Dialogic® Diva® SIPcontrol™ Software

v2.0 Linux

Reference Guide

November 2008 206-479-04

www.dialogic.com

Contents

About Dialogic® Diva® SIPcontrol™ Software

The Diva SIPcontrol software version 2.0 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 Media 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.

Copyright and Legal Notice

Fourth Edition (November 2008) **206-479-04**

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.

Feature Overview

New features in the Dialogic® Diva® SIPcontrol™ Software version 2.0

- Support for TLS and SSL encryption and authentification
- Support for SRTP (secure Real-time Transport Protocol)
- Support for SIPS (Secure SIP)
- Support for Windows Vista® and Windows Server® 2008
- Diva SIPcontrol software update via web interface
- Support for G.726 codec (16,24,32, and 40 kbps)

General Features

- 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 (only applicable for Microsoft® Windows® operating systems)
  - 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.
- Support for North-American numbering plan: The configuration of multiple area codes are 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.
- 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.
- 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** for the supported codecs.
- Support for Proxy and Registrar registration
- 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
- Configurable IP transport layer TCP, UDP, or TLS
- Basic call including 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, is used to provide the feature Message Waiting Activation / Deactivation with regular SIP clients. However, in a gateway configuration, applications use the features without the need for the 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 17 for more information.

Note: iLBC is only available on Dialogic® Diva® V-2PRI and V-4PRI Media Boards.

- 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 and 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)
- RFC 3551 - 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
- RFC3851 - Internet Low Bit Rate Codec (iLBC)
- RFC3952 - Real-time Transport Protocol (RTP) Payload Format for internet Low Bit Rate Codec (iLBC) Speech
- 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

- Number manipulation is defined 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):

Dialogic® Diva® BRI Media Boards

- Diva BRI-2M PCI v2
- Diva BRI-2M PCIe v2
- Diva 4BRI-8M PCI v2
- Diva 4BRI-8M 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/E1/T1-8 PCI v3
- 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-PRI/E1-120 PCI v1

Dialogic® Diva® Analog Media Boards

- Diva Analog-2 PCI v1
- Diva Analog-2 PCIe v1
- Diva Analog-4 PCI v1

- Diva V-Analog-4 PCI v1 1)
- Diva V-Analog-4 PCIe v1 1)
- Diva V-Analog-8 PCI v1 1)

- Diva UM-Analog-4 PCI v1
- Diva UM-Analog-4 PCIe v1
- Diva UM-Analog-8 PCI v1

- Diva Analog-4 PCIe v1
- Diva V-Analog-8 PCIe v1[1)]
- Diva UM-Analog-8 PCIe v1
- Diva Analog-8 PCI v1
- Diva 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 8.5 LIN Service Update 2 software.

Supported operating systems

The Dialogic® Diva® SIPcontrol™ software supports Linux 32 bit and 64 bit, kernel 2.2.x, 2.4.x and 2.6.x up to 2.6.20. For further information, see ***www.dialogic.com*** http://www.dialogic.com.

Software Installation

The Dialogic® Diva® SIPcontrol™ software is automatically installed together with the Dialogic® Diva® for Linux package in /usr/lib/opendiva/diva.sipcontrol.

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:

- Licenses for G.729, V.17, and V.34 need to be activated in the Dialogic® Diva® Configuration Manager. See the Dialogic® Diva® Configuration Manager Online Help for more information.
- The fax functionality needs to be licensed only for Dialogic® Diva® PRI Media Boards with multiple ports.
- Dialogic® Host Media Processing (HMP) Software licenses for SIP channels are also valid for SIPcontrol, but they require HMP software to be installed on the same system as the Diva SIPcontrol software.

To activate your license file, you need the Device Unique ID (DUID) and the Proof of Purchase Code (PPC).

Once you have both, the DUID and the PPC, visit the Dialogic activation web site to register your PPC together with the DUID to receive the license file. See ***To register your DUID and PPC*** on page 17 for more information. Activate this license file in the Diva SIPcontrol software configuration web interface. For more information, see ***To activate the license file*** on page 20.

Device Unique ID (DUID)

The DUID binds the installed Dialogic® Diva® SIPcontrol™ Software to your PC (PC fingerprint).

To get the DUID:

1. Open the 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 the web activation using another computer, open an editor, paste the DUID, and save the file.

Proof of Purchase Code (PPC)

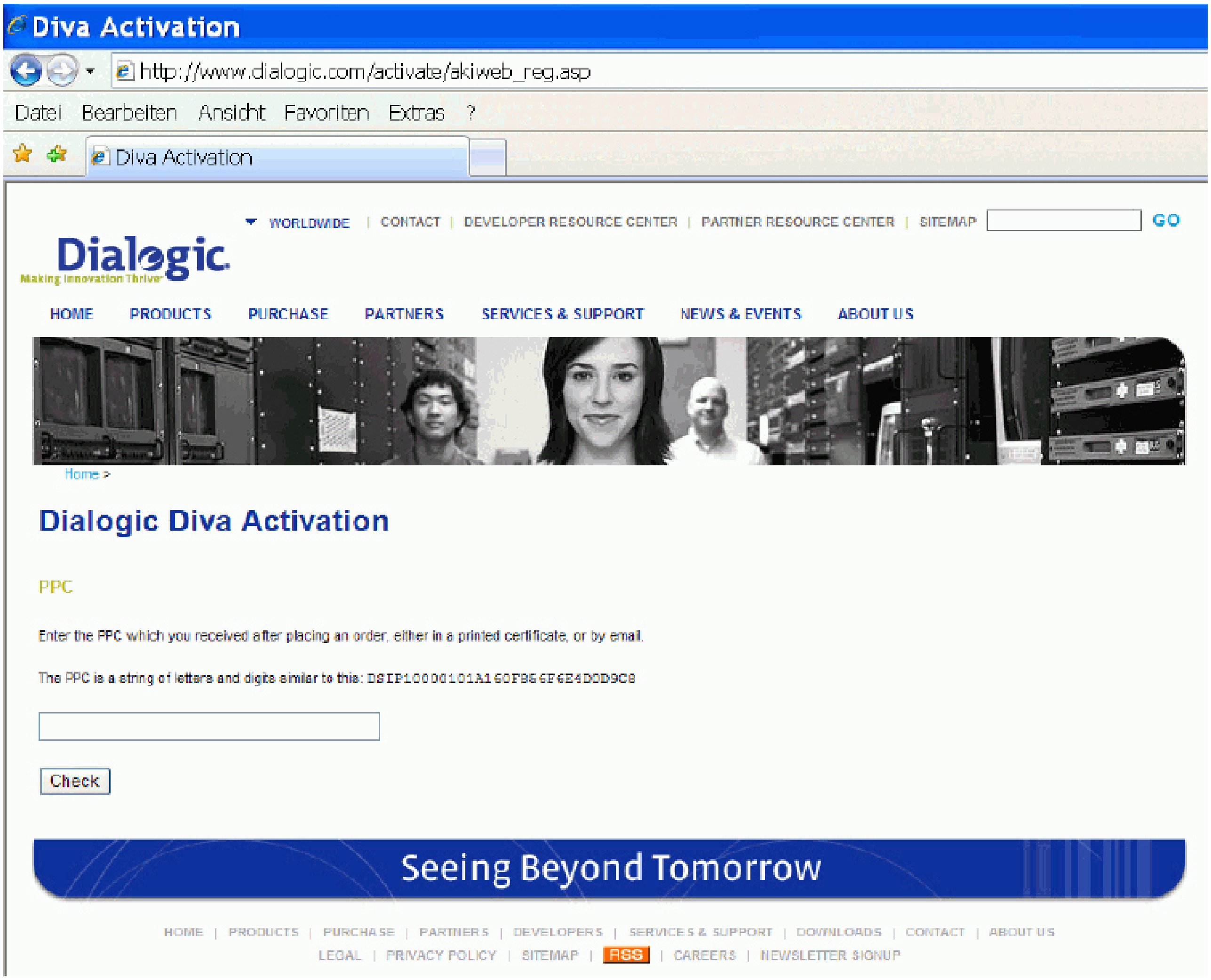
When you purchase the Dialogic® Diva® SIPcontrol™ Software license, you receive a PPC either in printed form or via email. By registering this PPC, you represent and warrant that you lawfully purchased the license.

To register your DUID and PPC

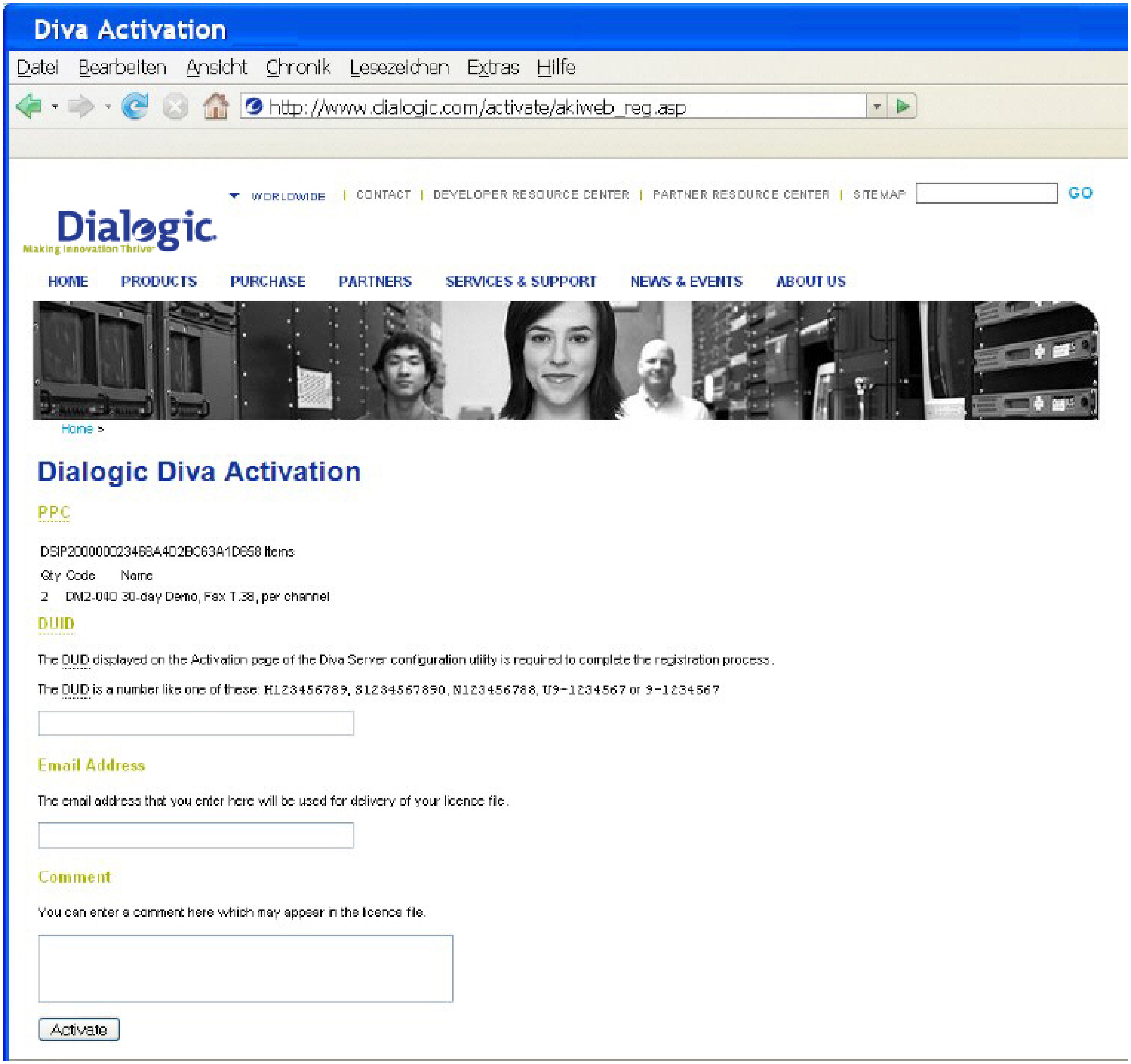
Once you have your DUID and PPC, you can register them as follows:

1. Open the following web site: ***www.dialogic.com/activate*** http://www.dialogic.com/activate.

2. Enter the 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 received license file and activate it. For more information, see ***To activate the license file*** on page 20.

To activate the license file

After you have received your license file by email and have saved it, you can activate it.

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

To activate the license:

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.

Dialogic® Diva® SIPcontrol™ Software Configuration

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

To open the Diva SIPcontrol software web interface:

1. Open an internet browser on the computer where the Diva SIPcontrol software is installed and enter http://127.0.0.1:10005. By default, the access to the web interface is only allowed from the 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 and click **Password** on the left hand side under **Configuration**. Enter an at least 7 digit long password and confirm it. Click **Save** to make the new password active.
3. For remotely accessing the configuration, open the port in the local firewall settings.
4. Restart the Dialogic® Diva® WebConfig service.

Now, you can access the Diva SIPcontrol software web interface on any of the IP addresses of the PC where SIPcontrol is installed.

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.

Configuration Tips and Hints

- Changes to the configuration will only take effect after you clicked **Save** at the bottom of the main configuration page.
- All 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.

- All 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.
- 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 Dialogic® 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.

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 in ***Dialplan Configuration*** see "Dialplans" on page 44.

To change the settings for the enabled controller, click **Details** 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.

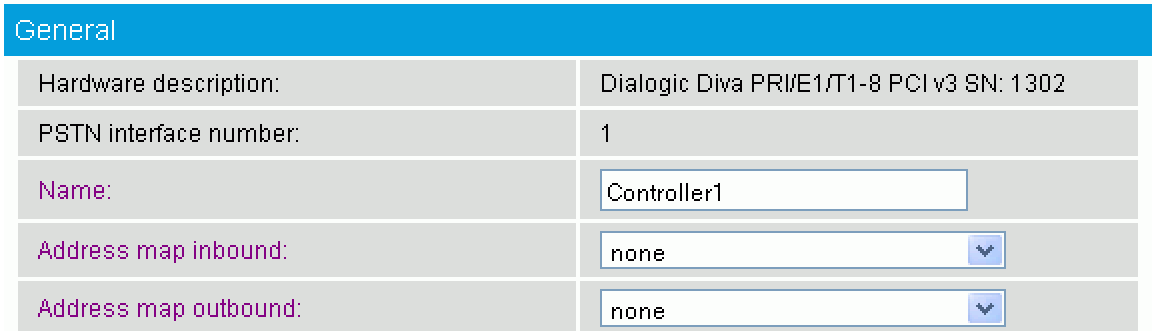
Note: PSTN interfaces without a binding to the CAPI service in the Dialogic® Diva® Configuration Manager are disabled in the Diva SIPcontrol software web interface and cannot be configured.

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

- ***General*** see "General Configuration" on page 22
- ***Address Normalization*** on page 23
- ***PSTN Call Transfer Settings*** on page 25
- ***Message Waiting Indication (MWI)*** on page 26

General Configuration

You can configure the parameters shown in the graphic and explained 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 can 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 incoming calls on this interface. See ***Address Map Configuration*** see "Address Maps" on page 47 for more information about setting up a regular expression list.

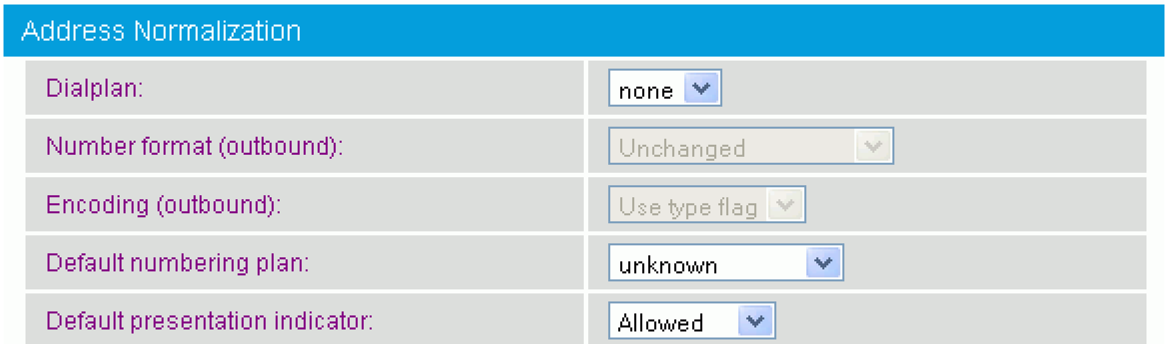
Regular expressions may be used to add or remove dial prefixes required by a PBX or to rewrite public phone numbers of different number ranges into a common format. See the regular expression ***examples*** on page 70 for more information.

Address map outbound: Select the name of a regular expression list to be applied on outgoing calls on this interface. See ***Address Map Configuration*** see "Address Maps" on page 47 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 regular expression ***examples*** on page 70 for more information.

Address Normalization

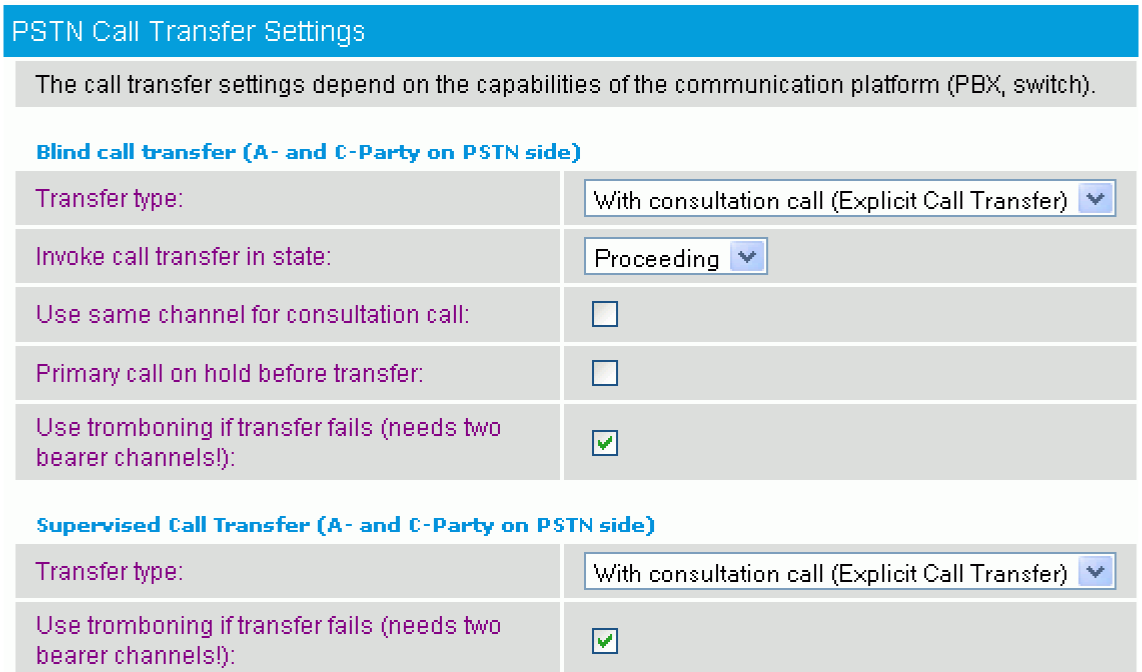
You may configure the parameters shown in the graphic and explained below:



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, all 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. You need to configure the local dialplan as described under ***Dialplan Configuration*** see "Dialplans" on page 44 before you can select it here.
Number format (outbound):	This parameter determines the shortest format allowed that is sent on outbound calls. 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 65.
Encoding (outbound):	Determines if numbers of outbound calls 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 Dialogic® 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.

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:

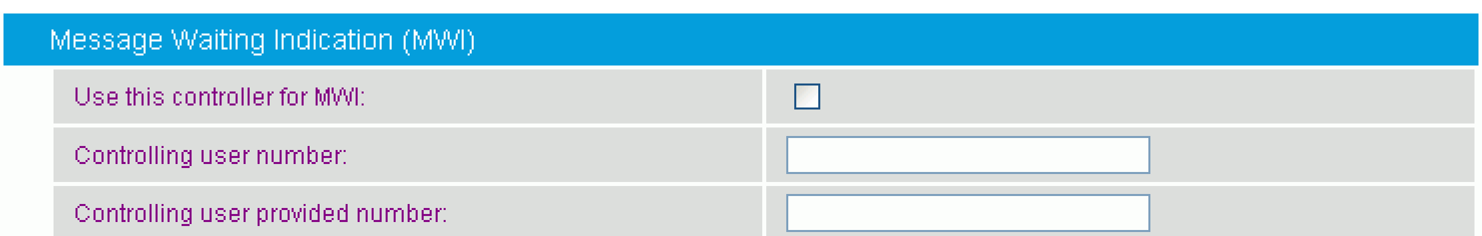
Choose this option if the first call should be on hold when transferring the call.

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.

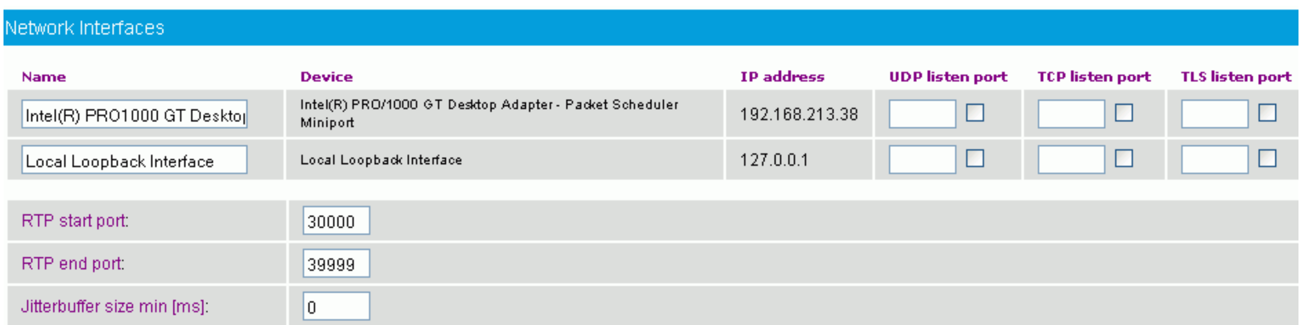
Controlling user number: A PBX typically requests an authentication to allow for updating of the message waiting indication. This authentication is done by a **Controlling user number**. The administrator of the PBX can provide this number.

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 interface 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 2.0 supports only a single IP address and port number. 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 Dialogic® Diva® SIPcontrol™ Software is installed.
Protocol	From the drop down menu, select the IP protocol supported in calls from SIP: either TCP, UDP or both.
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 Dialogic® 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 Dialogic® 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 on the **Global Security** configuration page.
Enabled	Enable the network interface to use for the configuration. Note that you may only enable one network interface.
RTP Start Port	Defines the lowest port of the range in which the Dialogic® 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 Dialogic® Diva® SIPcontrol™ Software sends and receives RTP streams. Change this value only if problems occur.
Jitterbuffer Size Min (ms)	Specifies the minimum time in milliseconds used by the Dialogic® Diva® SIPcontrol™ Software to buffer RTP data before streaming it to the ISDN. Normally, the value is adjusted automatically according to network quality and network usage, but in some cases it may need to be increased to prevent buffer underruns. However, increasing the value also increases latency and therefore it should be left at the default of 0 milliseconds.

SIP Peers

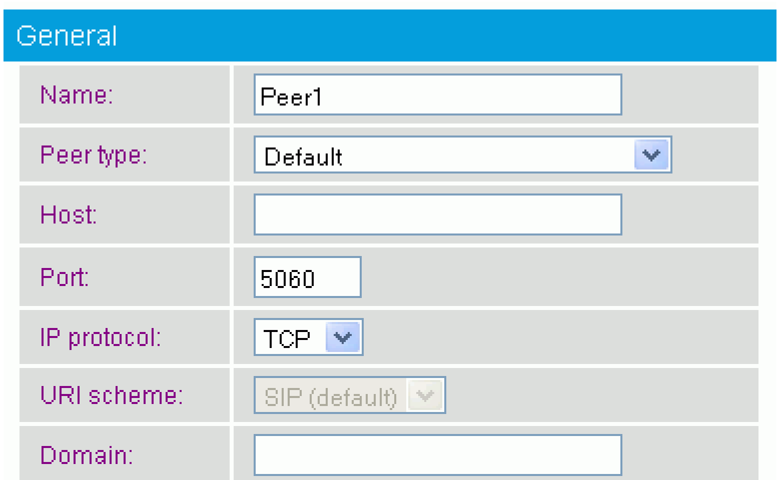
A SIP peer is a specific endpoint to and from which the Dialogic® Diva® SIPcontrol™ Software will establish calls. The peer-specific settings may be used to adapt the Diva SIPcontrol software's behavior towards this peer.

To add a SIP peer, click **Add**. To change the settings for the enabled SIP peer, click **Details** 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:

- ***General*** on page 29
- ***Enhanced*** on page 31
- ***Security*** on page 34
- ***Session Timer*** on page 35
- ***Address Normalization*** on page 35
- ***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 Dialogic® Diva® SIPcontrol™ Software establishes the calls.

Peer type: Some SIP peers need a specific peer, such as a Microsoft® Exchange or an ephone server to work properly with the Dialogic® 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: From the drop down menu, select the IP protocol to be used for calls to this peer. 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**.

Calls from this peer are accepted with all protocols and on all ports/addresses configured in ***Network Interface Configuration*** see "Network Interfaces" on page 27.

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

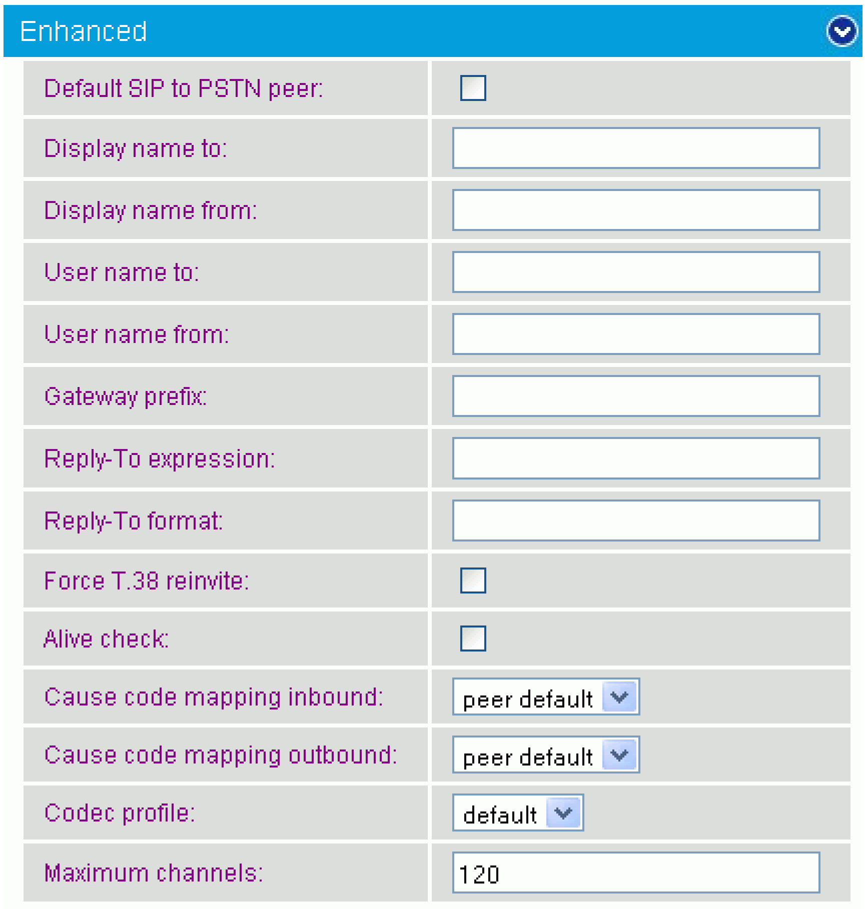
Calls are transmitted via various proxy servers. Some of them do not transmit the calls as encrypted calls. If you select **SIP (default)**, you allow that calls are transmitted via such proxy servers.

To make sure that a call is sent encrypted to the proxy of the remote side, select **SIPS (secure SIP)**. If 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.

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 Dialogic® 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 to this peer on calls from the PSTN to SIP. To sent 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 "\\".

Display name from: Enter the name that is to be sent in the "From" header of the INVITE message to this peer on calls from the PSTN to SIP. To sent 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: If you selected **e-phone** as **Peer Type**, you can enter the prefix of the the e-phone server.

This prefix is added at the start 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 **Edit SIP Peer Configuration**.

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**.

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 Some peers do not switch the media channel to T.38 if they receive a fax call, e.g., if

reinvite: 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 Dialogic® Diva® SIPcontrol™ Software does not wait for a call timeout 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.

Address map inbound: The regular expressions list applied to the addresses received on calls from this SIP peer. See ***Address Map Configuration*** see "Address Maps" on page 47 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 regular expression ***examples*** on page 70 for more information.

Address map outbound: The name of a regular expression list to be applied on outgoing calls on this SIP peer. See ***Address Map Configuration*** see "Address Maps" on page 47 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 regular expression ***examples*** on page 70 for more information.

Cause code mapping inbound: Select the cause code mapping for incoming calls that you configured under ***Cause Code Configuration*** see "Cause Code Maps" on page 49.

Cause code mapping outbound: Select the cause code mapping for outgoing calls that you configured under ***Cause Code Configuration*** see "Cause Code Maps" on page 49.

Codec profile: Select the codec list that you configured under ***Codec Configuration*** see "Codec Profiles" on page 51. If you do not select a list, an internal default list is used with the following default priority order:

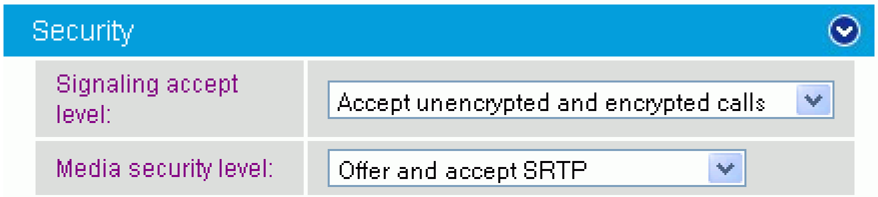
1. G.711A-law
2. G.711u-law
3. G.726 (16, 24, 32, and 40 kbps)
4. G.729, if licensed
5. iLBC, if available on the used Dialogic® Diva® Media Board
6. GSM-FR
7. DTMF via RFC2833 (no real codec, but internally handled as codec)
8. T.38, if supported by the used Diva Media Board

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 Dialogic® Diva® SIPcontrol™ Software.

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 Dialogic® 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.

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.

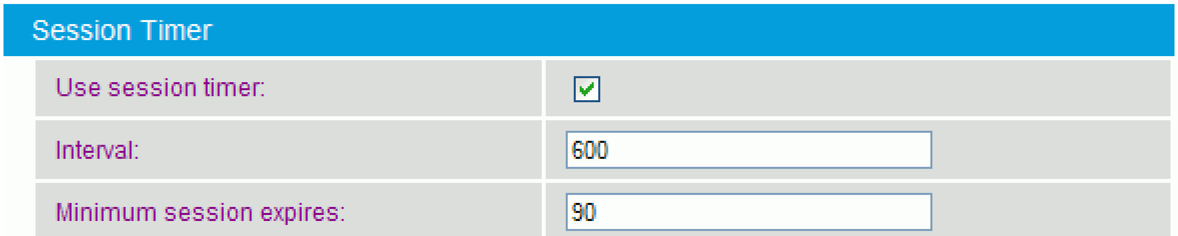
Offer and accept SRTP: The voice stream is secured with SRTP, if possible.

Require SRTP for encrypted calls: Calls via TLS have 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

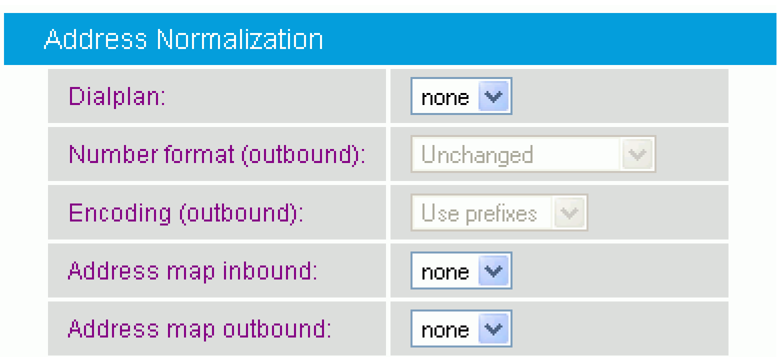
You may configure the parameters shown in the graphic and explained below:



Use session timer:	Activates session monitoring via SIP session timers using the timeout values given here. Refer to RFC4028 for details.
Interval:	If **Use session timer** is enabled, you may set a timeout 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 Dialogic® 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 **Dialplan Configuration** 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 out on outbound calls. You can 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 if no country code is given or if the area code matches the location settings.

Extension: The number is converted to the extension only if no additional information is given or if the country / area code and basic phone number match the location settings.

Encoding (outbound): Determines if numbers of outbound calls should either be encoded as unknown number with national or international prefix digits or as national or international call 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 Map Configuration*** see "Address Maps" on page 47 for more information about setting up a regular expression list.

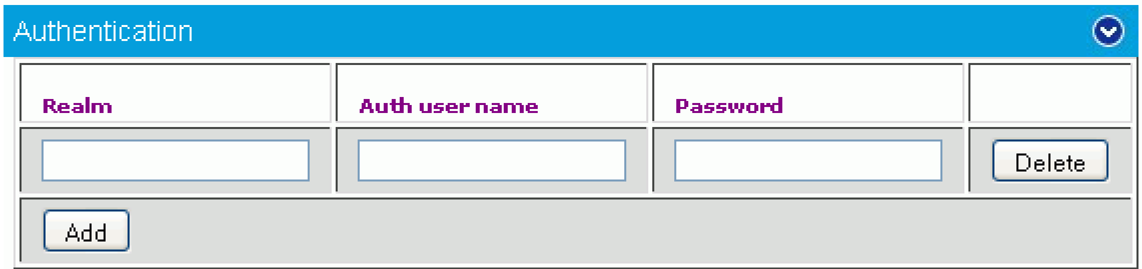
Regular expressions may be used to add or remove dial prefixes required by a PBX or to rewrite public phone numbers of different number ranges into a common format. See the regular expression ***examples*** on page 70 for more information.

Address map outbound: Select the name of a regular expression list to be applied on outgoing calls on this interface. See ***Address Map Configuration*** see "Address Maps" on page 47 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 regular expression ***examples*** on page 70 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:

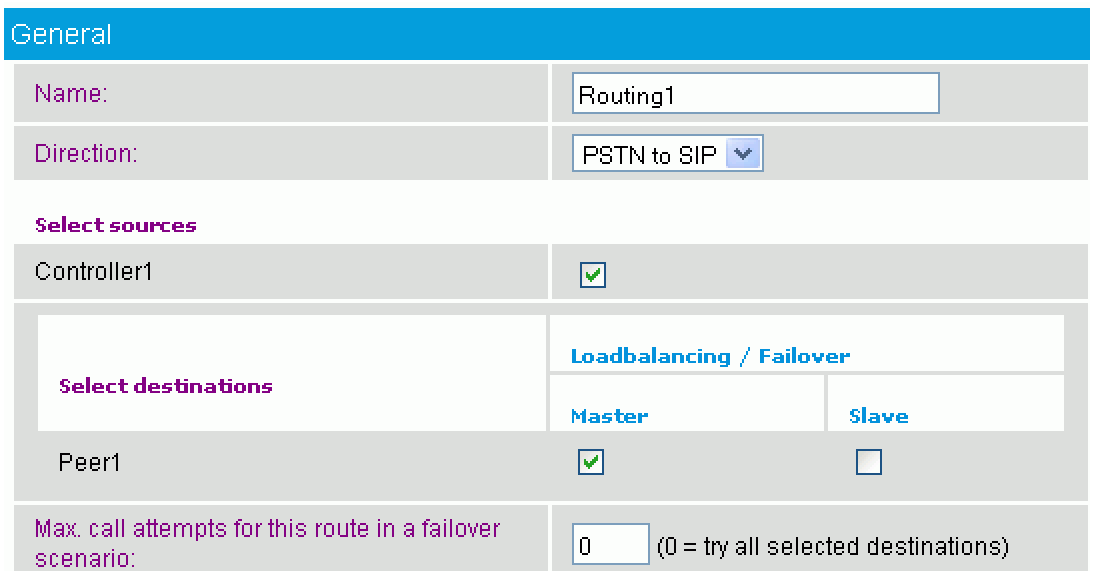
- Called, calling, and redirected number or SIP address of a call for which the redirected number is only available for calls originating in the PSTN,
- the source where a call originated, i.e., a PSTN interface name or a specific SIP peer,
- the current channel allocation across a set of several possible destinations in a load-balancing environment, and
- the current status of a destination. See ***How a Call Is Processed*** see "How Calls Are Processed" on page 58for more information.

For more information about possible routing configurations, see ***Routing Examples*** on page 61.

To add a routing, click **Add**. To configure an existing routing, click **Details**. 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 will pop up.

Edit Routing Configuration

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



Name: Enter a name to easily identify the cause code mapping table. If you create your own cause code mapping table, make sure to select it in the **SIP Peer Configuration** under **Enhanced Configuration**.

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 all configured PSTN interfaces or SIP peers. The route will only be considered for a call if the call originated from a selected source.

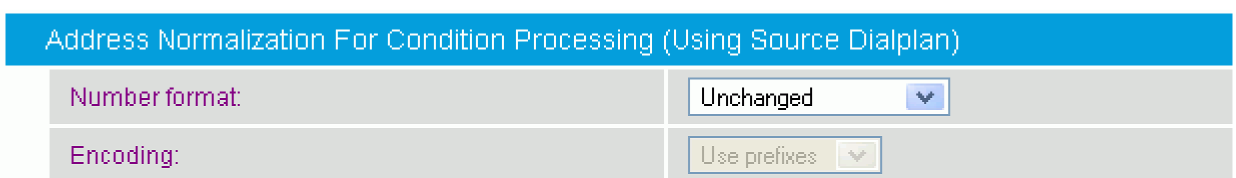
Note: A source may be selected even if it is currently disabled. In this case, the call will already have been rejected before the route is queried. At least one source interface is required for the route.

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. numbers of call attempts for this route: Enter the number of times that the Dialogic® 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 of a route. 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 that is sent on outbound calls. 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 65.

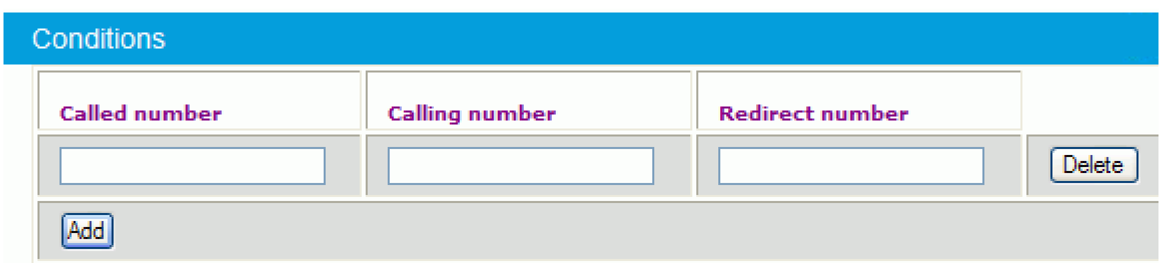
Encoding: Determines if numbers of outbound calls should either be encoded as unknown number with national or international prefix digits, or as national or international number with type flags.

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.

Note: A route can only be matched if all 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 all three condition parts left empty will always apply, thus working as a default route.

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 Dialogic® 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.

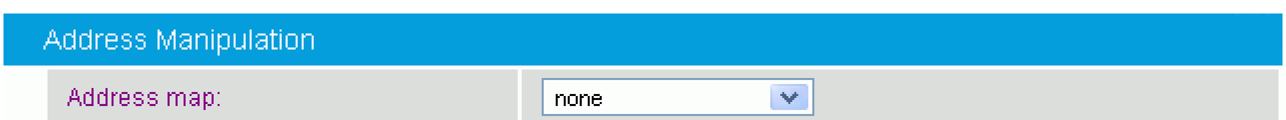
Note: A route can only be matched if all three condition parts (called number, calling number, and redirect number) match their call address counterpart in any of the lines. Empty condition entries always match, i.e., a line with all three condition parts left empty will always apply, thus working as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

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 Dialogic® 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 all three condition parts (called number, calling number, and redirect number) match their call address counterpart in any of the lines. Empty condition entries match always, i.e., a line with all 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:



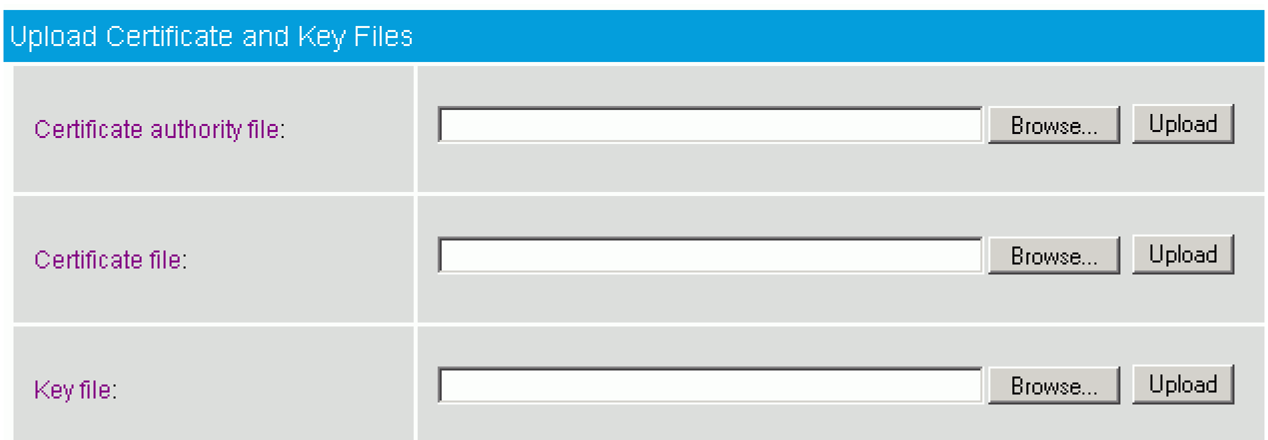
Address Map: If a route matches, the address manipulation setting allows for modifying the call addresses according to your needs. For example, if all calls with the called party number starting with "9" should be directed to a specific peer, it might be desirable to remove this digit. This can be done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

Security Profiles

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

Upload Certificate and Key Files

For authentification and data encryption, certificates need to be installed on the computer with the Dialogic® Diva® SIPcontrol™ Software and on remote computers. When a secure domain is opened, server and client authentify 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. All files need to have the extension "pem".

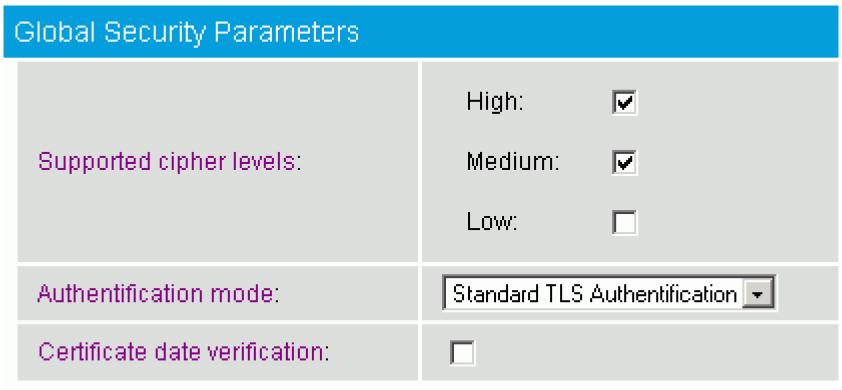


Certificate authority file: With this file, the CA enssures that the public key contained in the certificate belongs to the server stated in the certificate.

Certificate file: This file contains the public key of the server on which the Dialogic® Diva® SIPcontrol™ Software is installed.

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. Here you can select the level of en-/decryption:

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.

Authentification mode: Select how the server-client authentification should be handled.

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 engine supports the following features:

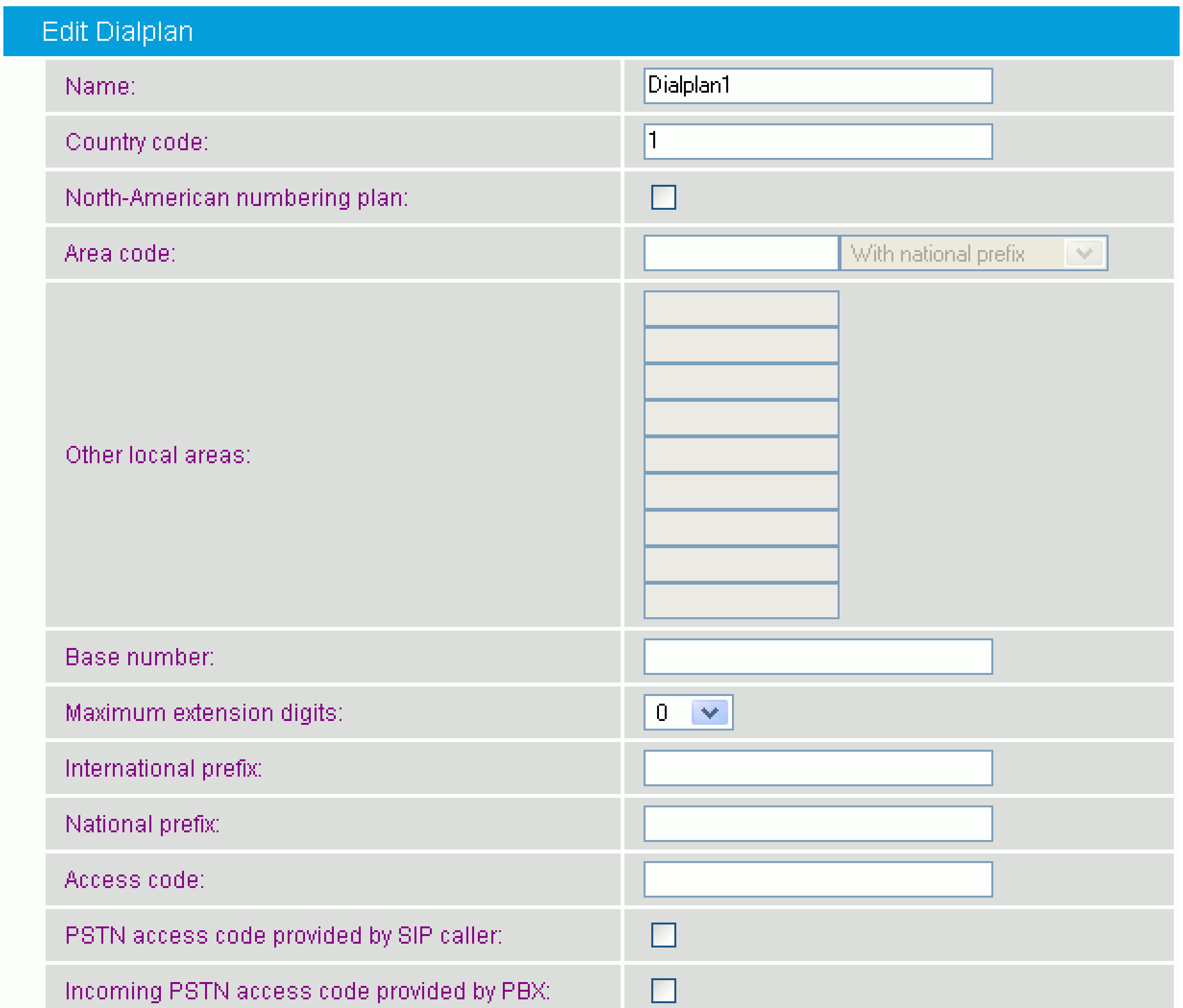
- Number expansion and reduction: called, calling, and redirected numbers are converted to one of the following formats: international, national, local, or internal (extension-only) format; for each format, either prefix digits or digital number type flags may be used.
- Adding and removing of the line 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 neighbouring 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 Dialogic® 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 of 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 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, 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 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 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 **Add**. To configure an existing dialplan, click **Details**. 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 dialplan, e.g., Stuttgart office.

Country code: Enter the country where the computer with the installed Dialogic® Diva® SIPcontrol™ Software is located.

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 Dialogic® 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 may 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 (NANP) 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.

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

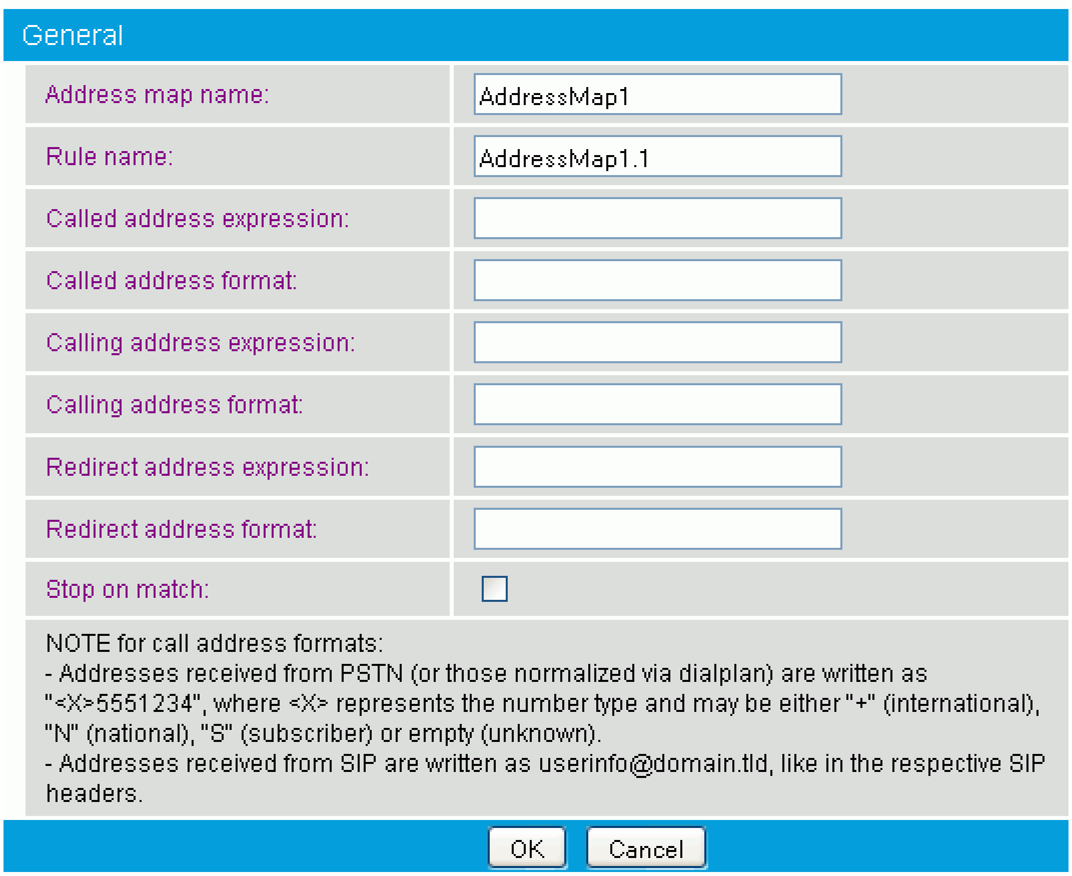
In general, address maps should be used for cases that are not covered by the dialplan. Possible scenarios are:

- 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 configuration, click the **Add** button. To configure an existing address map, click the **Details** button. 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:



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 can 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 ***Regular Expressions*** see "Number modification using regular expressions" on page 68 for more information.
Called address format:	If the address format entered here matches a called address, the format string is applied to the result. See ***Regular Expressions*** see "Number modification using regular expressions" on page 68 for more information.
Calling address expression:	If the regular expression entered here matches a calling address, the format string is applied to the result. See ***Regular Expressions*** see "Number modification using regular expressions" on page 68 for more information.
Calling address format:	If the address format entered here matches a calling address, the format string is applied to the result. See ***Regular Expressions*** see "Number modification using regular expressions" on page 68 for more information.
Redirect address expression:	If the regular expression entered here matches a redirected address, the format string is applied to the result. See ***Regular Expressions*** see "Number modification using regular expressions" on page 68 for more information.
Redirect address format:	If the address format entered here matches a redirected address, the format string is applied to the result. See ***Regular Expressions*** see "Number modification using regular expressions" on page 68 for more information.
Stop on match:	If all expressions match all addresses of a call, this parameter determines if the Dialogic® Diva® SIPcontrol™ Software should continue to search for matching rules. If set, the address matching is aborted.

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

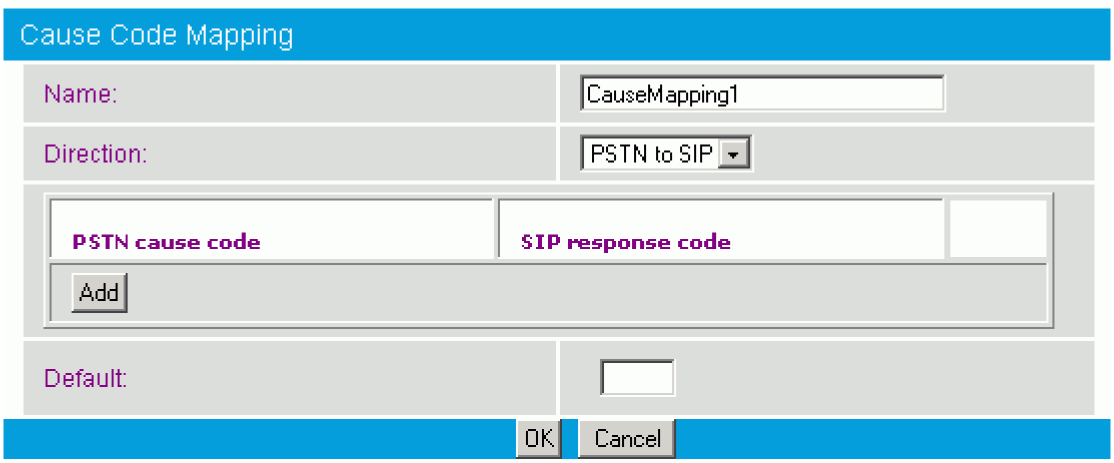
Cause Code Maps

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

If the internal default mapping table provided by the 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 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*** on page 31.

To add a cause code, click **Add**. To change the settings, click **Details** 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:



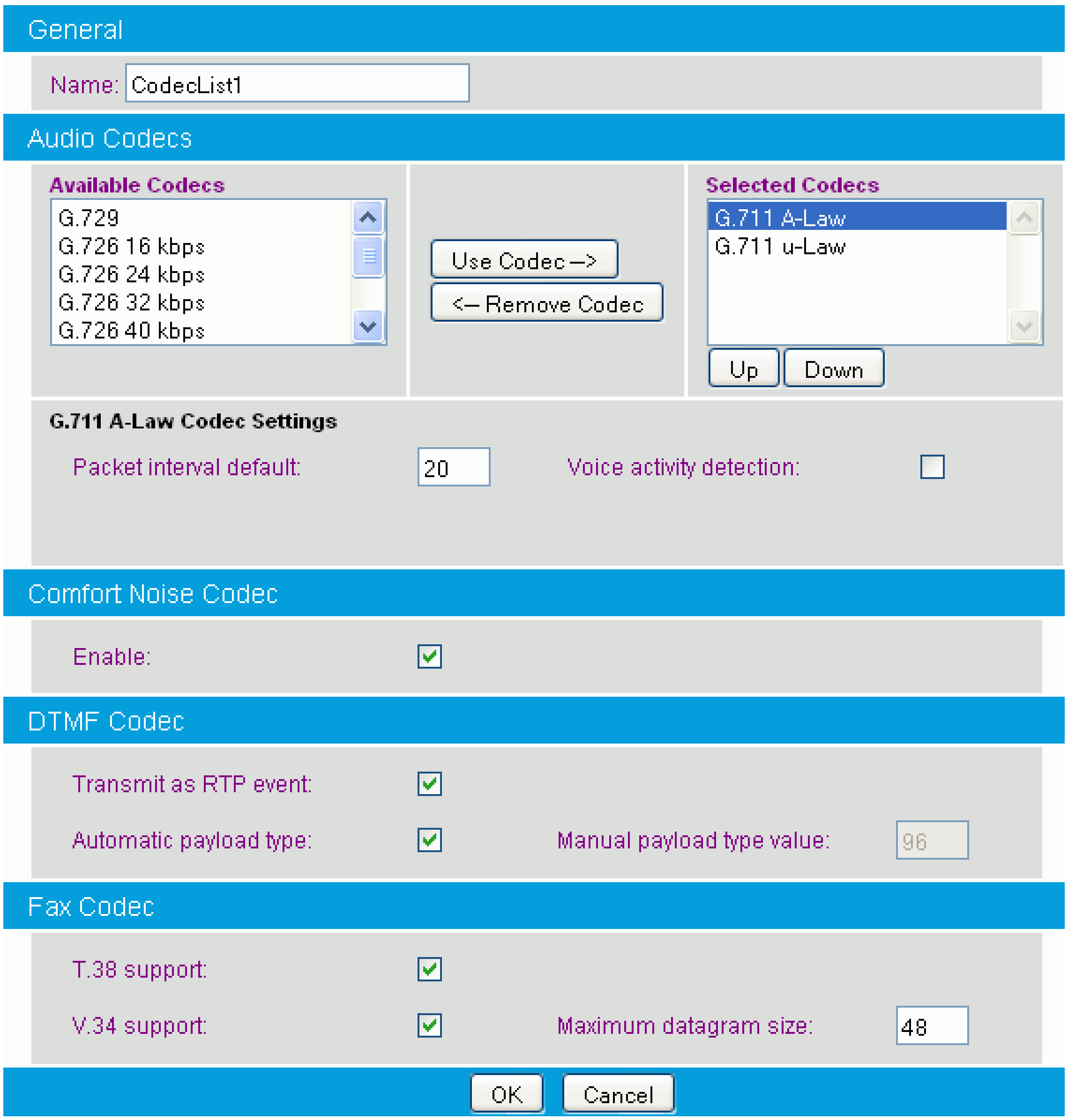
Name	Enter a name to easily identify the cause code mapping table. If you create your own cause code mapping table, make sure to select it in the **SIP Peer Configuration** under **Enhanced Configuration**.
Direction	Select the direction for which this table is used: • Select **PSTN to SIP**, to configure 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. The values are only valid in the range from 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. See the chapter "Cause Code Mapping" in the Diva SIPcontrol Software Reference Guide for the default mapping table.

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*** on page 31.

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. If you create your own codec list, make sure to select it in the **SIP Peer Configuration** under **Enhanced 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 purchased and activated a license. For more information, see ***License Activation*** on page 17.

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.

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 Dialogic® Diva® SIPcontrol™ Software uses the value suggested by the endpoint. Generally, this parameter is left at its default value.

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.

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

DTMF 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 Dialogic® Diva® SIPcontrol™ Software uses the value suggested by the endpoint. Generally, this parameter is left at its default value.

T.38 support: T.38 is a protocol that enables fax transmissions of 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. For more information, see ***License Activation*** on page 17.

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. For more information, see ***License Activation*** on page 17.

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.

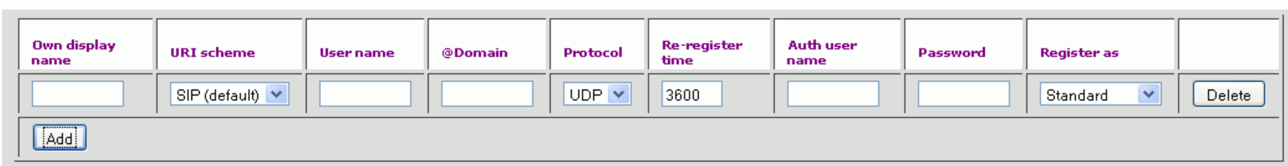
Registrar Protocol: Select the protocol the registrar server uses.

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 on the device of the called party.

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.

User Name: Enter the name or number that the Dialogic® 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.

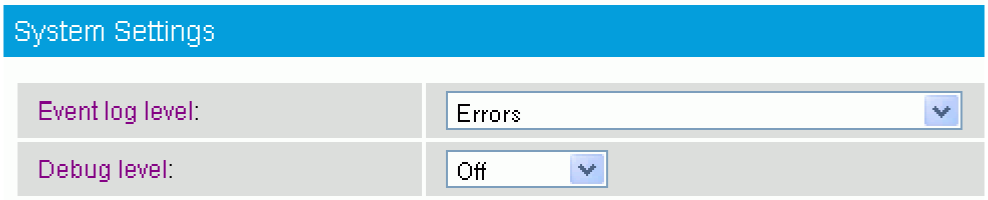
Auth User Name: Enter a user name for authentication at the registrar server.

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 Dialogic® Diva® SIPcontrol™ Software to function as gateway for e-phone.

System Settings

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:



Event Log Level: A computer with the Dialogic® Diva® SIPcontrol™ Software installed, may write different types of events into the System Event Log. The details for each event log are described in the chapter Event Logging of the Dialogic® Diva® SIPcontrol™ Software Reference Guide.

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.

Data Security Overview

With 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 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, however, 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 signalling 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*** see "Network Interfaces" on page 27 and enable TLS as transport protocol as described in ***Network Interfaces*** on page 27. For general information about certificates, see the section below.

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 "so called" 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.

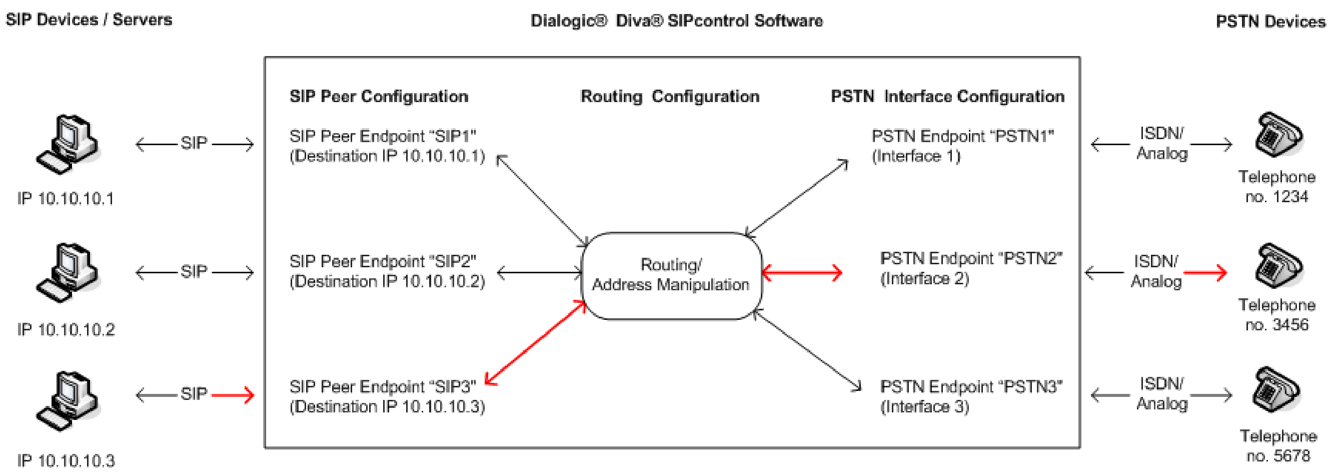
SRTP can be set for each SIP peer in the ***Security*** on page 34 configuration. The cipher level can be set in the ***Global Security Parameters*** see "Security Profiles" on page 42 as described in ***Security Profiles*** on page 42.

Certificates

For authentification 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 via 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, 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 unsecure.

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.

A 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).

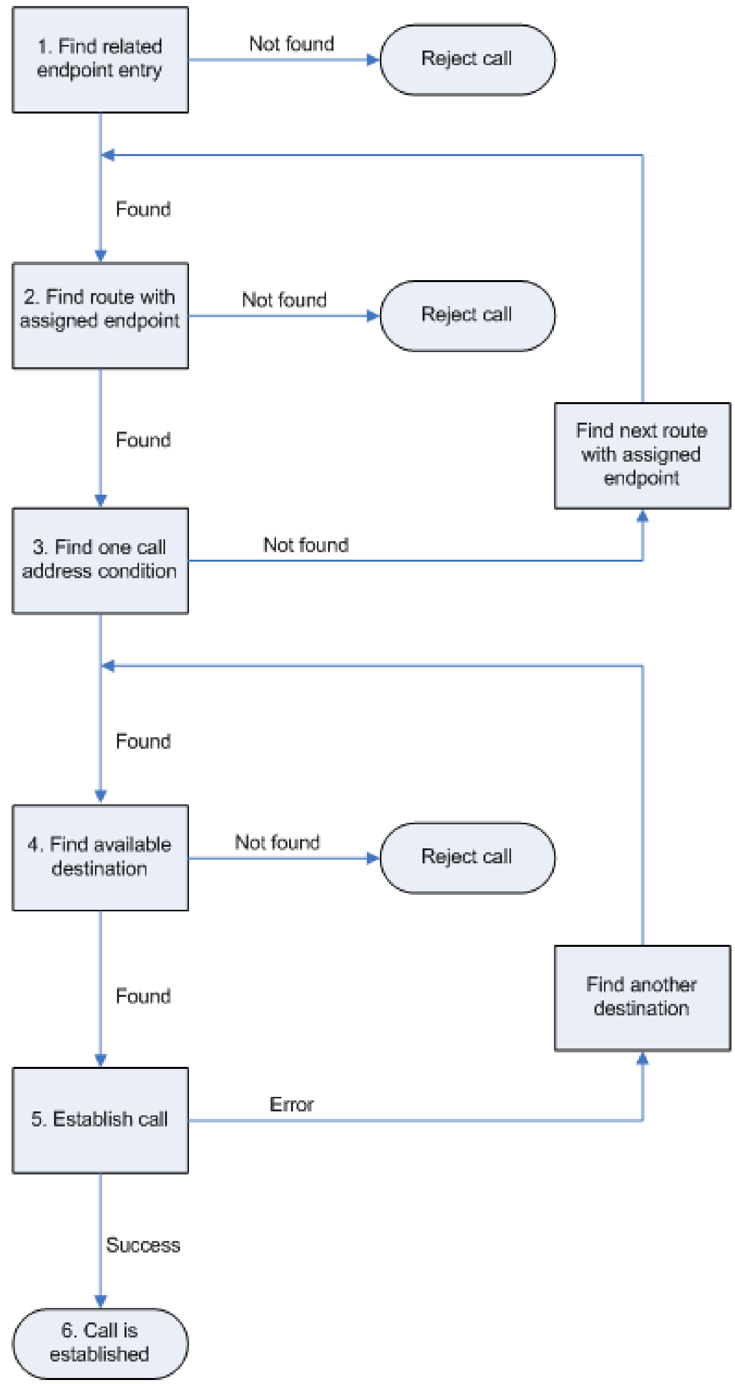
2. Go sequentially through the list of routes and find the first route that has this endpoint defined in its configured sources list.

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 failures, 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, so be careful when placing default routes at the beginning. 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 USA, 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*** on page 62
- ***Connect two SIP peers to two PSTN interface exclusively*** see "Connect two SIP peers to two PSTN interfaces exclusively" on page 62
- ***Connect two SIP peers to the same PSTN interface*** on page 63
- ***Load-balancing or failover between two SIP peers*** see "Load balancing or failover between two SIP peers" on page 63

Direct routing between one PSTN interface and one SIP peer

If you choose to route all calls from PSTN to the same SIP peer, and calls from that SIP peer to 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

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".

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 entries 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 entries 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.

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.

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 ***Number modification using regular expressions*** on page 68 for a list of common formats.

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.

Address manipulation is done as follows

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.

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.

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*** on page 66
2. ***Number modification using regular expressions*** on page 68

Number normalization based on a Dialplan

The number normalization based on a dialplan can work in an environment in which the Dialogic® 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 ***Dialplan Configuration*** see "Dialplans" on page 44 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, as 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 Dialogic® 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 of 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 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, 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 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 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
N	Indicates a national number type
S	Indicates a subscriber number type
$(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 nth 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

The leading prefix "33" should be removed from the number 33-444-5555 and thus be converted into 444-5555.

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

Expression entry: ^33

Format entry: (none)

Add the prefix digits

The number 444-5555 needs the leading prefix "9" and should be dialed as 9-444-5555.

Expression entry: .*

Format entry: 9$&

Replace an international number type by prefix

A call indicated as an international call should be placed with prefixes instead.

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

Expression entry: ^\+

Format: 01

Replace the international dial prefix by number type

A call with an international dial prefix should be placed with an international number type instead.

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

Calls for specific extensions should be indicated with other extensions, e.g., the extension 1111 should be replaced by 2222, and extension 3333 by extension 4444.

Note: In calls from PSTN to SIP, the dialed SIP peer remains the same although the number is replaced.

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 on calls from 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

Software Uninstallation

The Dialogic® Diva® SIPcontrol™ software is uninstalled automatically when the Dialogic® Diva® for Linux software package is uninstalled.

Cause Code Mapping

The Dialogic® 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 Configuration*** see "Cause Code Maps" on page 49.

For ISDN to SIP code mappings, see ***ISDN cause code to SIP response code*** on page 73.

For SIP to ISDN code mappings, see ***SIP response code to ISDN cause code*** on page 75.

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

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	500	Server internal error
127	Interworking, unspecified	500	Server internal error
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
480	Temporarily unavailable	19	No answer from 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
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
606	Not acceptable	65	Bearer capability not implemented
Any code other than listed above:		31	Normal, unspecified

Event Logging

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

- ***Errors*** on page 77
- ***Warnings*** on page 78
- ***Informational Messages*** on page 79

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 the following table 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 a text that explains why the service could not start.
2001	Service could not stop. <Reason>	The <Reason> is a 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 alternative destination without TLS encryption is available.

Warnings

A warning is an event that is not necessarily significant. But it might 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 the Dialogic® Diva® SIPcontrol™ Software 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.
3005	SIP peer <Host Name> is available again	An inactive SIP peer 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 supported by and allowed for the SIP peer could be used for the call and no alternative targets were available.
3007	Cannot 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 occuring during TLS data processing. The trace may give additional information.

Informational messages

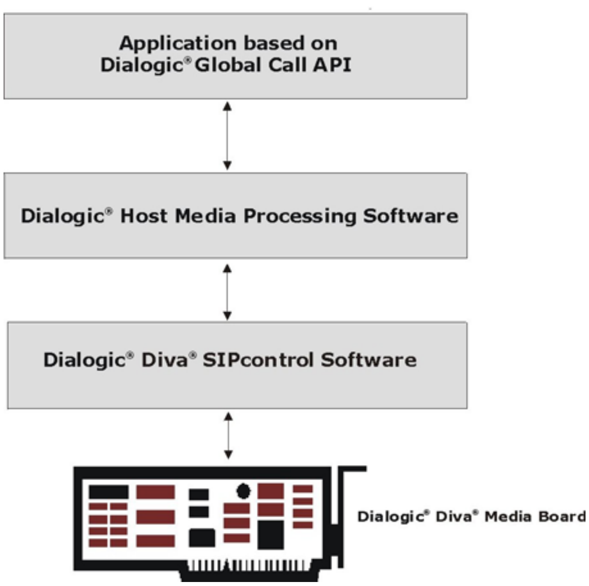
Informational messages refer to successful operation events such as starting or stopping the service:

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.

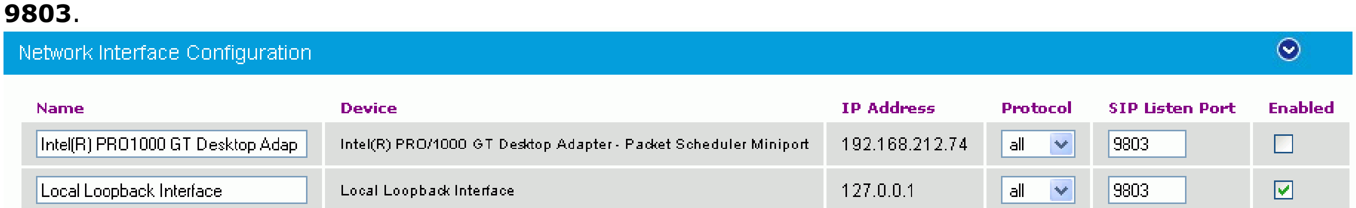
Use Case for Dialogic® HMP software

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 Diva SIPcontrol software version 1.8 and 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.

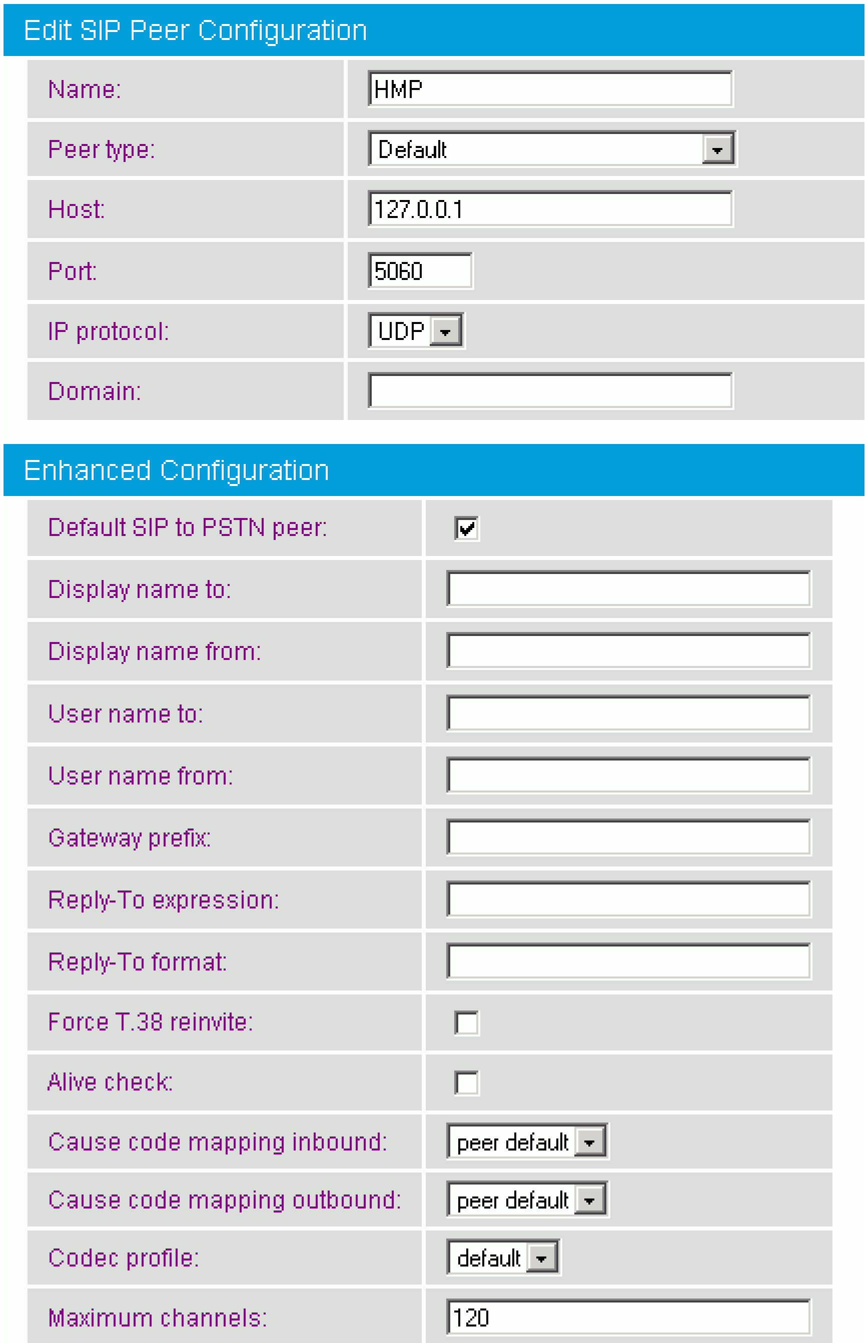


To configure the Diva SIPcontrol software to function with your Global Call application:

1. Open the 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 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:



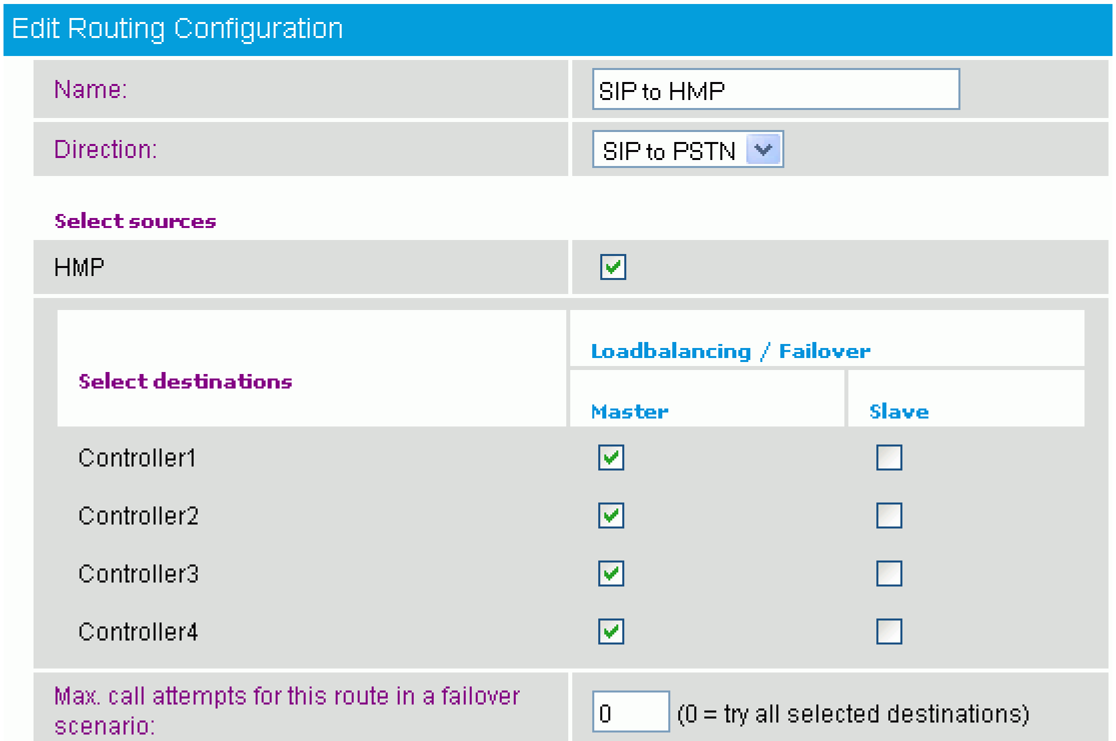
Under **Edit SIP Peer Configuration**, configure the following parameters:

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

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

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

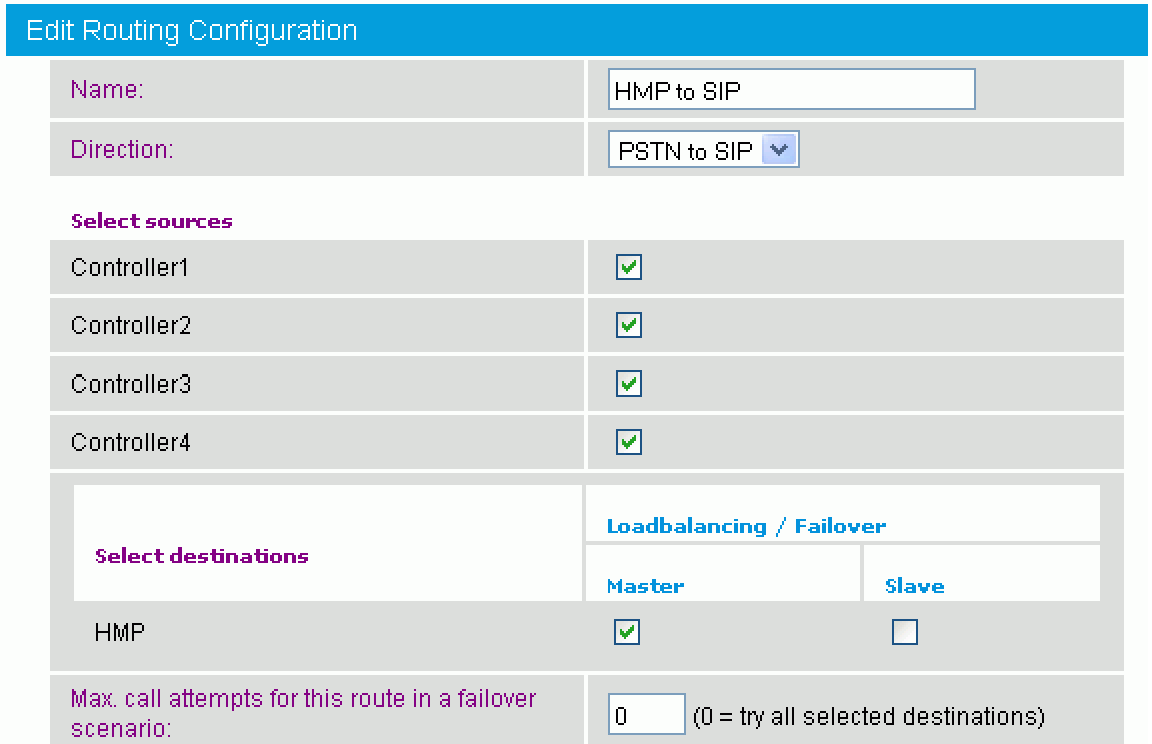
5. Create two routings, one for each direction (SIP to PSTN and PSTN to SIP). To configure the routing from SIP to PSTN, open the **Routing Configuration**, click **Add**, and configure the following parameters:



- **Name**: Enter a unique name to easily identify the routing.
- **Direction**: Select **SIP to PSTN** from the drop down menu.
- **Select sources**: Select the above configured SIP peer as source.
- **Select destinations**: Select the controllers of the Dialogic® 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 drop down 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.

Index

S

T

U