



Dialogic[®] 4000 Media Gateway Series

Reference Guide

Copyright and Legal Notice

Copyright © 2008-2011 Dialogic Inc. All Rights Reserved. You may not reproduce this document in whole or in part without permission in writing from Dialogic Inc. at the address provided below.

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

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

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

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

It is possible that the use or implementation of any one of the concepts, applications, or ideas described in this document, in marketing collateral produced by or on web pages maintained by Dialogic may infringe one or more patents or other intellectual property rights owned by third parties. Dialogic does not provide any intellectual property licenses with the sale of Dialogic products other than a license to use such product in accordance with intellectual property owned or validly licensed by Dialogic and no such licenses are provided except pursuant to a signed agreement with Dialogic. More detailed information about such intellectual property is available from Dialogic's legal department at 926 Rock Avenue, San Jose, California 95131 USA. Dialogic encourages all users of its products to procure all necessary intellectual property licenses required to implement any concepts or applications and does not condone or encourage any intellectual property infringement and disclaims any responsibility related thereto. These intellectual property licenses may differ from country to country and it is the responsibility of those who develop the concepts or applications to be aware of and comply with different national license requirements.

Dialogic, Dialogic Pro, Dialogic Blue, Veraz, Brooktrout, Diva, Diva ISDN, Making Innovation Thrive, Video is the New Voice, Diastar, Cantata, TruFax, SwitchKit, SnowShore, Eicon, Eicon Networks, NMS Communications, NMS (stylized), Eiconcard, SIPcontrol, TrustedVideo, Exnet, EXS, Connecting to Growth, Fusion, Vision, PowerMedia, PacketMedia, BorderNet, inCloud9, I-Gate, Hi-Gate, NaturalAccess, NaturalCallControl, NaturalConference, NaturalFax and Shiva, among others as well as related logos, are either registered trademarks or trademarks of Dialogic Inc. and its affiliates or subsidiaries. Dialogic's trademarks may be used publicly only with permission from Dialogic. Such permission may only be granted by Dialogic's legal department at 926 Rock Avenue, San Jose, California 95131 USA. Any authorized use of Dialogic's trademarks will be subject to full respect of the trademark guidelines published by Dialogic from time to time and any use of Dialogic's trademarks requires proper acknowledgement.

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

Any use case(s) shown and/or described herein represent one or more examples of the various ways, scenarios or environments in which Dialogic® products can be used. Such use case(s) are non-limiting and do not represent recommendations of Dialogic as to whether or how to use Dialogic products.

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.

Contents

Copyright and Legal Notice	2
About This Manual	5
Dialogic® 4000 Media Gateway Features	7
Dialogic® Diva® SIPcontrol™ software features	7
Dialogic® Diva® Media Board features	10
PBX Interoperability	11
Initial Configuration and License Activation.....	13
Initial Log On	13
Preparing for Configuration	13
License Activation	13
Important Note	15
Dialogic® Diva® Media Board Configuration	17
Dialogic® Diva® Media Board Configuration via the Dialogic® Diva® Web Interface	17
Supported Switch Types and Supported PBXs	21
Dialogic® Diva® SIPcontrol™ Configuration	25
About Diva SIPControl Configuration	25
Configuring Dialogic® Diva® SIPcontrol™	27
Saving Configuration Settings	29
Deleting a Configuration Profile	30
PSTN Interfaces	30
Network Interfaces	34
SIP Peers	35
Routing	41
Security Profiles	44
Setting up a Security Profile	45
LDAP	47
Dialplans	51
Address Maps	53
Cause Code Maps	57
Codec Profiles	58
Registrations	59
Logging and Diagnostics	60
Data Security Overview.....	61
Secure HTTP	61
TLS	61
Secure RTP	61
Certificates	62
How Calls Are Processed.....	67
Information about Call Processing	68
Emergency Calls	69
Routing Conditions	69
Routing Examples	69

How Address Maps Are Processed	73
How Call Addresses Are Processed	75
Possible Scenarios	75
How Addresses Are Manipulated	75
How Numbers Are Processed	77
Number Normalization Based on a Dialplan	77
Number Modification Using Regular Expressions	78
Examples	79
Cause Code Mapping	81
Default Cause Code Mapping	81
Default Cause Code Mapping for Microsoft® Office Communications Server 2007 and Lync Server 2010 Peers	83
Software Uninstallation	87
Event Logging	89
Use Case Examples	93
Use Case for Dialogic® HMP Software	93
Use Case for Microsoft® Exchange Server 2007	96
Use Cases for Microsoft® Office Communications Server 2007	99
Using the Gateway Computer Between the PSTN and Microsoft® Lync™ Server 2010	130
SNMP Support For A Dialogic® Diva® Media Board	149
To activate SNMP support for a Dialogic® Diva® Media Board	149
Supported MIBs, OIDs, and traps	153
Verify The Line Configuration With The Dialogic® Diva® Line Test Tool.	157
Line Check	157
Hardware test	158
Phone/Loop test	158
Call Transfer	160
Fax test	161
Create a Trace With The Dialogic® Diva® Diagnostics Tool.....	163
Backing up and Restoring the Configuration	165
Customer Service	167

CHAPTER 1

About This Manual

The Dialogic® 4000 Media Gateway Series are pre-installed with the Windows® versions of the Dialogic® Diva® System Release software and the Dialogic® Diva® SIPcontrol™ software. This reference guide contains relevant information about both software versions, such as Diva SIPcontrol configuration parameters, the Dialogic® Diva® Diagnostics tool, the Dialogic® Diva® Line Test tool, and the SNMP configuration for Dialogic® Diva® Media Boards. Various configuration scenarios are also included, as well as information about the different support options.

The term "Dialogic® 4000 Media Gateways" is used herein to refer collectively to the Dialogic® 4000 Media Gateway Series, and the term "Dialogic® 4000 Media Gateway" is used herein to refer a gateway in the Dialogic® 4000 Media Gateway Series.

For a list of Dialogic® Diva® SIPcontrol™ software features, see [Dialogic® Diva® SIPcontrol™ software features](#) on page 7.

For a list of Dialogic® Diva® Media Board features, see [Dialogic® Diva® Media Board features](#) on page 10.

CHAPTER 2

Dialogic® 4000 Media Gateway Features

This chapter describes the DMG4000 Gateway software features and Diva Media Board features.

Dialogic® Diva® SIPcontrol™ software features

General Features

- Support for Microsoft® Lync™ Server 2010
- Noise suppression support
- Echo cancellation selectable via GUI
- Forward the display name from SIP to Q.SIG and vice versa
- Interoperability with Dialogic® Host Media Processing (HMP) software 3.0WIN and 3.1LIN
- Configuration via the Diva SIPcontrol web interface
- Standard web browsers can be used for configuring. Diva SIPcontrol has been tested with the following browsers:
 - Microsoft® Internet Explorer® version 7 and 8
 - Mozilla Firefox version 3.6.x
- Remote configuration of Diva SIPcontrol from any computer in the network. The configuration may be encrypted.
- Cause codes: Configurable translation of ISDN cause code to SIP response code and vice versa; consequently, Diva SIPcontrol can adapt to the specific behavior of the PSTN, PBX, and/or SIP peer.
- Configuration changes during runtime: Modify most parameters of Diva SIPcontrol without the need to restart the service; active calls are not affected by configuration updates and continue undisturbed.
- Support for North American numbering plan: The configuration of multiple area codes is handled as local. Therefore, the Diva SIPcontrol dialplan engine is able to automatically format dialed numbers according to local phone provider requirements without any additional regular expressions.
- Codec configuration: Configuration options for supported audio codecs. See [Media Processing](#) on page 8 for supported codecs.
- Support for Proxy and Registrar authentication.
- Support for early media. Early media is supported to and from the PSTN due to Any-to-Any routing, if the line protocol supports it. A call using early media does not need to have a SIP leg.
- Configuration of Diva Media Board parameters via the Diva web interface
- Support for up to 64 ports per system for Dialogic® Diva® BRI and Analog Media Board installations
- Support for up to 240 ports per system for Dialogic® Diva® PRI Media Board installations

Call Handling

- SIP methods: ACK, BYE, INVITE, NOTIFY, REFER, CANCEL, OPTIONS, PRACK
- Configurable IP transport layer TCP, UDP, or TLS
- Support for TLS encryption and authentication
- Support for SRTP (secure Real-time Transport Protocol)
- Support for SIPS (Secure SIP)

- Basic call incl. numbering services:
 - Called Party Number
 - Calling Party Number
 - Redirecting Number
- Call Routing
- Call Hold/Retrieve (e.g., Re-Invite mapping towards ISDN)
- SIP-side Call Transfer as transfer target (C-party) and as transferee (A-party)
- PSTN-side incoming Call Diversion
- Support for SIP 302 REDIRECT, which works as follows: a SIP call is redirected per 302 Redirect with new IP port numbers (as used with Microsoft® Office Communications Server 2007, Microsoft® Office Communications Server 2007 R2, and Microsoft® Exchange Server 2007 without changing the IP address)
- Support for SIP Refer: a SIP call is redirected per SIP Refer to a new SIP target, using Replaces and Referred By
- SIP Session Timer (RFC 4028)
- Simplified Number Normalization based on PSTN connection parameters
- Number Manipulation using Regular Expressions

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**
 - sRTP
- RTP dynamic payload audio/telephony event
- RTP profile RTP/AVP
- DTMF via RTP payload/telephony event (RFC 2833 or RFC 4733)
- PSTN-side fax tone detection via RTP event (RFC 2833 or RFC 4733)
- 128 ms Echo Canceller supported on all boards, and additionally, 256 ms EC supported on those boards listed in MultiPRI boards section.

*For G.729, you need to purchase and activate a license before you can use it. For more information, see the *Dialogic® 4000 Media Gateway Series Quickstart Guide*, which is available at <http://www.dialogic.com/manuals/dmg30004000>. G.729 is only available on Dialogic® Diva® Multiport V-PRI Media Boards.

**iLBC is only available on Diva Multiport V-PRI Media Boards. On Dialogic® Diva® V-4PRI/E1/T1-120 PCIe HS boards and Dialogic® Diva® V-8PRI/E1/T1-240 PCIe FS boards, up to 18 channels for each PRI port are supported.

Reliability

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

Supported RFCs

- RFC 2617 - HTTP Digest Authentication
- RFC 2833 - RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals
- RFC 3261 - Session Initiation Protocol
- RFC 3262 - Reliability of Provisional Responses in Session Initiation Protocol (SIP)
- RFC 3264 - An Offer/Answer Model with Session Description Protocol
- RFC 3265 - SIP-specific Event Notification
- RFC 3326 - The Reason Header Field for the Session Initiation Protocol (SIP)
- RFC 3389 - RTP Payload for Comfort Noise
- RFC 3398 - ISDN to SIP mapping
- RFC 3420 - Internet Media Type message/sipfrag
- RFC 3515 - REFER method
- RFC 3550 - Realtime Transport Protocol (RTP)
- RFC 3551 - RTP/AVP profile
- RFC 3711 - The Secure Real-time Transport Protocol (SRTP)
- RFC 3891 - SIP "Replaces" header
- RFC 3892 - SIP Referred - By Mechanism
- RFC 3951 - Internet Low Bit Rate Codec (iLBC)
- RFC 3952 - Real-time Transport Protocol (RTP) Payload Format for internet Low Bit Rate Codec (iLBC) Speech
- RFC 3960 - Early Media and Ringing Tone Generation in the Session Initiation Protocol (SIP), only gateway model
- RFC 4028 - Session Timers in SIP
- RFC 4497 - Interworking between SIP and QSIG
- RFC 4566 - Session Description Protocol (SDP)
- RFC 4568 - SDP Security for Media Streams
- RFC 4733 - RTP Payload for DTMF Digits, Telephony Tones, and Telephony Signals
- Draft: Diversion Indication in SIP (draft-levy-sip-diversion-08)

Enhanced Routing

- Support for Any-to-Any routing (SIP to PSTN, PSTN to SIP, SIP to SIP, PSTN to PSTN)
- 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
- Routing based on Active Directory information

Enhanced Address Manipulation

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

Dialogic® Diva® Media Board features

This list includes only features relevant for the Dialogic® 4000 Media Gateways. If you are interested in the complete list of features, consult the *Dialogic® Diva® System Release Reference Guide*, which is available at: www.dialogic.com/manuals.

General features

- Support for the ISDN basic rate interface (BRI), the ISDN primary rate interface (PRI), the channelized E1 interface, and the channelized T1 interface
- Support for fractional PRI, E1, and T1 lines
- Support for multiple PRI, E1, and T1 lines
- Automatic Diva Media Board detection
- Support for ISDN lines with a transfer rate of 64 kbps or 56 kbps (for example some regions in the USA)
- Support for channelized T1 lines with a transfer rate of 56 kbps (see [Channelized T1 \(robbed bit signaling\)](#) on page 11)
- Support for unchannelized lines with a transfer rate of 64 kbps or 56 kbps
- Support for R2 signaling E1 lines with a transfer rate of 64 kbps
- Support for up to 120 B-channels
- Support for all known switch types (ISDN protocols)
- Support for Q.SIG protocol (see [Q.SIG features](#) on page 11)
- Additional security through support of RSA
- Dialogic® Diva® V-PRI Multipoint Media Boards: Creation of a trace message in the trace file if maximum operation temperature is exceeded.
- Support for collecting phone number ranges or a specific number on incoming calls by the software.
- Support for a wide range of Windows® event logs. Driver and connection errors and informative messages are listed in the MOM (Microsoft® Operation Manager). For a detailed description of the errors and messages see the Dialogic® Diva® Configuration Manager Online Help file (DSMain.chm).
- Support for call deflection or call rerouting
- Support for redirecting number emulation (for incoming calls). In this case, the called party number is delivered as redirecting number to the application.
- ECT Link Balance: To avoid confusion with call transfer and multiple incoming calls, each incoming call is delivered to a separate TEI. This feature is only valid for Dialogic® Diva® BRI Media Boards and Point-to-Multipoint interfaces.
- Call Rate Limiter: Limitation of the amount of outgoing calls per second. Some switches may require limitation of calls in order to grant stability of the PSTN network.
- Support for DTMF transmission, DTMF detection, DTMF clamping

DSP-based features

- Real time protocol (RTP)
- Dynamic anti-jitter buffering
- Comfort noise generation (CNG)
- Voice activity detection (VAD)
- Support for 256 ms echo cancellation on all channels in parallel on Diva V-PRI Multipoint Media Boards

Q.SIG features

- Support for generic Q.SIG according to ECMA and ISO (For more information, see "Supplementary services" in the *Dialogic® Diva® System Release Reference Guide*, which is available at: www.dialogic.com/manuals.)
- Tests have been conducted for the various switch types (for a complete list of all supported types see "Supplementary services" in the *Dialogic® Diva® System Release Reference Guide*, which is available at: www.dialogic.com/manuals.)

Channelized T1 (robbed bit signaling)

- Trunk modes (loop, ground, and wink start)
- Tone dialing (DTMF and MF)
- Pulse dialing
- Ringer and busy tone detection
- 56 kbps transfer rate
- Call transfer

PBX Interoperability

Dialogic® 4000 Media Gateways are designed and tested for PBX interoperability with the installed base of enterprise communications systems. They are also tested and approved for use with Microsoft® Unified Communications. The general use configuration guides and PBX interoperability matrix at http://www.dialogic.com/microsoftuc/pbx_integration.htm provide guidance and configuration information for many different PBX vendors and models.

CHAPTER 3

Initial Configuration and License Activation

Initial Log On

The initial configuration allows the unit to be configured using a remote desktop connection.

The Dialogic® 4000 Media Gateway Series is initially configured with:

- Ethernet port 1: with fixed IP address 192.168.1.1
- Ethernet port 2: with fixed IP address 192.168.2.1
- Ethernet port 3 and 4: enabled with DHCP, only available on older DMG4000 models

Note: The above numbering of the Ethernet ports refers to the numbering at the rear panel of the Media Gateway and not to the numbering displayed in the Control Panel of your operating system.

- User name: Administrator
- Password: Dialogic (Change the password after the initial log on.)

Preparing for Configuration

Before you start to configure your Dialogic® Media Gateway, it is necessary to gather some information about the environment in which it will be used.

Collect the following information:

1. In case the gateway is to be connected to a PBX: Which vendor and which PBX type will be used?
2. What protocol will be used on the PSTN/PBX side of the gateway? Examples are EuroISDN (ETSI-DSS1), Q-SIG, and DMS100.

License Activation

The SIP Control license and V.34 fax license for the default amount of SIP and T.38 fax channels (model-based) are already installed and activated upon shipment. You must purchase and activate additional licenses, if you need additional channels for Diva SIPcontrol, G.729 speech compression, or T.38 fax.

During the activation process of the license, you need to choose a Diva Media Board to which the license should be bound. After having activated the license for this Diva board, the license cannot be transferred to be used with another Diva board.

Notes:

- Diva SIPcontrol licenses need to be activated via the Diva SIPcontrol web interface, as described under [To Activate the License File](#) on page 15.
- Licenses for G.729 need to be uploaded and activated in the Dialogic® Diva® Configuration Manager. See the Dialogic® Diva® Configuration Manager Online Help for more information.
- The Dialogic® Host Media Processing (HMP) Software licenses for SIP channels are also valid for SIPcontrol, but they require the Dialogic HMP software to be installed on the same system as Diva SIPcontrol.

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

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

- [Device Unique ID \(DUID\)](#)
- [Proof of Purchase Code \(PPC\)](#)

Once you have both, the DUID and PPC, visit the Dialogic® Diva® Activation site to register your PPC together with the DUID, and you will receive your license file. Activate this license file in the Diva SIPcontrol web interface. For more information, see [To Activate the License File](#) on page 15.

Device Unique ID (DUID)

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

To obtain the DUID:

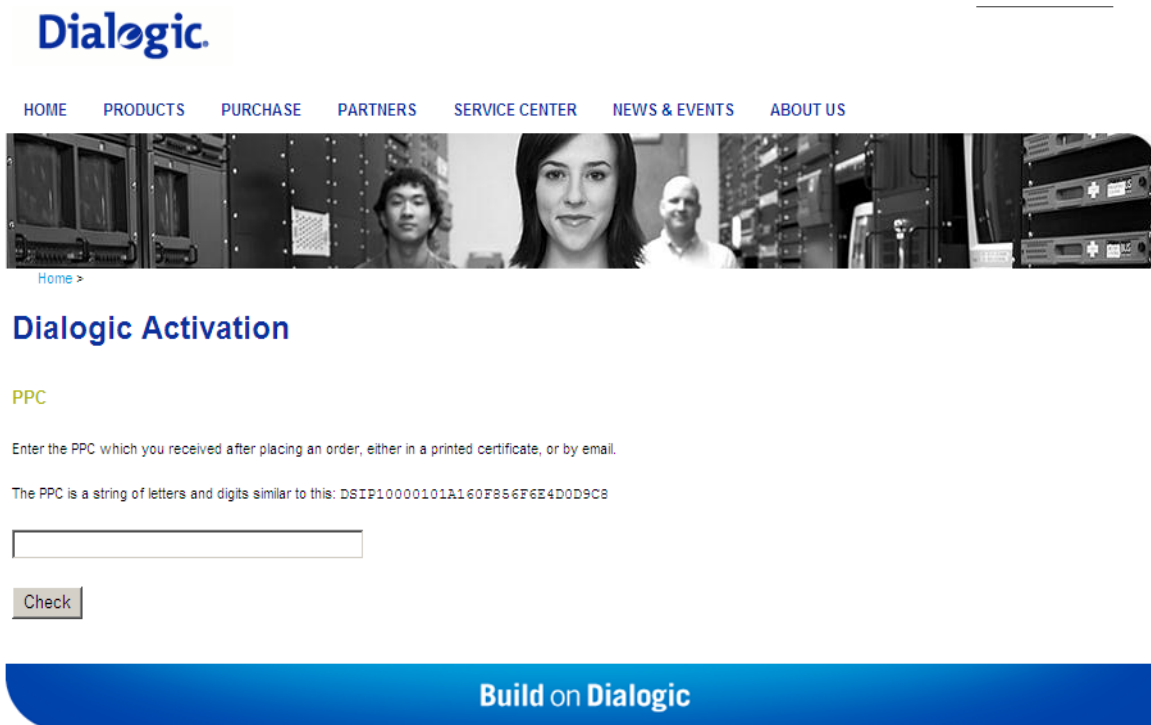
1. Click **Start > Programs > Dialogic Diva > SIPcontrol Configuration** to open the Diva SIPcontrol web interface.
2. Click **License Management** on the left side of the Diva SIPcontrol web interface to open the **License Status** dialog.
3. In the **License Status** dialog, copy the DUID number of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

Proof of Purchase Code (PPC)

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

To Register Your PPC and DUID

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



Dialogic

HOME PRODUCTS PURCHASE PARTNERS SERVICE CENTER NEWS & EVENTS ABOUT US

Home >

Dialogic Activation

PPC

Enter the PPC which you received after placing an order, either in a printed certificate, or by email.

The PPC is a string of letters and digits similar to this: DSIP10000101A160F856F6E4D0D9C8

Check

Build on Dialogic

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

Dialogic
Making Innovation Visible

HOME PRODUCTS PURCHASE PARTNERS SERVICES & SUPPORT NEWS & EVENTS ABOUT US

Dialogic Diva Activation

PPC

Qty	Code	Name
2	DM2-040	30-day Demo, Max 1.38, per channel

DUID

The DUID displayed on the Activation page of the Diva Server configuration utility is required to complete the registration process.

The DUID is a number like one of these: K123456789, S1234567890, N123456788, 09-1234567 or 9-1234567

Email Address

The email address that you enter here will be used for delivery of your license file.

Comment

You can enter a comment here which may appear in the license file.

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

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

To Activate the License File

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

1. Click **License Management** on the left side of the Diva SIPcontrol 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.

Important Note

The Dialogic® 4000 Media Gateway SBA is shipped with automatic updates disabled. Customers are strongly advised to double-check their deployment and ensure that the domain WSUS service is properly configured NOT to install Windows Service Packs on the SBA device. Applicable Microsoft Service Packs are scheduled to be included as part of future Dialogic® 4000 Media Gateway updates.

For example, if automatic updates are turned on, and Windows 2008 R2 Service Pack 1 is applied to a Dialogic® 4000 Media Gateway that is being used as an SBA, a boot failure can occur. This type of failure will require intervention by the administrator to restore the unit's operation. For more information, see <http://www.dialogic.com/support/helpweb/mg/iw2756.aspx>.

CHAPTER 4

Dialogic® Diva® Media Board Configuration

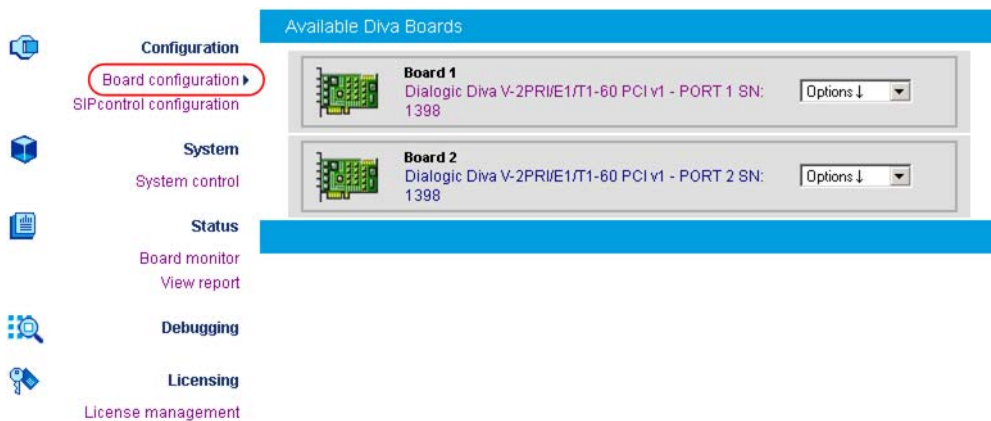
Since Diva SIPcontrol version 1.8, Diva Media Boards can be configured via the Diva web interface. The configuration via the Diva web interface can be accessed and updated remotely. The classic configuration via the Dialogic® Diva® Configuration Manager is also available, but it can only be accessed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

You can find information about the Diva web interface in [Dialogic® Diva® SIPcontrol™ Configuration](#) on page 25 and [Configuration Tips and Hints](#) on page 26.

Dialogic® Diva® Media Board Configuration via the Dialogic® Diva® Web Interface

To configure Diva media boards via the Diva web interface, follow these steps:

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



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

Dialogic Diva V-2PRI/E1/T1-60 PCI v1 - PORT 1, SN: 1398

Parameter	Value
D-Channel Protocol:	Europe/other countries, Euro-ISDN (ETSI-DSS1) - (ETSI)
Interface Mode/Resource Board:	TE - mode
Direct Dial In (NT2):	Yes
DDI Number Length:	3
DDI Collect Timeout:	0
DDI Special Number:	
Layer 1 Framing:	National default (default)
Layer 2 Connect Mode:	Permanent
Voice Companding:	Protocol default
View Extended Configuration	No

Save Cancel

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

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

Extended Parameter	Value
TEI Value:	0 (standard)
Source Of Local Tones (BUSY, ALERTING, ...):	Tones provided by ISDN equipment (default)
Trunk Operation Mode:	Standard (default)
Fraction Starts At Channel:	1
ETSI Call Transfer:	Default
Deflection Mode:	Deflection (default)
ETSI Message Waiting:	Default
Extended Voice Processing	
DTMF Clamping:	Off
Audio Recording Automatic Gain Control (AGC):	Off
Echo Canceller Tail Length:	128 ms (default)
Suppression of ambient noise:	Off
Part 68 Voice Signal Limiter:	Protocol default
Redirecting Number Emulation:	Disabled (default)

- For more detailed information, click the parameter, and a window with the help text will appear.

The Board Monitor

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

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

Dialogic Diva V-2PRI/E1/T1-60 PCI v1 - PORT 1, SN:1398				
Type	Name	Value	Operation	
DIR	.		Refresh	
UINT	CardType	79		
HINT	MIF Version	0x00000117		
ASCIIZ	Build	TE_DMLT, Build 110-6, F		
UINT	Events Down	0		
DIR	Info		Read	
DIR	Config		Read	
DIR	Statistics		Read	
DIR	State		Read	
DIR	StateT		Read	
DIR	Trace		Read	
DIR	Test		Read	
DIR	Debug		Read	

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

The View Report Option

If you click **View report**, the state and the cumulative statistics for the active Diva Media Boards appear:

Configuration Board configuration SIP control configuration SBA configuration System System control Status Board monitor View report ▶ Licensing License management	Call Statistics							
	No	Board Name	SN	Layer 1 Layer 2	Connected Calls (IN/OUT)	Abandoned Calls (IN/OUT)	Failed Calls (IN/OUT)	Details
	All Boards Summary				0 (0/0)	0 (0/0)	0 (0/0)	
	1	Dialogic Diva V-2PRI/E1/T1-60 PCI v1 - PORT 1	1033	Activated Idle	0 (0/0)	0 (0/0)	0 (0/0)	
	2	Dialogic Diva V-2PRI/E1/T1-60 PCI v1 - PORT 2	1033-1	Activated Idle	0 (0/0)	0 (0/0)	0 (0/0)	

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

Board:1 Dialogic Diva V-2PRI/E1/T1-60 PCI v1 - PORT 1 SN: 1398 >>	
Build	
Version	TE_DMLT, Build 110-11, Protocol 6.03(V23) 110-1 [F#03FF]
Layer 1	
State	Activated
Red Alarm	
State	NO
Yellow Alarm	
State	NO
Blue Alarm	
State	NO
Layer 2	
State	Layer2 UP
Outgoing Calls	
Calls	0
Connected	0
Incoming Calls	
Calls	0
Connected	0
D-Layer1	
X-Frames	19855
X-Bytes	79423
X-Errors	0

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

Supported Switch Types and Supported PBXs

Supported Switch Types

Diva Media Boards currently support the following switch types:

Public Line ISDN Protocols

EMEA PRI and BRI

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

Line Side E.1

- Australian P2
- Ericsson
- Melcas
- NEC
- Nortel

R2 CAS (E.1 only)

- Argentina
- Brazil
- China
- India
- Indonesia

- Korea
- Mexico
- Philippines
- Thailand
- Venezuela

USA PRI and BRI

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

USA T.1 / PRI

- 4ESS
- T.1 RBS

Carrier Grade

ITU-T ISUP SS7

POTS

Worldwide POTS

PBX Protocols

- Generic QSIG T.1 and E.1

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

- ETSI

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

Specific Major PBX Types

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

- Siemens Hipath 3000
- Siemens Hipath 4000
- Tenovis QSig

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

CHAPTER 5

Dialogic® Diva® SIPcontrol™ Configuration

This chapter describes how to configure Diva SIPcontrol. It provides configuration tips and hints, includes general information about each configuration, and gives an overview of the configurable Diva SIPcontrol parameters. The configuration of the Diva Media Boards is described in [Dialogic® Diva® Media Board Configuration](#) on page 17.

About Diva SIPControl Configuration

Diva SIPcontrol is configured via the Diva SIPcontrol web interface.

Opening the Dialogic® Diva® SIPcontrol™ Web Interface

To open the Diva SIPcontrol web interface, follow these steps:

1. Click **Start > Programs > Dialogic Diva > SIPcontrol Configuration**. By default, access to the web interface is only allowed from localhost (127.0.0.1), and 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:
 - Click **System control** on the left side of the web interface.

The System control window appears:

- In the **Password** section, enter the current and new passwords, and then retype the new password. A password must be seven digits or longer, and the use of non-alphanumeric characters for a password is discouraged.
- Click **Change Password**.

If necessary, open the port in the local firewall settings. To do this under Windows® Vista, Windows® 7, Windows Server® 2008, or Windows 2008® R2, open the command prompt with elevated rights.

Enter the following command on a 64-bit operating system:

```
netsh advfirewall firewall add rule name="Diva Webserver" dir=in
action=allow program="%ProgramFiles%\
Diva Server\DivaWebConfig.exe" protocol=tcp
```

Enter the following command on a 32-bit operating system:

```
netsh advfirewall firewall add rule name="Diva Webserver" dir=in
action=allow program="%ProgramFiles%\
Diva Server\DivaWebConfig.exe" protocol=tcp
```

You can now access the Diva SIPcontrol web interface on any of the IP addresses of the computer where SIPcontrol is installed, and then you can configure the settings according to your needs.

Dialogic® Diva® SIPcontrol™ Configuration Sections

Diva SIPcontrol configuration is divided into the following sections:

- [PSTN Interfaces](#), as described on page 30
- [Network Interfaces](#), as described on page 34
- [SIP Peers](#), as described on page 35
- [Routing](#), as described on page 41
- [Security Profiles](#), as described on page 44
- [LDAP](#), as described on page 47
- [Dialplans](#), as described on page 51
- [Address Maps](#) on page 53
- [Cause Code Maps](#), as described on page 57
- [Codec Profiles](#), as described on page 58
- [Registrations](#), as described on page 59
- [Logging and Diagnostics](#), as described on page 60

Configuration Tips and Hints

This section contains useful information about SIPcontrol configuration:

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

Note: The restart will terminate active connections.

- The names for specific configuration elements are limited to 32 alphanumeric characters and must not be repeated, i.e., you cannot assign the same name for two SIP peers.
- The configuration session times out after 30 minutes of inactivity and a new login is required to access the session again. If the new login screen appears when you try to save the configuration, login again and click the "Back" button of the browser. The configuration session opens with the settings before the time out and you can save the configuration.
- To restart the Dialogic® Diva® WebConfig service, in the SIPcontrol web interface, click **System control** on the left hand side, and then click **Restart** in the **System status management** section.
- Diva SIPcontrol provides a secure configuration via the web interface (HTTPS). The default port for HTTPS is 10006. Diva SIPcontrol provides a default certificate, but for security reasons you can install your own webserver certificates. To install a webserver certificate and corresponding key file, upload and install these files in the **Webserver certificate management** section under **System Control**.
- To use TLS for SIP calls, you need to upload the certificates as described under [Security Profiles](#) on page 44 and enable the TLS port as described under [Network Interfaces](#) on page 34.
- To open the online help for a specific parameter, click the parameter, and a window with the help text will appear.

Configuring Dialogic® Diva® SIPcontrol™

At a minimum, a Diva SIPcontrol configuration must contain the following components:

- At least one enabled network interface
- At least one enabled SIP peer
- At least one route for PSTN to SIP calls and another route for SIP to PSTN calls

There are four ways to configure Diva SIPcontrol:

- Use the configuration wizard, as described in [Using the Configuration Wizard](#), below.
- Load an existing configuration profile, as described in [Loading an Existing Configuration Profile](#) on page 28.
- Import an existing configuration file, as described in [Importing an Existing Configuration File](#) on page 28.
- Configure Diva SIPcontrol manually, as described in [Configuring Diva SIPcontrol Manually](#) on page 29.

Using the Configuration Wizard

The easiest way to configure Diva SIPcontrol is to use the Diva SIPcontrol configuration wizard. The wizard provides a step-by-step interface that helps you generate configurations for the following use cases:

- Empty configuration that resets existing Diva SIPcontrol web interface settings
- Simple configuration for a general purpose gateway
- DMG4000 hybrid gateway
- DMG4000 Survivable Branch Appliance

The configuration prompts for the minimum required parameters.

To use the configuration wizard, follow these steps:

1. In the **Overview** section of the Diva SIPcontrol Configuration page, click **Start Configuration Wizard**.
The configuration wizard asks whether you want the wizard to delete all unsaved configuration changes.
2. Click **OK**.
3. Follow the configuration wizard prompts.

Loading an Existing Configuration Profile

Diva SIPcontrol configurations can be saved on the server as a configuration profile. You can load an existing configuration profile to use the saved configuration settings.

To load a configuration profile, follow these steps:

1. From the web interface, click **SIPcontrol configuration**.

The SIPcontrol Configuration page appears.

2. In the **Overview** section of the SIP Configuration page, access the Config.-Profiles field, and select the configuration profile file you want to load:

Overview	
Configuration	Activate Discard Start Configuration Wizard
Config.-Profiles	SBA_Use_Case Load into GUI... Delete... Export to file... Save GUI settings... Browse... Import from file...
PSTN Interfaces	Controller1, Controller2
Network Interfaces	Intel(R) PRO1000 EB Network (TCP/TLS)
Peers	Lync, ATA2201, ATA2202
Routing	Block ATA numbers from PSTN, PSTNtoSIP, Call transfer routing by Lync, To ATA1, To ATA2, Lync-to-PSTN, From ATA
Dialplans	US Dialplan
Address Maps	FromATA.1
Codec Profiles	Lync-Codecs, ATACodecs

3. Click **Load into Gui**.

A confirmation message appears, warning you that current GUI settings will be overwritten.

4. Click **OK** on the message box to complete the load process.
5. Click **Activate Configuration** at the bottom of the SIPcontrol Configuration page to use the loaded configuration.

Importing an Existing Configuration File

Diva SIPcontrol configurations can be exported to a file on the computer running the browser. You can import an exported configuration file to use the saved configuration settings.

To import a configuration file, follow these steps:

1. From the web interface, click **SIPcontrol configuration**.

The SIPcontrol Configuration page appears.

- In the **Overview** section of the SIP Configuration page, access the Config.-Profiles field, click **Browse**, and locate the configuration (.cfg) file you want to import:

Overview	
Configuration	Activate Discard Start Configuration Wizard
Config.-Profiles	SBA_Use_Case Load into GUI... Delete... Export to file... Save GUI settings... C:\Documents and Settings\ Browse... Import from file...
PSTN Interfaces	Controller1, Controller2
Network Interfaces	Intel(R) PRO1000 EB Network (TCP/TLS)
Peers	Lync, ATA2201, ATA2202
Routing	Block ATA numbers from PSTN, PSTNtoSIP, Call transfer routing by Lync, To ATA1, To ATA2, Lync-to-PSTN, From ATA
Dialplans	US Dialplan
Address Maps	FromATA.1
Codec Profiles	Lync-Codecs, ATACodecs

- Click **Import from file**.
A confirmation message appears, warning you that current GUI settings will be overwritten.
- Click **OK** on the message box to complete the import process.
- Click **Activate Configuration** at the bottom of the SIPcontrol Configuration page to use the loaded configuration.

Configuring Diva SIPcontrol Manually

To configure Diva SIPcontrol settings manually:

- From the Diva SIPcontrol web interface, click **SIPcontrol configuration**.
The SIPcontrol Configuration page appears:
- Configure each of the sections on the SIPcontrol Configuration page:
 - To expand a section, click on it.
 - To close a section, click the left arrow at the top right of the section.
 - To save the new settings, click **Activate Configuration** at the bottom of each configuration page.

The portion of this chapter starting with [PSTN Interfaces](#) on page 30 describes the settings in each section of Diva SIPcontrol web interface.

Saving Configuration Settings

Once you configure Diva SIPcontrol as desired, you can save the configuration settings for future use. There are two ways to save the configuration settings:

- Save the settings as a configuration profile on the server.
- Save the settings by exporting them to a file on the computer running the browser.

Saving Configuration Settings as a Configuration Profile

To save the current configuration settings as a configuration profile on the server, follow these steps:

- Configure Diva SIPcontrol by following the instructions in this chapter.
- In the **Overview** section of the SIP Configuration page, access the Config.-Profiles field, and click **Save GUI settings**.

The Explorer User Prompt window appears.

3. Enter a name for the saved profile, and click **OK**.
The profile name now appears in the Config.-Profiles listbox.

Exporting Configuration Settings

To export current configuration settings to the computer running the browser, follow these steps:

1. Configure Diva SIPcontrol by following the instructions in this chapter.
2. In the **Overview** section of the SIP Configuration page, access the Config.-Profiles field, and click **Export to file**.
The File Download window appears, and asks whether you want to open or save the file.
3. Click **Save**.
The Save As window appears.
4. Locate the directory where you want to save the file, enter a file name, and click **Save**. Diva SIPcontrol uses the .cfg extension for exported files.

Deleting a Configuration Profile

To delete a configuration profile, follow these steps:

1. In the **Overview** section of the SIP Configuration page, access the Config.-Profiles field, and select the profile you want to delete.
2. Click **Delete**.
A confirmation message appears.
3. Click **OK** on the confirmation message to delete the selected profile.

PSTN Interfaces

This section describes Diva SIPcontrol's PSTN interface related settings, e.g., which lines are used by Diva SIPcontrol or how call transfer is performed on this line. Line parameters such as the signalling protocols (Q.Sig, ETSI) can be configured on the **Board Configuration** page. For more information, see [Dialogic® Diva® Media Board Configuration](#) on page 17.

At least one PSTN interface must be enabled for Diva SIPcontrol to be able to work. Disabled PSTN interfaces are ignored for both inbound and outbound calls. For each line, you can select a dialplan that you can configure as described in [Dialplans](#) on page 51.

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

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

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

- [General](#), as described on page 31
- [Enhanced](#), as described on page 31
- [Address Normalization](#), as described on page 33

General

You can configure the following parameters in the **General** section when you create or modify a PSTN interface:

General	
Hardware description:	Dialogic Diva PRI/E1/T1-8 PCI v3 SN: 1302
PSTN interface number:	1
Name:	Controller1
Address map inbound:	none
Address map outbound:	none

- Hardware description:** Displays the installed 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 Diva Media Board. The name can be modified in order to display the purpose of the interface or the name of the PBX to which the interface is connected.
- Address map inbound:** Select the name of a regular expression list to be applied on calls received on this interface. See [Address Maps](#) on page 53 for more information about setting up a regular expression list. If you upgraded from Diva SIPcontrol version 1.5 or 1.5.1, an address map is automatically generated here to provide the same number processing behavior in the current Diva SIPcontrol version as in former Diva SIPcontrol versions. If you used regular expressions in Diva SIPcontrol version 1.5.1, they will be included in this address map as well, unless they cannot be converted to the new scheme. In this case, the entry **<Use Windows Registry values>** is available. Diva SIPcontrol will then use the regular expressions defined in the registry keys that were used by Diva SIPcontrol 1.5.1.
- Regular expressions can be used to add or remove dial prefixes required by a PBX or to rewrite public phone numbers with different number ranges into a common format. See the [Examples](#) on page 79 for more information.
- Address map outbound:** Select the name of a regular expression list to be applied on calls sent out by this interface. See [Address Maps](#) on page 53 for more information about setting up a regular expression list. If you upgraded from Diva SIPcontrol version 1.5 or 1.5.1, an address map is automatically generated here to provide the same number processing behavior in the current Diva SIPcontrol version as in former Diva SIPcontrol versions. If you used regular expressions in Diva SIPcontrol version 1.5.1, they will be included in this address map as well, unless they cannot be converted to the new scheme. In this case, the entry **<Use Windows Registry values>** is available. Diva SIPcontrol will then use the regular expressions defined in the registry keys that were used by Diva SIPcontrol 1.5.1.
- Regular expressions can be used to add or remove dial prefixes required by a PBX or to rewrite public phone numbers of different number ranges into a common format. See the [Examples](#) on page 79 for more information.

Enhanced

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

You can configure the following parameters in the **Enhanced** section when you create or modify a PSTN interface:

Enhanced	
Early B3 connect:	auto
Disable progress:	☐
Early B3 default disconnect timeout [s]:	30
Early B3 disconnect timeout [s]: Cause 1: Unallocated number	30
Early B3 disconnect timeout [s]: Cause 2: No route to network	30
Early B3 disconnect timeout [s]: Cause 3: No route to destination	30
Early B3 disconnect timeout [s]: Cause 16: Normal call clearing	30
Early B3 disconnect timeout [s]: Cause 22: Number changed	30
Early B3 disconnect timeout [s]: Cause 28: Invalid number format	30

Early B3 connect:

With this parameter, you can determine if early media should be enabled on this controller (EarlyB3) or whether early media should be enabled even if an "inbound tones available" signal is not received from the PSTN.

The following values determine whether EarlyB3 and EarlyB3ForceMedia are enabled:

Value	EarlyB3	EarlyB3ForceMedia
auto	enabled	not enabled
on	enabled	enabled
off	not enabled	not enabled

The default value is **auto**.

Disable progress

Disables the sending of PROGRESS messages to ISDN if a 183 Session Progress message is received from the SIP peer.

This field is disabled by default.

EarlyB3 default disconnect timeout [s]:

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

The default value is **30** seconds. This value also applies to all causes not listed in the **Enhanced** section.

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

Address Normalization

You can configure the following parameters in the **Address Normalization** section when you create or modify a PSTN interface:

Address Normalization	
Dialplan:	none
Type of number (outbound):	Unchanged
Encoding (outbound):	Use type flag
ISDN numbering plan - Default:	unknown
Presentation indicator - Default:	Allowed
Internal interface:	☐

Dialplan:

Select the local dialplan to be used by the dialplan module of Diva SIPcontrol. The selected dialplan applies only to this controller.

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

Configure the local dialplan as described under [Dialplans](#) on page 51 before you select it here.

Type of number (outbound):	This parameter determines the shortest format allowed in calls sent out by this interface. You can modify this parameter only if you selected a dialplan from the drop down menu. The following options are available: Unchanged: The number type signaled on the received call request or the type previously set via an inbound dialplan or address map will be used unchanged for dialing. International number: The number is always converted to an international number, including country and area code. National number: The number is converted to a national number unless it is an international number with a different country code. Extension: The number is reduced as much as possible. An internal number is reduced to its extension only. For more information about number formats, see How Numbers Are Processed on page 77.
Encoding (outbound):	This parameter determines if numbers in calls sent out by this interface should be encoded as unknown numbers with national or international prefix digits, or as national or international numbers with type flags.
ISDN numbering plan - Default	Change this setting only if the PBX rejects calls from Diva SIPcontrol despite the dialed number being correct. This might occur, for example, if the signaled numbering plan is not supported.
Presentation indicator - Default	If no presentation is specified via address rewriting, this parameter specifies the presentation indicator to set on the calling party number for calls to ISDN. The presentation indicator determines whether the calling party number is shown or hidden from the called user. This default does not apply to PSTN-PSTN calls, unless the known presentation indicator is explicitly removed via an address map.
Internal interface:	This setting controls the usage of the outside access digit by the dialplan in conjunction with this interface. If no outside access digit is configured in the dialplan, this setting has no relevance. Basically, this setting controls whether the outside access digit is expected in the called or calling number depending on the call direction. • If this setting is enabled, the outside access digit is expected in the called number for calls received on this interface and in the calling number for calls sent by this interface. • If this setting is disabled, the outside access digit is expected in the calling number for calls received on this interface and in the called number for calls sent by this interface. In most cases this setting is directly related to the NT/TE mode of the interface. If the interface is in NT mode, this setting usually needs to be enabled. If the interface is in TE mode or an FXO board is used, the setting usually needs to be disabled. If the Internal Interface option is enabled, calls to the connected network will have a calling number with an outside access digit, unless the calling party has an internal number or the number is converted to the number type format instead of a number with a dialing prefix. Also, the dialplan expects that calls from the connected network have a called number with outside access digit, unless the called party has an internal number. This expectation can be disabled in dialplan configuration, if necessary. If the option is disabled, calls to the connected network will have a called number with an outside access digit, unless the called party has an internal number or the number is converted to the number type format instead of a number with dialing prefix. Also, the dialplan expects that calls from the connected network have a calling number with outside access digit, unless the calling party has an internal number. This expectation can be disabled in dialplan configuration, if necessary.

Network Interfaces

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

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

You can configure the following parameters when you define or modify a network interface:

Network Interfaces					
Name	Device	IP address	UDP listen port	TCP listen port	TLS listen port
Intel(R) PRO1000 GT Desktop	Intel(R) PRO1000 GT Desktop Adapter - Packet Scheduler Miniport	192.168.213.38	☐	☐	☐
Local Loopback Interface	Local Loopback Interface	127.0.0.1	☐	☐	☐
RTP start port:	30000				
RTP end port:	39999				

Name	Displays the name of the installed Ethernet adapter. The preset designation can 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 Diva SIPcontrol is installed.
UDP listen port	If you use UDP as the 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 Diva SIPcontrol. Note that you can only enable one network interface.
TCP listen port	If you use TCP as the 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 Diva SIPcontrol. Note that you can 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 can change the port number, but it must not be the same as the TCP Listen Port number. Note that you can only enable one network interface. If you use TLS, you need to upload security certificates and set the cipher level, as described in Security Profiles on page 44.
RTP start port	Defines the lowest port of the range in which Diva SIPcontrol sends and receives RTP streams. Change this value only if problems occur.
RTP end port	Defines the highest port of the range in which Diva SIPcontrol sends and receives RTP streams. Change this value only if problems occur.

SIP Peers

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

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

- [General](#), as described below
- [Enhanced](#), as described on page 37
- [Security](#), as described on page 39
- [Session Timer](#), as described on page 39
- [Address Normalization](#), as described on page 40
- [Authentication](#), as described on page 41

General

You can configure the following parameters in the **General** section when you define or modify a SIP Peer:

General	
Name:	Peer1
Peer type:	Default ▼
Host:	
Port:	5060
IP protocol:	TCP ▼
URI scheme:	SIP (default) ▼
Domain:	

- Name:** Enter a name for the SIP peer. A SIP peer is a specific endpoint to and from which Diva SIPcontrol can establish calls.
- Peer type:** SIPcontrol needs special workarounds to work properly with some SIP peers, such as Microsoft® Exchange Server. 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 to a different format. For more information about name resolution, see the Windows® documentation.
- Port:** Displays the SIP port on which the remote peer is listening. The default is 5060, which is the standard port for SIP.
- IP protocol:** Select the IP protocol to be used for calls to this peer. Calls from this peer are accepted with all protocols and on all ports/addresses configured in [Network Interfaces](#), as described on page 34. If you selected:
- **MS Exchange 2007** or **MS OCS 2007 / 2007 R2 - Mediation Server** as the **Peer type**, set the protocol to **TCP**.
 - **MS Lync 2010 - Mediation Server** as the **Peer type**, set the protocol to **TCP** or **TLS**.
 - **e-phone**, as the **Peer type**, set the protocol to **UDP**.
- URI scheme:** This option is only available if you selected **TLS** as the **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 calls to be transmitted via proxy servers. To make sure that a call is sent encrypted to the proxy of the remote side, select **SIPS** (secure SIP). If the call is routed via a proxy server that is not able to route the call encrypted, it rejects the call and the call is sent to another proxy until it can be transmitted.
- Domain:** Enter the domain name, e.g., dialogic.com, or the IP address. The domain name must comply with the DNS rules. The domain name entry here is only needed if the SIP peer does not use its hostname as the source domain when it places a call.

Enhanced

You can configure the following parameters in the **Enhanced** section when you create or modify a SIP Peer:

Enhanced	
Default peer for received SIP calls:	☐
Display name to:	
Display name from:	
User name to:	
User name from:	
Gateway prefix:	
Reply-To expression:	
Reply-To format:	
Force T.38 reinvite:	☐
Alive check:	☐ 0 seconds (0=auto)
Disconnect tone support:	☐
Cause code mapping inbound:	peer default
Cause code mapping outbound:	peer default
Codec profile:	default
Maximum channels:	480
Early media support:	☒
Reliable provisional response:	Optional

Default peer for received SIP calls

Enable this option if the selected peer type should be used as the default peer. Calls from unconfigured SIP peers will be assigned to this peer, and therefore are handled with these settings. This option can also be changed via the Default Peer option on the main SIPcontrol page.

Note: When a peer is selected as the default, the previously selected default peer is automatically unselected.

Display name to:

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

Display name from:

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

User name to:

You can 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 Diva Analog Media Boards.

If a call from SIP does not contain a user name, the name entered here is transmitted to the receiver as the calling party number. This applies to all references to PSTN in this section. (The opposite side can either be PSTN or SIP.)

User name from:

Enter the user name that is added to the SIP address when a number from the PSTN is suppressed. You can 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 to the PSTN as the called party number.

Gateway prefix:

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

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

Reply-To expression:	You can configure this parameter only if you selected e-phone as Peer type in the Edit SIP Peer Configuration window. Enter the expression that may be necessary for the e-phone server to handle the call. Normally, this is necessary to omit the 0 (zero) for external calls and to manipulate the address so the e-phone server is able to call back.
Reply-To format:	You can configure this parameter only if you selected e-phone as Peer type in the Edit SIP Peer Configuration window. Enter the format that may be necessary for the e-phone server to handle the call. Normally, this is necessary to omit the 0 (zero) for external calls and to manipulate the address so the e-phone server is able to call back.
Alive check:	If you select this option, the failover procedure is expedited, because Diva SIPcontrol does not wait for a call time-out if a peer does not respond. To achieve this, Diva SIPcontrol 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.". In this case, Diva SIPcontrol will automatically direct calls to this peer again.
Disconnect tone support:	If the remote side is able to provide inband tones or signals on disconnect, check here to play those inband tones to the SIP peer instead of terminating the SIP call immediately. The SIP call ends either by the client sending a BYE or after the Disconnect Timer of the PSTN interface ends (normally with "Normal call clearing"). Normally this option is set only if the peer is a human talker.
Cause code mapping inbound:	Select the cause code mapping for calls coming from this SIP peer that you configured under Cause Code Maps, as described on page 57.
Cause code mapping outbound:	Select the cause code mapping for calls to this SIP peer that you configured under Cause Code Maps, as described on page 57.
Codec profile:	Select the codec list that you configured under Codec Profiles, as described on page 58. If you do not select a list, an internal default list is used with the following default priority order: 1. G.711A 2. G.711u 3. G.729, if licensed* 4. GSM-FR* 5. G.726 (16, 24, 32, and 40 kbps)* 6. Comfort Noise 7. DTMF via RFC 2833/RFC 4733 (no real codec, but internally handled as codec) In calls from SIP to the PSTN, the first codec offered by the peer that is also in the set of supported and available codecs is selected. This can be changed by a manual configuration that is not currently available via the Diva SIPcontrol web interface. *For Office Communications Server 2007, Office Communications Server 2007 R2, and Lync Server, G.729, GSM-FR, and G.726 are disabled by default.
Maximum channels:	Specifies the number of channels that this SIP peer is able to handle at the same time. This setting is used by Diva SIPcontrol to distribute calls in a load-balancing scenario and to avoid speech quality degradation and/or call failures at the peer due to overload conditions.
Early media support:	Specifies whether the peer supports early media for calls to the PSTN. For non-human callers, this option should be disabled.

Reliable provisional response:

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

This parameter specifies whether reliable provisional responses (RFC 3262) should be used. The following values are available:

- **Disabled:** Reliable provisional response is not used.
- **Optional:** Reliable provisional response can be used.
- **Required:** Reliable provisional response is mandatory.

Security

You can configure the following parameters in the **Security** section when you define or modify a SIP Peer:

Security	
Signaling accept level:	Accept unencrypted and encrypted calls
Media security level:	Offer and accept SRTP

Signaling accept level:

This parameter defines how 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, regardless of the encryption mode.
- **Accept encrypted calls only:** Only signaling with TLS is accepted; unencrypted signaling is rejected.
- **Accept encrypted call with SIPS URI only:** Only signaling encrypted with the URI scheme secure SIP is accepted. Calls sent with TLS encryption are rejected.

Media security level:

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

- **No SRTP:** The voice stream is not secured with SRTP.
- **Offer and accept SRTP:** The voice stream is secured with SRTP, if possible.
- **Require SRTP for encrypted calls:** Calls via TLS need to use SRTP, otherwise they are rejected.
- **Require STP for all calls:** All calls are established with SRTP only, regardless of the signaling protocol.

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 can configure the following parameters in the **Session Timer** section when you define or modify a SIP Peer:

Session Timer	
Use session timer:	☒
Interval:	600
Minimum session expires:	90

Use session timer:

Activates session monitoring via SIP session timers using the time-out values given here. Refer to RFC 4028 for details.

Interval:

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

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

Address Normalization

You can configure the following parameters in the **Address Normalization** section when you define or modify a SIP Peer:

Address Normalization	
Dialplan:	none
Number format (outbound):	Unchanged
Encoding (outbound):	Use prefixes
Address map inbound:	none
Address map outbound:	none

Dialplan: Select the local dialplan to be used by the dialplan module of Diva SIPcontrol. Configure the local dialplan under [Dialplans](#), as described on page 51, before you select it here.
The dialplan selected here applies only to outgoing calls.

Number format (outbound): This parameter determines the shortest format allowed that is sent in calls to this SIP peer. You 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 unless it is an international number with a different country code.
- **Extension:** The number is reduced as much as possible. An internal number is reduced to its extension only.

For more information about number formats, see [How Numbers Are Processed](#) on page 77.

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

Address map inbound: Name of the regular expressions list applied to the addresses received on calls from this SIP peer. See [Address Maps](#) on page 53 for more information about setting up a regular expression list.
Regular expressions can be used to add or remove dial prefixes required by a PBX or to rewrite public phone numbers of different number ranges into a common format. See the [Examples](#) on page 79 for more information.

Address map outbound: Select the name of a regular expression list to be applied on calls to this SIP peer. See [Address Maps](#) on page 53 for more information about setting up a regular expression list.
Regular expressions can be used to add or remove dial prefixes required by a PBX or to rewrite public phone numbers of different number ranges into a common format. See the [Examples](#) on page 79 for more information.

Authentication

You can configure the following parameters in the **Authentication** section when you define or modify a SIP Peer:

Authentication			
Realm	Auth user name	Password	
			Delete
Add			

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 can 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.
- The current status of a destination. See [How Calls Are Processed](#) on page 67 for more information.
- The result of an Active Directory query.

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

For more information about possible route configurations, see [Routing Examples](#) on page 69.

The following menus are available for configuration:

- [General](#), as described on page 42
- [Address Normalization For Condition Processing \(Using Source Dialplan\)](#), as described on page 43
- [Conditions](#), as described on page 43
- [Address Manipulation](#), as described on page 44

General

You can configure the following parameters in the **General** section when you define or modify a route:

General

Name:	Routing1	
Type: Name	Source	Destination
PSTN: Controller1	☐	-
PSTN: Controller2	☐	-
SIP: SBA	☐	-
Max. call attempts for this route in a failover scenario:	0 (0 = try all selected destinations)	

- Name:

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

Select either the configured PSTN interfaces or SIP peer as a source. The route will only be considered for a call if the call originated from a selected source.

You can select the same interface as a source and destination, e.g., if a call from the PSTN should be routed back to the PSTN.

Calls arriving at disabled sources are immediately rejected without querying any route.

At least one source interface is required for the route.
- Destination:

The master or slave option in the dropdown menu allows for configuring priorities. Diva SIPcontrol 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.
- Maximum call attempts for this route in a failover scenario:

Enter the maximum number of destinations in a route that Diva SIPcontrol should call in a failover environment. If you enter 0 (zero), Diva SIPcontrol tries all selected destinations. A value of 1 disables the failover functionality and tries only the first destination of a route.

If LDAP is used and the LDAP query requires various call attempts, this counts only as one call attempt in a failover environment, because the LDAP queries are not counted as call attempts here but in a different instance.

Address Normalization For Condition Processing (Using Source Dialplan)

You can configure the following parameters in the **Address Normalization For Condition Processing (Using Source Dialplan)** section when you define or modify a route:

Address Normalization For Condition Processing (Using Source Dialplan)	
Use Dialplan:	☒
Number format:	Unchanged
Encoding:	Use prefixes

Use Dialplan

This parameter defines whether the interface-specific dialplan should be applied to the call addresses in the route being defined. If you set this parameter to false, neither the inbound nor outbound dialplan is applied, and only the address maps are used for the numbers.

Disable this parameter for emergency numbers such as 911 in the U.S. and 110 in Germany, because these numbers can falsely be converted to E.164 using a dialplan. To be sure that special numbers like emergency numbers pass unchanged, you should also define special break-out rules for these numbers in the address maps.

Note: If **Use Dialplan** is disabled, the Number format and Encoding parameters will not be evaluated.

Number format:

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

Unchanged: The number signaled in the received call request will be used unchanged for dialing.

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

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

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

For more information about number formats, see [How Numbers Are Processed](#) on page 77.

Encoding:

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

Conditions

You can configure certain conditions for a route. If you do not configure any conditions, the route is used as a 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 can configure the following parameters in the **Conditions** section when you create or modify a route:

Conditions			
Called number	Calling number	Redirect number	
			Delete
Add			

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

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

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

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

Address Manipulation

You can configure the following parameter in the **Address Manipulation** section when you create or modify a route:

Address Manipulation	
Address map:	none v

Address Map: If a route matches, the address manipulation setting allows you to modify the call addresses according to your needs. For example, if calls with the called party number starting with "9" should be directed to a specific peer, it might be desirable to remove this digit. This can be done with a configured address map. You need to configure the address map as described under [Address Maps](#) on page 53 before you can select it here.

Security Profiles

For authentication and data encryption for TLS, certificates need to be installed on the computer with Diva SIPcontrol and on remote computers. When a secure domain is opened, the server and client authenticate each other with a so called "SSL handshake". With this handshake, the identity of a user is certified and the user can be trusted. All necessary certificates are provided by a Certificate Authority (CA), and they are issued for one domain name.

For test purposes or internal usage, you can also create and sign your own self-signed certificate, e.g., with one of the many tools available on the internet. Search for "self-signed certificate" and you will find a list of possible tools. But you need to be aware that self-signed certificates do not provide the same security as CA-signed certificates. Also, many web browsers check if the certificate is signed by a CA, and, if it is not, a warning message will appear asking whether the user really wants to trust that web site, which can make the user feel insecure.

Certificate files can be generated in different formats, e.g., .pem, .der, .cer, or .pfx. All files need to be in PEM format (base64 encoded), in order to be used by Diva SIPcontrol. For more information about secure connections and certificates, see [Data Security Overview](#) on page 61.

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

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

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

How to Retrieve Keys and Certificates from a PFX file for Use in Diva SIPcontrol

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

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

```
openssl pkcs12 -in filename.pfx -nocerts -out protected-key.pem
```
2. Remove the passphrase from the private key as required by Diva SIPcontrol:

```
openssl rsa -in protected-key.pem -out key.pem
```
3. Export the certificate file from the PFX file:

```
openssl pkcs12 -in filename.pfx -clcerts -nokeys -out cert.cer
```
4. Export the Root CA certificate file from the PFX file:

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

Setting up a Security Profile

To set up or modify a security profile, click the **Details button** in the **Security Profiles** section. To open the online help for a specific parameter, click the parameter, and a window with the help text will appear.

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

Upload Certificate and Key Files	
Certificate authority file: Not available	Browse... Upload
Certificate file: Not available	Browse... Upload
Key file: Not available	Browse... Upload

To upload a certificate or key file:

1. Click the **Browse** button next to the type of file you want to upload.
2. In the **Choose File to Upload** window locate the certificate or key file, and click **Open**.

3. In the Diva SIPcontrol web interface, click **Upload**. After the certificates are uploaded, the information below the certification files changes from "Not available" to "Uploaded". You will not see the paths to the directory in which the files are stored:

Upload Certificate and Key Files	
Certificate authority file: Uploaded	Browse... Upload
Certificate file: Uploaded	Browse... Upload
Key file: Uploaded	Browse... Upload

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

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

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

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

Global Security Parameters

You can configure the following parameters in the **Global Security Parameters** section when you set up a security profile:

Global Security Parameters	
Host name:	must match 'CommonName' of certificate!
Supported cipher levels:	High: ☒ Medium: ☒ Low: ☐
Authentication mode:	Standard TLS Authentication ▼
Certificate date verification:	☐

Host name The common name used in the certificate to identify the Diva SIPcontrol host machine.

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

- **High:** This currently means cipher suites with key lengths larger than 128 bits, and some with 128-bit keys.
- **Medium:** This currently means cipher suites using 128-bit encryption.
- **Low:** This currently means cipher suites using 64- or 56-bit encryption algorithms but excluding export cipher suites.

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

LDAP

The Lightweight Directory Access Protocol (LDAP), is an application protocol that programs use for querying information from a server. The protocol runs over TCP/IP. Deployments today tend to use Domain Name System (DNS) names for structuring the topmost levels of the hierarchy. LDAP servers index all the data in their entries, and "filters" can be used to select the person or group for which you are looking. LDAP is appropriate for any kind of directory-like information, where fast lookups and less-frequent updates are the norm. For example, when you use Microsoft® Outlook and search the address book for a colleague, you access the Microsoft® Active Directory database via LDAP.

How to Use LDAP to Access Active Directory for Routing Calls via Diva SIPcontrol

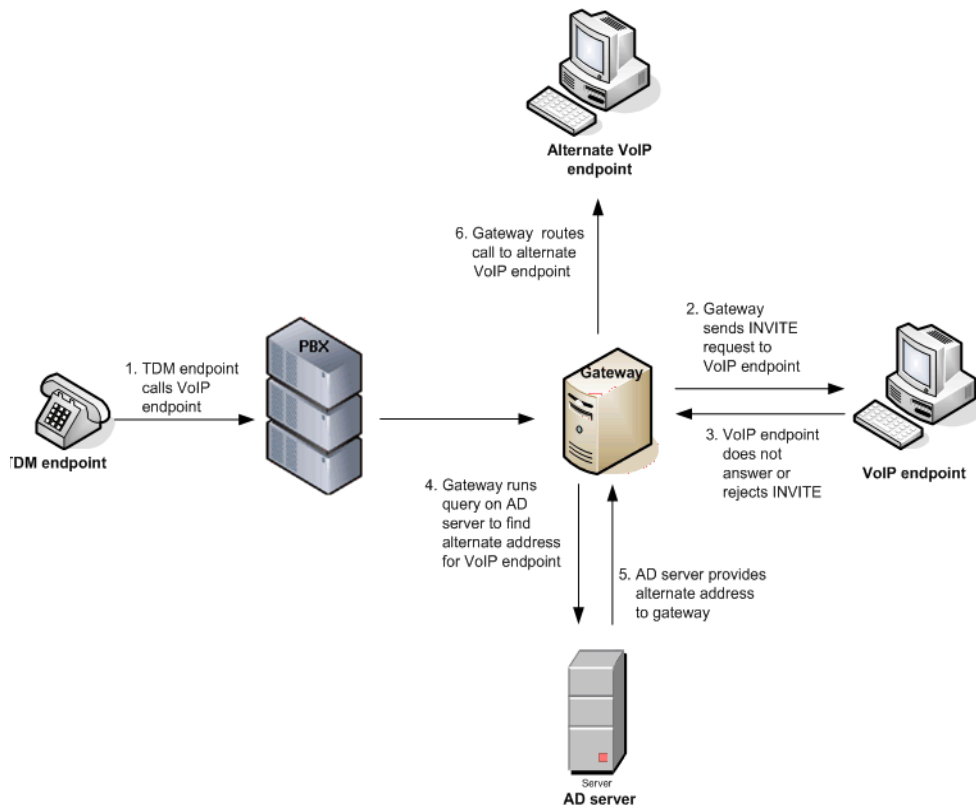
You can enable LDAP functionality via Diva SIPcontrol web configuration. When LDAP is activated, Diva SIPcontrol will query the server on startup and store the query results internally for a faster lookup. In a default configuration, this internal storage will be updated once a day to reflect changes on the LDAP database. If you use LDAP, you need to configure two routes for one LDAP call:

- One route should contain the LDAP destination.
- The other route should contain the final destination.

The order of the routes is irrelevant, but it is important to configure the first route with the conditions needed to avoid recursion.

Use Case for LDAP

In this scenario, the gateway is connected between the PSTN or PBX and a VoIP endpoint. Additionally, the gateway receives a call from the TDM network that is intended for the VoIP endpoint. However, the VoIP endpoint does not respond to the original INVITE request or it responds with a failure. The gateway must query the Active Directory server to determine if there is an alternate address (i.e. phone number, etc.) where the VoIP endpoint can be contacted, and if so, the gateway must route the call to the alternate address.



To add LDAP query settings, click the **Add** button in the **LDAP** section. To change the settings for each LDAP, click the **Details** button on the right hand side.

LDAP Query

You can configure the following parameters in the **LDAP Query** section when you create or modify an LDAP:

LDAP Query	
Name:	QUERY1
Search Attribute:	telephoneNumber
Result (1st):	
Result (2nd):	
Result (3rd):	

Name

Enter a name to easily identify the LDAP query.

Search attribute:

Select the attribute to search for:

- **telephoneNumber**: The primary office number.
- **homePhone**: The primary home/private number.
- **mobile**: The primary mobile number.
- **facsimileTelephoneNumber**: The primary fax number.
- **proxyAddresses**: E-mail address attributes that can have either format SMTP:bob@domain.de or sip:bob@domain.de.

The following attributes are used by Office Communications Server 2007, Office Communications Server 2007 R2, and Lync Server 2010:

- **msRTCSIP-PrimaryUserAddress**: This attribute contains the SIP address of a given user.
- **msRTCSIP-Line**: Refers to a user's primary office number as specified in the Active Directory msRTCSIP-line attribute, which the Microsoft® Office Communications Server uses to perform reverse number lookup to obtain all the user's SIP endpoints.

Result:

The list defines the attributes for which to search. The called address searched for will be replaced by the contents of the result attribute with the highest priority value. The attributes in result 2 and 3 are sequentially searched only if the address with the highest priority fails.

LDAP Domain

You can configure the following parameters in the **LDAP Domain** section when you define or modify an LDAP:

LDAP Domain				
Domain:				
Base Search DN:				
Search Scope:	base (search the object itself)			
Max. No Search Results:	100			
Server Address	Server Port	User Name	Password	
Add				

Domain:

Enter the domain name of the LDAP server, e.g., dialogic.com.

Base Search DN:

This is the starting point in the Active Directory hierarchy at which your search will begin, e.g., ou=EMEA,ou=corp,dc=dialogic,dc=com.

- Search Scope:** The LDAP search scope indicates the set of entries at or below the base search DN that can be considered potential matches for a search operation.
- There are three search scope values:
- **base (search the object itself)**: This specifies that the search should only be performed against the entry specified as the base search DN. No entries below it will be considered. Use this option if the base search DN is close to the data to be searched for, because this way desired data can be found quickly.
 - **one level (search the object's immediate children)**: This specifies that the search operation should only be performed against entries that are immediate subordinates of the entry specified as the base search DN. Neither the base entry itself nor the entries below the immediate subordinates of the search base entry are included.
 - **subtree (search the object and all its descendants)**: This specifies that the search operation should be performed against the base search DN itself and all of its subordinates.
- Max. No Search Results:** This value specifies the maximum number of search results to be returned by the LDAP server. The default value is **100**. A value of 0 indicates that the results are returned unlimitedly.
- If the value is too small, not all addresses stored in the LDAP database will be considered for routing; that is, the excess entries will be considered non-existent.
- Server Address:** Enter the IP address of the Active Directory server. This entry is mandatory, because Diva SIPcontrol does not use a default server.
- You can enter the server address either as an IP address or as an FQDN, e.g., 11.11.11.11 or ldap.dialogic.com.
- It is possible to configure multiple servers for an LDAP query. In this case, SIPcontrol will use the second server if the first one fails.
- Server Port:** Enter the port to which the server is listening. The default value is **389**. If you set the port to 0, Diva SIPcontrol will select a port automatically.
- If you use an indexed database, such as Microsoft® Active Directory, set the port to 3268 to speed up LDAP queries.
- User Name:** Enter a user name. This can be a DN, UPN (User Principal Name, e.g., name@domain.name), Windows NT style username (e.g., domain\username), or another name that the directory server will accept as an identifier.
- In some cases, it is possible to connect to an LDAP server without a user name and password. If it is not possible, you can create a dummy user for this gateway task.
- Password:** Enter a password for the user account.
- Note:** Diva SIPcontrol currently supports Simple authentication, which means that the password is transmitted in clear text over the network. The password also is stored and processed locally in clear text.
- It is recommended that you use a separate user account with restricted permissions for Diva SIPcontrol access.

LDAP Cache

You can configure the following parameters in the **LDAP Cache** section when you define or modify an LDAP:

LDAP Cache	
Max. Entries:	100
Update Interval (sec):	86400
Persistent Save:	☐

- Max. Entries** The maximum amount of entries in the cache, which is the maximum number of entries retrieved from the LDAP server. Note that if the value is too small, some LDAP entries will not be resolved.
- Default is **100**.

Update Interval (sec)	Update interval in seconds for the cache. The longer the update time, the longer the data is kept in the cache. It is recommended that you leave the default value. A long update interval takes more time to update because of the big cache, but a short update interval uses both Diva SIPcontrol resources and LDAP server resources too often. Default is 86400 seconds.
Persistent Save	If set, the gateway accesses the persistent cache first without connecting to the LDAP server. If the next update time is within the range configured in Update Interval (sec), the gateway uses the saved cache; otherwise, it tries to connect to the LDAP server in order to update the cache. This option is not set by default.

Dialplans

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

The dialplan module supports the following features:

- **Number expansion and reduction:** called, calling, and redirected numbers are converted to one of the following formats: international, national, local, or internal (extension-only) format. For each format, either prefix digits or digital number type flags can be used.
- **Adding and removing the line access code:** If not present, dialed numbers are automatically prepended by the digits needed to access the public telephone network.
- **Support for the North American numbering plan:** Up to 10 area codes can be configured to be treated differently. For example, in many areas, dialing into neighboring areas does not require dialing 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 Diva SIPcontrol, 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 Diva SIPcontrol 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 of incoming external calls in order to enable callback functionality at internal phones. If this is the case, enable this option.
- **PSTN access code provided by the caller:** This option defines whether Diva SIPcontrol expects the outside access digit in the called number of external calls. It is normally required to prepend the outside access digit to call an external number from an internal phone. However, in some configurations this is not required, such as a configuration that is part of the North American numbering plan (NANP), where an internal number can be identified based on its length.

Enable this option if the internal users that use SIPcontrol for external calls prepend the outside access digits in their calls; otherwise disable it.
- Diva SIPcontrol's number normalization function does not remove outside access digits as a PBX can do for external calls. If Diva SIPcontrol needs to behave like a PBX with an outside access digit for external calls, use the Address Map functionality in combination with a Routing module.

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

You can configure the following parameters in the **General** section when you create or modify a dialplan:

General	
Name:	Dialplan1
Country code:	
North-American numbering plan:	☐
Area code:	With national prefix ▼
Other local areas:	
Base number:	
Maximum extension digits:	0 ▼
International prefix:	
National prefix:	
Access code:	
PSTN access code provided by SIP caller:	☐
Incoming PSTN access code provided by PBX:	☐
OK Cancel	

- Name:** Enter a name to easily identify the dialplan, e.g., Stuttgart office.
- Country code:** Enter the country code without any prefixes for the country in which the computer with the installed Diva SIPcontrol is located, e.g. 1 for US or 49 for Germany.
- North-American numbering plan:** Select this option if the North American numbering plan (NANP) is needed for your configuration. With the NANP, a city can have more than one area code, consequently it is not evident how to dial a number in the same city. Diva SIPcontrol 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 the NANP, you can choose between the following number transmission methods:
With national prefix: The long-distance code is added to the number.
Local: The number is transmitted without any area code.
Without national prefix: The number is transmitted without the long-distance prefix.
- Other local areas:** You can enter various area codes that are considered local and should be called without the long-distance prefix. This is the case in some countries where the North American numbering plan is deployed, e.g., in the USA. With the NANP, a city can have more than one area code; consequently, it is not clear how to dial a number in the same city.
- Base number:** Enter your subscriber or trunk number without a country and area code. If you use MSNs, leave this field empty and enter the length of the MSNs in **Maximum extension digits**.
- Maximum extension digits:** Specify the maximum number of extension digits. Use the "arrow up" and "arrow down" buttons to do so.
- International prefix:** Enter the international prefix for your country, e.g., 00.
- National prefix:** Enter the digits of the national prefix, e.g., 0 in Germany.

Access code:	Enter the digits that are needed to get access to the public network, e.g., 9.
PSTN access code provided by 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 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 conditions 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 be changed with the "arrow down" and "arrow up" buttons in Microsoft® Internet Explorer® or the **Up** and **Down** buttons in Mozilla Firefox.

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

You can configure the following parameters when you create or modify an address map:

General	
Address map name:	AddressMap1
Rule name:	AddressMap1.1
Stop on match:	☐
Enhanced configuration:	☒

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 can be selected.

Note: The name can be edited only during the creation of an address map.

Rule name: Enter a name for the rule of the map, e.g., "Remove 9 from all incoming calls".

Stop on match: This flag determines whether Diva SIPcontrol should continue to search for matching rules when all expressions match all addresses of a call. If set, the address matching is aborted when there is a match.

Enhanced configuration This flag determines whether Diva SIPcontrol uses the new interface for configuring address maps. The new interface supports the ability to specify the number type, numbering plan, and presentation indicator directly, while the older version supported prefixing the address with "+," "N", and "S", respectively, to specify a limited subset of number types.

Leave this option enabled (the default), unless you need to use the old interface for compatibility reasons. For address maps created in previous versions of SIPcontrol, this option is disabled by default.

Note: In the old interface, number type flags from digital networks, e.g., ISDN or SS7, are converted into special prefixes on the SIP side. Therefore, the following address formats apply only to the old interface:

- + indicates an international number type, if it is the first character in the string
- N indicates a national number type, if it is the first character in the string
- S indicates a subscriber number type, if it is the first character in the string

Called address rules

	Condition	Result
Address:		
Name:		
Number type:	☒ Unknown ☒ International ☒ National ☒ Network specific ☒ Subscriber ☒ Abbreviated	No change v
Numbering plan:	☒ Unknown ☒ ISDN/telephony E.164 ☒ National standard ☒ Private	No change v

Calling address rules

	Condition	Result
Address:		
Name:		
Number type:	☒ Unknown ☒ International ☒ National ☒ Network specific ☒ Subscriber ☒ Abbreviated	No change v
Numbering plan:	☒ Unknown ☒ ISDN/telephony E.164 ☒ National standard ☒ Private	No change v
Presentation:	☒ Allowed ☒ Restricted ☒ Number not available ☒ Undefined	No change v

Redirect address rules

	Condition	Result
Address:		
Name:		
Number type:	☒ Unknown ☒ International ☒ National ☒ Network specific ☒ Subscriber ☒ Abbreviated	No change v
Numbering plan:	☒ Unknown ☒ ISDN/telephony E.164 ☒ National standard ☒ Private	No change v
Presentation:	☒ Allowed ☒ Restricted ☒ Number not available ☒ Undefined	No change v

OK Cancel

Address	Checks or manipulates the current address (normally a number for a PSTN address or a SIP-URI for a SIP address). To remove the part matched by the condition, set the Result field to empty. To check for a specific condition and keep the original address, set the Result field to \$& .
Name	Checks or manipulates the current name. To remove the part matched by the condition, set the Result field to empty. To check for a specific condition and keep the original address, set the Result field to \$& .
Number type	Checks or manipulates the number type of the current address. For unmodified SIP addresses, the number type is "unknown". To check for a number type without changing it, set the Result field to No change .
Numbering plan	Checks or manipulates the numbering plan of the current address. For unmodified SIP addresses, the numbering plan is Unknown . To check for a numbering plan without changing it, set the Result field to No change .
Presentation	Checks or manipulates the presentation indicator. For unmodified SIP addresses, the presentation is Undefined . To check for a presentation without changing it, set the Result field to No change .

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

Number: 1234567

Expression: ^123

Format: 4567

Result: 45674567

Cause Code Maps

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

If the internal default mapping table provided by Diva SIPcontrol does not fulfill your needs, e.g., because your local PBX uses non-standard cause codes, you can configure your own cause code mapping table, which will be checked before the default table is checked. See [Cause Code Mapping](#) on page 81 for the cause/response code mapping table. If you create your own cause code mapping table, make sure to select it in the **SIP Peers** section under [Enhanced](#).

To add a cause code, open the **Cause Code Maps** section and 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 appear. You can configure the following parameters when you create or modify a cause code:

Name	Enter a name to easily identify the cause code mapping table.
Direction	Select the direction for which this table is used: • Select PSTN to SIP to configure mappings of PSTN cause codes to SIP response codes. This mapping is used if a call from a SIP endpoint to a PSTN endpoint cannot be completed. • Select SIP to PSTN to configure mappings of SIP response codes to PSTN cause codes. This mapping is used if a call from a PSTN endpoint to a SIP endpoint cannot be completed.
PSTN cause code	Enter the PSTN cause code equivalent to the SIP response code entered in this menu. The PSTN cause code is also known as Q.850 cause code. Valid values are 1 to 127. Note: For SIP to SIP calls or PSTN to PSTN calls, the original cause code is preserved, so mapping is unnecessary.
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. Note: For SIP to SIP calls or PSTN to PSTN calls, the original cause code is preserved, so mapping is unnecessary.
Default	Enter the cause or response code that Diva SIPcontrol 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, Diva SIPcontrol's internal default mapping table will be used.

Codec Profiles

To configure a codec profile, 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 Peers** section, under [Enhanced](#). To open the online help for a specific parameter, click the parameter, and a window with the help text will appear.

You can configure the following parameters when you create or modify a codec profile:

General

Name:

Audio Codecs

Available Codecs

G.729

G.726 16 kbps

G.726 24 kbps

G.726 32 kbps

G.726 40 kbps

Use Codec ->

<- Remove Codec

Selected Codecs

G.711 A-Law

G.711 u-Law

Up

Down

G.711 A-Law Codec Settings

Packet interval default:

Voice activity detection:

☐

Comfort Noise Generation:

☐

Audio Quality

Support comfort noise payload:

☒

Noise suppressor:

☐

Echo canceller:

☒

DTMF Codec

Transmit as RTP event:

☒

Automatic payload type:

☒

Manual payload type value:

Disable CNG event:

☐

OK

Cancel

- Name:

Enter a name to easily identify the codec profile You can select the codec profile in the **SIP Peers** section.
- Available Codecs:

This list includes all available codecs. If you want to use a certain codec, select it and click **Use Codec**. The codec will be moved to the **Selected Codecs** list. The G.729 codec can only be used after you have purchased and activated a license. See [License Activation](#) on page 13 for more information.
- Selected Codecs:

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

Interval between RTP packets in an RTP stream. Also known as packetization time or RTP frame size.
- Voice activity detection:

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

If you enable this parameter, packets with low artificial background noise are sent to fill periods where no data packets are received from the SIP peer. This helps prevent the other party from thinking the transmission has been lost (because of the silence) and hanging up prematurely.

Note:

Support for this feature depends on the type of Diva Media Board present in the system. If the hardware does not support this feature, the setting is ignored.

Support comfort noise payload:	If you enable this parameter and VAD is configured for the codec used for the call, periods of silence will be replaced by sending a special "comfort noise" signal to the SIP peer. This allows a supporting SIP device to generate appropriate artificial background noise in order to remove the impression of the call being interrupted. If the SIP peer does not support this type of event, this setting has no effect.
Noise suppressor:	Enable this parameter if you want to use the noise suppressor functionality.
Echo canceller:	If you enable this parameter, the audio echo canceller is active for calls to or from the PSTN.
Transmit as RTP event:	This option enables DTMF and fax tones to be sent and received as RTP events instead of audio signals.
Automatic payload type:	G.726, iLBC, and DTMF have a dynamic RTP payload. If you enable this option, Diva SIPcontrol sets the values automatically. 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, Diva SIPcontrol uses the value suggested by the endpoint. Generally, this parameter is left at its default value.
Disable CNG event:	Select this option to transmit the CNG event as an in-band audio signal instead of an RTP event according to RFC 4733. Note: This option is only available if the option Transmit as RTP event is enabled.

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 can 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 for the user.

If Diva SIPcontrol 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 can use either a private registrar service or a public registrar server.

To configure a registrar server, open the **Registrations** section and 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 appear.

You can configure the following parameters when you create or modify a registration:

General	
Name:	Registrar1
Registrar address:	
Registrar port:	
Registrar protocol:	TCP
URI scheme:	SIP (default)

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 calls to be 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 sent 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	URI scheme	User name	@Domain	Protocol	Re-register time	Auth user name	Password	Register as	
	SIP (default) ▼			UDP ▼	3600			Standard ▼	Delete
Add									

- Own display name:** Enter the name that should be displayed at the registrar server.
- URI scheme:** Select either **SIP (default)** or **SIPS** as URI scheme.
- User name:** Enter the name or number that Diva SIPcontrol uses to register at the registrar server.
- Domain:** Enter the domain name of the registrar server.
- Protocol:** Select **UDP** if you register as an e-phone gateway.
- Re-register time:** Enter the re-register time in seconds. This is the time for which 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 Diva SIPcontrol to function as a gateway for e-phone.

Logging and Diagnostics

You can configure the following parameters shown in **Logging and Diagnostics** section:

Logging and Diagnostics	
Event log level:	Errors ▼
Debug level:	Off ▼
XML Configuration file:	Show
Activate Configuration Discard Configuration	

- Event Log Level:** A computer with Diva SIPcontrol installed can write different types of events into the System Event Log. The details for each event log are described in [Event Logging](#) on page 89.
- Debug Level:** The debug level setting can be used for debugging and tracing purposes. During normal operation, it should be set to **Off** to lessen the effect on system performance.
- XML configuration file:** Shows the configuration in raw format. This option is used only by Dialogic Support.

CHAPTER 6

Data Security Overview

Since version 2.0, Diva SIPcontrol provides additional security options for transmitted and received data:

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

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

Secure HTTP

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

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

For 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 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 Diva SIPcontrol and the computer on which the web browser used to connect to Diva SIPcontrol via HTTPS is running must be configured with the proper certificate.
- When accessing the Diva SIPcontrol web interface, use `https://<IP-address-or-URL-of-Diva-Webserver>:10006/` instead of `http://<IP-address-or-URL-of-Diva-Webserver>:10005/`.

TLS

SIP (Session Initiation Protocol) is a signaling protocol used for VoIP calls over the Internet. SIP messages contain information such as call-party information, call media type, whether it is a secure call, and if so, what encryption algorithm is used, etc. SIP can be carried by UDP, TCP, or TLS transports. Both UDP and TCP transport data in clear text. As a result, UDP and TCP can easily be monitored by a third party. TLS, on the other hand, carries SIP data in a secure way by encrypting the data and authenticating the transport connections. Authentication helps to ensure that you are talking to the intended peer. For authentication purposes, you need to install [Certificates](#), as described in [Security Profiles](#), as described on page 44, and enable TLS as the transport protocol, as described in [Network Interfaces](#) on page 34.

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, and the parameters are negotiated during call initiation time. SRTP mode is activated typically in combination with TLS, but in some cases (e.g., testing, intranet connections only) it is useful to allow SRTP also without TLS being activated.

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

SRTP can be set for each SIP peer in the [Security](#) configuration, as described on page 39. The cipher level can be set in the [Global Security Parameters](#), as described on page 46.

Certificates

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

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

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

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

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

How to Retrieve Keys and Certificates from a PFX File for Use in Diva SIPcontrol

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

1. Export the private key file from the PFX file:
`openssl pkcs12 -in filename.pfx -nocerts -out protected-key.pem`
2. Remove the passphrase from the private key as required by Diva SIPcontrol:
`openssl rsa -in protected-key.pem -out key.pem`
3. Export the certificate file from the PFX file:
`openssl pkcs12 -in filename.pfx -clcerts -nokeys -out cert.cer`
4. Export the Root CA certificate file from the PFX file:
`openssl pkcs12 -in filename.pfx -cacerts -nokeys -out cacert.cer`

Using Certificates with Microsoft® Office Communications Server 2007

Microsoft® Office Communications Server 2007 requires that:

- Server certificates contain one or more CRL (Certificate Revocation List) distribution points.
CRL distribution points are locations from which CRLs can be downloaded to verify that the certificate has not been revoked since the time it was issued. The CRL distribution point is an extension within the digital certificate that can be used if the CA (certification authority) in your PKI (Public Key Infrastructure) has a CRL distribution point.
- Server certificates support EKU (Enhanced Key Usage).
EKUs are needed for server authentication and ensure that the certificate is valid only for the purpose of authenticating servers. This EKU is essential for MTLS (Mutual TLS).

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

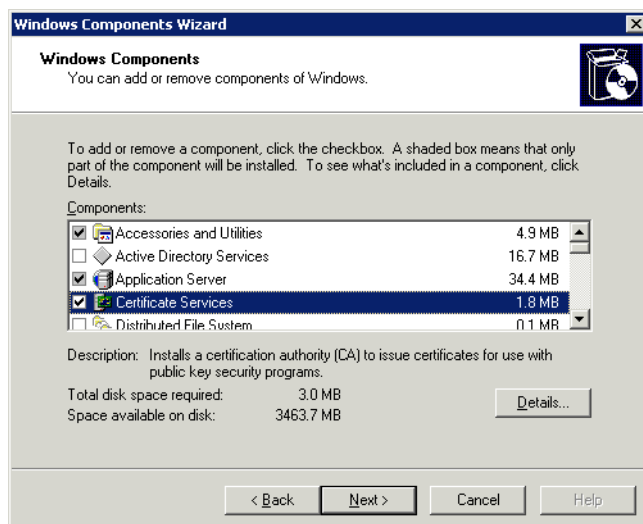
Using Certificates with Microsoft® Lync™ Server 2010

Lync Server requires that the gateway server certificate contain the FQDN configured for the gateway in the Lync Topology Builder. This FQDN must be specified in the CN or SAN. Alternatively, it can be specified in both locations.

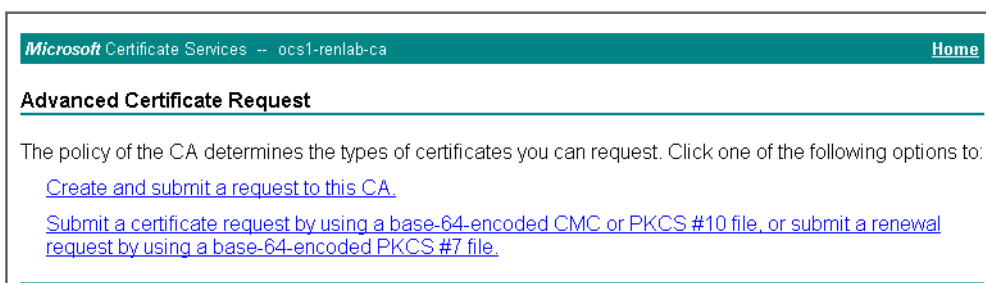
How to Generate Certificates Using Microsoft® Certificate Services and Upload Them in the Dialogic® Diva® SIPcontrol™ Web Interface

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

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



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



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

Microsoft Certificate Services -- ocs1-renlab-ca [Home](#)

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
CCsGAQUFBwMCMBEgcWCGSAGG+EIBAQQEAwIGwDAN
PyfBoLxszjSVUL56SsxysotU+ToCmuwFEEJXO3eX
oa4FuYiE3FeRZaM9iEO8/1+dXKHgtDHf9GD/FzUO
JnMfbyjA51DQApQo7bwOOaEkXCOQ7rGUjKIdOp+x
-----END CERTIFICATE REQUEST-----
```

[Browse for a file to insert.](#)

Additional Attributes:

Attributes:

4. Go to the Microsoft® Certification Authority Management console and sign the certificate request.
5. To download the signed certificate, go to the Microsoft® Certificate Services download page for signed certificates, select **Base 64 encoded**, and click **Download certificate**.

Microsoft Certificate Services -- ocs1-renlab-ca

Certificate Issued

The certificate you requested was issued to you.

☐ DER encoded or ☒ Base 64 encoded

 [Download certificate](#)
[Download certificate chain](#)

6. In the File Download dialog box, select **Save This File to Disk**, and click **OK**.

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

Microsoft Certificate Services -- ocs1-renlab-ca

Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority, [install this CA certificate chain](#).

To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.

CA certificate:

Current [ocs1-renlab-ca]

Encoding method:

☐ DER

☒ Base 64

[Download CA certificate](#)

[Download CA certificate chain](#)

[Download latest base CRL](#)

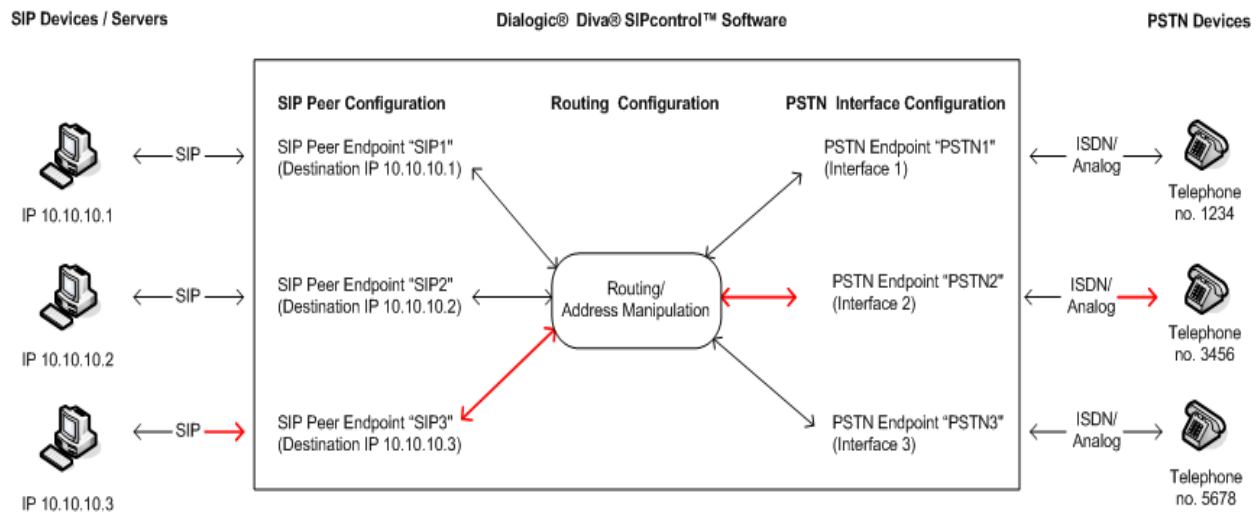
8. In the File Download dialog box, select **Save This File to Disk**, and click **OK**.
9. Upload the key file, certificate file, and certificate authority file. To do so, open the Diva web interface and click **SIPcontrol configuration** on the left hand side to access the Diva SIPcontrol web interface.
10. Click **Security Profiles**, and then click **Details**.
11. Click **Browse** next to **Certificate authority file**, locate the folder where you stored the file, and click **Open** to upload the file.
12. Repeat Step 9 for the certificate file and the key file.
13. In the **Authentication mode** field, select how the server-client authentication should be handled.
14. Click **OK** to close the **Security Profiles** window.
15. At the bottom of the Diva SIPcontrol web interface, click **Activate Configuration** to save the configuration.
16. Since changes in the Security Profiles require a restart, click **System control** at the left hand side of the Diva web interface, and then click **Restart**.

CHAPTER 7

How Calls Are Processed

In the following discussion, SIP and PSTN endpoints/interfaces are interchangeable, and they may be used on no, one, or two sides of the call.

Diva SIPcontrol 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 holds Diva SIPcontrol 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 two endpoints of any type 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 holds 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 a SIP peer endpoint in the **SIP Peers** section.
- Settings PSTN Device 2 needs to be configured as a PSTN endpoint in the **PSTN Interfaces** section.
- Condition "called address is 3456" needs to be configured in the **Routing** section to route the call to the correct device.

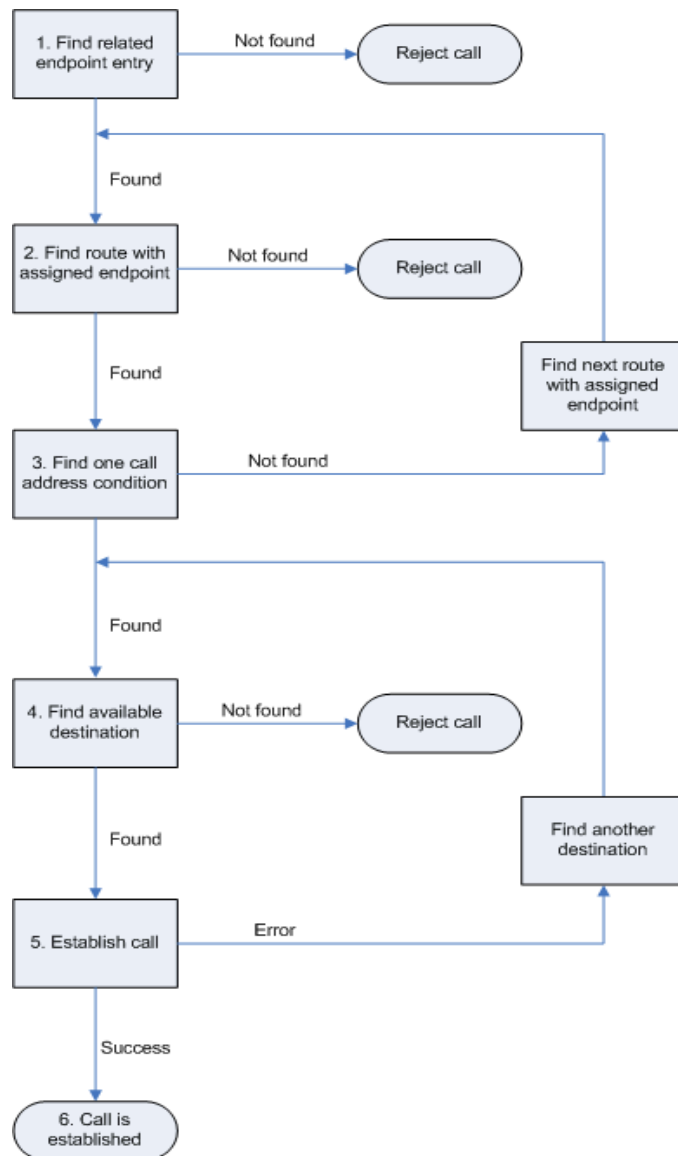
For example, if you have a SIP or PSTN Device 4 with no endpoints configured in Diva SIPcontrol, you cannot establish a call, because Diva SIPcontrol will not know the settings of the device.

The PSTN endpoint is found via its controller number. On the SIP side, multiple SIP peers can 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, Diva SIPcontrol looks for a SIP peer with the **Default SIP 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 [Information about Call Processing](#) below for more information.
5. Try to establish the call via this destination. If the destination is unavailable or rejects the call, try the next destination of the route. Note that the call will be aborted immediately if a cause code is received that signals final failure, e.g., user busy or unallocated number.
6. The call is established.



Information about Call Processing

- Each route can point to several destinations, between which Diva SIPControl 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 also matches the call criteria, only the first matching route is ever evaluated. Therefore, default routes should be created carefully and located at the end of the routing table, if appropriate.
- Load balancing/failover is only performed between the destinations of a single route.
- Routes without any conditions always match (as long as the source endpoint is listed in route sources).

Emergency Calls

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

This can be achieved by creating an additional route from any configured SIP peers to one or more PSTN interfaces and setting the called address condition 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

Diva SIPcontrol 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](#), as described below
- [Connecting Two SIP Peers to Two PSTN Interfaces Exclusively](#), as described on page 70
- [Connecting Two SIP Peers to the Same PSTN Interface](#), as described on page 71
- [Load Balancing or Failover between Two SIP Peers](#), as described on page 71

Direct Routing between One PSTN Interface and One SIP Peer

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

1. Under **PSTN Interfaces**, enable and configure all PSTN interfaces connected to a PBX. Confirm each dialog box with **OK**.
2. Under **SIP Peers**, create a SIP peer with the necessary settings, and make sure that the option **Default peer for received SIP calls** is enabled. Confirm with **OK**.
3. Under **Routing**, create Route 1 and do the following:
 - Select each required PSTN interface as a source peer.
 - Select the SIP peer configured in Step 2 as a Master destination.
 - Set the **Number format** field to **Unchanged**.
 - Confirm with **OK**.
4. Under **Routing**, create Route 2 and do the following:
 - Enable the SIP peer configured in Step 2 as a source peer.
 - Enable all required PSTN interfaces as Master destinations.
 - Set the **Number format** field to **Unchanged**.
 - Confirm with **OK**.
5. Save the configuration in the main configuration interface.

Direct Routing between Two SIP Peers

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

1. Under **SIP Peers**, create one SIP peer with the necessary settings, and make sure that the option **Default peer for received SIP calls** is enabled. Confirm with **OK**.
2. Under **SIP Peers**, create the other SIP peer with the necessary settings. Confirm with **OK**.
3. Under **Routing**, create Route 1 and do the following:
 - Select the SIP Peer configured in Step 1 as a source peer.
 - Select the SIP peer configured in Step 2 as a Master destination.
 - Set the **Number format** field to **Unchanged**.
 - Confirm with **OK**.
4. Under **Routing**, create Route 2 and do the following:
 - Select the SIP peer configured in Step 2 as a source peer.
 - Select the SIP peer configured in Step 1 as a Master destination.
 - Set the **Number format** field to **Unchanged**.
 - Confirm with **OK**.
5. Save the configuration in the main configuration interface.

Connecting 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 can 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 Interfaces**, enable and configure the two PSTN interfaces. Confirm with **OK**.
2. Under **SIP Peers**, create both SIP peers and make sure the entry in **Domain** exactly matches the domain used by the SIP peer in its SIP address for outgoing calls. Do not enable the option **Default peer for received SIP calls** for any of these peers. Confirm with **OK**.
3. Under **Routing**, create Route 1 and do the following:
 - Enable the first PSTN interface as a source peer.
 - Enable the first SIP peer configured in Step 2 as a Master destination.
 - Confirm with **OK**.
4. Under **Routing**, create Route 2. Then, repeat Step 3 for the second PSTN interface and the second SIP peer.
5. Under **Routing**, create Route 3 and do the following:
 - Enable the first SIP peer configured in Step 2 as a source peer.
 - Enable the first PSTN interface as a Master destination.
 - Confirm with **OK**.
6. Under **Routing**, create Route 4. Then, repeat Step 5 for the second PSTN interface and the second SIP peer.
7. Save the configuration in the main configuration interface.

Connecting Two SIP Peers to the Same PSTN Interface

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

1. Under **PSTN Interfaces**, enable and configure the PSTN interface. Confirm with **OK**.
2. Under **SIP Peers**, 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 peer for received SIP calls** for any of these peers. Confirm with **OK**.
3. Under **Routing**, create Route 1 and do the following:
 - Enable the first PSTN interface as a source peer.
 - Enable the first SIP peer configured in Step 2 as a Master destination.
 - Under **Conditions**, click **Add** and set the **Called address** to "1.*".
 - Confirm with **OK**.
4. Under **Routing**, create Route 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**, create Route 3 and do the following:
 - Enable both SIP peers as source peers.
 - Enable the first PSTN interface as a 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

To configure two servers for load balancing or failover, follow these steps:

1. Under **PSTN Interfaces**, enable and configure all required PSTN interfaces. Confirm with **OK**.
2. Under **SIP Peers**, create both SIP peers and make sure the entry in **Domain** exactly matches the domain used by the SIP peer in its SIP address for outgoing calls. Do not enable the option **Default peer for received SIP calls** for any of these peers. If you configure a failover, SIP peer 1 (a Master) should have the option **Alive check** enabled. Confirm with **OK**.
3. Under **Routing**, create Route 1 and do the following:
 - Enable the first PSTN interface as a source peer.
 - Enable the first SIP peer configured in Step 2 as a Master destination. For load-balancing configurations, SIP peer 2 should be configured as a Master destination. For failover configurations, it should be configured as a Slave destination.
 - Confirm with **OK**.
4. Under **Routing**, create Route 2 and do the following:
 - Enable both SIP peers as source peers.
 - Enable the first PSTN interfaces as a Master destination.
 - Confirm with **OK**.
5. Save the configuration in the main configuration interface.
6. Under **Routing**, create Route 2 and repeat Step 3 for the second SIP peer with the only difference that the called address condition for this route is 2.*.

7. Under **Routing**, create Route 3 and do the following:
 - Enable both SIP peers as source peers.
 - Enable the first PSTN interface as a Master destination.
 - Confirm with **OK**.
8. Save the configuration in the main configuration interface.

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

CHAPTER 8

How Address Maps Are Processed

Address maps are processed as follows:

1. Get the first map rule of the address map.
2. Verify whether the called, calling, and redirect conditions each match the respective parts of the call addresses (or are empty). If not, verify the next map rule.
3. If all conditions match, apply each result setting of the rule to the respective address match.
4. If the option **Stop on match** is enabled, stop processing. Otherwise, continue with the next rule as described in Step 2.

CHAPTER 9

How Call Addresses Are Processed

The call addresses provided by the caller can be modified at different stages of the call processing within Diva SIPcontrol. 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.

When using a dialplan, Diva SIPcontrol converts addresses automatically, without any intervention from the user. This means that Diva SIPcontrol adds or removes a special prefix to a number with a known number type when converting between a number and an address. The automatic conversions are done for calling numbers, called numbers, and redirected numbers. See [Common Results](#) on page 79 for a list of prefixes.

For complex conversions, you can configure an address map for Diva SIPcontrol to use when converting addresses.

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 the 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 can also receive calls to other numbers (via other routes) without having to deal with different number formats.
- SIP peer "A" needs the dialed numbers to be formatted in E.164 format, while SIP peer "B", which is in load-balancing or fail-over partnership with "A", needs it in an extension-only format.
Solution: Define different number formats in the SIP peer settings.
- SIP peer "A" is located at a different location than SIP peer "B", e.g., London and Stuttgart. Therefore, both need different location settings regarding country and area codes, etc.
Solution: Create different dialplans and assign each dialplan to one SIP peer.

How Addresses Are Manipulated

Diva SIPcontrol manipulates call addresses as follows:

Note: Each step is optional, depending on the configuration.

1. Saves the inbound call addresses as "A".
2. Applies the "address map inbound" of the endpoint assigned to the call setup request to "A", resulting in "B".
3. To check the first route: applies the number format settings of the route together with the dialplan of the source endpoint to the call addresses "B", resulting in "C".
4. Checks the route against addresses "C". If the route does not match, Diva SIPcontrol discards the changes and tries the next route with "B" again. For information about routes, see [Routing](#) on page 41.
5. If the route matches, Diva SIPcontrol applies the route address map to the addresses "C", resulting in "D".
6. After selecting one of the destinations of the route, Diva SIPcontrol normalizes the addresses "D" using the dialplan and number format of the destination endpoint, resulting in addresses "E".
7. Applies 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 there are other endpoints in a fail-over configuration, Diva SIPcontrol starts with Step 6 again with the respective settings of the next endpoint.

CHAPTER 10

How Numbers Are Processed

Diva SIPcontrol provides two mechanisms for number processing. Both mechanisms can be used together:

1. [Number Normalization Based on a Dialplan](#) as described below.
2. [Number Modification Using Regular Expressions](#) as described on page 78.

Number Normalization Based on a Dialplan

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

Diva SIPcontrol also supports dialplans using the North American numbering plan (NANP). See [North-American numbering plan](#) on page 52 for more information.

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 result. Six target results 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 a different country code will be converted to an international number with a prefix for international calls and an outside access digit, if required.
 - **National number with number type:** If possible, all numbers are converted to a national number with the number type flag set to "national". Exception: Numbers with a different country code will be converted to an international number with the number type set to "international". **Note:** This target result 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 result 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 Diva SIPcontrol, 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 Diva SIPcontrol expects the outside access digit in the calling number in external calls from the PBX. The PBX normally prepends the outside access digit to the calling number in incoming external calls in order to enable callback functionality at internal phones. If this is the case, enable this option.
 - **PSTN access code provided by the SIP caller:** This option defines whether Diva SIPcontrol expects the outside access digit in the called number of external calls. It is normally required to prepend the outside access digit to call an external number from an internal phone. However, in some configurations this is not required, such as a configuration that is part of the North American numbering plan (NANP), where an internal number can be identified based on its length.

Enable this option if the internal users that use SIPcontrol for external calls prepend the outside access digits in their calls; otherwise disable it.

- Diva SIPcontrol's number normalization function does not remove outside access digits like a PBX can for external calls. If Diva SIPcontrol needs to behave like a PBX with an outside access digit for external calls, use the address map functionality in combination with a route.

Number Modification Using Regular Expressions

Diva SIPcontrol organizes regular conditions into address maps, and each endpoint or route can be assigned one map. Each address map contains a number of regular conditions together with the respective output result strings. This helps to ensure 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. Therefore, these PSTN interfaces can share an address map that Diva SIPcontrol lets you assign for each individual controller.

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

Common Conditions:

Character	Meaning
.	Matches any character
^	Matches the beginning of an address
\$	Matches the end of an address
\+	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-condition to be referenced in result string and also groups sets of characters
	Alternate operator, matches either the left or right sub-condition
[]	Matches any character given within the square brackets, i.e [123] matches either 1, 2, or 3, but not 4, 5, or 123.
(?i)	Considers case for everything after the tag. For example "username@(?)i hostname.tld" matches "username\$HOSTNAME.TLD" and "username@hostname.TLD", but not "USERNAME@hostname.tld".

Common Results

Character	Meaning
0-9, +	Inserts the respective character into the output
(?n(digits))	Inserts the digits given only if the n th sub-condition of the condition matched
\$&	Outputs what matched the whole condition
\$n	Outputs the n th matched sub-condition
\$(S)	Inserts the current calling (source) number
\$(D)	Inserts the called (destination) number
\$(R)	Inserts the first redirected number
\$(R2)	Inserts the second redirected number
\$(Rn)	Inserts the n th redirected number (up to the 9th)

Examples

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

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

Omit the Prefix Digits

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

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

Address Condition: ^33

Address Result: (none)

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

Add the Prefix Digits

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

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

Address Condition: .*

Address Result: 9\$&

Replace the International Number Type by Prefix

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

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

Address Condition: .*

Address Result: 01\$&

Number type Condition: International

International Dial Prefix by Number Type

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

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

Address Condition: ^01

Address Result: (none)

Number type Condition: Unknown

Number type Result: International

Replace an Extension by Another

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

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

First Address Condition: 1111(@.*)?\$

First Address Result: 2222

Stop on Match: true

Second Address Condition: 3333(@.*)?\$

Second Result Condition: 4444

Stop on Match: true

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

Replace the National Number Type with a Prefix

Task: Replace the National number type in a national number with the national prefix 0.

Example: National number 123-45678 should be signaled as 0123-45678

Address Condition: .*

Address Result: 0\$&

Number type Condition: National

Number type Result: Unknown

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

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

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

Example: Present the phone number 727-0203 without E.164. The local area code is +1(123).

Address Condition: ^(.*)

Address Result: \$1;phone-context=+1(123)\$1

CHAPTER 11

Cause Code Mapping

If Diva SIPcontrol uses Microsoft® Office Communications Server 2007 or Lync Server 2010 as a SIP peer, the cause/response code tables are used as specified by Microsoft. See [Default Cause Code Mapping for Microsoft® Office Communications Server 2007 and Lync Server 2010 Peers](#) on page 83 for a detailed list of cause/response codes.

If Diva SIPcontrol does not use Microsoft® Office Communications Server 2007 or Lync Server 2010, the default cause/response code mapping is used. See [Default Cause Code Mapping](#) below for a detailed list of cause/response codes.

Default Cause Code Mapping

Diva SIPcontrol 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 Maps** section.

For ISDN to SIP code mappings, see [ISDN Cause Code to SIP Response Code](#), below.

For SIP to ISDN code mappings, see [SIP Response Code to ISDN Cause Code](#) on page 82.

ISDN Cause Code to SIP Response Code

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

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

SIP Response Code to ISDN Cause Code

SIP response code from the SIP peer	Description	ISDN cause code	Description
400	Bad Request	41	Temporary failure
401	Unauthorized	21	Call rejected
402	Payment required	21	Call rejected
403	Forbidden	21	Call rejected
404	Not found	1	Unallocated number
405	Method not allowed	63	Service or option unavailable
406	Not acceptable	79	Service/option not implemented
407	Proxy authentication required	21	Call rejected
408	Request timeout	41	Temporary failure
410	Gone	22	Number changed
413	Request entity too large	63	Service or option unavailable
414	Request-URI too long	63	Service or option unavailable
415	Unsupported media type	79	Service/option not implemented
416	Unsupported URI scheme	79	Service/option not implemented
420	Bad extension	79	Service/option not implemented
421	Extension required	79	Service/option not implemented
423	Interval too brief	63	Service or option unavailable
429	Provide Referrer Identity	31	Normal, unspecified

SIP response code from the SIP peer	Description	ISDN cause code	Description
480	Temporarily unavailable	19	No answer from the user
481	Call/transaction does not exist	41	Temporary failure
482	Loop detected	25	Exchange routing error
483	Too many hops	25	Exchange routing error
484	Address incomplete	28	Invalid number format (address incomplete)
485	Ambiguous	1	Unallocated number
486	Busy here	17	User busy
487	Request Terminated	127	Interworking, unspecified
488	Not acceptable here	65	Bearer capability not implemented
500	Server internal error	41	Temporary failure
501	Not implemented	79	Service/option not implemented
502	Bad gateway	38	Network out of order
503	Service unavailable	63	Service or option unavailable
504	Server time-out	41	Temporary failure
505	Version not supported	79	Service/option not implemented
513	Message too large	63	Service or option unavailable
600	Busy everywhere	17	User busy
603	Decline	21	Call rejected
604	Does not exist anywhere	1	Unallocated number
606	Not acceptable	65	Bearer capability not implemented
Any code other than listed above:		31	Normal, unspecified

Default Cause Code Mapping for Microsoft® Office Communications Server 2007 and Lync Server 2010 Peers

Diva SIPcontrol includes a default cause/response code mapping table for Microsoft® Office Communications Server 2007 SIP peers and Lync Server 2010 SIP peers that includes the most common (as of the date of publication of this document) cause codes according to RFC 3398 and RFC 4497. If you need to define a cause code mapping other than in the table, you can configure it in the Cause Code Maps section, as described in [Cause Code Maps](#) on page 57.

For ISDN to SIP code mappings, see [Microsoft® Office Communications Server 2007 and Lync Server 2010 ISDN Cause Code to SIP Response Code](#) on page 84.

For SIP to ISDN code mappings, see [Microsoft® Office Communications Server 2007 and Lync Server SIP Response Code to ISDN Cause Code](#) on page 85.

Microsoft® Office Communications Server 2007 and Lync Server 2010 ISDN Cause Code to SIP Response Code

ISDN cause code	Description	SIP response code forwarded to Microsoft® Office Communications Server 2007 or Lync Server 2010	Description
1	Unallocated number	404	Not found
2	No route to specified transit network	404	Not found
3	No route to destination	404	Not found
16	Normal call clearing	603	Decline (The PBX of Philips sends this code during call set-up if the user rejects the call.)
17	User busy	486	Busy here
18	No user response	408	Request timeout
19	No answer from the user	480	Temporarily unavailable
20	Subscriber absent	480	Temporarily unavailable
21	Call rejected	603	Decline
22	Number changed	410	Gone
23	Redirection to new destination	410	Gone
26	Non-selected user clearing	404	Not found
27	Destination out of order	502	Bad gateway
28	Address incomplete	484	Address incomplete
29	Facility rejected	501	Not implemented
31	Normal, unspecified	480	Temporarily unavailable
34	No circuit available	503	Service unavailable
38	Network out of order	503	Service unavailable
41	Temporary failure	503	Service unavailable
42	Switching equipment congestion	503	Service unavailable
47	Resource unavailable	503	Service unavailable
55	Incoming class barred within Closed User Group (CUG)	403	Forbidden
57	Bearer capability not authorized	403	Forbidden
58	Bearer capability not presently available	503	Service unavailable
65	Bearer capability not implemented	488	Not acceptable here
69	Requested Facility not implemented	501	Not implemented
70	Only restricted digital available	488	Not acceptable here
79	Service or option not implemented	501	Not implemented
87	User not member of Closed User Group (CUG)	403	Forbidden
88	Incompatible destination	400	Bad request
102	Recover on Expires timeout	504	Server time-out
111	Protocol error	503	Service unavailable

ISDN cause code	Description	SIP response code forwarded to Microsoft® Office Communications Server 2007 or Lync Server 2010	Description
127	Interworking, unspecified	500	Server internal error
Any code other than listed above:		500	Server internal error

Microsoft® Office Communications Server 2007 and Lync Server SIP Response Code to ISDN Cause Code

SIP response code from Microsoft® Office Communications Server 2007 or Lync Server 2010	Description	ISDN cause code	Description
400	Bad Request	41	Temporary failure
401	Unauthorized	21	Call rejected
402	Payment required	21	Call rejected
403	Forbidden	21	Call rejected
404	Not found	1	Unallocated number
405	Method not allowed	63	Service or option unavailable
406	Not acceptable	79	Service/option not implemented
407	Proxy authentication required	21	Call rejected
408	Request timeout	102	Recovery on timer expiry
410	Gone	22	Number changed
413	Request entity too large	127	Interworking, unspecified
414	Request-URI too long	127	Interworking, unspecified
415	Unsupported media type	79	Service/option not implemented
416	Unsupported URI scheme	127	Interworking, unspecified
420	Bad extension	127	Interworking, unspecified
421	Extension required	127	Interworking, unspecified
423	Interval too brief	127	Interworking, unspecified
429	Provide Referrer Identity	31	Normal, unspecified
480	Temporarily unavailable	18	No user responding
481	Call/transaction does not exist	41	Temporary failure
482	Loop detected	25	Exchange routing error
483	Too many hops	25	Exchange routing error
484	Address incomplete	28	Invalid number format (address incomplete)
485	Ambiguous	1	Unallocated number
486	Busy here	17	User busy
487	Request Terminated	127	Interworking, unspecified
488	Not acceptable here	65	Bearer capability not implemented
500	Server internal error	41	Temporary failure
501	Not implemented	79	Service/option not implemented

SIP response code from Microsoft® Office Communications Server 2007 or Lync Server 2010	Description	ISDN cause code	Description
502	Bad gateway	38	Network out of order
503	Service unavailable	41	Temporary failure
504	Server time-out	102	Recovery on timer expiry
505	Version not supported	127	Interworking, unspecified
513	Message too large	127	Interworking, unspecified
600	Busy everywhere	17	User busy
603	Decline	21	Call rejected
604	Does not exist anywhere	1	Unallocated number
606	Not acceptable	65	Bearer capability not implemented
Any code other than listed above.		31	Normal, unspecified

CHAPTER 12

Software Uninstallation

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

The uninstallation procedure depends on the installed operating system.

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

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

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

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

CHAPTER 13

Event Logging

A computer with Diva SIPcontrol installed can write the following types of events into the System Event Log:

- [Errors](#)
- [Warnings](#)
- [Informational Messages](#)

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

Errors

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

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

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

Warnings

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

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

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

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

CHAPTER 14

Use Case Examples

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

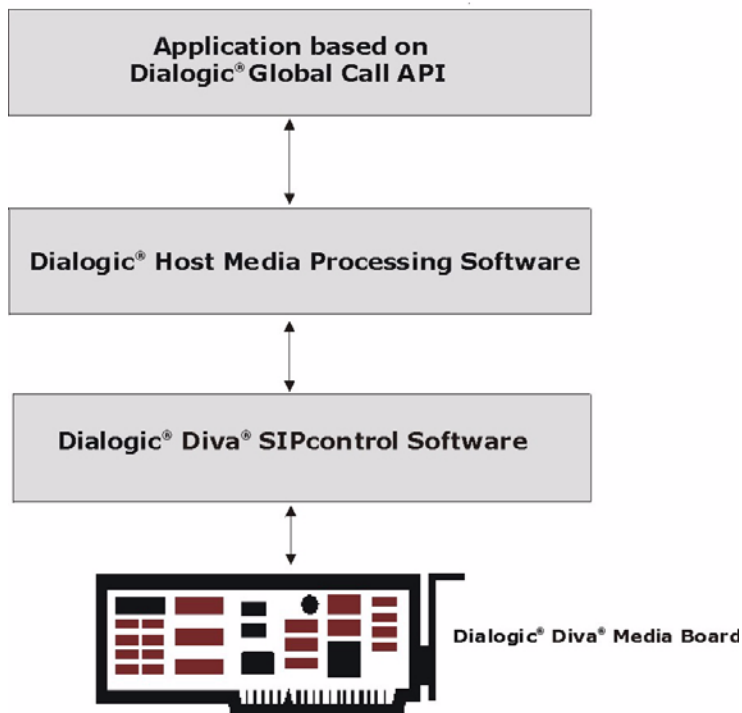
The following scenarios describe configurations for a gateway computer with:

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

The gateway computer is a server with a Diva Media Board and Diva SIPcontrol installed. The use cases are based on Diva SIPcontrol version 2.5.

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 Diva SIPcontrol, as shown in the graphic below. However, Diva SIPcontrol also supports the interoperability with HMP over the LAN. The use case is based on HMP version 3.0WIN and 3.1LIN. In order for the application based on the Dialogic® Global Call API to connect with Diva SIPcontrol, 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.



For this configuration scenario, the network interface, one SIP peer, and two routes need to be configured.

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

1. Open the Diva SIPcontrol 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.

3. Under **Network Interfaces**, enable the local loopback interface by enabling one or more listen ports, and enter **9803** for the UDP and TCP listen ports:

Network Interfaces						
Name	Device	IP address	UDP listen port	TCP listen port	TLS listen port	
Intel(R) PRO1000 GT Desktop	Intel(R) PRO1000 GT Desktop Adapter - Packet Scheduler Miniport	192.168.213.38	5060 ☐	5060 ☐	5061 ☐	
Local Loopback Interface	Local Loopback Interface	127.0.0.1	9803 ☒	9803 ☒	0 ☐	

4. Under **SIP Peers**, click **Add new peer**, and configure the following parameters:

General	
Name:	HMP
Peer type:	Default
Host:	127.0.0.1
Port:	5060
IP protocol:	UDP
URI scheme:	SIP (default)
Domain:	

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

In the **Enhanced** section, enable **Default peer for received SIP calls**:

Enhanced	
Default peer for received SIP calls:	☒
Display name to:	
Display name from:	
User name to:	
User name from:	
Gateway prefix:	
Reply-To expression:	
Reply-To format:	
Force T.38 reinvite:	☐
Alive check:	☐ 0 seconds (0=auto)
Disconnect tone support:	☐
Cause code mapping inbound:	peer default
Cause code mapping outbound:	peer default
Codec profile:	default
Maximum channels:	120
Early media support:	☒
Reliable provisional response:	Optional

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

5. Create two routes: one for each direction (SIP to PSTN and PSTN to SIP).

- Configure the SIP to PSTN route. To do so, open the **Routing** section, click **Add**, and configure the following parameters:

General		
Name:	SIP to HMP	
Type: Name	Source	Destination
PSTN: Controller1	☐	Master
PSTN: Controller2	☐	Master
SIP: HMP	☒	-
Max. call attempts for this route in a failover scenario:	0 (0 = try all selected destinations)	

- Name:** Enter a unique name to easily identify the route.
- Source:** Select the configured SIP peer as a source.
- Destination:** Select the controllers of the Diva Media Board as Master destinations.

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

- Configure the SIP to PSTN route. To do so, click **Add** again, and configure the following parameters:

General		
Name:	HMP to SIP	
Type: Name	Source	Destination
PSTN: Controller1	☒	-
PSTN: Controller2	☒	-
SIP: HMP	☐	Master
Max. call attempts for this route in a failover scenario:	0 (0 = try all selected destinations)	

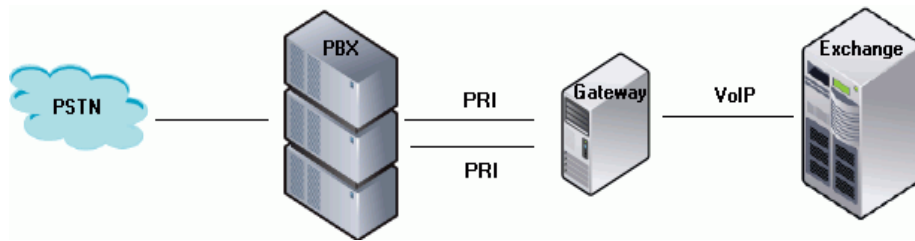
- Name:** Enter a unique name to easily identify the route.
- Source:** Select the controllers of the Diva Media Board as sources.
- Destination:** Select the configured SIP peer as a Master destination.

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

6. Click **Activate Configuration** on the main configuration page to save the settings and activate the changes.

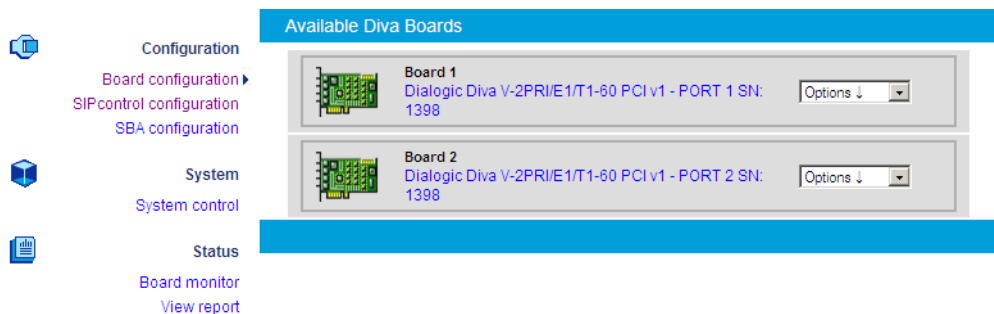
Use Case for Microsoft® Exchange Server 2007

This configuration scenario describes the necessary steps for configuring the gateway computer between the PBX and the Microsoft® Exchange Server 2007, as shown below.



For this configuration scenario, the PSTN interface, the network interface, one SIP peer, and one route need to be configured.

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



3. Click either the board icon or the name of the Diva Media Board to access the board configuration options.
4. Configure the **D-Channel Protocol** of the PBX. In this example, **PBX, QSIG E1-(QSIG)** is selected:

Dialogic Diva V-2PRI/E1/T1-60 PCI v1 - PORT 1, SN:1398	
Parameter	Value
D-Channel Protocol:	PBX, QSIG E1 - (QSIG)
Interface Mode/Resource Board:	TE - mode
Direct Dial In (NT2):	Yes
DDI Number Length:	3
DDI Collect Timeout:	0
DDI Special Number:	
Layer 1 Framing:	National default (default)
Layer 2 Connect Mode:	Permanent
Voice Companding:	Force A-Law
View Extended Configuration	No

5. Click **Save**.
6. Repeat Steps 2 through 5 for the other PRI line.
7. In the Diva SIPcontrol web interface, click **SIPcontrol configuration** on the left hand side to open the **SIPcontrol Configuration** page.

8. In the **Network Interfaces** section, set the listen ports of your Ethernet adapter to **5060**, and enable the listen port by checking the associated check box:

Network Interfaces					
Name	Device	IP address	UDP listen port	TCP listen port	TLS listen port
Intel(R) PRO1000 GT Desktop	Intel(R) PRO1000 GT Desktop Adapter - Packet Scheduler Miniport	192.168.213.38	5060 ☒	5060 ☒	5061 ☐
Local Loopback Interface	Local Loopback Interface	127.0.0.1	5060 ☐	5060 ☐	0 ☐

9. Configure the SIP peer settings. To do so, open the **SIP Peers** section, click **Add new peer**, and configure the following parameters:

General	
Name:	MS Exchange
Peer type:	MS Exchange 2007
Host:	IP address of UM server
Port:	5060
IP protocol:	TCP
URI scheme:	SIP (default)
Domain:	

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

In the **Enhanced** Section, enable **Default peer for received SIP calls**:

Enhanced	
Default peer for received SIP calls:	☒
Display name to:	
Display name from:	
User name to:	
User name from:	
Gateway prefix:	
Reply-To expression:	
Reply-To format:	
Force T.38 reinvoke:	☐
Alive check:	☐ 0 seconds (0=auto)
Disconnect tone support:	☐
Cause code mapping inbound:	peer default
Cause code mapping outbound:	peer default
Codec profile:	default
Maximum channels:	480
Early media support:	☒
Reliable provisional response:	Optional

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

10. Configure one PSTN to SIP route and one SIP to the PSTN route.

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

General		
Name:	PSTN-SIP-Exchange	
Type: Name	Source	Destination
PSTN: Controller1	☒	-
PSTN: Controller2	☒	-
SIP: MS-Exchange	☐	Master
Max. call attempts for this route in a failover scenario:	0 (0 = try all selected destinations)	

- Name:** Enter a unique name to easily identify the route.
- Source:** Select both controllers as sources.
- Destination:** Select the SIP peer configured above as a Master destination.

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

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

General		
Name:	SIP-PSTN-Exchange	
Type: Name	Source	Destination
PSTN: Controller1	☐	Master
PSTN: Controller2	☐	Master
SIP: MS-Exchange	☒	-
Max. call attempts for this route in a failover scenario:	0 (0 = try all selected destinations)	

- Name:** Enter a unique name to easily identify the route.
- Source:** Select the SIP peer configured above as a source.
- Destination:** Select both controllers as Master destinations.

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

11. Click **Activate Configuration** in the main configuration page to save the settings and activate the changes.

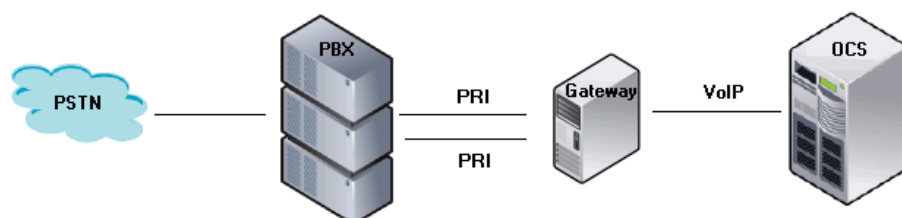
Use Cases for Microsoft® Office Communications Server 2007

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

- [Using the Gateway Computer Between the PBX and Microsoft® Office Communications Server 2007](#): Both lines of the Diva Media Board are connected between the PBX and the Microsoft® Office Communications Server 2007.
- [Using the Gateway Computer Between the PBX/PSTN and Microsoft® Office Communications Server 2007](#): One line of the Diva Media Board is connected to the PBX and one line is connected directly to the PSTN. The gateway computer is connected to the Microsoft® Office Communications Server 2007.
- [Using the Gateway Computer Between the PSTN and PBX/Microsoft® Office Communications Server 2007](#): One line of the Diva Media Board is connected to the PBX and one line is connected to the PSTN. The gateway computer is connected between the PSTN and the PBX. The Microsoft® Mediation Server is installed on the gateway computer.

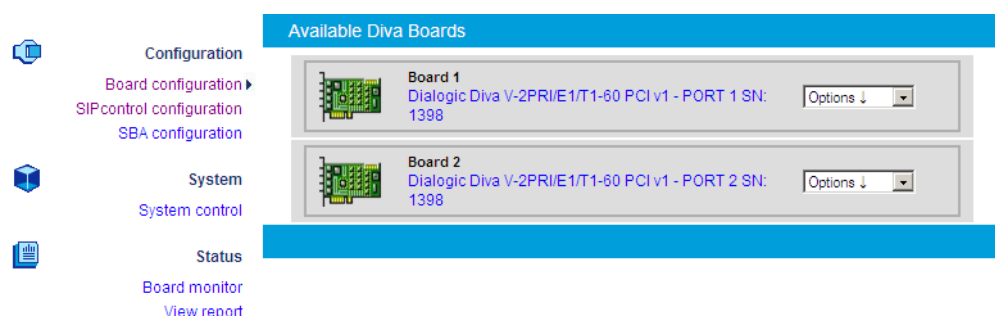
Using the Gateway Computer Between the PBX and Microsoft® Office Communications Server 2007

This configuration scenario describes the necessary steps for configuring the gateway computer between the PBX and the Microsoft® Office Communications Server 2007, as shown below:



For this configuration scenario, one dialplan, the PSTN interface, the network interface, one SIP peer, and one route need to be configured.

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



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

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

Dialogic Diva V-2PRI/E1/T1-60 PCI v1 - PORT 1, SN:1398	
Parameter	Value
D-Channel Protocol:	PBX, QSIG E1 - (QSIG)
Interface Mode/Resource Board:	TE - mode
Direct Dial In (NT2):	Yes
DDI Number Length:	3
DDI Collect Timeout:	0
DDI Special Number:	
Layer 1 Framing:	National default (default)
Layer 2 Connect Mode:	Permanent
Voice Companding:	Force A-Law
View Extended Configuration	No

Save **Cancel**

- Repeat Steps 2 through 4 for the other PRI line.
- In the Diva SIPcontrol web interface, click **SIPcontrol configuration** on the left hand side to open the **SIPcontrol Configuration** page.
- Under **Dialplans**, click **Add**, and enter the following parameters:

General	
Name:	Dialplan-PBX
Country code:	49
North-American numbering plan:	☐
Area code:	7159 With national prefix
Other local areas:	
Base number:	4066
Maximum extension digits:	4
International prefix:	00
National prefix:	0
Access code:	0
PSTN access code provided by SIP caller:	☒
Incoming PSTN access code provided by PBX:	☒

OK **Cancel**

- Name:** Enter a unique name to easily identify the dialplan.
- Country code:** Enter the country code of the country in which the gateway computer is located.
- Area code:** Enter the area code of the region in which the gateway computer is located.
- Base number:** Enter the subscriber or trunk number.

- **Maximum extension digits:** Select the maximum number of extension digits that are provided.
- **International prefix:** Enter the international prefix of the country in which the gateway computer is located.
- **National prefix:** Enter the national prefix that needs to be dialed for long distance calls within the country in which the gateway computer is located.
- **Access code:** Enter the digit that is necessary to access the public network.
- Enable the options **PSTN access code provided by SIP caller** and **Incoming PSTN access code provided by PBX**.

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

- Under **PSTN Interfaces**, configure the first Diva Media Board line. To do so, click **Details** at the right and configure the following parameters:

General	
Hardware description:	Dialogic Diva V-2PRI/E1/T1-60 PCI v1 - PORT 1 SN: 1398
PSTN interface number:	1
Name:	Controller1
Address map inbound:	none
Address map outbound:	none

Enhanced	

Address Normalization	
Dialplan:	Dialplan-PBX
Type of number (outbound):	Extension
Encoding (outbound):	Use prefixes
ISDN numbering plan - Default:	unknown
Presentation indicator - Default:	Allowed
Internal interface:	☐

- **Dialplan:** Select the configured dialplan.
- **Type of number (outbound):** Select **Extension**.
- **Encoding (outbound):** Select **Use prefixes**.
- Leave the remaining parameters at their default values.

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

- Configure the second line with the same settings as the first line.

- Under **Network Interfaces**, enable your Ethernet adapter, and set the SIP listen ports to **9803**.

Network Interfaces					
Name	Device	IP address	UDP listen port	TCP listen port	TLS listen port
Intel(R) PRO1000 EB Network	Intel(R) PRO/1000 EB Network Connection with I/O Acceleration #2	172.16.22.144	9803 ☒	9803 ☒	☐
Intel(R) PRO1000 EB Network1	Intel(R) PRO/1000 EB Network Connection with I/O Acceleration	10.242.202.134	☐	☐	☐
Local Loopback Interface	Local Loopback Interface	127.0.0.1	☐	☐	☐
RTP start port:	30000				
RTP end port:	39999				

11. Under **SIP Peers**, click **Add new peer**, and configure the following parameters:

General	
Name:	OCS-Mediation-Server
Peer type:	MS OCS 2007/2007 R2 - Mediation Server
Host:	172.16.22.144
Port:	5060
IP protocol:	TCP
URI scheme:	SIP (default)
Domain:	default routing domain of OCS

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

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

12. Create one PSTN to SIP route and one SIP to PSTN route. To do so, click **Routing** and click **Add** to open the routing options.

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

General		
Name:	PSTNto-SIP	
Type: Name	Source	Destination
PSTN: Controller1	☒	-
PSTN: Controller2	☒	-
SIP: OCS-Mediation-Server	☐	Master
Max. call attempts for this route in a failover scenario:	0 (0 = try all selected destinations)	

Address Normalization For Condition Processing (Using Source Dialplan)	
Use Dialplan:	☒
Number format:	International number
Encoding:	Use type flag

- **Name:** Enter a unique name to easily identify the route.
- **Source:** Select both controllers of the Diva Media Board as sources.

Under **Address Normalization for Condition Processing (Using Source Dialplan)**, configure the following parameters:

- **Destination:** Select the above configured SIP peer as a Master destination.
- **Number format:** Select **International number** from the dropdown menu.
- **Encoding:** Select **Use type flag** from the dropdown menu.

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

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

General		
Name:	SIP4to-PSTN	
Type: Name	Source	Destination
PSTN: Controller1	☐	Master ▼
PSTN: Controller2	☐	Master ▼
SIP: OCS-Mediation-Server	☒	- ▼
Max. call attempts for this route in a failover scenario:	0 (0 = try all selected destinations)	

Address Normalization For Condition Processing (Using Source Dialplan)	
Use Dialplan:	☒
Number format:	Unchanged ▼
Encoding:	Use prefixes ▼

- **Name:** Enter a unique name to easily identify the route.
- **Source:** Select the configured SIP peer as a source.
- **Destination:** Select both controllers of the Diva Media Board as Master destinations.

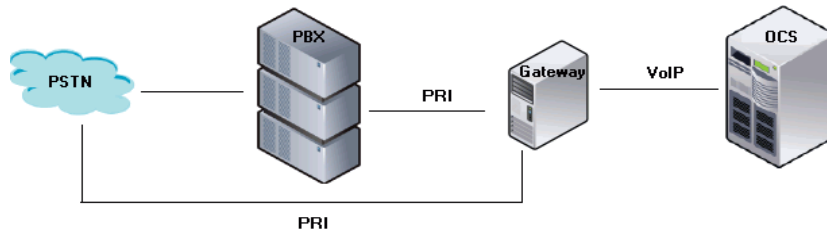
Click **OK** to save the settings and close the window.

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

14. Configure Microsoft® Office Communications Server 2007.

Using the Gateway Computer Between the PBX / PSTN and Microsoft® Office Communications Server 2007

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



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

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



3. Click either the board icon or the name of the first Diva Media Board to access the board configuration options.
4. Configure the **D-Channel Protocol** of port 1. In the example, **PBX. QSIG E1 - (Q.SIG)** is selected.

Dialogic Diva V-2PRI/E1/T1-60 PCI v1 - PORT 1, SN:1398

Parameter	Value
D-Channel Protocol:	PBX, QSIG E1 - (Q.SIG)
Interface Mode/Resource Board:	TE - mode
Direct Dial In (NT2):	Yes
DDI Number Length:	3
DDI Collect Timeout:	0
DDI Special Number:	
Layer 1 Framing:	National default (default)
Layer 2 Connect Mode:	Permanent
Voice Companding:	Force A-Law
View Extended Configuration	No

Save Cancel

5. Click **Save**.
6. Click **Board configuration** again, and select port 2 of your Diva Media Board to access the board configuration options.

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

Dialogic Diva V-2PRI/E1/T1-60 PCI v1 - PORT 2, SN:1398

Parameter	Value
D-Channel Protocol:	Europe/other countries, Euro-ISDN (ETSI-DSS1) - (ETSI)
Interface Mode/Resource Board:	TE - mode
Direct Dial In (NT2):	Yes
DDI Number Length:	3
DDI Collect Timeout:	0
DDI Special Number:	
Layer 1 Framing:	National default (default)
Layer 2 Connect Mode:	Permanent
Voice Companding:	Force A-Law
View Extended Configuration	No

Save Cancel

8. Click **Save**
9. In the Diva SIPcontrol web interface, click **SIPcontrol configuration** on the left hand side to open the **SIPcontrol Configuration** page.
10. Configure two dialplans; one for the line connected to the PBX and one for the line connected directly to the PSTN.
- To create the dialplan for the line connected to the PBX, open the **Dialplans** section, click **Add**, and configure the following parameters:

General

Name:	Dialplan-at-PBX
Country code:	49
North-American numbering plan:	☐
Area code:	7159 With national prefix
Other local areas:	
Base number:	4066
Maximum extension digits:	4
International prefix:	00
National prefix:	0
Access code:	0
PSTN access code provided by SIP caller:	☒
Incoming PSTN access code provided by PBX:	☒

OK Cancel

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

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

- To configure the dialplan for the line connected directly to the PSTN, click **Add** again, and configure the following parameters.

General	
Name:	Dialplan-at-PSTN
Country code:	49
North-American numbering plan:	☐
Area code:	7159 With national prefix
Other local areas:	
Base number:	4066
Maximum extension digits:	4
International prefix:	00
National prefix:	0
Access code:	
PSTN access code provided by SIP caller:	☒
Incoming PSTN access code provided by PBX:	☒
OK Cancel	

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

- **National prefix:** Enter the national prefix that needs to be dialed for long distance calls within the country in which the gateway computer is located.

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

11. Under **PSTN Interfaces**, configure Controller 1 with the PBX-specific settings and Controller 2 with the PSTN-specific settings. The controller number that you configure with the PBX-specific settings needs to correspond to the line number in the Diva Configuration Manager on which you configured the switch type of your PBX. Similarly, the controller number that you configure with the PSTN-specific settings needs to correspond to the line number in the Diva Configuration Manager on which you configured the switch type of your PSTN line.

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

General	
Hardware description:	Dialogic Diva V-2PRI/E1/T1-60 PCI v1 - PORT 1 SN: 1033
PSTN interface number:	1
Name:	Controllerto-PBX
Address map inbound:	none
Address map outbound:	none
Enhanced	
Address Normalization	
Dialplan:	Dialplan-at-PBX
Type of number (outbound):	Extension
Encoding (outbound):	Use prefixes
ISDN numbering plan - Default:	unknown
Presentation Indicator - Default:	Allowed
Internal interface:	☐
PSTN Call Transfer Settings	
Message Waiting Indication (MWI)	
OK Cancel	

- **Dialplan:** Select the dialplan you configured for the PBX.
- **Type of number (outbound):** Select **Extension**.
- **Encoding (outbound):** Select **Use prefixes**.

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

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

General	
Hardware description:	Dialogic Diva V-2PRI/E1/T1-60 PCI v1 - PORT 2 SN: 1033
PSTN interface number:	2
Name:	Controller-to-PSTN
Address map inbound:	none
Address map outbound:	none

Enhanced	
Address Normalization	
Dialplan:	Dialplan-at-PSTN
Type of number (outbound):	National number
Encoding (outbound):	Use prefixes
ISDN numbering plan - Default:	unknown
Presentation indicator - Default:	Allowed
Internal interface:	☐

PSTN Call Transfer Settings	
Message Waiting Indication (MWI)	

OK Cancel

- Dialplan**: Select the dialplan you configured for the PSTN
- Type of number (outbound)**: Select **National number**.
- Encoding (outbound)**: Select **Use prefixes**.

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

- Under **Network Interfaces**, enable your Ethernet adapter, and set the SIP listen ports to **9803**.

Network Interfaces					
Name	Device	IP address	UDP listen port	TCP listen port	TLS listen port
Intel(R) PRO1000 EB Network	Intel(R) PRO/1000 EB Network Connection with I/O Acceleration #2	172.16.22.144	9803 ☒	9803 ☒	☐
Intel(R) PRO1000 EB Network 1	Intel(R) PRO/1000 EB Network Connection with I/O Acceleration	10.242.202.134	☐	☐	☐
Local Loopback Interface	Local Loopback Interface	127.0.0.1	☐	☐	☐

RTP start port:	30000
RTP end port:	39999

13. Under **SIP Peers**, click **Add new peer**, and configure the following parameters:

General	
Name:	OCS-Mediation-Server
Peer type:	MS OCS 2007/2007 R2 - Mediation Server
Host:	172.16.22.144
Port:	5060
IP protocol:	TCP
URI scheme:	SIP (default)
Domain:	default routing domain of OCS
Enhanced	
Security	
Session Timer	
Address Normalization	
Dialplan:	Dialplan-at-PBX
Number format (outbound):	Unchanged
Encoding (outbound):	Use prefixes
Address map inbound:	none
Address map outbound:	none
Authentication	
OK Cancel	

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

Under **Address Normalization**, select the dialplan you configured for the controller connected to the PBX. Click **OK** to save the settings and close the window.

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

General		
Address map name:	SIP-to-PSTN-Address-Map	
Rule name:	Remove Outside Access Digit	
Stop on match:	☐	
Enhanced configuration:	☒	

Called address rules		
Address:	^0	
Name:		
Number type:	☒ Unknown ☒ International ☒ National ☒ Network specific ☒ Subscriber ☒ Abbreviated	No change
Numbering plan:	☒ Unknown ☒ ISDN/telephony E.164 ☒ National standard ☒ Private	No change

Calling address rules		

Redirect address rules		

- **Address map name:** Enter a descriptive name for the address map.
- **Rule name:** Enter a name that explains the address map rule.
- **Address Condition** in the **Called address rules** section: Enter the expression **^0** to remove the outside access digit.

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

15. Create three routes:

- Route from Microsoft® Office Communications Server 2007 directly to the PSTN
- Route from Microsoft® Office Communications Server 2007 via the PBX to the PSTN
- Route from the PSTN/PBX via the gateway computer to Microsoft® Office Communications Server 2007

In this example, the routes are configured in the correct order. The order of the routes is important, because only one route will be configured with a condition. This example also explains how to change the order, in case you configured the routes differently.

16. Create the route from Microsoft® Office Communications Server 2007 to the PSTN first. To do so, open the **Routing** section, click **Add** and configure the following parameters:

General		
Name:	SIP-to-PSTN	
Type: Name	Source	Destination
PSTN: Controller-to-PBX	☐	-
PSTN: Controller-to-PSTN	☐	Master
SIP: OCS-Mediation-Server	☒	-
Max. call attempts for this route in a failover scenario:	0 (0 = try all selected destinations)	
Address Normalization For Condition Processing (Using Source Dialplan)		
Use Dialplan:	☒	
Number format:	Extension	
Encoding:	Use prefixes	
Conditions		
Called number	Calling number	Redirect number
^0		
Add		
Address Manipulation		
Address map:	SIPto-PSTN-Address-Map	
OK Cancel		

- **Name:** Enter a unique name to easily identify the route.
- **Source:** Select the SIP peer configured above as a Master destination.
- **Destination:** Select the controller you configured for the PSTN.

Under Address Normalization for Condition Processing (Using Source Dialplan), configure the following parameters:

- **Number format:** Select **Extension** from the dropdown menu.
- **Encoding:** Select **Use prefixes** from the dropdown menu.

Under **Conditions**, click **Add**, and enter **^0** in the **Called number** field to omit the outside access digit. Click **OK** to save the settings and close the window.

17. Configure the route from Microsoft® Office Communications Server 2007 to the PBX. To do this, click **Add** and configure the following parameters:

General		
Name:	SIPto-PBX	
Type: Name	Source	Destination
PSTN: Controller-to-PBX	☐	Master
PSTN: Controller-to-PSTN	☐	-
SIP: OCS-Mediation-Server	☒	-
Max. call attempts for this route in a failover scenario:	0 (0 = try all selected destinations)	

Address Normalization For Condition Processing (Using Source Dialplan)	
Use Dialplan:	☒
Number format:	Unchanged
Encoding:	Use prefixes

Conditions		
Called number	Calling number	Redirect number
Add		

Address Manipulation	
Address map:	none

- **Name:** Enter a unique name to easily identify the route.
- **Source:** Select the configured SIP peer as a Master destination.
- **Destination:** Select the controller you configured for the PBX.

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

18. Create the route from the PSTN/PBX to Microsoft® Office Communications Server 2007. To do this, click **Add** and Configure the following parameters:

General		
Name:	PSTN-and-PBX-to-SIP	
Type: Name	Source	Destination
PSTN: Controller-to-PBX	☒	-
PSTN: Controller-to-PSTN	☒	-
SIP: OCS-Mediation-Server	☐	Master
Max. call attempts for this route in a failover scenario:	0 (0 = try all selected destinations)	
Address Normalization For Condition Processing (Using Source Dialplan)		
Use Dialplan:	☒	
Number format:	International number	
Encoding:	Use type flag	
Conditions		
Called number	Calling number	Redirect number
Add		
Address Manipulation		
Address map:	none	
OK Cancel		

- **Name:** Enter a unique name to easily identify the route.
- **Source:** Select both controllers of the Diva Media Board.
- **Destination:** Select the SIP peer configured above as a Master destination.

Under **Address Normalization for Condition Processing (Using Source Dialplan)**, configure the following parameters:

- **Number format:** Select **International number** from the dropdown menu.
- **Encoding:** Select **Use type flag** from the dropdown menu.

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

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

Routing						
Name	Sources	Destinations	Address map	Enabled		
SIP-to-PSTN	OCS-Mediation-Server	Controller-to-PSTN (Master)	SIP-to-PSTN-Address-Map	☒	Up	Down
SIP-to-PBX	OCS-Mediation-Server	Controller-to-PBX (Master)	none	☒	Up	Down
PSTN-and-PBX-to-SIP	Controller-to-PBX, Controller-to-PSTN	OCS-Mediation-Server (Master)	none	☒	Up	Down
Add						

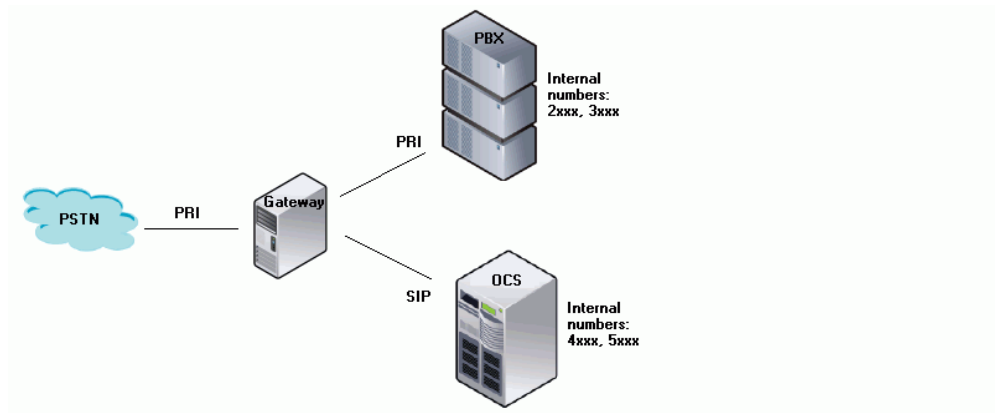
20. Click **Activate Configuration** in the main configuration page to save the settings and activate the changes.

21. Configure Microsoft® Office Communications Server 2007.

Using the Gateway Computer Between the PSTN and PBX / Microsoft® Office Communications Server 2007

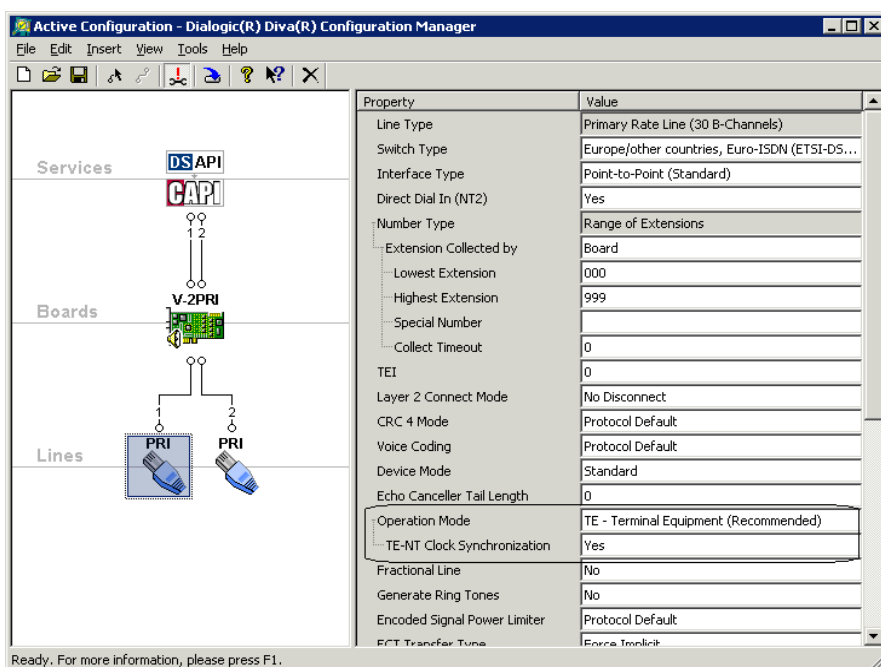
This configuration scenario describes the necessary steps if the gateway computer is connected between the PSTN and PBX/Microsoft® Office Communications Server 2007. This way, Diva SIPcontrol can also route calls from the PBX to the PSTN, and vice versa. One PRI line is connected to the PBX and one PRI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

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

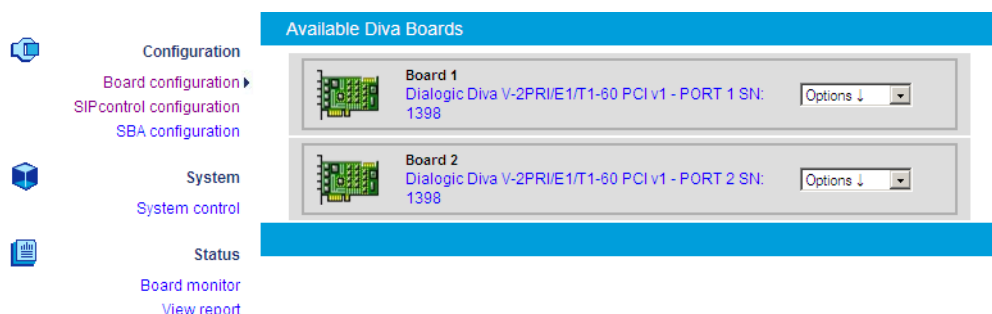


For this configuration scenario, one dialplan, five address maps, the two PSTN interfaces, the network interface, two SIP peers, and five routes need to be configured.

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



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



5. Click either the board icon or the name of the first Diva Media Board line (the PRI line connected to the PSTN) to open the **Board Configuration - Detail** page, and then configure the following parameters:.

Dialogic Diva V-2PRI/E1/T1-60 PCI v1 - PORT 1, SN:1398	
Parameter	Value
D-Channel Protocol:	Europe/other countries, Euro-ISDN (ETSI-DSS1) - (ETSI)
Interface Mode/Resource Board:	TE - mode
Direct Dial In (NT2):	Yes
DDI Number Length:	3
DDI Collect Timeout:	0
DDI Special Number:	
Layer 1 Framing:	National default (default)
Layer 2 Connect Mode:	No disconnect
Voice Companding:	Protocol default
View Extended Configuration	No

[Save](#) [Cancel](#)

- **D-Channel Protocol:** Select **Europe / other countries, Euro-ISDN (ETSI-DSS1) - (ETSI)** as the D-channel protocol.
- **DDI Number Length:** Set the value to **3**.

Click **Save** to close the window.

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

Dialogic Diva V-2PRI/E1/T1-60 PCI v1 - PORT 2, SN:1398	
Parameter	Value
D-Channel Protocol:	Europe/other countries, Euro-ISDN (ETSI-DSS1) - (ETSI)
Interface Mode/Resource Board:	NT - mode
Direct Dial In (NT2):	Yes
DDI Number Length:	20
DDI Collect Timeout:	3
DDI Special Number:	
Layer 1 Framing:	National default (default)
Layer 2 Connect Mode:	No disconnect
Voice Companding:	Protocol default
View Extended Configuration	No

[Save](#) [Cancel](#)

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

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

8. Open the **Dialplans** section, click **Add**, and configure the following parameters for the dialplan:

General	
Name:	Dialplan-PSTN
Country code:	49
North-American numbering plan:	☐
Area code:	7159 With national prefix
Other local areas:	
Base number:	4066
Maximum extension digits:	4
International prefix:	00
National prefix:	0
Access code:	0
PSTN access code provided by SIP caller:	☒
Incoming PSTN access code provided by PBX:	☒
OK Cancel	

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

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

9. Create five address maps: two for incoming calls, two for outgoing calls, and one for the special number, which is normally the reception's number. The first four address maps are necessary for either adding or omitting the OAD (Outside Access Digit).

- To create the first address map for incoming calls from the PSTN, open the **Address Maps** section, click **Add**, and configure the following parameters:

General		
Address map name:	PSTN-Access-Inbound	
Rule name:	Add OAD in Calling Number	
Stop on match:	☐	
Enhanced configuration:	☐	
Called address rules		
Calling address rules		
Address:	^[0-9].*	0\$&
Name:		
Number type:	☒ Unknown ☒ International ☒ National ☒ Network specific ☒ Subscriber ☒ Abbreviated	No change
Numbering plan:	☒ Unknown ☒ ISDN/telephony E.164 ☒ National standard ☒ Private	No change
Presentation:	☒ Allowed ☒ Restricted ☒ Number not available ☒ Undefined	No change
Redirect address rules		
OK Cancel		

- Address map name:** Enter a name for the incoming call address map.
- Rule name:** Enter a name that describes the address map rule. This name will be displayed on the main configuration page.
- Address Condition** in the **Calling address rules** section: Enter `^[0-9].*`. This expression matches all calls from the PSTN.
- Address Result** in the **Calling address rules** section: Enter the **0** (zero), so that it is added in the output, followed by the **\$&**, which adds the incoming number after the **0**.

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

- To create the second address map for outgoing calls to the PSTN, click **Add** again, and configure the following parameters:

General		
Address map name:	PSTN-Access-Outbound	
Rule name:	Remove OAD in Called Number	
Stop on match:	☐	
Enhanced configuration:	☐	
Called address rules		
	Condition	Result
Address:	^0	
Name:		
Number type:	☒ Unknown ☒ International ☒ National ☒ Network specific ☒ Subscriber ☒ Abbreviated	No change
Numbering plan:	☒ Unknown ☒ ISDN/telephony E.164 ☒ National standard ☒ Private	No change
Calling address rules		
Redirect address rules		
OK Cancel		

- Address map name:** Enter a name for the outgoing call address map.
- Rule name:** Enter a name that describes the address map rule. This name will be displayed on the main configuration page.
- Address Condition** in the **Called address rules** section: Enter **^0**. With this expression, the OAD (0) will be removed from the outgoing calls.

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

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

General		
Address map name:	From-PBX	
Rule name:	Add OAD in Called Number	
Stop on match:	☐	
Enhanced configuration:	☐	

Called address rules		
	Condition	Result
Address:	^[0-9]*	0\$&
Name:		
Number type:	☒ Unknown ☒ International ☒ National ☒ Network specific ☒ Subscriber ☒ Abbreviated	No change
Numbering plan:	☒ Unknown ☒ ISDN/telephony E.164 ☒ National standard ☒ Private	No change

Calling address rules

Redirect address rules

- Address map name:** Enter a name for the address map for calls from the PBX.
- Rule name:** Enter a name that describes the address map rule. This name will be displayed on the main configuration page.

Under **Called Address rules**, configure the following parameters:

- **Address Condition** in the **Calling address rules** section: Enter **^[0-9].***. This expression matches all calls from the PSTN.
- **Address Result** in the **Calling address rules** section: Enter the **0** (zero), so that it is added in the output, followed by the **\$&**, which adds the incoming number after the **0**.

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

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

General		
Address map name:	To-PBX	
Rule name:	Remove OAD in Calling Number	
Stop on match:	☐	
Enhanced configuration:	☐	

Called address rules		
Calling address rules		
	Condition	Result
Address:	^0	
Name:		
Number type:	☒ Unknown ☒ International ☒ National ☒ Network specific ☒ Subscriber ☒ Abbreviated	No change
Numbering plan:	☒ Unknown ☒ ISDN/telephony E.164 ☒ National standard ☒ Private	No change
Presentation:	☒ Allowed ☒ Restricted ☒ Number not available ☒ Undefined	No change

Redirect address rules		
OK Cancel		

- **Address map name:** Enter an address map name for calls from the gateway to the PBX.
- **Rule name:** Enter a name that describes the address map rule. This name will be displayed on the main configuration page.
- **Address Condition** in the **Calling address rules** section: Enter **^0**. With this expression, the OAD will be removed from calls to the PBX.

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

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

General		
Address map name:	Map-to-Central-Number	
Rule name:	Map-to-Central-Number-1	
Stop on match:	☐	
Enhanced configuration:	☐	

Called address rules		
Address:	^.*\$	+49715940662000
Name:		
Number type:	☒ Unknown ☒ International ☒ National ☒ Network specific ☒ Subscriber ☒ Abbreviated	No change
Numbering plan:	☒ Unknown ☒ ISDN/telephony E.164 ☒ National standard ☒ Private	No change

Calling address rules		

Redirect address rules		

- Address map name:** Enter an address map name for calls to the reception.
- Rule name:** Enter a name that describes the address map rule. This name will be displayed on the main configuration page.

Under **Called address rules**, configure the following parameters:

- Address Condition:** Enter **^.*\$**. Because this address map will be associated with a route for internal unassigned numbers, this expression will match all of those numbers.
- Address Result:** Enter the number of the reception, to which the unassigned internal numbers will be routed. Include the country code, area code, base number, and extension, as shown in the graphic above.

- Under **PSTN Interfaces**, configure Controller 1 with PSTN-specific settings and Controller 2 with PBX-specific settings. The controller number that you configure with the PBX-specific settings needs to correspond to the line number in the Diva Configuration Manager on which you configured the switch type of your PBX. Similarly, the controller number that you configure with the PSTN-specific settings needs to correspond to the line number in the Diva Configuration Manager on which you configured the switch type of your PSTN line.

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

General	
Hardware description:	Dialogic Diva V-2PRI/E1/T1 - PORT 1 SN: 1033
PSTN interface number:	1
Name:	Controller-to-PSTN
Address map inbound:	PSTN-Access-Inbound
Address map outbound:	PSTN-Access-Outbound
Enhanced	
Address Normalization	
Dialplan:	Dialplan-PSTN
Number format (outbound):	National number
Encoding (outbound):	Use prefixes
Default numbering plan:	unknown
Default presentation indicator:	Allowed
Internal interface:	☐
PSTN Call Transfer Settings	
Message Waiting Indication (MWI)	
OK Cancel	

- Name:** Enter a unique name for this controller.
- Address map inbound:** Select the inbound address map that you configured for access from the PSTN.
- Address map outbound:** Select the outbound address map that you configured for access to the PSTN.

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

- Dialplan:** Select the dialplan you configured for the PSTN.
- Number format (outbound):** Select **National number** from the dropdown menu.
- Encoding (outbound):** Select **Use prefixes** from the dropdown menu.

Leave the remaining parameters at their default values.

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

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

General	
Hardware description:	Dialogic Diva V-2PRI/E1/T1 - PORT 2 SN: 1033
PSTN interface number:	2
Name:	Controller-to-PBX
Address map inbound:	From-PBX
Address map outbound:	To-PBX
Enhanced	
Address Normalization	
Dialplan:	Dialplan-PSTN
Number format (outbound):	National number
Encoding (outbound):	Use prefixes
Default numbering plan:	unknown
Default presentation indicator:	Allowed
Internal interface:	☒
PSTN Call Transfer Settings	
Message Waiting Indication (MWI)	
OK Cancel	

- Name:** Enter a unique name for this controller.
 - Address map inbound:** Select the inbound address map that you configured for access from the PBX.
 - Address map outbound:** Select the outbound address map that you configured for access to the PBX.
- Under **Address Normalization**, configure the following parameters:

- Dialplan:** Select the dialplan you configured for the PSTN.
- Number format (outbound):** Select **National number** from the dropdown menu.
- Encoding (outbound):** Select **Use prefixes** from the dropdown menu.
- Activate the **Internal Interface** option. This option must be activated, because this interface connects to internal devices only. (It does not directly connected to the PSTN.)

Leave the remaining parameters at their default values.

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

- Under **Network Interfaces**, enable your Ethernet adapter, and set the SIP listen ports to **9803**.

Network Interfaces					
Name	Device	IP address	UDP listen port	TCP listen port	TLS listen port
Intel(R) PRO1000 GT Desktop	Intel(R) PRO1000 GT Desktop Adapter - Packet Scheduler Miniport	192.168.213.38	9803 ☒	9803 ☒	5061 ☐
Local Loopback Interface	Local Loopback Interface	127.0.0.1	5060 ☐	5060 ☐	0 ☐

12. Create a SIP peer for the Microsoft® Mediation Server installed on the gateway computer. To configure this SIP peer, open the **SIP Peers** section, click **Add**, and enter the following parameters:

General	
Name:	OCS-Mediation-Server
Peer type:	MS OCS 2007/2007 R2 - Mediation Server
Host:	192.168.212.136
Port:	5060
IP protocol:	TCP
URI scheme:	SIP (default)
Domain:	ocs-name.ad-domain.tld
Enhanced	
Security	
Session Timer	
Address Normalization	
Dialplan:	Dialplan-PSTN
Number format (outbound):	International number
Encoding (outbound):	Use type flag
Address map inbound:	none
Address map outbound:	none
Authentication	
OK Cancel	

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

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

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

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

13. Create the following routes:

- PSTN to Microsoft® Office Communications Server 2007
- Microsoft® Office Communications Server 2007 to the PBX
- Microsoft® Office Communications Server 2007 to the PSTN
- A route for calls to the reception

In this scenario, the order of the routes is important because of the used conditions.

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

General			
Name:	Route-to-OCS		
Type: Name	Source	Destination	
PSTN: Controller-to-PSTN	☒	-	
PSTN: Controller-to-PBX	☒	-	
SIP: OCS-Mediation-Server	☐	Master	
Max. call attempts for this route in a failover scenario:	0 (0 = try all selected destinations)		

Address Normalization For Condition Processing (Using Source Dialplan)	
Use Dialplan:	☒
Number format:	International number
Encoding:	Use type flag

Conditions			
Called number	Calling number	Redirect number	
^\\+4971594066[45]			Delete
Add			

Address Manipulation	
OK Cancel	

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

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

- Create the second route from the Microsoft® Office Communications Server 2007 to the PBX. To do so, click **Add** in the **Routing** section, and configure the following parameters:

General		
Name:	Route-to-PBX	
Type: Name	Source	Destination
PSTN: Controller-to-PSTN	☒	-
PSTN: Controller-to-PBX	☐	Master
SIP: OCS-Mediation-Server	☒	-
Max. call attempts for this route in a failover scenario:	0 (0 = try all selected destinations)	
Address Normalization For Condition Processing (Using Source Dialplan)		
Use Dialplan:	☒	
Number format:	International number	
Encoding:	Use type flag	
Conditions		
Called number	Calling number	Redirect number
~\+4971594066[23]		
Add		
Address Manipulation		
OK Cancel		

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

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

- Create the third route from the Microsoft® Office Communications Server 2007 to the PSTN. To do so, click **Add** in the **Routing** section, and configure the following parameters:

General		
Name:	Route-to-PSTN	
Type: Name	Source	Destination
PSTN: Controller-to-PSTN	☐	Master ▾
PSTN: Controller-to-PBX	☒	. ▾
SIP: OCS-Mediation-Server	☒	. ▾
Max. call attempts for this route in a failover scenario:	0 (0 = try all selected destinations)	

Address Normalization For Condition Processing (Using Source Dialplan)	
Use Dialplan:	☒
Number format:	International number ▾
Encoding:	Use type flag ▾

Conditions

Address Manipulation

OK Cancel

- **Name:** Enter a unique name to easily identify the route.
- **Source:** Select the PBX controller and the SIP peer configured for the Microsoft® Mediation Server as sources.
- **Destination:** Select the PSTN controller as a Master destination.

Under **Address Normalization For Condition Processing (Using Source Dialplan)**, configure the following parameters:

- **Number format:** Select **International number** from the dropdown menu.
- **Encoding:** Select **Use type flag** from the dropdown menu.

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

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

General		
Name:	Route-to-Central-Number	
Type: Name	Source	Destination
PSTN: Controller-to-PSTN	☒	-
PSTN: Controller-to-PBX	☐	Master
SIP: OCS-Mediation-Server	☐	-
Max. call attempts for this route in a failover scenario:	0 (0 = try all selected destinations)	

Address Normalization For Condition Processing (Using Source Dialplan)	
Use Dialplan:	☒
Number format:	International number
Encoding:	Use type flag

Conditions		
Called number	Calling number	Redirect number
+4971594066[016789]		
Add		

Address Manipulation	
Address map:	Map-to-Central-Number

OK Cancel

- **Name:** Enter a unique name to easily identify the route.
- **Source:** Select the PSTN controller as a source.
- **Destination:** Select the SIP peer configured for the Microsoft® Mediation Server as a destination. We select this destination, because in this scenario, the reception is connected to the Microsoft® Mediation Server. If the reception is connected to the PBX instead, select the PBX controller as the destination.

Under **Address Normalization For Condition Processing (Using Source Dialplan)**, configure the following parameters:

- **Number format**: Select **International number** from the dropdown menu.
- **Encoding**: Select **Use type flag** from the dropdown menu.

Under **Conditions**, click **Add**, and in **Called number**, enter a regular expression that matches all extensions that should be routed to the reception, i.e., all unassigned extensions. In our example, the unassigned extensions do NOT start with 0, 1, 6, 7, 8, or 9, because those extensions are not used by the PBX or Microsoft® Office Communications Server 2007.

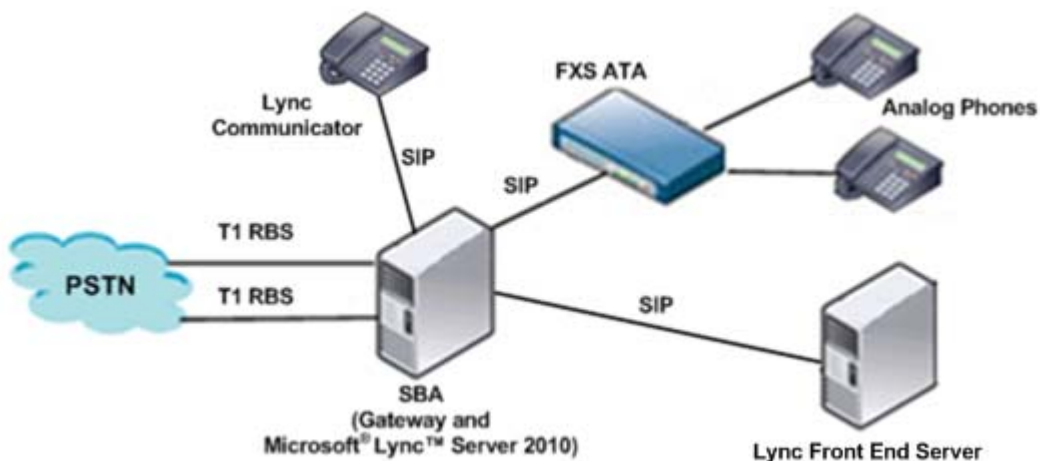
- **Address map** in the **Address Manipulation** section: Select the mapping for the reception.

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

Using the Gateway Computer Between the PSTN and Microsoft® Lync™ Server 2010

This configuration scenario describes the necessary steps for configuring a gateway computer that is directly connected to the PSTN via two T1 RBS links and also connected to a Lync SBA server on the SIP side. This scenario has the following characteristics:

- There is no PBX between the gateway and the PSTN.
- The Lync Server is co-located with the gateway. Together, the Lync Server and the gateway create a Survivable Branch Appliance Solution (SBA).
- The gateway is connected to an FXS (Foreign eXchange Subscriber interface) Analog Telephone Adapter (ATA) via SIP. The FXS ATA is connected to analog phones or fax devices.
- Internal extensions have four digits.
- The Lync Server routes calls to extensions 2201 and 2202 to the FXS ATA via the gateway.
- The gateway blocks calls from the PSTN that have origination extensions of 2201 or 2202, because the Lync Server would treat these calls as calls from the FXS ATA rather than calls from the PSTN.



1. Open the Diva web interface to configure the required parameters. To do so, click **Start > Programs > Dialogic Diva > SIPcontrol Configuration**.

For this configuration scenario, two codec profiles, one dialplan, one address map, the two PSTN interfaces, the network interface, four SIP peers, and seven routes need to be configured.

- In the Diva web interface, click **Board configuration** on the left hand side to open the **Available Diva Boards** page.



- Click either the board icon or the name of the first Diva Media Board line to open the **Board Configuration - Detail** page.
- Configure the first board by configuring the following parameters:

Dialogic Diva V-2PRI/E1/T1-60 PCI v1 - PORT 1, SN:1033	
Parameter	Value
D-Channel Protocol:	USA_RBS_T1 (Robbed Bit Signaling) - (RBSCAS)
Interface Mode/Resource Board:	TE - mode
Direct Dial In (NT2):	Yes
DDI Number Length:	4
DDI Collect Timeout:	2 (default)
DDI Special Number:	
Layer 1 Framing:	National default (default)
Layer 2 Connect Mode:	Permanent
Voice Companding:	Protocol default
View Extended Configuration	No

Save Cancel

- D-Channel Protocol:** Select a protocol with T1 Robbed Bit Signaling (RBS).
- DDI Number Length:** Select 4.

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

- Configure the second board with the same parameters as the first one.
- In the Diva SIPControl web interface, click **SIPcontrol configuration** on the left hand side to open the **SIPcontrol Configuration** page.
- Create two codec profiles: One for the Lync Server and the other for FXS ATA 3.

- To create the a codec profile for the Lync Server, open the **Codec Profiles** section, click **Add**, and configure the following parameters:

The screenshot shows a configuration window for a codec profile named "Lync-Codecs". The window is divided into several sections:

- General**: A text field for "Name" containing "Lync-Codecs".
- Audio Codecs**:
 - Available Codecs**: A list box containing "G.729", "G.726 16 kbps", "G.726 24 kbps", "G.726 32 kbps", and "G.726 40 kbps".
 - Selected Codecs**: A list box containing "G.711 A-Law" and "G.711 u-Law".
 - Buttons: "Use Codec ->", "<- Remove Codec", "Up", and "Down".
 - G.711 A-Law Codec Settings**:
 - "Packet interval default": A text field with "20".
 - "Voice activity detection": A checked checkbox.
 - "Comfort Noise Generation": A checked checkbox.
- Audio Quality**:
 - "Support comfort noise payload": A checked checkbox.
 - "Noise suppressor": An unchecked checkbox.
 - "Echo canceller": A checked checkbox.
- DTMF Codec**:
 - "Transmit as RTP event": A checked checkbox.
 - "Automatic payload type": A checked checkbox.
 - "Manual payload type value": A text field with "101".
 - "Disable CNG event": An unchecked checkbox.
- Buttons**: "OK" and "Cancel" at the bottom right.

- Enter a unique name to easily identify the codec.
- In the **Audio Codecs** section, enable **Comfort Noise Generation** and **Voice activity detection**. Click **OK** to save the settings and close the window.

- To create a codec profile for the FSX ATA, open the **Codec Profiles** section, click **Add**, and configure the following parameters:

The screenshot shows a configuration window for a codec profile. It is divided into four main sections: General, Audio Codecs, Audio Quality, and DTMF Codec. The General section has a 'Name' field with the value 'ATACodecs'. The Audio Codecs section contains two lists: 'Available Codecs' and 'Selected Codecs'. The 'Available Codecs' list includes G.729, G.726 16 kbps, G.726 24 kbps, G.726 32 kbps, and G.726 40 kbps. The 'Selected Codecs' list contains G.711 u-Law. Between these lists are buttons for 'Use Codec -->' and '<-- Remove Codec'. Below the lists are 'Up' and 'Down' buttons. The 'G.711 u-Law Codec Settings' section includes 'Packet interval default' (set to 20), 'Voice activity detection' (unchecked), and 'Comfort Noise Generation' (unchecked). The 'Audio Quality' section includes 'Support comfort noise payload' (unchecked), 'Noise suppressor' (unchecked), and 'Echo canceller' (checked). The 'DTMF Codec' section includes 'Transmit as RTP event' (checked), 'Automatic payload type' (unchecked), 'Manual payload type value' (set to 101), and 'Disable CNG event' (checked). At the bottom are 'OK' and 'Cancel' buttons.

General

Name: ATACodecs

Audio Codecs

Available Codecs

- G.729
- G.726 16 kbps
- G.726 24 kbps
- G.726 32 kbps
- G.726 40 kbps

Use Codec -->

<-- Remove Codec

Selected Codecs

- G.711 u-Law

Up Down

G.711 u-Law Codec Settings

Packet interval default: 20

Voice activity detection: ☐

Comfort Noise Generation: ☐

Audio Quality

Support comfort noise payload: ☐

Noise suppressor: ☐

Echo canceller: ☒

DTMF Codec

Transmit as RTP event: ☒

Automatic payload type: ☐

Manual payload type value: 101

Disable CNG event: ☒

OK Cancel

- Enter a unique name to easily identify the codec.
- Remove **G.711 A-Law** from the list of selected codecs.
- In the **Audio Quality** section, disable **Support comfort noise payload**.
- Click **OK** to save the settings and close the window.

8. Create a dialplan that reflects the PSTN dialing rules for the T1 trunks connected to the gateway. To do so, open the **Dialplans** section, click **Add**, and configure the following parameters:

General	
Name:	US Dialplan
Country code:	1
North-American numbering plan:	☒
Area code:	716 With national prefix
Other local areas:	
Base number:	555
Maximum extension digits:	4
International prefix:	011
National prefix:	1
Access code:	
PSTN access code provided by SIP caller:	☒
Incoming PSTN access code provided by PBX:	☒
OK Cancel	

- **Name:** Enter a unique name to easily identify the dialplan.
- **North-American number plan:** Enable **North-American numbering plan** if the dialplan is for North American numbers (country code 1).
- **Country code:** Enter the country code of the country in which the gateway computer is located.
- **Area code:** Enter the area code of the region in which the gateway computer is located.
- **Base number:** Enter the subscriber or trunk number.
- **Maximum extension digits:** Select the maximum number of extension digits that are provided.
- **International prefix:** Enter the international prefix of the country in which the gateway computer is located.
- **National prefix:** Enter the national prefix that needs to be dialed for long distance calls within the country in which the gateway computer is located.
- **Access code:** Enter the digit that is necessary to get access to the public network, if any.

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

9. Create an address map for calls from the FXS ATA to the Lync Server, to make them appear like internal Lync Server calls. To do this, open the **Address Maps** section, click **Add**, and configure the following parameters:

General		
Address map name:	FromATA	
Rule name:	FromATA.1	
Stop on match:	☒	
Enhanced configuration:	☐	

Called address rules		
Address:	^(.*)@192\168\212\138	\$1@sba.domain.example.com
Name:		
Number type:	☒ Unknown ☒ International ☒ National ☒ Network specific ☒ Subscriber ☒ Abbreviated	No change
Numbering plan:	☒ Unknown ☒ ISDN/telephony E.164 ☒ National standard ☒ Private	No change

Calling address rules		
Address:	^(.*)@192\168\212\138	\$1@sba.domain.example.com
Name:		
Number type:	☒ Unknown ☒ International ☒ National ☒ Network specific ☒ Subscriber ☒ Abbreviated	No change
Numbering plan:	☒ Unknown ☒ ISDN/telephony E.164 ☒ National standard ☒ Private	No change
Presentation:	☒ Allowed ☒ Restricted ☒ Number not available ☒ Undefined	No change

Redirect address rules		

- **Address map name:** Enter a name for the incoming call address map.
- **Rule name:** Enter a name that describes the address map rule. This name will be displayed on the main configuration page.

- Optionally enable **Stop on match** to have the gateway stop searching for matching rules when all specified address conditions match all addresses of a call.

Under **Called address rules**, configure the following parameters:

- Address Condition:** Enter the called address condition as shown in the graphic above. This condition matches all calls to 192.168.212.138, which is the IP address of the FSX ATA.
- Address Result:** Enter the called address result as shown in the graphic above, with the FDQN of the SBA after the @ sign. This address result converts the matched called addresses to a form accepted by the Lync Server.

Under **Calling address rules**, configure the following parameters:

- Address Condition:** Enter the calling address condition as shown in the graphic above. This condition matches all calls from 192.168.212.138, which is the IP address of the FXS ATA.
- Address Result:** Enter the calling address result as shown in the graphic above, with the FDQN of the SBA after the @ sign. This address result converts the matched calling addresses to a form accepted by the Lync Server.

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

- Under **PSTN Interfaces**, configure both Controller 1 and Controller 2 with PSTN-specific settings. The controller numbers that you configure with PSTN-specific settings needs to correspond to the line numbers in the Diva Configuration Manager on which you configured the switch type of your PSTN lines.

- To configure PSTN-specific parameters for Controller 1, click **Details** to the right of the respective controller, and configure the following parameters:

General	
Hardware description:	Dialogic Diva V-2PRI/E1/T1-60 PCI v1 - PORT 1 SN: 1033
PSTN interface number:	1
Name:	Controller1
Address map inbound:	none
Address map outbound:	none
Enhanced	
Address Normalization	
Dialplan:	US Dialplan
Type of number (outbound):	Unchanged
Encoding (outbound):	Use type flag
ISDN numbering plan - Default:	unknown
Presentation indicator - Default:	Allowed
Internal interface:	☐
PSTN Call Transfer Settings	
Message Waiting Indication (MWI)	
OK Cancel	

- Name:** Enter a unique name for this controller.
- Dialplan:** Select the configured dialplan.

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

- Configure Controller 2 by using the same settings you specified for Controller 1, except for the value of the Name parameter:

General	
Hardware description:	Dialogic Diva V-2PRI/E1/T1-60 PCI v1 - PORT 2 SN: 1033
PSTN interface number:	2
Name:	Controller2
Address map inbound:	none
Address map outbound:	none

Enhanced	
Address Normalization	
Dialplan:	US Dialplan
Type of number (outbound):	Unchanged
Encoding (outbound):	Use type flag
ISDN numbering plan - Default:	unknown
Presentation indicator - Default:	Allowed
Internal interface:	☐

PSTN Call Transfer Settings	
Message Waiting Indication (MWI)	

OK Cancel

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

- Under **Network Interfaces**, enable your Ethernet adapter, and set the TCP listen port to **5081** and the TLS listen port to **5082**:

Network Interfaces					
Name	Device	IP address	UDP listen port	TCP listen port	TLS listen port
Intel(R) PRO1000 EB Network	Intel(R) PRO/1000 EB Network Connection with I/O Acceleration #2	192.168.212.136	5060 ☐	5081 ☒	5082 ☒
Local Loopback Interface	Local Loopback Interface	127.0.0.1	0 ☐	0 ☐	0 ☐
RTP start port:	30000				
RTP end port:	39999				

- Create the following SIP peers:

- A SIP peer for the Lync Server
- Two SIP peers to correspond to each ATA extension.
- A dummy SIP peer that is used for rejecting PSTN calls made to the same extensions as the FXS ATA (extensions 2201 and 2202).

- Create the first SIP peer for the Lync Server. To do this, open the **SIP Peers** section, click **Add**, and enter the following parameters:

General	
Name:	Lync
Peer type:	MS Lync 2010 - Mediation Server
Host:	lba
Port:	5067
IP protocol:	TLS
URI scheme:	SIP (default)
Domain:	domain.example.com

Enhanced	
Default peer for received SIP calls:	☒
Display name to:	
Display name from:	
User name to:	
User name from:	
Gateway prefix:	
Reply-To expression:	
Reply-To format:	
Force T.38 reinvite:	☐
Alive check:	☐ 60 seconds (0=auto)
Disconnect tone support:	☐
Cause code mapping inbound:	peer default
Cause code mapping outbound:	peer default
Codec profile:	Lync-Codecs
Maximum channels:	480
Early media support:	☒
Reliable provisional response:	Optional

Security	
----------	--

Session Timer	
---------------	--

Address Normalization	
Dialplan:	US Dialplan
Number format (outbound):	International number
Encoding (outbound):	Use type flag
Address map inbound:	none
Address map outbound:	none

Authentication	
----------------	--

OK Cancel

- **Name:** Enter a unique name to easily identify the SIP peer.
- **Peer type:** Select **MS Lync 2010 - Mediation Server** from the dropdown menu.
- **Host:** Enter the FDQN of the Lync Server to which you are connected, which in this scenario, is also the FDQN of the gateway.

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

- **Default peer for received SIP calls:** Enable this parameter.
- **Codec profile:** Select the codec you defined for the Lync Server.

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

- **Dialplan:** Select the configured dialplan.
- **Number format (outbound):** Select **International number** from the dropdown menu.
- **Encoding (outbound):** Select **Use type flag** from the dropdown menu.

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

- Create the second SIP peer for the first ATA extension. To do this, open the **SIP Peers** section, click **Add**, and enter the following parameters:

General	
Name:	ATA2201
Peer type:	Grandstream HT-502
Host:	192.168.212.138
Port:	5068
IP protocol:	TCP
URI scheme:	SIP (default)
Domain:	

Enhanced	
Default peer for received SIP calls:	☐
Display name to:	
Display name from:	
User name to:	
User name from:	
Gateway prefix:	
Reply-To expression:	
Reply-To format:	
Force T.38 reinvite:	☐
Alive check:	☐ 1800 seconds (0=auto)
Disconnect tone support:	☐
Cause code mapping inbound:	peer default
Cause code mapping outbound:	peer default
Codec profile:	ATACodecs
Maximum channels:	480
Early media support:	☐
Reliable provisional response:	Disabled

Security

Session Timer

Address Normalization	
Dialplan:	US Dialplan
Number format (outbound):	Unchanged
Encoding (outbound):	Use type flag
Address map inbound:	none
Address map outbound:	none

Authentication

OK Cancel

- **Name:** Enter a unique name to easily identify the SIP peer.
- **Peer type:** Select **Grandstream HT-502** from the dropdown menu.
- **Host:** Enter the host name for the SIP peer.

Under **Enhanced**, select the codec you defined for the ATA as the **Codec profile**, and disable **Reliable provisional response**.

Under **Address Normalization**, select the configured dialplan.

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

- Create the third SIP peer for the second ATA extension. Use the same configuration values as you did for the first ATA extension, except for the values of the **Name**, **Host**, and **Port** parameters in the **General** section.
- Create the fourth SIP peer as a dummy peer that will be used for rejecting calls. (The routing rules will determine which calls will be rejected.) To create this SIP peer, open the **SIP Peers** section, click **Add**, and enter values for the **Name**, **Host**, and **Port** parameters in the **General** section. The values for these parameters do not matter. For example:

General	
Name:	Forbidden Call
Peer type:	Default
Host:	127.0.0.1
Port:	5060
IP protocol:	TCP
URI scheme:	SIP (default)
Domain:	

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

13. In the SIP Peers section of the main SIP Configuration screen, disable the dummy SIP peer (the fourth one) by unchecking the **Enabled** parameter for this peer.

The SIP Peers section of the main configuration screen should now look like this:

SIP Peers							
Name	Host	Port	IP protocol	Codec Profile	Dialplan	Enabled	
Lync	sba	5067	TLS	Lync-Codecs	US Dialplan	☒	Details Delete
ATA2201	192.168.212.138	5068	TCP	ATACodecs	US Dialplan	☒	Details Delete
ATA2202	192.168.212.138	5070	TCP	ATACodecs	US Dialplan	☒	Details Delete
Forbidden Call	127.0.0.1	5060	TCP	default	none	☐	Details Delete
Default peer for received SIP calls: Lync							Add new peer

14. Create the following routes in the order specified:

- Route to block numbers from the PSTN that have the same extension as the ATA
- Route from the PSTN to the Lync Server
- Route for call transfers in a Lync Server environment
- Two routes from the Lync Server to the FXS ATA extensions
- Route from the Lync Server to the PSTN
- Route from FXS ATA to the Lync Server

In this scenario, the order of the routes is important because of the conditions used.

- Create the first route to block numbers from the PSTN that have the same extension as the ATA (extensions 2201 and 2202). To do so, open the **Routing** section, click **Add** and configure the following parameters:

General		
Name:	Block ATA numbers from PSTN	
Type: Name	Source	Destination
PSTN: Controller1	☒	-
PSTN: Controller2	☒	-
SIP: Lync	☐	-
SIP: ATA2201	☐	-
SIP: ATA2202	☐	-
SIP: Forbidden Call (disabled)	☐	Master
Max. call attempts for this route in a failover scenario:	0 (0 = try all selected destinations)	

Address Normalization For Condition Processing (Using Source Dialplan)	
Use Dialplan:	☒
Number format:	International number
Encoding:	Use type flag

Conditions			
Called number	Calling number	Redirect number	
	+17165552201\$		Delete
	+17165552202\$		Delete
Add			

- **Name:** Enter a unique name to easily identify the route.
- **Source:** Select both PSTN controllers as sources.
- **Destination:** Select the disabled SIP peer as a Master destination.

Under **Address Normalization for Condition Processing (Using Source Dialplan)**, configure the following parameters:

- **Use Dialplan:** Leave this field enabled (the default) so that the gateway uses the configured Dialplan when selecting this route.
- **Number format:** Select **International number** from the dropdown menu.
- **Encoding:** Select **Use type flag** from the dropdown menu.

Under **Conditions**, click **Add**, and in **Calling number**, enter the regular expressions that match the extensions for the ATA including country code, area code, trunk prefix, and extension number. In this scenario, the expressions `^\+17165552201$` and `^\+17165552202$` match both extensions for the ATA.

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

- Create the second route from the PSTN to the Lync Server. To do so, click **Add** in the **Routing** section, and configure the following parameters:

General		
Name:	PSTNto-SIP	
Type: Name	Source	Destination
PSTN: Controller1	☒	-
PSTN: Controller2	☒	-
SIP: Lync	☐	Master
SIP: ATA2201	☐	-
SIP: ATA2202	☐	-
SIP: Forbidden Call (disabled)	☐	-
Max. call attempts for this route in a failover scenario:	0 (0 = try all selected destinations)	
Address Normalization For Condition Processing (Using Source Dialplan)		
Use Dialplan:	☒	
Number format:	Unchanged	
Encoding:	Use type flag	
Conditions		
Address Manipulation		
OK Cancel		

- **Name:** Enter a unique name to easily identify the route.
- **Source:** Select both PSTN controllers as sources.
- **Destination:** Select the SIP Peer configured for the Lync Server as a Master destination.

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

- Create the third route to have all call transfers routed by the Lync Server. To do so, click **Add** in the **Routing** section, and configure the following parameters:

General			
Name:	Call transfer routing by Lync		
Type: Name	Source	Destination	
PSTN: Controller1	☐	-	
PSTN: Controller2	☐	-	
SIP: Lync	☒	Master	
SIP: ATA2201	☐	-	
SIP: ATA2202	☐	-	
SIP: Forbidden Call (disabled)	☐	-	
Max. call attempts for this route in a failover scenario:	0 (0 = try all selected destinations)		
Address Normalization For Condition Processing (Using Source Dialplan)			
Use Dialplan:	☒		
Number format:	Unchanged		
Encoding:	Use type flag		
Conditions			
Called number	Calling number	Redirect number	
~192\168\212\136			Delete
~SBA.domain.example.com			Delete
Add			
Address Manipulation			
OK Cancel			

- **Name:** Enter a unique name to easily identify the route.
- **Source:** Select the SIP peer configured for the Lync Server as both a source and Master destination. This causes all calls matching the specified conditions to be routed back to the Lync Server, so it can handle the routing.

Under **Conditions**, enter the address of the Lync Server as both an FQDN and an IP address. This condition will match all transfer requests from the Lync Server.

Note: If the Gateway is connected to a Lync Front End Server Pool instead of a Lync SBA or single Lync Front End Server, you need to use the FQDN of the pool and IP address of each pool member to match all transfer requests from the Lync Server.

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

- Create the fourth route to route calls from the Lync Server to one of the ATA extensions. To do so, click **Add** in the **Routing** section, and configure the following parameters:

General		
Name:	To ATA1	
Type: Name	Source	Destination
PSTN: Controller1	☐	-
PSTN: Controller2	☐	-
SIP: Lync	☒	-
SIP: ATA2201	☐	Master
SIP: ATA2202	☐	-
SIP: Forbidden Call (disabled)	☐	-
Max. call attempts for this route in a failover scenario:	0 (0 = try all selected destinations)	
Address Normalization For Condition Processing (Using Source Dialplan)		
Use Dialplan:	☒	
Number format:	International number	
Encoding:	Use type flag	
Conditions		
Called number	Calling number	Redirect number
17165552201\$		
Add	Delete	
Address Manipulation		
OK Cancel		

- **Name:** Enter a unique name to easily identify the route.
- **Source:** Select the SIP peer configured for the Lync Server as a source.
- **Destination:** Select the SIP peer configured for one of the ATA extensions as a Master destination.

Under **Address Normalization for Condition Processing (Using Source Dialplan)**, configure the following parameters:

- **Use Dialplan:** Leave this field enabled (the default) so that the gateway uses the configured Dialplan when selecting this route.
- **Number format:** Select **International number** from the dropdown menu.
- **Encoding:** Select **Use type flag** from the dropdown menu.

Under **Conditions**, click **Add**, and in **Called number**, enter a regular expression that matches all calls to the ATA extension 2201.

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

15. Create the fifth route to route calls from the Lync Server to the second ATA extension. To do so, use the same settings you specified for the fourth route (in Step 12), except for the value of the **Name** and **Called number** parameters. For **Called number**, enter a regular expression that matches all calls to the ATA extension 2202:

General		
Name:	To ATA2	
Type: Name	Source	Destination
PSTN: Controller1	☐	-
PSTN: Controller2	☐	-
SIP: Lync	☒	-
SIP: ATA2201	☐	-
SIP: ATA2202	☐	Master
SIP: Forbidden Call (disabled)	☐	-
Max. call attempts for this route in a failover scenario:	0 (0 = try all selected destinations)	

Address Normalization For Condition Processing (Using Source Dialplan)	
Use Dialplan:	☒
Number format:	International number
Encoding:	Use type flag

Conditions			
Called number	Calling number	Redirect number	
~+17165552202\$			Delete
Add			

Address Manipulation	
OK	Cancel

16. Create the sixth route to route calls from the Lync Server to the PSTN. To do so, click **Add** in the **Routing** section, and configure the following parameters:

General		
Name:	Lync-to-PSTN	
Type: Name	Source	Destination
PSTN: Controller1	☐	Master
PSTN: Controller2	☐	Master
SIP: Lync	☒	-
SIP: ATA2201	☐	-
SIP: ATA2202	☐	-
SIP: Forbidden Call (disabled)	☐	-
Max. call attempts for this route in a failover scenario:	0 (0 = try all selected destinations)	
Address Normalization For Condition Processing (Using Source Dialplan)		
Conditions		
Address Manipulation		
OK Cancel		

- **Name:** Enter a unique name to easily identify the route.
- **Source:** Select the SIP peer configured for the Lync Server as a source.
- **Destination:** Select both controllers as Master destinations.

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

17. Create the seventh route to route calls from the FSX ATA to the Lync Server. To do so, click **Add** in the **Routing** section, and configure the following parameters:

General		
Name:	From ATA	
Type: Name	Source	Destination
PSTN: Controller1	☐	-
PSTN: Controller2	☐	-
SIP: Lync	☐	Master
SIP: ATA2201	☒	-
SIP: ATA2202	☒	-
SIP: Forbidden Call (disabled)	☐	-
Max. call attempts for this route in a failover scenario:	0 (0 = try all selected destinations)	
Address Normalization For Condition Processing (Using Source Dialplan)		
Conditions		
Address Manipulation		
Address map:	FromATA	
OK Cancel		

- **Name:** Enter a unique name to easily identify the route.
- **Source:** Select the SIP peers for the two ATA extensions as sources.
- **Destination:** Select the SIP peer for the Lync Server as a master destination.

Under **Address Manipulation**, select the address map configured for calls from the ATA to the Lync Server. This address map makes the calls appear like internal calls to the Lync Server.

18. To use TLS for authentication and data encryption purposes, upload a certificate and key as described in [Setting up a Security Profile](#) on page 45. The host name in the security profile must match the common name in the certificate.

CHAPTER 15

SNMP Support For A Dialogic® Diva® Media Board

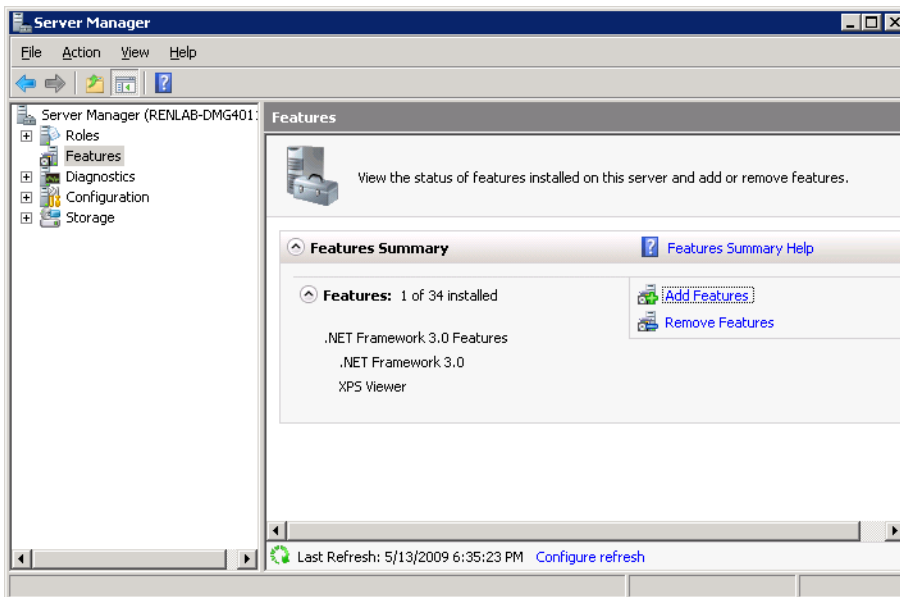
The Windows® implementation of the Simple Network Management Protocol (SNMP) is used to configure remote devices or to monitor network performance, to audit network usage, and to detect network faults or inappropriate access. The SNMP support is only available if the service is installed for your operating system. The output formats are defined in the MIB specification. To see the messages of the SNMP, you need specific SNMP tools that are not part of the Dialogic® Diva® System Release software. To activate the SNMP service, use the Dialogic® Diva® Configuration Manager as described below.

To activate SNMP support for a Dialogic® Diva® Media Board

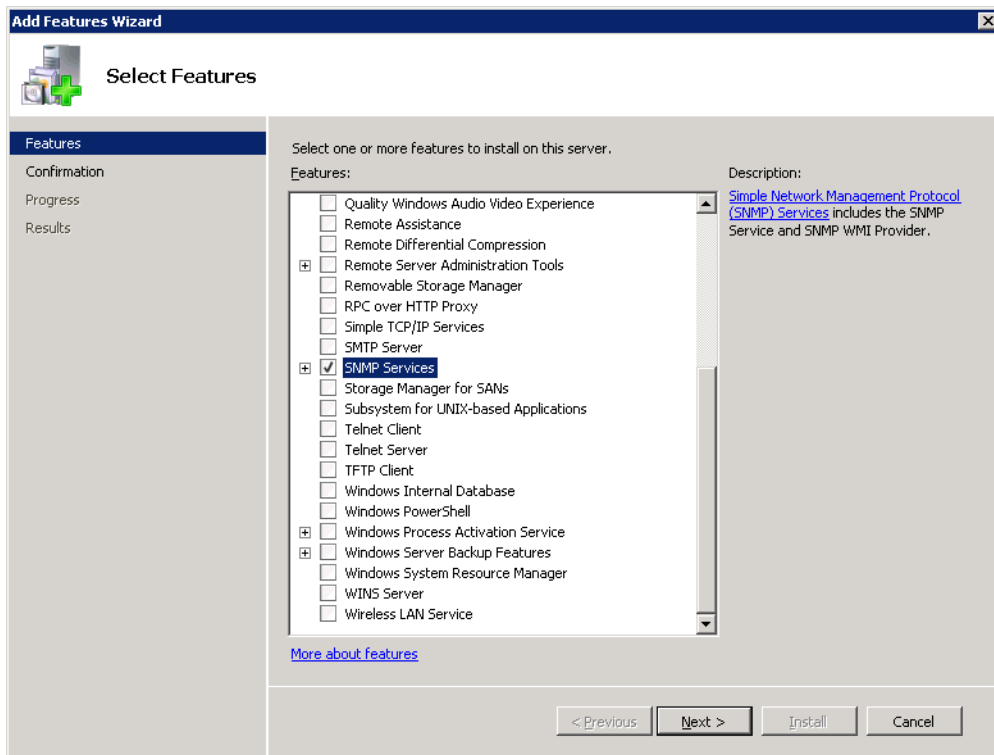
1. Install the Windows® SNMP Service as described below.
2. Add the SNMP Service in the Diva Configuration Manager as described on page 151.
3. Install an SNMP tool, e.g., Net.SNMP (optional, for testing only).
4. Restart your computer.
5. Verify the service status as described on page 151.
6. Verify the function of the SNMP Service as described on page 153.

To install the Windows® SNMP Service under Microsoft® Windows Server® 2008 and Microsoft® Windows Server® 2008 R2:

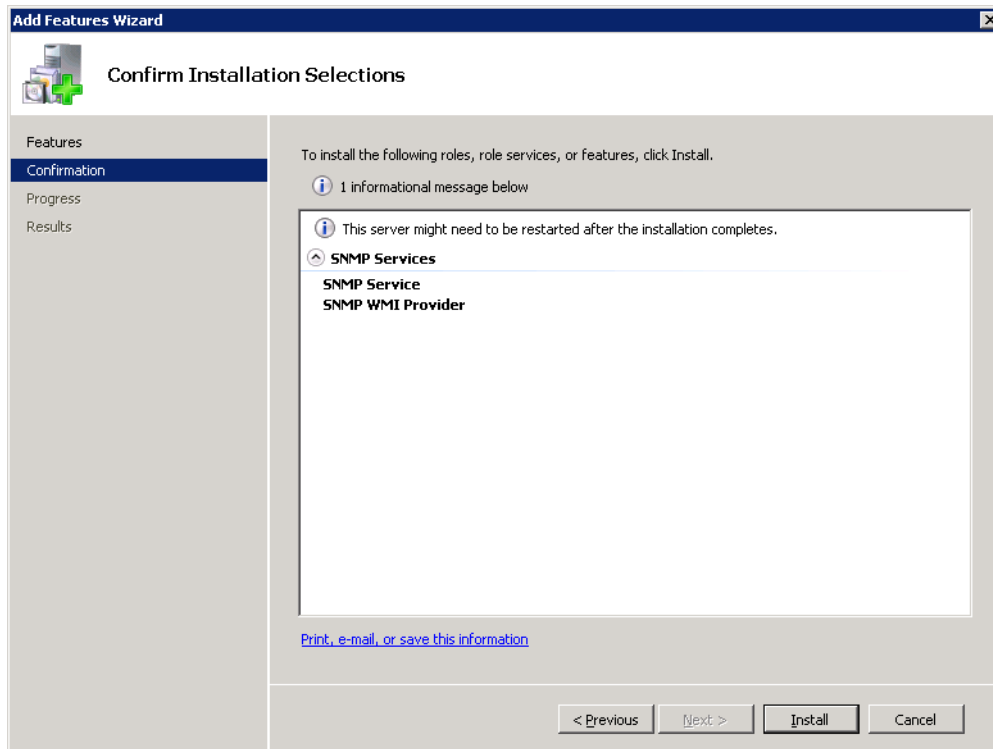
1. Open the Microsoft® Server Manager via **Start > Server Manager**.
2. In the **Server Manager** window, go to **Features** and click the **Add Features** link.



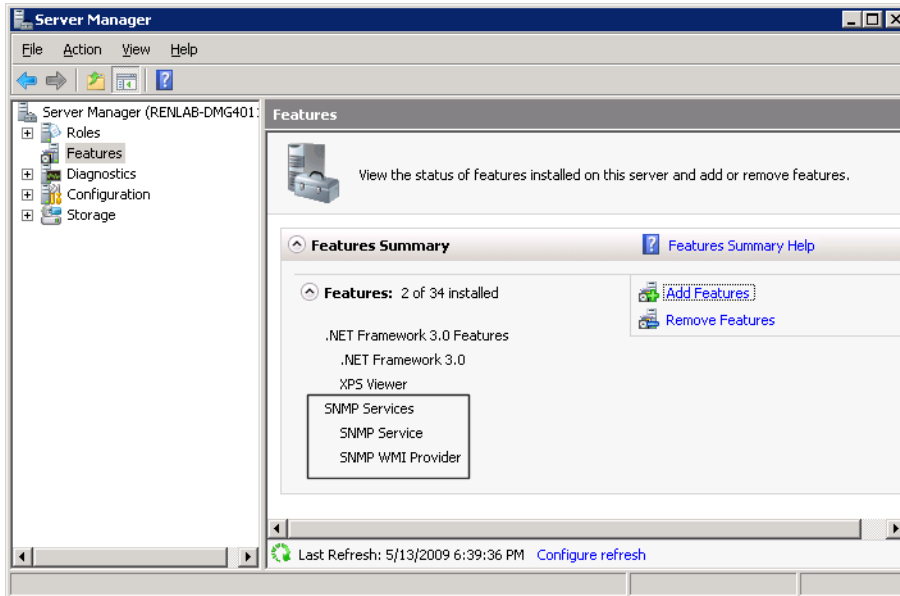
3. In the **Add Features Wizard** window, select **SNMP Services** and click **Next**.



4. Click **Install**, to install the SNMP Services.



5. After the installation of the SNMP Services has finished, close the **Add Features Wizard** window. You will see the SNMP Services added to the list of installed features in the **Server Manager** window.



You can now add the SNMP Service to the Dialogic® Diva® Configuration Manager as described below.

To add the SNMP Service in the Dialogic® Diva® Configuration Manager

1. Click **Start > All Programs > Dialogic Diva > Configuration Manager** to open the Diva Configuration Manager.
2. In the menu bar, click **Insert > SNMP Service**. The SNMP Service is added to the Services layer.
3. Activate the configuration. Once the configuration is activated, the Dialogic® Diva® System Release software validates if Windows® SNMP support is available. If it is not available, an error message is displayed and the SNMP icon is removed from the configuration.

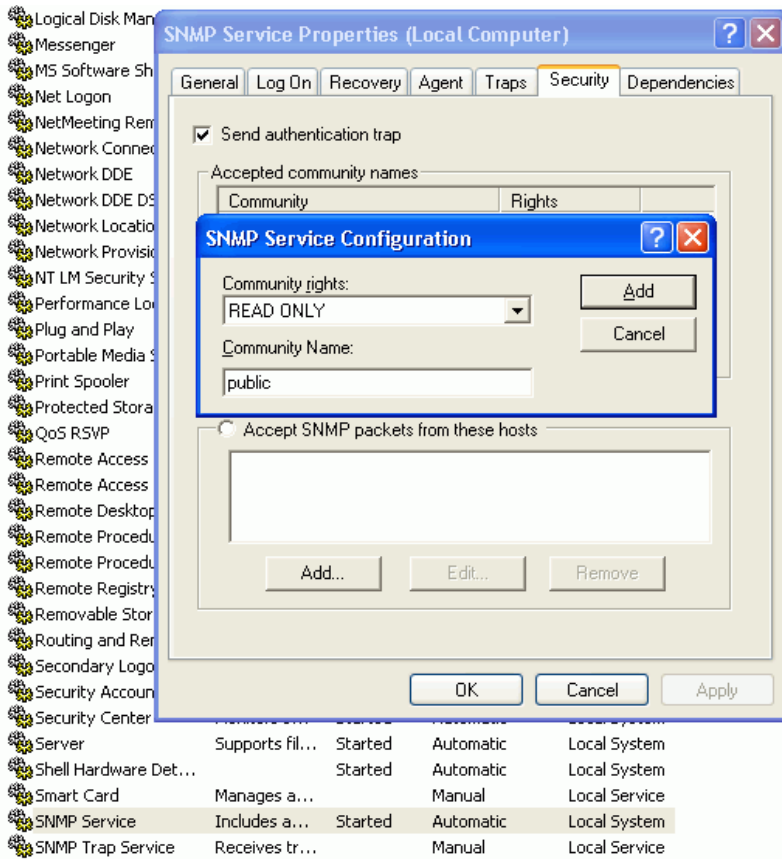
Note: You do not need to connect the SNMP service to any Dialogic® Diva® Media Board. The SNMP is always available for all installed Diva Media Boards.

You can now install the SNMP tool and restart the PC. To install the SNMP tool correctly, consult the documentation of the tool.

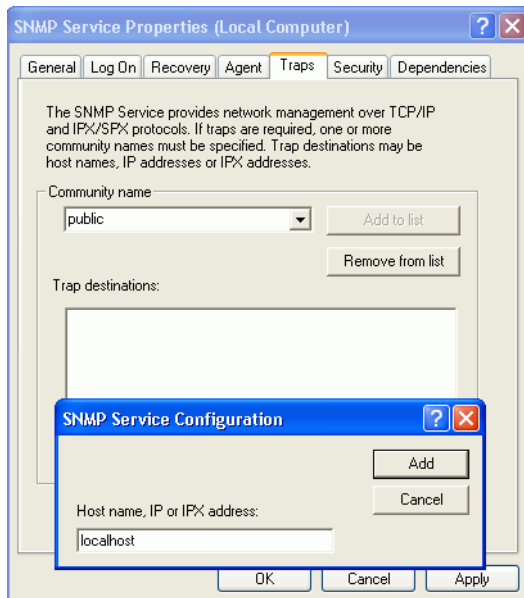
To verify the service status

1. Click **Start > Control Panel > Administrative Tools** to open the **Administrative Tools** window.
2. In the **Administrative Tools** window, double-click **Services**.
3. In the **Services** window, right-click **SNMP Service** and select **Properties** from the list.

4. In the **Properties** dialog box, click the **Security** tab and under **Accepted community names**, click **Add**. Enter a community name, for instance, public, and for **Community rights**, select **READ ONLY**.



5. Click the **Traps** tab, enter the community name you added in the **Security** tab, and click **Add to list**.
6. Under **Traps destinations**, click **Add**, enter the name or IP address of the host computer, and click **Add**.



7. The host name is added to the list of Trap destinations.
8. Click **OK** to close the dialog box.

9. Restart the SNMP Service. To do so, right-click **SNMP Service** in the **Services** window and select **Restart** from the list.
10. Close the **Services** window.

To verify the function of the SNMP Service

1. Click **Start > Run** and type cmd to open a DOS window.
2. In the DOS window type: `snmpwalk -v 2c -c public localhost interface | find "Diva"`

The result should be similar to the following, which is for a Dialogic® Diva® V-4PRI Media Board:

```
IF-MIB::ifDescr.101 = STRING: Dialogic_Diva_V-4PRI/E1/T1_1030
IF-MIB::ifDescr.133 = STRING: Dialogic_Diva_V-4PRI/E1/T1_1030
IF-MIB::ifDescr.164 = STRING: Dialogic_Diva_V-4PRI/E1/T1_1030
IF-MIB::ifDescr.195 = STRING: Dialogic_Diva_V-4PRI/E1/T1_1030
```

3. In the DOS window type: `snmptrapd -f -L o`

The result should be similar to the following:

```
2006-01-28 11:14:35 NET-SNMP version 5.2.1.2 Started.
```

You can create an output of traps if you change the status of the layer 1/2, for instance by disconnecting the cable from the Diva Media Board. The result after changing the status of layer 1/2 should be similar to the following:

```
2006-01-28 11:16:25 localhost [127.0.0.1] (via UDP: [127.0.0.1]:1053) TRAP, SNMP v1, community public
```

```
SNMPv2-SMI::enterprises.434.2 Link Up Trap (0) Uptime: 1:16:47.06
```

```
IF-MIB::ifIndex.101 = INTEGER: 101
```

```
SNMPv2-SMI::enterprises.434.2 Link Down Trap (0) Uptime: 1:16:48.57
```

```
IF-MIB::ifIndex.101 = INTEGER: 101
```

```
2006-01-28 11:16:26 localhost [127.0.0.1] (via UDP: [127.0.0.1]:1053) TRAP, SNMP v1, community public
```

```
SNMPv2-SMI::enterprises.434.2 Link Up Trap (0) Uptime: 1:16:48.81
```

```
IF-MIB::ifIndex.101 = INTEGER: 101
```

Supported MIBs, OIDs, and traps

This section provides information about supported MIBs, OIDs, and traps by the Dialogic® Diva® SNMP service and about the relationship between supported OIDs and Dialogic® Diva® Media Board management interface variables.

MIB-II (RFC 1213/2233)	Path	Description
MIB-II	interfaces.ifTable.ifEntry.	
	ifIndex	Unique index of Dialogic® Diva® interfaces starting with ifIndex-offset + 1 (see option -oN). First, all installed Dialogic® Diva® Media Boards are listed, followed by the available B-channels.
	ifDescr	For Diva Media Boards, the board name and it's serial number are returned. For B-channels, the string "BRI + ifIndex_of_board + number_of_b- channel_on_board" is returned.
	ifType	The type of the interface according to IANA: PRI, BRI, ISDN.
	ifMTU	Since the concept of MTU is not applicable on Dialogic® Diva® interfaces, they return always 0.
	ifSpeed	The maximum interface speed in bps
	ifAdminStatus	Always up
	ifOperStatus	The current operating status of the interface

	ifInBytes, ifInPackets, ifInErrors, ifOutBytes, ifOutPackets, ifOutErrors	For Dialogic® Diva® Media Boards, the added values of the D- and B-channel interface counters are returned. mantool reports these values in the following paths "Statistics\\[D B]-Layer2\\[R X]-[Bytes Frames Errors]". For B-channels, the following values are reported: "State\\B[n]\\L2 Stats\\R- [Bytes Frames Errors]".
	ifPhysAddr	Returns vendor-id, PnP-id, serial number of Diva Media Boards formatted as hex string. Returns no information for B-channels.
	LinkUp/LinkDown Traps	For status changes of interfaces a trap is generated that includes the appropriate ifOperStatus varbind. Trap destinations and access parameters must be configured in the underlying master agent (trapsink, etc.).
ISDN-MIB (RFC2127)	transmission.isdnMib.isdnMibObjects.isdnSignalingGroup	
	isdnSignalingGetIndex	Number of possible D-channels (equals number of installed Diva Media Boards)
ISDN-MIB	transmission.isdnMib.isdnMibObjects.isdnBasicRateGroup.isdnBasicRateTable.isdnBasicRateEntry	Dialogic® Diva® BRI Media Boards
	isdnBasicRateIfType	isdns or isdnu (IANA-ifType 75, 76)
	isdnBasicRateLineTopology	pointToPoint or pointToMultipoint
	isdnBasicRateIfMode	TE mode or NT mode
	isdnBasicRateSignalMode	D-channel active or inactive
ISDN-MIB	transmission.isdnMib.isdnMibObjects.isdnBearerGroup.isdnBearerTable.isdnBearerEntry	B-channels
	isdnBearerChannelType	dialup or leased
	isdnBearerOperStatus	idle, active, unknown
	isdnBearerChannelIndex	Index of B-channel per Diva Media Board
	isdnBearerPeerAddress	Remote address
	isdnBearerPeerSubAddress	Remote sub address
	isdnBearerCallOrigin	Answer or originate
	isdnBearerInfoType	Info type as per Q.931 (unrestrictedDigital)
	isdnBearerCallConnectTime	Time measured from start of divasnmplx
DIAL-CONTROL-MIB	transmission.dialControlMib.dialControlMibObjects.callActive.callActiveTable.callActiveEntry	
	callActiveSetupTime	Timeticks at start of call, measured from start of divasnmplx .
	callActiveIndex	Unique index
	callActivePeerAddress	Address of remote partner
	callActivePeerSubAddress	Subaddress of remote partner
	callActivePeerId	Always 0 (unknown)
	callActivePeerIfIndex	Always 0 (unknown)

	callActiveLogicalIfIndex	Index of entry in ifTable for the interface used by this call.
	callActiveConnectTime	0 if the call was not connected, otherwise timeticks measured from start of divasnmpx .
	callActiveCallState	State of call
	callActiveCallOrigin	Direction of call: Answer or originate
DIAL-CONTROL-MIB (RFC2128)	transmission.dialControlMib.dialControlMibObjects.callHistory	
	callHistoryTableMaxLength	The maximum number of entries in the callHistoryTable (read/write).
	callHistoryRetainTimer	The minimum amount of time in minutes that a callHistoryEntry will be maintained before being deleted.
DIAL-CONTROL-MIB	transmission.dialControlMib.dialControlMibObjects.callHistory.callHistoryTable.callHistoryEntry	
	callHistoryPeerAddress	Address of remote partner
	callHistoryPeerSubAddress	Subaddress of remote partner
	callHistoryPeerId	Always 0
	callHistoryPeerIfIndex	Always 0
	callHistoryLogicalIfIndex	Index of entry in ifTable for the interface used by this call.
	callHistoryDisconnectCause	Reason for disconnecting this call
	callHistoryDisconnectText	empty
	callHistoryConnectTime	Timeticks measured from start of divasnmpx .
	callHistoryDisconnectTime	Timeticks measured from start of divasnmpx .
	callHistoryCallOrigin	Direction of call: Answer or originate.

The definition for the ISDN-, DIAL-CONTROL-, and DS1-MIB can be imported into any management application to decode the OIDs reported by **divasnmpx**. For net-snmp, simply copy these files to the standard MIB path (usually <%program files%>\netsnmp\share\snmp\mibs) and tell the snmp command line tools to use them by exporting/setting the environment variable "MIBS" with the names of the appropriate MIBs (or simply the keyword ALL), e.g., **Set MIBS=ALL**.

CHAPTER 16

Verify The Line Configuration With The Dialogic® Diva® Line Test Tool

To check the line configuration, use the Dialogic® Diva® Line Test tool available under **Start > Programs > Dialogic Diva > Line Test**. You need to login via Remote Desktop or on the local console with local administrative rights to use this tool.

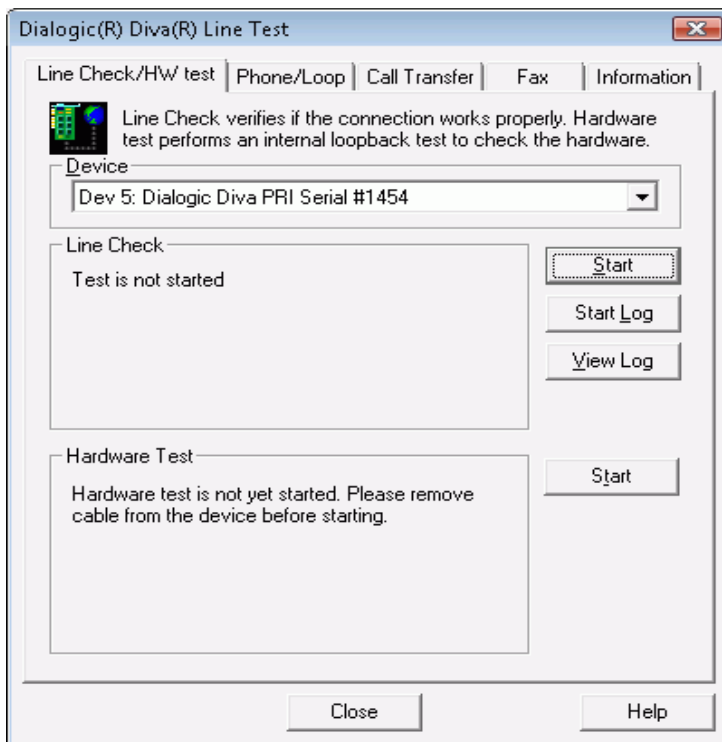
The Diva Line Test tool offers the following tests:

- [Line Check](#): Performs a quick check of your Dialogic® Diva® System Release software installation and the physical connection.
- [Hardware test](#): Performs a test of the physical controller only.
- [Phone/Loop test](#): Performs basic inbound or outbound phone tests to test the connection to other telephones or to itself.
- [Call Transfer](#): Performs different call transfer tests, with the option to choose the transfer type.
- [Fax test](#): Performs basic inbound or outbound fax tests.

The Diva Line Test tool also has a Blink LED button integrated on the information page to easily identify a physical Diva Media Board or the physical line of a controller.

Line Check

1. Open the Diva Line Test tool and click the **Line Check / HW Test** tab.



2. Under **Device** select the line of the Dialogic® Diva® Media Board to test.
3. Click **Start** to begin the test.

If the line check test reports an error, verify that:

- the cabling is connected correctly.
 - the switch type, network type, and ISDN or phone numbers are configured correctly in the Dialogic® Diva® Configuration Manager.
 - the SPIDs (Service Profile Identifiers) are configured correctly in the Diva Configuration Manager if you use a North American switch type.
 - the Diva Media Board is not conflicting with any other hardware.
 - the telco company is not experiencing any issues.
4. If line check reports no issues, and you are still having trouble connecting, there might be a problem in the configuration of the application you are using with your Diva Media Board (such as Dial-Up Networking or fax software). Check the configuration and repeat the test.
 5. Click **Stop** to abort the test.
 6. If you wish to trace the test for analyzing purposes, you can create a trace file.
 7. Click **Close** to end the configuration dialog.

Hardware test

The hardware test performs a test of the controller only. It changes the controller to run under the internal loop-back mode. Starting with the first channel, the hardware test tries to connect/disconnect each channel and stops when the highest channel is tested.

1. Open the Diva Line Test tool and click the **Line Check / HW Test** tab
2. Select under **Device** the line of the Dialogic® Diva® Media Board to test.
3. Click **Start** to begin the test.

If the hardware test reports an error, verify that:

- the cable is NOT connected to the board,
- the Diva Media Board is loaded correctly,
- the newest Dialogic® Diva® System Release software is installed,
- the test is successful with a standard protocol like ETSI or NT1.
- If the test still fails, contact the Dialogic Customer Support personnel. For more information, see [Customer Service](#) on page 167.

Note: To help you as efficiently as possible, the Customer Support personnel will ask you for details of the tests you have conducted and their results. So, be sure you have all information handy when contacting them.

4. Click **Stop** to abort the test.
5. Click **Close** to end the configuration dialog.

Phone / Loop test

The phone test performs an outgoing call to verify the connectivity to another telephone. You can stop the test once the remote phone is ringing. If the phone answers the call, an announcement is played.

The loop test performs an incoming call to itself to test the end-to-end connectivity with an inbound tone test. Since some networks use a different channel allocation (like different Q.SIG versions), it might be possible to connect a call despite the wrong physical channel being in use or not operational at all.

1. Under **Device** select the line of the Dialogic® Diva® Media Board to test.
2. Enter the **Called Party Number** and **Calling Party Number**.
3. To configure advanced settings, click **Advanced**. For more information, see [Advanced setup](#) on page 159.
4. If you wish to test incoming calls, select **Loop Test (enables incoming calls)**.

For incoming calls, the program accepts the call if it is pending and the address is valid or not specified. Then it activates the detection of DTMF tones and an announcement is played. If a DTMF tone is detected,

the announcement is stopped and the same DTMF tone is replied with delay to the calling party. The test is passed successfully only if the DTMF tone is received at the calling party.

5. To trace outgoing or incoming calls for analysis, you can create a trace file.
6. After you have entered all necessary information, you can start the test by clicking **Call**.
7. If a issues occurs that you cannot resolve, you may obtain technical support. For more information, see .
8. To abort the test manually, click **Disconnect** during the test.
9. To delete all messages from the status box, click **Clear**.
10. All performed tests are saved in a text file. To view this file, click **History**.

Note: The information in the history file is overwritten every time you open the Diva Line Test tool. If you want to keep the information of a specific call, save the file in a different folder.

Advanced setup

Normally it is not necessary to change the predefined advanced settings. Change the values only for test purposes. The following settings are available in the **Advanced Setup** dialog box:

1. If you wish to test incoming calls on a specific number, enter it in **Dialed for**. Incoming calls for another number are not accepted.
2. Under **Type of Number** you can choose from the following:
 - **Unknown (Default)**: Use this type of number if you do not know how your PBX is configured or when the PBX has no knowledge of the type of number, e.g., international or national. You need to enter all necessary prefixes.
 - **International**: Select **International** if the PBX understands the number as international. Instead of entering 0049 as international prefix and country code for Germany for example, you need to enter only 49.
 - **National**: Select this type of number if the PBX understands it as national. Instead of entering 0711 as city code for example, you need to enter only 711.
 - **Network**: Select this type of number if you use a network specific coding.
 - **Subscriber**: Select **Subscriber** if your PBX understands that it is a number without country code and city code.
 - **Abbreviated**: Select if you use a quick dialing number to test the line.
3. Under **Number Plan ID** you can choose from the following:
 - **Unknown (Default)**: Change in specific cases and for test purposes only.
 - **ISDN Telephony**: Some countries require an ISDN number plan.
 - **Data**: Select this option if the call you want to test is a specific number plan for a data call.
 - **National**: Select this option if your provider is using a national numbering plan.
 - **Private**: Select this option if your provider or PBX is using a private numbering plan.
4. Under **Presentation Indicator** you can choose from the following:
 - **Allowed**: The calling party number is presented to the called party.
 - **Restricted**: The calling party number is not presented to the called party.
 - **Not Available**: You may want to use this option for test purposes.
5. Under **Screening Indicator** you can choose from the following:
 - **Not screened**: If you specify a calling party number and select this option, the number is not screened.
 - **Verified and passed**: If you specify a number, it is verified by the network. If the number is correct, it is passed to the application.

- **Verified and failed:** If you specify a number, it is verified by the network. If the number is wrong and you have a Point-to-Point configuration, the number is not passed to the application. If you have a Point-to-Multipoint configuration, the wrong number is ignored and the MSN is added.
- **Network-provided:** If you do not specify a number, the network generates one with the bit set to "Network provided".

Call Transfer

This test transfers a call to the configured destination number. In this tab you can select the transfer method, e.g., if a consultation call is used or if the call is put on hold before it is transferred.

Note: To test a call transfer, the supplementary services Call Deflection and Explicit Call Transfer need to be supported.

1. Under **Device** select the line of the Dialogic® Diva® Media Board to test.
2. Enter the number to which the call should be transferred in **Called Party Number** under **Transfer Destination**.
3. To configure the transfer type, consultation call, and completion mode, click **Advanced** under **Transfer Type**. For more information, see [Advanced transfer setup](#) on page 160.
4. Click **Start**.
5. If you are prompted in the **Status** box, dial in from another application or phone.
6. The displayed message in the **Status** box notifies you if the test was successful or not. If the test is not terminated automatically, click **Stop**.
7. During the transfer test you can also create a trace file.
8. If you cannot set up a call transfer and you cannot locate the cause of the issue, you may obtain technical support. For more information, see [Customer Service](#) on page 167.
9. All performed tests are saved in a text file. To view this file, click **History**.

Note: The information in the history file is overwritten every time you open the Diva Line Test tool. Thus, if you want to keep the information of a specific call, save the file in a different folder.

Advanced transfer setup

Note: The settings are only valid while the Dialogic® Diva® Line Test tool is opened.

Select under **Transfer Type** how the call should be transferred:

- the call should be transferred without consultation call, or
- the call should be answered and the incoming call should be placed on hold, or
- the call should be answered but the incoming call is not placed on hold.

If the incoming call is put on hold, you can choose under **Consultation Call** whether to transfer the consultation call on the same or on a different line.

Moreover, if you transfer the call with a consultation call, you can decide under **Complete Transfer Type** whether the call is completed in ringing state or after the call is connected.

Fax test

With the fax test you can send or receive a fax document that you can view with a fax viewer.

1. Under **Device** select the line of the Dialogic® Diva® Media Board to test.
2. Enter the **Called Party Number** and **Calling Party Number**.
3. To configure advanced settings, click **Advanced**.
4. If you wish to test incoming fax calls from another device, select **Receive incoming fax**. With this test you can verify if another Diva Media Board, a controller of a Diva multiport Media Board, or the PBX is working correctly.

If you do not have another application to test incoming fax calls, you can open the Dialogic® Diva® Line Test tool twice and configure one utility as the calling party and the other utility as the called party. For more information, see [To set up a test for incoming fax calls](#) below.

5. To trace outgoing or incoming calls for analysis, you can create a trace file. After you traced an incoming or outgoing fax, the option **Play Audio** is available. Click this button to save a wave file of the transmitted or received fax. This might be necessary for analysis.

Note: You can only save the wave file of the trace as long as the Diva Line Test Tool is opened. Once you close the tool, the unsaved wave file will be deleted.

6. After you have entered all necessary information you can start the test. To do so, click **Call**.
7. If an issue occurs that you cannot resolve, you may obtain technical support. For more information, see [Customer Service](#) on page 167.
8. To abort the test manually, click **Disconnect** during the test.
9. To delete all messages from the status box, click **Clear**.
10. All performed tests are saved in a text file. To view this file, click **History**.

Note: The information in the history file is overwritten every time you open the Diva Line Test tool. If you want to keep the information of a specific call, save the file in a different folder.

To set up a test for incoming fax calls

1. Open two Dialogic® Diva® Line Test tools and click the **Fax** tab.
2. Select the devices to test under **Device**.
3. At one utility enter the **Called Party Number** and **Calling Party Number** under **Call Settings**.
4. At the other utility do not enter any number under **Call Settings** and select **Receive incoming fax** for the fax test.
5. You can also configure advanced settings for both Diva Line Test tools.
6. Click **Call** on the sending Diva Line Test tool to start the test.
7. To see if the fax was transmitted correctly, click **View Fax**.

Note: If the tool receives a fax more than twice without saving, the fax result file will be overwritten.

8. During the test you can also create a trace.
9. If an issue occurs that you cannot resolve, you may obtain technical support.

To write a message into a trace file

1. Click **Start Log**.
2. Click **Call** or **Start** to start the test call.
3. If the call is finished, click **Stop Log**.
4. Click **View Log** to open the log file in a separate editor. You might want to save the file for analysis.
5. After you traced an incoming or outgoing fax, the option **Play Audio** is available. Click this button to save a wave file of the transmitted or received fax. This might be necessary for analysis.

Note: You can only save the wave file of the trace as long as the Dialogic® Diva® Line Test tool is open. Once you close the tool, the unsaved wave file will be deleted.

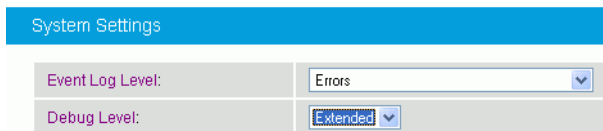
CHAPTER 17

Create a Trace With The Dialogic® Diva® Diagnostics Tool

To create a trace for the Dialogic® Media Gateway Series, you need to set the correct debug level in the Dialogic® Diva® SIPcontrol™ software web interface first. Then you can create a trace in the Dialogic® Diva® Diagnostics tool. You need to login via Remote Desktop or on the local console with local administrative rights to use this tool.

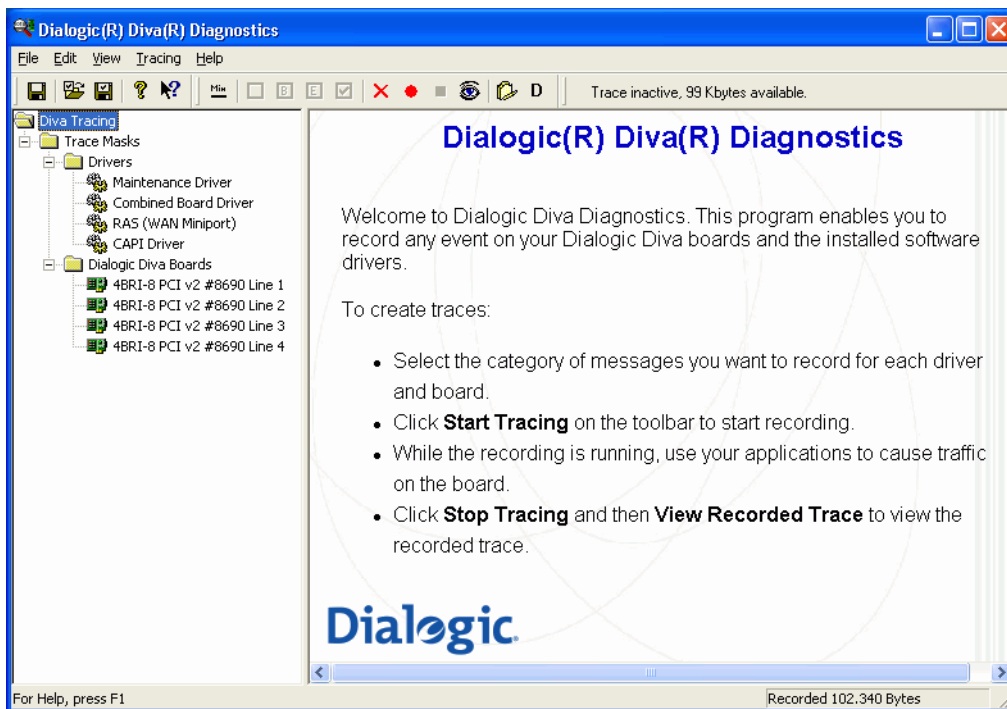
To set the correct debug level in the Dialogic® Diva® SIPcontrol™ software web interface:

1. Click **Start > Programs > Dialogic Diva > SIPcontrol Configuration** to open the Diva SIPcontrol software web interface.
2. Click **SIPcontrol** on the left hand side to open the configuration interface.
3. In the configuration interface, click **System Settings** and set the **Debug level** to **Extended**.

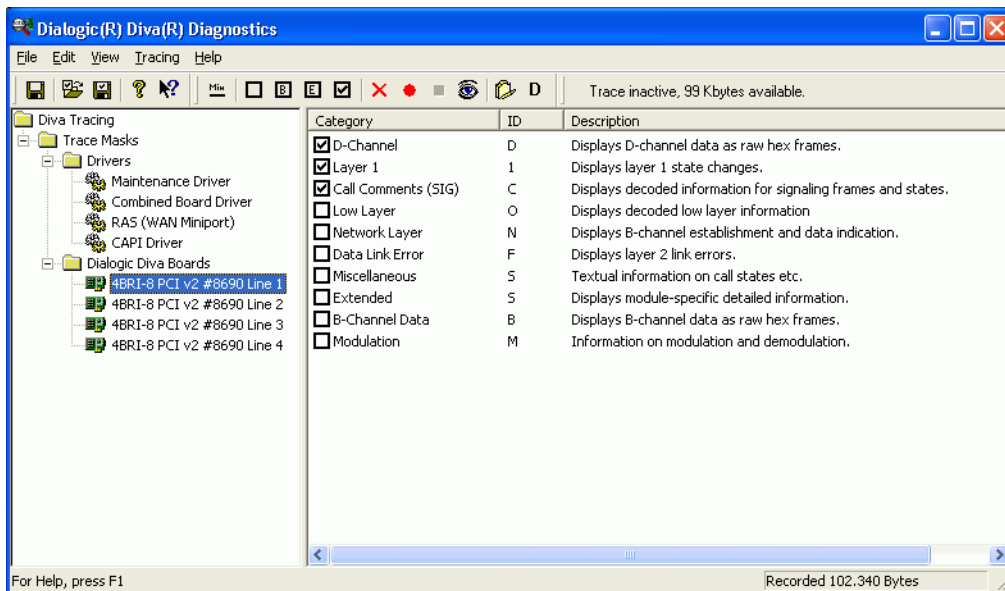


To create a trace with the Diva Diagnostics tool:

1. Click **Start > Programs > Dialogic Diva > Diagnostics**, to open the Diva Diagnostics tool. In the left pane you will see the installed software drivers and the controllers of the installed Dialogic® Diva® Media Boards.



- Click the controller of the Dialogic® Diva® Media Board for which you want to create a trace. In the right pane, the different trace categories and their descriptions are displayed. Leave the trace settings at their default values.



- Click **Tracing > Start Tracing** or click the start trace button  in the toolbar, to start the trace.
- Use your applications to cause traffic on the board.
- Click **Tracing > Stop Tracing** or click the stop trace button  in the toolbar, to stop the trace.
- Click **View > View Recorded Trace** or click the view trace button  in the toolbar, to view the trace.
- You can also save the recorded trace. To do so, click **File > Save Recorded Trace** or click the save trace button .
- In the displayed dialog box, select the folder where you want to save the trace file or create a new folder if required.
- Enter the file name and click **Save**.

For detailed information about the Diva Diagnostics tool, see the Dialogic® Diva® Diagnostics Online Help under **Help > Help Topics**.

CHAPTER 18

Backing up and Restoring the Configuration

The Dialogic® 4000 Media Gateways provide a restore and backup menu. You can access this menu if you press the left ALT key during the boot sequence. The menu provides the following options:



Restore to factory defaults: The system partition C: is set to default factory state. If you choose this option and you accept to restore the factory defaults, the current system partition will be deleted.

Create backup: An image of the current Dialogic® 4000 Media Gateway system partition C:, including all settings, is created and stored under D:/backup. The backup is overwritten every time you create a new backup. If you need to keep a backup with certain settings, save it in a different directory or on an external medium.

Restore previous backup: With this option, you can restore a previously saved backup of the system partition, including all Dialogic® 4000 Media Gateway settings. This might be necessary if you need to re-activate the settings of a configuration you saved earlier. If you choose this option, the current system partition C: will be deleted.

Reboot: Restarts the Dialogic® 4000 Media Gateway.

Shut Down: Shuts down the Dialogic® 4000 Media Gateway.

If you do not choose any of the settings, the Dialogic® 4000 Media Gateway will be restarted after the time displayed at the bottom of the dialog box has elapsed.

CHAPTER 19

Customer Service

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

For more information see:

- [Dialogic® Diva® Support Tools](#)
- [Dialogic Services and Support Web Site](#)
- [Dialogic Customer Support](#)

Dialogic® Diva® Support Tools

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

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

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

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

Dialogic Services and Support Web Site

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

- Detailed information about the Dialogic® Pro™ Services (1 or 5 year 24/7 service contracts) at <http://www.dialogic.com/support/DialogicPro/>
- A Help web section for Dialogic® products at <http://www.dialogic.com/support/helpweb>
- A download section to install the newest version of your software at <http://www.dialogic.com/support/downind.asp>
- A training section with information about webinars, online, and onsite trainings at <http://www.dialogic.com/training/default.htm>
- A manuals section that provides a complete set of available documentation at <http://www.dialogic.com/manuals/default.htm>
- Technical discussion forums about different developer-specific Q&A at <http://www.dialogic.com/den/groups/developers/default.aspx>
- The Dialogic Customer Support site. For detailed information about how to contact Dialogic Customer Support, see [Dialogic Customer Support](#) on page 168.

Dialogic Customer Support

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

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

- A debug trace (see the Dialogic® Diva® Diagnostics Online Help file - DivaTrace.chm.)
- A copy of your active Dialogic® Diva® System Release configuration (see the Dialogic® Diva® Configuration Manager Online Help file - DSMain.chm).
- A copy of your Diva SIPcontrol configuration.

To save a copy of your Diva SIPcontrol configuration, follow these steps:

1. Access the Diva SIPcontrol web interface.
2. In the Overview section, click **Save GUI settings**.
A User Prompt dialog appears.
3. Enter a name for the saved profile, and click **OK**. The profile name can contain characters, digits, and the underscore character (_).
4. In the Config.-Profiles field in the Overview section, select the saved profile, and click **Export to file**.
The File Download dialog appears.
5. Click **Save** to save the exported file, and then follow the prompts.
6. Send the saved file to Dialogic Customer Support.