OfficeMaster Gate

Installation
Worth knowing
Configuration
Advanced Configuration
Appendix

User manual for administrators | Ferrari electronic AG

Copyright © 2017 Ferrari electronic AG

Ferrari electronic

We endeavoured to collect and describe information with best accuracy. However, we cannot exclude the possibility of minor faults within this manual. Ferrari electronic will not be held liable for mistakes and their consequences. Please address hints and comments to:

info@ferrari-electronic.de.

Ferrari electronic provides a forum for technical discussions and quick help. Access the forum at

http://forum.ferrari-electronic.de

Publisher: Ferrari electronic AG
Ruhlsdorfer Str. 138
(DE) 14513 Teltow

Internet: www.ferrari-electronic.com
Phone: +49 3328 455 90
Fax: +49 3328 455 960
E-Mail: info@ferrari-electronic.de
Authors: Johann Deutinger, Chris Helbing, Jeffrey Nimpadu

Correct as of 19.05.2017

Preamble

Thank you for your trust in products of Ferrari electronic AG and your decision to use OfficeMaster.

Ferrari electronic is a leading German manufacturer of hardware and software for unified communications. The OfficeMaster range of products enhances all popular e-mail and application systems with functions for fax, SMS and voicemail. The hardware seamlessly connects a company's telecommunications infrastructure with the existing information technology. Customers benefit from greater efficiency and streamlined business processes.

We hope the product satisfies your companies needs entirely. In case of questions or suggestions please email:

info@ferrari-electronic.de

Table of content

Ferrari electronic

1. INSTALLATION

Network Integration

SBA

Update & Upgrade

User manual for administrators | Ferrari electronic AG

Copyright © 2017 Ferrari electronic AG

Ferrari electronic

1. Installation

1.1. ISDN Port

An important use of OfficeMaster Gate is as phone gateway for Microsoft's UC-systems. The Gateways passed the necessary certification tests for those systems and can therefore be used restrictive free - both as stand-alone Gateways and in combination with the OfficeMaster software, using the hardware and ISDN-ports together for all communication services (Fax, SMS, voice mail and telecommunication).

The communication can optionally take place encrypted (SIP/TCP, RTP) or unencrypted (SIP/TLS, SRTP).

Table 1.1: Signal flow on the ISDN ports

3	Rx+ (a2)	→ +	3
4	Tx+ (a1)	← +	4
5	Tx- (b1)	← -	5
6	Rx- (b2)	→ -	6
1		→ +	1
2		→ -	2
4		← +	4
5		← -	5

Located left and right below the BRI port of OfficeMaster Gate are two LED's. These are triggered by the firmware of the controller:

- The right hand side LED is triggered, when layer 1 of the ISDN protocol is activated.
- The left hand side is triggered, when the in-build ISDN terminating resistors are triggered via the configuration program.

Note! In older versions of the hardware, the left hand side LED is triggered, when the terminating is turned off! In all cases though, the settings in the configuration program apply.

Should an additional ISDN device be connected to the same BRI as OfficeMaster Gate it is mandatory that the ISDN port is declared as a multiple-device-port (point-to-multi point). When used in parallel connection, OfficeMaster Gate and others connected to this line need differing MSN (Multiple Subscriber Number) to be assigned to them. Is the ISDN line in point-to-point mode, no parallel connection is possible.

1.2. Network Integration

OfficeMaster Gate is addressed by the OfficeMaster Server-Software or, if used as media gateway, via the network. The Server-Software in this case is the component OMCUMS of the messaging server.

OfficeMaster Gate and OMCUMS communicate via TCP/IP. For this, they need to know each others IP addresses.

If used as media gateway, the communication with Microsoft servers occurs in the same way.

To make this possible, every OfficeMaster Gate is in need of a fitting network address. Possible ways of ensuring this:

With DHCP server

OfficeMaster Gate in delivery condition (standard, even after resetting) receives its IP-configuration from the in the network existing DHCP server. Via a DHCP server, IP-addresses and the Domain Name Server (DNS) are assigned to computers in the network.

In OMCUMS, the IP-address of OfficeMaster Gate is manually declared.

The uniqueness of the IP-addresses is ensured and an address conflict ruled out, because only one side requires a manual entry.

Without DHCP server

Is no DHCP server existing in the LAN or is the existing DHCP server not assigning an address to OfficeMaster Gate (because he for example is out of valid addresses), then OfficeMaster Gate will after a while automatically assign itself a private address (a so called Zeroconf-Address, also called APIPA-method). This address allows the activation of the build-in network interface, to ensure at least the availability via UDP broadcast. For the normal use however, in this case a static address will have to be assigned.

The program OfficeMaster Gate Configuration (OfficeMasterGateConfig.exe) is used to find OfficeMaster Gate in the network. By clicking the correct button, sub network wide search for OfficeMaster Gate is started via UDP broadcast. Sub network in this case is the physical network, in which the computer with the IP configuration program is integrated. This sub network is usually restricted by network routers, for example firewalls, that do not redirect the UDP broadcast.

In order to assign an address to OfficeMaster Gate, Office Master Software either uses an distinct IP address or the resolved name.

If OfficeMaster Gate, as described above, is used as DHCP client, than it should be ensured, that OfficeMaster Gate is available under the same IP address after reboots, so that the Server-Software can continue working properly.

Possible ways of ensuring this:

At the DHCP server, an IP address is reserved for the MAC address of OfficeMaster Gate. This way, OfficeMaster Gate receives the same IP address after every reboot. In the OfficeMaster Server Software, instead of the IP address, the resolved name is configured. Now when the DHCP server automatically refreshes the DNS server, OfficeMaster Gate will still be reachable by the Server Software, even after having been assigned a

different address.

1.3. Installation of the Survivable Branch Appliance

1.3.1. Rear view of server machine

OfficeMaster SBA is shipped as an Appliance with preinstalled components:

- Industrial grade server machine (e.g. HP ProLiant)
- Main Gateway Board with 4BRI / 2PRI interfaces (can be licensed on demand)
- Separate 4FXS analog interface card (optional)

Separate Y-cables are available if all 4 BRI ports are to be used – the first 2 BRI ports can be utilized using standard ISDN-cables.

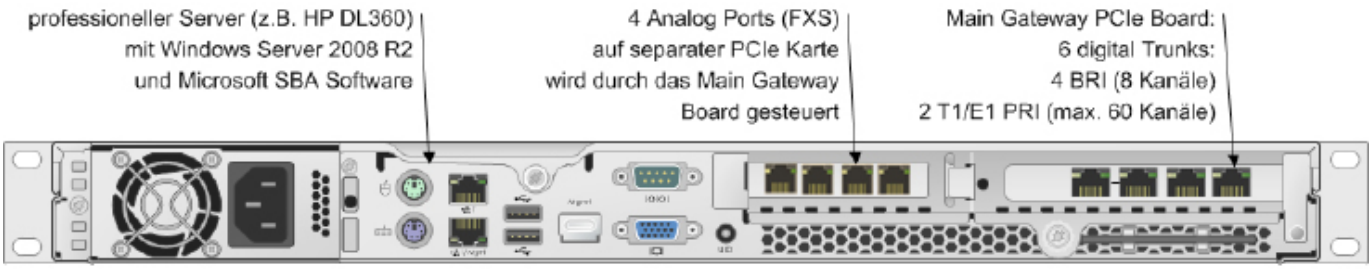

Image 1.1: Rear view SBA

1.3.2. Anatomy of the Media Gateway Board (MGB)

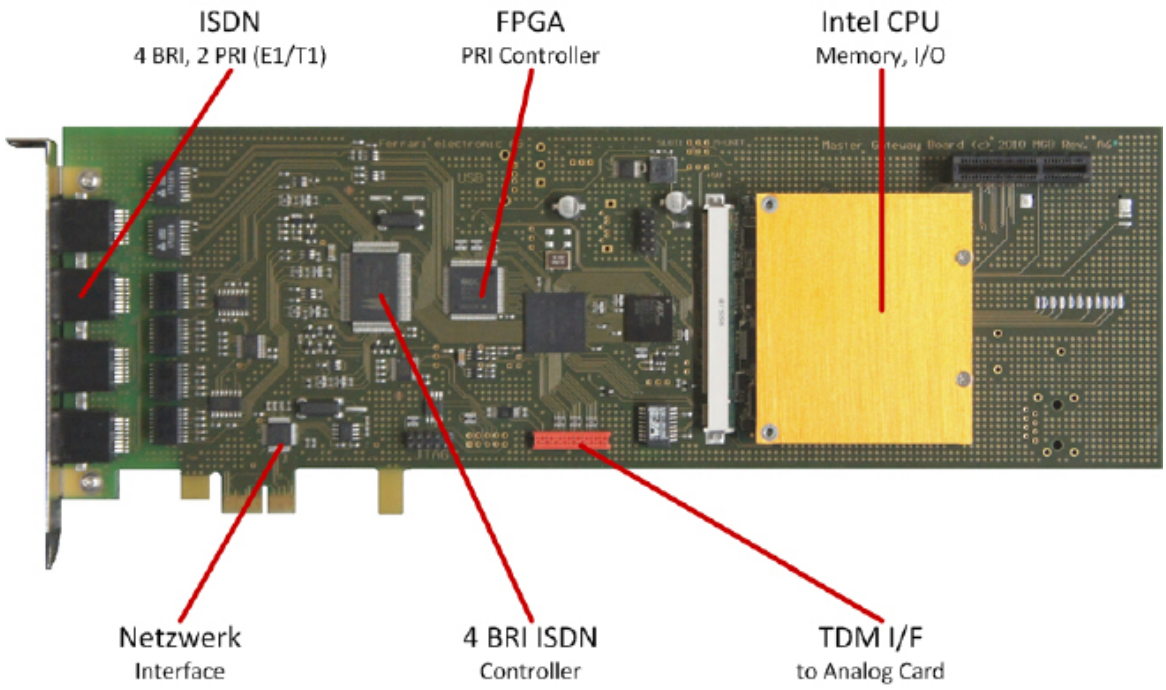

Image 1.2: Detailed view of Media Gateway Board

The Primary Rate Interface (E1/T1) is implemented in a FPGA (Field Programmable Gate Array), which contains additional support algorithms. It can even be upgraded in the field to implement more features as needed!

1.3.3. Analog Card – 4 Port (FXS)

Four analog ports are contained on a separate low-profile PCI-Express Card connected to the main gateway board using a flat ribbon cable.

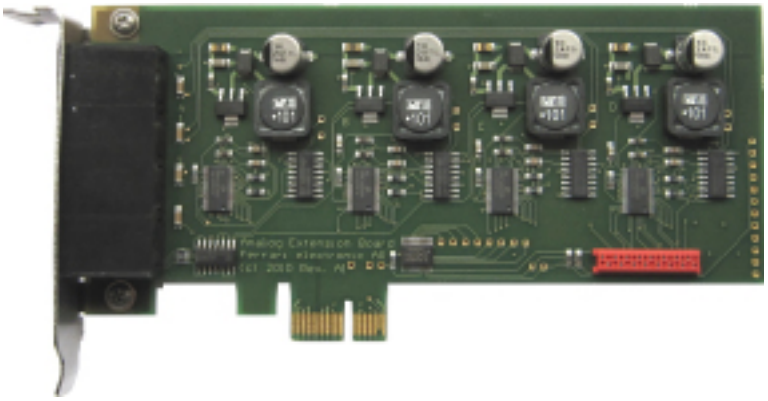

Image 1.3: Analog Card

The cable transports audio signals through a TDM bus as well as separate control information. High quality faxing is possible since no VoIP technology is involved between PSTN and FXS ports.

1.3.4. ISDN and Analog Interfaces

Positions of analog and digital interface connectors are shown in this picture (rear view):

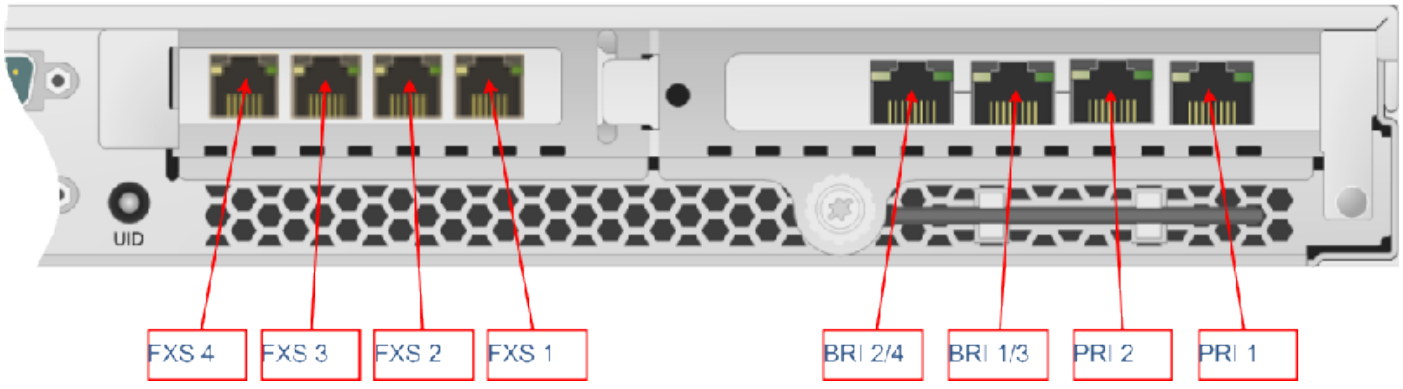

Image 1.4: Interfaces of the OfficeMaster SBA

For BRI ports a separate Y-cable must be used if more than two BRI lines are needed.

Note! Never use PRI 2 without PRI 1 – if only one PRI interface is connected always use PRI 1, otherwise clock synchronization will not work!

Table 1.2: Pin assignment

1	Rx+		Tx+
2	Rx-		Tx-
3		Tx+	
4	Tx+	Rx+	
5	Tx-	Rx-	
6		Tx-	
7			Rx+
8			Rx-

Note! If BRI interfaces are used in the US, a separate FCC approved NT1 Network Termination Unit must be installed to connect to OfficeMaster SBA S/T BRI ports. For LAN-connection, please plug in the network cable into the upper interface (LAN1):

Image 1.5: LAN Port to be used

1.4. Recovery

1.4.1. Survivable Branch Appliance

Use of the Recovery USB Stick

The SBA system software can be reset to factory settings at any time by using the USB recovery stick.

Please follow these steps:

1. Connect the SBA device to Keyboard, Monitor and Mouse, either physically, using KVM or through tools like HP ILO
2. Plug the USB stick into the front USB port
3. Power up SBA, it will automatically boot from the USB
4. At the end (message: press any key to shutdown computer) press a key
5. Remove USB stick
6. Power up SBA
7. Set the local Administrator password to OfficeMaster!
8. Check network interface configuration (see below)

9. Open a cmd console and enter the following commands: %systemroot%\system32\inetsrv\appcmd.exe set APPPOOL omsba_admin_pool -processModel.userName:ofmadmin %systemroot%\system32\inetsrv\appcmd.exe set APPPOOL omsba_admin_pool -processModel.password:Sefte25AuTib

10. Now the deployment Web UI is ready for use

Note! When a SBA is shipped, the serial number of the embedded gateway board is already preconfigured. After using the recovery image, the gateway serial number will be queried later by the Web UI during deployment. The serial number of the gateway board can be found on a card, which can be pulled out at the front side:

Image 1.6: SBA serial number

In this example the number to be entered is 259 (last 5 digits without leading zeros). (On some models, the number may be handwritten and may contain the serial number only, without the prefix, e.g. 234).

Check of the network interface configuration

During deployment of the Windows image via USB stick, the desired network configuration is automatically established:

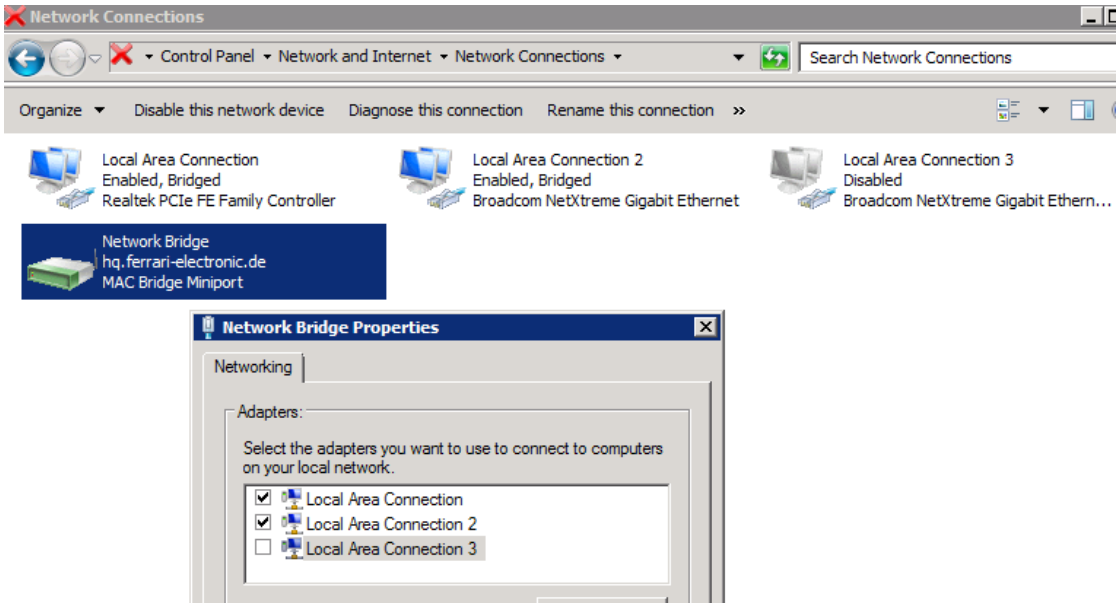

Image 1.7: Network bridge on the SBA

This is the standard configuration, where the gateway board (can be identified as Realtek Controller) is bridged with the LAN port (Local Area Connection 2), which is used for connecting to a switch. The unused second LAN port (Local Area Connection 3) is disabled. In some situations (e.g. due to different BIOS revisions), the physical LAN adapters have different internal id's, meaning that the restored configuration must be corrected manually.

Image 1.8: Example of a network configuration that needs to be corrected

The necessary changes in this case are:

- Right click on Network Bridge – Properties
- Make Local Area Connection 4 (LAN Port) and Local Area Connection 5 (Gateway board) the only members of the bridge
- Disable Local Area Connection 6

Now all network configuration settings should be made on the network bridge only. The SBA is ready for deployment after a final reboot.

1.5. Stainless steel box - Restore to factory settings

At the front as well as at the back of the case of the version for BRI's, there is one micro button each:

Table 1.3: Button on the stainless steel box

Micro button front	Hardware Reset	reboot system
Micro button rear	Software Reset	reset configuration parameters Function is deactivated one minute after booting is completed (signaled by blinking diodes)

Reinstalling the software

Should OfficeMaster Gate (in the stainless steel version with 4 BRI) stop working properly, a recovery can be done with newer versions of the product (February 2011 onwards, distinguishable by the USB port on the side). To do this, the Gateway needs to be disconnected from the power supply and the recovery stick from the bottom of the case has to be plugged into the USB port. Afterwards, reconnect the Gateway to the power supply. Turn off the Gateway after roughly 30mins and remove the stick. When used afterwards, make sure a backup of the configuration is loaded and, if needed, an update of the firmware is made.

1.6. Update and Upgrade

Ferrari electronic constantly releases updates for the OfficeMaster Gate firmware. Check the release notes if the latest version provides any practical changes for your particular IT infrastructure. In order to update the firmware, simply select Firmware update from the OfficeMaster Gate configuration program dialogue.

Leave the settings for automatic update on its default and initiate an update request via internet.

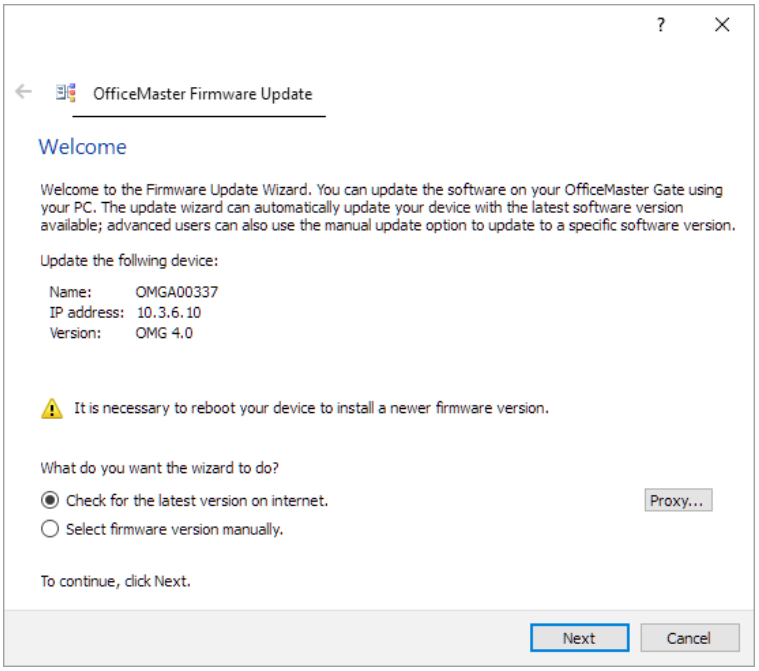

Image 1.9: Firmware update via internet

OfficeMaster Gate initially tries to access the update server; if it fails the configuration programme attempts the same. Please only select firmware version manually if the latter attempt fails again.

Various firmware versions are available to you, such as

- the official release
- the test release preview for the upcoming major release
- the developer release (on request only)
- the release as it was during certification by Microsoft

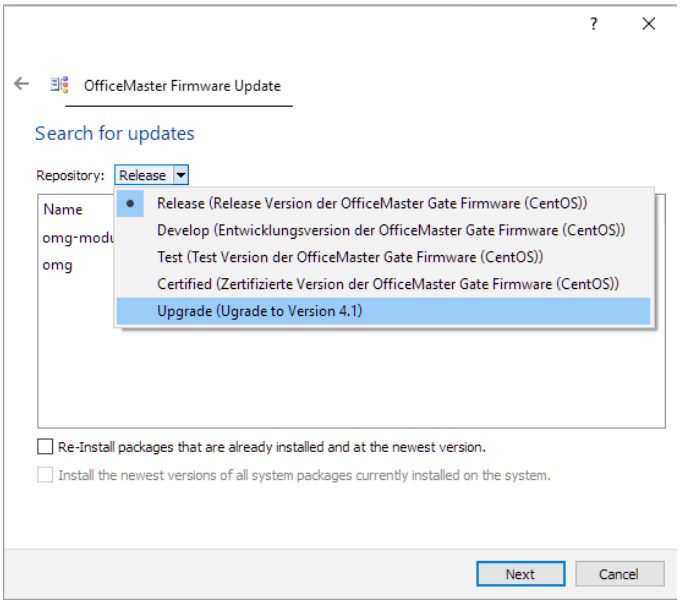

Image 1.10: Selecting the desired firmware version

Upgrade

The 4.1. release offered the opportunity to voluntarily upgrade the version 4.0.xyz to 4.1.xyz.

To do that, choose ***upgrade***. The configuration programme will subsequently install the release version of firmware 4.1. If, however, you want to change to a test version, restart the OfficeMaster Gate and select Test.

Downgrade

Downgrading to another version can only be carried out by downloading the respective firmware as .tar file (available on our website) and installing it via the configuration interface.

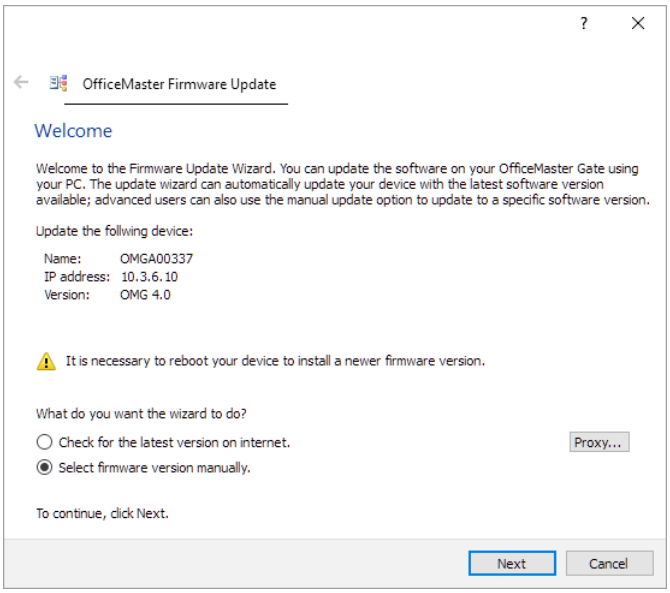

Image 1.11: Selecting firmware manually

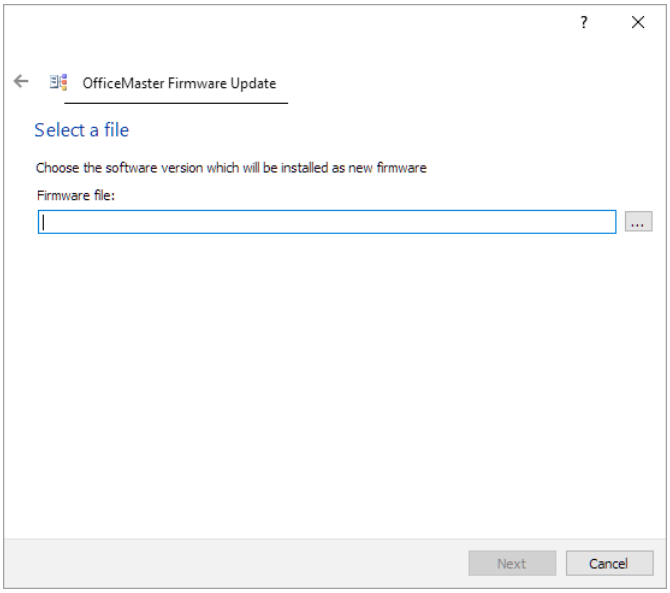

Image 1.12: Selecting the firmware file

2. WORTH KNOWING

Offline configuration

Firmware update

Licensene management

User manual for administrators | Ferrari electronic AG

Copyright © 2017 Ferrari electronic AG

2. Worth knowing

2.1. Offline Configuration

The settings can be configured and then tested without the hardware and ISDN interface being present. This enables, among other things, the following scenarios:

- The creation and testing of a customer configuration which is then transferred by email. The customer loads the *.cfg* file they receive into the gateway.
- Displaying and, if required, correcting a customer configuration
- For training purposes: provides a way for staff to practice using the options for configuring OfficeMaster Card/Gate.

Select File > Offline Mode to toggle the configuration program to this operating mode. Then click *Open...* or select File > Open... to open an existing configuration (*.ofg* file). Alternatively, a new configuration can be created by selecting File > New... and then selecting the hardware variant.

2.2. Logging/Syslog

Programs running in OfficeMaster Gate can send information about the ongoing processes to the Syslog-Server if needed. This is especially helpful when trying to determine the cause of errors. In order to activate this function, Edit > Logging... has to be activated.

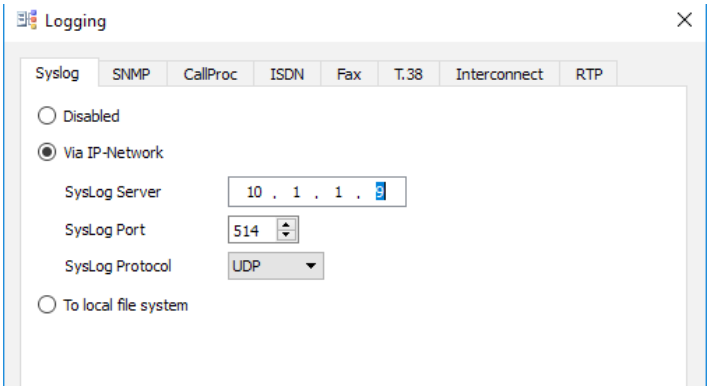

Image 2.1: Syslog Server

In the tab *Syslog*, the IP address of the Syslog Server and the used port (Default: 514) have to be inserted. In the other tabs, detailed settings as to how detailed the logging is supposed to be can be edited. In order to prevent as many errors as possible, the Ferrari electronic Support and other helping instances will set specific settings. Following an error, the logs of the Syslog Server can be forwarded for example as ZIP archive.

If no Syslog Server is available within the network, the program ***syslog.exe*** can be found in the program folder of the configuration software (Default: C:\Programs\FFUMS\omgatecfg). In the prompt ***cmd.exe*** the windows service can be installed via the option -install and configured via -config.

2.3. Saving the configuration

The current configuration can be saved to a PC via File > Backup. Vice versa can the saved configuration be loaded into OfficeMaster Gate via File > Restore.

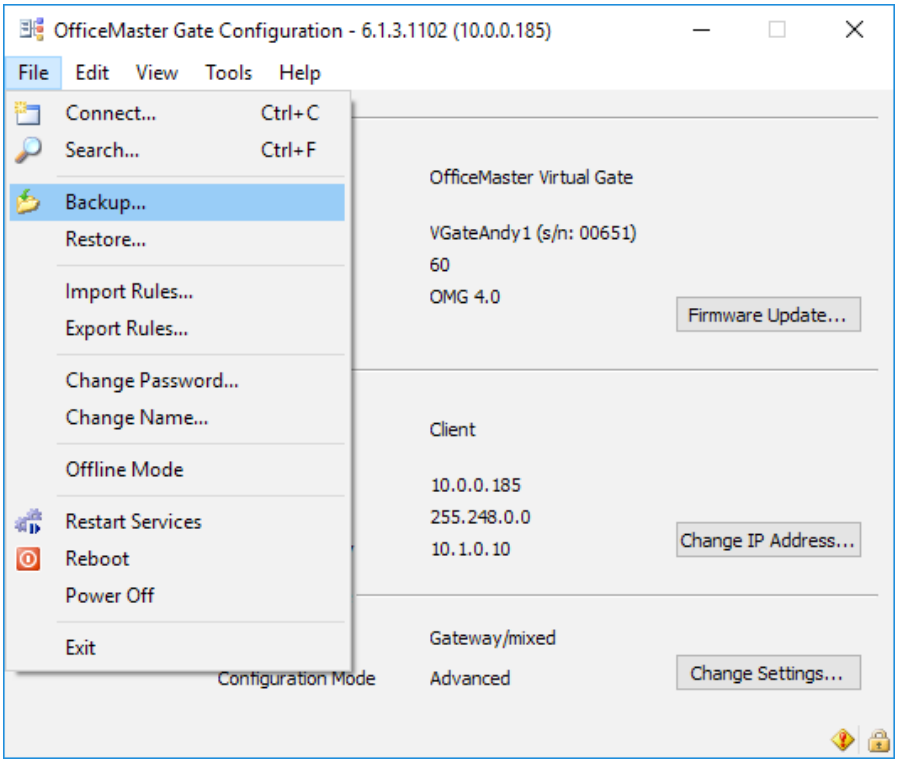

Image 2.2: Saving the OfficeMaster Gate configuration

The following information is not saved:

- Network configuration
- Certificates
- License files

Backups are therefore portable and can be implemented on further gateways.

2.4. Firmware update OfficeMaster Gate

New versions of the firmware running in OfficeMaster Gate are provided frequently in order to implement additional functions as well as bug fixes. Information about the currently available version can be found in the download area of www.officemaster.de as well as in the release notes in the forum. Information about the version used in OfficeMaster Gate can be found in the OfficeMaster Gate configuration (OfficeMasterGateConfig.exe).

Note! The following specifications are based on Office Master Gate. For older OfficeMaster Card/Gate products and the for them needed firmware version 1.xx please refer to the documentation received with the hardware.

After the connection to OfficeMaster Gate has been established, *Firmware-Update* has to be pressed. The update process will start after pressing Start and can take a few minutes. The controller will in the end restart automatically. There are multiple possible scenarios for an update of the firmware.

1. Integration of the firmware via the OfficeMaster Gate configuration through manual selection of the firmware package. The current firmware can be found in the download area of www.office-master.de.

2. Integration of the firmware through the OfficeMaster Gate configuration by automatically downloading the current firmware via the internet connection of OfficeMaster Gate.

3. Integration of the firmware through the OfficeMaster Gate configuration by automatically downloading the current firmware via the internet connection of the administrators computer and automatic transfer through the OfficeMaster Gate configuration to OfficeMaster Gate.

4. Integration of the firmware through SSH-Login on OfficeMaster Gate. Execute the command ***omgupdate*** via the internet connection of OfficeMaster Gate.

Prereleases of the firmware which have not been cleared for distribution can be found on our website under the Test section. These can also be installed.

2.5. Changing Password

The password for logging in to the controller (Standard: „omc“) can be changed via File > Change Password.

2.6. License management

OfficeMaster Gate are upgradeable in regards of ISDN ports or functionalities locally via extension licenses. The activation of additional functions takes place in two steps:

- The by the customer purchased extension license, which possesses its own serial number, has to be registered with Ferrari electronic first.

- Based on the registration the customer will receive a fresh extension license which is tailored specifically to the serial number of the customers OfficeMaster Gate. The extension license can only be used for this specific OfficeMaster Gate.

The configuration program supports the registration and activation of extension licenses. The configuration program has to be connected to the OfficeMaster Gate on which the extension license is to be used. The license management can be accessed via Edit > Manage licenses... .

2.6.1. General settings

► License State

License State displays which ports and functions are activated for the with the configuration program connected OfficeMaster Gate.

► Supported Interfaces

Here, the maximum number of interfaces is displayed. This is unrelated to the number of integrated licenses.

The actually licensed interfaces are listed below and depend on the hardware as well as the integrated licenses.

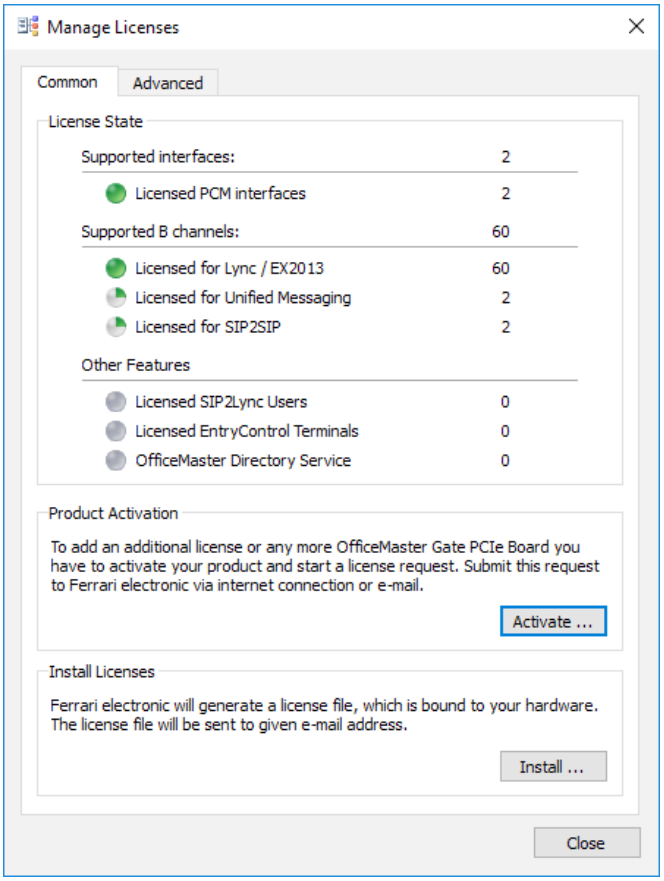

Image 2.3: License management - Overview

▶ Request new License

Create... opens a dialog for the integration and registration of or more extension licenses. ***Add*** includes one or more extension license files into the list. A file selected in the list can be deleted, edited or replaced.

The registration information can be submitted either via email or via the internet. ***Next*** opens additional dialogs for entering customer and personal data, which are needed for the registration.

Note! The information regarding company and contact person (Last name and email address) are essentially required for the distribution of the activation license.

The first step of installing the extension license is completed once the registration information has been send. Based on the information gives in the registration Ferrari electronic will distribute a license file for each registered extension license. This license file has to be implemented into OfficeMaster Gate via the configuration program. The name of the license file is combined out of the original name of the extension license and the serial number of the to be extended OfficeMaster Gate.

Example 2.1.

Serial number of the extension license:

99-EOMGB00010.fle

Serial number of OfficeMaster Gate:

OMG200123

Name of the distributed extension license:

99-EOMGb00010_OMG200123.fle

»**End of example**

► Install Additional License

Install… in the dialog window opens a file selection dialog, which enables the selection of the modified extension license. The selected license is then imported. Here it will also be checked if the configuration program is connected to the OfficeMaster Gate for which the license was created. A message will inform about the successful import. Otherwise an error report will be shown.

Following a successful import the license management can be closed by clicking on *Close*.

Note! Only after a reboot of OfficeMaster Gate will the license information become active.

2.6.2. Advanced settings

The tab *Advanced* displays already imported extension licenses. An already imported extension license can be deleted by selecting it and clicking *Remove selected*. *Export…* enables the export of the license files onto another medium.

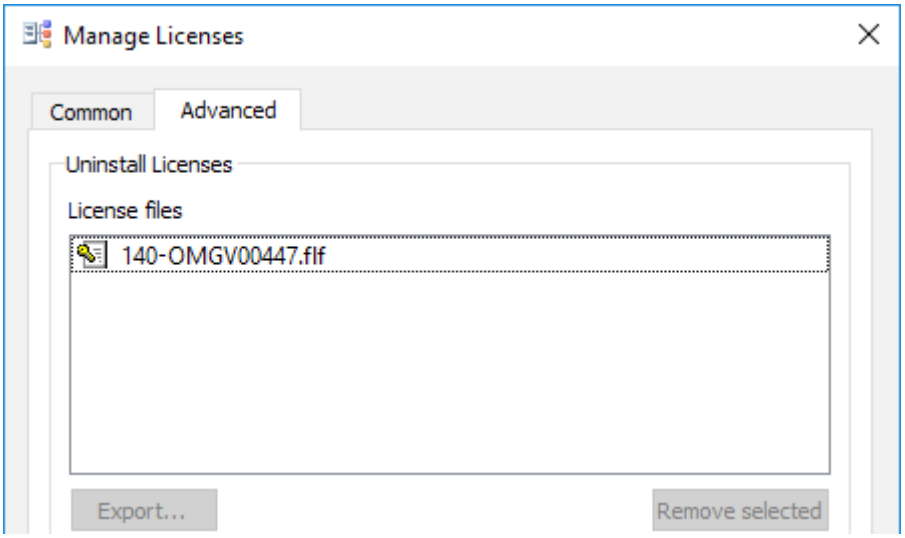

Image 2.4: managing existing licenses

3. CONFIGURATION

Basics

Media Gateway configuration

Drop & Insert

User manual for administrators | Ferrari electronic AG

Copyright © 2017 Ferrari electronic AG

3. Configuration

The products of the OfficeMaster Gate family use a coherent firmware as a base, which operates the depending on hardware available ports

Because of the coherent base and the therefore identical configuration-ports, every OfficeMaster Gate of the 3rd generation can be operated with the same user interface.

Even though the essential configurations of OfficeMaster Gate are identical, when installing the SBA and the Hybrid Gate, additional steps of configuration are necessary.

3.1. OfficeMaster Gate Basic Settings

If OfficeMaster Gate is used solely in combination with the Unified Messaging Software OfficeMaster, then the configuration is made via the integrated administration program (see manual for OfficeMaster Administration). The gateway function of OfficeMaster Gate can be enabled if needed.

For the activation and configuration of the gateway function, an administration program (*OmGateConfig.exe*, installed via *SetupOfficeMasterGateConfig.exe*) is provided, which can be installed at any work space. A mixed use as gateway and Unified Messaging Controller for OfficeMaster can be set up with this program. The main dialog will pop up after starting the configuration program:

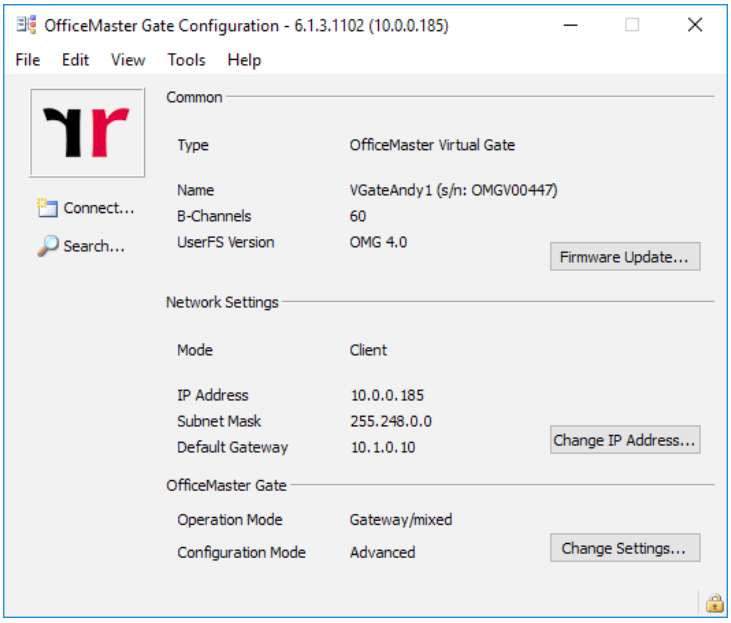

Image 3.1: Connected OfficeMaster Gate

Some of the elements will only become active once a connection to the controller is provided (see next section).

Note! The language can be toggled between German and English in the help menu.

3.1.1. Connecting to OfficeMaster Gate

After the start of OfficeMaster Gate configuration, the connection to OfficeMaster Gate has to be established. Via File > Search or by pressing the search symbol, name, IP address, version and number of channels of the found controllers are listed:

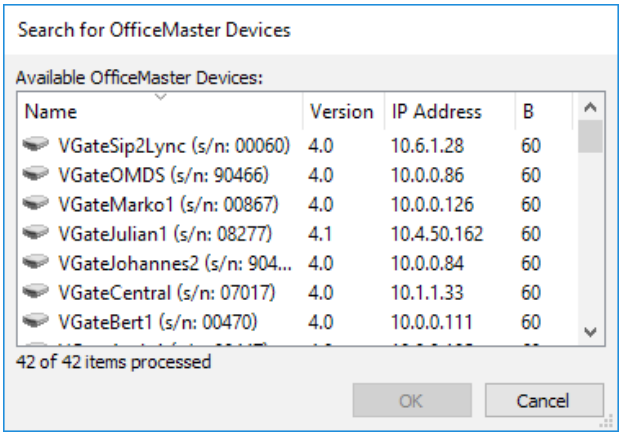

Image 3.2: Available OfficeMaster Gate in the Network

In this list, the preferred entry is selected and confirmed by pressing *OK*. This login dialog will then appear:

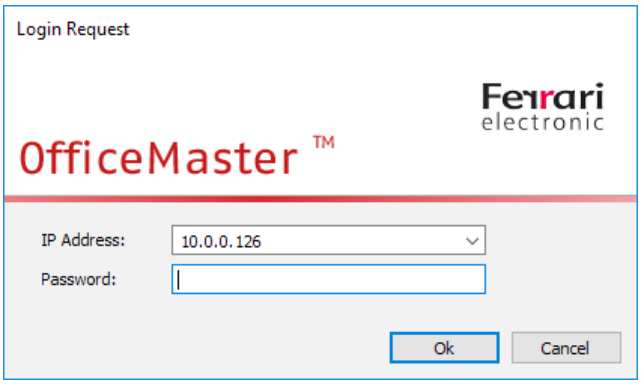

Image 3.3: OfficeMaster Gate login

This dialog can also be accessed directly via File > Connect, in order to enter the IP address of OfficeMaster Gate manually. For authentication purposes, a password is required.

Note! The default password is ***omc***.

3.1.2. Network configuration

In order to change the network settings (for example IP address) the button *change IP address...* has to be pressed. Alternatively the same can be achieved via Edit > change IP address. Depending on the structure of the used network, IPv4 and/or IPv6 addresses can be declared.

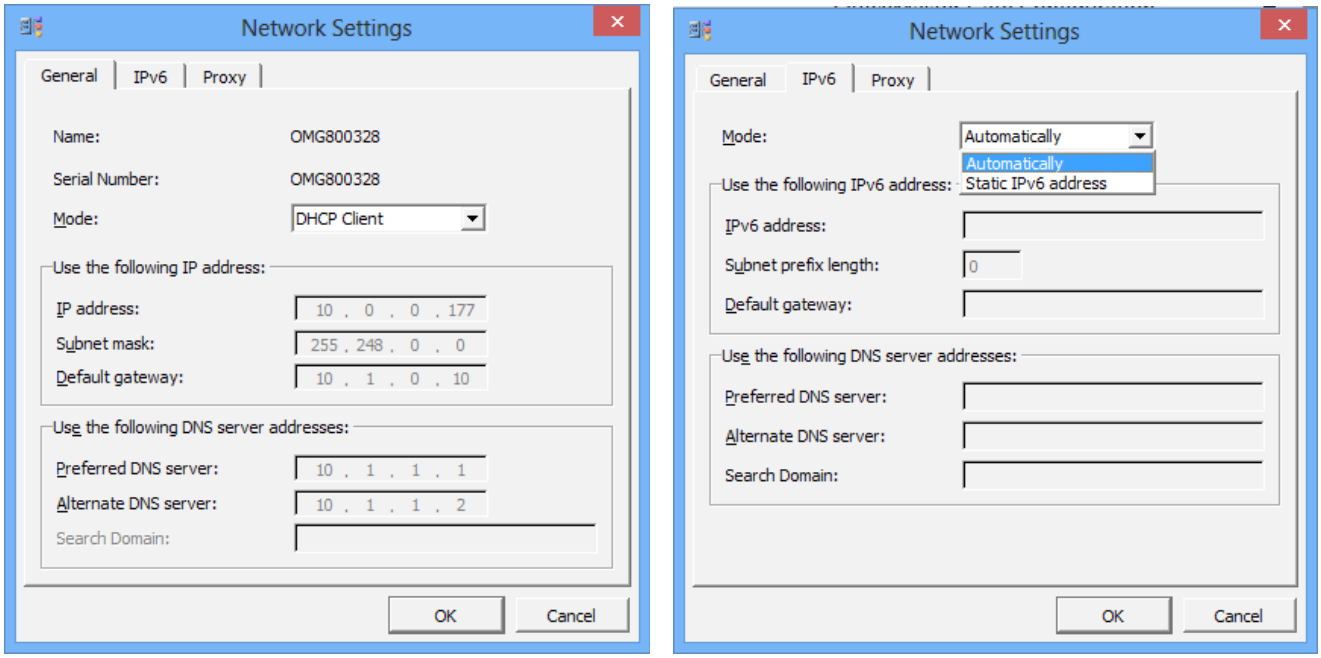

Image 3.4: Network settings

Note! The configuration program communicates through UDP-Broadcasts via the port 3216. With OfficeMaster this also works through interposed switches, while routers usually will not forward the Broadcast-Messages.

The mode activated on shipment of OfficeMaster Gate is DHCP-Client. Possible modes of operation are ***DHCP-Server (IPv4 only)***, ***DHCP-Client*** and ***static***.

► DHCP-Server (IPv4)

The DHCP-Server mode is only useful for OfficeMaster Gate, if OfficeMaster Gate is connected to a host computers network card via cross cable and when this network card is run in DHCP-Client mode.

► DHCP-Client (IPv4)

This is the standard setting of OfficeMaster Gate. In this mode of operation it is assumed that there is a DHCP-Server existent in the network, which will assign the controller with an IP address and every other required value. OfficeMaster Gate registers itself under the name that is shown in the first slot of the IP configuration program. If the DHCP-Server automatically initiates a DNS refresh then OfficeMaster Gate can be contacted directly under that name in the network.

► Static (IPv4)

Is the network run without a DHCP-Server then OfficeMaster Gate needs to get a static IP address, a subnetwork mask, a gateway address (optional) as well as the address(es) of the DNS Server(s) assigned to it.

A Domain Server Name (DNS) has to be assigned, when the target systems are addressed via FQDN (Fully Qualified Domain Name). Because these can, on occasion, malfunction, a alternative DNS should be configured as DNS2.

► Automatically

With this setting, an automatically assigned IPv6 address will be used.

► Static IPv6 Address

Similar to IPv4, with IPv6 as well the declaring of a static IP address is possible. Are the target systems contacted via FQDN (Fully Qualified Domain Name), at least one Domain Name Server (DNS) has to be declared. Since one DNS server can fail at any time, an additional one should be configured as DNS2.

► Proxy

Should a connection in the network be restricted to a Proxy only, it can be configured in the tab *Proxy*.

3.1.3. „Common“

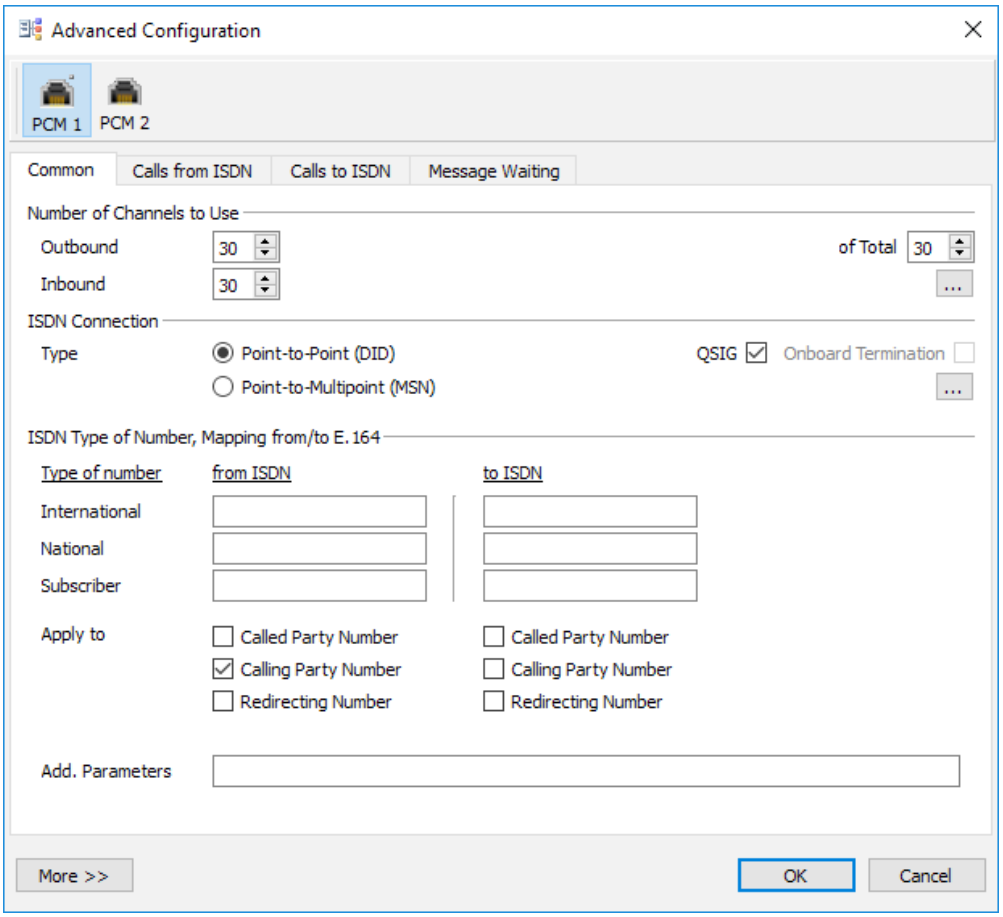

Image 3.5: ISDN Settings

▶ Number of Channels to use

In the following it is decided, whether the existing B-Channels are to be used completely for in-and outgoing connections or if, for example outgoing calls are only allowed to use a certain percentage, so that there are free channels for incoming calls under any given circumstances.

▶ Outbound

Defines the maximum amount of channels that will be used for outgoing calls.

▶ Inbound

Defines the minimum amount of channels that will be used for outgoing calls.

▶ of Total

Total of B-channels used.

▶ [...]

By pressing *[...]* , a dialog will open up, enabling the user to define the maximum amount of B-Channels, for example with „halved“ PRI ports. This „incomplete“ pin assignment is relatively common outside of Germany.

▶ ISDN Connection

The different types of connection are Point-to-Multi point and Point-to-Point.

▶ Point-to-Point (DID)

Point-to-Point only supports one ISDN device, usually a telephone system or a media gateway. A Point-to-Point connection assigns a complete dial through numbers area.

▶ Point-to-Multi point (MSN)

Point-to-Multi point connection only supports a limited number of recipient call numbers (usually 3 to 10), so called MSN (Multiple Subscriber Number). Here, multiple ISDN devices (Phone 1, Phone 2, Fax) can be connected.

▶ QSIG

Additional to Euro-ISDN or DSS1, there is also QSIG. This is an ISDN protocol that is sometimes used by a selective number of telephone systems. Via QSIG, additional information like the callers name can be transmitted.

▶ Onboard Termination

OfficeMaster Gate for BRI allows the addition of ISDN terminating resistors, which should usually be existent in the ISDN socket. By default, these internal terminating resistors are deactivated.

A LED can be found on the left side below the ISDN socket of OfficeMaster Gate (stainless steel edition). If this one is lit, then the firmware enabled the terminating resistors according the configuration settings.

Note! Usage without terminating resistors can lead to ISDN errors. In older versions of the hardware, this LED will be triggered if the terminating resistors are off! The settings in the configuration program are in effect in any way.

► NT Mode (Network Termination)

This option is usually used in order to place the gateway between the telephone network and the PBX. Towards the telephone network the gateway acts like a PBX (as TE, meaning Terminal Equipment), while towards the PBX it acts similar to the trunk.

Note! This only works in Point-to-Point mode. Common terminals will not be usable on this line as such devices usually run in Point-to-Multi point mode. Additionally, a cross cable needs to be used for the connection with the PBX.

► [...]– Advanced Connection Parameter

► Dial Timeout

When simulating an external line, numbers of any random length will be communicated by the telephone system. In order to decide which calls are supposed to be redirected outward, a timeout is set, after which no more digits are to be expected. This timeout usually happens after 3-5 seconds.

► Caller Name Display Mode

Is QSIG activated in the ISDN protocol, caller names can be transmitted for incoming and outgoing calls. Since this is based on different protocol versions depending on the system, testing is the only way to find the right setting.

► No L2 auto-activation (Point-to-Point Options)

With a Point-to-Point connection, the gateway will try to keep active the layers 1 and 2 in the D-Channel at all times. This behavior can be deactivated here.

► ISDN Type of Number, Mapping from/to E.164

Type of Number is usually defined in ISDN in order to define information about the type of call. Internally (for example Lync or OfficeMaster Suite) calls are usually in E.164 format, meaning that they need to be adjusted properly.

► International

With calls from ISDN, the configured ***call number*** (for example „+“) is fronted when the ***Type of Number*** (TON) is set to ***international***.

For outbound calls, meaning to ISDN, the TON is recognized via the configured call number and the call number removed.

► National

National numbers are treated equivalently to international numbers.

► Subscriber

The local connection is entered under *Subscriber*.

► Apply to

Insert here, for which numbers the adaptations are to be made.

Example 3.1.

Creating an E.164 number from TON for inbound calls

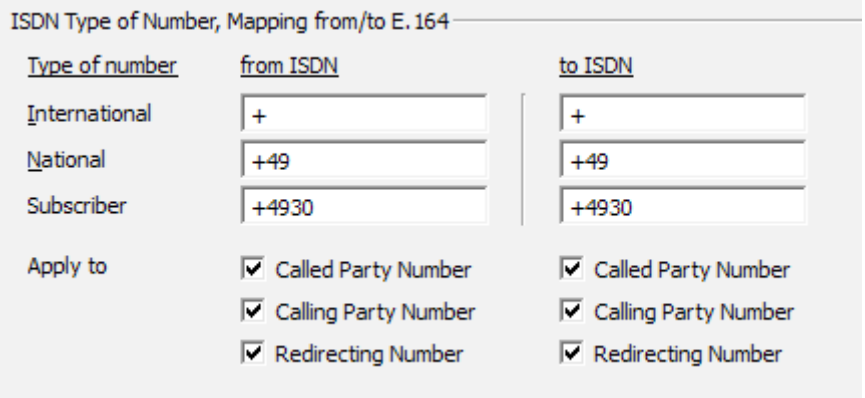

Image 3.6: Example for an automatic creation of an E.164 number

Table 3.1: Submitted information on inbound call

Called Party Number	National 89123	+493055948
Calling Party Number	Subscriber 55948	+4989123

With settings as seen in Image 3.6, the inbound signal from Table 3.1 is converted into an E.164 number. Afterwards, OfficeMaster Gate's set of rules are applied for further customization of the phone numbers and for the delivery towards the appropriate destination as described in the following paragraph (3.1.4).

»**End of example**

Example 3.2. Generating the ISDN information for outbound calls

For outbound calls the process is inverted. The settings of the sector *ISDN* apply.

Table 3.2: Conversion of E.164 to ISDN

Called Party Number	National 89123	+493055948
Calling Party Number	Subscriber 55948	+4989123

»**End of example**

Note! More complex setting for TON are available via the creation of single rules for inbound, respectively outbound rules.

▶ More – Settings for multiple channels

OfficeMaster Gate is available in versions with multiple ISDN channels. The configuration program supports this by letting the user configure channels individually. Alternatively, all channels can be defined to copy the settings of the first channel. This can be activated via the button *More>>* in the configuration dialog. Here the user defines which channels are to be used. Pressing *More<<* again hides the area. Has the individual configuration of the channels been selected, the upper area of the dialog will display the channels that are available for configuration.

3.1.4. Calls from ISDN

For the selection of the target gateway, a separate tab is available in the advanced mode. In this tab, targets are chosen depending on the calling number and reshaping can be done.

In the tab *Calls from ISDN* a list of the configured rules is shown:

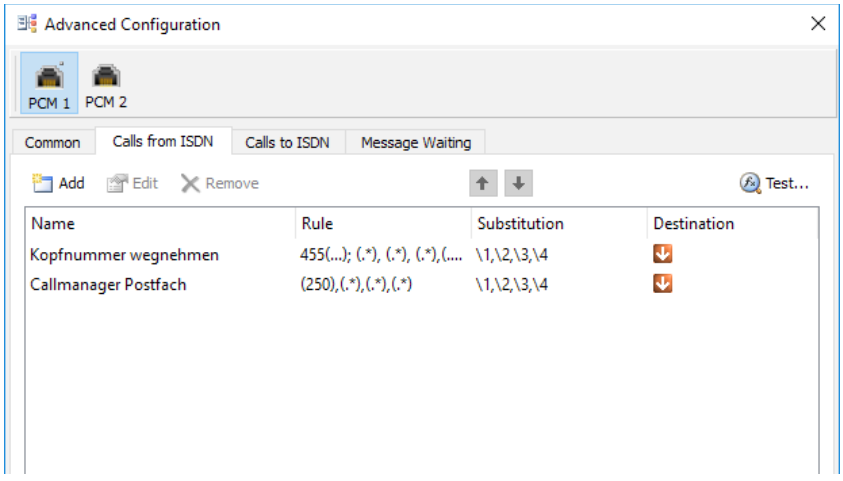

Image 3.7: Rules for inbound calls

Ferrari electronic

In this dialog you can add, delete, process and change the sequence of these rules. To edit, delete or move a rule, click on it with the mouse button to select it and then select the action you require.

Additional options are offered by the context menu, which is opened by right clicking an entry:

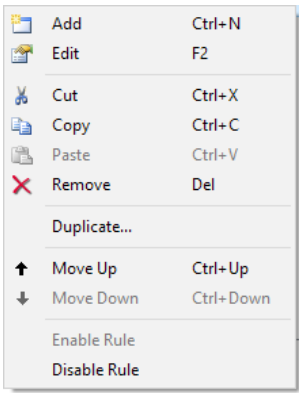

Image 3.8: Context menu for Gateway rules

Many of these functions can be used with multiple rules at the same time. For this, the rules need to be selected via multi-marking (Shift resp. Ctrl + left mouse button).

For when a new rule is created, the fields are set up to select any number and to remain unchanged after substitution (substitution by itself.)

Usually, at least the pattern for the *Calling Party Number* will have to be edited in order to suit the extension number length or specific MSNs. The rule should be given a descriptive name. For every rule, a type (e.g. ***Routing***, ***Replacement***, ***Blocking***) and for rerouting rules, a target will need to be configured.

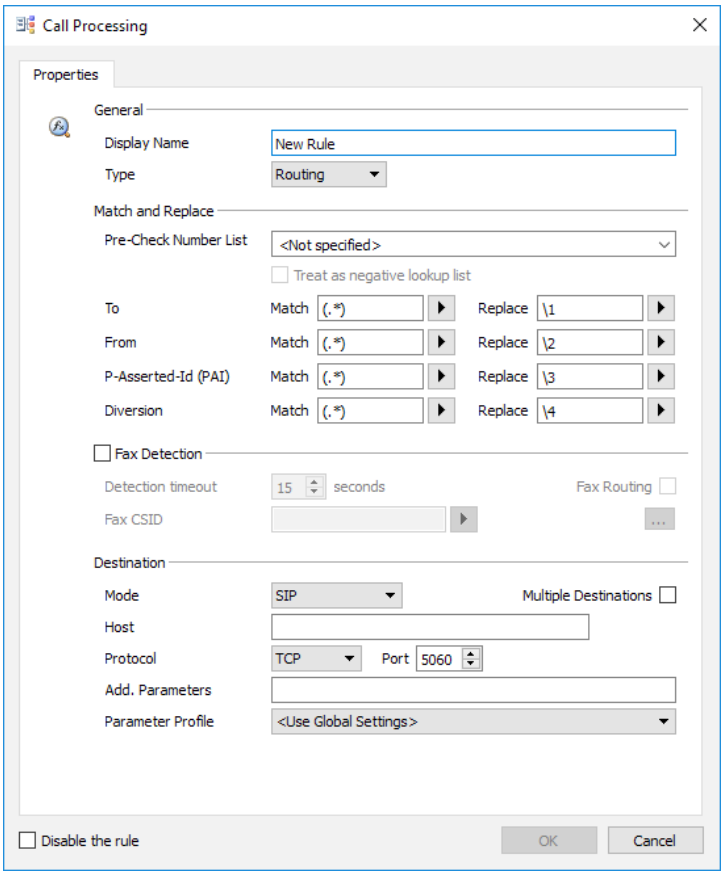

Image 3.9: Creating a new rule for inbound calls

Possible settings regarding rules for incoming calls

► General

► Display Name

Here, the rule should be given a descriptive name.

► Type

Defines the type of rule.

- Routing - Defines a target, to which the call is redirected should this rule become active. Other rules below this one are then disregarded.
- Replacement - Manipulates the phone number by, for example, adding or cutting digits to or from the number. After that, the next rules are processed.
- Blocking - The processing of the call is ended should this rule become active. Most useful for outgoing calls, in order to direct those to specific ISDN ports and block them from others.

▶ Match and Replace

▶ Pre-Check Number List

A separately licensed software can enable the gateway to provide number lists, which the rules can call upon. With this, complex dial plans which have no clear pattern to the numbers involved, can be realized. Additionally, the separate software Lync phone numbers can be regularly replicated from the AD into the gateway, so that it can be decided automatically whether incoming calls are meant for the telephone system of for the Lync server.

▶ Match/Replace

In the match fields, patterns for comparison are given in form of regular expressions. These are compared with the existing values and information is saved in brackets. Afterwards the replace field is processed, in which information is referenced and if needed completed by additional characters. Detailed information for this and for the fields *Called Party Number*, *Calling Party Number*, *Calling Party Number 2* and *Redirected Number* can be found under Basics of telephone numbers.

▶ Fax Detection

The following settings only come into effect once this check box is activated.

▶ Detection Timeout

Is this box checked then the incoming audio signal at the start of the connection is, for the duration of the set Detection Timeout, scanned for CNG tones. Depending on the settings in the VoIP parameters, either CNG events are redirected in the RTP protocol or a reINVITE for a T.38 connection is issued. T.38 is used in combination with Exchange 2007 for incoming fax messages. With Exchange 2010 UM, OfficeMaster Gate can directly receive fax messages, without having to use T.38 (see Receiving Fax with Microsoft Exchange 2010).

▶ Fax Routing

Via this option, an Exchange fax receive can be realized in Lync resp. OCS environments without a separate dial through number. Unfortunately, the recognition of a fax connection only works after picking up the call. In this case, the user would pick up the call, which would be ended a few seconds late again if it is a fax call. This call would then be redirected to Exchange. Due to this restriction, this function is rarely used.

Receiving fax in Exchange 2007 always requires a connection to the voice box of the user. After that, the gateway needs to recognize that a fax is to be received and then inform the Exchange server.

Should no receiving of fax messages be wanted this way (f. Ex. because separate dial through numbers exist for fax), the recognition of fax calls can be deactivated as well. For this, the check box *Fax Detection* has to be deactivated.

If Fax Detection is activated, then it is only trying to do so for a limited time, as otherwise longer connections to the voice mailbox could lead to sound signals falsely triggering the switch to fax mode.

Caution! When Lync or OCS 2007 (for telephony) and Exchange 2007 (for voice mail) are used together, the switch to fax will not work, as Lync and OCS contact the Voice mailbox themselves and don‘t support fax.

In order to enable fax none the less, without having to set separate fax dial through numbers, OfficeMaster is able to switch to an alternate target (Exchange or OfficeMaster), should a fax connection be recognized. For this, the check box *Fax Routing* has to be activated in the according rule (which usually routes to Lync resp. OCS).

In the following dialog, the target responsible for receiving fax messages is configured. The configuration is comparable to other rules for incoming calls.

► Fax CSID

Here, a separate fax ID can be declared, in which by referencing to the Called Party Number, the user dial through number could be displayed individually.

► Destination

Multiple destinations are possible destinations for incoming calls.

► Mode

The mode for a connection to Exchange UM or Lync/Office Communication Server should be SIP. Shall a call (fax, SMS, voice mail) be handled by the OfficeMaster Messaging Server, OfficeMaster has to be chosen. Further modes are *ISDN* (for when a call shall be directed via ISDN once again) as well as *REGISTERED* (the call is redirected to a SIP installation, as long as that installation is registered under the number accompanied by the call).

► Host

For SIP mode you must specify the target computer either by entering its IP address or a fully qualified host name.

► Protocol

The protocol used for the targets described here is either TCP or TLS. UDP is for example often used in combination with analog adapters.

► Port

Typical values for the target port: *Exchange/TCP 5060*, *Exchange/TLS 5061*, *Lync/TCP 5068* and *Lync/TLS 5067*. With Lync Servers, the actual value can be seen in the Topology Builder in the section Mediation Pool.

► Add. Parameters

This is where you edit additional settings. This box usually remains empty. You should only use it if told so by the Ferrari electronic hotline.

► Multiple Destinations

In SIP mode you can specify more than one target so that, for example, if a computer crashes, any inbound calls can be forwarded to another computer. If you click the *Multiple Destinations* check box, the dialog changes.

In OfficeMaster mode, additional priorities can be set. Destinations with equal priority trigger an automatic divide onto those destinations.

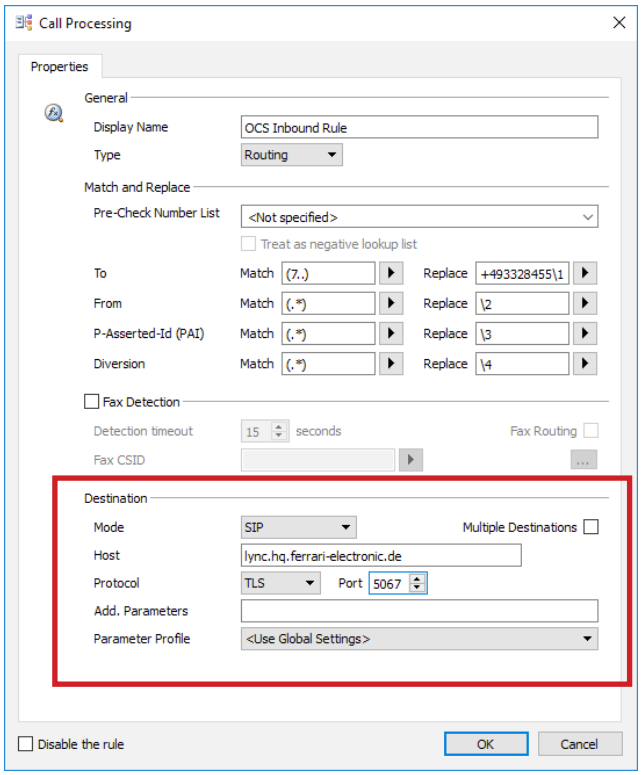

Image 3.10: Destination for calls in the rule section

3.1.5. Calls to ISDN

Aside from the manipulation of incoming calls, the manipulation of outgoing connections is also possible. With this, for example an automatic trunk seizure can be set up.

Example 3.3.

In the tab *Calls to ISDN*, a list of outbound rules is shown. Rules can be added, edited or deleted. Different to incoming calls, outbound calls are checked for a match with all active ports. Has a matching rule been found, the call is send on the port, that this rule was assigned to. If multiple matches occur, the ports are used interchangeably, as long as there is an open B-channel.

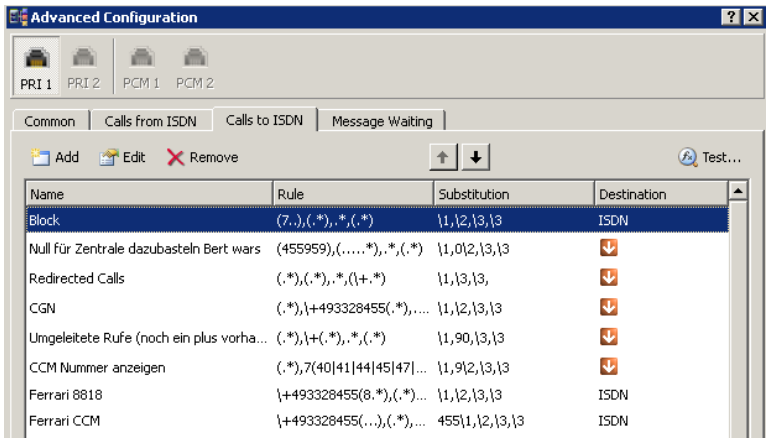

Image 3.11: Set of rules for outbound routing

»End of example

Example 3.4.

The picture below shows a rule, which recognizes German phone numbers in the E.164 format (plus-sign, country code, area code without initial 0, participant number) and converts them into dialable numbers. The character sequence +49 is replaced by two zeros, one for the trunk seizure and one for the area code. +49332845590 is converted into 00332845590.

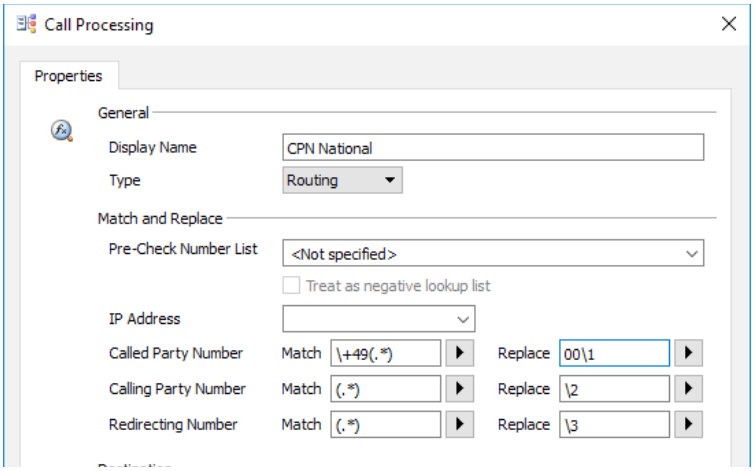

Image 3.12: Rule for an outbound call

»**End of example**

3.1.6. Testing routing rules

The functionality of the configured rules can be tested directly in the configuration program, even without an existing ISDN connection. For this, press the *Test* button on the right side above the rules.

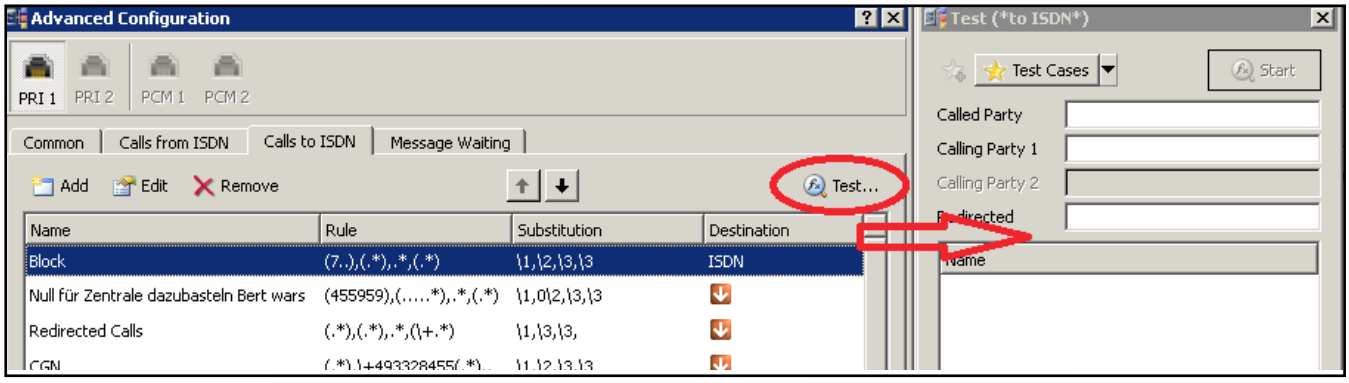

Image 3.13: Testing routing rules

This will open a test window, in which different values can be tested.

Note! Switching between incoming and outgoing rules is possible, the test dialog will automatically adjust itself. Additionally, rules can be adjusted or added while the test dialog is open. All values entered are kept.

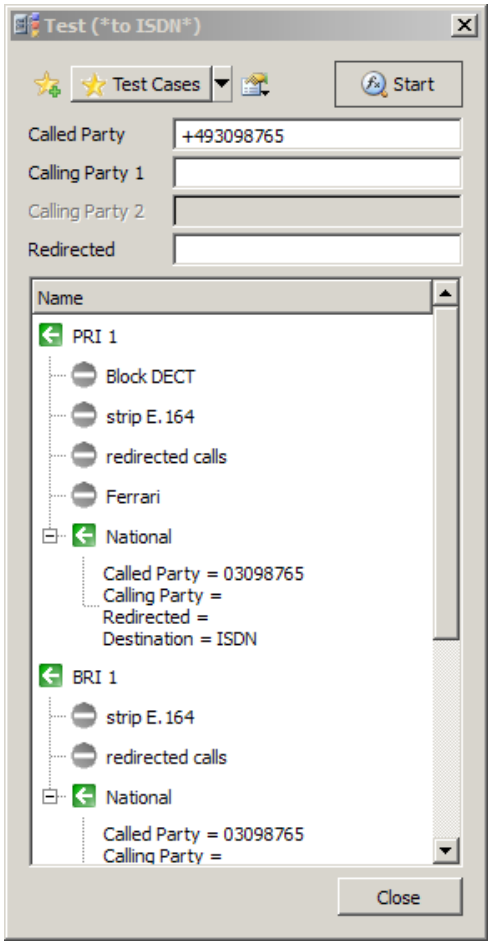

Image 3.14: Analyzing test results

► Called Party

For testing, a phone number is entered in *Called Party*, all other fields are optional. After starting, the rules are checked for matches. In the result it can be observed, for which rules a match was found and what their effect was.

Note! In the example above it can be seen, that the test for outbound rules was held over all ports and that multiple ways can be found.

3.2. Configuration and Activation of OfficeMaster SBA

This chapter describes the necessary steps to install OfficeMaster SBA. Some prerequisites have to be made in the central data center -the technician in the branch office only needs limited administrative rights to make the necessary steps.

Note! The SBA can be reset to factory settings at any time via the use of the USB recovery stick. Details on this can be found near the end of this document.

3.2.1. Preparations in the central computing center

Before OfficeMaster SBA can be used, a few preparations have to be made in the central data center. Please mind the applicable instructions by Microsoft regarding the Lync Server Software. The necessary steps include setting up a computer account for the SBA and adding a serverPrincipalName via the ADSI Edit for this account. Furthermore, a user account for the SBA administrator of the domain group RTCUniversalSBATechnicians has to be added.

Note! This membership has to be configured directly via the explained groups and not indirectly via additional groups!

Additionally, a site has to be declared in the Topology-Builder (if not already existent) and in that site, the Survivable Branch Appliance including Gateway has to be defined. The Gateway in the SBA receives its own IP address respectively the fitting DNS entry. Lastly, the topology has to be published. Here, the SBA computer accounts automatically receive the necessary rights.

3.2.2. Installation OfficeMaster SBA

Connect to the web-based administration of the appliance -addressing via the address noted on the provided label. Is there no DHCP server in the network, the appliance will automatically assume the IP address 192.168.101.101 and the network mask 255.255.255.0

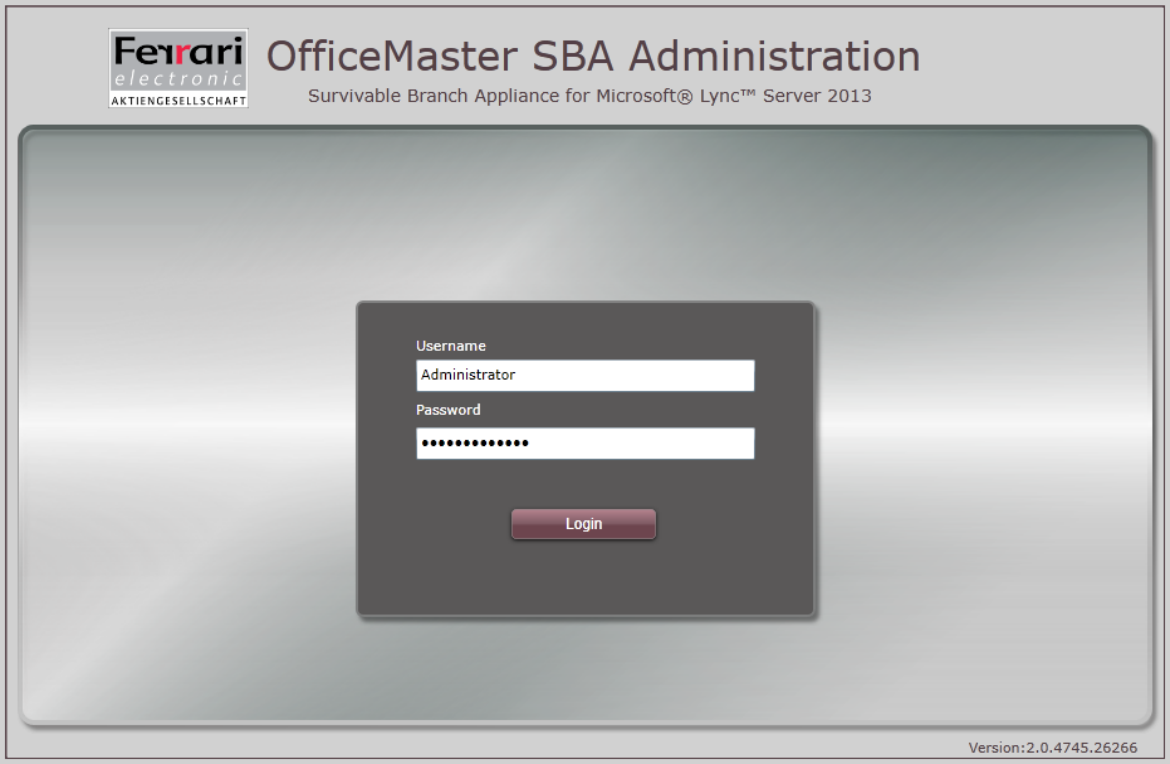

Image 3.15: First Login

Enter ***Administrator*** as Username and ***OfficeMaster!*** as Password (will be changed in a later step).

The first dialog after the log-in leads to the network configuration. By selecting *Done*, the DHCP settings will be saved and applied. Alternatively, a static IP address can be entered.

Image 3.16: Initial Network configuration

Select *Apply Changes*, restart the browser and connect via the new IP address.

The following dialog allows the admin to change the password. By selecting *Change Password*, the process is finished.

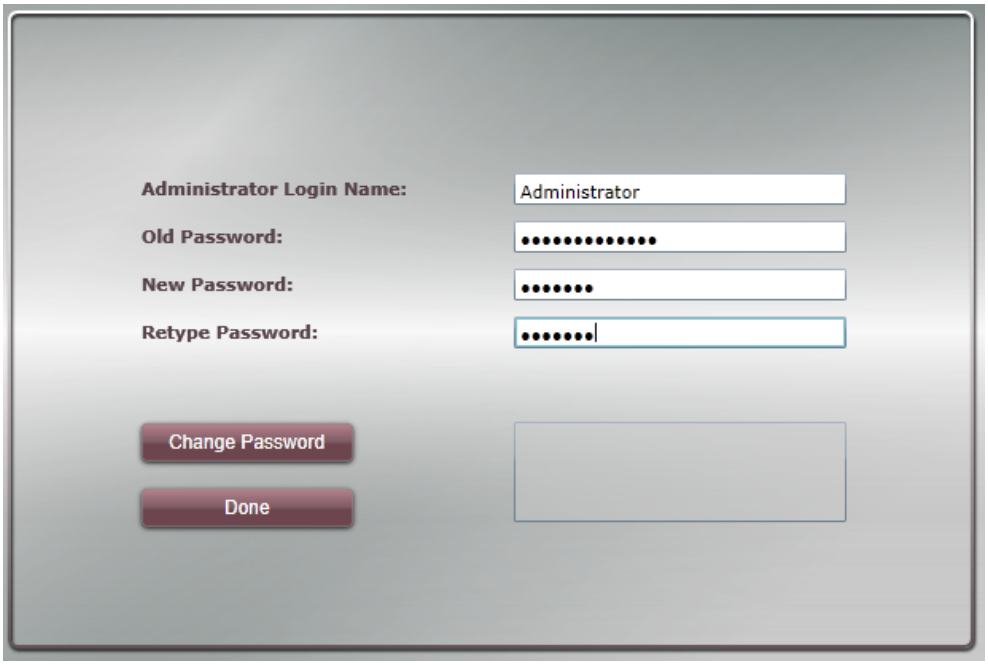

Image 3.17: Setting the password of the Administrator

By selecting *Done*, the dialog moves on to the time and date configuration.

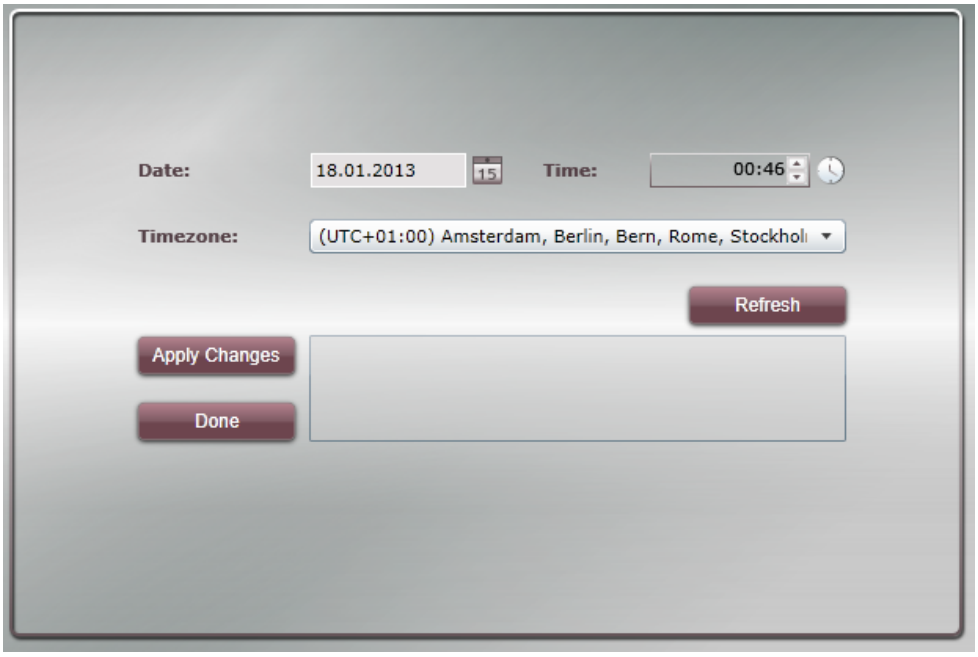

Image 3.18: Time and date configuration

By selecting *Apply Changes*, all changes are applied and by pressing *Done*, the dialog moves on to the next step.

Here, enter a computer name and join the desired domain. After a few moments, the *Reboot* button will become active. The appliance now has to be rebooted and a log-in with the local admin is required.

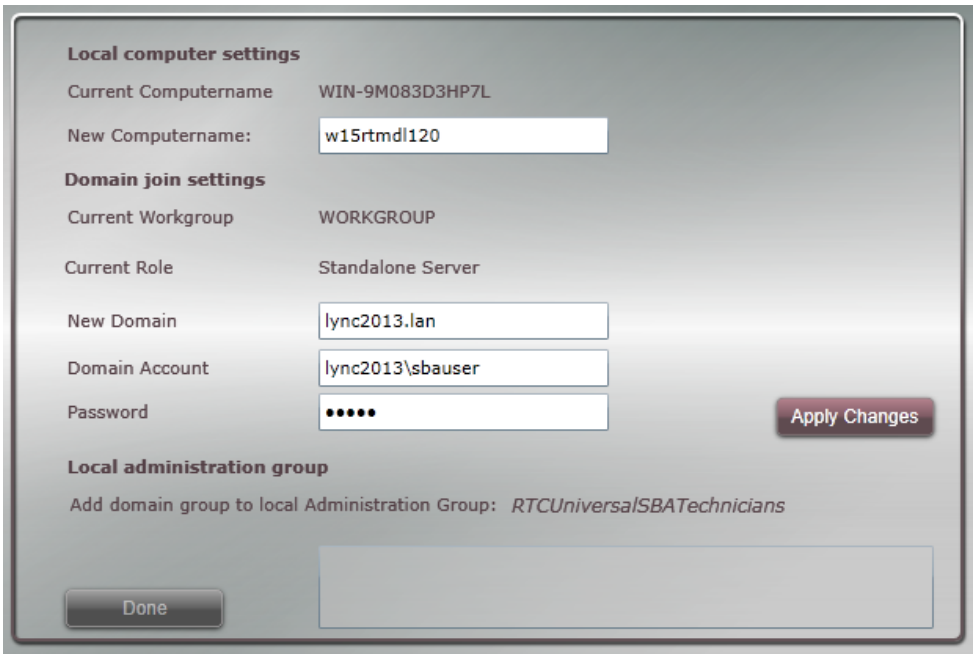

Image 3.19: Adding the SBA to the local domain

After the reboot, the predefined domain group *RTCUniversalSBATechnicians* will automatically be added to the local admins. Leaving the dialog by pressing *Done* results in *Bootstrap* being terminated and the installation part being started.

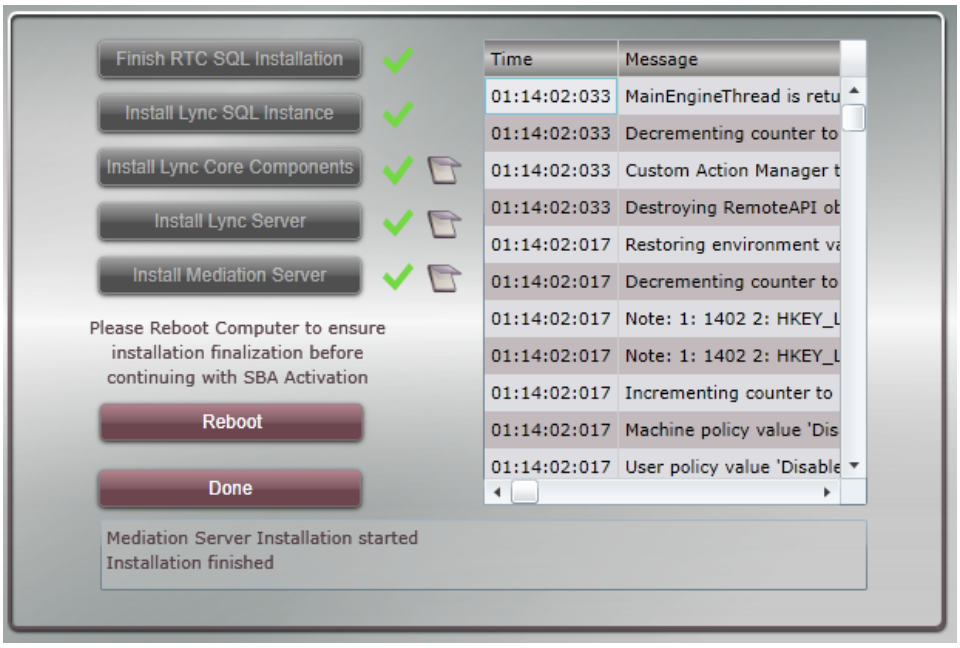

Image 3.20: Overview of the installation progress

The installation will run nearly by itself and is concluded with a reboot. The installation log files can be loaded after every finished step -which can be very helpful in case of any errors.

Note! For the next login, the for the SBA activation prepared account will have to be used. Under this user, the activation of the Microsoft SBA component is executed.

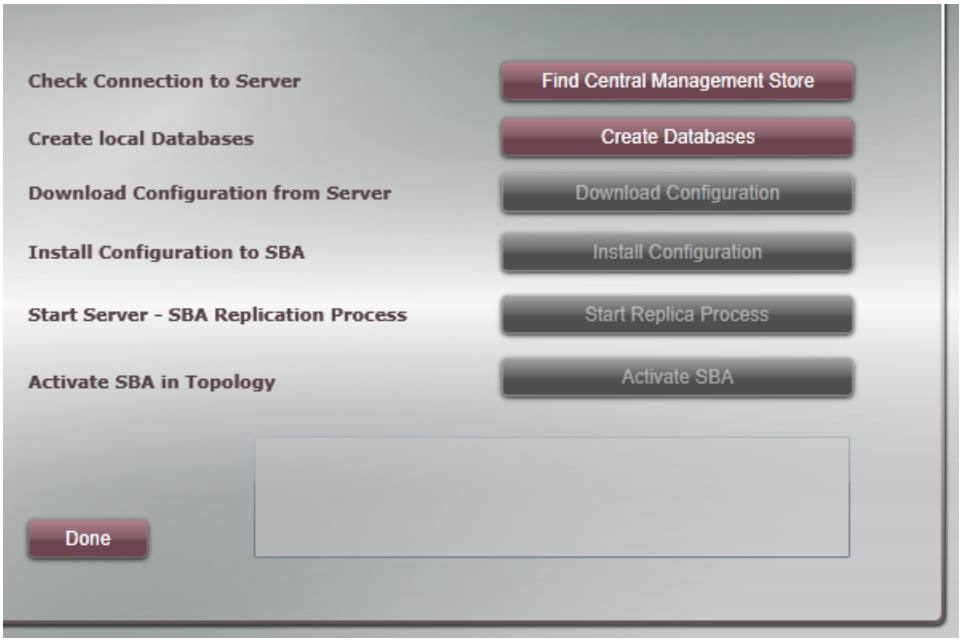

Image 3.21: Checking Connection

- *Find Central Management Store* -makes sure, that a connection to the data base is available
- *Create Databases* -is only used with Lync 2013 SBA
- *Download Configuration* -loads the configuration data from the central Management Store
- *Install Configuration* -applies the information and saves it in the local Store
- *Start Replica Process* -enables the continuous replication of changes

After successful execution of the previous steps, the SBA can be activated and the next dialog can be started by pressing *Done*.

Note! If a certificate server exists within the Active Directory, than that server can be used to acquire and install the required certificate. Alternatively, a ***certificate sign request*** can be generated.

Requesting a certificate online via AD-CA and assigning it

- Enter Username and Password on the left side
- Press *Auto-Install Certificate* – as soon as the certificate is assigned and locally installed, the ***Thumbprint*** appears
- Press *Assign Certificate*

► Offline Certificate Installation

- Press *Offline Certificate Installation* -> a separate dialog appears
- Follow the instructions in the dialog window
- Press *Done*

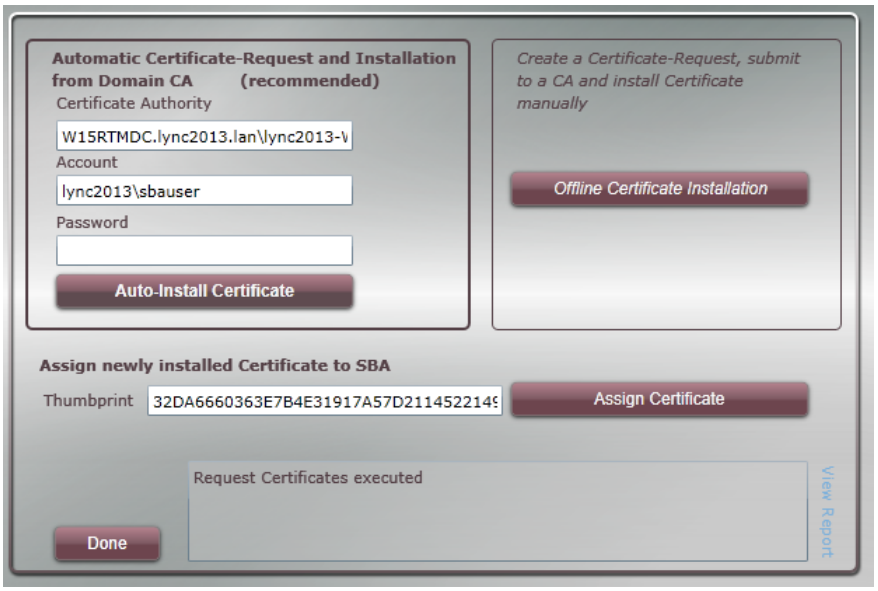

Image 3.22: Requesting certificate

Done finishes the section.

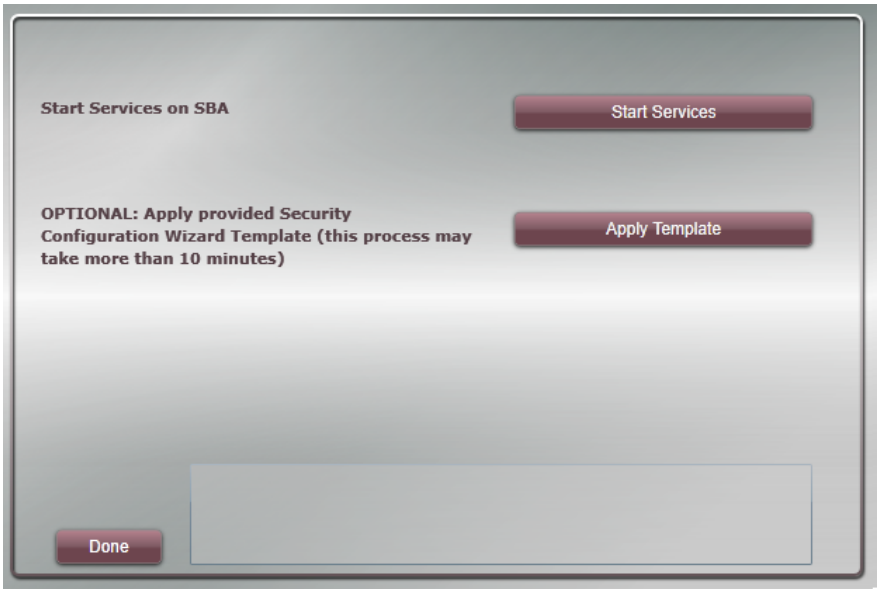

Image 3.23: Start of the SBA Services

All local services can now be started by pressing *Start Services*.

Note! The provided security template can optionally be applied at this point in order to disable undesired services and ports. This should only be done in case of very high system requirements as useful functions like Remote-Desktop will be disabled. Additionally this process will take a long time and can also lead to timeout errors – pressing *Done* right after the start will cause the process to continue in the background. It is advised not to take this step.

Selecting *Done* concludes the activation.

3.2.3. Media Gateway Configuration

The concluding step is the configuration of the Gateway. Most of the time, the Gateway is configured via a separate configuration tool which can be downloaded by pressing the *Gateway* button on the left hand side. A description of this particular configuration step can be found in the chapters OfficeMaster Gate and Lync 2010 and OfficeMaster Gate Configuration.

Media Gateway Board Basic Configuration

The basic configuration of the in-build Gateway card can be made directly via the web interface (The Gateway is a network device and therefore needs its own IP settings).

By pressing *Save*, all the settings are saved and applied. Pressing *Restart Gateway* activates the changes. The Gateway will need roughly one minute to reboot.

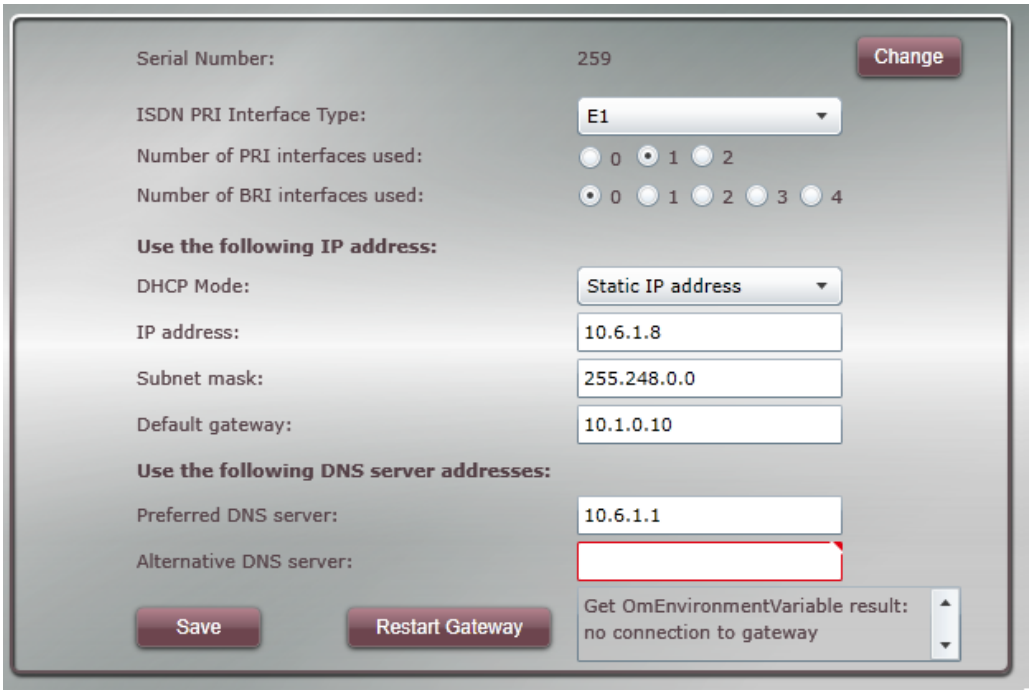

Image 3.24: Network configuration of the Media Gateway Board

In the next dialog, a simple dial plan can be entered. The Gateway will usually only receive the direct dial through (number of digits is important), therefore the number will have to be completed into a E.164 number by adding the „*local prefix*“. Are only BRI Interfaces with MSN (multiple subscriber numbers) in use, then the length has to be set to 0.

Additionally it is necessary that the number code is set and also that the certificate is requested, should it be planned to use TLS and SRTP for VoIP communication.

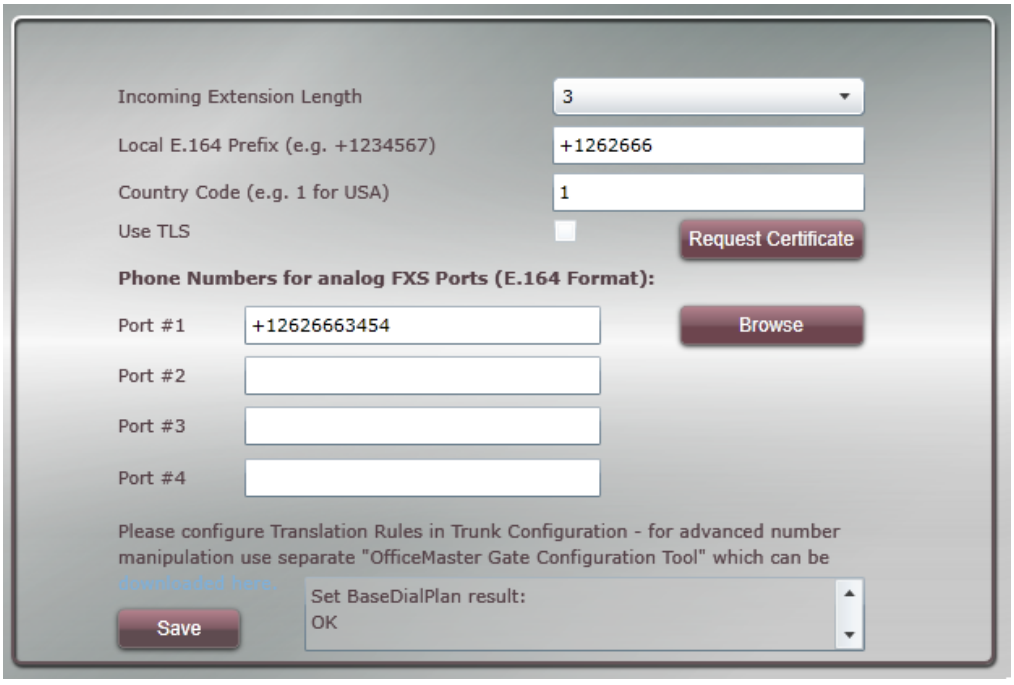

Image 3.25: Basic ISDN Configuration

Based on these rules, a few rules for incoming and outgoing calls are automatically created. For a more advanced configuration OfficeMaster Gate configuration software is required, which can be installed on any PC.

3.2.4. Testing Media Gateway Routing for OfficeMaster SBA

The PSTN connection can be tested via the following dialog. Outgoing calls can if chosen be initialized via the Lync Server functions. Those are contacted via the web interface. Before such a test, the respective users have to be created and configured. Alternatively one can also connect the Gateway directly for test calls.

The test functionality in the lower area controls the Gateway directly, without using the Lync Server Component.

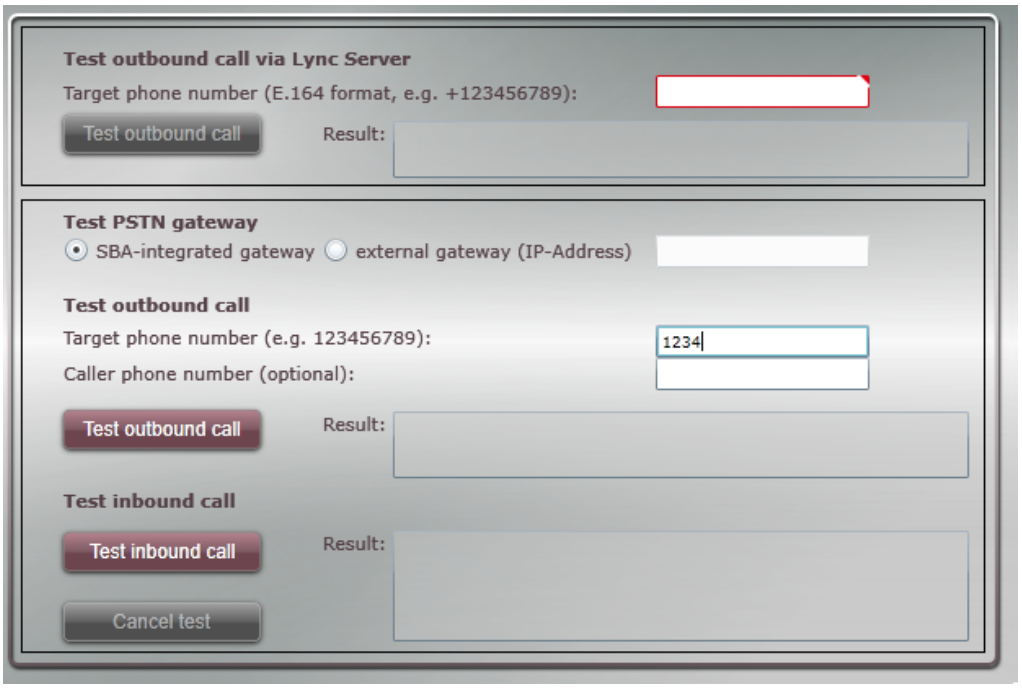

Image 3.26: Test of the Configuration via the web interface

3.2.5. Display Event Logs and Syslog File

After starting OfficeMaster SBA Administration via browser and logging in with the adequate credentials (e.g. SBA technician account created for bootstrapping), pressing the *Diagnostics* button on the left side shows information from several sources (Lync server log, Windows event logs and Gateway syslog).

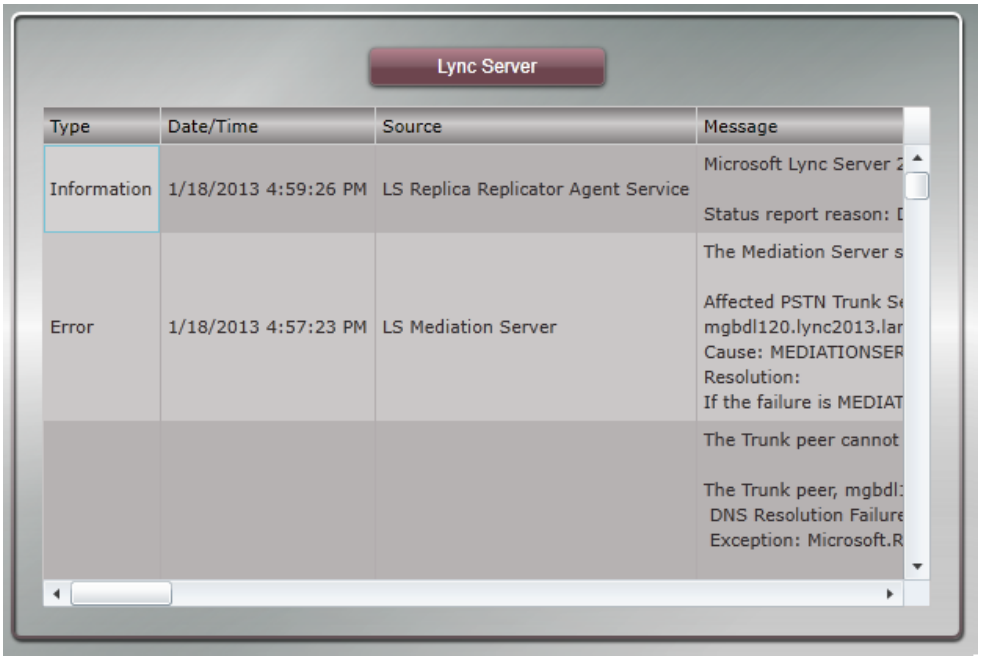

Image 3.27: SBA Log files

3.2.6. System Status

Clicking the *Status* button shows the administration page, where Lync related services can be started or stopped. The status of the service can be queried.

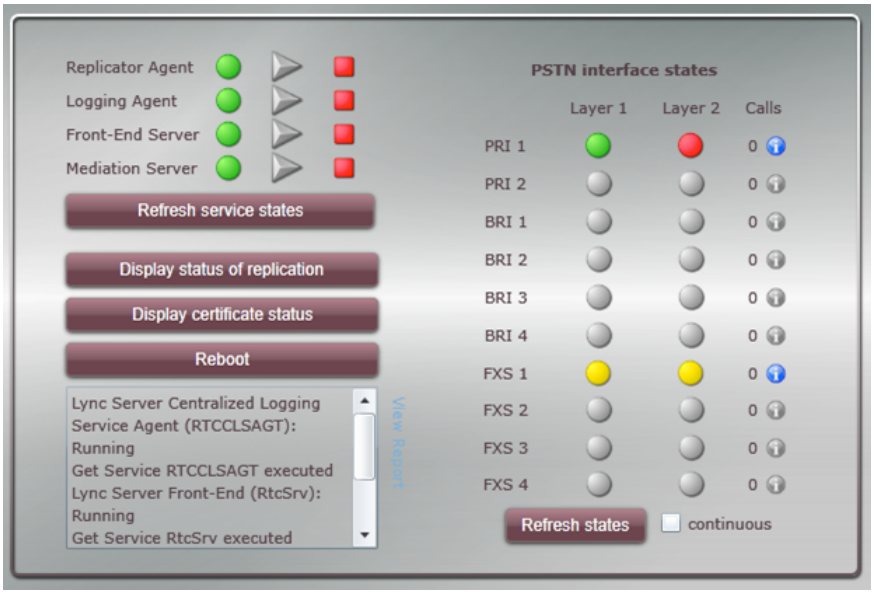

Image 3.28: Performance status Master Gateway Board

Table 3.3: The Status of the PSTN ports are displayed via colored buttons

grey	not used
yellow	idle
green	Layer (1 or 2) active/activated
red	Layer (1 or 2) inactive/disabled

3.3. OfficeMaster Gate and Lync Server 2010

This chapter documents the necessary configurations for using the phone functions of Microsoft Lync Server 2010 and OfficeMaster Gate. For reasons of comprehension, the connection via TCP and RTP (also unencrypted) is explained first. The configuration of an encrypted connection via TLS and SRTP is explained afterwards.

3.3.1. Connection via TCP/RTP (not encrypted)

For the complete phone function with external participants (***Enterprise Voice***), a few configuration steps have to be carried out on the Lync side.

► Topology

Before any Lync components can be installed or used, they have to be made known in the topology. For this, ***Lync Server Topology Builder*** was designed, with which all servers and server rolls but also components like a PSTN gateway are laid out. The gateway object is created at the respective site in the folder ***PSTN gateways*** via the function *New IP/PSTN Gateway...*.

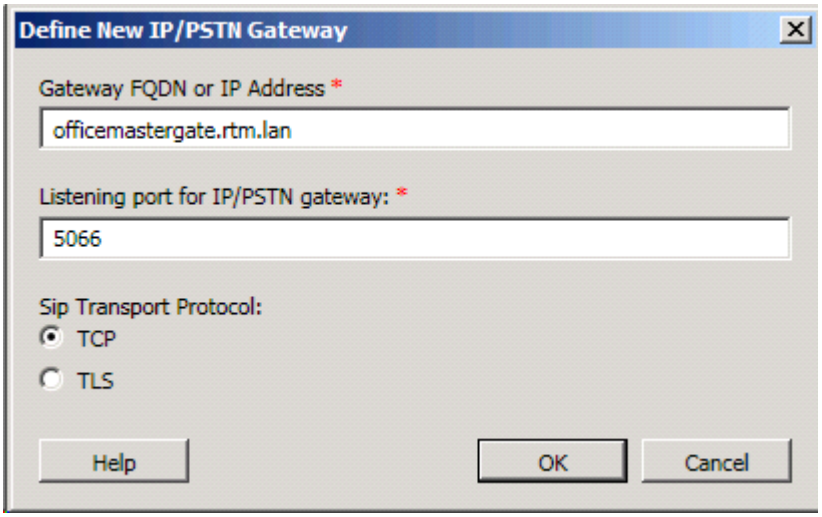

Image 3.29: Setting Gateway in Topology

In the first step, an unencrypted configuration is set up, also via TCP. As target port, we suggest using ***5066***.

Note! Has in the gateway the normal value of 5060 been used for TCP, 5060 must be used here as well. Alternatively the suggested value 5066 can be used. In that case the VoIP parameter for TCP in the gateway configuration has to be changed as well. The definition of target ports in both directions (Lync --> Gateway / Gateway --> Lync) is independent from one another. Important is only, that both sides are set up with fitting configurations.

Usually, the Lync-Mediation Server will use the port 5068 for incoming TCP connections and the port 5067 for incoming TLS connections. Those ports are therefore to be set up in the rules of the gateway for incoming calls. For the other way, so towards the gateway, there are two possible ways:

- Use of the SIP standard port (5060 for TCP and 5061 for TLS)
- Use of the suggestions of the Topology Builder (5066 for TCP and 5067 for TLS)

Whatever was is chosen, it is important that in any given case, the settings of the Topology Builder and those of the VoIP parameter in the gateway are consistent with each other.

This will have laid out the gateway, but the assignment to a Mediation Pool is still missing. This is why the Topology Builder will still show an icon at the top left side, indication that the configuration is yet to be completed. A click on Lync Server 2010 (top) will show applicable details under *Topology validation errors* in the main window:

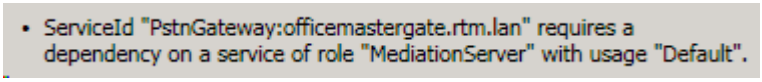

Image 3.30: Topology builder error message

Under „Mediation pools“ the preferred server is selected and editing activated by pressing *Edit Properties...*. There, the gateway is selected and added to the server.

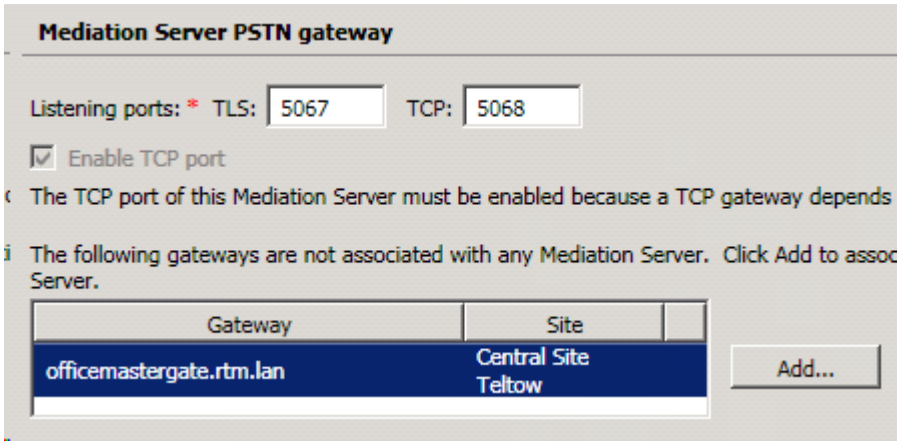

Image 3.31: Mediation Pools

The ports that the Mediation Server will accept incoming connections are also selected here. These, contrary to common belief, do not have to be identical to the ports at the gateway side. Important is solely, that the respective side addresses the right ports of the other side. The Lync side was just configured when the gateway was set up, the gateway side will be explained further down where the advanced gateway configuration mode is explained. In the simple mode, that the ports shown are automatically used as targets.

After every change in settings, the Topology has to be published by pressing Publish... . Afterwards, in the Lync Control Panel under Topology it can be checked whether or not the changes have been replicated by every server.

▶ Dial Plan

Another important part of telephony is an appropriate Dial Plan. Dial Plans can very easily be set up and configured via the „*Lync Server Control Panel*“. A standard Dial Plan called *Global* exists from the start and cannot be deleted either. Has nothing contrary been configured, this is true for every user.

The Dial Plan mainly is a collection of normalizing rules for phone numbers. These rules are responsible for making it possible, that the user can call phone numbers in the familiar way, independent from for example his location. The result of normalizing should always be a phone number in the E.164 format, as that is what is used as standard in Lync. Every site should have its own dial plan, as the rules are highly dependent on local circumstances.

Example 3.5.

(E.164-Number: +498931769876)

+49 = Germany

89 = Prefix Munich

3176 = participant number (Microsoft)

9876 = extension

»End of example

The format has to be exactly like the example, no spaces or separators may be used. Normalizing rules usually are configured for:

- local calls
- long-distance calls
- international calls
- internal calls
- emergency calls

For all those cases, E.164 numbers should be the result. These then are automatically recognized by Lync and otherwise redirected to the appropriate gateway. There, through the use of additional rules, they are adjusted to the requirements of the existing telephone infrastructure.

The example shows a normalizing rule for long-distance calls. Fundamentally, the setting up of a rule is supported by a graphic interface, which helps to set up the rule correctly. More complex formulas will have to be built manually though.

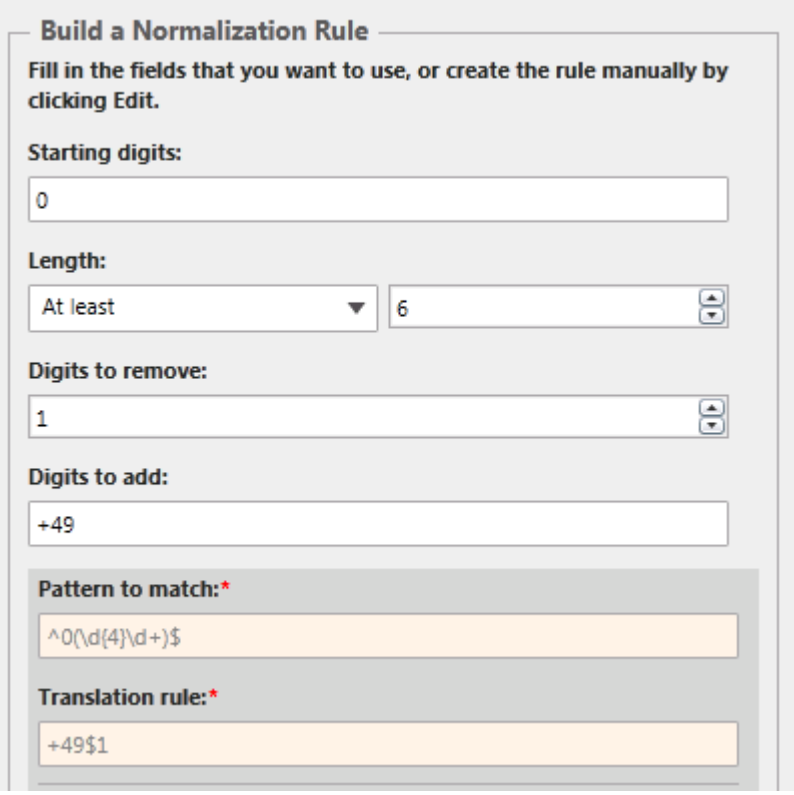

Image 3.32: Building a normalization rule

This rule is activated for all numbers that start with a 0 and are in total 6 digits long. One digit (the leading 0) is then eliminated and the numeric sequence +49 is added at the beginning. This changes 0301234567 into +49301234567 and therefore the required the E.164 format. All other rules need to be built in the same way. Mind that the rules are processed from the top to the bottom, until a match has been found.

A rule for international calls could be constructed similarly (Difference: two leading 00's, those are eliminated). This rule should be located above the long-distance rule, as the long distance rule would also be triggered because of the first 0. That would lead to the number 0043198765 being converted into the wrong number +49043198765 instead of +43198765. Alternatively, the long-distance calls rule could also be constructed that way, that not only the first digit has to be a 0, but also that the second digit cannot be a 0 as well („Starting digits" would then be ***0[1-9]***).

- ▶ Routing

Lastly, it has to be secured that outgoing calls are directed via the configured gateway. For this, a connection will have to be made between the ***PSTN Usage***, meaning the call classes like internal or local, the ***Voice Policy*** assigned to the users and the ***Route***, meaning the path to the gateway.

This process will not be explained here, as there is a detailed explanation by Microsoft available. This mechanism allows for a flexible definition of calling allowances as well as Least Cost Routing.

For example, the following settings should be used:

► Lync server settings

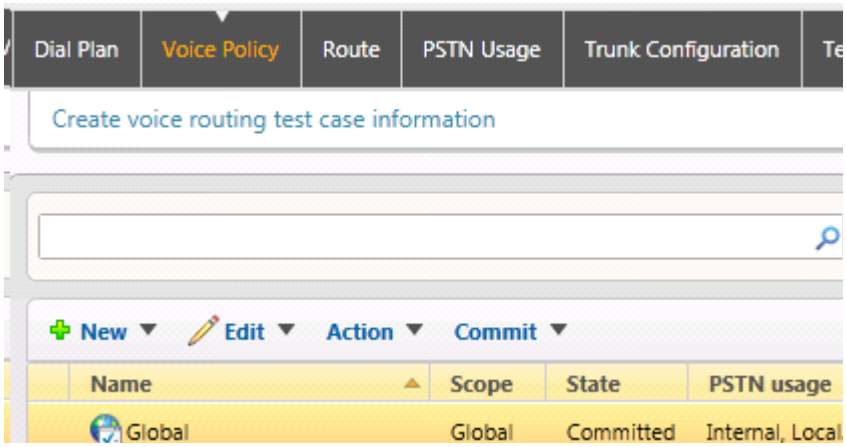

Image 3.33: Voice Policy:

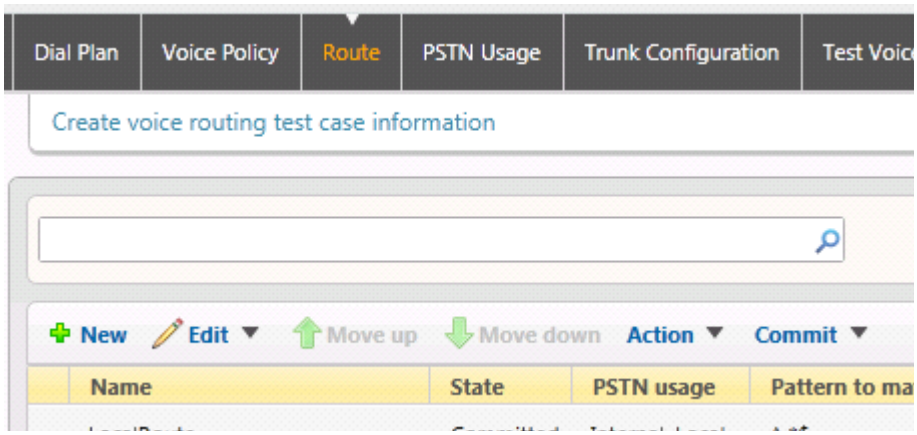

Image 3.34: Route

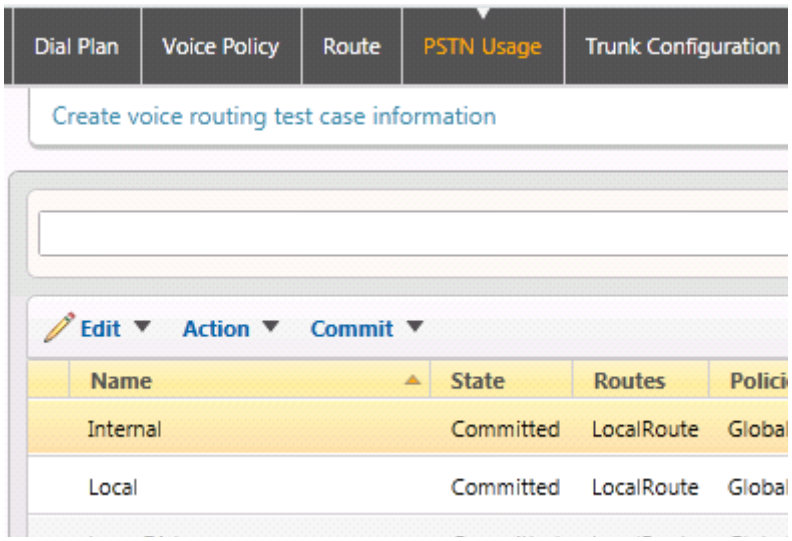

Image 3.35: PSTN Usage

Ferrari electronic

In *Route*, enter the pattern **^.*$**. This way, the pattern is true for any calling number. (^ = match from the first sign on, Dot = followed by any sign, Asterisk = any number of repetitions).

▶ User settings for Lync telephony

In order to be able to make external calls, the user needs to be activated for ***Enterprise Voice***. Furthermore, every user needs a phone number in E.164 format:

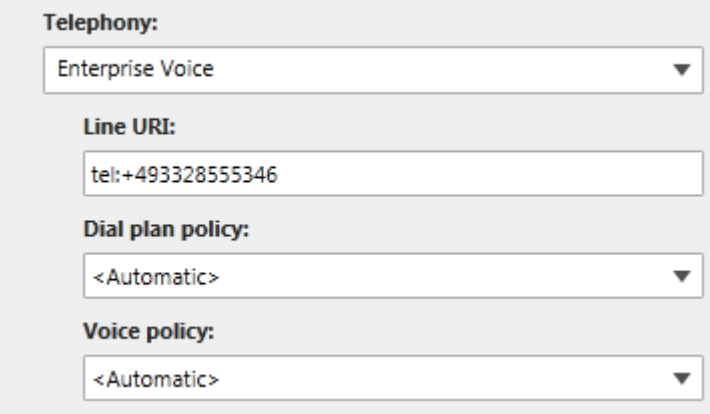

Image 3.36: User settings

If the user wants to sign in on a Lync phone via dial through, this dial through has to be additionally and separately configured:

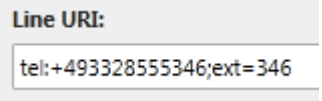

Image 3.37: Line URI

▶ In the Topology Builder of the Microsoft Lync Server, the gateway is defined

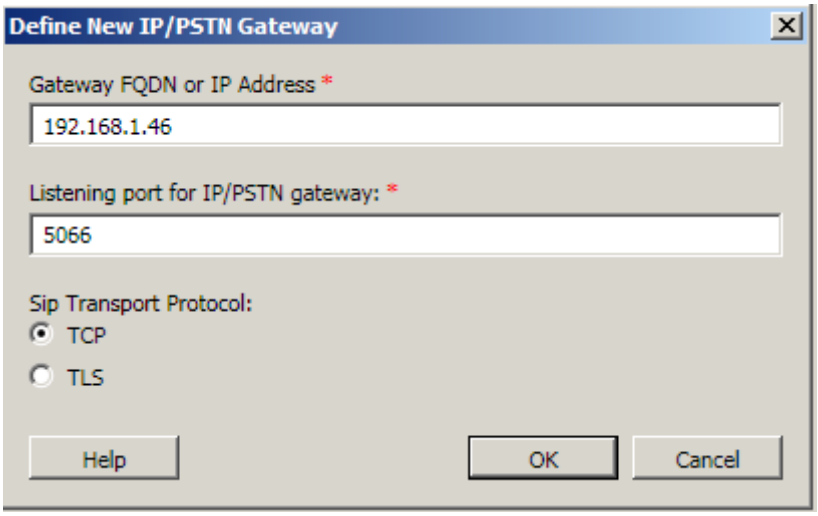

Image 3.38: Adding a Gateway in the Topology Builder

The Topology Builder also has an overview, were the ports are listed on which the mediation server accepts incoming calls. For this, TCP has to be activated.

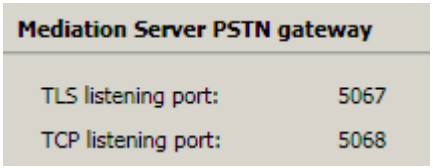

Image 3.39: Ports for incoming calls

▶ Settings for OfficeMaster Gate

In the OfficeMaster Gate configuration program, (Start> Programs> OfficeMaster Gate configuration) ports are configured via Edit> VoIP parameters. The values should be the same as shown here (the ports can vary in the way described earlier on).

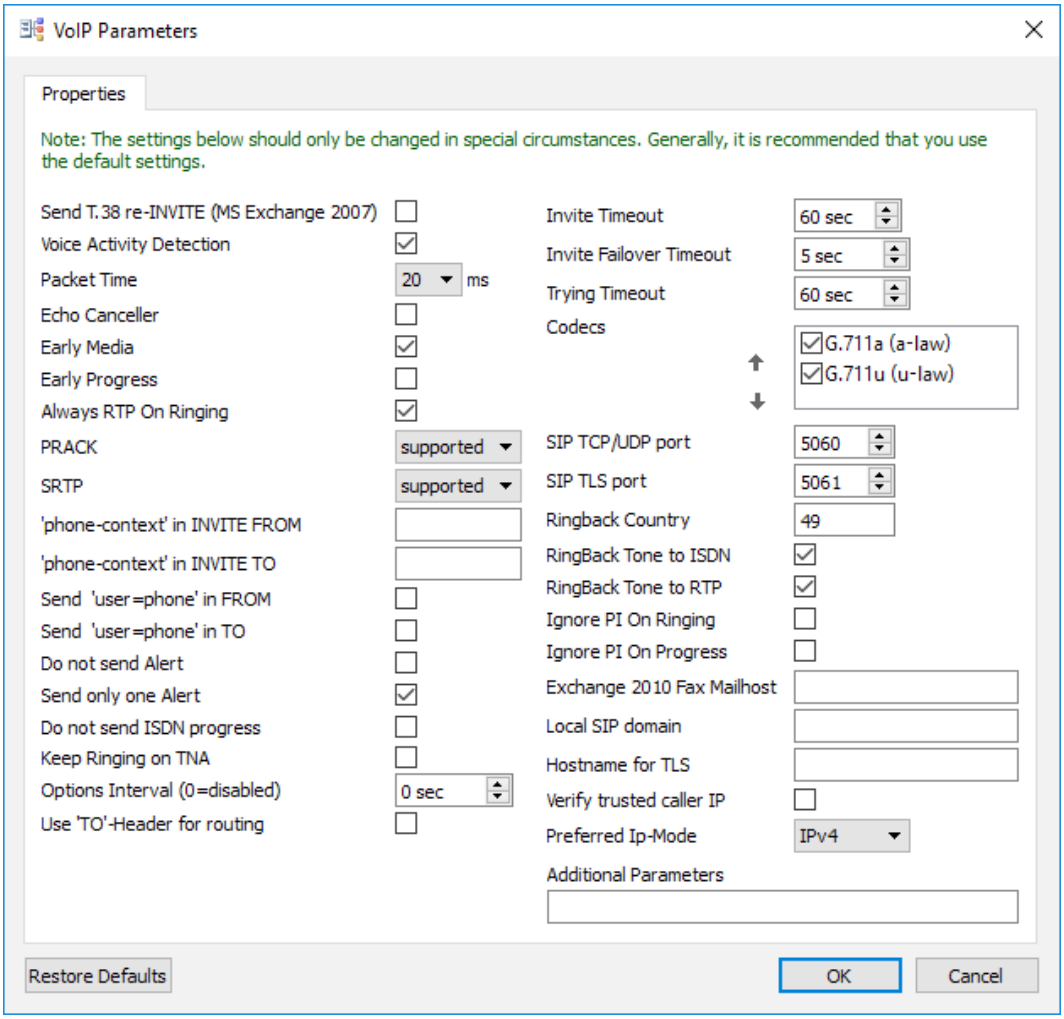

Image 3.40: Configuration of the VoIP-Parameters

The *Operation Mode* of the gateway has to be set to ***Gateway/mixed*** and the *Configuration Mode* has to be set to ***basic***. (Both options can be found at Edit> Operation Mode and Edit> Configuration Mode respectively.

Note! It is advised to at first use the basic configuration mode as this will create a first standard rule base which can be used as a starting point in the advanced mode.

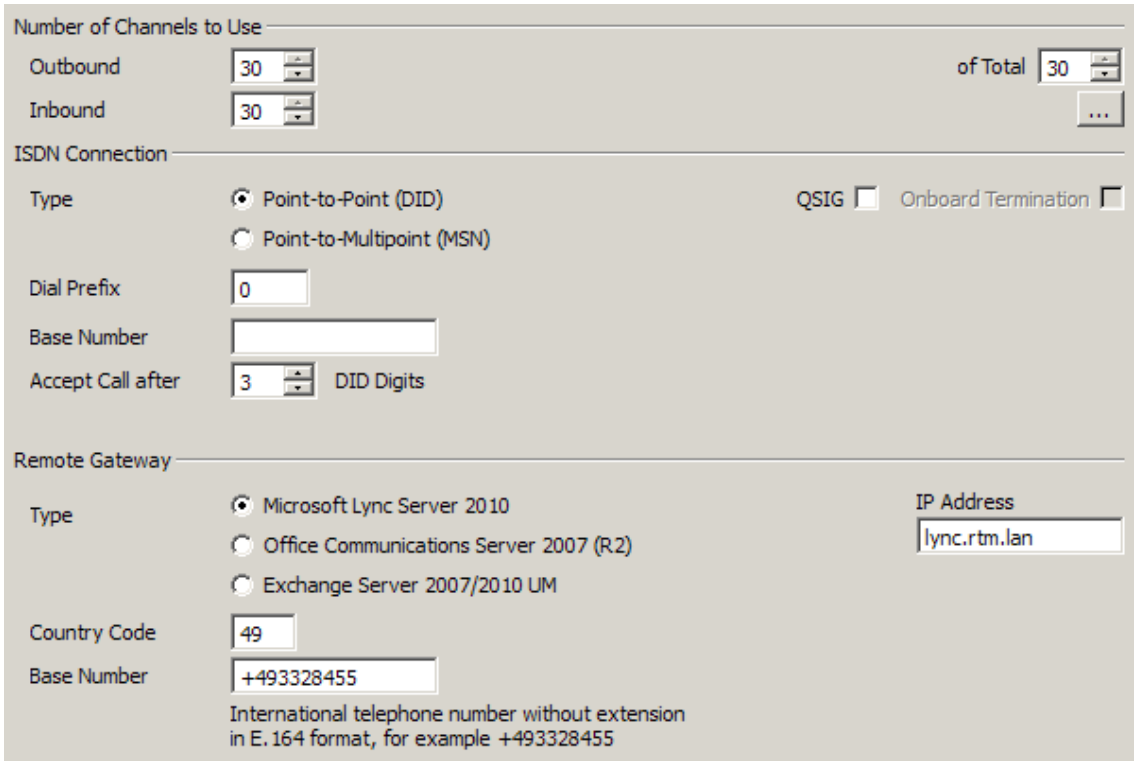

Image 3.41: Linking Lync 2010 in basic mode

Should, for the manipulation of calling numbers, more rules be needed, then the *Configuration Mode* can be set to ***Advanced***. A test of the rules is also possible offline, by simply pressing the *Test* button.

3.3.2. Configuring TLS/SRTP

► Time Settings

For the use of certificates it is important, that the internal clock is as accurate as possible. For this, a NTP-Server should be configured. The necessary settings can be found under Edit-> Time Settings

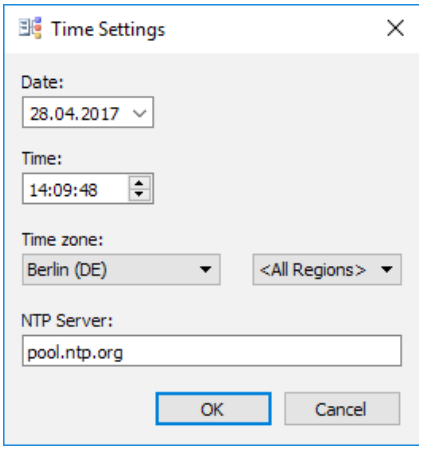

Image 3.42: Time Settings

► Adjusting in the Topology

In order to process the communication between gateway and Lync Server via encrypted TLS, a few changes have to be made in comparison to those in the Connection via TCP/ RTP chapter.

First, the ***topology*** in the gateway configuration has to be fixed with the Topology Builder:

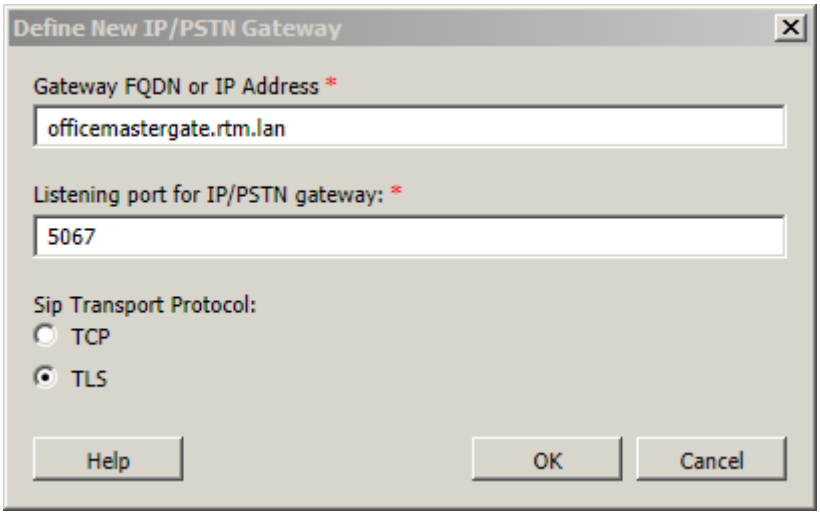

Image 3.43: Configuring Gateway for TLS

Afterwards, the changed Topology has to be published.

► Adjustments in the Gateway

First off, the *gateway configuration* has to be set to advanced mode. There, the rule for incoming calls is adjusted:

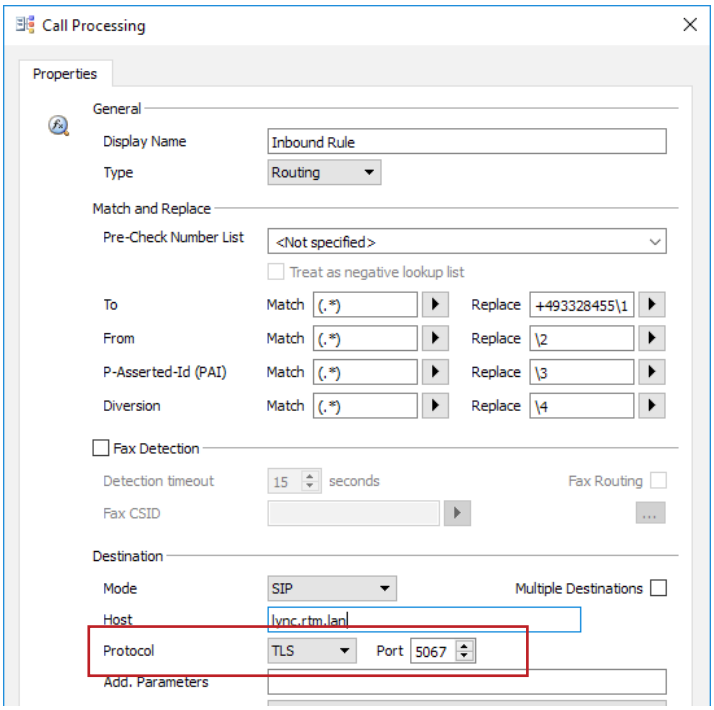

Image 3.44: Incoming rules for TLS

Additionally, a certificate has to be requested and installed for the gateway. The base certificate of the providing certification office has to also be copied into the gateway.

Via Edit > Certificates> Create, a certificate request is created:

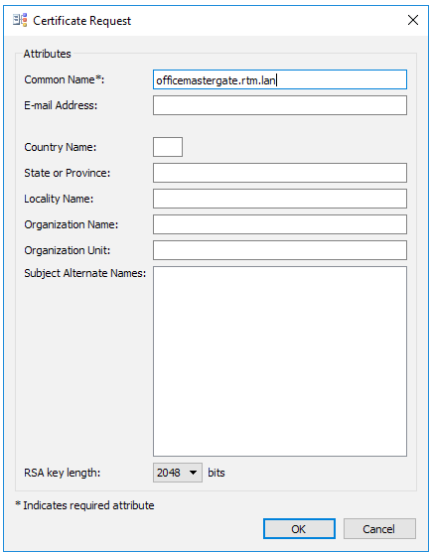

Image 3.45: Requesting Certificate

Important to note is that the *Common Name* has to be identical to the name of the gateway in the DNS! All other fields can be left empty, unless the certification office requires those in order to issue a certificate.

The certificate request can afterwards be taken out of the clipboard and handed into the certification office:

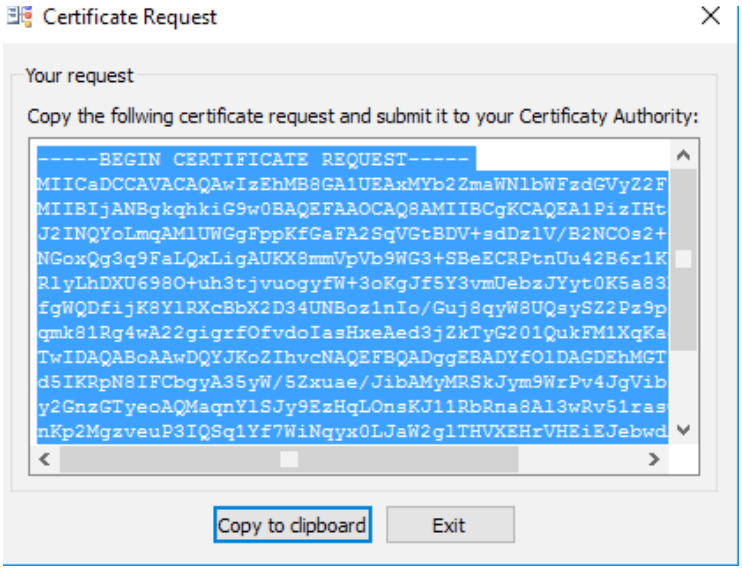

Image 3.46: Certificate Request

With a Windows certification office, these are the steps that need to be taken:

- Selection of the certification administration in the browser („..../certsrv“)
- Certificate Request

- Advanced Certificate Request
- base-64-encoded...
- Copy the request from the clipboard into *Saved Request*
- choose template *Web Server*
- "*Submit >*"
- Download certificate

The locally saved certificate is afterwards loaded into the gateway by pressing *Import...* in the *Install Certificate* section.

Now the certificate of the certification office has to be saved locally by pressing *Download a CA certificate...* and *Download CA certificate*. After that, the certificate is copied into the gateway by pressing *Import...* in *Root CA Certificate*.

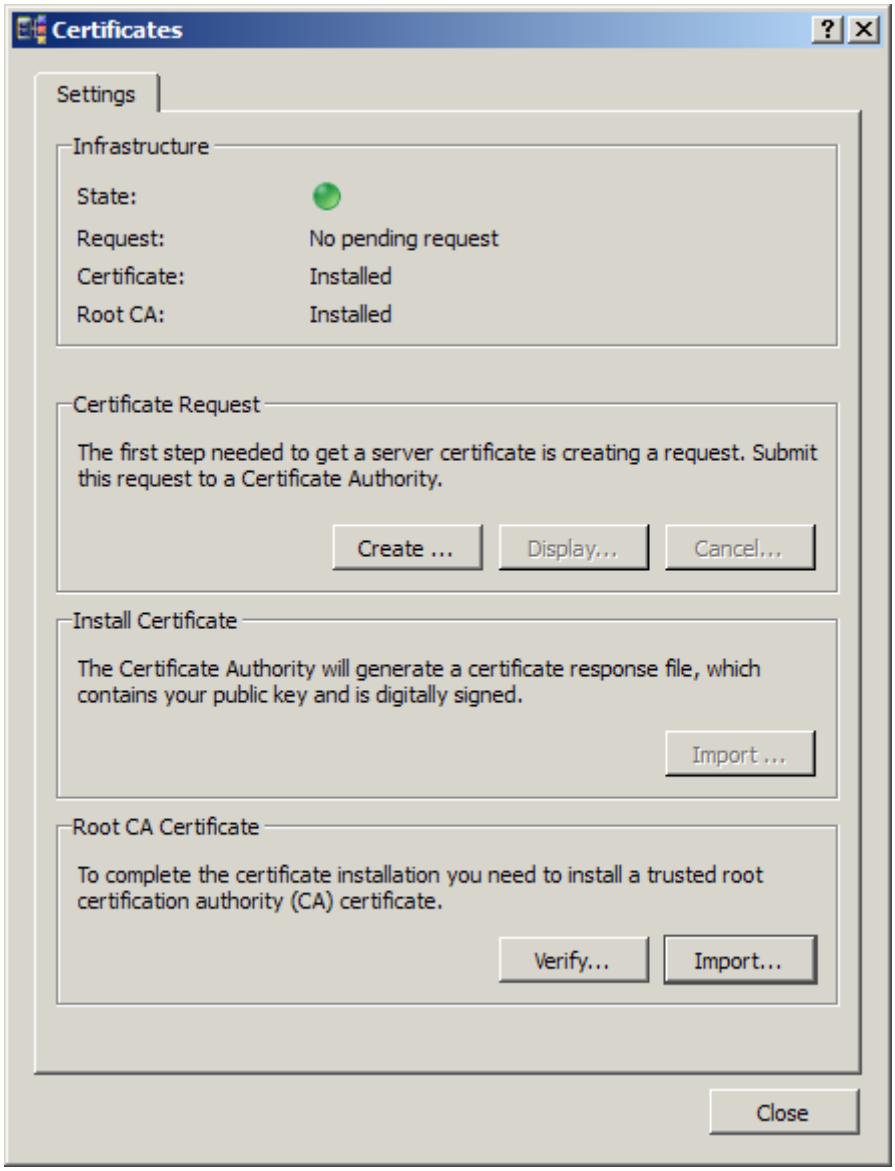

Image 3.47: Imported Certificate

With this, the setting up of the SIP encryption via TLS is completed. By pressing *Verify...*, it can be tested if a TLS connection can be set up to the target.

Note! If the same gateway is addressed by multiple Mediation Servers, it has to be defined in the Topology under multiple DNS names (all with the same IP address). To further use TLS in this case, the additional names have to be stated as ***Subject Alternate Names*** when requesting a certificate.

3.4. OfficeMaster Gate and Exchange Unified Messaging

Note! If Exchange UM is used as a voice mail system with OCS or Lync, no additional configuration of the gateway for Exchange is needed. The systems mentioned above independently set up the connection to the UM role.

Shall an ordinary telecommunications installation be connected to Exchange UM via OfficeMaster Gate, begin the configuration in the basic mode of the configuration program (see basic configuration mode).

With this, the gateway should already be ready for use. Further information can be found under *Functionality* and *Connection*.

3.4.1. Receiving Fax with Microsoft Exchange 2010

Introduction

Microsoft Exchange Server 2007 with the Unified Messaging Role provides the possibility to receive fax, without having to use third-party software. This fax function is based on the voice mail system, meaning that incoming fax calls need to reach the Voice-Mailbox of the respective user first. After successfully having set up the connection, the protocol has to be changed from language to T.38 Fax to enable fax receiving. The VoIP gateway in use has to support T.38 for this function.

Fax is not part of Exchange UM, additionally some useful features for fax like ECM (error correction) are missing. Nevertheless, this solution has proven to be a useful extension to the Unified Messaging-Software of a wide range of users.

Receiving Fax with Exchange 2010 UM

With Exchange 2010, Microsoft decided to completely leave fax communication to third party software, quite like in their Exchange 2007 versions. In order to enable users to still receive fax messages, Microsoft built in the option of switching between Voice-Mailbox and fax. This is realized via separate fax solutions, which receive the fax via T.38 and then, like in Exchange 2007, send an email with TIFF attachment to the mailbox of the user.

Concept of the Partner Fax solution for Exchange 2010

The following graphic shows, how incoming fax messages are processed with Exchange 2010 in combination with a partner solution (T.38 based fax server):

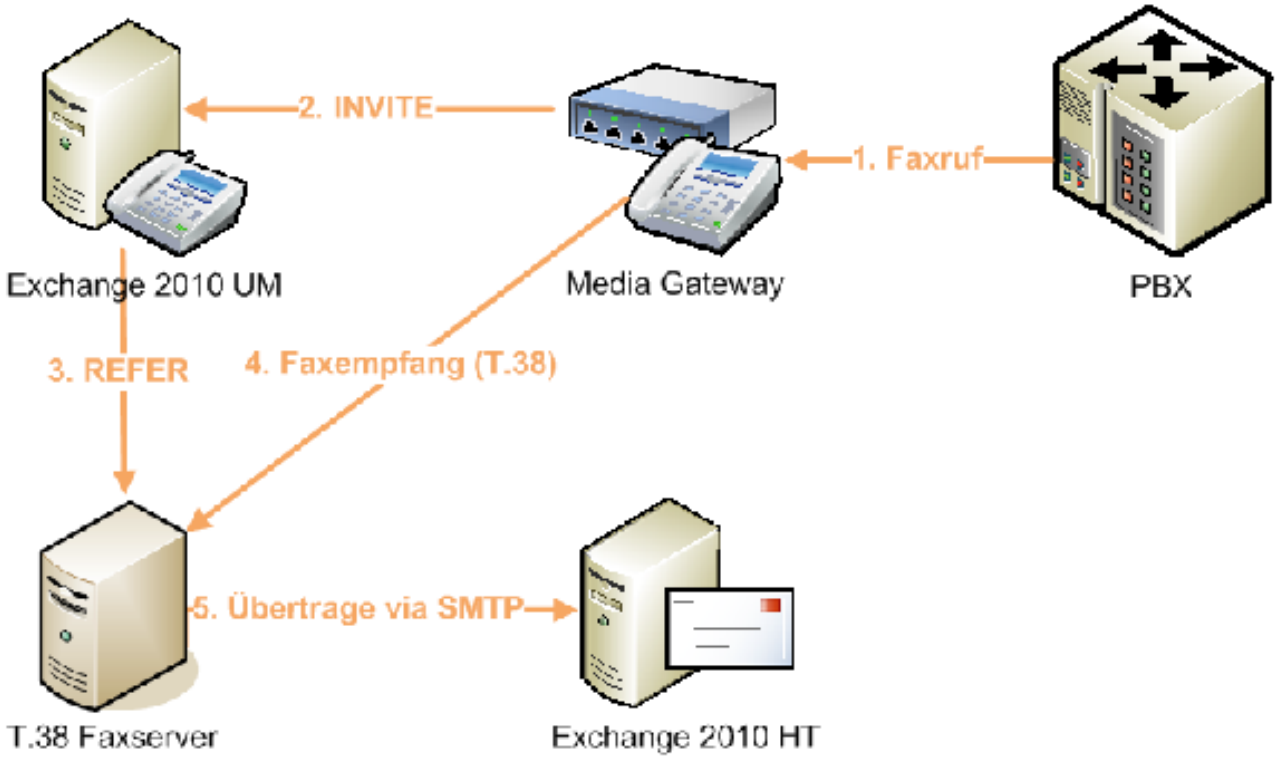

Image 3.48: Receiving Fax with Exchange 2010

Internal Fax solution vs external provider

Partner fax solutions can either be installed directly at the customer or provided by an external third-party provider. If all fax features including dispatching are required, an installation on site is usually the best way to go. The applied UM-Gateway should for this be compatible with this fax solution.

With external fax solutions, usually only the receiving of fax solutions (which is enough for most users especially in the USA) is supported. In this case T.38 fax data is routed via the normal internet connection, which results in lowered service quality (rate of successful fax messages). The translation of T.38 to connection with Jitter and packet-loss on the internet as well as several different sending fax devices can lead to a decrease in the success rate from 100% (with direct TDM/ISDN connection) down to 90%.

OfficeMaster Gate - UM Gateway with in-built fax solution

OfficeMaster Gate, the Ferrari electronic UM/UC Gateway for Exchange UM and OCS 2007 (R2), provides a unique solution for this. Media gateway and partner fax solution are here combined in one device!

Incoming fax connections, that reach the Exchange UM-Mailbox, are directed back to the Gateway, which still holds the PSTN connection. OfficeMaster Gate receives the fax directly via the T.30 fax protocol (without converting it to T.38) and forwards it after successfully receiving it to the mailbox of the user.

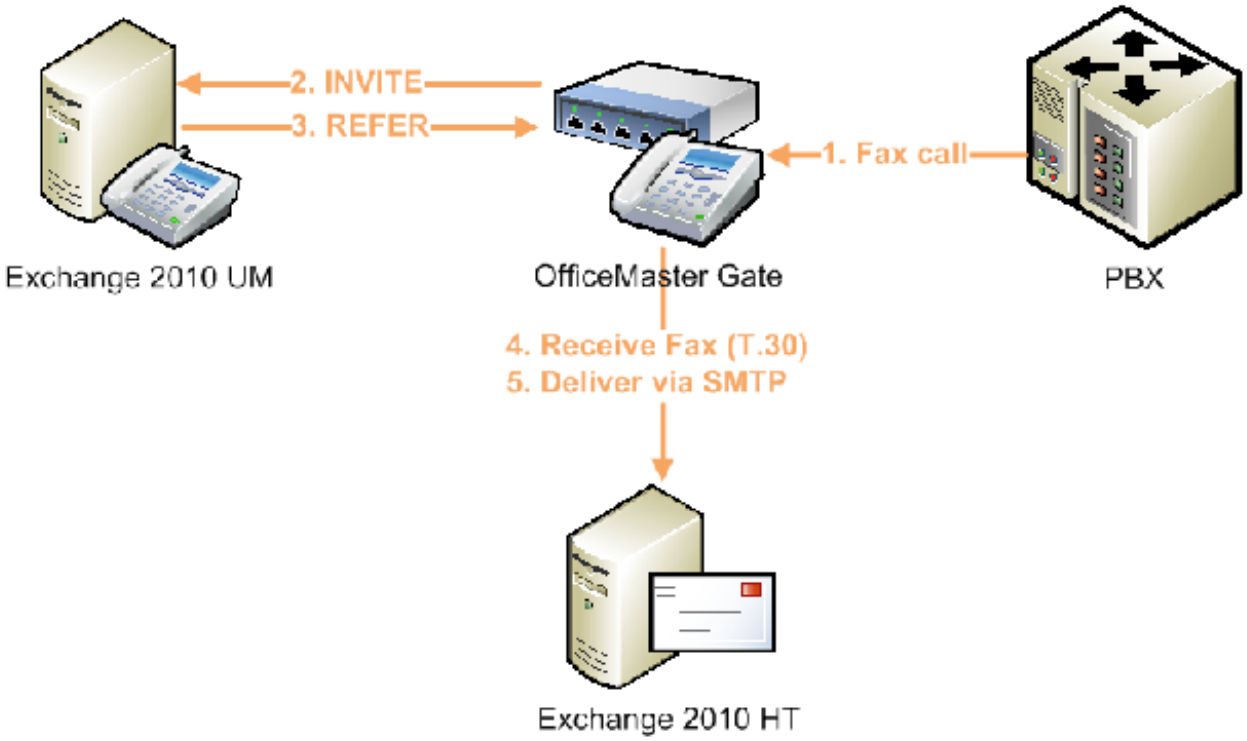

Image 3.49: Integrated fax income in OfficeMaster Gate

This provides several advantages for the user:

- No separate fax solution of a partner of service provider is needed.
- The success rate is very high, due to the fax message being directly received via the T.30 protocol at the ISDN port.
- This function is provided without further cost with every OfficeMaster Gate that supports fax.

Configuration of fax with Exchange 2010 and OfficeMaster Gate

Only a few simple steps are required in order to configure the function to receive fax via Exchange 2010 and OfficeMaster Gate:

- Fax has to be activated in the dial plan, the mailbox policies and the mailboxes of Exchange 2010. Additionally, the *Partner Fax Server URI* has to be declared in the mailbox policies.
- The address of the Hub-Transport Servers has to be configured with the port of the reception connector at OfficeMaster Gate.

Exchange 2010 configuration steps

The settings can either be configured via the Exchange Management Shell or via the Exchange Management console. Experienced administrators will know of the steps required in the Shell. The settings of the console are explained in the following.

To enable fax in a dial plan, check the appropriate box in the *General* tab. In the linked mailbox policy, select *Allow inbound faxes* and declare the SIP URI of OfficeMaster Gate:

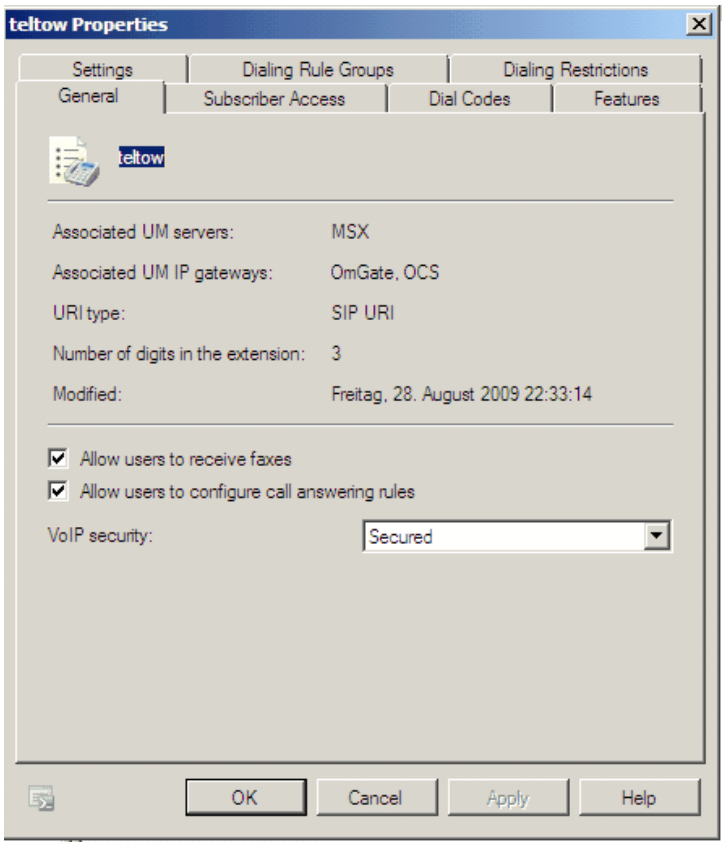

Image 3.50: Activating fax in the dial plan

In the connected mailbox rules, *Allow inbound faxes* has to be selected and the SIP URI of OfficeMaster Gate has to be set.

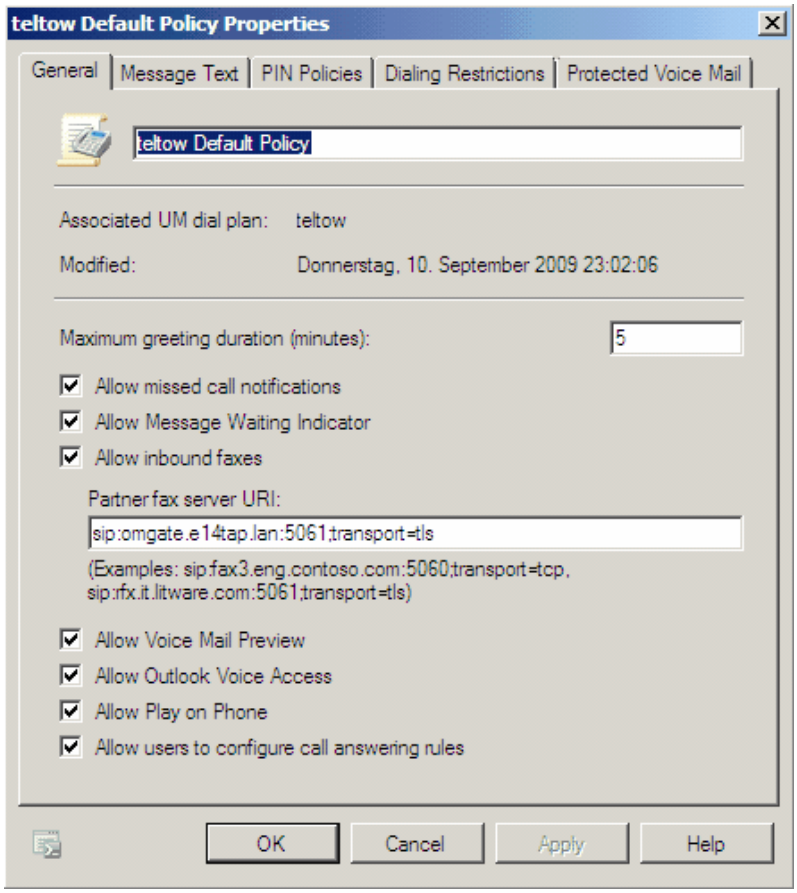

Image 3.51: Allowing incoming fax

As addition to the address of OfficeMaster Gate (Partner fax server URI), ***5061; transport=tls*** has to be added for a saved dial plan, ***5060;transport=tcp*** for an unsaved dial plan. Saved dial plans are required, should the policy also be used for OCS and/or Lync.

Additionally, a separate reception connector has to be set up, in order to accept fax messages which are received via SMTP of the partner fax solution (OfficeMaster Gate). The connector has to allow that mails, send from the IP of the OfficeMaster Gate via an idle port (for example 2525), are received.

The following additional settings have to be made for this connector:

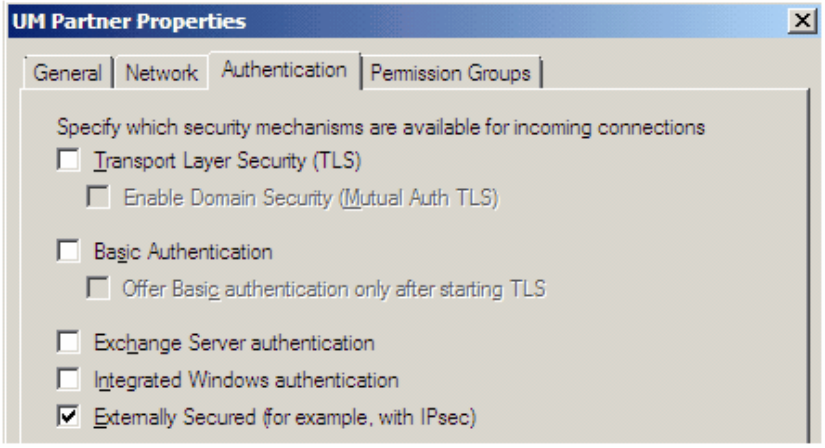

Image 3.52: Connector Settings - Authentication

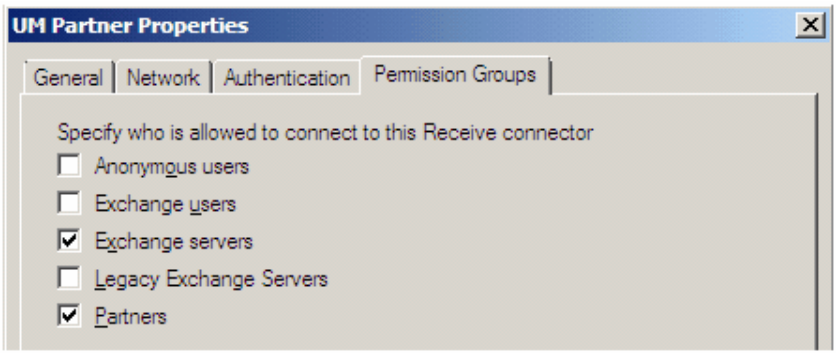

Image 3.53: Connector Settings - Permission Groups

OfficeMaster Gate Settings

Incoming calls are processed by OfficeMaster Gate via one or more rules. *Fax Detection* has to be activated, so that OfficeMaster Gate can switch between receiving faxes and incoming voice mails:

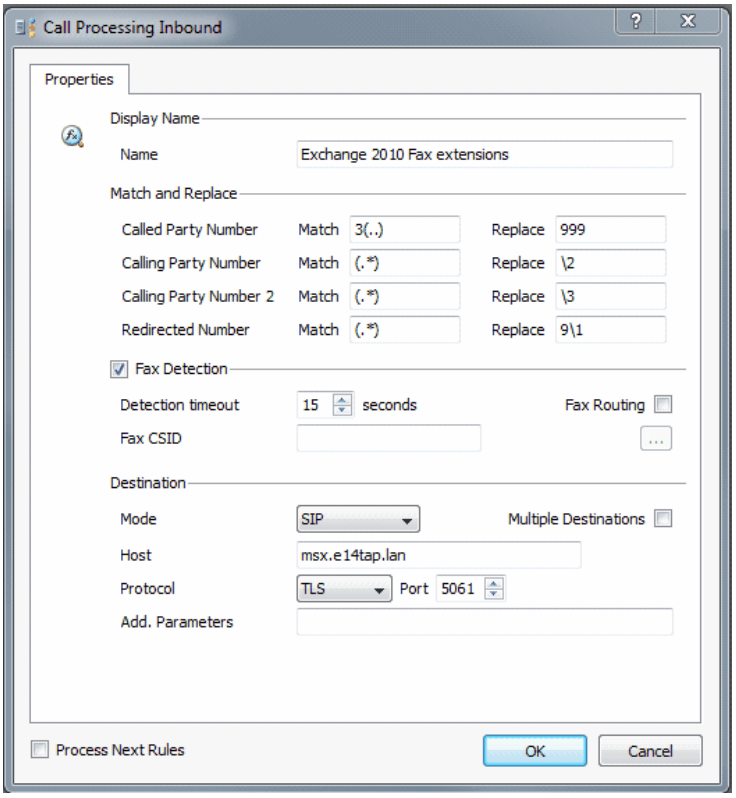

Image 3.54: Rules in OfficeMaster Gate

According to the dial plan, *TLS/5061* or *TCP/5060* has to be selected. Under Edit > VoIP Parameters..., FQDN and port are inserted in the Exchange 2010 Fax Mail-host box

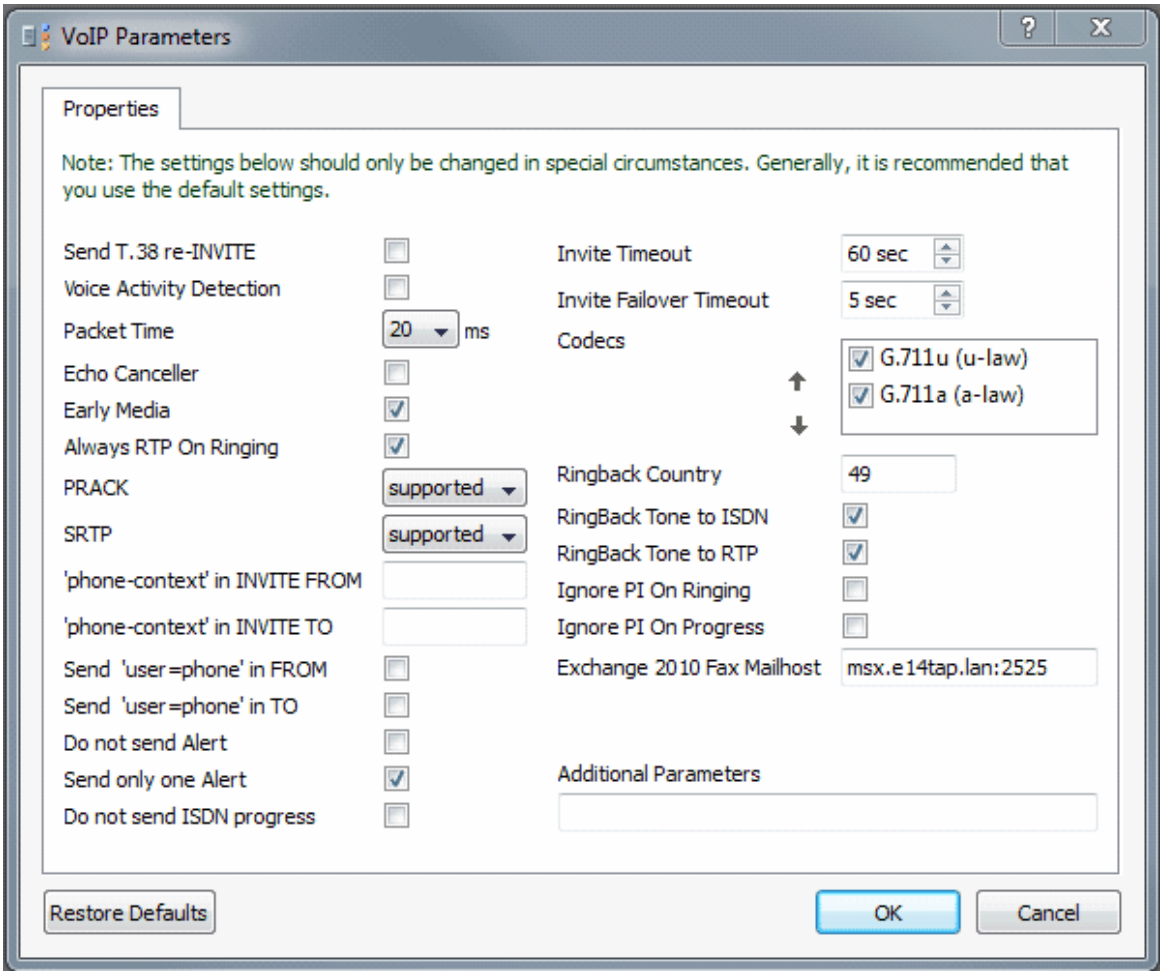

Image 3.55: Setting Exchange Mail-host in OfficeMaster Gate

When using a secured dial plan, OfficeMaster Gate has to be prepared for the use of TLS. For this, a certificate has to be requested and installed. Besides that, the certificate of the certification office has to be loaded in as well. This is done under Edit > Certificate... .

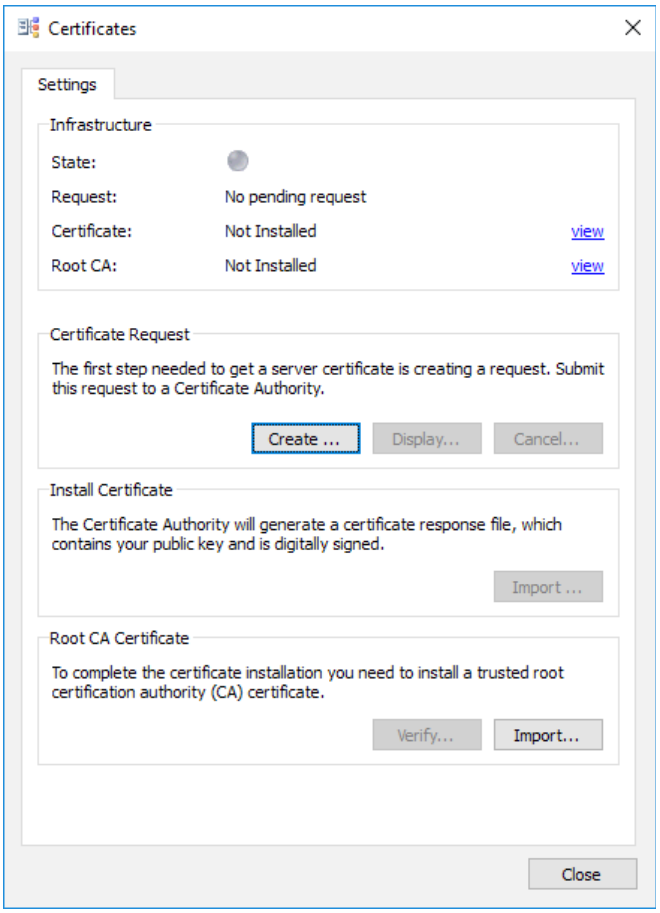

Image 3.56: Inserting certificate in OfficeMaster Gate

Exchange Fax in full functionality with OfficeMaster for Exchange

The solution introduced here will only support the receiving of fax messages, which for many users, especially in Europe, will not be enough. Many companies still send fax messages as an integral part of business communication.

From 1990 on, starting with MS-DOS and Windows 2.11 as well as MS-Mail and MS Exchange 4.0, Ferrari electronic AG has been a provider of fax solutions.

„OfficeMaster for Exchange“ is one of the leading products and supports Exchange 2000, 2003, 2007 and 2010. It includes a long range of functions and can be incorporated into all major applications (CRM, ERP, DMS, etc.) Detailed information can be found under http://www.officemaster.de

3.5. Drop & Insert – OfficeMaster Gate between Trunk and PBX

Base scenario: When migrating to Microsoft Skype for Business/ Lync, the previous PBX is often used parallel to the new Lync environment. This can be realized in two ways:

1. The Gateway is set up behind the PBX - for this, additional ISDN ports as well as changes to the PBX are required.

2. Installation of the Gateway between the Trunk and the PBX („Drop & Insert“) - no changes need to be made on the PBX. Also enables the automatic distribution of incoming calls to Lync resp. PBX (requires additional Windows Software to automatically recognize migrated users).

In order to enable communication between all users, six different paths need to be configured.

3.5.1. Inbound routing

Trunk > OMG > PBX, Connection to the Trunk

An interface of OfficeMaster Gate is connected with the Trunk. This Interface has to be run in *TE mode*. These are the standard settings for ISDN interfaces with OfficeMaster Gate.

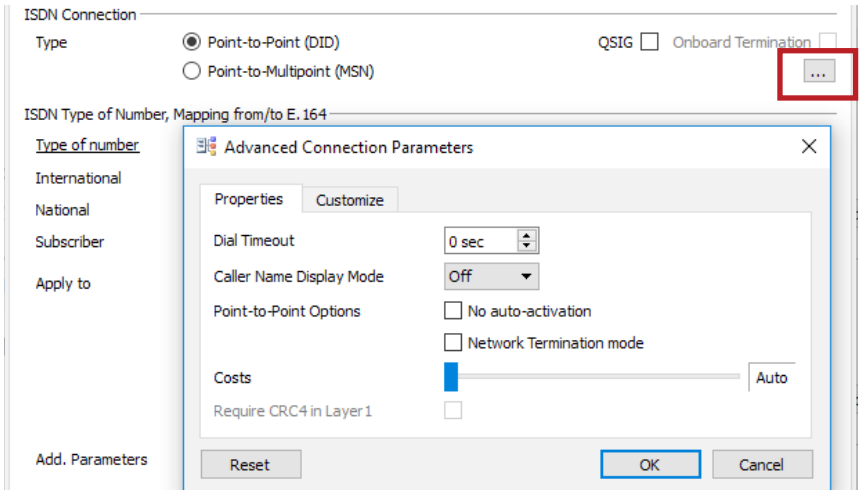

Image 3.57: Running the interface to the Trunk in TE mode

The rule set has to re-route all incoming calls from the Trunk, respectively all calls incoming on this interface, back to ISDN. For this, a new rule for incoming calls (*Calls from ISDN*) is created with the target ISDN:

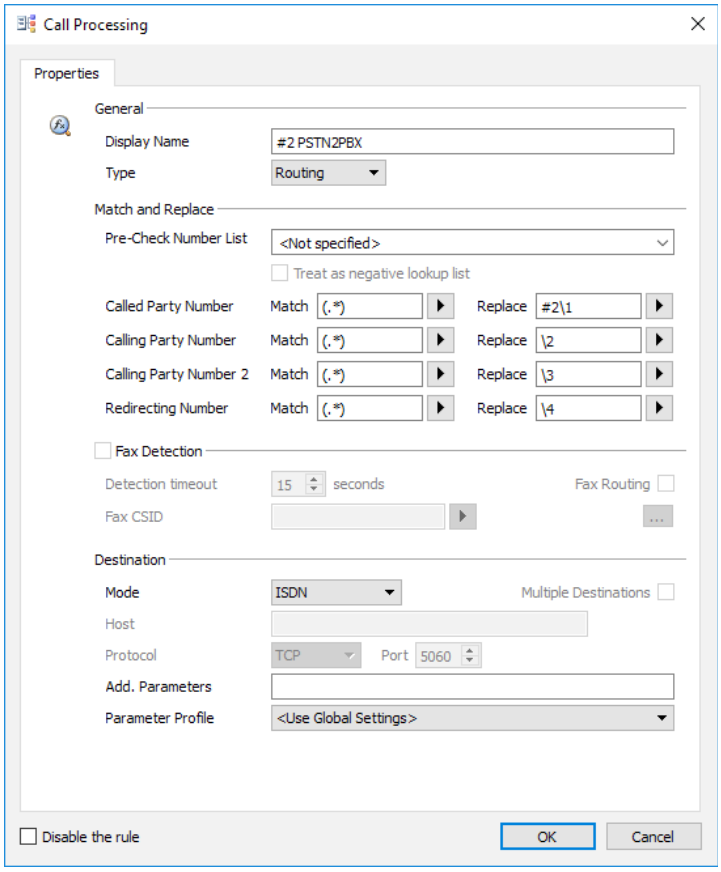

Image 3.58: Routing Trunk to ISDN

The calls are in most cases supposed to be issued to a defined interface. It is therefore advisable to name the routing rules in relation to their function. In any case it is needed to use a unique combination of characters in front of the call number under *Replace* so that calls can be identified properly.

Linking to the PBX

For the second interface to be connected to the PBX properly, usually a cross ISDN cable as well as the NT mode are needed.

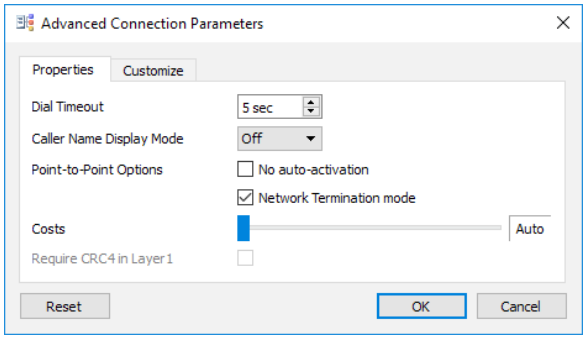

Image 3.59: Advanced Connection Parameters

Additionally, a timeout has to be set for outbound calls from the PBX to the Trunk.

After the interface has been configured, a rule has to be created that receives re-routed calls from the Trunk and routes them to the PBX. For this, a new rule has to be created under *Calls to ISDN*. The Prefix added in the first interface is needed for recognition. Before routing to the PBX, it has to be removed.

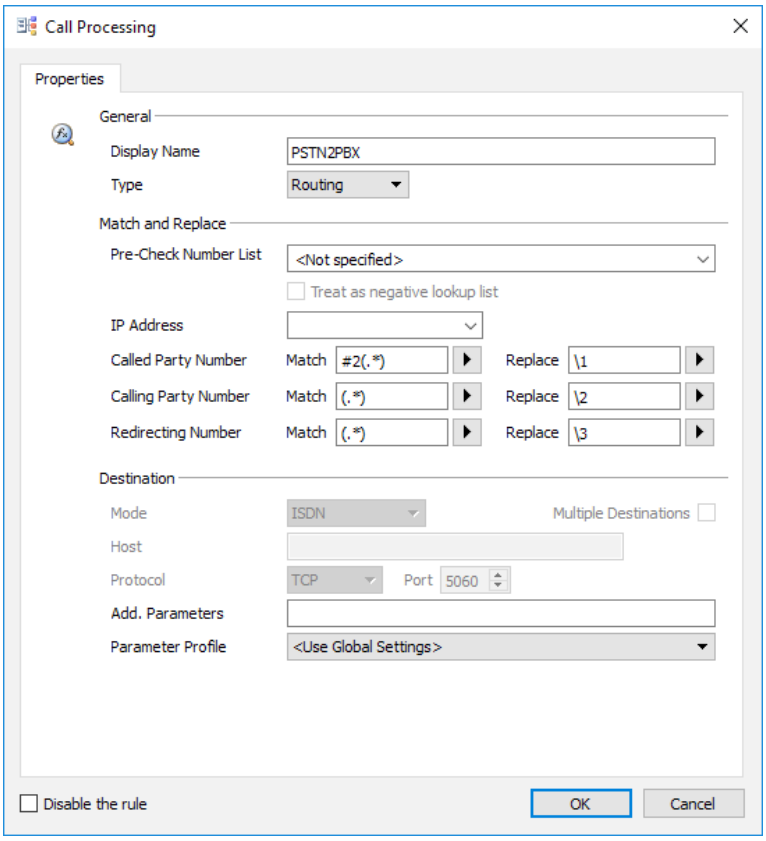

Image 3.60: Receiving calls from the first interface, removing prefix and routing to the PBX

Result

After those settings have been made, all calls from the Trunk are forwarded via OfficeMaster Gate to the PBX.

3.6. Outbound routing

PBX > OfficeMaster Gate > Trunk

The two interfaces are already configured via the steps in section 3.5.1 Seite 69. Now the required rules have to be created.

Linking to the PBX

Under *Calls from ISDN* rules need to be created for calls that are to be taken by the PBX. For this, a new rule has to be created with the target *ISDN*.

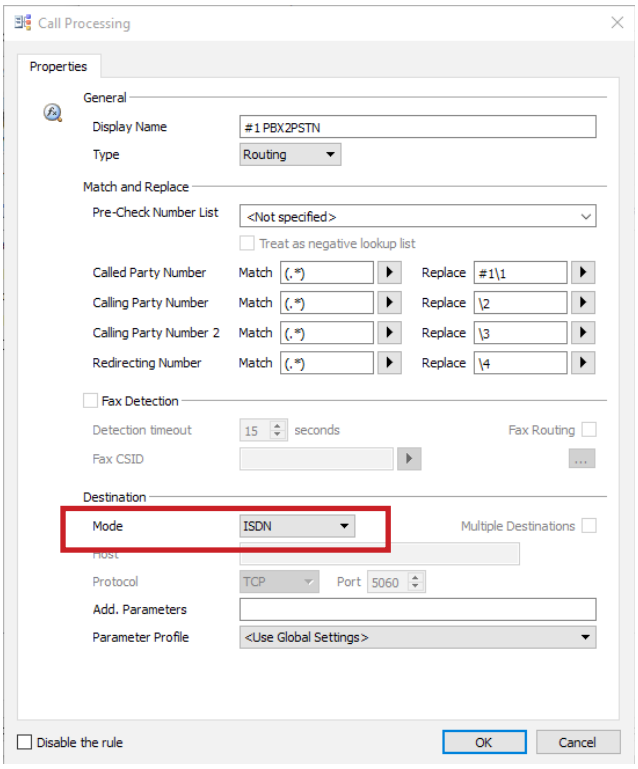

Image 3.61: Routing PBX to ISDN

Linking to the Trunk

Here the interface for the trunk is selected and a rule for *Calls to ISDN* is created. The previously added prefix has to be removed.

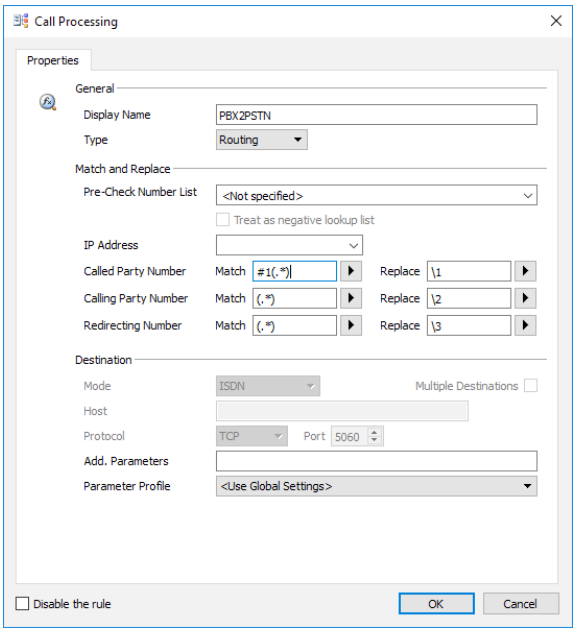

Image 3.62: Receiving calls from the interface, removing the prefix and routing to the trunk

4. ADVANCED CONFIGURATION

SIP Trunk access

VoIP parameter

User manual for administrators | Ferrari electronic AG

Ferrari electronic

4. Advanced Configuration

4.1. Sign in at a SIP-Trunk

OfficeMaster Gate can alternatively or additionally to the ISDN connection be connected to a SIP-Trunk.

Edit > SIP Trunk Registration opens the login dialog.

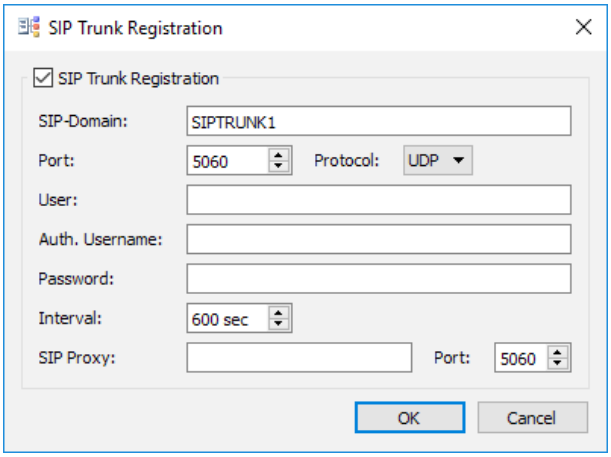

Image 4.1: SIP-Trunk login

► SIP Trunk Registration

If this box checked, OfficeMaster Gate will attempt to sign in at the defined SIP-Trunk.

► Host

Enter the IP or Host name provided by the provider.

► Port/Protocol

This information is also available from the provider or network administrator.

► User/Password

Username and password to sign in with the provider.

► Interval

Set the interval in which REGISTER messages are send to the provider.

Table 4.1: List of supported SIP-Trunks[1]

QSC	certified, including Fax
Telekom	tested and approved
IP Austria	tested, including Fax
Vodafone	tested, including Fax
SIPGate	being tested
BT	being tested

4.2. Registering SIP devices

Telephones and other devices can use SIP to register on the OfficeMaster Gate and initiate or take calls. However, as OfficeMaster Gate is no PBX, the device administration can only be carried out on a limited basis.

Click Edit-> SIP device registration to edit basic settings for the respective SIP devices.

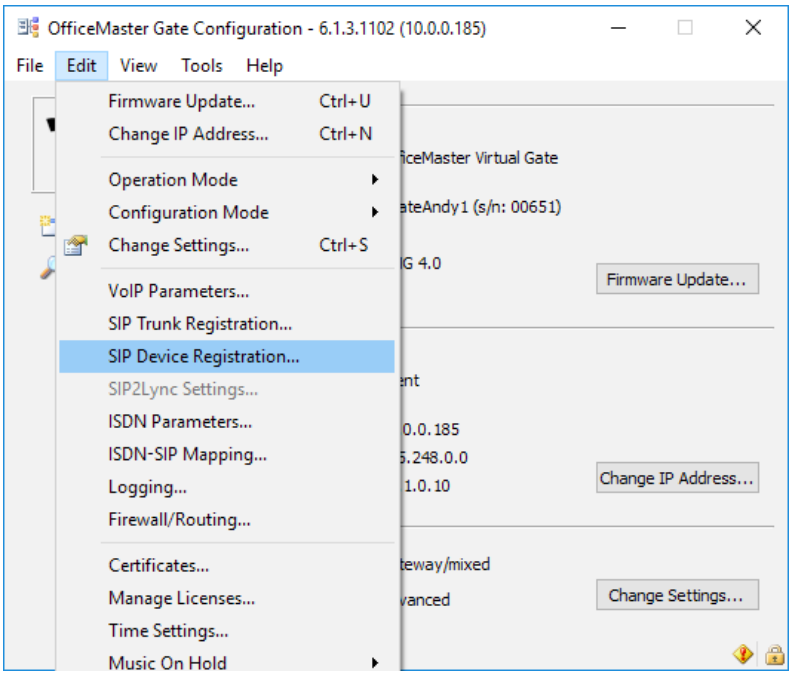

Image 4.2: SIP device registration

Note! We endeavour to enhance the list of supported SIP trunks constantly. The SIP devices shown here those available as of April 2017.

You can choose between various registration settings in the subsequent dialogue.

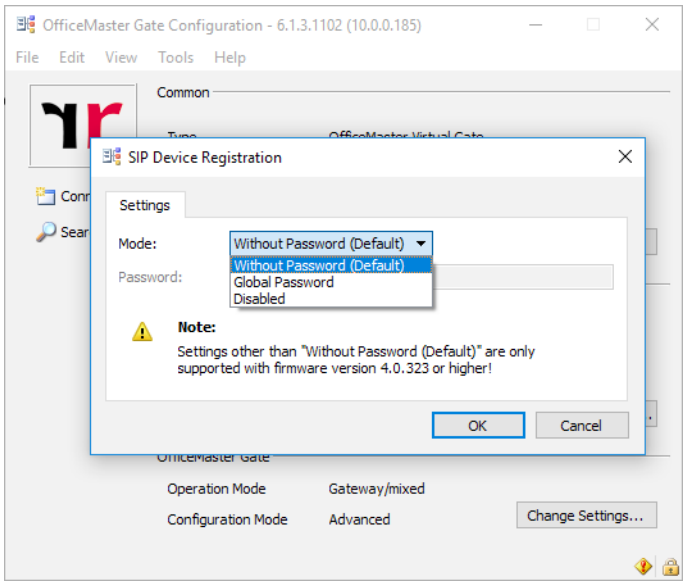

Image 4.3: Possible settings for SIP device registration

- Without password (Default)

  Any devices can register without the necessity of entering a password.

- Global password

  The password entered here affects all SIP registrations to the OfficeMaster Gate.

- Disabled

  OfficeMaster Gate won't allow any registrations.

4.3. Settings for OfficeMaster SIP2Lync

These functions have to be activated if OfficeMaster SIP2Lync is to be used with OfficeMaster Gate. Licensing in this case is done by the OfficeMaster Gate. Edit > SIP2Lync Settings is therefore only available after the correct extension license has been integrated into OfficeMaster Gate.

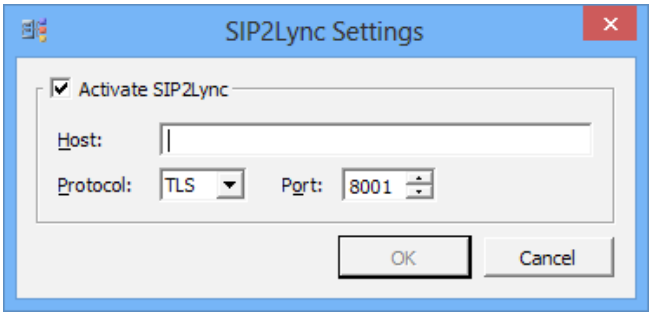

Image 4.4: Activating SIP2Lync

► Activate SIP2Lync

By selecting this option, OfficeMaster SIP2Lync can be run with the OfficeMaster Gate in use.

► Host

Enter the IP or Host name of the server on which the OfficeMaster SIP2Lync Service was installed.

► Port/Protocol

Communications port and decision between UDP/TCP

4.4. VoIP Parameter

Edit > VoIP-Parameter allows more detailed settings for the voice processing in the IP network.

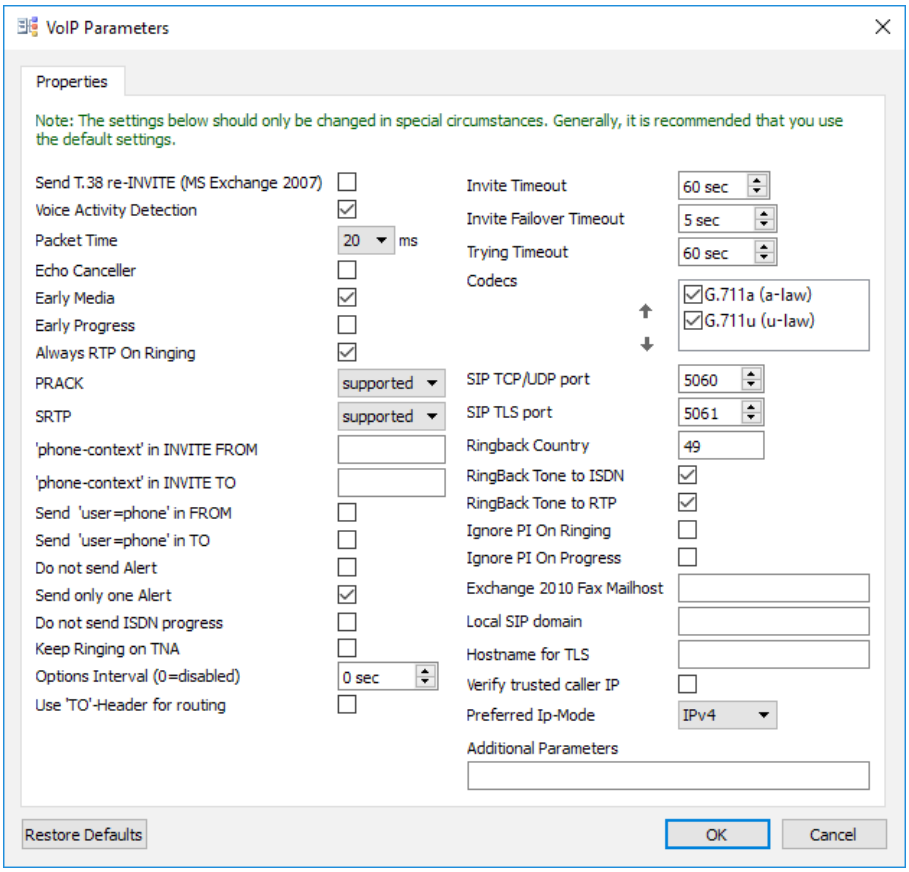

Image 4.5: VoIP Parameter settings

Note! This option should usually be left unaltered. Some of the options are not operative in older versions of the firmware.

▶ Left column

▶ Send T.38 re-INVITE

Activating this option will lead to OfficeMaster Gate initiating the switch to T.38 fax receive. Otherwise this is handled via the Exchange UM server.

▶ Voice Activity Detection (VAD)

is the option to stop the transmission of voice data during pauses in the conversation in order to save bandwidth („Silence Suppression"). This can also help to avoid echo in certain situations. More on the topic of echo can be found under in „Appendix B: Echo Canceling" auf Seite iii.

▶ Packet Time

The Packet Time of 20 milliseconds is standard. A change to the Packet Time has no advantages.

▶ Echo Canceler

The Echo Canceler can in certain situations reduce echo. More on the topic of echo can be found under „Appendix B: Echo Canceling" auf Seite iii.

▶ Early Media

Early Media activates the connect through of the voice channel before the connection is completely established in order to make dialing tones and messages audible. We recommend to activate this.

▶ Early Progress

If Early Progress activated, outbound calls coming from Lync will via a PROGRESS message with SDP in all cases establish an internal voice connection (RTP) before the call is passed over to the ISDN. Improves the behavior of Early Media in order to prevent clipping. Should be activated.

▶ Always RTP On Ringing

Establishes the RTP connection even when no in-band information is signaled in ISDN.

▶ PRACK

Via this element, the confirmation of provisional messages can be activated. It has to be set to *supported / required* in combination with Microsoft counterparts.

▶ SRTP

Controls voice encryption (***disabled, supported, required***). We recommend to set it to *supported*. In that case the encryption is used in cases that the counterpart supports it as well.

▶ 'phone-context' in INVITE FROM/TO

The SIP-Header of an ***INVITE*** contains in ***FROM*** respectively ***TO*** a phone context with the here entered information. The entry user in the description field results in the SIP-Header in the appendix phone-context=user. Not commonly used.

▶ Send 'user=phone' in FROM/TO

User=phone is included in the INVITE of SIP-URIs when this box is checked.

▶ Do not send Alert

Is this option activated, no ***SIP ALERT*** messages are send.

▶ Send only one Alert

Only sends ***ALERTING*** once into ***ISDN*** even if SIP recognizes ***RINGING*** multiple times.

▶ Do not send ISDN progress

For inbound calls Lync receives a ***PROGRESS*** message while a connection is established, which then results in a ***PROGRESS*** message in ISDN. Some PBXs react to this with an error - in those cases this option should be activated.

▶ Keep Ringing on TNA

With common PBXs, devices also ring for inbound calls when the user is not present. If Lync used without a voice mail system and the user is not logged in on any client, the caller will relatively quickly receive a f***ast busy*** notice. Is this option activated, the behavior of a PBX will be simulated.

▶ Options Interval

If this value is unequal to 0, the gateway will regularly send a ***SIP OPTIONS*** request to all configured destinations to check if the counterpart is available. Does not yield any advantages in regular use and therefore can be left at 0 (=inactive).

▶ Right column

▶ Invite Timeout

Sets the time that is waited for a response after an INVITE.

▶ Invite Failover Timeout

This time setting defines the time it takes to switch to an alternate target should the first server not respond. This only applies when multiple targets or DNS load balancing are used.

▶ Trying Timeout

Sets the time that is waited for additional messages after receiving ***TRYING***.

▶ Codecs

Defines with which priority which Codecs are used. At least a-law should be activated in Europe.

▶ SIP TCP/UDP port

On this port the SIP-Stack expects inbound packages via UDP and TCP. More information can be found in section Connection via TCP/RTP.

▶ SIP TLS port

Port for incoming TLS packages, default is set to ***5061***. If Lync Server used, this port has to be set accordingly in the topology for the gateway.

▶ RingBack Country

The country code chooses the country specific ring back tone. Common values: 1 (USA), 44 (UK), 49 (Germany and other countries). The country code also directs the properties of the analog interface on the PCIe-FXS card.

▶ RingBack Tone to ISDN

Internally created ring tone is send to ISDN participants.

▶ RingBack Tone to RTP

Internally created ring tone is send to VoIP participants.

▶ Ignore PI on Ringing

Suppresses the evaluation of the „Progress Indicator Information Element“ in the SIP message RINGING and the ISDN message ALERTING. Only needed for specific test cases.

▶ Ignore PI on Progress

Suppresses the evaluation of the ***Progress Indicator Information Element*** in the ISDN/SIP message PROGRESS. Only needed for specific test cases.

▶ Exchange 2010 Fax Mail host

Address and port, when fax is processed via Exchange 2010. More information can be found under Fax rececption with Microsoft Exchange 2010.

► Local SIP domain

A value set here will be used as SIP-Domain for SIP messages. Usually not needed.

► Host name for TLS

Enter the name of the OfficeMaster Gate used in the creation of the certificate.

► Verify trusted caller IP

If this box is checked, only SIP messages from known counterparts are accepted (that also appear as destinations in the rules).

► Preferred IP-Mode

Select which network protocol is preferred by OfficeMaster Gate.

► Additional Parameters

If requested by the Ferrari electronic support, additional parameters can be set here.

Note! *Restore to defaults* will reverse all changes.

4.5. ISDN Parameter

Edit > ISDN-Parameters enables the editing of further details for ISDN

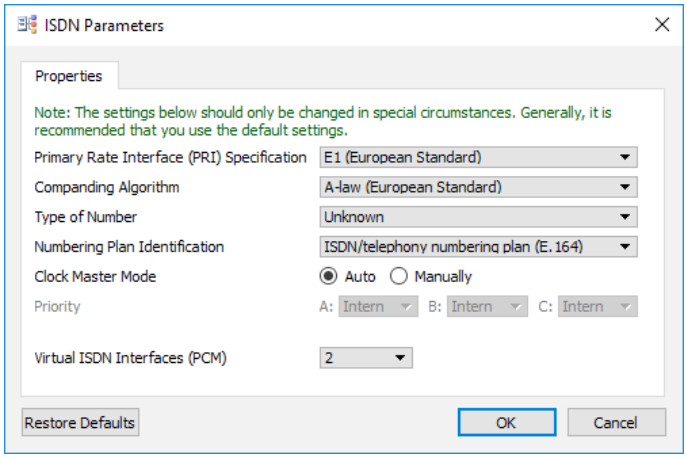

Image 4.6: Global ISDN settings

► PRI Specification

For use in the USA select T1 (23 usable channels), otherwise leave it at E1 (30 B-channels).

► Companding Algorithm

Use u-Law in combination with T1, otherwise use a-Law.

► Type of Number

Defines how Called Party Numbers are qualified if not defined differently by the setting of rules.

► Numbering Plan Identification

Defines the numbering plan for Called Party Numbers.

► Clock Master Mode

Set to ***Auto***, the hardware will independently select the proper clock source. Set to ***manually*** will let the user select the priority.

Other options like the Network Termination Mode can be found in the advanced mode of the section ISDN settings.

Type of Number / Numbering Plan Identification

It can occasionally be useful to set the parameter for TON and NPI differently to the global default. For that, a specific string needs to be added to the respective telephone number, additional to the phone number, This string is constructed as follows:

- for the calling party number: <nx:oy>
- for the called party number: <Mx:Oy>

x is the value of TON, while y is the value of NPI in accordance with the following table.

Table 4.2: Individual values for Type of Number/Numbering Plan Identification in the set of rules

1	Unknown	Unknown
2	International number	ISDN/telephony
3	National number	
4	Network specific number	Data numbering plan
5	Subscriber number	Telex numbering plan
7	Abbreviated number	
9		National standard numbering plan
10		Private numbering plan

(individual classification of the calling party number for outbound calls)

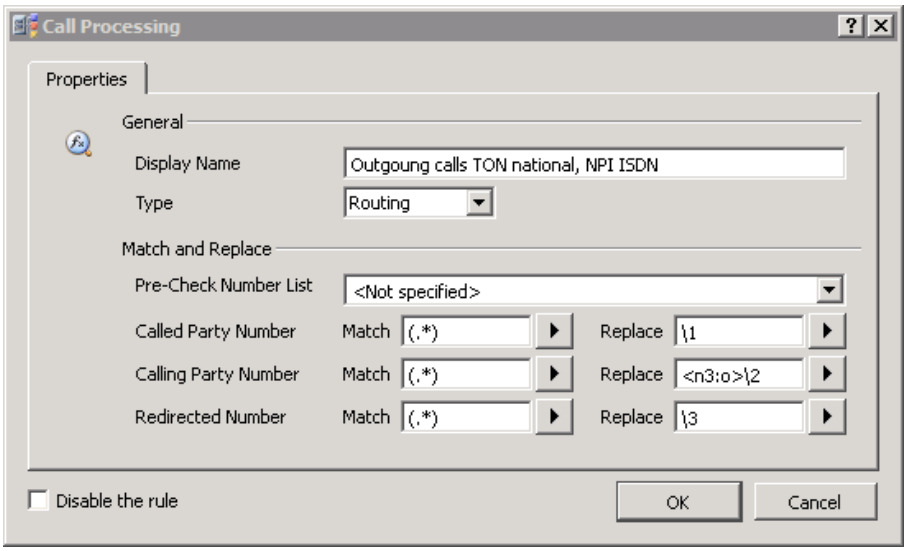

Image 4.7: TON/NPI individual per rule

This rule delivers the calling party number as TON:National number, NPI:ISDN/telephony.

4.6. ISDN-SIP Mapping

OfficeMaster Gate as a Mediagateway establishes a connection between two different signaling protocols (SIP resp. ISDN Q.931). At both ends different events and statuses can be registered through status and error codes.

SIP deals with so called Response-Codes while ISDN works with Causes.

Edit > ISDN – SIP Mapping... enables the editing of which codes belong to which side. Usually not needed.

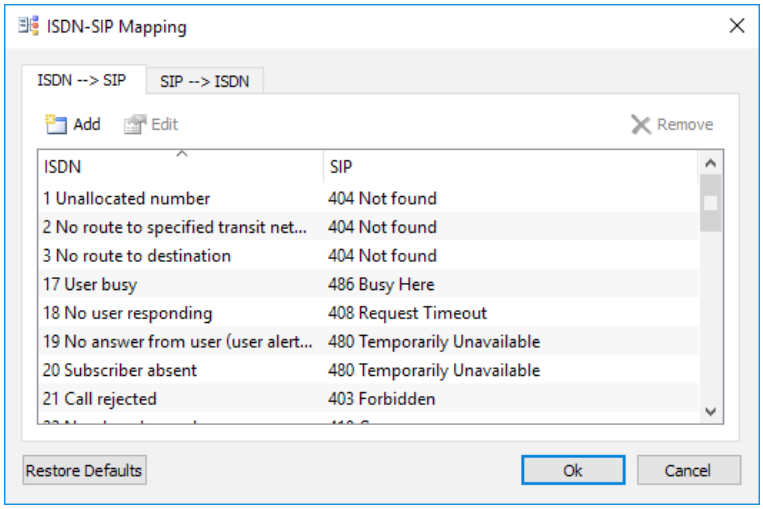

Image 4.8: ISDN/SIP Mapping

Restore Defaults reverts all changes.

4.7. Music on hold

When used as telephony gateway, a music on hold can be integrated. Are no changes made, the default melody will be used.

Music that is to be integrated has to be in the following uncompressed format:

- Mono, 8000Hz, a-Law

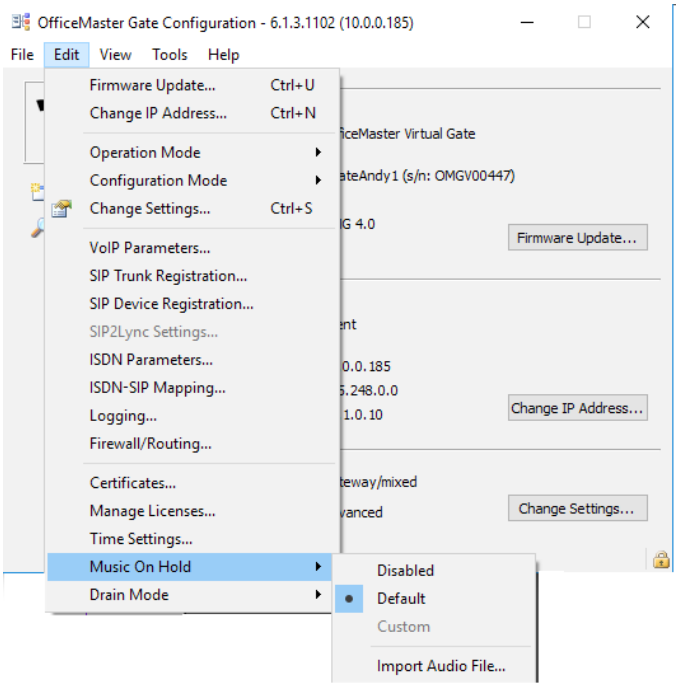

Image 4.9: Integrating music on hold

Note! Additional information can be found in the forum of Ferrari electronic AG.

5. APPENDIX

List of abbreviations

Echo canceling

Basics on telephony numbers

User manual for administrators | Ferrari electronic AG

Copyright © 2017 Ferrari electronic AG

Appendix A: Telephone number basics

In the following the general functionalities of call routing are described, followed by a short introduction into the regular expressions used in the Syntax. The description of the configuration dialog is followed by examples of use and hints.

A.1. Rule based treatment of inbound calls

The treatment of inbound calls in OfficeMaster Gate is handled via adjustable regular expressions. These regular expressions are filed in tabular format and can be analyzed regarding the run time with the help of an interpreter. This presentation at first will appear complicated to an inexperienced administrator. In time and with the help of the provided examples this should however turn into a highly flexible tool. For every inbound call the following information is processed.

- Called Party Number (CPN)

  The CPN is the number the caller dialed, respectively the part of the number that is received by the ISDN port.

- Calling Party Number (CGN1) and Calling2 Party Number (CGN2)

  CGN1 and CGN2 include the telephone numbers of the caller. In most cases there will only be one Calling Party Number, the second element then remains empty. The first element can also be empty if the caller does not submit a number at all. CGN1 and CGN2 are for example used together when receiving land line SMS. In this case, CGN1 is the telephone number of the sender while the CGN2 is the telephone number of the SMS center. The analysis of the number included in the CGN2 enables the software to recognize that the call serves the transmission of a SMS.

- Redirecting Number (RN)

  The RN includes the telephone number that was originally dialed by the caller, for which a redirect had been set up.

Example A.1 From a mobile phone with the telephone number 01520189524 the internal telephone number 947 (dial through of the participant) is dialed; this participant has programmed a call forwarding to the Pilot-ID 999 of the voice mail system. The above described errors supply the values listed in the following table.

Table A.1: Description of the Example

CPN	Called Party Number (CPN) is 999 because of call forwarding.
CGN1	Calling Party Number (CGN1) is the number of the mobile phone
CGN2	usually empty
RN	Redirecting Number (RN) is 947, meaning the originally called but fowarded number with which the voice mail system recognizes to which user the call is assigned

»**End of example**

Rules have to be defined on how OfficeMaster Gate is to deal with different types of calls, for example forwarded calls that go directly towards the voice box. For this it is also important how the ISDN port of the PBX on which OfficeMaster Gate is run is configured. S2M connections are in all cases able point-to-point ports with the ability to execute dial through. S0 ports (BRI) have to be divided into point-to-point and multi device ports with MSN (Multiple Subscriber Number).

A.2. Regular expressions

Regular expressions, as common in telephony, are used for the recognition and handling of telephone numbers.

Regular expressions create patterns in form of characters (letters, digits) as well as symbols (special characters with special meaning). In order to for example describe all telephone numbers beginning with 1234 followed by three additional spaces, the expression 1234... is used. The dot resembles any character. Parts of such a pattern can be framed in round brackets. The content of the brackets can be referenced in future replacements - this is done by using \n, whereby n defines, which brackets are referenced (1...m). Is a special character to be used as a normal character, a backslash ("\") has to be used as a prefix for this special character.

Example A.2

Lync internally uses E.164 numbers like +493328455854. In order to recognize this number in a pattern (and after that to extract the dial through of the user) the pattern \+493328455(...) has to be set. The replacement \1 accesses the content of the bracket and provides the sender extension number 854. The plus sign has a special meaning in regular expressions (1-n times repetition of the previous character) and therefore needs to be written with a backslash for when it is to be recognized as a normal character. Backslash in this case functions as a so called escape character.

»**End of example**

Example A.3

For the Called Party Number the pattern 1234(...) is entered which, like in the example, matches all numbers that start with 1234 and continue with three more characters.

For a trunk connection the 1234 would for example be the base number followed by the three character extension. To insert this extension into the field for Redirecting Number, the bracket content is referenced with \1. The 1 refers to the first pair of brackets; are multiple brackets used they are referred to with consecutive numbers.

Areas can be specified instead of digits as well. The expression 1234[1-3] for example refers to all five character numbers that start with 1234 and have the digits one, two or three as a fifth character. The expression in the squared brackets represents exactly one character and is treated as a list. This can be defined as an area or as a list. [124-68-9] for example matches the digits 1,2,4,5,6,8,9.

A star (*) signifies that the previous character can appear any number of times; the expression .* is used very often - the expression means that any arbitrary number can appear any number of times. With (xyz)* the whole expression can be quantified. xyz can in turn stand for either characters or symbols. (12.)* means, that the sequence starting with 12 and any arbitrary number as a third character can occur any number of times.

In order to accept multiple possible strings like for example MSNs, vertical lines have to be used; the pattern (12|13|14) means that either 12, 13 or 14 are accepted.

»End of example

In the advanced configuration, rules for CPN, CGN1, CGN2 and RN are defined that are tested in the defined order of the rule until all four patterns match. The in the rule defined replacement pattern is then applied and the call accepted. With every further incoming digit the set of rules is worked through until a match has been found or the inbound call has been ended.

Example A.4

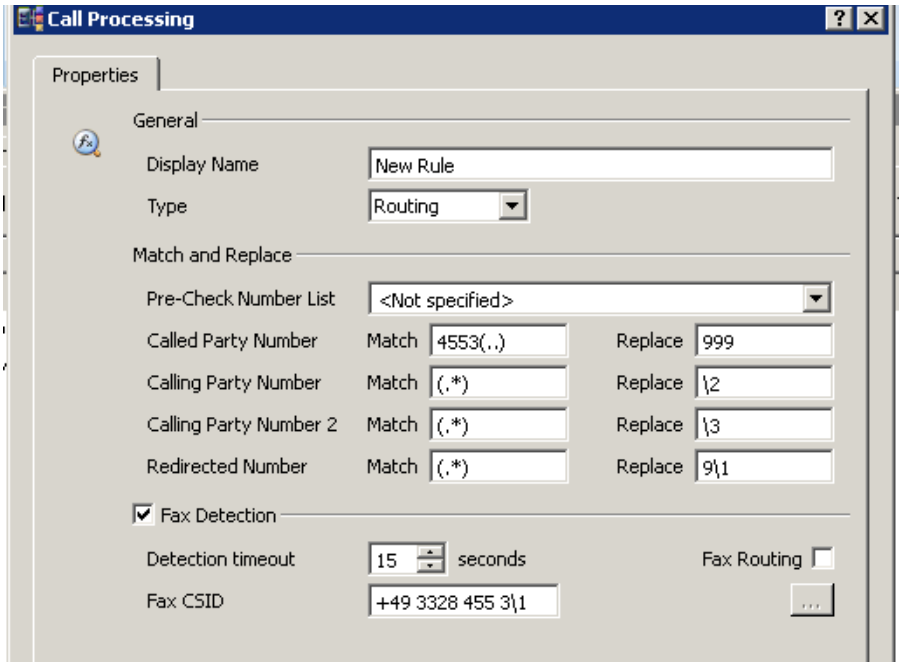

Image A.1: Working with basic regular expressions

This image shows a rule that matches all numbers that start with 4553 followed by two characters; the areas CGN1, CGN2 and RN can be arbitrary, even empty. There are four brackets whose content can be referred to with \1 through \4. After the replacement the CPN receives the 999 (for example a Pilot-ID), CGN1 and CGN2 remain unchanged as they with \2 and \3 are replaced with their original content. The Redirecting Number (RN) now contains a three digit number that starts with 9 and then contains the last two characters of the original Called Party Number. The originally dialed telephone number 455347 then for example changes into the redirecting number 947 which resembles the device number of the participant as well as his EUM address in Exchange 2007/2010). Should during the connection a fax receive be recognized and executed, the sender will receive the entire CSID (Called Subscriber Identification) +49 3328 455 347 including the user's extension number.

»End of example

A.3. Configuration examples

The diverse configuration and application possibilities of OfficeMaster Gate are best explained with practical examples. Aside from standard applications more complex cases are also explained.

Inbound calls multi device connection

PBXs inwards often only provide a multi device connection that is designed for the use of ISDN devices, phones in particular. In most cases 1-10 telephone numbers are supported, in rare cases more than that. This restriction is significant for the Office Communications Server 2007 as it means that the number of telephone participants that are directly reachable from the outside is limited. Exchange 2007 UM can be used in the by Microsoft planed way (use of a Pilot-ID) as this only requires one number.

Example A.5

Table A.2: Exchange 2007/2010 UM on multi device connection

Called Party Number	(100)	\1
Calling Party Number	(.*)	\2
Calling2 Party Number	(.*)	\3
Redirecting Number	(.*)	\4
Fax identifier	+49 30 12345 \4	
Destination	SIP: 10.2.3.4	

This rule causes:

- all calls on the ISDN-Bus are forwarded to the number 100 in Exchange (IP address 10.2.3.4).
- other devices on the same Bus can be targeted via additional numbers (MSNs)
- redirected calls transmit the originally dialed extension via SIP to Exchange so that the respective mail box will answer directly.
- Is a fax receive recognized and executed during the connection, the sender receives the entire CSID (Called Subscriber Number) including the user's extension number.

Additional rules are not needed for this specific case. The configuration can be carried out in basic mode.

»End of example

Inbound calls DID Trunk

More flexibility and applicability is gained through the ability of the connection to handle extensions. This includes:

- Introduction of separate fax extensions for Exchange users (without additional EUM address) by prefixing a digit to the extension or by shifting the range of numbers (example below).

- Addressing of different destinations (multiple Exchange UM Server, Lync Server or OfficeMaster Messaging Server) depending on the dialed extension.
- Correction of telephone numbers, for example clipping of all information except for the extension (for example +49(30)1234947 turns into 947) or completion of the extension to a canonical data representation (for example 947 turns into +49(30)1234947).
- Distribution of the calls by Calling Party Number.

Example A.6

In a company three character numbers between 700 and 999 are used for telephony. These are cultivated as EUM addresses in Exchange. For the direct accessibility via fax in Exchange, the prefix 6 is to be added for the telephone extension, meaning that the participant with the device number 845 has the fax extension 6845. The Pilot-ID is 100.

»End of example

Table A.3: Set of rule for „example B.6“

Called Party Number	6(...)	100
Calling Party Number	(.*)	\2
Calling2 Party Number	(.*)	\3
Redirecting Number	(.*)	\1
Fax Recognition	+49 30 1234 6 \1	
Destination	SIP: 10.2.3.4	

Example A.7

For telephony four character numbers between 9000 and 9999 are used. These are cultivated as EUM addresses in Exchange. For the direct accessibility via fax in Exchange, the range of numbers 8000 through 8999 is to be used, whereby telephone and fax extensions are only different in the first character. The participant with the device number 9451 then has the fax extension 8451. Pilot-ID is 7000.

»End of example

Table A.4: Exchange 2007 UM fax extension in separate area

Called Party Number	8(...)	7000
Calling Party Number	(.*)	\2
Calling2 Party Number	(.*)	\3
Redirecting Number	(.*)	9\1
Fax Recognition	+49 30 1234 8 \1	

By defining a number of sequential rules, many different ranges can be processed separately. However, it is important to remember that the rules will be checked in the predefined sequence until a rule is found that matches the specifications (“first match” principle). The order of the rules therefore might have to be changed in order to ensure the desired processing.

Example A.8

Five digit extension that start with 61 are to be directed to the OfficeMaster Messaging Server. All other numbers beginning with 6 are to be directed to the Exchange Server. The rule 61(...) therefore has to be placed before the rule 6(.....) as it would otherwise never be processed because the other rule would match before that.

»End of example

In the following examples rules are displayed in compact form in order to show the interconnection between rules. One rule is displayed in three columns:

```
Pattern                  Replacement       Destination
```

whereby Pattern and Replacement incorporates the four individual boxes (Called Party Number, Calling Party Number, Calling2 Party Number and Redirecting Number) separated by commas.

Example A.9

The rule Exchange 2007 fax extension in a separate area in the earlier example would look as follows:

```
8(...),(.*),(.*),(.*)    7000,\2,\3,9\1          SIP: 10.2.3.4
```

The adjustable fax identifier is left out in this representation. In front of every rule the display name is shown in a separate row.

»End of example

Example A.10 (complex case)

OfficeMaster Gate is connected to the PBX via a cross-connection. The PBX transmits all calls to this connection that start with the digit 3. Exchange 2007 UM is reachable via the Pilot-ID 999. Telephone numbers are in the range from 100 through 299. Exchange 2007 is only to be used for voice mail and Outlook Voice Access, fax and SMS are handled by OfficeMaster for Exchange. Voice mail boxes can be called directly when the device number is complemented by the number 30.

In order to reach users via fax, 31 is used as an extension. For SMS the 32 is used. The numbers are transmitted complete in form of 3XXXX to OfficeMaster. Additionally, an Office Communications Server 2007 is being tested. The users there receive the number 33XXX, whereby XXX resembles their device number. The 33 is not to be transmitted to the Office Communications Server for calls. The Exchange 2007 switchboard, that internally in Exchange has the number 998, is to be reached via 34000. Calls to invalid numbering ranges (34001 through 39999) are redirected to the central voice box with the number 100 where an according message is deposited.

Table A.5: The complete list of rules:

30(...),(.*),(.*),(.*)	999,\2,\3,\1	SIP: 10.2.3.4
(3[1-2]...),(.*),(.*),(.*)	\1,\2,\3,\4	OfficeMaster
33(...),(.*),(.*),(.*)	\1,\2,\3,\4	SIP: 10.2.3.5
34(000),(.*),(.*),(.*)	998,\2,\3,\4	SIP: 10.2.3.4
3(....),(.*),(.*),(.*)	999,\2,\3,100	SIP: 10.2.3.4

By adding additional rules, special treatment for specific numbers respectively numbering ranges can be realized.

»**End of example**

Outbound calls

While for inbound calls at least one rule is needed, rules for outbound calls are optional. They server the transformation of call information.

Areas of appliance are for example:

- Rules for accessing an outside line
- Replacement of extensions by a central number
- Transformation from canonical data representation to dial-able numbers

Example A.11

In a company certain extension are not to be signaled outward. These numbers are 830, 846 and 852. For calls from these devices the extension 800 is to be transmitted instead. At the same time an accessing of an outside line (number 0) for national numbers is to be executed.

Table A.6: Individual outbound calls with central sender number

Called Party Number	(0\+49)(.*)	00\2
Calling Party Number	(830|846|852)	800
Redirecting Number	(.*)	\4

To realize the accessing of an outside line for all participants, an additional rule has to follow this one.

Table A.7: Remaining telephone numbers are signaled

Called Party Number	(0\+49)(.*)	00\2
Calling Party Number	(.*)	\3
Redirecting Number	(.*)	\4

It is important for both rules that the Called Party Number is in brackets. As brackets are numbered consecutively, the Calling Party Number is referenced with \3. A second Calling Party Number is non existent for outbound rules.

»**End of example**

Example A.12

All employees have mobile phone with numbers beginning with 01521 19582. Is one of those numbers dialed, the suppression of the extension is not to happen.

This means, that an additional rule has to precede the rule in the example above:

Table A.8: Defined mobile numbers see the correct sender telephone number

Called Party Number	(0\+49)(152119582.*)	00\2
Calling Party Number	(.*)	\3
Redirecting Number	(.*)	\4

»**End of example**