q.SIG and vice versa
- Diva SIPcontrol software update via web interface
- Interoperability with Dialogic® Host Media Processing (HMP) software 3.0WIN and 3.1LIN
- Configuration via web interface
- Standard web browsers can be used for configuring. The Dialogic® Diva® SIPcontrol™ Software has been tested with the following browsers:
  - Microsoft® Internet Explorer® version 6 and 7
  - Mozilla Firefox version 2.0 and 3.0
- Remote configuration of the Diva SIPcontrol software from any computer in the network
- Cause codes: Configurable translation of ISDN cause code to SIP response code and vice versa; consequently, the Diva SIPcontrol software can adapt to the specific behavior of the PSTN, PBX, and/or SIP peer.
- Configuration changes during runtime: Modify most parameters of the Diva SIPcontrol software without the need to restart the service; active calls are not affected by configuration updates and continue undisturbed.
- Support for North American numbering plan: The configuration of multiple area codes is handled as local. Therefore, the Dialogic® Diva® SIPcontrol™ Software dialplan engine is able to automatically format dialed numbers according to local phone provider requirements without any additional regular expressions.
- Interoperability with the Dialogic® Brooktrout® Bfv API SDK: The Dialogic® Brooktrout® SR140 Fax Software version 5.2.1 has been confirmed via testing to be V.34/T.38 interoperable with the Diva SIPcontrol software. The Brooktrout SR140 Fax Software is high-performance, host-based T.38 fax software for IP networks.
- Codec configuration: Configuration options for supported audio and fax codecs. See Media processing on page 10 for supported codecs.
- Support for Proxy and Registrar authentication
- Support for registering the Diva SIPcontrol software as an e-phone gateway
- Support for Early Media: Early Media is supported for calls from SIP to the PSTN. For calls from the PSTN to SIP, it depends on the used line protocol.
- Configuration of Dialogic® Diva® Media Board parameters via the web interface
- Interoperability with the Dialogic® Host Media Processing (HMP) software
- Support for up to 64 ports per system for Dialogic® Diva® BRI and Analog Media Board installations
- Support for up to 240 ports per system for Dialogic® Diva® PRI Media Board installations

Call handling

- SIP methods: ACK, BYE, INVITE, NOTIFY*, REFER, CANCEL, OPTIONS, PRACK
- Configurable IP transport layer TCP, UDP, or TLS
- Support for TLS and SSL encryption and authentication
- Support for SRTP (secure Real-time Transport Protocol)
- Support for SIPS (Secure SIP)
- Basic call incl. numbering services:
  - Called Party Number
  - Calling Party Number
  - Redirecting Number
- Call Routing
- Call Hold/Retrieve (e.g., Re-Invite mapping towards ISDN)
- PSTN-side Call Transfer (i.e., Refer points to PSTN)
- PSTN-side incoming Call Diversion
- Message Waiting Activation / Deactivation
- Support of REDIRECT (Moved Temporarily)
- SIP Session Timer (RFC 4028)
- Simplified Number Normalization based on PSTN connection parameters
- Number Manipulation using Regular Expressions

* NOTIFY in combination with SUBSCRIBE are used to provide the feature Message Waiting Activation / Deactivation with regular SIP clients. However, in a gateway configuration applications are using the features without the need for the Dialogic® Diva® SIPcontrol™ software to use SUBSCRIBE.

Media processing

- Support for the following codecs:
  - G.711 A-law and u-law
  - G.726 (16, 24, 32, and 40 kbps)
  - G.729
  - GSM-FR
  - iLBC

Note: For G.729, you need to purchase and activate a license before you can use it. See License Activation on page 16 for more information.

Note: iLBC is only available on Dialogic® Diva® V-2PRI PCI, V-4PRI PCI, V-1PRI PCIe HS, V-2PRI PCIe HS, and V-4PRI PCIe FS Media Boards. On Dialogic® Diva® V-4PRI PCIe HS Media Boards, only up to 72 channels are supported.

- RTP dynamic payload audio/telephony event
- RTP profile RTP/AVP
- DTMF via RTP payload/telephony event (RFC 2833)
- PSTN-side fax tone detection via RTP event (RFC 2833)
- Echo Canceller with 128 ms echo tail used with RTP (On some Diva Media Boards up to 256 ms. See the Dialogic® Diva® System Release Reference Guide for more information.)
- T.38 Fax up to V.34 (SuperG3 Fax)

Reliability

- Load balancing and failover on PSTN side
- Load balancing and failover on SIP side (optionally uses OPTIONS for keep-alive check)
- Alive check for active calls on SIP side via SIP session timer

Supported RFCs

- RFC2617 - HTTP Digest Authentication
- RFC2833 - RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals
- RFC3261 - Session Initiation Protocol
- RFC3262 - Reliability of Provisional Responses in Session Initiation Protocol (SIP)
- RFC3264 - An Offer/Answer Model with Session Description Protocol
- RFC3265 - SIP-specific Event Notification
- RFC3326 - The Reason Header Field for the Session Initiation Protocol (SIP)
- RFC3389 - RTP Payload for Comfort Noise
- RFC3398 - ISDN to SIP mapping
- RFC3420 - Internet Media Type message/sipfrag
- RFC3515 - REFER method
- RFC3550 - Realtime Transport Protocol (RTP)
- RFC3551 - RTP/AVP profile
- RFC3711 - The Secure Real-time Transport Protocol (SRTP)
- RFC3842 - Message Waiting Indication for SIP
- RFC3891 - SIP "Replaces" header
- RFC3892 - SIP Referred - By Mechanism
- RFC3951 - Internet Low Bit Rate Codec (iLBC)
- RFC3952 - Real-time Transport Protocol (RTP) Payload Format for internet Low Bit Rate Codec (iLBC) Speech
- RFC3960 - Early Media and Ringing Tone Generation in the Session Initiation Protocol (SIP), only gateway model
- RFC4028 - Session Timers in SIP
- RFC4497 - Interworking between SIP and QSIG
- RFC4566 - Session Description Protocol (SDP)
- RFC4568 - SDP Security for Media Streams
- Draft: Diversion Indication in SIP (draft-levy-sip-diversion-08)

Enhanced routing

- Defines which CAPI controller is used for which calls from SIP
- Increased flexibility of load balancing and failover functionality; load balancing and failover can be used together and are available for calls to the PSTN as well
- Number-based routing also available for calls to the PSTN
- Matching rules for number-based routing can contain regular expressions
- Routing based on calling or redirected number, the redirected number is only available for calls from the PSTN

Enhanced address manipulation

- Define the number manipulation on three different stages of the call routing (inbound, route selection, outbound)
- Unlimited number of regular expressions for number manipulation at each stage of call routing
- Different dialplans can be entered for each controller and each SIP peer, which can ease the deployment in an environment with multiple locations

Supported hardware

The Dialogic® Diva® SIPcontrol™ software supports the following Dialogic® Diva® Media Boards (up to 240 channels are supported):

Dialogic® Diva® BRI Media Boards

- Diva BRI-2 PCI v2
- Diva BRI-2 PCIe v2
- Diva 4BRI-8 PCI v2
- Diva 4BRI-8 PCIe v2
- Diva V-BRI-2 PCI v2[1)]
- Diva V-BRI-2 PCIe v2[1)]
- Diva V-4BRI-8 PCI v2[1)]
- Diva V-4BRI-8 PCIe v2[1)]
- Diva UM-BRI-2 PCI v2
- Diva UM-BRI-2 PCIe v2
- Diva UM-4BRI-8 PCI v2
- Diva UM-4BRI-8 PCIe v2

Dialogic® Diva® PRI Media Boards

Diva PRI:

- Diva PRI/T1-24 PCI v3
- Diva PRI/T1-24 PCIe v3
- Diva PRI/E1-30 PCI v3
- Diva PRI/E1-30 PCIe v3

Diva UM-PRI:

- Diva UM-PRI/T1-24 PCI v3
- Diva UM-PRI/T1-24 PCIe v3
- Diva UM-PRI/E1-30 PCI v3
- Diva UM-PRI/E1-30 PCIe v3

Diva V-PRI:

- Diva V-PRI/T1-24 PCI v3
- Diva V-PRI/T1-24 PCIe v3
- Diva V-PRI/E1-30 PCI v3
- Diva V-PRI/E1-30 PCIe v3

Diva Multiport V-PRI:

- Diva V-2PRI/T1-48 PCI v1
- Diva V-2PRI/E1-60 PCI v1
- Diva V-4PRI/T1-96 PCI v1
- Diva V-4PRI/E1-120 PCI v1
-
- Diva V-1PRI/E1/T1-30 PCIe HS v1
- Diva V-2PRI/E1/T1-60 PCIe HS v1
- Diva V-4PRI/E1/T1-120 PCIe HS v1
- Diva V-4PRI/E1/T1-120 PCIe FS v1
- Diva V-8PRI/E1/T1-240 PCIe FS v1

Note: “HS” stands for the half size and “FS” for the full size board format.

Dialogic® Diva® Analog Media Boards

- Diva Analog-2 PCI v1
- Diva Analog-2 PCIe v1
- Diva Analog-4 PCI v1
- Diva Analog-4 PCIe v1
- Diva Analog-8 PCI v1
- Diva Analog-8 PCIe v1
- Diva V-Analog-4 PCI v1[1)]
- Diva V-Analog-4 PCIe v1[1)]
- Diva V-Analog-8 PCI v1[1)]
- Diva V-Analog-8 PCIe v1[1)]
- Diva UM-Analog-4 PCI v1
- Diva UM-Analog-4 PCIe v1
- Diva UM-Analog-8 PCI v1
- Diva UM-Analog-8 PCIe v1

[1)] After the installation, the Dialogic® Diva® V-BRI and V-Analog Media Boards are displayed as Dialogic® Diva® UM-BRI and UM-Analog Media Boards.

Supported software

The Dialogic® Diva® SIPcontrol™ Software requires Dialogic® Diva® System Release software version 8.5.8 or higher.

Supported operating systems

The Dialogic® Diva® SIPcontrol™ Software supports the following operating systems (32-bit and 64-bit versions):

- Windows® XP
- Windows Server® 2003
- Windows Vista®
- Windows Server® 2008
- Windows Server® 2008 R2
- Windows® 7

CHAPTER 2

Software Installation

To install the Dialogic® Diva® SIPcontrol™ Software, use the Dialogic® Diva® SIPcontrol™ Setup Wizard as described below:

Notes:

- If you want to upgrade from Diva SIPcontrol software version 1.5.1, DO NOT uninstall the software before you install the Diva SIPcontrol software version 2.1, since if you uninstall the software you might lose some settings, including your regular expressions.
- You must log on with administrator rights to install the Diva SIPcontrol software.
- If install the Diva SIPcontrol software under Windows Vista®, you might be asked for an administration password.

1. Insert your Dialogic® Diva® Media Board into the computer as described in the installation guide that came with your Diva board.
2. Install the Dialogic® Diva® System Release software as described in the Dialogic® Diva® System Release Reference Guide. The Reference Guide is available on the Dialogic web site under: www.dialogic.com/manuals.

   Note: If the correct version of the Diva software (8.5.6 or higher) is not detected during the installation, an error message is displayed and the installation is aborted.
3. Go to the directory in which the Windows® installer package "DSSIPControl.msi" is located and double-click it.
4. In the welcome dialog box, click **Next**.
5. The **End-User License Agreement** box appears. Accept the license agreement to start the installation.
6. If you are upgrading from a former version of the Diva SIPcontrol software and you kept the configuration files, the **Existing configuration found** box appears. Select whether you want to reuse the existing configuration files and click **Next**.
7. The **Ready to Install the Program** box appears. Click **Install** to install the Diva SIPcontrol software.
8. If the installation terminates prematurely, verify that:
   - the installed Diva Media Board is supported; see Supported hardware on page 13 for more information,
   - the correct Diva System Release software is installed; see Supported software on page 14 for more information,
   - the operating system is supported by the Diva SIPcontrol software; see Supported operating systems on page 14 for more information,
   - the CAPI driver is installed correctly, inserted in the Dialogic® Diva® Configuration Manager of the Diva System Release software, and connected to the Diva Media Board.

   If the installation still cannot be completed, contact Dialogic Customer Support personnel under www.dialogic.com/support.
9. After the installation is complete, the **Completing the Diva SIPcontrol Wizard** box appears.
   Click **Finish** to exit the installation.
10. Now, you can configure the settings. To do so, click **Start** > **Programs** > **Dialogic Diva** > **SIPcontrol Configuration**. If you need help during the configuration, click the parameter to display its online help text.

CHAPTER 3

License Activation

The Dialogic® Diva® SIPcontrol™ Software includes a default license for two channels. This license can be used for testing and evaluating the Diva SIPcontrol software.

You must activate a license if you need more than the two channels of the default license included with the Diva SIPcontrol software, or if you want to use G.729 speech compression, V.17 fax, or V.34 fax offered with the installed Dialogic® Diva® Media Board. During the activation process of the license, you need to choose a Diva Media Board to which the license should be bound. After having activated the license for this Diva board, the license cannot be transferred to be used with another Diva board.

Notes:

- Diva SIPcontrol software licenses need to be activated via the web interface as described under To activate the license file on page 18.
- Licenses for G.729, V.17 Fax, and V.34 Fax need to be uploaded and activated in the Dialogic® Diva® Configuration Manager. See the Dialogic® Diva® Configuration Manager Online Help for more information.
- V.17 or V.34 Fax is needed to enable T.38 FoIP support in the Diva SIPcontrol software. It needs to be licensed only for Dialogic® Diva® PRI Media Boards with multiple ports.
- The Dialogic® Host Media Processing (HMP) Software licenses for SIP channels are also valid for SIPcontrol, but they require the Dialogic HMP software to be installed on the same system as the Diva SIPcontrol software.

After purchasing the license, you will need to generate and activate it to unlock functionality in the product.

To activate your license key, you need the following information:

- Device Unique ID (DUID)
- Proof of Purchase Code (PPC)

Once you have both, the DUID and PPC, visit the Dialogic® Diva® Activation site to register your PPC together with the DUID and you will receive your license file. Activate this license file in the Diva SIPcontrol software configuration web interface. For more information, see To activate the license file on page 18.

Device Unique ID (DUID)

The DUID binds the installed Diva SIPcontrol software to your computer (PC fingerprint).

To get the DUID:

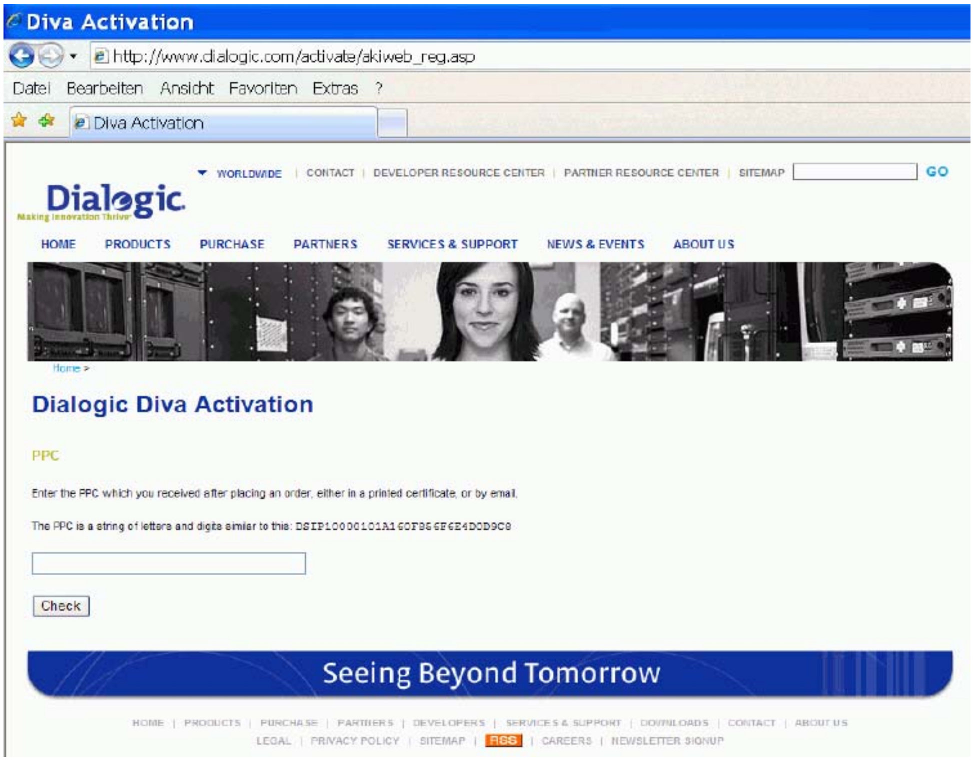
1. Click **Start** > **Programs** > **Dialogic Diva** > **SIPcontrol Configuration** to open the Dialogic® Diva® SIPcontrol™ Software configuration web interface.
2. Click **License Management** on the left side of the Diva SIPcontrol software configuration web interface to open the **License Status** dialog.
3. In the **License Status** dialog, copy the DUID number of the Dialogic® Diva® Media Board you want to activate to the clipboard.
4. If you need to do web activation using another computer, open an editor, paste the DUID, and save the file.

Proof of Purchase Code (PPC)

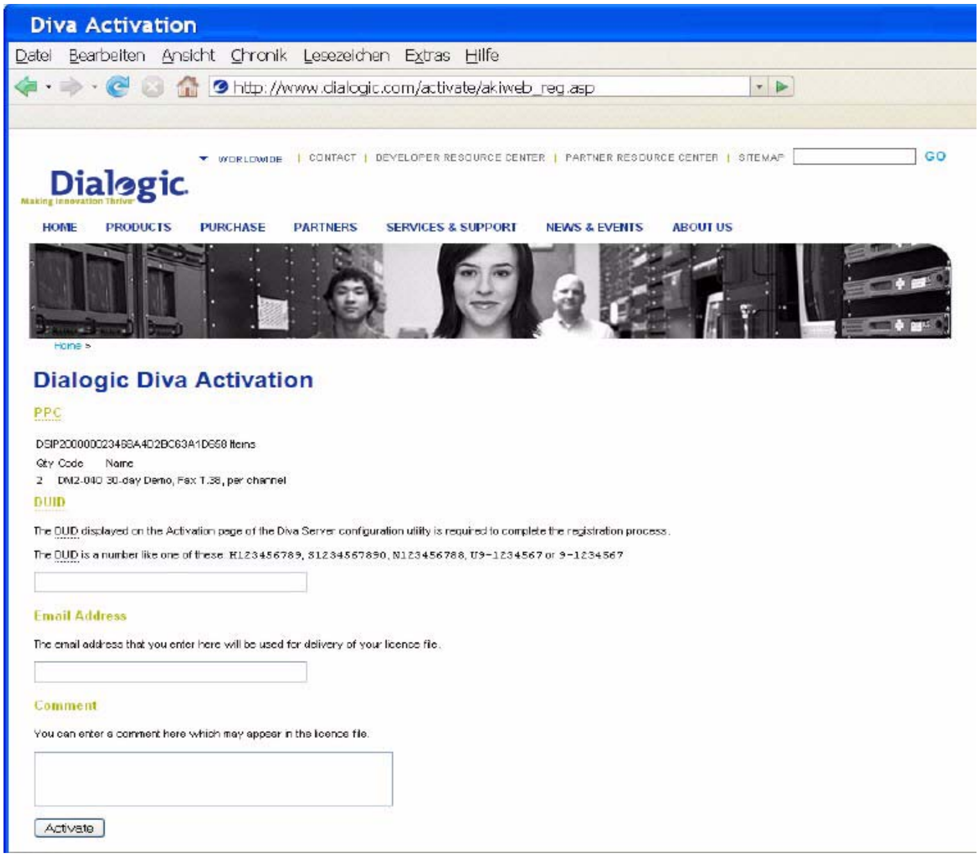
When you purchase the Dialogic® Diva® SIPcontrol™ Software license, you will receive a PPC either in printed form or via email. By registering this PPC, you represent and warrant that you lawfully purchased the license.

To register your PPC and DUID

1. Open the following web site: http://www.dialogic.com/activate.
2. Enter your PPC and click **Check**.



3. If your PPC is valid, the following web site will open:



Paste your Device Unique ID (DUID) that you saved earlier, and enter your email address to which the license file should be sent.

4. Click **Activate** to generate the license file that will be sent to the email address you have entered.
5. Save the license file and activate it. For more information, see To activate the license file below.

To activate the license file

Note: The date set in the system settings of your computer must be correct. Otherwise, you cannot add your license file.

1. Click **License Management** on the left side of the Dialogic® Diva® SIPcontrol™ Software configuration web interface to open the **License Status** dialog.
2. In the **License Status** dialog, click **Browse**, go to the directory in which you saved the license file, and click **Open**.
3. Click **Upload** to activate the license file.

CHAPTER 4

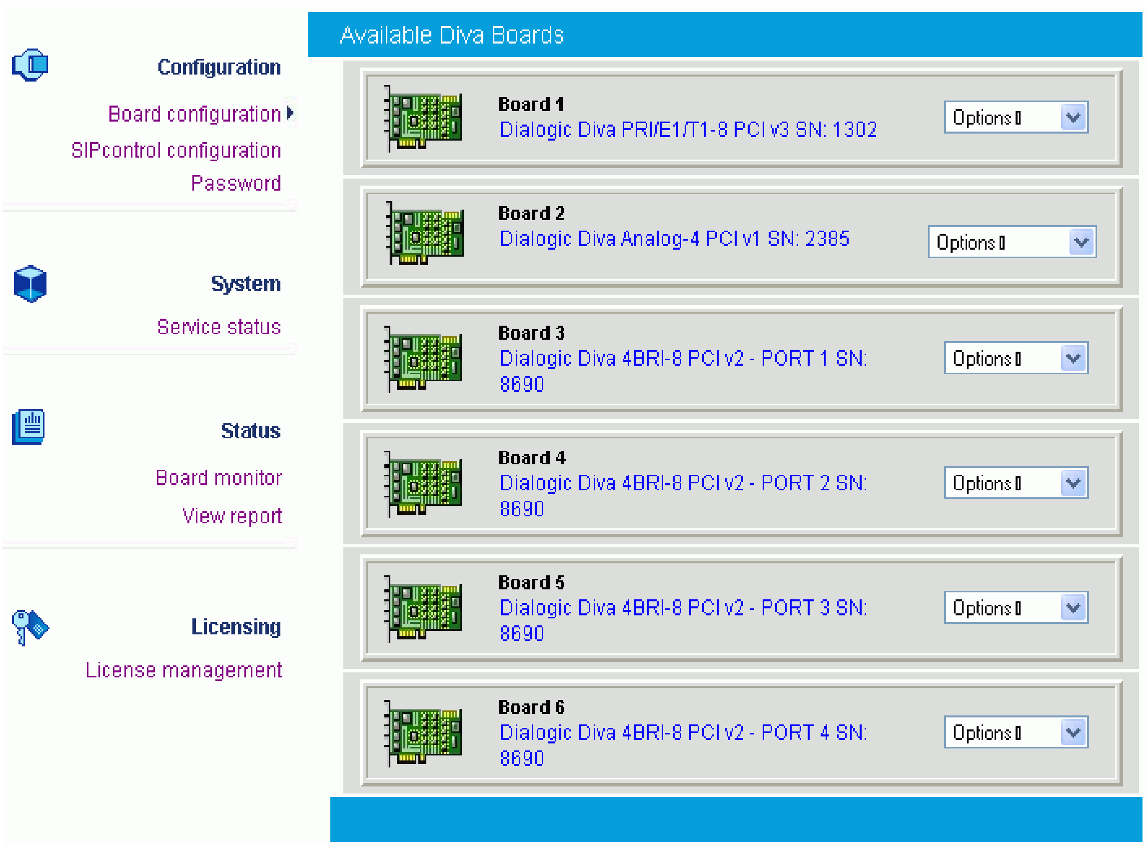
Dialogic® Diva® Media Board Configuration

Since Dialogic® Diva® SIPcontrol™ Software version 1.8, Dialogic® Diva® Media Boards can be configured via the web interface. The configuration via the web interface can be accessed and updated remotely. The classic configuration via the Dialogic® Diva® Configuration Manager is also available, but it can only be accessed from the computer on which the Dialogic® Diva® System Release software is installed. Any changes will be reflected in both configuration tools, meaning that if you change a parameter in the web interface, the change is automatically done in the Diva Configuration Manager as well (and vice versa). The update of the configuration between both tools will only take effect after you have saved the configuration, and, in case of the Diva Configuration Manager, after you activated the configuration. For more information about activating the configuration, see the Dialogic® Diva® Configuration Manager Online Help.

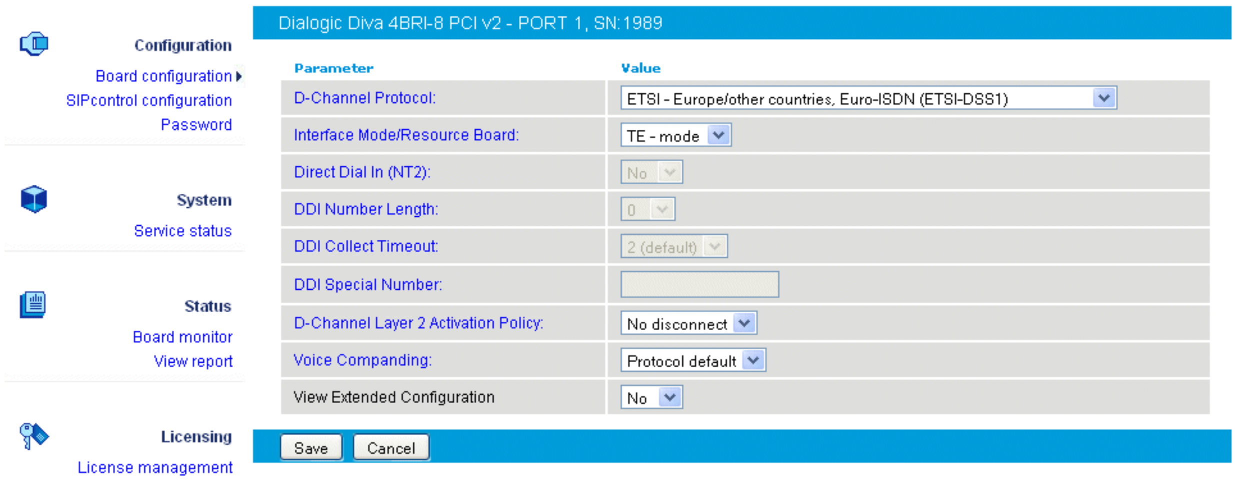
You can find information about the web interface in Dialogic® Diva® SIPcontrol™ Software Configuration on page 26 and in Configuration Tips and Hints on page 27.

Dialogic® Diva® Media Board Configuration via the web interface

1. Click **Start** > **Programs** > **Dialogic Diva** > **SIPcontrol Configuration**.
2. In the Dialogic® Diva® SIPcontrol™ Software web interface, click **Board configuration** on the left hand side. A page displaying all installed Diva Media Boards will open:

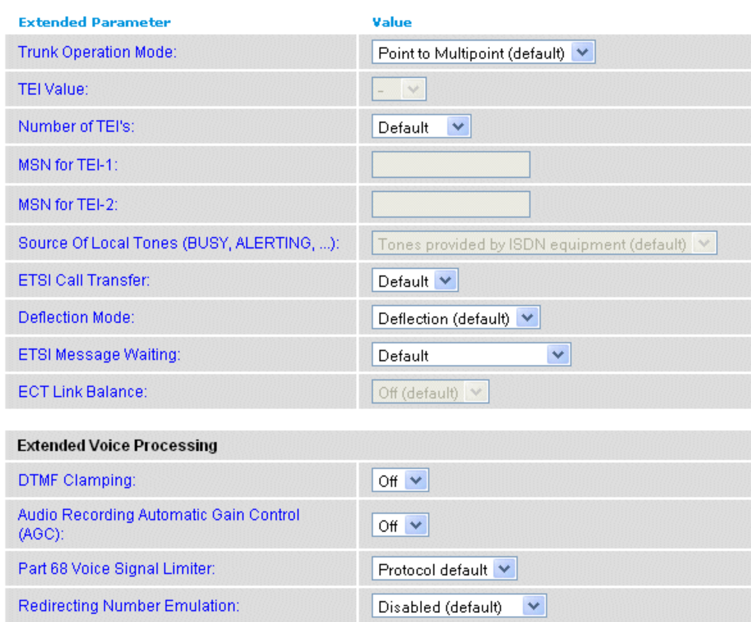


To configure Diva Media Board parameters, either click the board name or click the down arrow and select **Configuration**. A page displaying the basic parameters will open:



Depending on the selected D-channel protocol, an additional menu opens in which you may configure protocol-specific parameters.

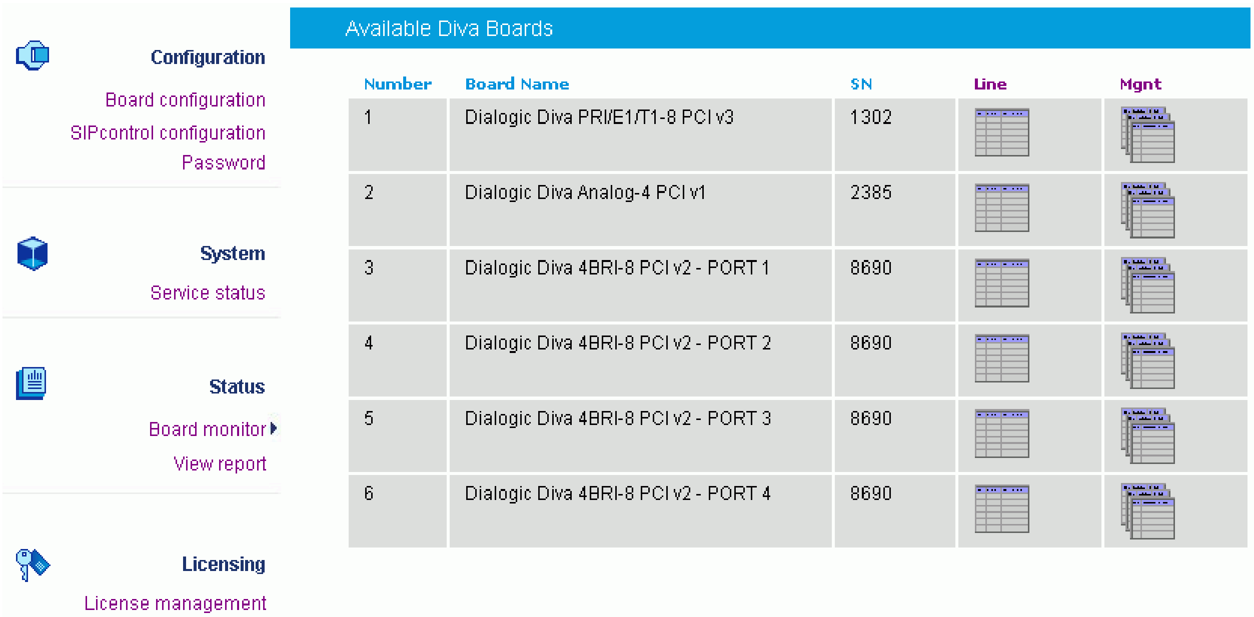
3. You can also configure extended parameters that depend on the D-channel protocol you selected. To configure those parameters, select **Yes** under **View Extended Configuration**. An additional menu will open:



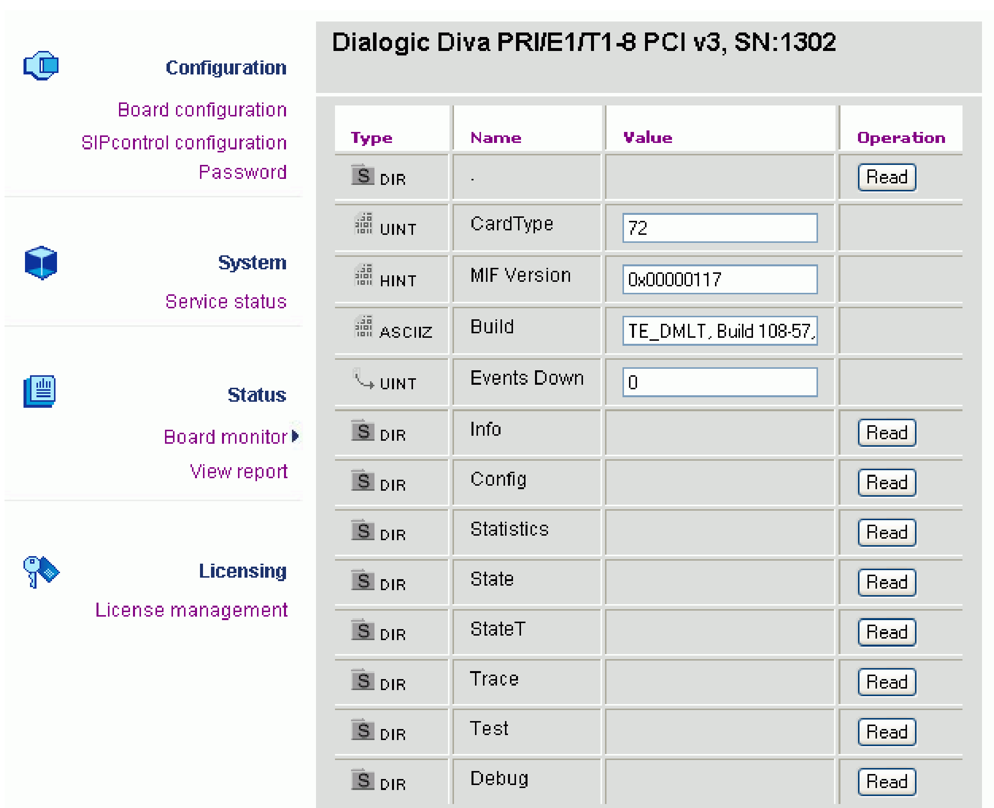
4. For more detailed information, click the parameter and a window with the help text will pop up.

The Board monitor

If you click **Board monitor** on the left hand side, a page opens that allows one to control the current status and the configuration of the installed Dialogic® Diva® Media Boards, to read internal board trace buffers (XLOG) and to gain access to the management interface of Diva Media Boards and drivers:



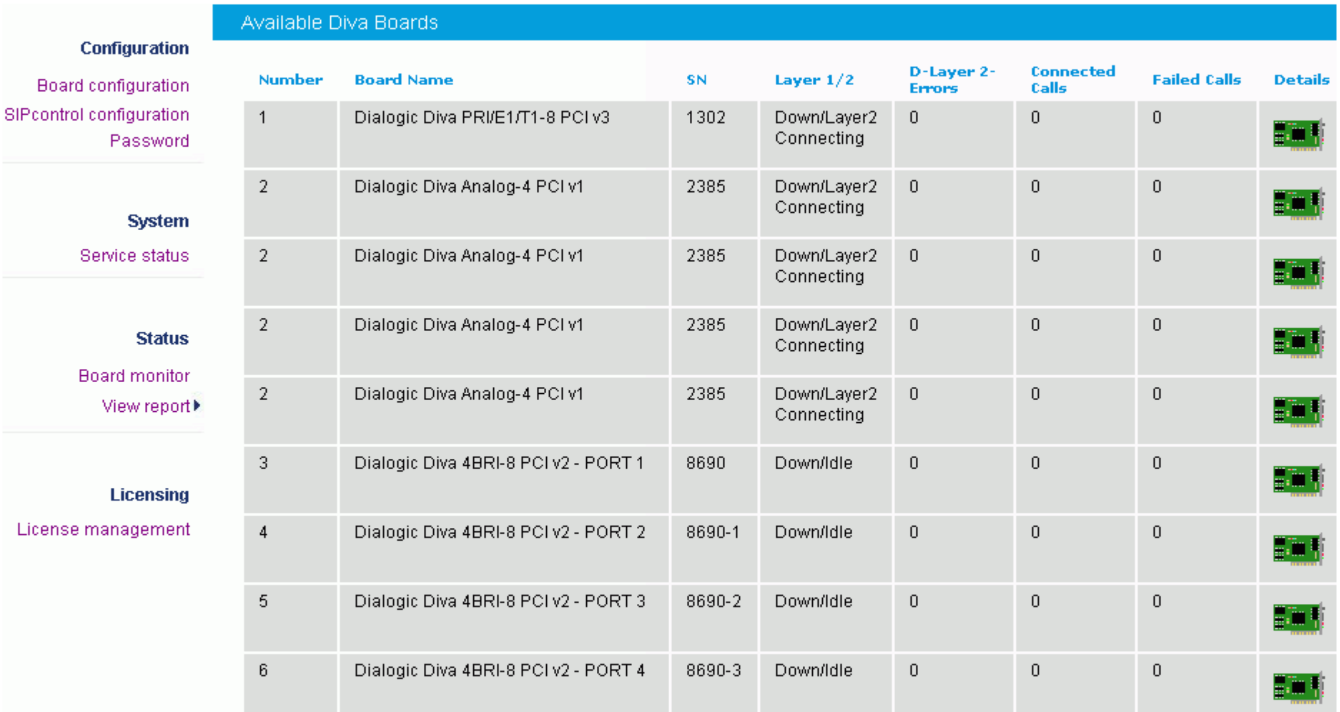
If you click the icon below **Mgnt** in the **Available Diva Boards** section, the management interface browser opens:



The management interface browser allows you to navigate through the management interface directories, and to read, write, and execute management interface variables using the buttons under **Operation**.

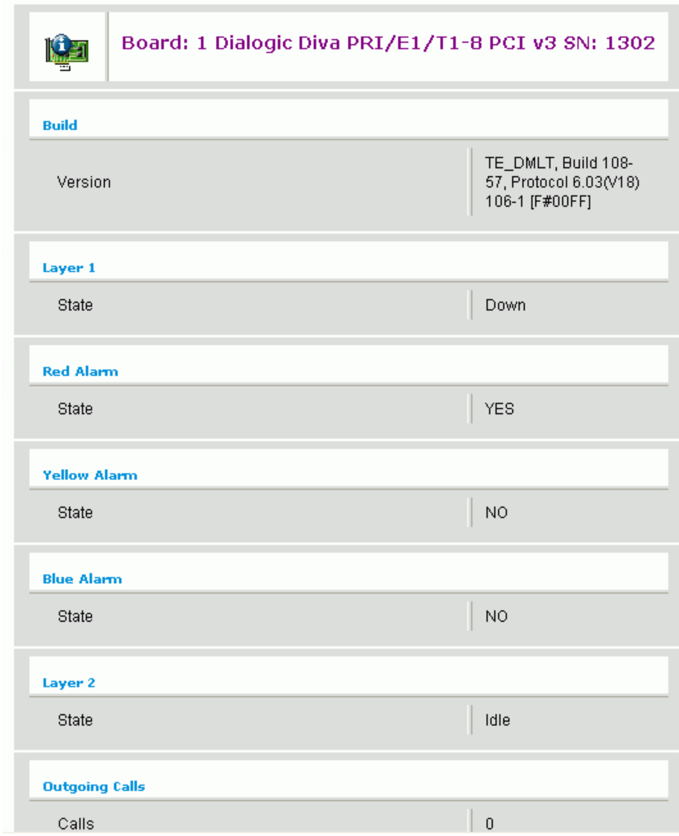
The view report option

If you click **View report**, the state and the cumulative statistics for the active Dialogic® Diva® Media Boards are shown:



Number	Board Name	SN	Layer 1/2	D-Layer 2-Errors	Connected Calls	Failed Calls	Details
1	Dialogic Diva PRI/E1/T1-8 PCI v3	1302	Down/Layer2 Connecting	0	0	0	
2	Dialogic Diva Analog-4 PCI v1	2385	Down/Layer2 Connecting	0	0	0	
2	Dialogic Diva Analog-4 PCI v1	2385	Down/Layer2 Connecting	0	0	0	
2	Dialogic Diva Analog-4 PCI v1	2385	Down/Layer2 Connecting	0	0	0	
2	Dialogic Diva Analog-4 PCI v1	2385	Down/Layer2 Connecting	0	0	0	
3	Dialogic Diva 4BRI-8 PCI v2 - PORT 1	8690	Down/Idle	0	0	0	
4	Dialogic Diva 4BRI-8 PCI v2 - PORT 2	8690-1	Down/Idle	0	0	0	
5	Dialogic Diva 4BRI-8 PCI v2 - PORT 3	8690-2	Down/Idle	0	0	0	
6	Dialogic Diva 4BRI-8 PCI v2 - PORT 4	8690-3	Down/Idle	0	0	0	

If you click the board icon below **Details**, the following report information is displayed. The information contained in the report originates from the management interface of the Diva Media Boards.



- Link status (Layer 1 state, Layer 1 alarms, Layer 2 state).
- Total number of Layer1/Layer2 frames/bytes transferred over the D-channel.
- Total number of Layer1/Layer2 errors detected in the D-channel frames.
- Total number of Layer1/Layer2 frames/bytes transferred over the B-channels.
- Total number of Layer1/Layer2 errors detected in the B-channel frames.
- Total number of calls.
- Total number of successful calls.
- Total number of failed calls, sorted by cause (User Busy, Incompatible destination, etc.).
- Total number of successful modem calls.
- Total number of failed modem calls, sorted by cause (Not a modem device, etc.).
- Total number of successful fax calls.
- Total number of failed fax calls, sorted by cause (Not a fax device, Forced by application, etc.).

Supported switch types and supported PBXs

Supported Switch Types

Dialogic® Diva® Media Boards currently support the following switch types:

Public line ISDN protocols

EMEA PRI and BRI

- 1TR6 (legacy Germany and old PBXs)
- ETSI Australia variant (On Ramp ETSI)
- ETSI (Europe, Africa)
- ETSI Hong Kong variant
- ETSI Serbia variant
- ETSI Taiwan variant
- ETSI New Zealand variant
- INS-Net 64 / 1500 (Japan)
- VN4 (legacy France, old PBXs)
- VN6 (current France)

Line Side E.1

- Australian P2
- Ericsson
- Melcas
- NEC
- Nortel

R2 CAS (E.1 only)

- Argentina
- Brazil
- China
- India
- Indonesia
- Korea
- Mexico
- Philippines
- Thailand
- Venezuela

USA PRI and BRI

- 5ESS Custom (AT&T)
- 5ESS Ni Avaya (Lucent)
- DMS 100 (Nortel)
- EWSD (Siemens)

USA T.1/PRI

- 4ESS
- T.1 RBS

Carrier Grade

ITU-T ISUP SS7

POTS

Worldwide POTS

PBX protocols

- Generic QSIG T.1 and E.1

  Note: The Generic QSIG switch type can be used for the majority of PBXs
- ETSI

  Note: Many European PBXs use the regular ETSI protocol (PRI and BRI).

Specific major PBX types

- Alcatel 4200
- Alcatel 4400
- Alcatel 4410
- ASCOM Ascotel 2020
- ASCOM Ascotel 2030
- ASCOM Ascotel 2050
- ASCOM Ascotel 2060
- DeTeWe OpenCOM 1000
- Ericsson MD110/BP250
- GPT Realitis iSDX
- Lucent Definity
- Matracom 6500
- Nortel Meridian
- Nortel opt11 Rev23
- Siemens Hicom 150
- Siemens Hicom 300
- Siemens Hipath 3000
- Siemens Hipath 4000
- Tenovis QSig

For a list of PBXs that are currently supported and tested with gateways from the different Dialogic® Media Gateway Series, see http://www.dialogic.com/microsoftuc/ocs_integration.htm.

CHAPTER 5

Dialogic® Diva® SIPcontrol™ Software Configuration

This chapter provides configuration tips and hints, it includes general information about each configuration, and it gives an overview of the configurable Diva SIPcontrol parameters. The configuration of the Dialogic® Diva® Media Boards is described in Dialogic® Diva® Media Board Configuration on page 19.

The Dialogic® Diva® SIPcontrol™ Software can be configured via the Diva SIPcontrol software web interface.

To open the Diva SIPcontrol software web interface:

1. Click **Start** > **Programs** > **Dialogic Diva** > **SIPcontrol Configuration**. By default, the access to the web interface is only allowed from localhost (127.0.0.1) and by default, the port number to which the server is listening is set to 10005.
2. If you need to access the configuration via remote access, you must set a password. To do so, open the main configuration web interface locally and click **Password** on the left hand side under **Configuration**. Enter a minimum 7 digit long password and confirm it. Click **Save** to make the new password active.
3. If necessary, open the port in the local firewall settings.

   To do so:

   - Click **Start** > **Settings** > **Control Panel** > **Windows Firewall**.
   - In the **Windows Firewall** dialog box, click the **Exceptions** tab and click **Add Port...**.
   - In the **Add a Port** dialog box, enter a name, e.g., Diva SIPcontrol, and enter the port number 10005. Select **TCP** as protocol and click **OK** to close the dialog box.

Now you may access the Diva SIPcontrol software web interface on any of the IP addresses of the computer where SIPcontrol is installed, and configure the settings according to your needs. The Diva SIPcontrol software configuration is divided into the following sections:

- PSTN Interfaces on page 27
- Network Interfaces on page 32
- SIP Peers on page 33
- Routing on page 38
- Security Profiles on page 41
- Dialplans on page 44
- Address Maps on page 46
- Cause Code Maps on page 48
- Codec Profiles on page 49
- Registrations on page 50
- System Settings on page 51

Mandatory configurations are:

1. Choose and enable one network interface.
2. Create and enable one SIP peer.
3. Create and configure one route for PSTN to SIP calls and another route for SIP to PSTN calls.

Before you start configuring, you might want to take a look at the Configuration Tips and Hints on page 27 that include useful information for the configuration.

Configuration Tips and Hints

- Changes to the configuration will only take effect after you click **Save** at the bottom of each configuration page.
- The settings will be lost if you close the Dialogic® Diva® SIPcontrol™ software web interface without having saved the configuration at the bottom of each configuration page.
- A restart of the Diva SIPcontrol software is recommended if you change the IP address or the port on which SIPcontrol is listening. If you do not restart, the Diva SIPcontrol software will continue listening on the previously configured port and IP address.

  Note: The restart will terminate active connections.
- The names for specific configuration elements are limited to 32 alphanumeric characters and must not be repeated, i.e., you cannot assign the same name for two SIP peers.
- The configuration session times out after 30 minutes of inactivity and a new login is required to access the session again. If the new login screen appears when you try to save the configuration, login again and click the "Back" button of the browser. The configuration session opens with the settings before the time out and you can save the configuration.
- To remove the password login page, logout from the web interface and restart the Dialogic® Diva® WebConfig service as described below. Then open Windows® Explorer, go to C:\Program Files\Diva Server\httpd\login, and delete the login file.
- To restart the Dialogic® Diva® WebConfig service, click **Start** > **Settings** > **Control Panel** > **Administrative Tools**. In the **Administrative Tools** window, select **Services**. In the **Services** window, right-click the **Dialogic Diva WebConfig** service and select **Restart**.
- The Diva SIPcontrol software provides a secure configuration via the web interface (HTTPS). The default port for the HTTPS is 10006. The Diva SIPcontrol software provides a default certificate, but for security reasons you should install your own webserver certificates. The location depends on the operating system:
  - Windows® XP and Windows Server® 2003 (32-bit):
    Program Files > **Diva Server** > **divawebconfig** > **cert**.
  - Windows® XP and Windows Server® 2003 (64-bit):
    Program Files (x86) > **Diva Server** > **divawebconfig** > **cert**.
  - Windows Vista® and Windows Server® 2008 (both 32-bit and 64-bit):
    ProgramData > **Dialogic Diva** > **divawebconfig** > **cert**.
- To use TLS for SIP calls, you need to upload the certificates as described under Security Profiles on page 41 and enable the TLS port as described under Network Interfaces on page 32.
- To open the online help for a specific parameter, click the parameter and a window with the help text will pop up.

PSTN Interfaces

This section describes the Diva SIPcontrol software's PSTN interface related settings, e.g., which lines are used by the Diva SIPcontrol software or how Call Transfer is performed on this line. Line Parameters such as the signalling protocols (Q.Sig, ETSI) can be configured on the **Board Configuration** page. For more information, see Dialogic® Diva® Media Board Configuration on page 19.

At least one PSTN interface must be enabled for the Diva SIPcontrol software to be able to work. Disabled PSTN interfaces are ignored for both inbound and outbound calls. For each line, you may select a dialplan that you can configure as described in Dialplans on page 44.

To change the settings for the enabled interface, click the **Details** button on the right hand side. To open the online help for a specific parameter, click the parameter and a window with the help text will pop up.

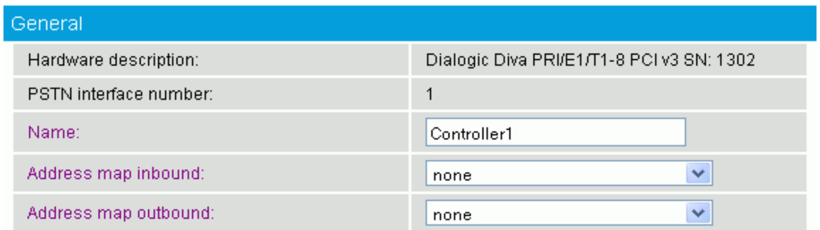
Note: PSTN interfaces without a binding to the CAPI service in the Dialogic® Diva® Configuration Manager are disabled in the Diva SIPcontrol software web interface and cannot be configured.

The following configuration menus are available for each Diva Media Board:

- General on page 28
- Enhanced on page 28
- Address Normalization on page 29
- PSTN Call Transfer Settings on page 30
- Message Waiting Indication (MWI) on page 31

General

You may configure the parameters shown in the graphic and explained in the table below:



Hardware description: Displays the installed Dialogic® Diva® Media Board. This entry is predefined by the system and cannot be changed.

PSTN interface number: Displays the number of the CAPI controller. The number is set automatically by the system.

Name: Displays the name of the installed Dialogic® Diva® Media Board. The name may be modified in order to display the purpose of the interface or the name of the PBX it is connected to.

Address map inbound: Select the name of a regular expression list to be applied on calls received on this interface. See Address Maps on page 46 for more information about setting up a regular expression list. If you upgraded from Dialogic® Diva® SIPcontrol™ Software version 1.5 or 1.5.1, an address map is automatically generated here to provide the same number processing behavior in the current Diva SIPcontrol software version as in former Diva SIPcontrol software versions. If you used regular expressions in Diva SIPcontrol software version 1.5.1, they will be included in this address map as well, unless they cannot be converted to the new scheme. In this case, the entry **<Use Windows Registry values>** is available. The Diva SIPcontrol software will then use the regular expressions defined in the registry keys that were used by Diva SIPcontrol software 1.5.1.

Regular expressions may be used to add or remove dial prefixes required by a PBX or to rewrite public phone numbers of different number ranges into a common format. See the Examples on page 66 for more information.

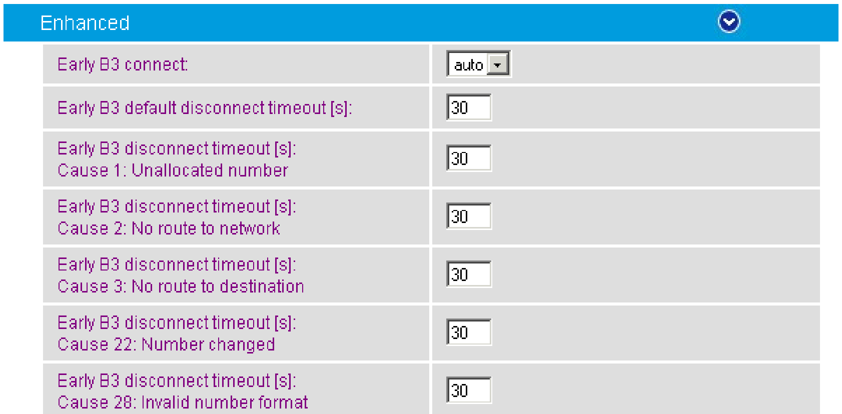
Address map outbound: Select the name of a regular expression list to be applied on calls sent out by this interface. See Address Maps on page 46 for more information about setting up a regular expression list. If you upgraded from Dialogic® Diva® SIPcontrol™ Software version 1.5 or 1.5.1, an address map is automatically generated here to provide the same number processing behavior in the current Diva SIPcontrol software version as in former Diva SIPcontrol software versions. If you used regular expressions in Diva SIPcontrol software version 1.5.1, they will be included in this address map as well, unless they cannot be converted to the new scheme. In this case, the entry **<Use Windows Registry values>** is available. The Diva SIPcontrol software will then use the regular expressions defined in the registry keys that were used by the Diva SIPcontrol software 1.5.1.

Regular expressions may be used to add or remove dial prefixes required by a PBX or to rewrite public phone numbers of different number ranges into a common format. See the Examples on page 66 for more information.

Enhanced

Here you may configure the settings for Early media support. Early media refers audio and video data that is exchanged before a session is accepted by the called user. It may be unidirectional or bidirectional, and can be generated by the calling party, the called party, or both. Typical examples of early media generated by the called party are ringing tone and announcements (e.g., queuing status). Early media generated by the calling party typically consists of voice commands or DTMF tones to drive interactive voice response (IVR) systems.

You may configure the parameters shown in the graphic and explained below:



Early B3 connect: With this parameter you can determine if early media should be enabled on this controller (EarlyB3) or whether early media should be enabled even if no "inband tones available" signal is received from PSTN (EarlyB3ForceMedia).

The following values determine if EarlyB3 and EarlyB3ForceMedia are enabled or not:

Value	EarlyB3	EarlyB3Force Media
auto	enabled	not enabled
on	enabled	enabled
off	not enabled	not enabled

The default value is **auto**.

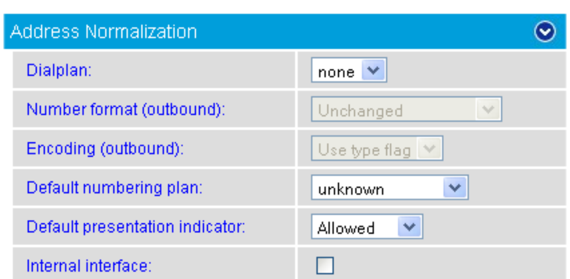
EarlyB3 default disconnect timeout [s]: Specifies the disconnect timeout value for early media calls to the PSTN, depending on the received cause value. The disconnect timer is released if a call to the PSTN is terminated before the receiver answers the call. This allows the caller to listen to a network announcement describing the reason for the failure (e.g., "The number you have dialed is not available. Please try again later.")

Default: **30** seconds

EarlyB3 disconnect timeout [s] Cause <x>:<reason for disconnect timeout>: With these parameters, you may define the disconnect timeout for the different disconnect timeout reasons. The default value for each reason is **30** seconds.

Address Normalization

You may configure the parameters shown in the graphic and explained below:



Dialplan: Select the local dialplan to be used by the dialplan module of the Dialogic® Diva® SIPcontrol™ Software. The selected dialplan applies only to this controller.

In most cases, the PSTN interfaces within the system share a common dialplan of the local environment, but configuring the dialplan per controller allows for handling variants, e.g., if the controllers are connected to different PBXs or if one controller is directly connected to the public network.

Configure the local dialplan as described under Dialplans on page 44 before you select it here.

Number format (outbound): This parameter determines the shortest format allowed in calls sent out by this interface. You may modify this parameter only if you selected a dialplan from the drop down menu. The following options are available:

Unchanged: The number signaled in the SIP message will be used unchanged for dialing.

International number: The number is always converted to an international number, including country and area code.

National number: The number is converted to a national number unless it is an international number with a different country code.

Extension: The number is reduced as possible. An internal number is reduced to its extension only.

For more information about number formats, see How Numbers Are Processed on page 64.

Encoding (outbound): Determines if numbers in calls sent out by this interface should either be encoded as unknown number with national or international prefix digits, or as national or international number with type flags.

Default numbering plan: Change this setting only if the PBX rejects calls from the Diva SIPcontrol software despite the dialed number being correct. This might occur if, for example, the signaled numbering plan is not supported.

Default presentation indicator: If no presentation is specified via address rewriting, the presentation indicator to set on calling party number for calls to ISDN. Select here, whether the calling party number should be shown or not.

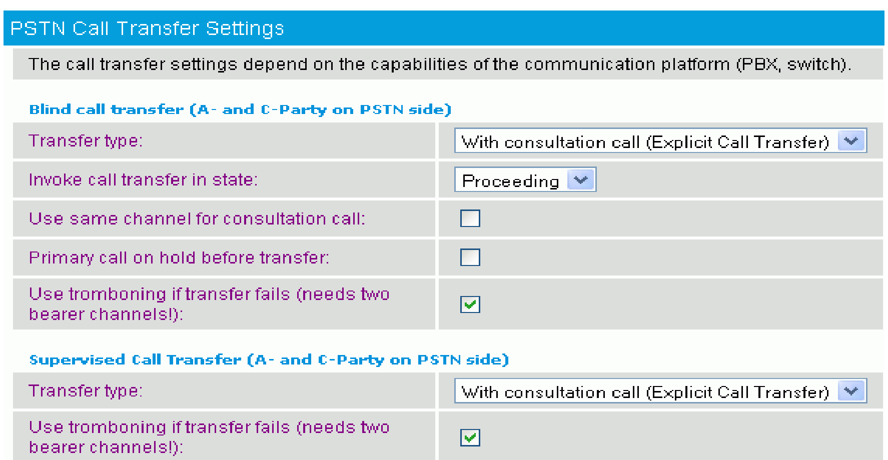
Internal interface: If calls to PSTN via this interface are received by this interface, then this is considered to be an internal interface and this option must be set for a correct number normalization. This is usually the case, if this interface is running in NT mode.

If calls to PSTN via this interface are sent by this interface, this is considered to be an external interface and this option must NOT be set for a correct number normalization. This is usually the case, if this interface is running in TE mode. (default)

If you use this interface to connect two facilities of a company, this interface is considered to be external as well, even if the calls are not routed via the PSTN and this option must NOT be set either.

PSTN Call Transfer Settings

Some Call Transfer options can be configured in the **Blind Call Transfer** section and in the **Supervised Call Transfer** section.



Transfer type: The following options are available:

Without consultation call (Call Deflection): The call is transmitted automatically.

With consultation call (Explicit Call Transfer): After the transfer to the destination party, the channel is freed. The transfer may be announced or unannounced.

With consultation call via tromboning: The call transfer is emulated. Two B-channels are blocked during the call transfer.

Complete transfer in state: The blind call transfer is typically handled via an implicit call to the transfer destination. Once this call reaches the state specified via the option **Invoke Call Transfer in state**, the call transfer is completed. Default setting is **Connected**. If the calling party should hear the ring back tone from the transfer destination, this parameter must be set to **Proceeding** or **Alerting**.

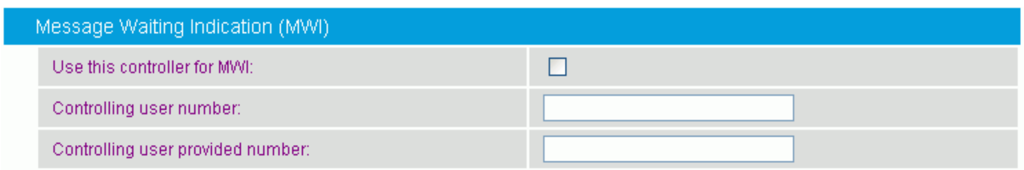
Use same channel for implicit call: The B-channel used for the primary call is used for the consultation call as well. This requires that the option **Hold primary call before transfer** is enabled. For Dialogic® Diva® Analog Media Boards and protocols using inband signaling, this option must be enabled.

Primary call on Hold before transfer: Select this option to place the primary call on hold before a call to the transfer destination is initiated.

Use tromboning if transfer fails (needs two bearer channels): Select this option if the Call Transfer should be emulated in case it could not be transferred with **Call Deflection** or **Explicit Call Transfer**.

Message Waiting Indication (MWI)

You may configure the parameters shown in the graphic and explained below:



Use this controller for MWI: The controller to use for MWI needs to be connected to a PBX port, which allows for updating of the message waiting indication.

Controlling user number: A PBX typically requests an authentication to allow for updating of the message waiting indication. This authentication is done by a **Controlling user number**. The administrator of the PBX can provide this number.

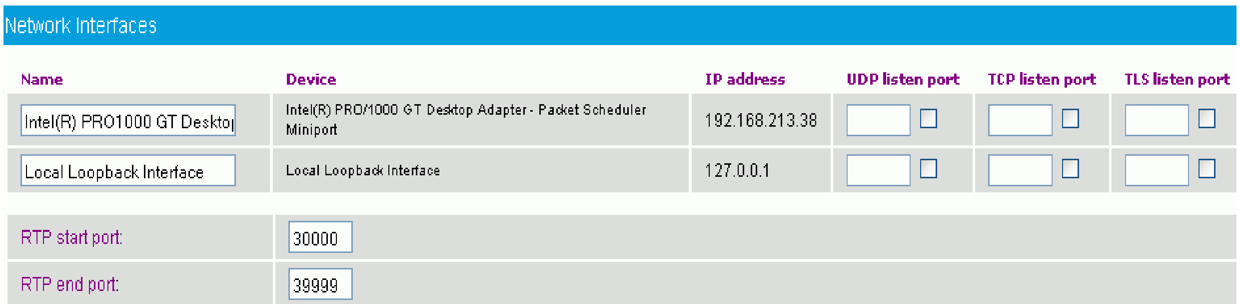
Controlling user provided number: The **Controlling user provided number** (CUPN) is the ISDN number provided by the controlling user, e.g., the ISDN number of the originating user of the indicated message. Few PBXs (e.g., Nortel) require the CUPN. The administrator of the PBX can provide more information.

Network Interfaces

The **Network Interfaces** configuration allows for configuring the global network parameters of the Dialogic® Diva® SIPcontrol™ software, such as the IP addresses and the ports on which the Diva SIPcontrol software will be listening. The Diva SIPcontrol software supports only a single IP address.

To open the online help for a specific parameter, click the parameter and a window with the help text will pop up.

You may configure the parameters shown in the graphic and explained below:



Name	Displays the name of the installed Ethernet adapter. The preset designation may be replaced with a unique identifier, such as "Internal Network".
Device	Displays the complete description of the installed Ethernet adapter assigned by the operating system.
IP address	Displays the IP address of the computer on which the Diva SIPcontrol software is installed.
UDP listen port	If you use UDP as IP protocol for calls from SIP, enable the check box to display the standard port number 5060. This standard port can be used if no other SIP application is running on the same computer as the Diva SIPcontrol software. Note that you may only enable one network interface.
TCP listen port	If you use TCP as IP protocol for calls from SIP, enable the check box to display the standard port number 5060. This standard port can be used if no other SIP application is running on the same computer as the Diva SIPcontrol software. Note that you may only enable one network interface.
TLS listen port	If you use TLS for encrypted calls, enable the check box to display the standard port number 5061. You may change the port number, but it must not be the same as the **TCP Listen Port** number. Note that you may only enable one network interface. If you use TLS, you need to upload security certificates and set the cipher level in the Security Profiles on page 41.
RTP start port	Defines the lowest port of the range in which the Diva SIPcontrol software sends and receives RTP streams. Change this value only if problems occur.
RTP end port	Defines the highest port of the range in which the Diva SIPcontrol software sends and receives RTP streams. Change this value only if problems occur.

SIP Peers

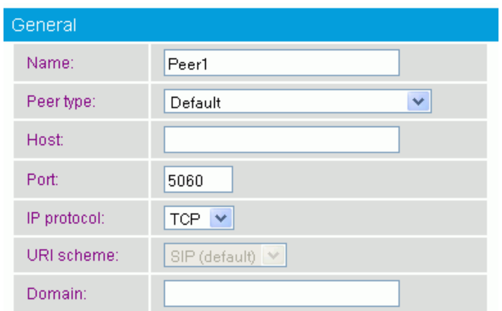
A SIP peer is a specific endpoint to and from which the Dialogic® Diva® SIPcontrol™ software will establish calls. The peer-specific settings may be used to adapt the Diva SIPcontrol software's behavior towards this peer.

To add a SIP peer, click the **Add** button. To change the settings for the enabled SIP peer, click the **Details** button on the right hand side. To open the online help for a specific parameter, click the parameter and a window with the help text will pop up. The following menus are available for configuration:

- General below
- Enhanced on page 34
- Security on page 36
- Session Timer on page 36
- Address Normalization on page 37
- Authentication on page 37

General

You may configure the parameters shown in the graphic and explained below:



Name: Enter a name for the SIP peer. A SIP peer is a specific endpoint to and from which the Diva SIPcontrol software establishes the calls.

Peer type: Some SIP peers need a specific peer, such as a Microsoft® Exchange Server, to work properly with the Diva SIPcontrol software. If this is the case for your configuration, select the specific SIP peer. If not, select **Default**.

Host: Enter the host name or IP address of the peer. The name must be resolvable by local name resolution. During the establishment of a call, the host name is sent by this peer exactly as entered here, unless an address map applies that converts the host name in a different format. For more information about name resolution, see the Windows® documentation.

Port: Displays the SIP port on which the remote peer is listening. The default is 5060, which is the standard port for SIP.

IP protocol: Select the IP protocol to be used for calls to this peer. Calls from this peer are accepted with all protocols and on all ports/addresses configured in Network Interfaces as described on page 32.

If you selected **MS Exchange 2007** or **MS OCS2007 / Mediation Server** as **Peer type**, set the protocol to **TCP**. If you selected **e-phone**, set the protocol to **UDP**.

URI scheme: This option is only available if you selected **TLS** as **IP protocol**.

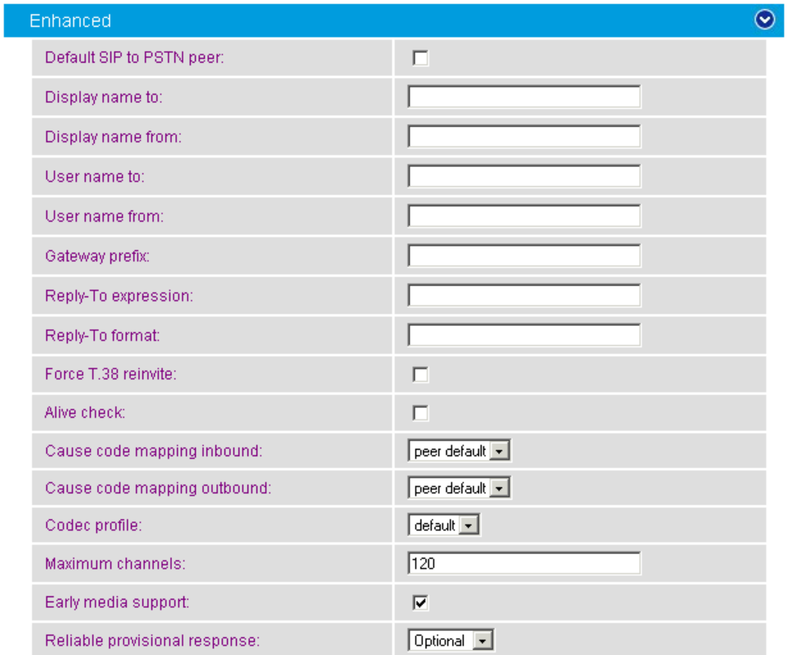
Calls are transmitted via various proxy servers. Some of them do not transmit the calls as encrypted calls. If you select **SIP (default)**, you allow that calls are transmitted via such proxy servers.

To make sure that a call is sent encrypted to the proxy of the remote side, select **SIPS** (secure SIP). If the call is routed via a proxy server that is not able to route the call encrypted, it rejects the call and the call is sent to another proxy until it can be transmitted.

Domain: Enter the domain name, e.g., dialogic.com, or the IP address. The domain name must comply with the DNS rules. The domain name entry here is only needed if the SIP peer does not use its hostname as source domain when it places a call.

Enhanced

You may configure the parameters shown in the graphic and explained below:



Default SIP to PSTN peer: Enable this option if the selected peer type should be used as default peer. Calls from unconfigured SIP peers will be assigned to this peer, and therefore are handled with these settings. If several peers are configured as default, the Diva SIPcontrol software takes the first to transmit the call.

Display name to: Enter the name that is to be sent in the "To" header of the INVITE message on calls from the PSTN to SIP.

Display name from: Enter the name that is to be sent in the "From" header of the INVITE message on calls from the PSTN to SIP. To send the calling party number include an asterisk (*) in the display name. For instance, if the display name is "Dialogic *" and the calling number is 123, then the remote side receives "Dialogic 123". To include an asterisk in the display name, enter "*". To include a backslash enter "\\".

User name to: You may enter a user name in front of the host name, e.g., thomas@dialogic.com. The user name is needed for the default route when no called party number is transmitted, e.g., for Dialogic® Diva® Analog Media Boards.

If a call from SIP does not contain a user name, the name entered here is transmitted as calling party number to the PSTN.

User name from: Enter the user name that is added to the SIP address when a number from the PSTN is suppressed. You may also enter the complete SIP address consisting of <username>@<local-IP/hostname>.

If a call from SIP does not contain a user name, the name entered here is transmitted as called party number to the PSTN.

Gateway prefix: You can configure this parameter only if you selected **e-phone** as **Peer type** in the **Edit SIP Peer Configuration** window.

This prefix is added at the beginning of the address in the "Reply-To" and "Contact" headers, which are copies of the "From" address. If this string is not empty, the parameter "phone-context" will be added in both headers.

Reply-To expression: You can configure this parameter only if you selected **e-phone** as **Peer type** in the **Edit SIP Peer Configuration** window.

Enter the expression that may be necessary for the e-phone server to handle the call. Normally, this is necessary to omit the 0 (zero) for external calls and to manipulate the address so the e-phone server is able to call back.

Reply-To format: You can configure this parameter only if you selected **e-phone** as **Peer type** in the **Edit SIP Peer Configuration** window.

Enter the format that may be necessary for the e-phone server to handle the call. Normally, this is necessary to omit the 0 (zero) for external calls and to manipulate the address so the e-phone server is able to call back.

Force T.38 reinvite: Some peers do not switch the media channel to T.38 if they receive a fax call, e.g., if they do not evaluate the fax calling tone. If you select this option, the Dialogic® Diva® SIPcontrol™ software tries to initiate the media channel switch.

Alive check: If you select this option, the failover procedure is expedited because the Diva SIPcontrol software does not wait for a call time-out if a peer does not respond. To achieve this, the Diva SIPcontrol software sends "pings" periodically to the peer via OPTIONS requests. If the peer does not send a valid answer, it will be treated as "inactive" and no calls will be routed to this peer until the peer responds to the "pings" again. In this case, the Diva SIPcontrol software will automatically direct calls to this peer again.

Cause code mapping inbound: Select the cause code mapping for calls coming from this SIP peer that you configured under Cause Code Maps as described on page 48.

Cause code mapping outbound: Select the cause code mapping for calls to this SIP peer that you configured under Cause Code Maps as described on page 48.

Codec profile: Select the codec list that you configured under Codec Profiles on page 49. If you do not select a list, an internal default list is used with the following default priority order:

1. G.711A
2. G.711u
3. G.729, if licensed*
4. iLBC, if available on the used Dialogic® Diva® Media Board*
5. GSM-FR*
6. G.726 (16, 24, 32, and 40 kbps)*
7. Comfort Noise
8. T.38, if supported by the used Diva Media Board
9. DTMF via RFC2833 (no real codec, but internally handled as codec)

In calls from SIP to the PSTN, the first codec of the PSTN device is applied that is also in the default codec list of the Diva SIPcontrol software.

* Not included in default list on Dialogic® 4000 Media Gateways.

Maximum channels: Specifies the number of channels that this SIP peer is able to handle at the same time. This setting is used by the Diva SIPcontrol software to distribute calls in a load-balancing scenario and to avoid speech quality degradation and/or call failures at the peer due to overload conditions.

Early media support: Specifies whether the peer supports early media for calls to PSTN. For non-human peers this should be disabled.

Reliable provisional response: SIP defines two types of responses, provisional and final. Provisional responses provide information on the progress of the request processing and final responses transmit the result of the request processing.

This parameter specifies whether reliable provisional responses (RFC3262) should be used.

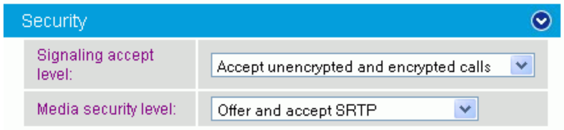
The following values are available:

Disabled: Reliable provisional response is not used.

Optional: Reliable provisional response may be used.

Required: Reliable provisional response is mandatory.

Security



You may configure the parameters shown in the graphic and explained below:

Signaling accept level: This parameter defines, how the call information should be accepted. To accept encrypted calls, you need to activate TLS as listen port in the Network Interfaces configuration.

Accept unencrypted calls only: Only signaling sent with TCP or UDP is accepted. Any encrypted signaling is rejected.

Accept encrypted and unencrypted calls: All calls are accepted, independent from the encryption mode.

Accept encrypted calls only: Only signaling with TLS is accepted; unencrypted signaling is rejected.

Accept encrypted call with SIPS URI only: Only signaling encrypted with the URI scheme secure SIP is accepted. Calls sent with TLS encryption are rejected.

Media security level: The Secure Real-time Transport Protocol (SRTP) authenticates packets and encrypts data and thus adds security to the voice stream. SRTP should be used together with TLS.

No SRTP: The voice stream is not secured with SRTP.

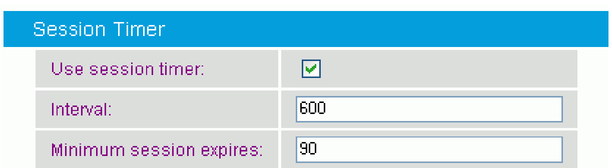
Offer and accept SRTP: The voice stream is secured with SRTP, if possible.

Require SRTP for encrypted calls: Calls via TLS need to use SRTP, otherwise they are rejected.

Note: If you select **Require SRTP for encrypted calls**, calls without SRTP are still allowed via UDP or TCP, unless **Signaling accept level** does not allow calls via UDP or TCP.

Session Timer

You may configure the parameters shown in the graphic and explained below:



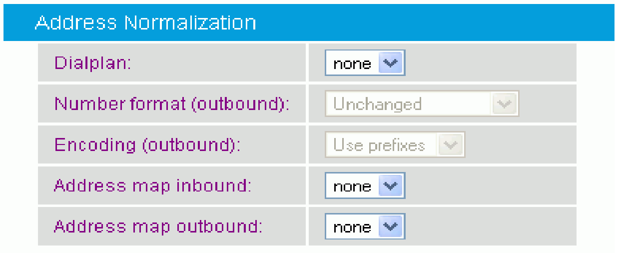
Use session timer: Activates session monitoring via SIP session timers using the time-out values given here. Refer to RFC4028 for details.

Interval: If **Use session timer** is enabled, you may set a time-out in seconds until a call is considered to be aborted. Refreshes are normally performed after the first half of the interval has elapsed. The minimum value is 90 seconds. The default value is 600 seconds.

Minimum session expires: If **Use session timer** is enabled, you may set a time in seconds between two session refresh messages that the Diva SIPcontrol software will accept. The minimum value is 90 seconds.

Address Normalization

You may configure the parameters shown in the graphic and explained below:



Dialplan: Select the local dialplan to be used by the dialplan module of the Dialogic® Diva® SIPcontrol™ Software. Configure the local dialplan under Dialplans as described on page 44 before you select it here.

The dialplan selected here applies only to outgoing calls.

Number format (outbound): This parameter determines the shortest format allowed that is sent in calls to this SIP peer. You may modify this parameter only if you selected a dialplan from the drop down menu. The following options are available:

Unchanged: The number signaled in the SIP message will be used unchanged for dialing.

International number: The number is always converted to an international number, including country and area code.

National number: The number is converted to a national number unless it is an international number with a different country code.

Extension: The number is reduced as much as possible. An internal number is reduced to its extension only.

For more information about number formats, see How Numbers Are Processed on page 64.

Encoding (outbound): Determines if numbers in calls to this SIP peer should either be encoded as unknown number with national or international prefix digits or as national or international number with type flags.

Address map inbound: Name of the regular expressions list applied to the addresses received on calls from this SIP peer. See Address Maps on page 46 for more information about setting up a regular expression list.

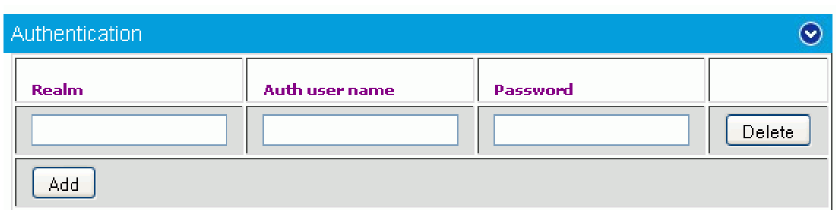
Regular expressions may be used to add or remove dial prefixes required by a PBX or to rewrite public phone numbers of different number ranges into a common format. See the Examples on page 66 for more information.

Address map outbound: Select the name of a regular expression list to be applied on calls to this SIP peer. See Address Maps on page 46 for more information about setting up a regular expression list.

Regular expressions may be used to add or remove dial prefixes required by a PBX or to rewrite public phone numbers of different number ranges into a common format. See the Examples on page 66 for more information.

Authentication

You may configure the parameters shown in the graphic and explained below:



Realm: A realm is a protection domain with its own user names and passwords. Enter the realm used by the SIP peer for authentication. The realm entered here needs to be the same as the realm of the endpoint.

Auth User Name: Enter a user name to be used with this realm.

Password: Enter the password to be used with this realm.

Routing

The **Routing** configuration defines the destination to which incoming calls are forwarded. Possible criteria that may determine the destination are:

- called, calling, and redirected number or SIP address of a call for which the redirected number is only available for calls originating in the PSTN,
- the source where a call originated, i.e., a PSTN interface name or a specific SIP peer,
- the current channel allocation across a set of several possible destinations in a load-balancing environment, and
- the current status of a destination. See How Calls Are Processed on page 57 for more information.

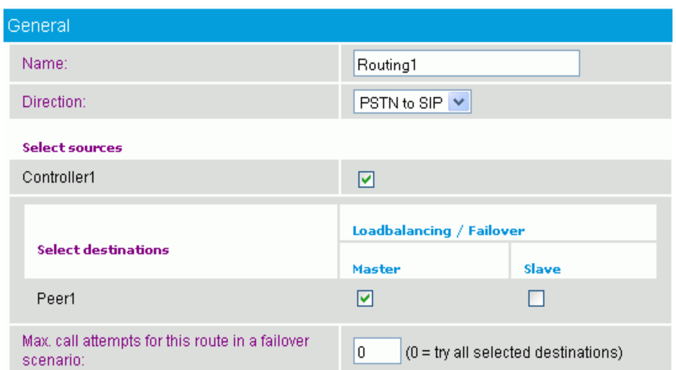
To add a routing, click the **Add** button. To change the settings for the enabled routing, click the **Details** button on the right hand side. Since routes are processed in their configured order, the first matching route takes the call. To change the order, click the "arrow up" and "arrow down" buttons. To open the online help for a specific parameter, click the parameter and a window with the help text pops up.

For more information about possible routing configurations, see Routing examples on page 59.

The following menus are available for configuration:

General

You may configure the parameters shown in the graphic and explained below:



Name: Enter a unique name for the route, e.g., "Calls to MS Exchange Server".

Direction: Select if this route is for calls from SIP to PSTN or vice versa.

Select Sources: Depending on the selected direction, this part either lists the configured PSTN interfaces or SIP peers. The route will only be considered for a call if the call originated from a selected source.

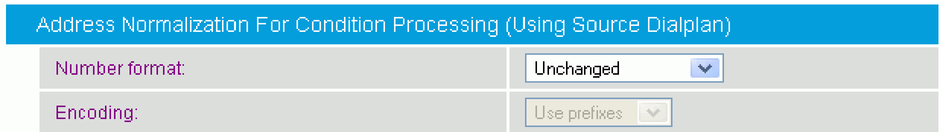
Note: A source may be selected even if it is currently disabled. In this case, the call will already have been rejected before the route is queried. At least one source interface is required for the route.

Select Destinations: You may select the possible destinations for the route, i.e., the set of CAPI controllers or SIP peers to which the call may be routed. The master or slave setting allows for configuring priorities. The Dialogic® Diva® SIPcontrol™ Software will always try to establish a call to one of the masters first and considers the slaves only if all masters have failed or could not accept calls due to their call load.

Max. call attempts for this route in a failover scenario: Enter the number of times the Diva SIPcontrol software should try to call the recipient in a failover environment. If you enter 0 (zero), the Diva SIPcontrol software tries all selected destinations. A value of 1 disables the failover functionality and tries only the first destination of a route.

Address Normalization For Condition Processing (Using Source Dialplan)

You may configure the parameters shown in the graphic and explained below:



Number format: This parameter determines the shortest format allowed in calls using this route. If the source interface of the call has no dialplan assigned, this setting has no effect. The following options are available:

Unchanged: The number signaled in the SIP message will be used unchanged for dialing.

International number: The number is always converted to an international number, including country and area code.

National number: The number is converted to a national number unless it is an international number with a different country code.

Extension: The number is reduced as much as possible. An internal number is reduced to its extension only.

For more information about number formats, see How Numbers Are Processed on page 64.

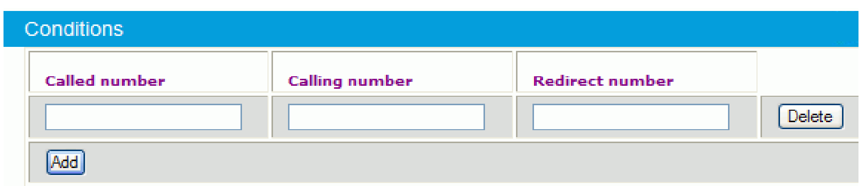
Encoding: Determines if numbers in calls using this route should either be encoded as unknown number with national or international prefix digits or as national or international number with type flags.

Conditions

You may configure certain conditions for a route. If you do not configure any conditions, the route is used as default route.

Note: If prefixes need to match, the digits of the prefix need to be prepended by a caret symbol ("^"); otherwise, these digits would match within the number as well, e.g. 0 would also match 1230@sipcontrol.com.

You may configure the parameters shown in the graphic and explained below:



Called number: If the routing is supposed to be valid only for specific calls, enter the called party number to which the route should apply. The Dialogic® Diva® SIPcontrol™ Software compares the current called party number against the called number entered here. If they do not match, the Diva SIPcontrol software verifies the next routing until it finds a match.

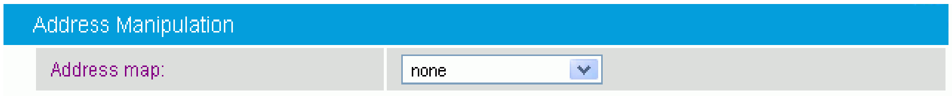
Calling number: If the routing is supposed to be valid only for specific calls, enter the calling party number to which the route should apply. The Diva SIPcontrol software compares the current calling party number against the calling number entered here. If they do not match, the Diva SIPcontrol software verifies the next routing until it finds a match.

Redirect number: If the routing is supposed to be valid only for specific calls, enter the redirecting number to which the route should apply. The Diva SIPcontrol software compares the current redirecting number against the redirect number entered here. If they do not match, the Diva SIPcontrol software verifies the next routing until it finds a match.

Note: A route can only be matched if the three condition parts (called number, calling number, and redirect number) match their call address counterpart in any of the lines. Empty condition entries always match, i.e., a line with the three condition parts left empty will always apply, thus working as a default route.

Address Manipulation

You may configure the parameter shown in the graphic and explained below:



Address Map: If a route matches, the address manipulation setting allows for modifying the call addresses according to your needs. For example, if calls with the called party number starting with "9" should be directed to a specific peer, it might be desirable to remove this digit. This can be done with a special address map configured. Note that you need to configure the address map as described under Address Maps on page 46 before you may select it here.

Security Profiles

When you use the Transport Layer Security (TLS) protocol for secure communication, you need to set various security settings.

The following menus are available for configuration:

- Upload Certificate And Key Files on page 41
- Global Security Parameters on page 42

Upload Certificate And Key Files

For authentication and data encryption, certificates need to be installed on the computer with the Diva SIPcontrol software and on remote computers. When a secure domain is opened, server and client authenticate each other with a so called "SSL handshake". With this handshake, the identity of a user is certified and the user can be trusted. All necessary certificates are provided by a Certificate Authority (CA) and they are issued for one domain name. For test purposes or internal usage, you can also create and sign your own self-signed certificate, e.g., with one of the many tools available on the internet, just search for "self-signed certificate" and you will find a list of possible tools. But you need to be aware that self-signed certificates do not provide the same security as CA-signed certificates. Also, many web browsers check if the certificate is signed by a CA, and, if it is not, a warning message will pop up asking whether the user really wants to trust that web site, which can make the user feel insecure.

Certificate files can be generated in different formats, e.g., .pem, .der, .cer, or .pfx. All files need to be in "pem" format, that means base64 encoded, in order to be used by the Diva SIPcontrol software. For more information about secure connections and certificates, see Data Security Overview on page 52.

A default certificate is provided with the software, but for security reasons, you should install your own web server certificate.

Note for CER files: CER files can be renamed to .pem directly if they are base64 encoded. No bag attribute lines and/or additional CR and empty lines are allowed. If CER files are ASN.1 coded, they need to be converted to with a converter tool.

Note for PFX files: The PFX or PKCS#12 format is a binary format for storing the server certificate, any intermediate certificates, and the private key in one encryptable file. When converting a PFX file to PEM format, tools like OpenSSL will put all the certificates and the private key into a single file. You will need to open the file in a text editor and copy each certificate and private key (including the BEGIN/END statments) to its own individual text file and save them as certificate.cer, CACert.cer, and privateKey.key respectively.

How to retrieve keys and certificates from a PFX file for use in the Diva SIPcontrol software

In the following procedure openssl is used as example converter tool.

1. Export the private key file from the PFX file:

   ```
   openssl pkcs12 -in filename.pfx -nocerts -out protected-key.pem
   ```

2. Remove the passphrase from the private key as required by the Diva SIPcontrol software:

   ```
   openssl rsa -in protected-key.pem -out key.pem
   ```

3. Export the certificate file from the PFX file:

   ```
   openssl pkcs12 -in filename.pfx -clcerts -nokeys -out cert.cer
   ```

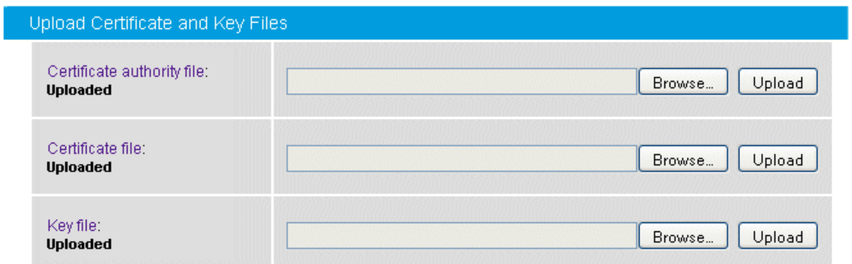
4. Export the Root CA certificate file from the PFX file:

   ```
   openssl pkcs12 -in filename.pfx -cacerts -nokeys -out cacert.cer
   ```

The screen below shows the web interface with no certificates uploaded.

To upload a certificate:

1. Click **Browse**, in the **File Upload** window go to the folder where the certificate file is located, and click **Open**.
2. In the Diva SIPcontrol software web interface, click **Upload**. After the certificates are uploaded, the information below the certification files changes from "Not available" to "Uploaded". Note that you will not see the paths to the directory in which the files are stored:



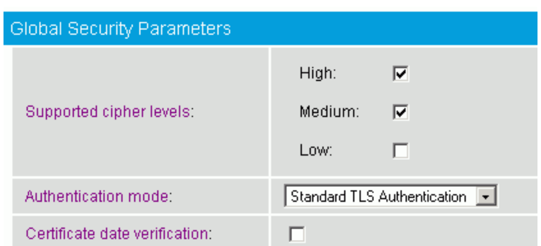
Certificate authority file: This file is the root certificate, which is used to sign a certificate. It is only needed for MTLS or TLS authentication.

With this file, the CA ensures that the public key contained in the certificate belongs to the server stated in the certificate.

Certificate file: This file is also generated from the CA and it contains the public key of the server on which the Diva SIPcontrol software is installed. This file is used for encrypting of information.

Key file: This file contains the private key for each endpoint, and it is used for decrypting of information. The key file must not be password protected.

Global Security Parameters



Supported cipher levels: Cipher is an algorithm for encrypting and decrypting data. During the SSL handshake between client and server, the cipher level is negotiated. A low cipher level should only be used for systems that do not transmit any important information.

High: This currently means cipher suites with key lengths larger than 128 bits, and some with 128-bit keys.

Medium: Currently some suites using 128-bit encryption.

Low: Currently suites using 64- or 56-bit encryption algorithms but excluding export cipher suites.

Authentication mode:	Select how the server-client authentication should be handled. **Mutual Authentication**: MTLS is used by Microsoft® Office Communications Server (OCS) 2007 Server roles and by Microsoft® Exchange 2007 UM role to communicate with each other. In this mode, both peers need to authenticate each other and both client and server exchange certificates. For connecting to Microsoft® OCS 2007 R2 Mediation Server via TLS, use Standard TLS authentication mode. For a direct connection to Microsoft® Exchange 2007 UM role via TLS, use MTLS authentication mode. **Standard TLS Authentication**: This is the normal authentication mode, in which the client asks the server for authentication to ensure a secure connection to the correct server. **No Authentication**: In this mode, neither the server nor the client need to proof its authentication. The default setting is: **Standard TLS Authentication**.
Certificate date verification:	If enabled, the expiration date of the peer certificate is verified. If the certificate is expired, an informational message is displayed and the call is aborted.

Dialplans

With help of the local phone settings, the Dialogic® Diva® SIPcontrol™ Software is able to convert a received call address to a normalized form, e.g., the E.164 format. This does not only ease the definition of subsequent conditions or maps, but it also converts the call to the format as required by the receiver.

The dialplan module supports the following features:

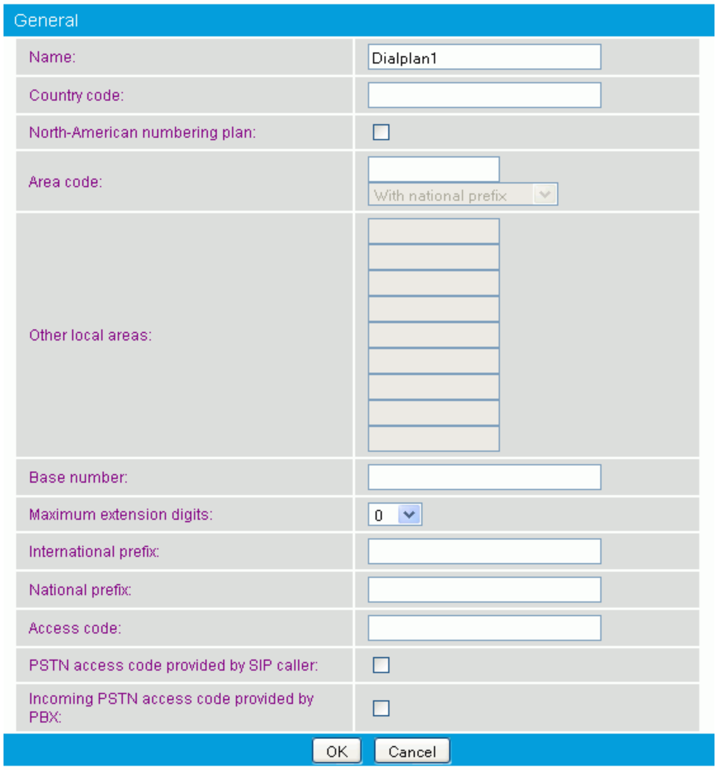
- Number expansion and reduction: called, calling, and redirected numbers are converted to one of the following formats: international, national, local, or internal (extension-only) format; for each format, either prefix digits or digital number type flags may be used.
- Adding and removing of the line access code: If not present, dialed numbers are automatically prepended by the digit(s) needed to get access to the public telephone network.
- Support for North American numbering plan: Up to 10 area codes may be configured to be treated differently. For example, in many areas dialing into neighboring areas requires to not dial a long-distance prefix.

Important information about the outside access digit configuration

- Configure the outside access digit only if there is a PBX between the PSTN and the Diva SIPcontrol software, and if this PBX requires the outside access digit for external calls. If you need to configure the outside access digit, also configure the following related options:
  - **Incoming PSTN access code provided by the PBX**: This option defines if the Diva SIPcontrol software expects the outside access digit in the calling number in external calls from the PBX.
    The PBX normally prepends the outside access digit to the calling number of incoming external calls in order to enable callback functionality at internal phones. If this is the case, enable this option.
  - **PSTN access code provided by the SIP caller**: This option defines if the Diva SIPcontrol software expects the outside access digit in the called number of external calls from SIP to the PSTN.
    It is normally required to prepend the outside access digit to call an external number from an internal phone, in this case, these are phones on the SIP side; however, in some configurations this is not required, such as a configuration that is part of the North American numbering plan (NANP), where an internal number can be identified based on its length. If it is possible to identify an internal call purely by the length of the called number, this option can be disabled. In all other configurations with outside access digits this option has to be enabled.
    It is recommended to have this option enabled in dialplans with the outside access digit set.
- The Diva SIPcontrol software's number normalization function does not remove outside access digits as a PBX can do for external calls. If the Diva SIPcontrol software needs to behave like a PBX with an outside access digit for external calls, use the Address Map functionality in combination with a Routing module.

To add a dialplan, click the **Add** button. To change the configuration settings, click the **Details** button on the right hand side. To open the online help for a specific parameter, click the parameter and a window with the help text pops up.

You may configure the parameters shown in the graphic and explained below:



Name: Enter a name to easily identify the dialplan, e.g., Stuttgart office.

Country code: Enter the country code without any prefixes of the country in which the computer with the installed Dialogic® Diva® SIPcontrol™ Software is located, e.g. 1 for US or 49 for Germany.

North-American numbering plan: Select this option if the North American numbering plan (NANP) is needed for your configuration. With the NANP, a city can have more than one area code, consequently it is not evident how to dial a number in the same city. The Diva SIPcontrol software allows you to enter various area codes that are considered local and should be called without long-distance prefix. See **Area code** and **Other local areas** for more information.

Area code: If you do not use the North American numbering plan (NANP), enter the area code without the leading zero here. If the NANP is needed for your configuration, enter the code for the home area here and enter the codes for the other local areas in **Other local areas**.

If you need to use NANP, you can choose between the following number transmission methods:

With national prefix: The long-distance code is added to the number.

Local: The number is transmitted without any area code.

Without national prefix: The number is transmitted without the long-distance prefix.

Other local areas: You may enter various area codes that are considered local and should be called without the long-distance prefix. This is the case in some countries where the North American numbering plan is deployed, e.g., in the USA. With the NANP a city can have more than one area code, consequently it is not clear how to dial a number in the same city.

Base number: Enter your subscriber or trunk number without country and area code. If you use MSNs, leave this field empty and enter the length of the MSNs in **Maximum extension digits**.

Maximum extension digits: Specify the maximum number of extension digits. Use the "arrow up" and "arrow down" buttons to do so.

International prefix: Enter the international prefix for your country, e.g., 00.

National prefix: Enter the digits of the national prefix, e.g., 0 in Germany.

Access code: Enter the digits that are needed to get access to the public network, e.g., 9.

PSTN access code provided by the SIP caller: Select this option if the SIP caller has to provide the access code. If the length of the called number is not sufficient to identify it as an internal number, activate this option to avoid ambiguous numbers. This is usually the case if you are not using the North American Numbering Plan (NANP).

Incoming PSTN access code provided by the PBX: Select this option if the PBX adds the access code to the calling number for incoming external calls.

Address Maps

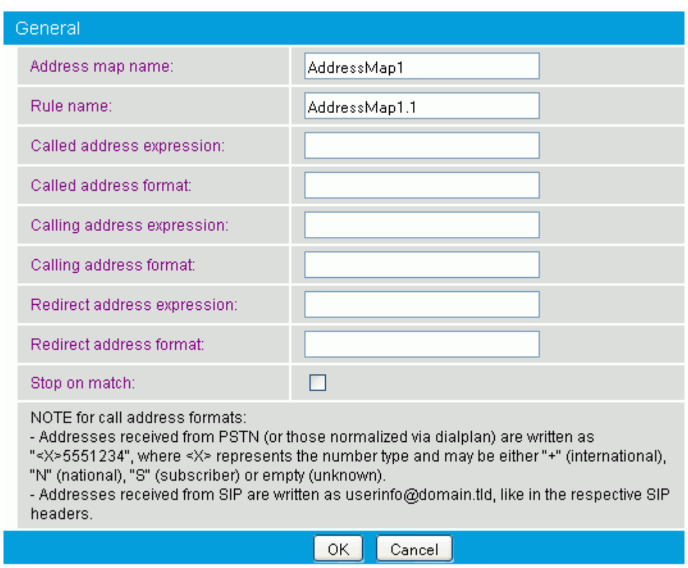
In general, address maps should be used for cases that are not covered by the dialplan. Possible scenarios are:

- set the calling number to that of the central office on SIP-to-PSTN calls,
- change the called extension to another value if an employee left,
- remove trunk prefixes while routing to a global voicemail server.

Each address map consists of a number of rules that are checked and applied from first to last until a matching rule is found that has the **Stop on match** option enabled. A rule matches only if all three expressions of that rule match. The order of the address maps is not important, but the order of the rules within a map is significant and can therefore be changed with the "arrow down" and "arrow up" buttons.

To add an address mapping, click the **Add** button. To change the settings for each address mapping, click the **Details** button on the right hand side. To open the online help for a specific parameter, click the parameter and a window with the help text pops up.

You may configure the parameters shown in the graphic and explained below:



Address map name:	Enter a name for the address map that helps you remember the purpose of the map. This name is shown in other menus where an address map may be selected. **Note:** The name may be edited only during the creation of a map.
Rule name:	Enter a name for the rule of the map, e.g., "Remove 9 from all incoming calls".
Called address expression:	If the regular expression entered here matches a called address, the format string is applied to the result. See How Numbers Are Processed on page 64 for more information on regular expressions.
Called address format:	If the address format entered here matches a called address, the format string is applied to the result. See How Numbers Are Processed on page 64 for more information on regular expressions and formats.
Calling address expression:	If the regular expression entered here matches a calling address, the format string is applied to the result. See How Numbers Are Processed on page 64 for more information on regular expressions.
Calling address format:	If the address format entered here matches a calling address, the format string is applied to the result. See How Numbers Are Processed on page 64 for more information on regular expressions and formats.
Redirect address expression:	If the regular expression entered here matches a redirected address, the format string is applied to the result. See How Numbers Are Processed on page 64 for more information on regular expressions.
Redirect address format:	If the address format entered here matches a redirected address, the format string is applied to the result. See How Numbers Are Processed on page 64 for more information on regular expressions and formats.
Stop on match:	If all expressions match all addresses of a call, this flag determines if the Dialogic® Diva® SIPcontrol™ Software should continue to search for matching rules. If set, the address matching is aborted.

Note: If expressions should match from the beginning, prepend the caret symbol ("^") at the beginning of the expression, for example:

Number: 1234567

Expression: ^123

Format: 4567

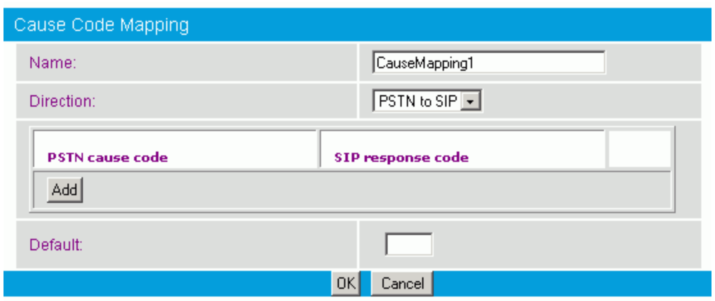
Result: 45674567

Cause Code Maps

Depending on the type of SIP peer selected, different default mapping tables are used to adapt SIPcontrol's responses to the values expected by that peer.

If the internal default mapping table provided by the Dialogic® Diva® SIPcontrol™ Software does not fulfill your needs, e.g., because your local PBX uses non-standard cause codes, you may configure your own cause code mapping table, which will be checked before the default table is. See Cause Code Mapping on page 69 for the cause/response code mapping table. If you create your own cause code mapping table, make sure to select it in the **SIP Peer Configuration** under Enhanced.

To add a cause code, click the **Add** button. To change the settings, click the **Details** button on the right hand side. To open the online help for a specific parameter, click the parameter and a window with the help text will pop up. You may configure the parameters shown in the graphic and explained below:



Name Enter a name to easily identify the cause code mapping table.

Direction Select the direction for which this table is used:

- Select **PSTN to SIP** to configure mappings of PSTN cause codes to SIP response codes. This mapping is used if a call from a SIP endpoint to a PSTN endpoint cannot be completed.
- Select **SIP to PSTN** to configure mappings of SIP response codes to PSTN cause codes. This mapping is used if a call from a PSTN endpoint to a SIP endpoint cannot be completed.

PSTN Cause Code Enter the PSTN cause code equivalent to the SIP response code entered in this menu. The PSTN cause code is also known as Q.850 cause code. Valid values are 1 to 127.

SIP Response Code Enter the SIP response code equivalent to the PSTN cause code entered in this menu. The values are only valid in the range from 400 to 699.

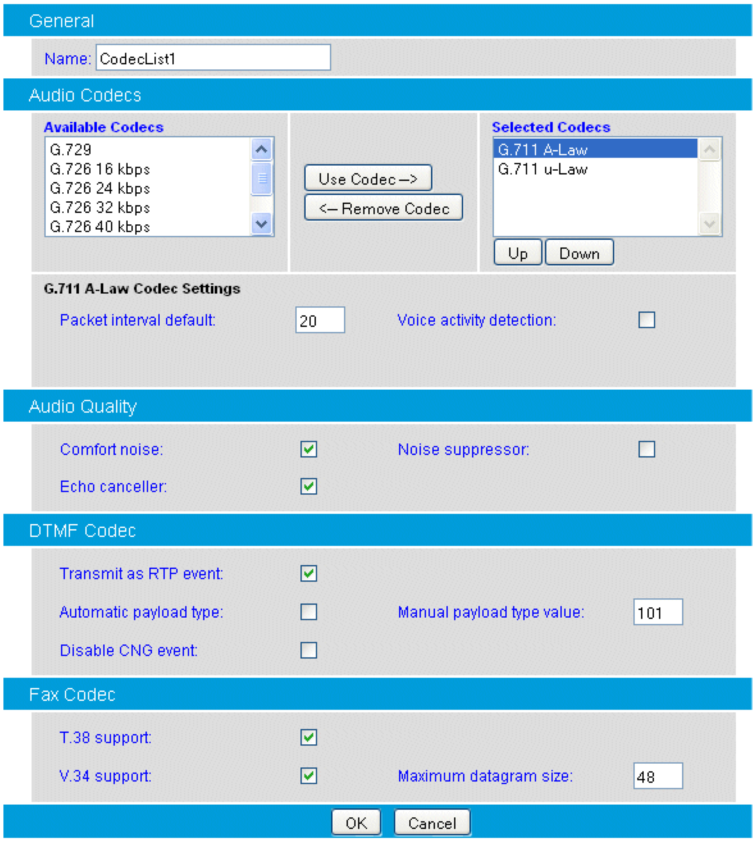
Default Enter the cause or response code that the Dialogic® Diva® SIPcontrol™ software should use per default if no mapping for the received cause or response code is specified in this table.

Note: If this value is not configured and no mapping for the received cause or response code is specified in this table, the Diva SIPcontrol software's internal default mapping table will be used.

Codec Profiles

To configure the codec list, click the **Add** button. To change the settings, click the **Details** button on the right hand side. If you create a codec profile, make sure to select it in the **SIP Peer Configuration** under Enhanced.

To open the online help for a specific parameter, click the parameter and a window with the help text will pop up. You may configure the parameters shown in the graphic and explained below:



Name: Enter a name to easily identify the codec list. You may select the codec list in the SIP Peer configuration.

Available Codecs: This list includes all available codecs. If you want to use a certain codec, select it and click **Use Codec**. The codec will be moved to the **Selected Codecs** list. The G.729 codec can only be used after you have purchased and activated a license. See License Activation on page 16 for more information.

Selected Codecs: By default, the G.711 A-law and G.711 µ-law codecs are selected. If you want to delete a certain codec, select it and click **Remove Codec**. The codecs are used according to their position in the list, with the first codec being the first to be used. To change the order, use the **Up** and **Down** buttons.

Packet interval default: Interval between RTP packets in an RTP stream. Also known as packetization time or RTP frame size.

Voice activity detection: If you activate voice activity detection, silence during a conversation is detected and the data rate is reduced.

Comfort noise support: If you enable the comfort noise feature and the voice activity detection (VAD) is active on your system, packets with low artificial background noise are sent to fill periods of total silence. Among others, total silence in digital transmissions can have the unwanted effect that the called party may think that the transmission has been lost and hang up prematurely.

Noise suppressor: Enable this parameter if you want to use the noise suppressor functionality.

Echo canceller: If you enable this parameter, the audio echo canceller is active.

Note: The echo canceller is activated as long as only one used codec has this parameter enabled.

Transmit DTMF as RTP event: With RTP events, DTMF and fax tones can be sent and received as digital notifications instead of audio signals.

Automatic payload type: G.726, iLBC, and DTMF have a dynamic RTP payload. If you select this option, the Dialogic® Diva® SIPcontrol™ software sets the values automatically. Only if the endpoint cannot handle the automatically set value, enter it manually under **Manual payload type value**.

Manual payload type value: Some endpoints expect a certain payload type value. You can enter any value between 96 and 127. In calls from SIP to the PSTN, the Diva SIPcontrol software uses the value suggested by the endpoint. Generally, this parameter is left at its default value.

Disable CNG event: This parameter defines which RTP events should NOT be supported locally, i.e., which events should be transported inband. Unsupported events are also negotiated as not available to the peer.

Each bit set defines the respective event as being NOT supported, with bit 0 of the first array entry representing event 0, and bit 8 of the 32nd entry representing event 255.

See http://www.iana.org/assignments/audio-telephone-event-registry/audio-telephone-event-registry.xhtml for a list of possible events.

Only events 0-15 (DTMF "0"-"9", "*", "#", "A"-"D"), and 36 (CNG) are supported; all other event bits are set to 1.

T.38 Support: T.38 is a protocol that enables fax transmissions on the IP network in real time. Enable this option if T.38 fax should be supported. Note that this feature is supported on Dialogic® Diva® Media Boards with multiple ports only after activating the respective license. See License Activation on page 16 for more information.

V.34 Support: The V.34 fax transmission protocol allows facsimiles to be transmitted at a maximum speed of 33.600 bps. Enable this option if V.34 should be supported. Note that this feature is supported on Diva Media Boards with multiple ports only after activating the respective license. See License Activation on page 16 for more information.

Maximum datagram size: This value defines the maximum amount of data that can be transmitted in one T.38 packet. Some endpoints are limited to packets of a certain size. You can enter a value between 32 and 192. Default is 48 bytes.

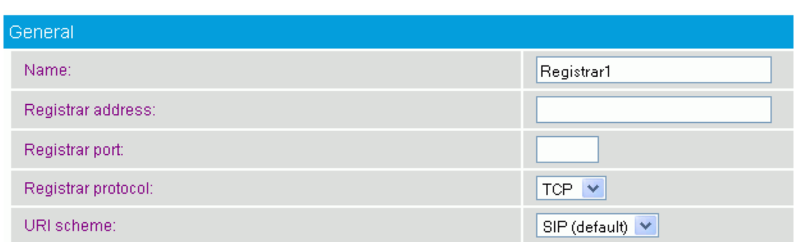
Registrations

SIP devices can communicate directly if the URL of both devices is known, but in general, SIP gateways are used in a network to enable functionalities such as routing, registration, authentication, and authorization.

Registration at a registrar server can be useful because in many cases, only the SIP address of a user is known but the location (SIP address of the device) is unknown or may change. A registrar server keeps track of the location of user agents from which the registrar server has received REGISTER requests. Thus, only the SIP address of the user needs to be sent to the registrar server, which then returns one or more contact addresses of the user.

If the Dialogic® Diva® SIPcontrol™ Software is configured to use a registrar server, it registers with the server as soon as it is active. Thus, all local addresses configured for registration are registered with the server. You may use either a private registrar service or a public registrar server.

To configure a registrar server, click the **Add** button. To change the settings, click the **Details** button on the right hand side. To open the online help for a specific parameter, click the parameter and a window with the help text will pop up. You may configure the parameters shown in the graphic and explained below:



Name: Enter a name for the registrar configuration.

Registrar address: Enter the IP address or the hostname of the registrar server.

Registrar port: Enter the port number of the registrar server. Usually, the registrar server is listening on port 5060.

Registrar protocol: Select the protocol the registrar server uses.

URI scheme: This option is only available if you selected **TLS** as **Registrar protocol**.

Calls are transmitted via various proxy servers. Some of them do not transmit the calls as encrypted calls. If you select **SIP (default)**, you allow that calls are transmitted via such proxy servers.

To make sure that a call is sent encrypted to the proxy of the remote side, select **SIPS** (secure SIP). If a call is routed via a proxy server that is not able to route the call encrypted, it rejects the call and the call is send to another proxy until it can be transmitted.

To configure the settings for each user that should register at the same registrar server, click **Add** and configure the following parameters:

Own display name: Enter the name that should be displayed at the registrar server.

URI scheme: Select either **SIP(default)** or **SIPS** as URI scheme.

User name: Enter the name or number that the Diva SIPcontrol software uses to register at the registrar server.

Domain: Enter the domain name of the registrar server.

Protocol: Select **UDP** if you register as e-phone gateway.

Re-register time: Enter the re-register time in seconds. This is the time the registration to the registrar server remains valid. After this time has elapsed, the SIP stack service would need to re-register to be available again. The default value is 3600 seconds.

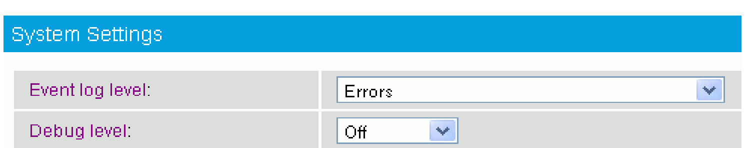
Auth user name: Enter a user name for authentication at the registrar server.

Password: Enter your password for authentication at the registrar server.

Register as: Leave the setting at the default value **Standard**. Select **e-phone GW** only if you use e-phone and you want the Dialogic® Diva® SIPcontrol™ Software to function as gateway for e-phone.

System Settings

You may configure the parameters shown in the graphic and explained below:



Event Log Level: A computer with the Diva SIPcontrol software installed may write different types of events into the System Event Log. The details for each event log are described in Event Logging on page 75.

Debug Level: The debug level setting may be used for debugging and tracing purposes. During normal operation, it should be set to **Off** to lessen the effect on system performance.

CHAPTER 6

Data Security Overview

Since version 2.0, the Dialogic® Diva® SIPcontrol™ software provides additional security options for transmitted and received data:

- Secure HTTP: You may use Secure HTTP (HTTPS) to transmit data between the web-based configuration interface of the Diva SIPcontrol software and your web browser.
- TLS: The Transport Layer Security (TLS) protocol may be used to encrypt and authorize SIP messages.
- Secure RTP: The Secure Real-time Transport Protocol (SRTP) may be used for encrypting the data of the actual conversation.

Note: The HTTPS and TLS protocols require digital identity Certificates (e.g., public key certificates).

Secure HTTP

HTTP is a protocol that transmits data between the web-based configuration interface of the Diva SIPcontrol software and your web browser. Even though the HTTP interface has access security (via a password), the transmitted data is not entirely secure. The data is transmitted as clear text and thus it is possible for the transmission to be intercepted and, in turn, for the data to be read.

HTTPS uses HTTP over an encrypted Secure Sockets Layer (SSL) or Transport Layer Security (TLS) connection and with a different default port than HTTP.

As an example, if a message containing a request to change a password was captured by a third party, the third party could log on to the Diva SIPcontrol software web interface and change the configuration. HTTPS encrypts and authenticates HTTP data, and thus the data is no longer transmitted as clear text and is not easily readable.

HTTPS requires two actions by the user:

- Both the Diva SIPcontrol software and the computer on which the web browser used to connect to the Diva SIPcontrol software via HTTPS is running must be configured with the proper certificate.
- When accessing the Diva SIPcontrol software web interface, use https:// instead of the non-secure http:// followed by the URL of the PC on which the Diva SIPcontrol software is installed.

TLS

SIP (Session Initiation Protocol) is a signaling protocol used for VoIP calls over the Internet. SIP messages contain information such as call-party information, call media type, whether it is a secure call, and if so, what encryption algorithm is used, etc. SIP can be carried by UDP, TCP, or TLS transports. Both UDP and TCP transport data in clear text. As a result, UDP and TCP can easily be monitored by a third party. TLS, on the other hand, carries SIP data in a secure way by encrypting the data and authenticating the transport connections. Authentication provides that you are talking to the intended peer. For authentication purposes, you need to install Certificates as described in Security Profiles on page 41 and enable TLS as transport protocol, as described in Network Interfaces on page 32.

Secure RTP

Once a Voice over IP (VoIP) call is established, voice data is transported in packets with the Real-time Transport Protocol (RTP). The voice data can be easily extracted from RTP packets and replayed using commercially available software. SRTP adds security by encrypting voice data and authenticating packets. Digital identity certificates are not required, the parameters are negotiated during call initiation time. SRTP mode is activated typically in combination with TLS, but in some cases (e.g., testing, intranet connections only) it is useful to allow SRTP also without TLS being activated.

For encryption and decryption of data, SRTP uses ciphers. The two parties involved in a conversation must be "compatible" in the sense that each party understands the other party's cipher requirements and supports them. The Diva SIPcontrol software supports the following ciphers: DH, ADH, AES (128-256 bits), 3DES (64 bits), DES (64 bits), RC4 (64bytes), RC4 (256 bytes), MD5, SHA1.

SRTP can be set for each SIP peer in the Security configuration, as described on page 36. The cipher level can be set in the Global Security Parameters as described on page 42.

Certificates

For authentication and data encryption, certificates need to be installed on the computer on which the Diva SIPcontrol software is installed and on remote computers. When a secure domain is opened, server and client authenticate each other with a so called "SSL handshake". With this handshake, the identity of a user is certified and it is assured that the user can be trusted. All necessary certificates should be provided by a Certificate Authority (CA), and they are issued for one domain name. For test purposes or internal usage, you can also create and sign your own self-signed certificate, e.g., with one of the many tools available on the internet, just search for "self-signed certificate" and you will find a list of possible tools. But you need to be aware that self-signed certificates do not provide the same security as CA-signed certificates. Also, many web browsers check if the certificate is signed by a CA, and, if it is not, a warning message will pop up asking whether the user really wants to trust that web site, which can make the user feel insecure.

Certificate files can be generated in different formats, e.g., .pem, .der, .cer, or .pfx. All files need to be in "pem" format, that means base64 encoded, in order to be used by the Diva SIPcontrol software.

A default certificate is provided with the software, but for security reasons, you should install your own web server certificate.

Note for CER files: CER files can be renamed to .pem directly if they are base64 encoded. No bag attribute lines and/or additional CR and empty lines are allowed. If CER files are ASN.1 coded, they need to be converted to with a converter tool.

Note for PFX files: The PFX or PKCS#12 format is a binary format for storing the server certificate, any intermediate certificates, and the private key in one encryptable file. When converting a PFX file to PEM format, tools like OpenSSL will put all the certificates and the private key into a single file. You will need to open the file in a text editor and copy each certificate and private key (including the BEGIN/END statments) to its own individual text file and save them as certificate.cer, CACert.cer, and privateKey.key respectively.

How to retrieve keys and certificates from a PFX file for use in the Diva SIPcontrol software

In the following procedure openssl is used as example converter tool.

1. Export the private key file from the PFX file:

   ```
   openssl pkcs12 -in filename.pfx -nocerts -out protected-key.pem
   ```

2. Remove the passphrase from the private key as required by the Diva SIPcontrol software:

   ```
   openssl rsa -in protected-key.pem -out key.pem
   ```

3. Export the certificate file from the PFX file:

   ```
   openssl pkcs12 -in filename.pfx -clcerts -nokeys -out cert.cer
   ```

4. Export the Root CA certificate file from the PFX file:

   ```
   openssl pkcs12 -in filename.pfx -cacerts -nokeys -out cacert.cer
   ```

Using certificates with Microsoft® Office Communications Server (OCS) 2007

Microsoft® OCS 2007 requires that:

- server certificates contain one or more CRL (Certificate Revocation List) distribution points.

  CRL distribution points are locations from which CRLs can be downloaded to verify that the certificate has not been revoked since the time it was issued.

- server certificates support EKU (Enhanced Key Usage).

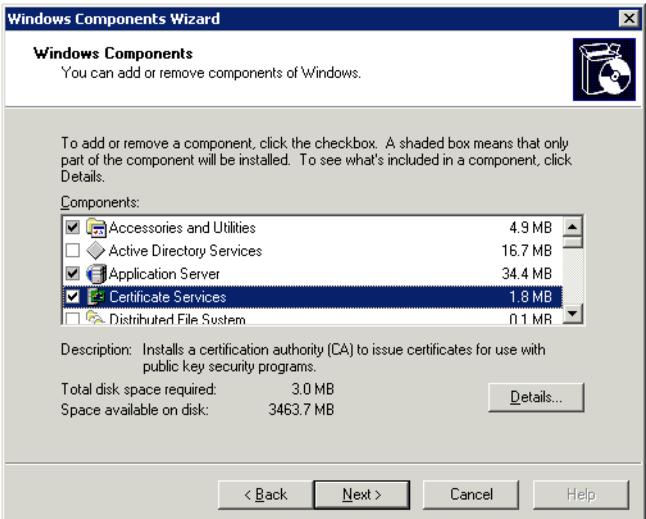
  EKUs are needed for server authentication and ensure that the certificate is valid only for the purpose of authenticating servers. This EKU is essential for MTLS (Mutual TLS).

- the gateway server certificate has a FQDN (Fully Qualified Domain Name) either in the Certification field CN (Common Name) / SN (Subject Name) or SAN (Subject Alternative Name) or both.

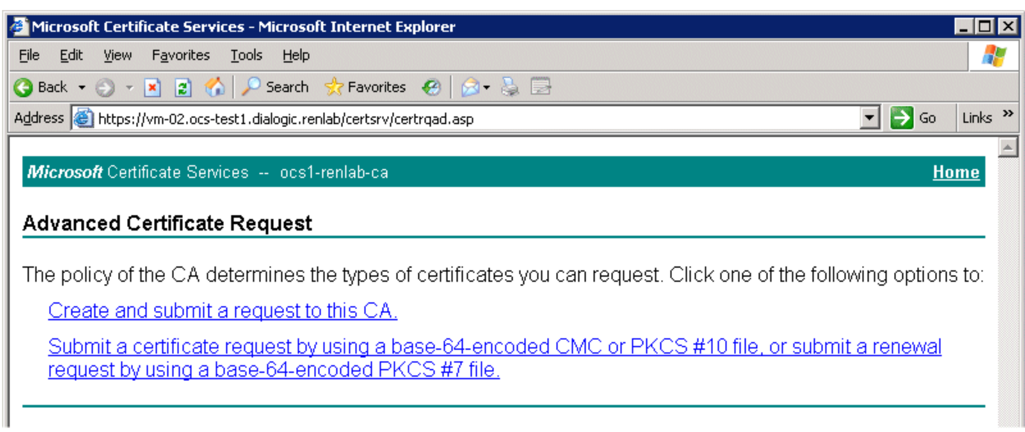
How to generate certificates using Microsoft® Certificate Services and upload them in the Diva SIPcontrol web interface

Microsoft® Certificate Services is a component of the Microsoft® Windows Server® operating system. On Microsoft® Windows Server® 2003, it can be installed through the Windows® Component Wizard.

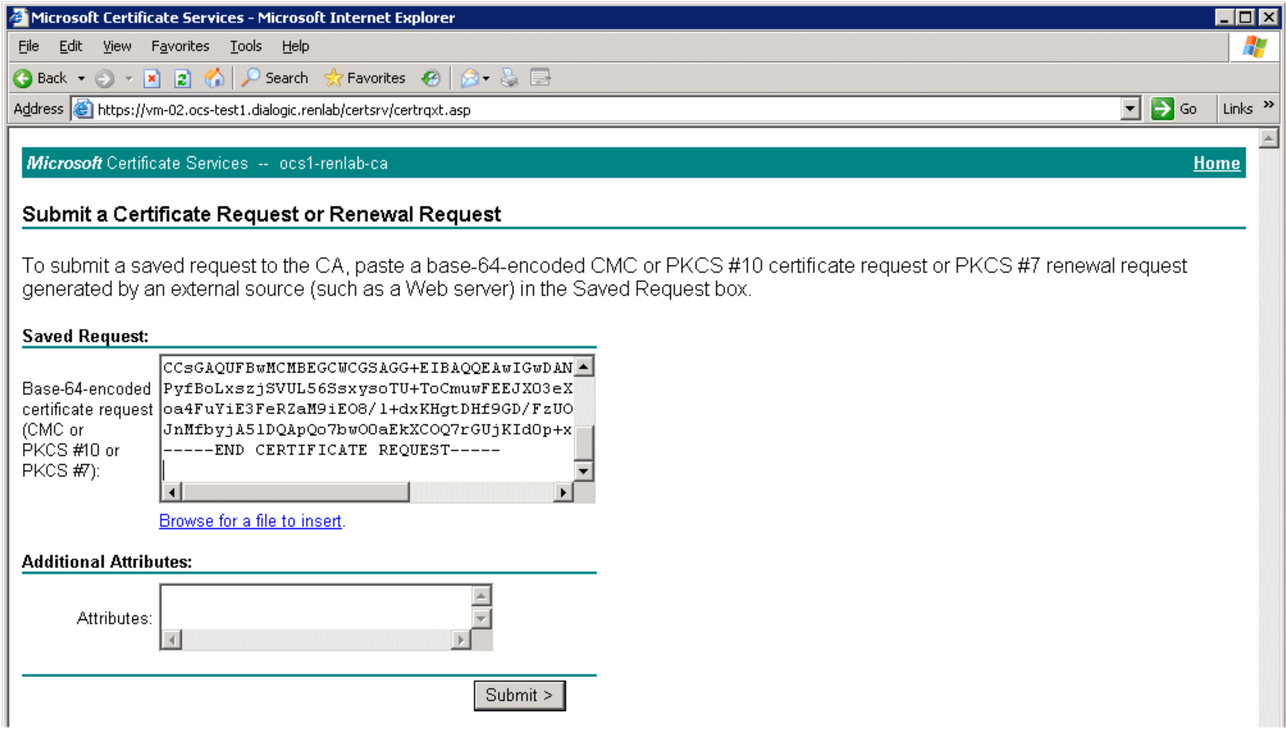
Note: Do not install the Microsoft® Certificate Services on your Dialogic® 4000 Media Gateway, but on a separate computer.



1. Create a key file and a certificate request with a third party program.
2. On your Microsoft® Certificate Services web site, got to **Advanced Certificate Request** and select the second option to submit a base-64-encoded request.

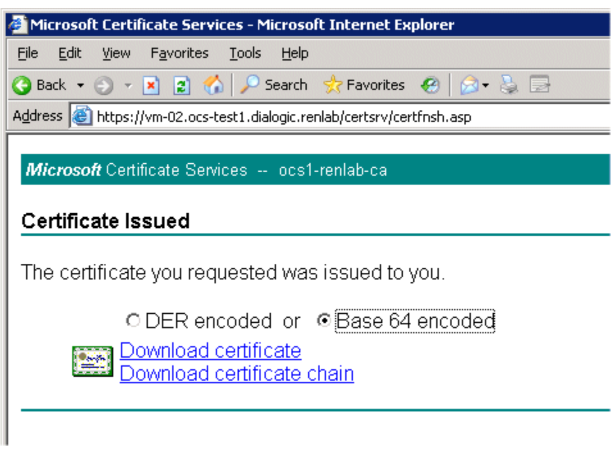


3. Open the key file with Wordpad, select the contents, paste it into the Microsoft® Certificate Services web site, and click **Submit**.

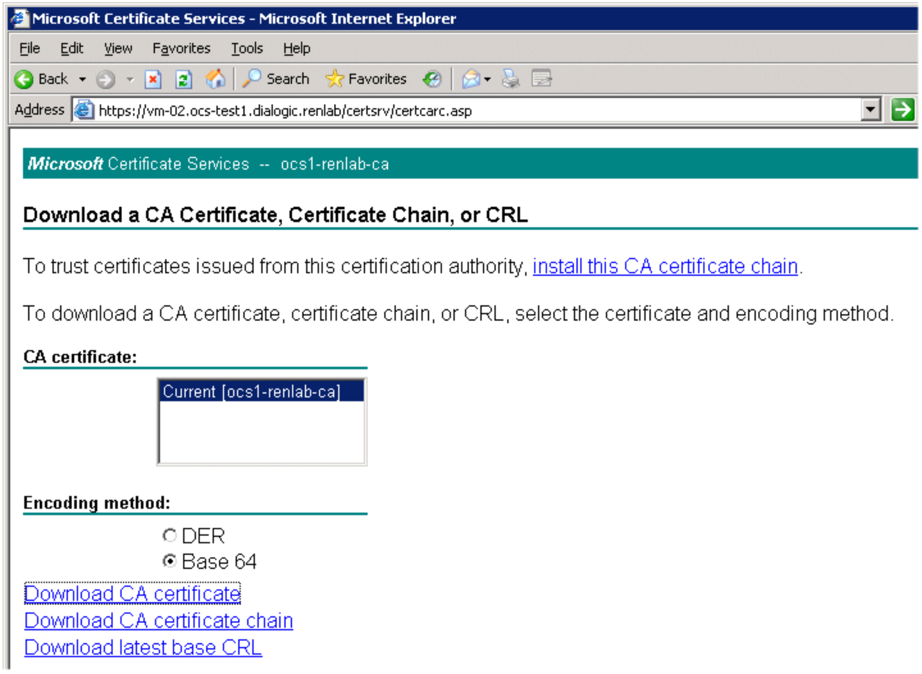


4. Go to the Microsoft® Certification Authority Management console and sign the certificate request.

5. Go to the Microsoft® Certificate Services download page for signed certificates, select **Base 64 encoded**, and click **Download certificate**.



6. Go to the Microsoft® Certificate Services download page for the CA certificate, select **Base 64**, and click **Download CA certificate**.

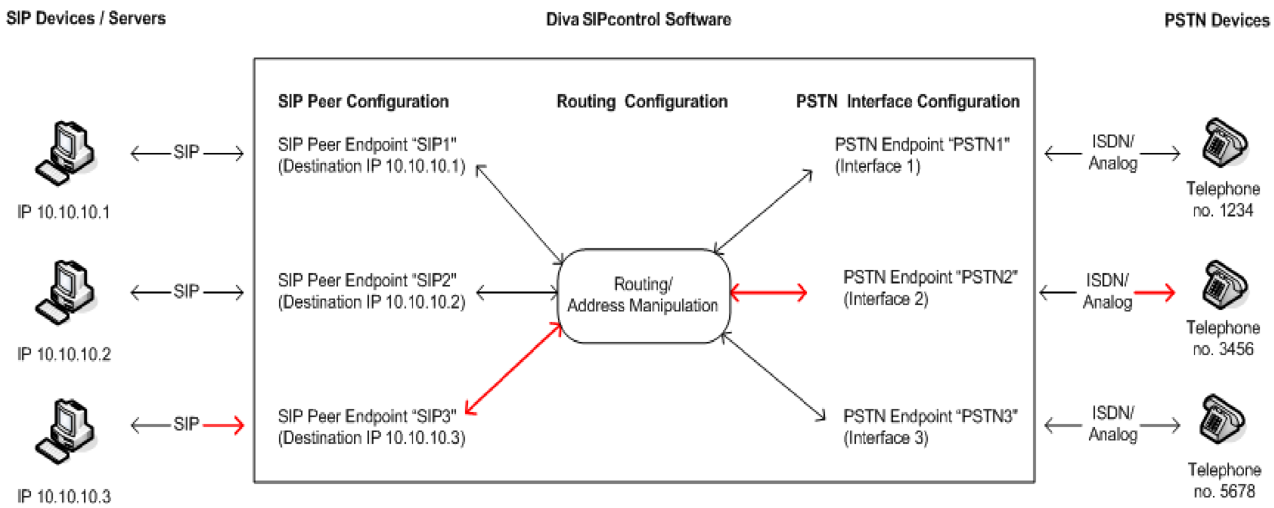


7. Upload the key file, the certificate file, and the certificate authority file. To do so, open the Diva SIPcontrol web interface and on the left hand side click **SIPcontrol configuration**.
8. Click **Security Profiles** and then **Details**.
9. Next to **Key file**, click **Browse**, go to the folder where you stored the file, and click **Open** to upload it.
10. Repeat the procedure in step 9 for the certificate file and the certificate authority file.
11. In **Authentication mode**, select how the server-client authentication should be handled.
12. Click **OK** to close the **Security Profiles** window.
13. At the bottom of the Diva SIPcontrol web interface click **Save** to save the configuration.
14. Since changes in the Security Profiles require a restart, click **Service status** at the left hand side of the web interface and then click **Restart SIPcontrol**.

CHAPTER 7

How Calls Are Processed

The Dialogic® Diva® SIPcontrol™ Software uses an endpoint-based approach to process calls, which means that every PSTN interface and every configured SIP peer is considered as a single endpoint. The endpoint saves the Diva SIPcontrol software settings for the respective PSTN interface or SIP peer. Each call originates at a specific endpoint (on the SIP side after assigning the SIP call request to one of the configured peers) and needs a route to find its designated endpoint (the destination). Thus, the most simple configuration needs one PSTN endpoint, one SIP peer, and one route as shown in red in the graphic below.



This graphic shows that an endpoint is only a virtual object of a real device. The endpoint saves the settings for the corresponding device. For example, if a call should be routed from SIP device 3 to PSTN device 2 as marked red in the graphic, then:

- The settings of SIP device 3 need to be configured as SIP peer endpoint in the **SIP Peer Configuration**,
- the settings PSTN device 2 needs to be configured as PSTN endpoint in the **PSTN Interface Configuration**, and
- the condition "called address is 3456" needs to be configured in the **Routing Configuration** to route the call to the correct device.

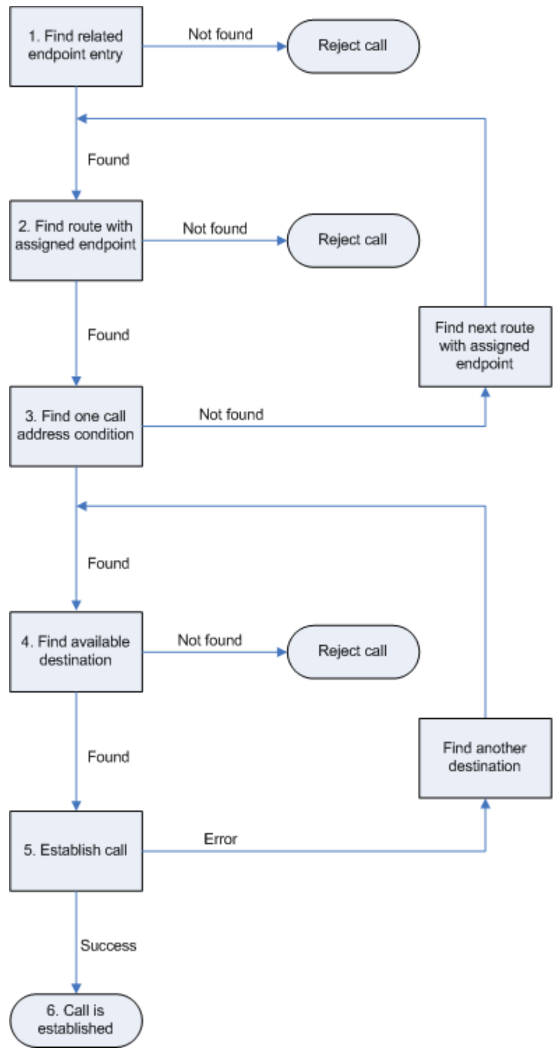
If you have for example a SIP or PSTN device 4 with no endpoints configured in the Diva SIPcontrol software, then you cannot establish a call, because the Diva SIPcontrol software will not know the settings of the device.

The PSTN endpoint is found via its controller number. On the SIP side, multiple SIP peers may connect via the same network interface. Therefore, the assignment is more complex:

1. The host/domain name and port number of the received "FROM" header is compared against the SIP peer settings.
2. If no host matches, the same address is compared against the "Domain" parameters of the SIP peers.
3. If no match is found, the Diva SIPcontrol software looks for a SIP peer with the **Default SIP to PSTN Peer** option enabled.
4. If the call cannot be assigned, regardless of whether the call originated in the PSTN or SIP network, the call is rejected.

Every route defines only one direction. Therefore, at least two routes are needed to support both PSTN-to-SIP and SIP-to-PSTN connections. The basic call (without address manipulation) is processed as follows:

1. Find and assign an endpoint for an incoming call request (PSTN: lookup by CAPI controller number; SIP: lookup by "From" address of received message).
2. Go sequentially through the list of routes and find the first route that has this endpoint defined in its configured sources list.
3. Determine whether at least one call address condition of this route matches simultaneously the called, calling, and redirected addresses of the call request; if not, find another route.
4. If any route condition matches, verify in the list of configured destinations which one is the most preferred. This is done based on settings. See Some things to know about call processing below for more information.
5. Try to establish the call via this destination. If the destination is unavailable or rejects the call, try the next destination of the route. Note that the call will be aborted immediately if a cause code is received that signals final failure, e.g., user busy or unallocated number.
6. The call is established.



Some things to know about call processing

- Each route may point to several destinations, between which the Diva SIPcontrol software chooses according to the following settings (in decreasing order of importance):
  - availability (destination enabled),
  - alive state of destination (if enabled to be verified),
  - priority (Master/Slave),
  - channel load quota (a factor calculated by comparing used vs. total supported channels).
- For each call only one route is chosen. Even if another route would also match the call criteria, only the first matching route is ever evaluated. Therefore, default routes should be created carefully.
- Load balancing/failover is only performed between the destinations of a single route.
- Routes without any conditions always match (as long as the source endpoint is listed in route sources).

Emergency calls

In many environments, certain numbers, e.g., 110/112 in Germany or 911 in the U.S., have to be handled differently from others. For example, they might need to be dialed without any access digit.

This can be achieved by creating an additional route from any configured SIP peers to one or more PSTN interfaces and setting the called address expression to the emergency number(s). The route should be placed at the top position in the list. Should there be a dialplan and/or address map configured for the respective PSTN interfaces, it may be necessary to add another regular expression to the address maps of the interfaces to handle those calls.

Routing conditions

The Dialogic® Diva® SIPcontrol™ Software organizes the conditions of a route in a list. Each list entry consists of different expressions for called, calling, and redirected address. The route matches only if all three expressions simultaneously match the respective call addresses. Empty expressions are considered to match, so there is no need to add wildcards into unused expressions. As a result, if a call should match either a called address or a calling number, two list entries have to be created, with called expression in the first and calling expression in the second row. If both have to match concurrently, both expressions have to be entered into the same list entry.

Routing examples

This section describes the configuration of four possible routing scenarios:

Direct routing between one PSTN interface and one SIP peer below

Connect two SIP peers to two PSTN interfaces exclusively on page 60

Connect two SIP peers to the same PSTN interface on page 60

Load balancing or failover between two SIP peers on page 61

Direct routing between one PSTN interface and one SIP peer

If you choose to route all calls from the PSTN to the same SIP peer, and calls from that SIP peer to the PSTN, configure the parameters as follows. For this configuration, no address rewriting is needed:

1. Under **PSTN Interface Configuration**, enable and configure all PSTN interfaces connected to a PBX. Confirm each dialog box with **OK**.
2. Under **SIP Peer Configuration**, create a SIP peer with the necessary settings and make sure that the option **Default SIP to PSTN peer** is enabled. Confirm with **OK**.
3. Under **Routing Configuration**, create route no. 1 and do the following:
   - Select **PSTN to SIP** as direction.
   - Enable all required PSTN interfaces.
   - Select the SIP peer configured in step 2 as the **Master** destination.
   - Set the parameter **Number format** to **Unchanged**.
   - Confirm with **OK**.
4. Under **Routing Configuration**, create route no. 2 and do the following:
   - Select **SIP to PSTN** as direction.
   - Enable the SIP peer configured in step 2 as source peer.
   - Enable all required PSTN interfaces as the **Master** destination.
   - Set the parameter **Number format** to **Unchanged**.
   - Confirm with **OK**.
5. Save the configuration in the main configuration interface.

Connect two SIP peers to two PSTN interfaces exclusively

If you choose to connect two SIP peers to two PSTN interfaces, so that each SIP peer may use one interface exclusively, then carry out the following configuration steps. The procedure is similar if you need to configure more PSTN interfaces, e.g., three PSTN interfaces to three SIP peers.

1. Under **PSTN Interface Configuration**, enable and configure the two PSTN interfaces. Confirm with **OK**.
2. Under **SIP Peer Configuration**, create both SIP peers and make sure the entry in **Domain** matches exactly the domain used by the SIP peer in its SIP address for outgoing calls. Do not enable the option **Default PSTN to SIP Peer** for any of these peers. Confirm with **OK**.
3. Under **Routing Configuration**, create route no. 1 and do the following:
   - Select **PSTN to SIP** as direction.
   - Enable the first PSTN interface as source.
   - Enable the first SIP peer configured in step 2 as the **Master** destination.
   - Confirm with **OK**.
4. Under **Routing Configuration**, create route no. 2 and repeat step 3 for the second PSTN interface and the second SIP peer.
5. Under **Routing Configuration**, create route no. 3 and do the following:
   - Select **SIP to PSTN** as direction.
   - Enable the first SIP peer configured in step 2 as source peer.
   - Enable the first PSTN interfaces as the **Master** destination.
   - Confirm with **OK**.
6. Under **Routing Configuration**, create route no. 4 and repeat step 5 for the second PSTN interface and the second SIP peer.
7. Save the configuration in the main configuration interface.

Connect two SIP peers to the same PSTN interface

If you want to connect two SIP peers to the same PSTN interface so that all calls from the PSTN are sent to the first SIP peer if the numbers begin with "1" and to the second peer if the numbers begin with "2", configure the parameters as follows:

1. Under **PSTN Interface Configuration**, enable and configure the PSTN interface. Confirm with **OK**.
2. Under **SIP Peer Configuration**, create both SIP peers and make sure the entry in **Domain** matches exactly the domain used by the SIP peer in its SIP address for outgoing calls. Do not enable the option **Default PSTN to SIP Peer** for any of these peers. Confirm with **OK**.
3. Under **Routing Configuration**, create route no. 1 and do the following:
   - Select **PSTN to SIP** as direction.
   - Enable the first PSTN interface as source.
   - Enable the first SIP peer configured in step 2 as the **Master** destination.
   - Under **Conditions**, click **Add** and set the **Called address** to "1.*".
   - Confirm with **OK**.
4. Under **Routing Configuration**, create route no. 2 and repeat step 3 for the second SIP peer with the only difference that the called address condition for this route is "2.*".
5. Under **Routing Configuration**, create route no. 3 and do the following:

- Select **SIP to PSTN** as direction.
- Enable both SIP peers as source peer.
- Enable the first PSTN interfaces as the **Master** destination.
- Confirm with **OK**.

6. Save the configuration in the main configuration interface.

If calls other than those beginning with 1 or 2 should also be directed to one peer, remove the condition from the respective PSTN to SIP route and move the route to the end of the list.

Load balancing or failover between two SIP peers

If two SIP servers should be configured as load balancing or failover, configure the following:

1. Under **PSTN Interface Configuration**, enable and configure all required PSTN interfaces. Confirm with **OK**.

2. Under **SIP Peer Configuration**, create both SIP peers and make sure the entry in **Domain** matches exactly the domain used by the SIP peer in its SIP address for outgoing calls. Do not enable the option **Default PSTN to SIP Peer** for any of these peers. If you configure a failover, SIP peer 1 (the master) should have the option **Alive check** enabled. Confirm with **OK**.

3. Under **Routing Configuration**, create route no. 1 and do the following:

- Select **PSTN to SIP** as direction.
- Enable the first PSTN interface as source.
- Enable the first SIP peer configured in step 2 as the **Master** destination. For load-balancing configurations, SIP peer no. 2 should be configured as the **Master** destination and for failover configurations it should be configured as **Slave** destination.
- Confirm with **OK**.

4. Under **Routing Configuration**, create route no. 2 and do the following:

- Select **SIP to PSTN** as direction.
- Enable both SIP peers as source peer.
- Enable the first PSTN interfaces as the **Master** destination.
- Confirm with **OK**.

5. Save the configuration in the main configuration interface.

6. Under **Routing Configuration**, create route no. 2 and repeat step 3 for the second SIP peer with the only difference that the called address condition for this route is "2.*".

7. Under **Routing Configuration**, create route no. 3 and do the following:

- Select **SIP to PSTN** as direction.
- Enable both SIP peers as source peer.
- Enable the first PSTN interfaces as the **Master** destination.
- Confirm with **OK**.

8. Save the configuration in the main configuration interface.

If calls other than those beginning with 1 or 2 should also be directed to one peer, remove the condition from the respective PSTN to SIP route and move the route to the end of the list.

CHAPTER 8

How Call Addresses Are Processed

The call addresses provided by the caller may be modified at different stages of the call processing within the Dialogic® Diva® SIPcontrol™ Software. The reason for multiple manipulation is that it allows for modifying the address where it is needed, which means that more complex environments can be configured with less effort, since data does not need to be entered redundantly at different places. It also makes it easier to "team" SIP peers or PSTN interfaces with different settings.

The Diva SIPcontrol software converts addresses automatically, without any intervention from the user. This means that the Diva SIPcontrol software adds or removes a special prefix to a number with a known number type, e.g. "+" for international numbers, when converting between a number and an address. See Common formats: on page 66 for a list of prefixes.

Note: Number type flags from digital networks, e.g., ISDN or SS7 are converted into special prefixes on the SIP side. International numbers get a "+" prefix, national numbers get an "N" prefix, and subscriber numbers get an "S" prefix.

The automatic conversions are done for calling numbers, called numbers, and redirected numbers.

Possible scenarios

- At a PSTN interface, a line access digit must be prepended in order to call to the public network, while another PSTN interface is directly connected and does not need an access digit.

  Solution: Add a regular expression to outbound address map of the first interface.
- All calls to a number beginning with "9" shall be routed to one specific SIP peer while removing this digit.

  Solution: Manipulate the called number in the route.This way the SIP peer may also receive calls to other numbers (via other routes) without having to deal with different number formats.
- SIP peer "A" needs the dialed numbers to be formatted in E.164 format, while SIP peer "B", which is in load-balancing or fail-over partnership with "A", needs it in an extension-only format.

  Solution: Define different number formats in the SIP peer settings.
- SIP peer "A" is located at a different location than SIP peer "B", e.g., London and Stuttgart. Therefore, both need different location settings regarding country and area codes, etc.

  Solution: Create different dialplans and assign each dialplan to one SIP peer.

How addresses are manipulated

Note: Each step is optional.

1. Save the inbound call addresses as "A".
2. Apply the "address map inbound" of the endpoint assigned to the call setup request to "A", resulting in "B".
3. To check the first route: apply the number format settings of the route together with the dialplan of the source endpoint to the call addresses "B", resulting in "C".
4. Check the route as described in the route processing section (5) against addresses "C". If the route does not match, discard the changes and try the next route with "B" again.
5. If the route matches, apply the route address map to the addresses "C", resulting in "D".
6. After selecting one of the destinations of the route, normalize the addresses "D" using the dialplan and number format of the destination endpoint, resulting in addresses "E".
7. Apply the outbound address map of the destination endpoint to "E", giving the effective call addresses "F" sent to the destination.
8. If the call to the selected destination endpoint fails and if there are other endpoints in a fail-over configuration, start with step 6 again with the respective settings of the next endpoint.

CHAPTER 9

How Address Maps Are Processed

Address maps are processed as follows:

1. Get the first map rule of the address map.
2. Verify if called, calling, and redirect expression each match the respective part of the call addresses (or are empty). If not, verify the next map rule.
3. If all three expressions match, apply each format string of the rule to the respective address match.
4. If the option **Stop on match** is enabled, stop processing. Otherwise, continue with the next rule as described in step 2.

CHAPTER 10

How Numbers Are Processed

The Dialogic® Diva® SIPcontrol™ Software provides two mechanisms for number processing. Both mechanisms can be used together:

1. Number normalization based on a dialplan as described below.
2. Number modification using regular expressions as described on page 65.

Number normalization based on a dialplan

The number normalization based on a dialplan can work in an environment in which the Diva SIPcontrol software is connected to a private SIP network and a public switched telephone network (PSTN), optionally with a PBX between the PSTN and the Diva SIPcontrol software. If the Diva SIPcontrol software is used as a gateway between a private circuit switched network and a public SIP-based network, the number normalization function of the Diva SIPcontrol software should not be used.

The Diva SIPcontrol software also supports dialplans using the North American numbering plan (NANP). See North-American numbering plan: on page 45 for more information.

The number normalization is done in two steps:

1. The received called, calling and redirected numbers are analyzed based on the dialplan configured for the PSTN Interface or SIP Peer.
2. The number is converted into the configured target format. Six target formats are available:
   - **International number with prefixes**: All numbers are converted to an international number with the prefix for international calls and, if required, an outside access digit.
   - **International number with number type**: All numbers are converted to an E.164 number with the number type flag set to "international" ("+" is used in SIP addresses).
   - **National number with prefixes**: If possible, all numbers are converted to a national number with the prefix for national calls and an outside access digit, as required. Exception: Numbers with different country code will be converted to an international number with prefix for international calls and outside access digit, if required.
   - **National number with number type**: If possible, all numbers are converted to a national number with the number type flag set to "national". Exception: Numbers with different country code will be converted to an international number with number type set to "international". **Note:** This target format should not be used for calls to SIP networks.
   - **Extension only with prefixes**: All numbers are reduced as much as possible; only the required prefixes are prepended.
   - **Extension only with number type**: All numbers are reduced as much as possible. Instead of prefixes the appropriate number type is set. **Note:** This target format should not be used for calls to SIP networks.

Important information about the outside access digit configuration

- Configure the outside access digit only if there is a PBX between the PSTN and the Diva SIPcontrol software, and if this PBX requires the outside access digit for external calls. If you need to configure the outside access digit, also configure the following related options:
  - **Incoming PSTN access code provided by the PBX**: This option defines whether the Diva SIPcontrol software expects the outside access digit in the calling number in external calls from the PBX.
    The PBX normally prepends the outside access digit to the calling number in incoming external calls in order to enable callback functionality at internal phones. If this is the case, enable this option.
  - **PSTN access code provided by the SIP caller**: This option defines whether the Diva SIPcontrol software expects the outside access digit in the called number in external calls from the SIP side to the PSTN.
    It is normally required to prepend the outside access digit to call an external number from an internal phone. In this case, these are phones on the SIP side. However, in some configurations this is not required, especially in a configuration that is part of the North-American numbering plan (NANP), where an internal number can be identified based on its length. If it is possible to identify an internal call purely by the

length of the called number, this option can be disabled. In all other configurations with outside access digit this option has to be enabled.
It is recommended to have this option enabled in dialplans with outside access digit.

- The Diva SIPcontrol software's number normalization function does not remove outside access digits as a PBX can for external calls. If the Diva SIPcontrol software needs to behave like a PBX with an outside access digit for external calls, use the Address Map functionality in combination with a Routing module.

Number modification using regular expressions

The Dialogic® Diva® SIPcontrol™ software organizes regular expressions into address maps, and each endpoint or route may be assigned one map. Each address map contains a number of regular expressions together with the respective output format string that ensures that virtually every required manipulation scheme can be configured.

By using separate address maps, instead of rules embedded into the routes and endpoints, it is possible to share the same settings across different objects. For example, if several PSTN interfaces are connected to the same PBX, they will most probably be configured with the same settings and, therefore, can share an address map that the Diva SIPcontrol software lets you assign for each individual controller.

The Diva SIPcontrol software uses the style of regular expressions used by Perl. Most tutorials and how-to's covering Perl regular expressions can apply to the Diva SIPcontrol software.

Common expressions:

Character	Meaning
.	Matches any character
^	Matches the beginning of a number only
$	Matches the end of a number
\+	Matches the plus sign ("+")
*	Matches any number of occurrences of the previous character
{n}	Matches the previous character exactly n times
{n,m}	Matches the previous character between n and m times, both inclusive
( )	Marks a sub-expression to be referenced in format string and also groups sets of characters
|	Alternate operator, matches either the left or right sub-expression
[ ]	Matches any character given within the square brackets, i.e [123] matches either 1, 2, or 3, but not 4, 5, or 123.

Common formats:

Character	Meaning
0-9,+	Inserts the respective character into the output
(?n(digits))	Inserts the digits given only if the n^{th} sub-expression of the expression matched
$&	Outputs what matched the whole expression
$n	Outputs the n^{th} matched sub-expression
+	Indicates an international number type, if it is the first character in the string
N	Indicates a national number type, if it is the first character in the string
S	Indicates a subscriber number type, if it is the first character in the string
$(S)	Inserts the current calling (source) number
$(D)	Inserts the called (destination) number
$(R)	Inserts the first redirected number
$(R2)	Inserts the second redirected number
$(Rn)	Inserts the n^{th} redirected number (up to the 9th)

Examples

Note: In all examples, the hyphen ("-") is only used for clarification. It must not be included either in the dialed numbers or in the configured expressions and formats.

The examples may be used for calling or called number normalization for both the inbound and outbound directions.

Omit the prefix digits

Task: A leading "33" prefix should be removed from the number.

Example: 33-444-5555 should be converted to 444-5555.

Expression entry: ^33

Format entry: (none)

Note: If the number does not start with "33", it passes unchanged.

Add the prefix digits

Task: The number needs the leading prefix "9".

Example: 444-5555 should go out as 9-444-5555.

Expression entry: .*

Format entry: 9$&

Replace the international number type by prefix

Task: A call that is indicated as an international call should be placed with prefixes instead.

Example: The number +1-472-333-7777 should be dialed as 011-472-333-7777

Expression entry: ^\+

Format entry: 01

Replace the international dial prefix by number type

Task: A call that has an international dial prefix should be placed with an international number type instead of the prefix.

Example: The number (01)1-472-333-7777 should be dialed as +1-472-333-7777

Expression entry: ^01

Format entry: +

Replace an extension by another

Task: Calls for specific extensions should be indicated with other extensions.

Example: The extension 1111 should be replaced by 2222, and extension 3333 by extension 4444.

First expression entry: 1111(@.*)?$

First format entry: 2222

Stop on Match: true

Second expression entry: 3333(@.*)?$

Second format entry: 4444

Stop on Match: true

Note: This example applies only for calls from the SIP to the PSTN.

Replace the "N" in a national number

The "N" can be set to signal a number as national number.

Task: Replace the "N" in a national number with the national prefix.

Example: N123-45678 should be signaled as 0123-45678

Expression: ^N

Format entry: 0

Display the "user=phone" parameter without E.164

The "user=phone" parameter is set automatically if the number is a valid "tel:" URI. The number is either in E.164 format or has the "phone-context=XXX" parameter added. If you need the "user=phone" without E.164, you need to provide the phone-context parameter.

Task: Display "user=phone" parameter without E.164 and provide phone-context parameter.

Example: Present the phone number +1(123)727-0203 without E.164.

Expression: ^(.*)

Format entry: $1;phone-context=+1(123)$1

CHAPTER 11

Software Uninstallation

Note: If you want to upgrade from Dialogic® Diva® SIPcontrol™ Software version 1.5.1, DO NOT uninstall the software before you install the current Diva SIPcontrol software version, because you might lose some settings, including your regular expressions.

The uninstallation procedure depends on the installed operating system:

To uninstall the Diva SIPcontrol software under Windows® XP or Windows Server® 2003:

1. Click **Start** > **Settings** > **Control Panel**.
2. Double-click **Add or Remove Programs**.
3. In the **Add or Remove Programs** box, select the Diva SIPcontrol software and click **Remove**.
4. When you are asked if you want to remove the Diva SIPcontrol software from your computer, confirm with **Yes**.
5. The Diva SIPcontrol software is now uninstalled.
6. If you want to uninstall the Dialogic® Diva® System Release software, see the Dialogic® Diva® System Release Reference Guide, which is available on the Dialogic web site: www.dialogic.com.

To uninstall the Diva SIPcontrol software under Windows Vista®, Windows Server® 2008, or Windows® 7:

1. Click **Start** > **Control Panel > Programs**.
2. Click **Uninstall a program**.
3. In the displayed window, right-click the Diva SIPcontrol software entry and select **Uninstall**.
4. If you are asked either to **Cancel** or **Allow** the uninstallation, click **Allow** to proceed.
5. The Diva SIPcontrol software is now uninstalled.
6. If you want to uninstall the Dialogic® Diva® System Release software, see the Dialogic® Diva® System Release Reference Guide, which is available on the Dialogic web site: www.dialogic.com.

CHAPTER 12

Cause Code Mapping

If the Dialogic® Diva® SIPcontrol™ Software uses Microsoft® Office Communications Server 2007 as SIP peer, the cause/response code tables are used as specified by Microsoft. See Default cause code mapping for Microsoft® Office Communications Server (OCS) 2007 SIP peers on page 72 for a detailed list of cause/response codes.

If the Diva SIPcontrol software does not use Microsoft® OCS 2007, the default cause/response code mapping is used. See Default cause code mapping below for a detailed list of cause/response codes.

Default cause code mapping

The Diva SIPcontrol software includes a default cause/response code mapping table that includes the most common cause codes according to RFC 3398 and RFC 4497. If you need to define a cause code mapping other than in the table, you can configure it in the Cause Code Mapping Configuration.

For ISDN to SIP code mappings, see ISDN cause code to SIP response code below.

For SIP to ISDN code mappings, see SIP response code to ISDN cause code on page 71.

ISDN cause code to SIP response code

ISDN cause code	Description	SIP response code forwarded to the SIP peer	Description
1	Unallocated number	404	Not found
2	No route to specified transit network	404	Not found
3	No route to destination	404	Not found
16	Normal call clearing	603	Decline (The PBX of Philips sends this code during call set-up if the user rejects the call.)
17	User busy	486	Busy here
18	No user response	603	Decline (The PBX of Philips sends this code during call set-up if the user rejects the call.)
19	No answer from the user	480	Temporarily unavailable
20	Subscriber absent	480	Temporarily unavailable
21	Call rejected	603	Decline
22	Number changed	410	Gone
23	Redirection to new destination	410	Gone
26	Non-selected user clearing	404	Not found
27	Destination out of order	502	Bad gateway
28	Address incomplete	484	Address incomplete
29	Facility rejected	501	Not implemented
31	Normal, unspecified	480	Temporarily unavailable
34	No circuit available	503	Service unavailable
38	Network out of order	503	Service unavailable
41	Temporary failure	503	Service unavailable
42	Switching equipment congestion	503	Service unavailable

ISDN cause code	Description	SIP response code forwarded to the SIP peer	Description
47	Resource unavailable	503	Service unavailable
55	Incoming class barred within Closed User Group (CUG)	403	Forbidden
57	Bearer capability not authorized	403	Forbidden
58	Bearer capability not presently available	503	Service unavailable
63	Service or option not available, unspecified	488	Not acceptable here
65	Bearer capability not implemented	488	Not acceptable here
69	Requested Facility not implemented	501	Not implemented
70	Only restricted digital available	488	Not acceptable here
79	Service or option not implemented	501	Not implemented
87	User not member of Closed User Group (CUG)	403	Forbidden
88	Incompatible destination	503	Service unavailable
102	Recover on Expires timeout	504	Server time-out
111	Protocol error	503	Service unavailable
127	Interworking, unspecified	503	Service unavailable
Any code other than listed above:		500	Server internal error

SIP response code to ISDN cause code

SIP response code from the SIP peer	Description	ISDN cause code	Description
400	Bad Request	41	Temporary failure
401	Unauthorized	21	Call rejected
402	Payment required	21	Call rejected
403	Forbidden	21	Call rejected
404	Not found	1	Unallocated number
405	Method not allowed	63	Service or option unavailable
406	Not acceptable	79	Service/option not implemented
407	Proxy authentication required	21	Call rejected
408	Request timeout	41	Temporary failure
410	Gone	22	Number changed
413	Request entity too large	63	Service or option unavailable
414	Request-URI too long	63	Service or option unavailable
415	Unsupported media type	79	Service/option not implemented
416	Unsupported URI scheme	79	Service/option not implemented
420	Bad extension	79	Service/option not implemented
421	Extension required	79	Service/option not implemented
423	Interval too brief	63	Service or option unavailable
429	Provide Referrer Identity	31	Normal, unspecified
480	Temporarily unavailable	19	No answer from the user
481	Call/transaction does not exist	41	Temporary failure
482	Loop detected	25	Exchange routing error
483	Too many hops	25	Exchange routing error
484	Address incomplete	28	Invalid number format (address incomplete)
485	Ambiguous	1	Unallocated number
486	Busy here	17	User busy
487	Request Terminated	127	Interworking, unspecified
488	Not acceptable here	65	Bearer capability not implemented
500	Server internal error	41	Temporary failure
501	Not implemented	79	Service/option not implemented
502	Bad gateway	38	Network out of order
503	Service unavailable	63	Service or option unavailable
504	Server time-out	41	Temporary failure
505	Version not supported	79	Service/option not implemented
513	Message too large	63	Service or option unavailable
600	Busy everywhere	17	User busy
603	Decline	21	Call rejected
604	Does not exist anywhere	1	Unallocated number

SIP response code from the SIP peer	Description	ISDN cause code	Description
606	Not acceptable	65	Bearer capability not implemented
Any code other than listed above:		31	Normal, unspecified

Default cause code mapping for Microsoft® Office Communications Server (OCS) 2007 SIP peers

The Dialogic® Diva® SIPcontrol™ Software includes a default cause/response code mapping table for Microsoft® OCS 2007 SIP peers that includes the most common (as of the date of publication of this document) cause codes according to RFC 3398 and RFC 4497. If you need to define a cause code mapping other than in the table, you can configure it in the Cause Code Mapping Configuration.

For ISDN to SIP code mappings, see Microsoft® OCS 2007 ISDN cause code to SIP response code below.

For SIP to ISDN code mappings, see Microsoft® OCS 2007 SIP response code to ISDN cause code on page 73.

Microsoft® OCS 2007 ISDN cause code to SIP response code

ISDN cause code	Description	SIP response code forwarded to Microsoft® OCS 2007	Description
1	Unallocated number	404	Not found
2	No route to specified transit network	404	Not found
3	No route to destination	404	Not found
16	Normal call clearing	603	Decline (The PBX of Philips sends this code during call set-up if the user rejects the call.)
17	User busy	486	Busy here
18	No user response	408	Request timeout
19	No answer from the user	480	Temporarily unavailable
20	Subscriber absent	480	Temporarily unavailable
21	Call rejected	603	Decline
22	Number changed	410	Gone
23	Redirection to new destination	410	Gone
26	Non-selected user clearing	404	Not found
27	Destination out of order	502	Bad gateway
28	Address incomplete	484	Address incomplete
29	Facility rejected	501	Not implemented
31	Normal, unspecified	480	Temporarily unavailable
34	No circuit available	503	Service unavailable
38	Network out of order	503	Service unavailable
41	Temporary failure	503	Service unavailable
42	Switching equipment congestion	503	Service unavailable
47	Resource unavailable	503	Service unavailable
55	Incoming class barred within Closed User Group (CUG)	403	Forbidden

ISDN cause code	Description	SIP response code forwarded to Microsoft® OCS 2007	Description
57	Bearer capability not authorized	403	Forbidden
58	Bearer capability not presently available	503	Service unavailable
65	Bearer capability not implemented	488	Not acceptable here
69	Requested Facility not implemented	501	Not implemented
70	Only restricted digital available	488	Not acceptable here
79	Service or option not implemented	501	Not implemented
87	User not member of Closed User Group (CUG)	403	Forbidden
88	Incompatible destination	400	Bad request
102	Recover on Expires timeout	504	Server time-out
111	Protocol error	503	Service unavailable
127	Interworking, unspecified	500	Server internal error
Any code other than listed above:		500	Server internal error

Microsoft® OCS 2007 SIP response code to ISDN cause code

SIP response code from Microsoft® OCS 2007	Description	ISDN cause code	Description
400	Bad Request	41	Temporary failure
401	Unauthorized	21	Call rejected
402	Payment required	21	Call rejected
403	Forbidden	21	Call rejected
404	Not found	1	Unallocated number
405	Method not allowed	63	Service or option unavailable
406	Not acceptable	79	Service/option not implemented
407	Proxy authentication required	21	Call rejected
408	Request timeout	102	Recovery on timer expiry
410	Gone	22	Number changed
413	Request entity too large	127	Interworking, unspecified
414	Request-URI too long	127	Interworking, unspecified
415	Unsupported media type	79	Service/option not implemented
416	Unsupported URI scheme	127	Interworking, unspecified
420	Bad extension	127	Interworking, unspecified
421	Extension required	127	Interworking, unspecified
423	Interval too brief	127	Interworking, unspecified
429	Provide Referrer Identity	31	Normal, unspecified
480	Temporarily unavailable	18	No user responding
481	Call/transaction does not exist	41	Temporary failure

SIP response code from Microsoft® OCS 2007	**Description**	**ISDN cause code**	**Description**
482	Loop detected	25	Exchange routing error
483	Too many hops	25	Exchange routing error
484	Address incomplete	28	Invalid number format (address incomplete)
485	Ambiguous	1	Unallocated number
486	Busy here	17	User busy
487	Request Terminated	127	Interworking, unspecified
488	Not acceptable here	65	Bearer capability not implemented
500	Server internal error	41	Temporary failure
501	Not implemented	79	Service/option not implemented
502	Bad gateway	38	Network out of order
503	Service unavailable	41	Temporary failure
504	Server time-out	102	Recovery on timer expiry
505	Version not supported	127	Interworking, unspecified
513	Message too large	127	Interworking, unspecified
600	Busy everywhere	17	User busy
603	Decline	21	Call rejected
604	Does not exist anywhere	1	Unallocated number
606	Not acceptable	65	Bearer capability not implemented
Any code other than listed above:		31	Normal, unspecified

CHAPTER 13

Event Logging

A computer with the Dialogic® Diva® SIPcontrol™ Software installed may write the following types of events into the System Event Log:

- Errors
- Warnings
- Informational messages

You can view the events in the Windows® Event Viewer. To do so, click **Programs** > **Settings** > **Control Panel** > **Administrative Tools**. In the **Administrative Tools** window, double-click **Event Viewer** and then **Application**, where the Diva SIPcontrol software stores the events.

Errors

An error is a significant problem, such as loss of data or loss of functionality. For example, if a service fails to load, an error event will be logged.

See below for possible error events. Variables are enclosed in angle brackets. Parameters enclosed in square brackets are optional:

Event ID	Event Text	Event Description
2000	Service could not start. <Reason>	The <Reason> is text that explains why the service could not start.
2001	Service could not stop. <Reason>	The <Reason> is text that explains why the service could not stop.
2002	Updating configuration failed. <Reason>	The new configuration could not be activated, probably due to invalid configuration data.
2003	Cannot bind to IP address. <IP address>:<port> [<protocol>].	The service cannot be bound to the IP address.
2004	TLS initialization failed, call attempt aborted.	The configured TLS settings are invalid, or a required file is missing. For calls to SIP only: the call is aborted unless an alternate destination without TLS encryption is available.

Warnings

A warning is an event that is not necessarily significant but may indicate a possible future problem.

See the following table for possible warnings. Variables are enclosed in angle brackets:

Event ID	Event Text	Event Description
3000	SIP peer <Host Name> is not available.	The SIP peer does not respond to keep-alive check requests, and has therefore been marked as inactive. It will receive no calls from SIPcontrol until the ongoing keep-alive check receives valid responses.
3001	Cannot process call from <Calling Number> to <Called Number>. No more licenses available.	The number of currently active calls has reached the number of licensed channels and a further call has been declined thereof. The <Calling Number> and <Called Number> of the PSTN call are inserted as signaled from the line.
3002	Cannot process outgoing PSTN call to <Called Number> from <Calling Number>. No free PSTN channel available.	The <Called Number> and <Calling Number> are inserted. It can be a PSTN or SIP address.
3003	Call transfer to <Called Number> failed. <Optional Reason>	The <Called Number> is the PSTN-based number. The reason is optional and may contain any text.
3004	Registration to <Registrar Host Name> with user<User Host Name> failed.	The Registration to a Registrar with the user to register failed.
3005	SIP peer <Host Name> is available again.	An inactive SIP peer is alive again (has responded to alive check request)
3006	Cannot process call from <Calling Address> to <Called Address>. Codec negotiation failed.	A call could not be established because non of the audio codecs support by and allowed for the SIP peer could be used for the call and no alternative targets were available.
3007	Can not establish TLS connection to <address>: <Reason>.	No TLS connection could be established to the SIP peer. <Optional Reason> gives more details if available.
3008	TLS certificate verification failed with error <OpenSSL errorcode>.	The TLS certificate presented by the peer could not be verified successfully. The error code is the value returned by the TLS library.
3009	TLS Data Error	An error occurring during TLS data processing. The trace may give additional information.

Informational messages

Informational messages refer to successful operation events such as starting or stopping the service:

See the following for informal events. Variables are enclosed in angle brackets:

Event ID	Event Text	Event Description
4000	Service started.	Service has been started successfully.
4001	Service stopped.	Service was requested to stop or shutdown, and did so successfully.
4002	Configuration successfully updated.	Called when service configuration has been successfully updated.
4003	Call from <Calling Number> to <Called Number> established.	The <Calling Number> and the <Called Number> are inserted. The Number can be a PSTN or SIP address.
4004	Call from <Calling Number> to <Called Number> disconnected.	The <Calling Number> and the <Called Number> are inserted. The Number can be a PSTN or SIP address.
4005	Call from <Calling Number> successfully transferred to <Called Number>.	The <Calling Number> is the calling number. The <Called Number> is the number of the transfer destination.
4006	Registration to <Registrar Host Name> with user<User Host Name> is successful.	The registration to a registrar with the user to register is successful.
4008	Cannot process call from <Calling Number> to <Called Number>, <Reason>.	The <Calling Number> and <Called Number> are inserted, the SIP or Q.850 cause code text is inserted at runtime. Different reasons (busy, rejected,…) are translated to runtime.

4009	Available/changed licensed channels <Licensed channels>.	List the amount of licensed channels. If no license file is read, the default is "8" licensed channels. Issued if the licensed amount changes, e.g., after a new license file has been installed.
4010	Available/changed PSTN channels <PSTNChannels>.	Gives the amount of available channels to the telephone network. Called if the number changes due to configuration updates or controllers being enabled/disabled.

CHAPTER 14

Use Case Examples

The Dialogic® Diva® SIPcontrol™ Software is designed to support standard VoIP RFCs, therefore, the usage of the Diva SIPcontrol software is not limited to the described use case samples below. The Diva SIPcontrol software is interoperable with many applications, e.g., Asterisk or e-phone.

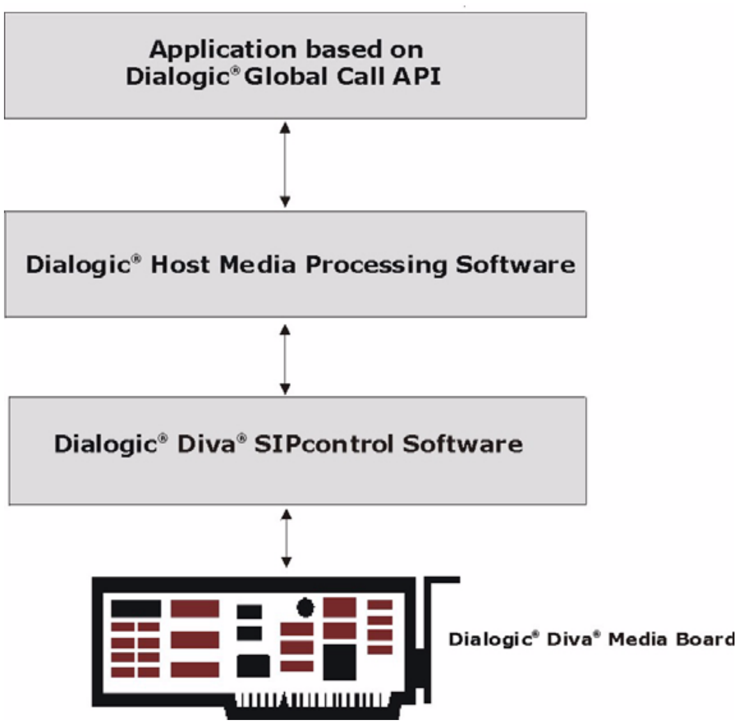
The following scenarios describe configurations for a gateway computer with the:

- Dialogic® Host Media Processing (HMP) software,
- Microsoft® Exchange Server,
- Microsoft® Office Communications Server.

The gateway computer is a server with a Dialogic® Diva® Media Board and the Diva SIPcontrol software installed. The use cases are based on Diva SIPcontrol software version 2.0.

Use case for Dialogic® HMP Software

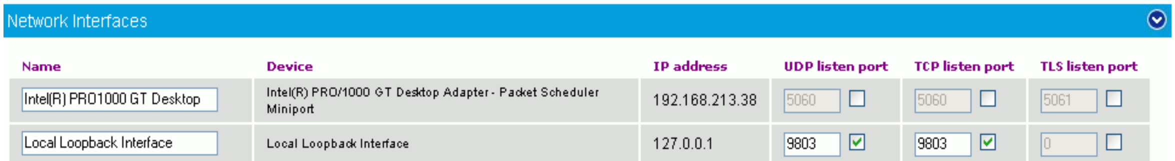
This use case describes the usage of the Dialogic® Host Media Processing (HMP) software running on the same computer as the Diva Media Board and the Diva SIPcontrol software as shown in the graphic below. However, the Diva SIPcontrol software supports also the interoperability with HMP over the LAN. The use case is based on HMP version 3.0WIN and 3.1LIN. In order for the application based on the Dialogic® Global Call API to connect with the Diva SIPcontrol software, it needs to be set to listen on port 5060 and to send SIP messages to the IP address 127.0.0.1 on port 9803.



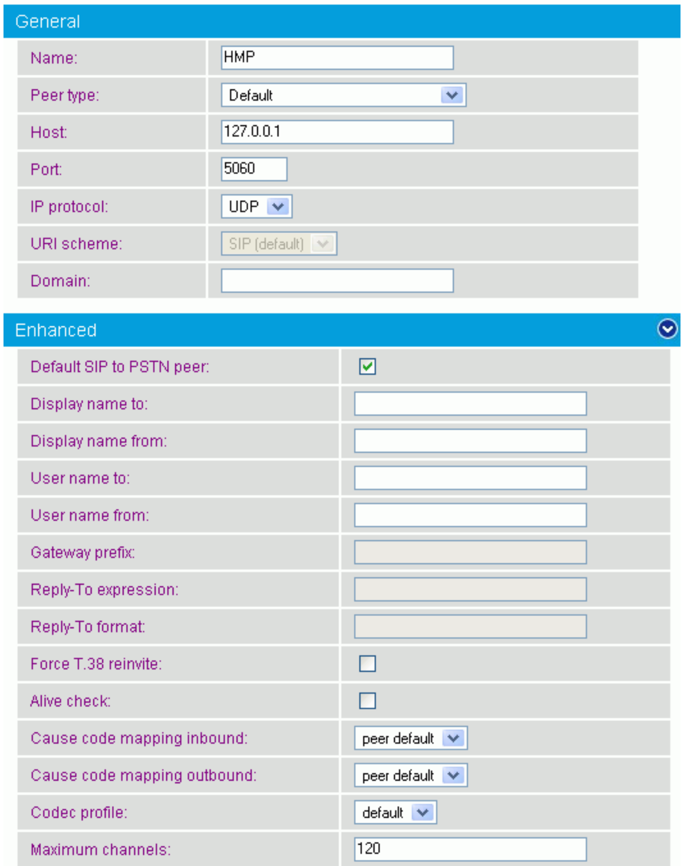
To configure the Diva SIPcontrol software to function with your Global Call application:

1. Open the Dialogic® Diva® SIPcontrol™ Software web interface to configure the required settings. To do so, click **Start** > **Programs** > **Dialogic Diva** > **SIPcontrol Configuration**.
2. In the Diva SIPcontrol software web interface, click **SIPcontrol configuration** on the left hand side to open the **SIPcontrol Configuration** page. For this configuration scenario, the network interface, a SIP peer, and two routings need to be configured.

3. Under **Network Interface Configuration**, set the **Local Loopback Interface** to **Enabled**, and as **SIP Listen Port** enter **9803**.



4. Open the **SIP Peer Configuration**, click **Add**, and configure the following parameters:



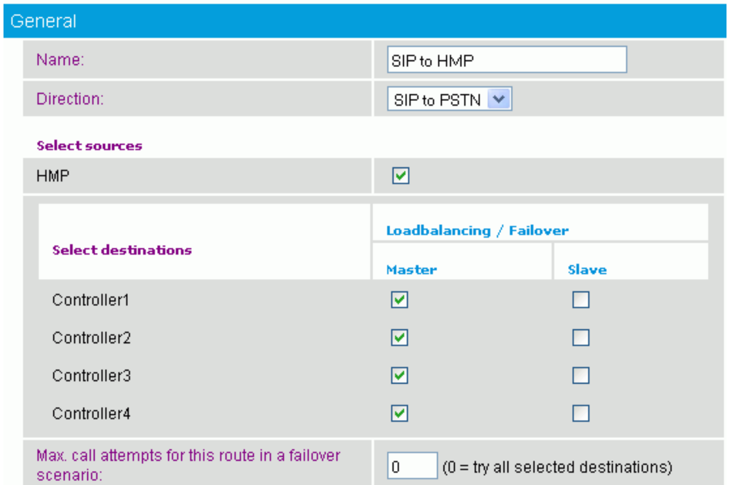
Under **Edit SIP Peer Configuration**, configure the following parameters:

- **Name**: Enter a unique name to easily identify the SIP peer.
- **Peer type**: Leave at **Default** setting.
- **Protocol**: Select **UDP**.

Under **Enhanced Configuration**, enable **Default SIP to PSTN peer**.

Click **OK** to save the settings and to close the window.

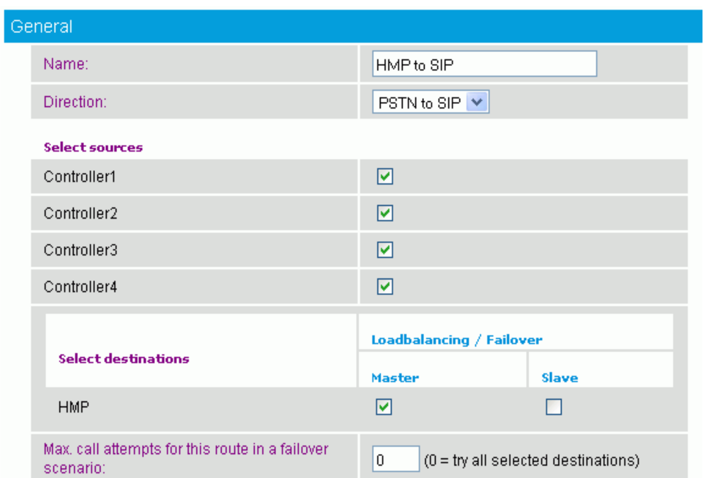
5. Create two routings, one for each direction (SIP to PSTN and PSTN to SIP). To configure the routing from SIP to PSTN, open the **Routing Configuration**, click **Add**, and configure the following parameters:



- **Name**: Enter a unique name to easily identify the routing.
- **Direction**: Select **SIP to PSTN** from the dropdown menu.
- **Select sources**: Select the above configured SIP peer as source.
- **Select destinations**: Select the controllers of the Diva Media Board.

Click **OK** to save the settings and to close the window.

6. For the routing from PSTN to SIP, click **Add** again, and configure the following parameters:



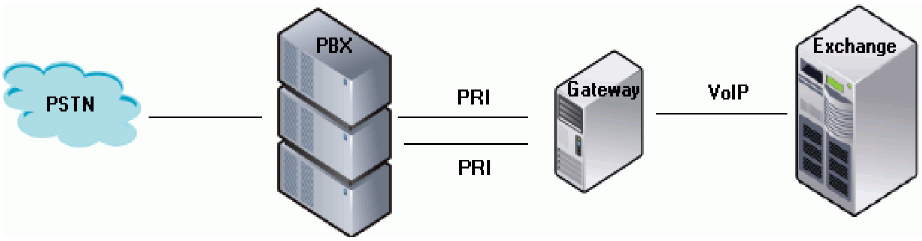
- **Name**: Enter a unique name to easily identify the routing.
- **Direction**: Select **PSTN to SIP** from the dropdown menu.
- **Select sources**: Select the controllers of the Diva Media Board.
- **Select destinations**: Select the above configured SIP peer as master destination.

Click **OK** to save the settings and to close the window.

7. Click **Save** in the main configuration page to save the settings and to activate the changes.

Use case for Microsoft® Exchange Server 2007

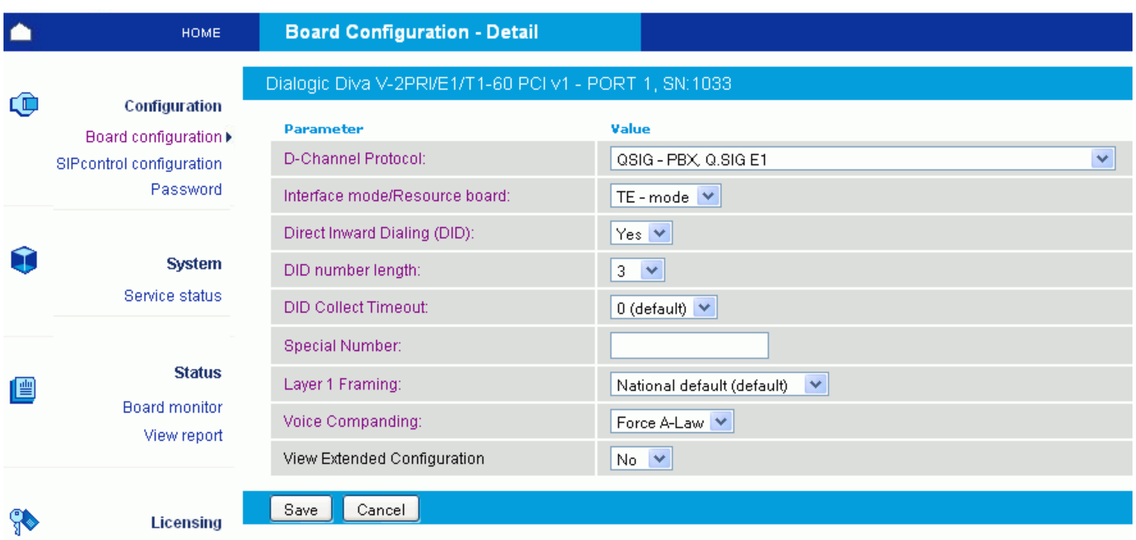
This configuration scenario describes the necessary steps to configure the gateway computer between the PBX and the Microsoft® Exchange Server 2007 as shown in the grapic.



1. Activate the fax license as described in License Activation on page 16.
2. Open the Dialogic® Diva® SIPcontrol™ Software web interface to configure the required parameters. To do so, click **Start** > **Programs** > **Dialogic Diva** > **SIPcontrol Configuration**.
3. In the Diva SIPcontrol software web interface, click **Board Configuration** on the left hand side to open the **Available Diva Boards** page.

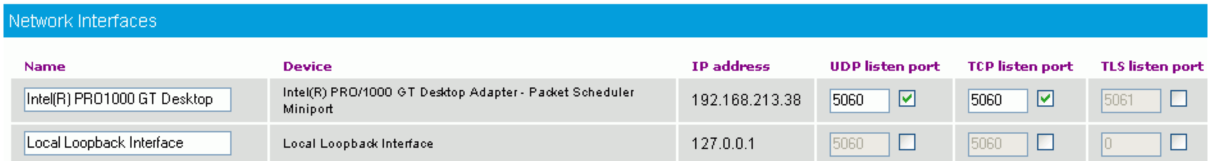
Click either the board icon or the name of the Dialogic® Diva® Media Board to open the **Board Configuration - Detail** page.

4. Configure the **D-Channel Protocol** of the PBX. In the example, **QSIG-PBX, Q.SIG E1** is selected. Click **Save**.

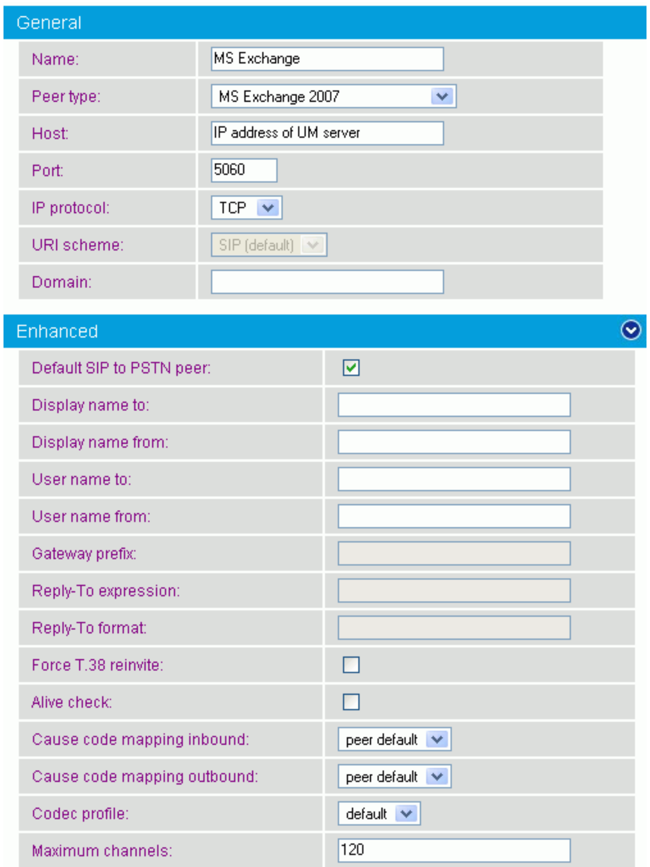


5. Repeat steps 3 and 4 for the other PRI line.
6. In the Diva SIPcontrol software web interface, click **SIPcontrol configuration** on the left hand side to open the **SIPcontrol Configuration** page. For this configuration scenario, the PSTN interface, the network interface, a SIP peer, and a routing need to be configured.

7. Go to **Network Interface Configuration**, set the **Listen Port** to **5060**, and check the **Enabled** box of your Ethernet adapter.



8. Configure the SIP peer settings. To do so, open the **SIP Peer Configuration**, click **Add**, and configure the following parameters:



Under **Edit SIP Peer Configuration**, configure the following parameters:

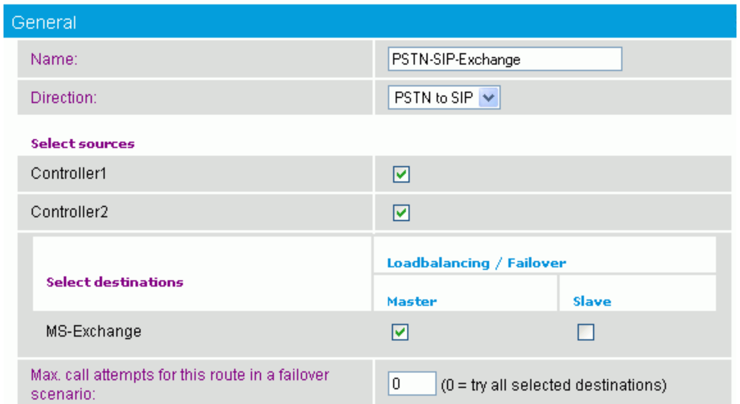
- **Name**: Enter a name for the SIP peer configuration.
- **Peer type**: Select **MS Exchange 2007** as peer type.
- **Host**: Enter the IP address or host name of your Unified Messaging server.

Under **Enhanced Configuration**, enable the **Default SIP to PSTN peer** check box.

Click **OK** to save the settings and to close the window.

9. Configure one routing for the PSTN to SIP and one for SIP to the PSTN. To do so, click **Routing Configuration** and then click **Add** to open the **Edit Routing Configuration** window.

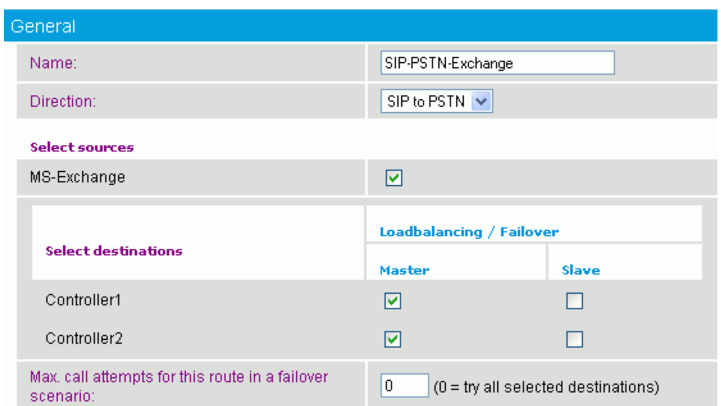
- For the PSTN to SIP route, configure the following parameters:



  - **Name**: Enter a unique name to easily identify the routing.
  - **Direction**: Select **PSTN to SIP** from the dropdown menu.
  - **Select sources**: Select both controllers as source.
  - **Select destinations**: Select the SIP peer as **Master** destination.

  Click **OK** to save the settings and to close the window.

- For the SIP to the PSTN route, click **Add** again and configure the following parameters:



  - **Name**: Enter a unique name to easily identify the routing.
  - **Direction**: Select **PSTN to SIP** from the dropdown menu.
  - **Select sources**: Select both controllers as source.
  - **Select destinations**: Select the SIP peer as **Master** destination.

  Click **OK** to save the settings and to close the window.

10. Click **Save** in the main configuration page to save the settings and activate the changes.

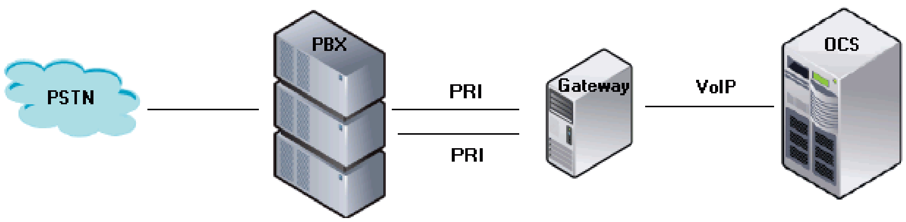
Use cases for Microsoft® Office Communications Server (OCS) 2007

The following scenarios describe common configurations for the gateway computer with one Dialogic® Diva® V-2PRI Media Board and the Dialogic® Diva® SIPcontrol Software installed. The scenarios assume that the gateway computer is based in Germany.

1. Using the gateway computer between the PBX and Microsoft® Office Communications Server 2007: Both lines of the Diva Media Board are connected between the PBX and the Microsoft® Office Communications Server (OCS) 2007.
2. Using the gateway computer between PBX/PSTN and the Microsoft® Office Communications Server 2007: One line of the Diva Media Board is connected to the PBX and one line is connected directly to the PSTN. The gateway computer is connected to the Microsoft® Office Communications Server (OCS) 2007.
3. Using the gateway computer between the PSTN and PBX/Microsoft® Office Communications Server 2007: One line of the Diva Media Board is connected to the PBX and one line is connected to the PSTN. The gateway computer is connected between the PSTN and the PBX. The Microsoft® Mediation Server is installed on the gateway computer.

Using the gateway computer between the PBX and Microsoft® Office Communications Server 2007

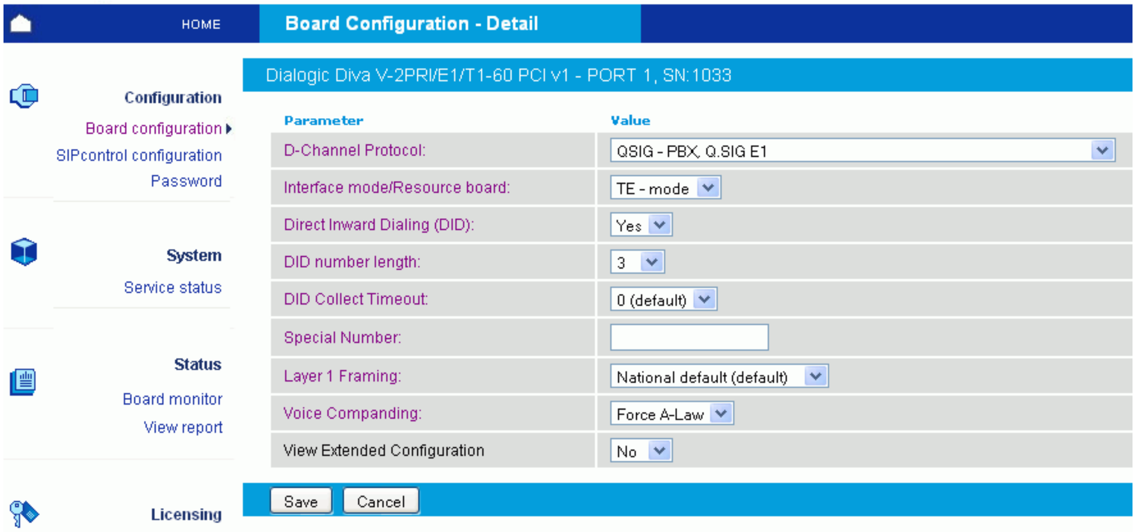
This configuration scenario describes the necessary steps to configure the gateway computer between the PBX and the Microsoft® Office Communications Server (OCS) 2007 as shown in the graphic.



1. Open the Dialogic® Diva® SIPcontrol™ Software web interface to configure the required parameters. To do so, click **Start** > **Programs** > **Dialogic Diva** > **SIPcontrol Configuration**.
2. In the Diva SIPcontrol software web interface, click **Board configuration** on the left hand side to open the **Available Diva Boards** page.

Click either the board icon or the name of the Dialogic® Diva® Media Board to open the **Board Configuration - Detail** page.

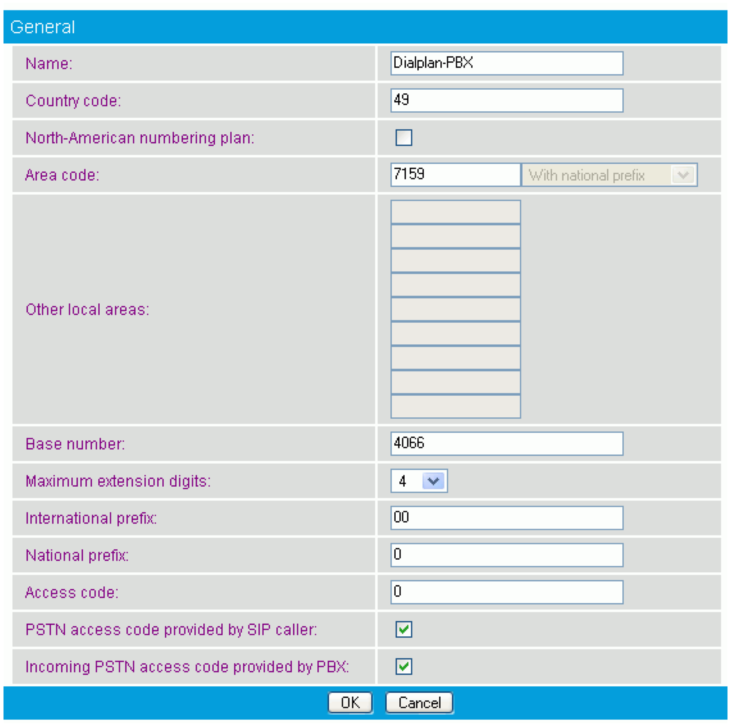
3. Configure the **D-Channel Protocol** of the PBX. In the example, **QSIG-PBX, Q.SIG E1** is selected. Click **Save**.



4. Repeat step 2 and 3 for the other PRI line.

5. In the Diva SIPcontrol web interface, click **SIPcontrol configuration** on the left hand side to open the **SIPcontrol Configuration** page. For this configuration scenario, a dialplan, the PSTN interface, the network interface, a SIP peer, and a routing need to be configured.

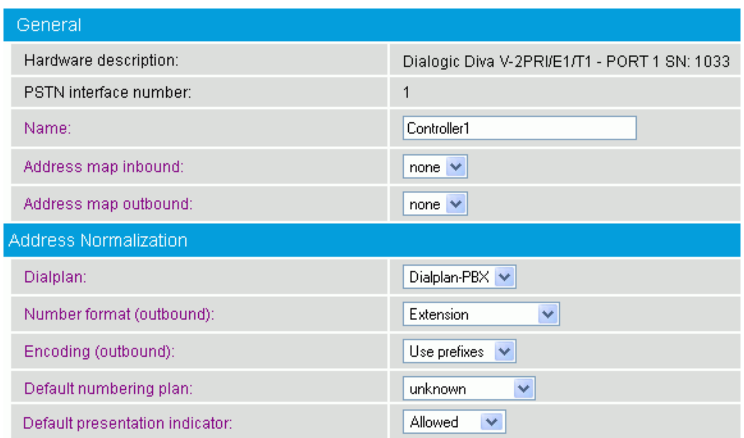
6. Open the **Dialplan Configuration**, click **Add**, and enter the following parameters:



- **Name**: Enter a unique name to easily identify the dialplan.
- **Country code**: Enter the country code of the country in which the gateway computer is located.
- **Area code**: Enter the area code of the region in which the gateway computer is located.
- **Base number**: Enter the subscriber or trunk number.
- **Maximum extension digits**: Select the maximum number of extension digits that are provided.
- **International prefix**: Enter the international prefix of the country in which the gateway computer is located.
- **National prefix**: Enter the national prefix that needs to be dialed for long distance calls within the country in which the gateway computer is located.
- **Access code**: Enter the digit that is necessary to access the public network.
- Enable the options **PSTN access code provided by SIP caller** and **Incoming PSTN access code provided by PBX**.

Click **OK** to save the settings and to close the window.

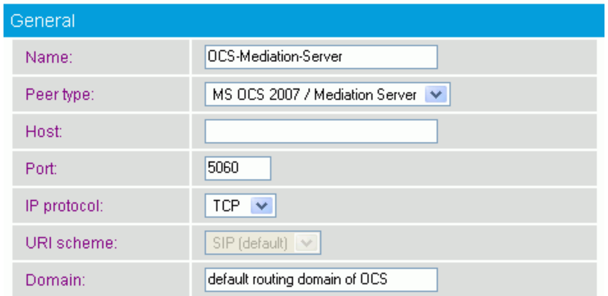
7. Under **PSTN Interface Configuration**, configure both lines of the Dialogic® Diva® Media Board with the same settings. To do so, click **Details** at the right and select the **Dialplan** you configured above and set **Number format (outbound)** to **Extension** and **Encoding (outbound)** to **Use prefixes**. Leave the remaining parameters at their default values.



Click **OK** to save the settings and to close the window.

8. Configure the second line with the same settings.
9. Under **Network Interface Configuration**, enable your Ethernet adapter, and set the **SIP Listen Port** to **9803**.

10. Open the **SIP Peer Configuration**, click **Add**, and configure the following parameters:

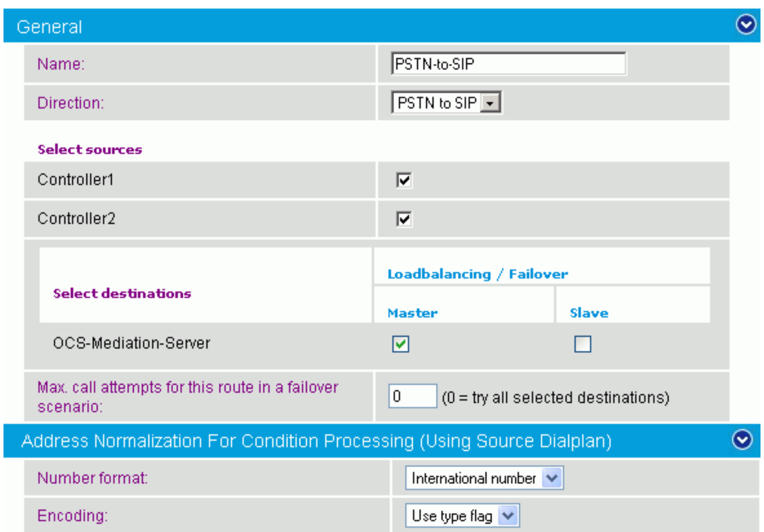


Under **Edit SIP Peer Configuration**, configure the following parameters:

- **Name**: Enter a unique name to easily identify the SIP peer.
- **Peer type**: Select **MS OCS 2007/ Mediation Server** from the dropdown menu.
- **Host**: Enter the IP address or host name of the host PC.
- **Domain**: For the correct domain entry, see the configuration of your Microsoft® Office Communications Server.

Click **OK** to save the settings and to close the window.

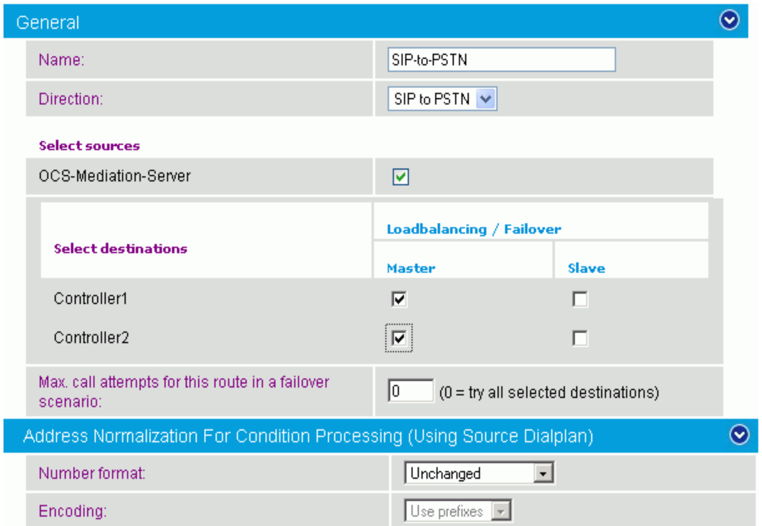
11. Create two routings, one for each direction (PSTN to SIP and SIP to PSTN). To configure the routing from PSTN to SIP, open the **Routing Configuration**, click **Add**, and configure the following parameters:



- **Name**: Enter a unique name to easily identify the routing.
- **Direction**: Select **PSTN to SIP** from the dropdown menu.
- **Select sources**: Select both controllers of the Diva Media Board.
- **Select destinations**: Select the above configured SIP peer as master destination.
- **Number format**: Select **International number** from the dropdown menu.
- **Encoding**: Select **Use type flag** from the dropdown menu.

Click **OK** to save the settings and to close the window.

12. For the routing from SIP to PSTN, click **Add** again, and configure the following parameters:



- **Name**: Enter a unique name to easily identify the routing.
- **Direction**: Select **SIP to PSTN** from the dropdown menu.
- **Select sources**: Select the above configured SIP peer as source.
- **Select destinations**: Select both controllers of the Diva Media Board.

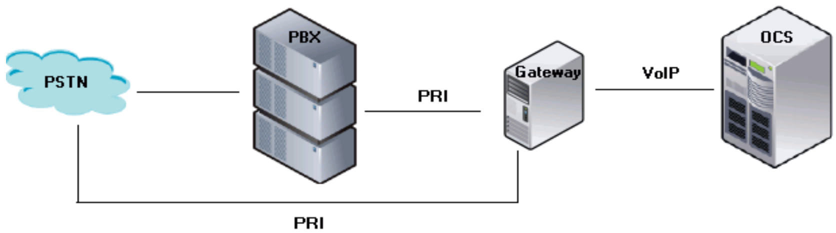
Click **OK** to save the settings and to close the window.

13. Click **Save** in the main configuration page to save the settings and to activate the changes.

14. Configure Microsoft® Office Communications Server 2007.

Using the gateway computer between PBX/PSTN and the Microsoft® Office Communications Server 2007

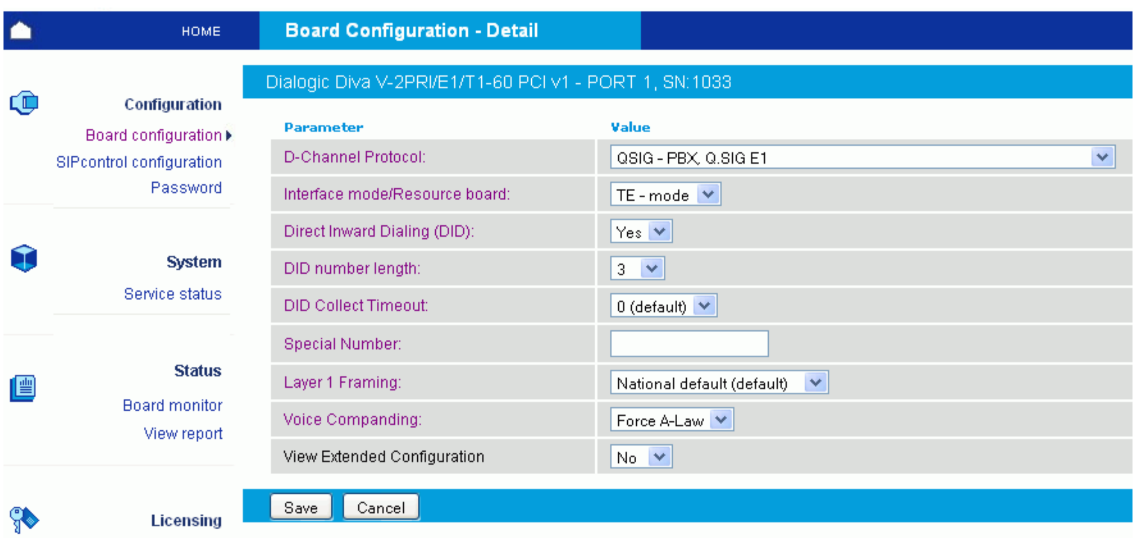
This configuration scenario describes the necessary steps if one line of the gateway computer is connected to the PBX and one line is connected directly to the PSTN as shown in the graphic.



1. Open the Dialogic® Diva® SIPcontrol™ Software web interface to configure the required parameters. To do so, click **Start** > **Programs** > **Dialogic Diva** > **SIPcontrol Configuration**.
2. In the Diva SIPcontrol software web interface, click **SIPcontrol** on the left hand side to open the **Board Configuration** page.

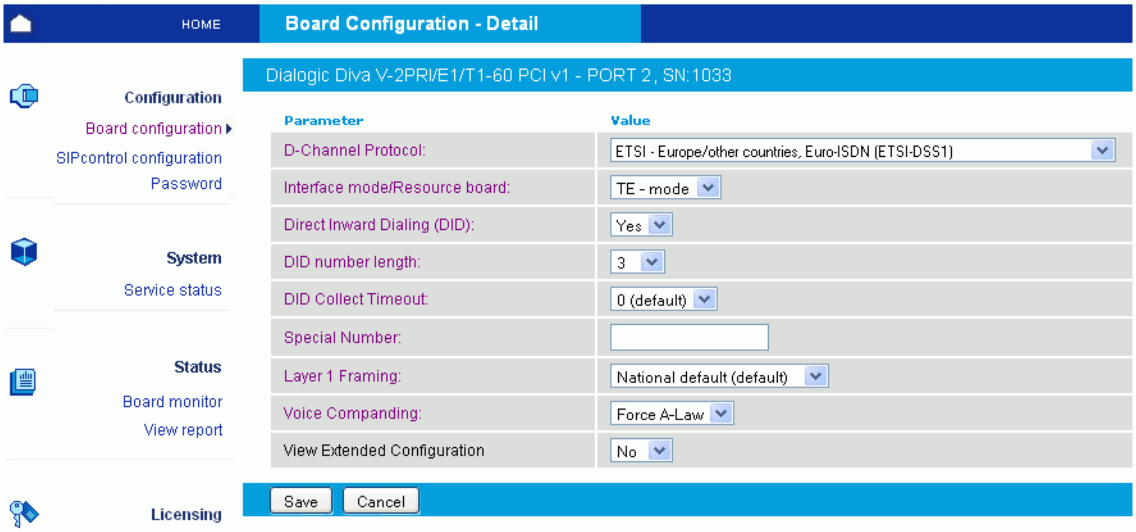
Click either the board icon or the name of the first Dialogic® Diva® Media Board line to open the **Board Configuration - Detail** page.

3. Configure the **D-Channel Protocol** of port 1. In the example, **QSIG-PBX, Q.SIG E1** is selected. Click **Save**.



4. Click **Board configuration** again and select port 2 of your Diva Media Board to open the **Board Configuration - Detail** page again.

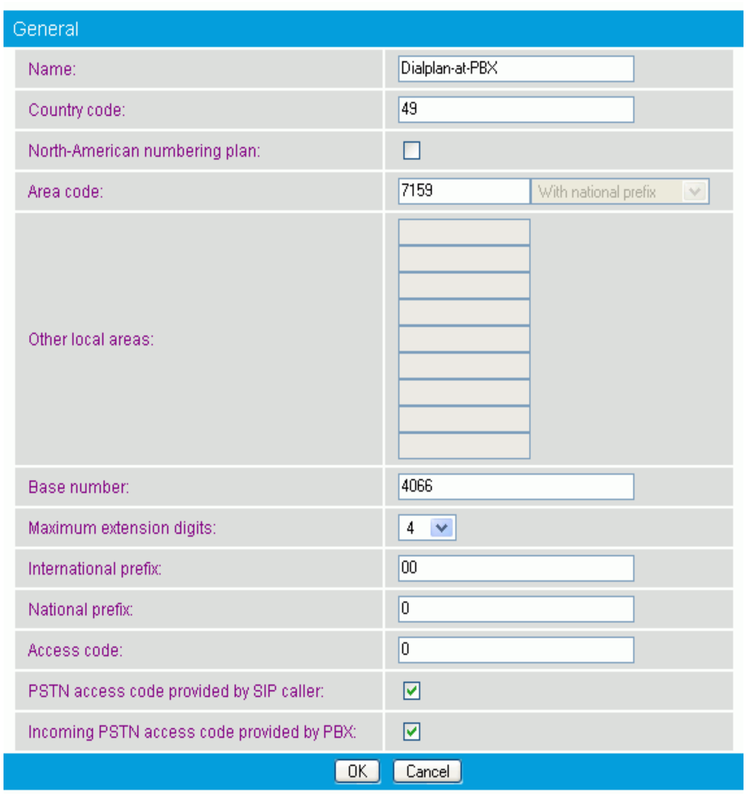
5. Configure the **D-Channel Protocol** of the PRI line connected to the PSTN. In the example, **ETSI-Europe/other countries, Euro-ISDN (ETSI-DSS1)** is selected. Click **Save**.



6. In the Diva SIPcontrol web interface, click **SIPcontrol configuration** on the left hand side to open the **SIPcontrol Configuration** page.

   For this configuration scenario, two dialplans, the two PSTN interfaces, the network interface, a SIP peer, an address map, and three routings need to be configured.

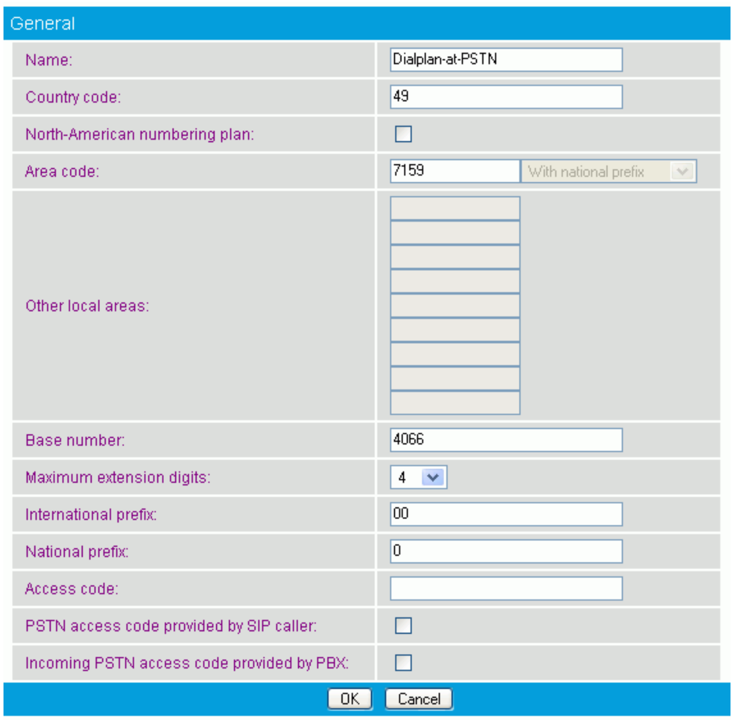
7. Configure two dialplans; one for the line connected to the PBX and one for the line connected directly to the PSTN. To do so, open the **Dialplan Configuration**, click **Add**, and configure the following parameters for the PBX dialplan:



- **Name**: Enter a unique name to easily identify the dialplan.
- **Country code**: Enter the country code of the country in which the gateway computer is located.
- **Area code**: Enter the area code of the region in which the gateway computer is located.
- **Base number**: Enter the subscriber or trunk number.
- **Maximum extension digits**: Select the maximum number of extension digits that are provided.
- **International prefix**: Enter the international prefix of the country in which the gateway computer is located.
- **National prefix**: Enter the national prefix that needs to be dialed for long distance calls within the country in which the gateway computer is located.
- **Access code**: Enter the digit that is necessary to access the public network.
- Enable the options **PSTN access code provided by SIP caller** and **Incoming PSTN access code provided by PBX**.

Click **OK** to save the settings and to close the window.

8. To configure the PSTN dialplan, click **Add** again, and configure the following parameters.

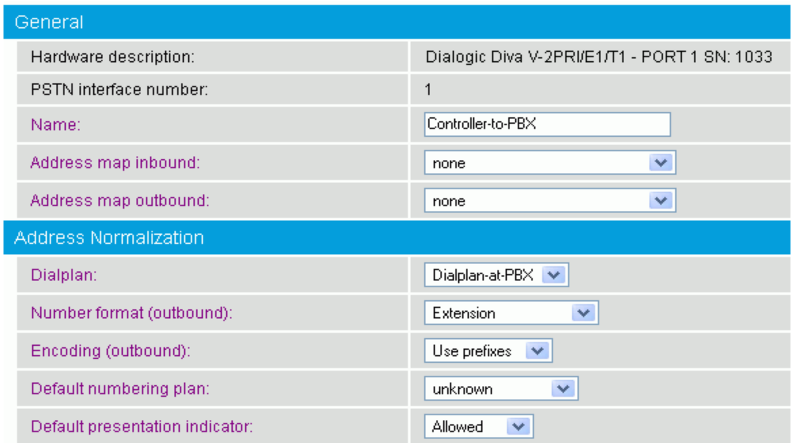


- **Name**: Enter a unique name to easily identify the dialplan.
- **Country code**: Enter the country code of the country in which the gateway computer is located.
- **Area code**: Enter the area code of the region in which the gateway computer is located.
- **Base number**: Enter the subscriber or trunk number.
- **Maximum extension digits**: Select the maximum number of extension digits that are provided.
- **International prefix**: Enter the international prefix of the country in which the gateway computer is located.
- **National prefix**: Enter the national prefix that needs to be dialed for long distance calls within the country in which the gateway computer is located.

Click **OK** to save the settings and to close the window.

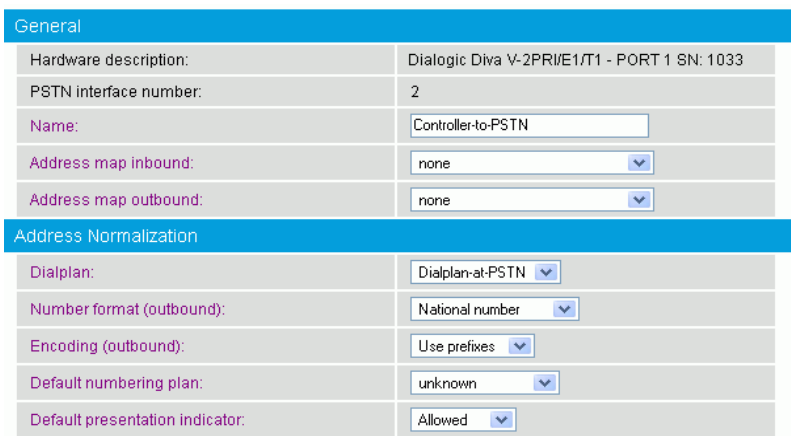
9. Under **PSTN Interface Configuration**, configure controller 1 with the PBX-specific settings and controller 2 with the PSTN-specific settings. The controller number that you configure with the PBX-specific settings needs to correspond to the line number in the Diva Configuration Manager that you configured with the switch type of your PBX. The same is true for the controller with the switch type of the PSTN line.

   - To configure the PBX-specific parameters, click **Details** at the right of the controller connected to the PBX. Select the **Dialplan** you configured for the PBX, set **Number format (outbound)** to **Extension**, and **Encoding (outbound)** to **Use prefixes**.



   Click **OK** to save the settings and to close the window.

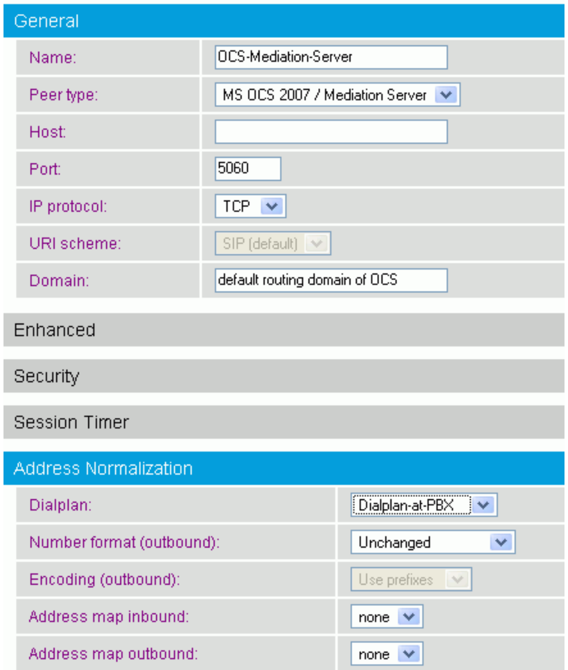
   - To configure the PSTN-specific parameters, click **Details** at the right of the controller connected to the PSTN line. Select the **Dialplan** you configured for the PSTN, set **Number format (outbound)** to **National Number**, and **Encoding (outbound)** to **Use prefixes**.



   Click **OK** to save the settings and to close the window.

10. Under **Network Interface Configuration**, enable your Ethernet adapter, and set the **SIP Listen Port** to **9803**.

11. Open the **SIP Peer Configuration**, click **Add**, and configure the following parameters:



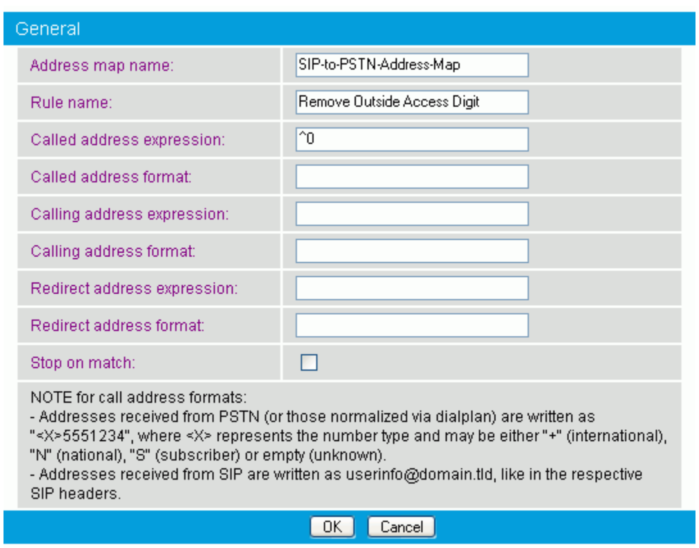
Under **Edit SIP Peer Configuration**, configure the following parameters:

- **Name**: Enter a unique name to easily identify the SIP peer.
- **Peer type**: Select **MS OCS 2007/ Mediation Server** from the dropdown menu.
- **Host**: Enter the IP address or host name of the host PC.
- **Domain**: For the correct domain entry, see the configuration of your Microsoft® Office Communications Server 2007.

Under **Address Normalization Configuration**, select the dialplan you configured for the controller connected to the PBX.

Click **OK** to save the settings and to close the window.

12. Create an address map for the SIP to PSTN direction to remove the outside access digit. To do so, open the **Address Map Configuration**, click **Add**, and configure the following parameters:



- **Address map name**: Enter a descriptive name of the address map.
- **Rule name**: Enter a name that explains the address map rule.
- **Called address expression**: Enter the expression as displayed in the graphic above to remove the outside access digit.

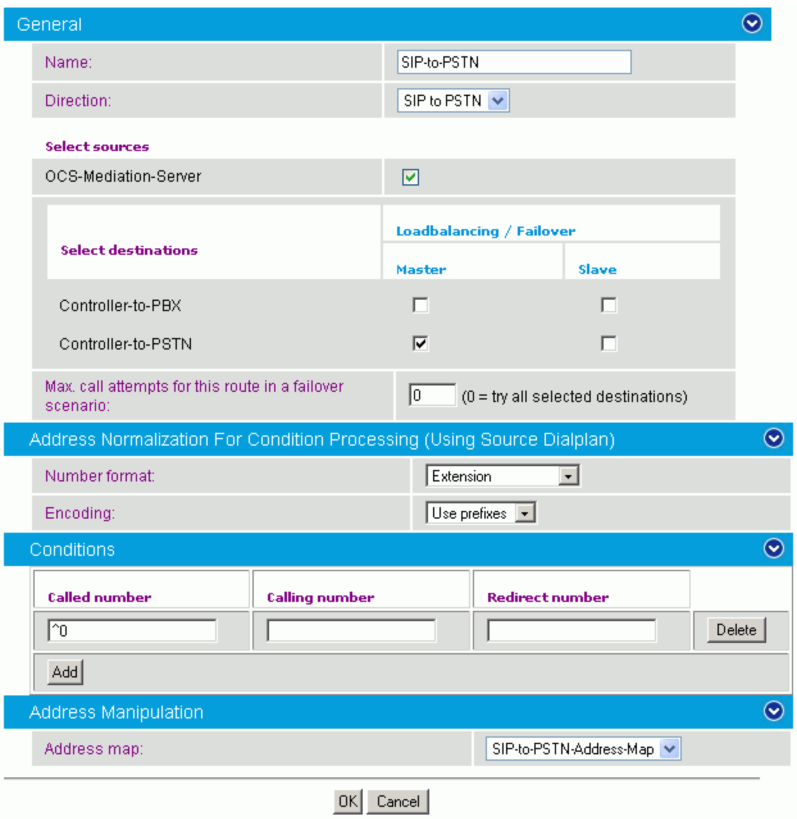
Click **OK** to save the settings and to close the window.

13. Create three routings:

- one from the Microsoft® Office Communications Server (OCS) 2007 directly to the PSTN,
- one from the Microsoft® OCS 2007 via the PBX to the PSTN, and
- one from the PSTN/PBX via the gateway computer to Microsoft® OCS 2007.

In this scenario, the order of the routings is important because only one routing will be configured with a condition. In this example, the routings are configured in the correct order but it is also explained how to change the order in case you configured them differently.

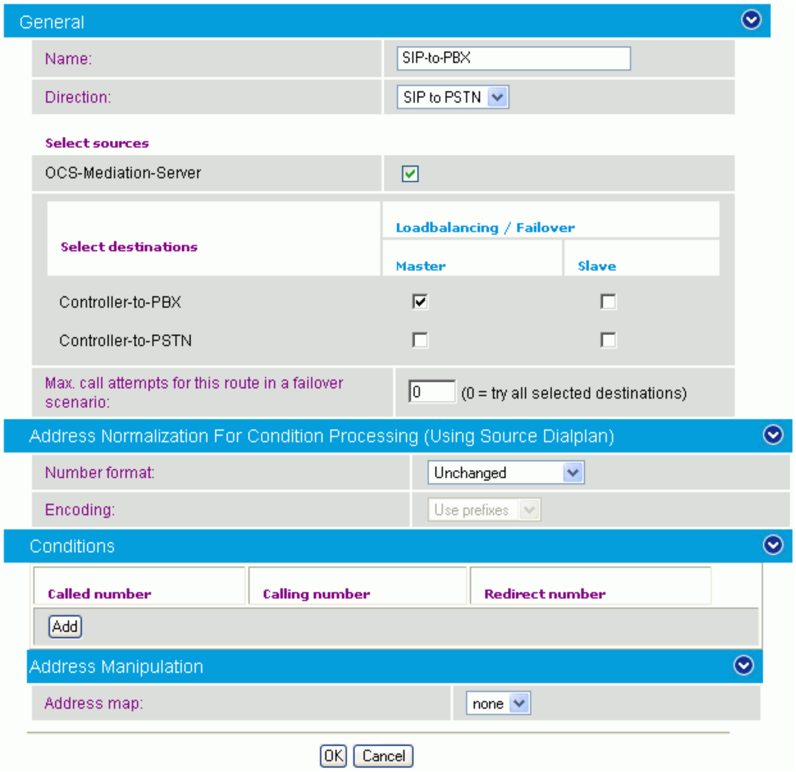
14. Create the route from Microsoft® OCS 2007 to the PSTN first. To do so, open the **Routing Configuration**, click **Add** and configure the following parameters:



- **Name**: Enter a unique name to easily identify the routing.
- **Direction**: Select **SIP to PSTN** from the dropdown menu.
- **Select sources**: Select the above configured SIP peer as master destination.
- **Select destinations**: Select the controller you configured for the PSTN.
- **Number format**: Select **Extension** from the dropdown menu.
- **Encoding**: Select **Use prefixes** from the dropdown menu.
- Under **Conditions**, click **Add**, and in **Called number** enter **^0** to omit the outside access digit.

Click **OK** to save the settings and to close the window.

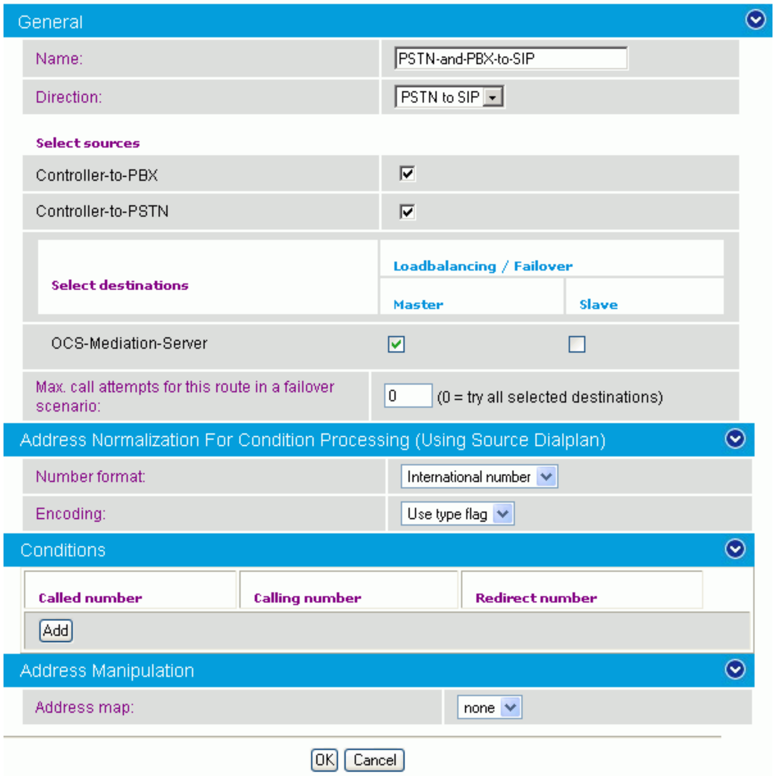
15. Click **Add** again, and configure the route from Microsoft® OCS 2007 to the PBX.



- **Name**: Enter a unique name to easily identify the routing.
- **Direction**: Select **SIP to PSTN** from the dropdown menu.
- **Select sources**: Select the above configured SIP peer as master destination.
- **Select destinations**: Select the controller you configured for the PBX.

Click **OK** to save the settings and to close the window.

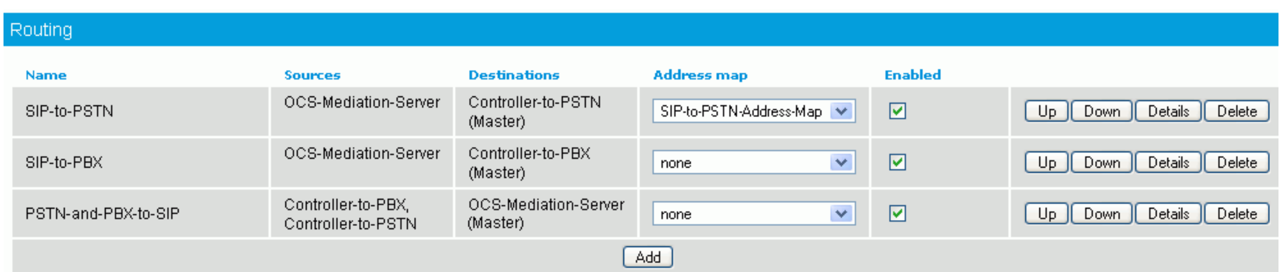
16. Click **Add** again to configure the third route. Configure the following parameters:



- **Name**: Enter a unique name to easily identify the routing.
- **Direction**: Select **PSTN to SIP** from the dropdown menu.
- **Select sources**: Select both controllers of the Diva Media Board.
- **Select destinations**: Select the above configured SIP peer as master destination.
- **Number format**: Select **International number** from the dropdown menu.
- **Encoding**: Select **Use type flag** from the dropdown menu.

Click **OK** to save the settings and to close the window.

17. To change the order of the routings in the main configuration page, click the arrow up or arrow down buttons. The order needs to be the same as shown in this graphic:



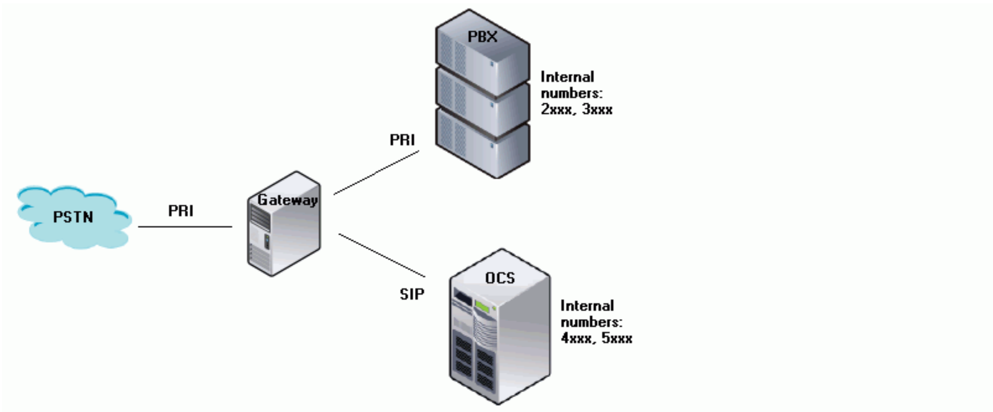
18. Click **Save** in the main configuration page to save the settings and to activate the changes.

19. Configure Microsoft® Office Communications Server 2007.

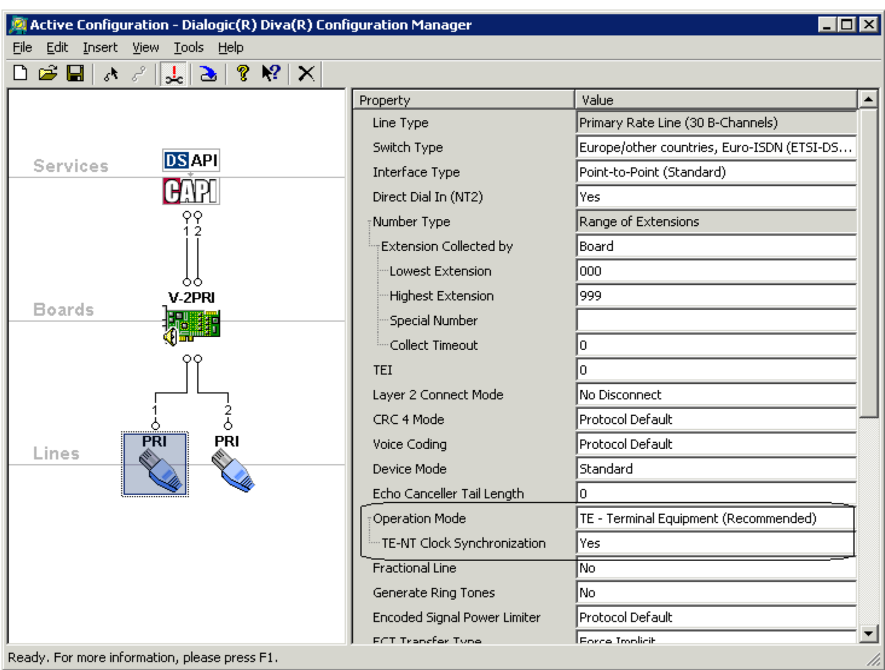
Using the gateway computer between the PSTN and PBX/Microsoft® Office Communications Server 2007

This configuration scenario describes the necessary steps if the gateway computer is connected between the PSTN and PBX/Microsoft® Office Communications Server (OCS) 2007. This way, the Diva SIPcontrol software can also route calls from the PBX to the PSTN, and vice versa. One PRI line is connected to the PBX and one PRI line is connected directly to the PSTN. This scenario also assumes that the PBX was previously connected to the PSTN directly and the PBX has not been reconfigured at all to cope with any changes introduced by the gateway or Microsoft® OCS 2007.

The Microsoft® Mediation Server is installed on the gateway computer. The PBX is configured for the extensions starting with 2 or 3 and the Microsoft® OCS 2007 is configured for the extensions starting with 4 or 5. The Diva SIPcontrol software expects a PSTN access code in calls from Microsoft® OCS 2007 or from the PBX to the PSTN; in our case it is an additional 0 (zero). The Diva SIPcontrol software is configured to remove the access code before forwarding the call to the PSTN. For convenience, the Diva SIPcontrol software is also configured to add the outside access code to the calling number in calls coming from the PSTN. Since the PBX is not aware of the presence of the gateway and Microsoft® OCS 2007, it does not send and expect any outside access code. Therefore, the Diva SIPcontrol software also removes the outside access code in calls to the PBX and adds it in calls from PBX.



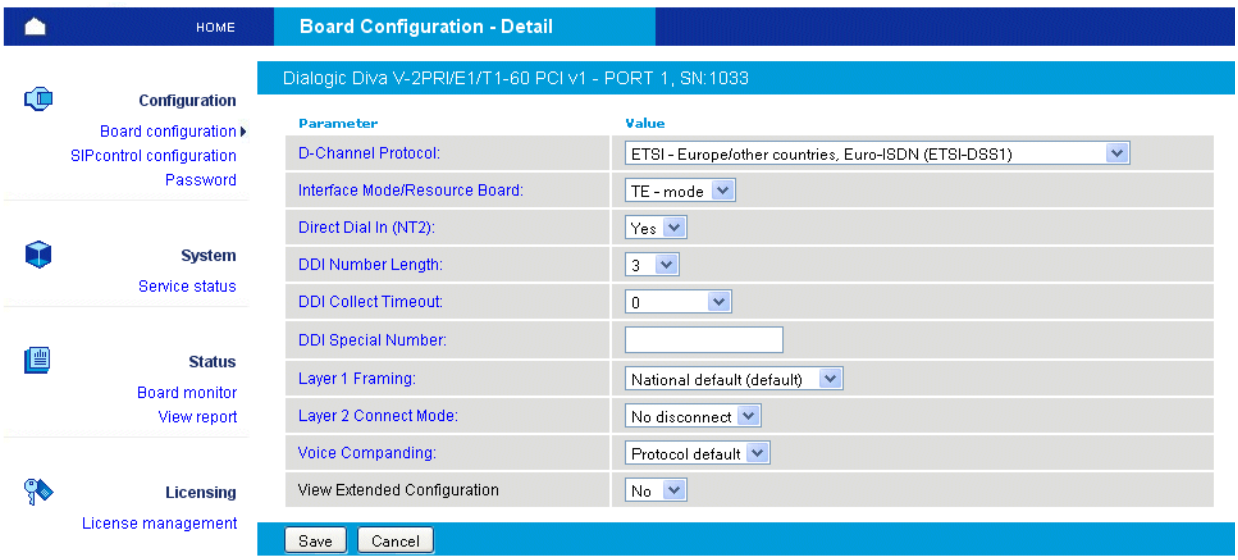
1. Open the Dialogic® Diva® Configuration Manager. To do so, click **Start** > **Programs** > **Dialogic Diva** > **Configuration Manager**.
2. Click the line icon for port one and under **Operation Mode** set **TE-NT Clock Synchronization** to **Yes**.



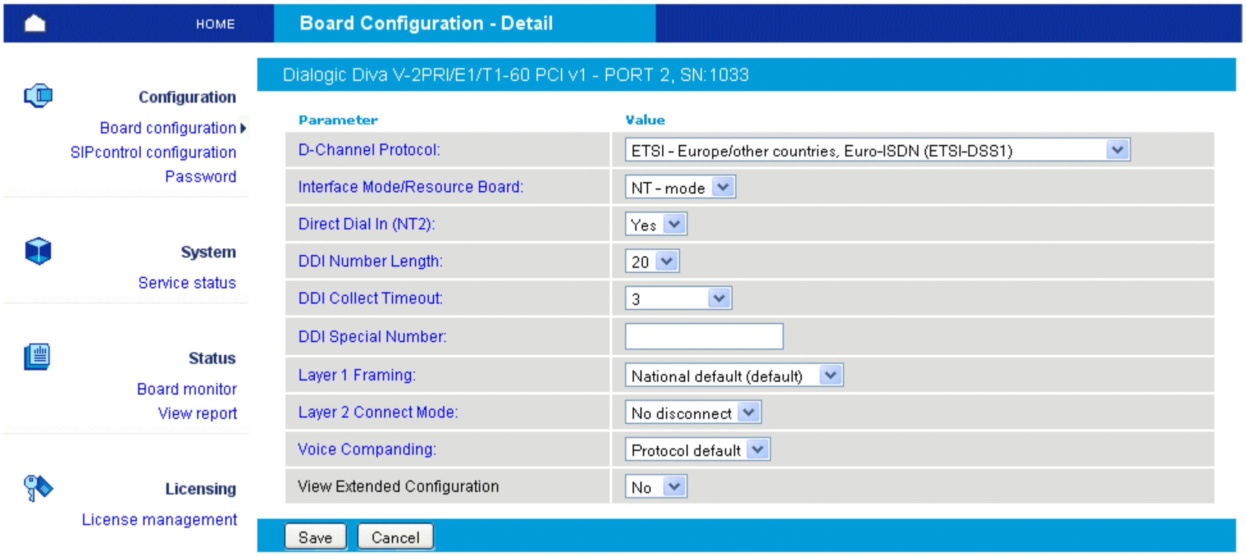
3. Open the Dialogic® Diva® SIPcontrol™ software web interface to configure the required parameters. To do so, click **Start** > **Programs** > **Dialogic Diva** > **SIPcontrol Configuration**.
4. In the Diva SIPcontrol software web interface, click **Board configuration** on the left hand side to open the **Available Diva Boards** page.

Click either the board icon or the name of the first Dialogic® Diva® Media Board line to open the **Board Configuration - Detail** page.

5. Configure the **D-Channel Protocol** of the PRI line connected to the PSTN. In the example, **ETSI-Europe/other countries, Euro-ISDN (ETSI-DSS1)** is selected and the **DDI Number Length** is set to **3**. Click **Save**.



6. Click **Board configuration** again and select port 2 of your Diva Media Board to open the **Board Configuration - Detail** page for this board and configure the following parameters:

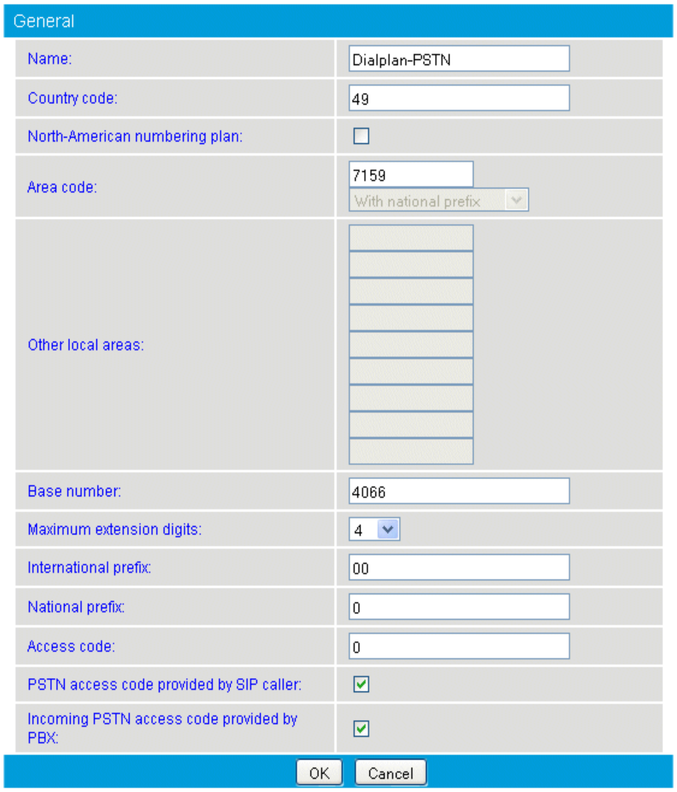


- **D-Channel Protocol**: Select **ETSI-Europe/other countries, Euro-ISDN (ETSI-DSS1)** as D-channel protocol.
- **Interface mode/Resource board**: Set the value of this parameter to **NT-mode**.
- **DDI Number Length**: Set the value to **20** to cover the possible length of the called number in an outgoing call.
- **DDI Collect Timeout**: Select a timeout in seconds after which the Diva Board stops collecting the digits of the calling number and passes the number to the application. In the example, the timeout value is **3** seconds.
- Click **Save** to close the window.

7. In the Diva SIPcontrol web interface, click **SIPcontrol configuration** on the left hand side to open the **SIPcontrol Configuration** page.

   For this configuration scenario, one dialplan, five address maps, the two PSTN interfaces, the network interface, two SIP peers, and five routings need to be configured.

8. Open the **Dialplan Configuration**, click **Add**, and configure the following parameters for the dialplan:

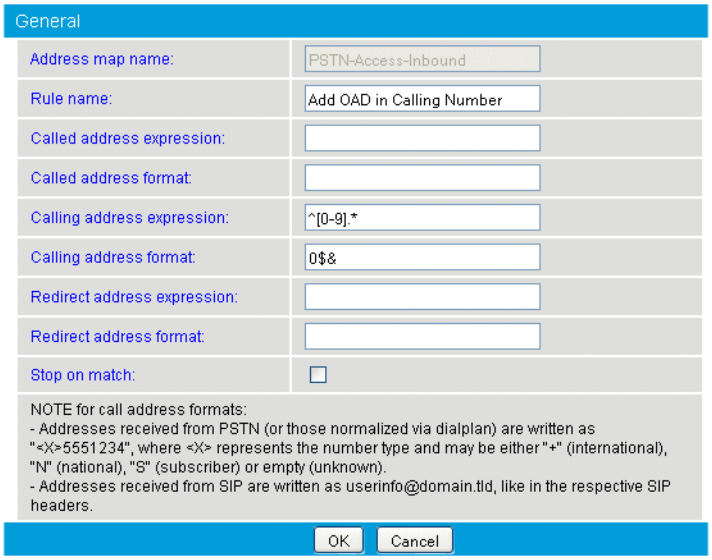


- **Name**: Enter a unique name to easily identify the dialplan.
- **Country code**: Enter the country code of the country in which the gateway computer is located.
- **Area code**: Enter the area code of the region in which the gateway computer is located.
- **Base number**: Enter the subscriber or trunk number.
- **Maximum extension digits**: Select the maximum number of extension digits that are provided.
- **International prefix**: Enter the international prefix of the country in which the gateway computer is located.
- **National prefix**: Enter the national prefix that needs to be dialed for long distance calls within the country in which the gateway computer is located.
- **Access code**: Enter the digit that is necessary to get access to the public network.
- Enable the options **PSTN access code provided by SIP caller** and **Incoming PSTN access code provided by PBX**.

Click **OK** to save the settings and to close the window.

9. Create five address maps, two for incoming calls, two for outgoing calls, and one for the special number, normally the number of the receptionist. The first four address maps are necessary to either add or omit the OAD (Outside Access Digit).

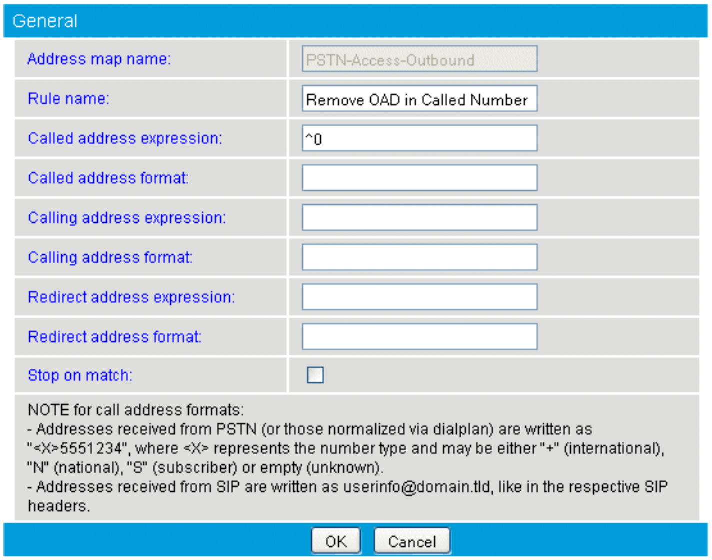
- To create the address map for incoming calls, open the **Address Map Configuration**, click **Add**, and configure the following parameters:



  - **Address map name**: Enter a name for the incoming call address map.
  - **Rule name**: Enter a name that describes the address map rule. This name will be displayed on the main configuration page.
  - **Calling address expression**: Enter the calling address expression as shown in the graphic above. With this expression, the OAD will be added to incoming calls.
  - **Calling address format**: As calling format enter the 0 (zero) so that it is added in the output followed by the $&, which means that the whole expression is matched.

Click **OK** to save the settings and to close the window.

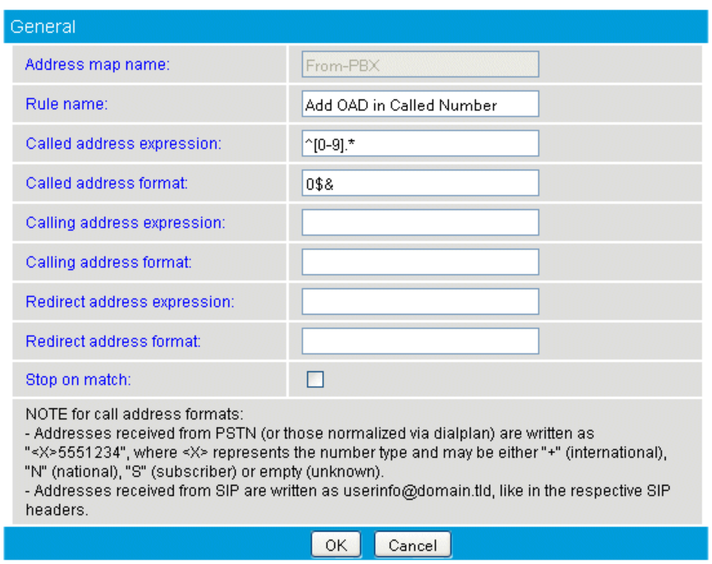
- To create the second address map, click **Add** again, and configure the following parameters:



  - **Address map name**: Enter a name for the outgoing call address map.
  - **Rule name**: Enter a name that describes the address map rule. This name will be displayed on the main configuration page.
  - **Called address expression**: Enter the called address expression as shown in the graphic above. With this expression, the OAD will be removed from outgoing calls.

Click **OK** to save the settings and to close the window.

- The third address map is only necessary if the PBX is configured as if it was still connected to the PSTN. To create the this address map, click **Add** again, and configure the following parameters:

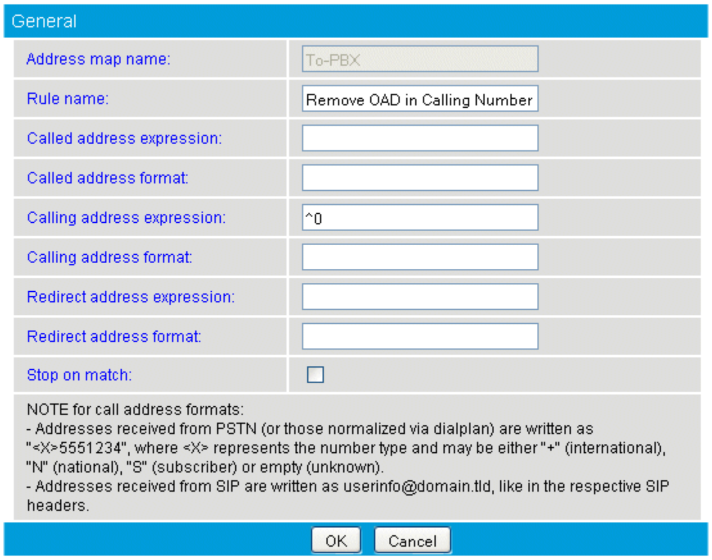


  - **Address map name**: Enter a name for the address map for calls from the PBX.
  - **Rule name**: Enter a name that describes the address map rule. This name will be displayed on the main configuration page.
  - **Called address expression**: Enter the called address expression as shown in the graphic above. With this expression, the OAD will be added to calls from the PBX.

- **Called address format**: Enter the called address format as shown in the graphic above.

Click **OK** to save the settings and to close the window.

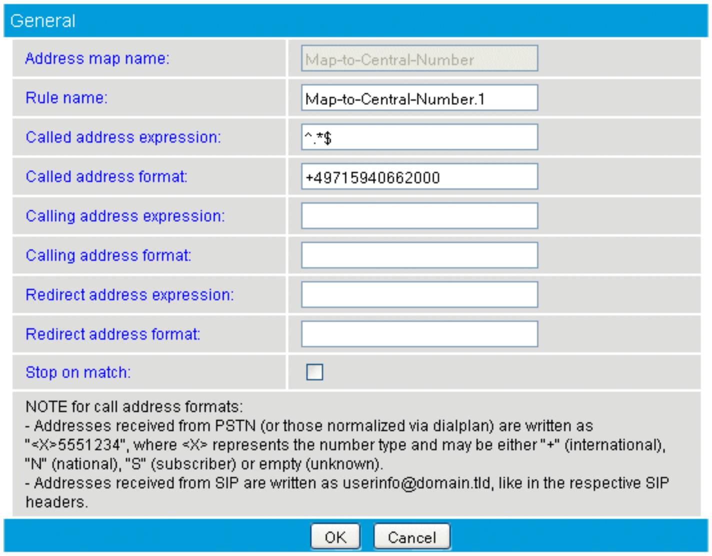
- The fourth address map is also only necessary if the PBX is configured as if it was still connected to the PSTN. To create this address map, click **Add** again, and configure the following parameters:



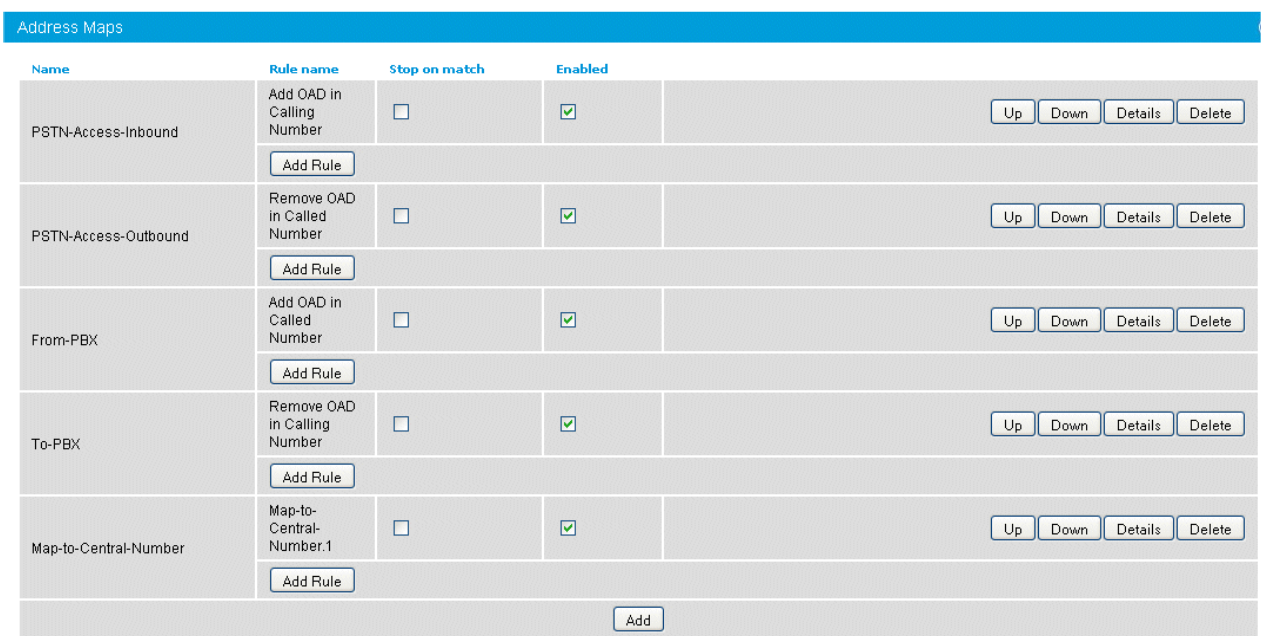
- **Address map name**: Enter an address map name for calls from the gateway to the PBX.
- **Rule name**: Enter a name that describes the address map rule. This name will be displayed on the main configuration page.
- **Calling address expression**: Enter the calling address expression as shown in the graphic above. With this expression, the OAD will be removed from calls to the PBX.

Click **OK** to save the settings and to close the window.

- The fifth address map is necessary to map the number of unassigned internal numbers to the number of the reception. In our case, the reception has the extension 2000. The address map is later used in a route for unassigned internal numbers. All numbers using this route will end up at the reception. To create the this address map, click **Add** again, and configure the following parameters:

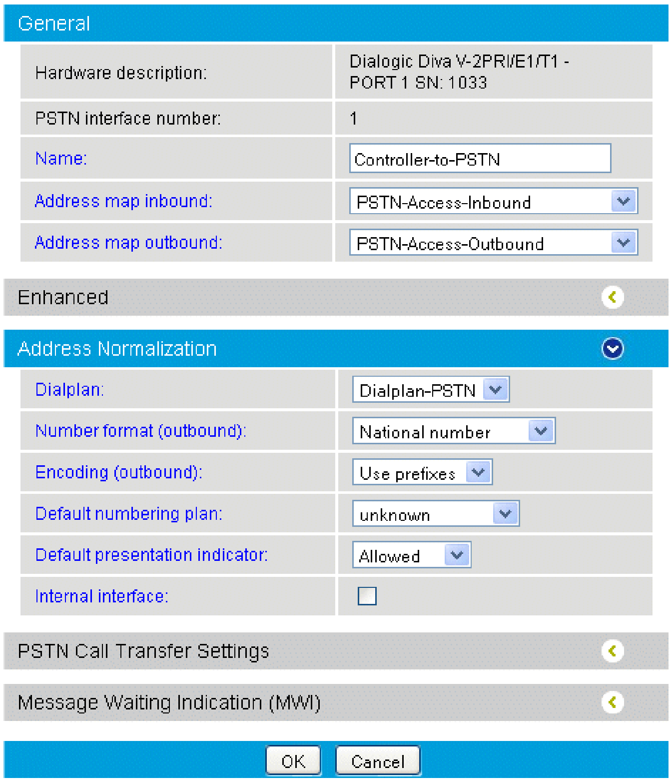


  - **Address map name**: Enter an address map name for calls to the reception.
  - **Rule name**: Enter a name that describes the address map rule. This name will be displayed on the main configuration page.
  - **Called address expression**: Enter the called address expression as shown in the graphic above.
  - **Called address format**: Enter the number of the receptionist including country code, area code, base number, and extension, as shown in the graphic above.
- To change the order of the mappings in the main configuration page, click the **Up** or **Down** buttons. The order needs to be the same, as shown in following graphic:



10. Under **PSTN Interface Configuration**, configure controller 1 with PSTN-specific settings and controller 2 with PBX-specific settings. The controller number you configure with PSTN-specific settings needs to correspond to the line number in the Diva Configuration Manager that you configured with the switch type of your PSTN line. The same is true for the controller with the switch type of the PBX.

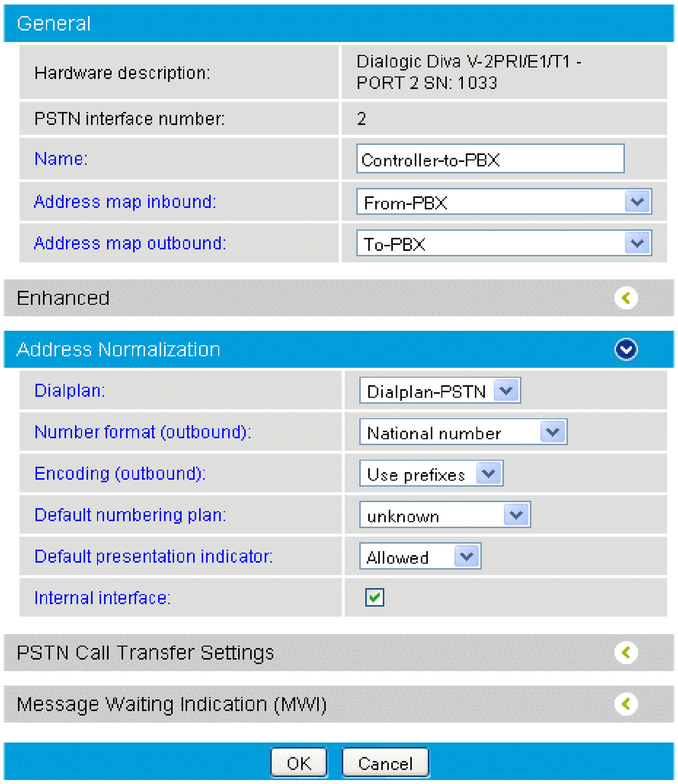
- To configure PSTN-specific parameters, click **Details** at the right of the controller connected to the PSTN line and configure the following parameters:



  - Enter a unique name for this controller, e.g., "Controller-to-PSTN".
  - Select the inbound and outbound address map that you configured for access from the PSTN.
  - Select the **Dialplan** you configured for the PSTN.
  - Set **Number format (outbound)** to **National Number**,
  - Set **Encoding (outbound)** to **Use prefixes**.

Click **OK** to save the settings and to close the window.

- To configure the controller that is connected to the PBX later in the configuration, click **Details** at the right of the respective controller.



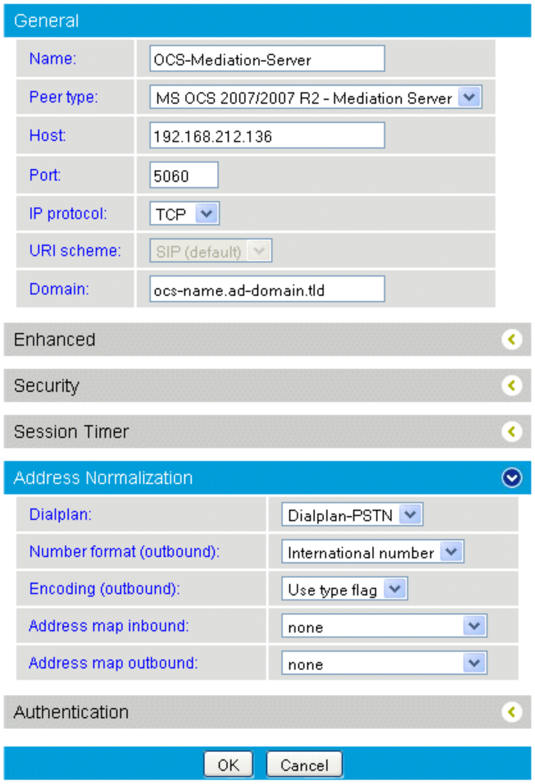
  - Enter a unique name for this controller, e.g., "Controller-to-PBX".
  - Select the inbound and outbound address map that you configured for access from the PBX.
  - Select the **Dialplan** you configured for the PSTN,
  - set **Number format (outbound)** to **National Number**,
  - and **Encoding (outbound)** to **Use prefixes**.
  - Also, activate the **Internal Interface** option, because this interface is not directly connected to the PSTN and operated in NT-mode.
  - Leave the remaining parameters at their default values.

Click **OK** to save the settings and to close the window.

11. Under **Network Interface Configuration**, enable your Ethernet adapter, and set the **SIP Listen Port** to **9803**.

12. Create two SIP peers, one for the PSTN to the Microsoft® Mediation Server installed on the gateway computer and one for the PSTN to PBX connection.

- To configure the first SIP peer, open the **SIP Peer Configuration**, click **Add**, and enter the following parameters:



Under **General**, configure the following parameters:

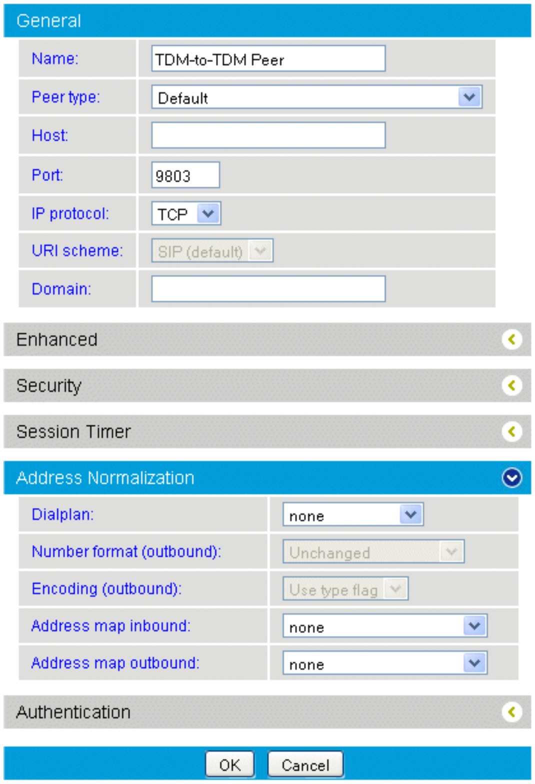
- **Name**: Enter a unique name to easily identify the SIP peer.
- **Peer type**: Select **MS OCS 2007/ 2007 R2 - Mediation Server** from the dropdown menu.
- **Host**: Enter the IP address or host name of the host PC.
- **Domain**: For the correct domain entry, see the configuration of your Microsoft® Office Communications Server 2007.

Under **Address Normalization Configuration**, configure the following parameters:

- **Dialplan**: Select the dialplan you configured for the controller connected to the PBX.
- **Number format (outbound)**: Select **International number** form the dropdown menu.
- **Encoding (outbound)**: Select **Use type flag** from the dropdown menu.

Click **OK** to save the settings and to close the window.

- To create the second SIP peer, click **Add** again, and configure the following parameters:



Under **General**, configure the following settings:

- **Name**: Enter a unique name to easily identify the SIP peer.
- **Peer type**: Select **Default** from the dropdown menu.
- **Host**: Enter the IP address or host name of the host PC.
- **Domain**: Enter the IP address of the host PC.

Click **OK** to save the settings and to close the window.

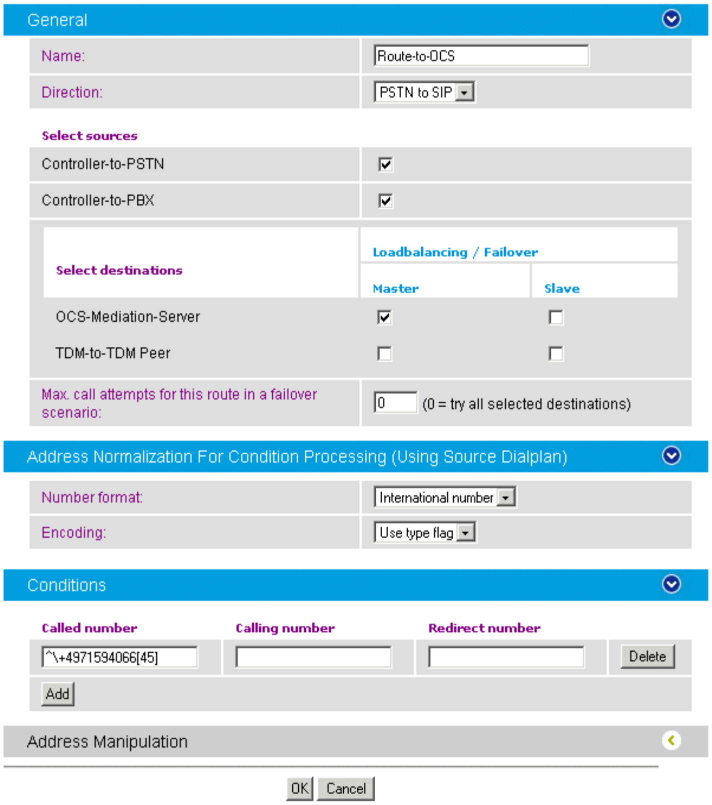
This peer is the loopback SIP peer that is needed to correctly route calls from the PBX to the PSTN.

13. Create five routings:

- one from the PSTN to Microsoft® Office Communications Server (OCS) 2007,
- one from Microsoft® OCS 2007 to the PBX,
- one from Microsoft® OCS 2007 to the PSTN,
- one for calls to the reception, and
- one to enable the TDM to TDM routing

In this scenario, the order of the routings is important because of the used conditions. In this example, the routings are configured in the correct order but it is also explained how to change the order in case you configured them differently.

- Create the route from the PSTN to Microsoft® OCS 2007 first. To do so, open the **Routing Configuration**, click **Add** and configure the following parameters:



- **Name**: Enter a unique name to easily identify the routing.
- **Direction**: Select **PSTN to SIP** from the dropdown menu.
- **Select sources**: Select both controllers as sources.
- **Select destinations**: Select the SIP peer you configured for the Microsoft® Mediation Server as **Master** destination.
- **Number format**: Select **International number** from the dropdown menu.
- **Encoding**: Select **Use type flag** from the dropdown menu.
- Under **Conditions**, click **Add**, and in **Called number**, enter a regular expression that matches only the numbers of the Microsoft® OCS 2007 in E.164 format including country code, area code, trunk prefix, and extension number. In this scenario, the extensions at the OCS start with 4 or 5. Within the regular expression, this is represented by [45].

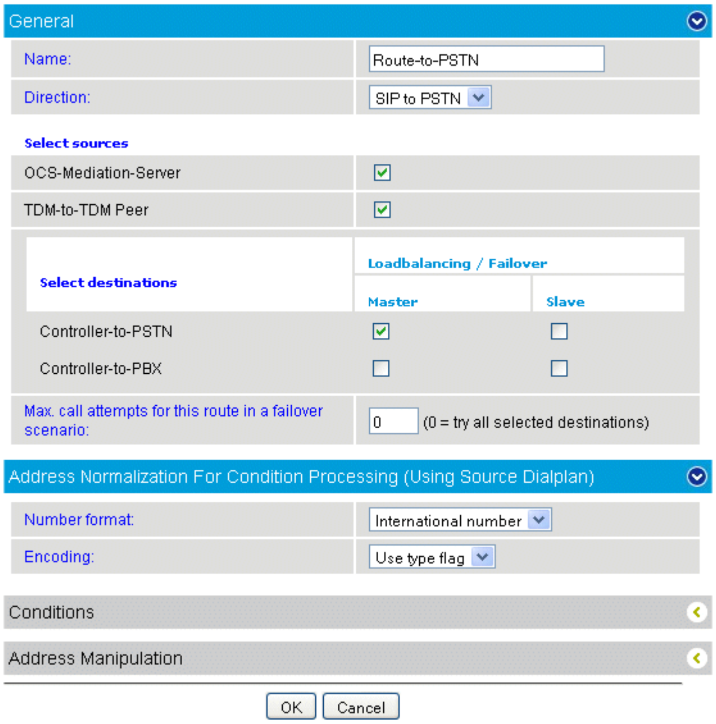
Click **OK** to save the settings and to close the window.

- Create the second route from the Microsoft® OCS 2007 to the PBX. To do so, click **Add** under **Routing Configuration** and configure the following parameters:

- **Name**: Enter a unique name to easily identify the routing.
- **Direction**: Select **SIP to PSTN** from the dropdown menu.
- **Select sources**: Select both controllers as sources.
- **Select destinations**: Select the SIP peer you configured for the Mediation Server as **Master** destination.
- **Number format**: Select **International number** from the dropdown menu.
- **Encoding**: Select **Use type flag** from the dropdown menu.
- Under **Conditions**, click **Add**, and in **Called number**, enter a regular expression that matches only the subscriber numbers of the PBX in E.164 format including country code, area code, trunk prefix, and extension number. In this scenario, the extensions at the PBX start with 2 or 3. Within the regular expression, this is represented by [23].

Click **OK** to save the settings and to close the window.

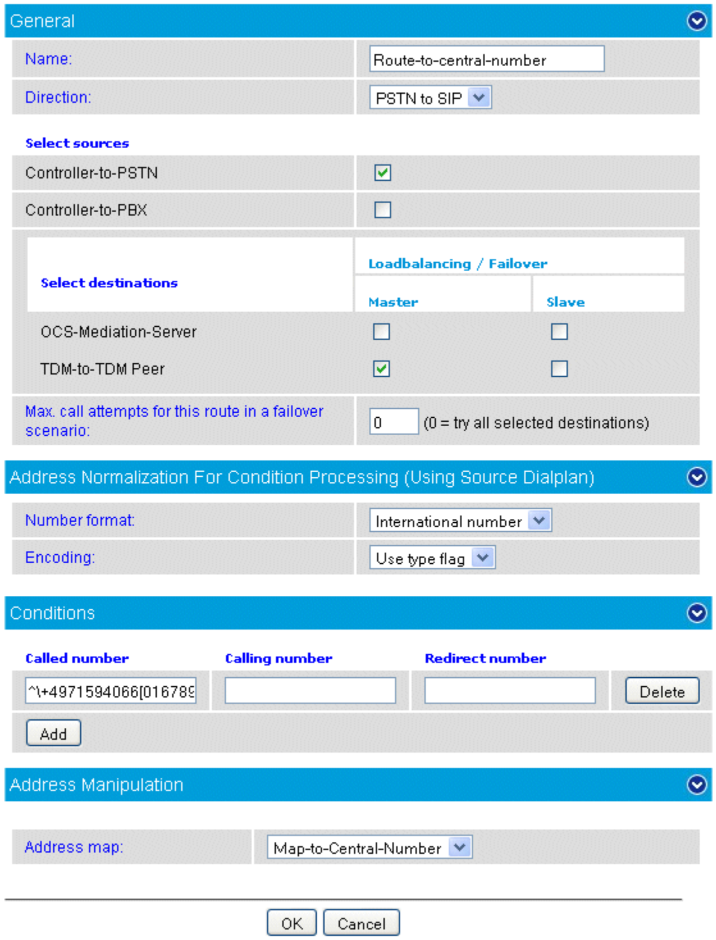
- Create the third route from the Microsoft® OCS 2007 to the PSTN. To do so, click **Add** under **Routing Configuration** and configure the following parameters:



- **Name**: Enter a unique name to easily identify the routing.
- **Direction**: Select **SIP to PSTN** from the dropdown menu.
- **Select sources**: Select both SIP peers as sources.
- **Select destinations**: Select the controller you configured for the PSTN as **Master** destination.
- **Number format**: Select **International number** from the dropdown menu.
- **Encoding**: Select **Use type flag** from the dropdown menu.

Click **OK** to save the settings and to close the window.

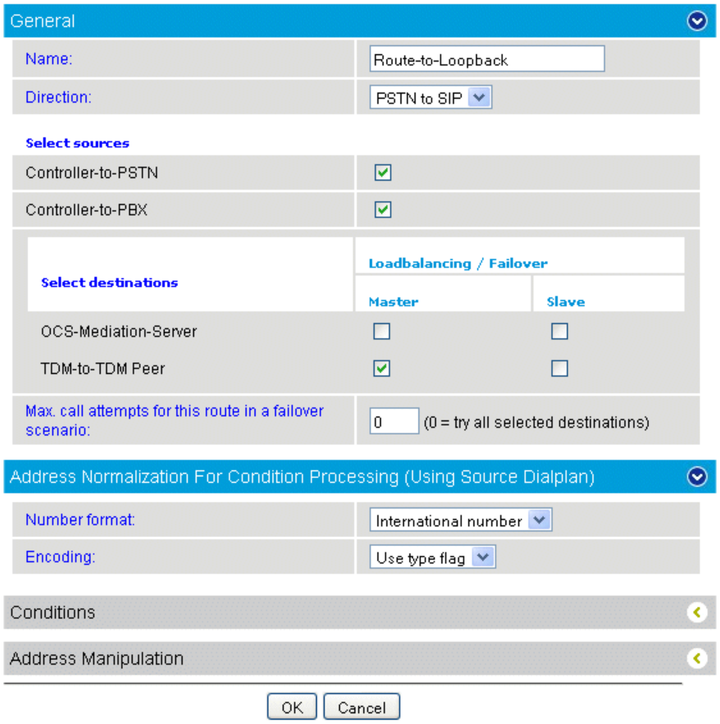
- Create the fourth route for calls to the reception. To do so, click **Add** under **Routing Configuration** and configure the following parameters:



- **Name**: Enter a unique name to easily identify the routing.
- **Direction**: Select **PSTN to SIP** from the dropdown menu.
- **Select sources**: Select the controller you configured for the PSTN as source.
- **Select destinations**: Select the TDM to TDM SIP peer as **Master** destination. We select this destination, because in this scenario the reception is connected to the PBX (extension 2000). If the reception is connected to the Microsoft® OCS 2007, select **OCS-Mediation-Server** as destination instead.
- **Number format**: Select **International number** from the dropdown menu.
- **Encoding**: Select **Use type flag** from the dropdown menu.
- Under **Conditions**, click **Add**, and in **Called number**, enter a regular expression that matches all extensions that should be routed to the reception, i.e., all unassigned extensions. In our example, the unassigned the extensions do NOT start with 2, 3, 4, or 5, because those are used either by the PBX or Microsoft® OCS 2007.
- Under **Address map** select the mapping for the reception.

Click **OK** to save the settings and to close the window.

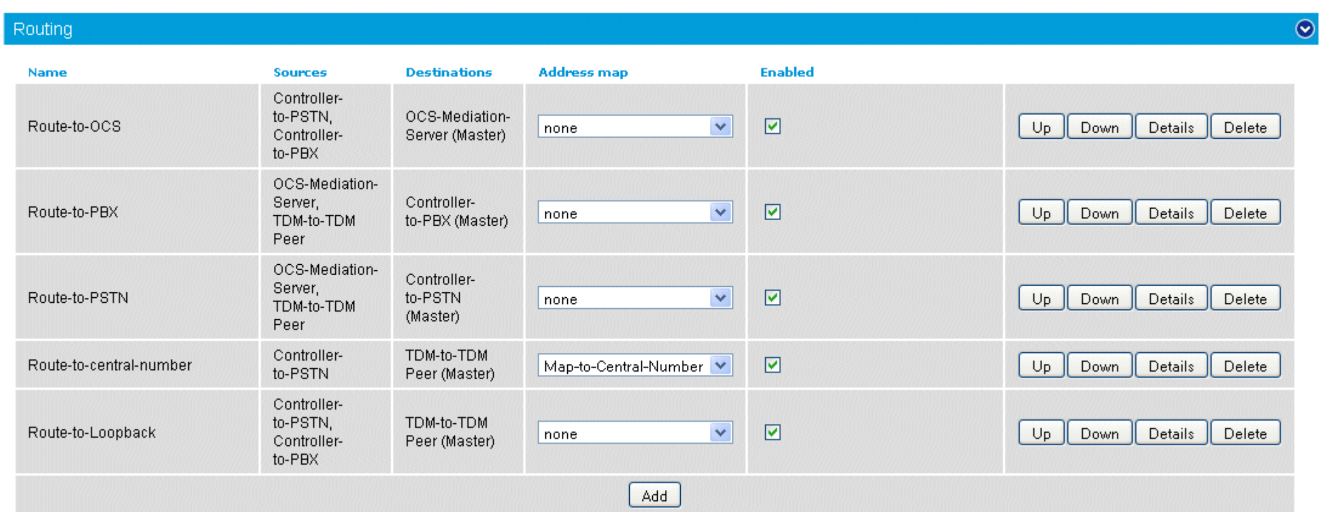
- Create the fifth route to enable the TDM to TDM routing. To do so, click **Add** under **Routing Configuration** and configure the following parameters:



- **Name**: Enter a unique name to easily identify the routing.
- **Direction**: Select **PSTN to SIP** from the dropdown menu.
- **Select sources**: Select both controllers.
- **Select destinations**: Select the SIP peer you configured for the PSTN as **Master** destination.
- **Number format**: Select **International number** from the dropdown menu.
- **Encoding**: Select **Use type flag** from the dropdown menu.

Click **OK** to save the settings and to close the window.

- To change the order of the routings in the main configuration page, click the **Up** or **Down** buttons. The order needs to be the same as in following graphic:



14. Click **Save** in the main configuration page to save the settings and activate the changes.

15. Configure the Microsoft® Office Communications Server 2007.

CHAPTER 15

Customer Service

Dialogic provides various options and arrangements for obtaining technical support for your Dialogic® product. We recommend that you use the Dialogic® Diva® Support Tools first before contacting your Dialogic supplier. Also, we suggest that you visit Dialogic Technical Services & Support site, as it includes detailed information about a variety of topics. In the unusual case that neither your supplier nor the information on the Services & Support site is able to adequately address your support issue, you can contact Dialogic Customer Support.

For more information see:

- Dialogic® Diva® Support Tools
- Dialogic Services and Support web site
- Dialogic Customer Support

Dialogic® Diva® Support Tools

If an issue occurs during the operation of your Dialogic® Diva® product, use the following Dialogic® Diva® Support Tools:

- Dialogic® Diva® Line Test: With the Diva Line Test tool, you can test your hardware and perform simple phone test calls, call transfers, or basic inbound and outbound calls.
- Dialogic® Diva® Diagnostics: With the Diva Diagnostics tool, you can write traces for each Dialogic® Diva® Media Board or driver into a file.
- Dialogic® Diva® Management tool: With the Diva Management tool, you can view the current status of the connected lines, the active connections, and the history of the connections.

For more information about the Diva Support Tools, see the respective online help files.

If you cannot address the issue through use of these tools, contact your Dialogic supplier.

Dialogic Services and Support web site

If your supplier is unable to help you to address your issue, visit the Services & Support web site, where you can find:

- detailed information about the Dialogic® Pro™ Services (1 or 5 year 24/7 service contracts) at http://www.dialogic.com/support/DialogicPro/
- a help web section for Dialogic® products at http://www.dialogic.com/support/helpweb
- a download section to install the newest version of your software at http://www.dialogic.com/support/downind.asp
- a training section with information about webinars, online, and onsite trainings at http://www.dialogic.com/training/default.htm
- a manuals section that provides a complete set of available documentation at http://www.dialogic.com/manuals/default.htm
- technical discussion forums about different developer-specific Q&A at http://www.dialogic.com/den/groups/developers/default.aspx
- the Dialogic Customer Support site. For detailed information about how to contact Dialogic Customer Support, see Dialogic Customer Support on page 115.

Dialogic Customer Support

If the information on the Services & Support site was not sufficient to help you address your issue, contact Dialogic Customer Support. See www.dialogic.com/support/contact for details.

Please note that when you contact Dialogic Customer Support, you may need to provide or have handy one or more of the following:

- A debug trace (see the Dialogic® Diva® Diagnostics Online Help file - DivaTrace.chm.)
- A copy of your active Dialogic® Diva® System Release configuration (see the Dialogic® Diva® Configuration Manager Online Help file - DSMain.chm).
- A copy of your Dialogic® Diva® SIPcontrol™ software configuration. To save a copy, open a DOS window, change to the directory in which the Diva SIPcontrol software files are stored and execute: regfile.exe save <nameofthefile>.txt or click **Show Configuration** at the bottom of the configuration web interface and copy and paste the contents into a separate file and save it as text file.