# SIP2LYNC

Version 1.1.0

## Installation & Configuration Guide

For Administrators only



Ferrari electronic

| | |
|---|---|
| Herausgeber | Ferrari electronic AG<br>Ruhlsdorfer Str. 138<br>14513 Teltow (bei Berlin)<br>www.ferrari-electronic.de |
| Phone | +49 3328 455 90 |
| Fax | +49 3328 455 960 |
| E-Mail | info@ferrari-electronic.de |
| Authors | Johann Deutinger<br>Nils Küchler<br>Chris Helbing |
| Editorial Team/Layout | Nils Küchler<br>Chris Helbing |
| Release | 2014/10/28, 1st edition |

Thank you for trusting in Ferrari electronic AG and your decision for OfficeMaster®. Ferrari electronic has been an established manufacturer of hardware and software for use in business-critical communications since the beginning of the 1990s. Our OfficeMaster products offer a variety of messaging services like Fax, SMS,and Voice for the use in every IT structure.

We hope that you are satisfied with our product and that it has fulfilled your requirements as best as possible. Should there be any questions or suggestions, please do not hesitate to contact us via email at:

info@ferrari-electronic.de

Teltow, Oktober 2014

# Table of Contents





Ferrari electronic

# 1. Introduction

## 1.1 Technical Overview

### Integrating non-system terminals into Microsoft Lync Server 2013

A prerequisite for a gateway to be certified as a full Lync Gateway is the support of analog terminals. Microsoft themselves solely communicate via a special version of SIP protocol, shifting all other technologies onto the Gateway manufacturers. Analog participants are created and assigned to a Gateway in the Lync Management Shell. With this, Lync is able to use policies, dial plans, normalizing rules and such even for those devices that do not represent a full Lync user with presence information.

In order to fully integrate external devices into Lync, an additional software has to be installed. With OfficeMaster SIP2Lync, Ferrari electronic provides a software solution that allows for the integration of external telephone sets, even if they themselves are not directly compatible with Lync. In particular, the often requested integration of DECT infrastructures is possible with this software. All the while, no difference to normal Lync terminals is noticeable to any of the participants. The devices ring together with the other instances registered for the user and update their status according to the status of the terminal.

OfficeMaster SIP2Lync works in combination with OfficeMaster Gate respectively OfficeMaster Gate UC and is licensed per individual gateway for specific numbers of users. Additionally, the extension SIP2SIP B2BUA (Back to Back User Agent) is required.

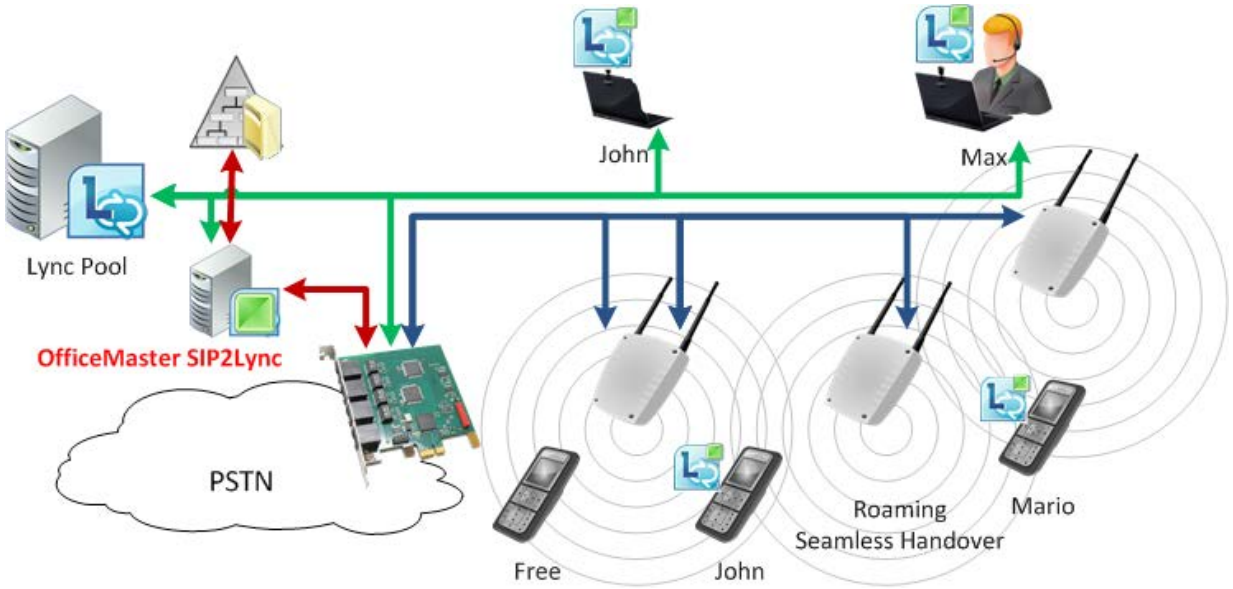


Image 1.1: System Overview

### SIP2SIP as prerequisite

While calls between SIP and ISDN can be directed via the Gateway in its standard function as a Media gateway, additional resources are needed for the Loop-back required for a connection between two SIP participants. This Loop-back is known as Back to Back User Agent (B2BUA) and is the basis for connecting external SIP devices to the Microsoft Lync Server.

The SIP B2BAU is licensed according to simultaneously used channels. A call of a Lync participant to a SIP participant not connected via Lync uses one channel.

## 1.2 Required Products and Licenses

An OfficeMaster Gate (or OfficeMaster SBA) with Firmware 4.150 or higher is required to use SIP2Lync. You may need some licensed interfaces (SIP or PRI/BRI) to interact with the PSTN or PBX. It is definitivly required to license SIP2Lync and SIP Channels to connect Lync with the Non-Lync-certified Devices.

# 2. Installation

This chapter documents the installation of SIP2Lync. The installation is controlled by a configuration tool and occurs almost fully automatically. Alternatively, manual installation is possible. Both options are described in the following.

## 2.1 Preparation

### System requirements

The installation takes place on a Windows Server 2008 R2 (SP1 optional) that is within the domain but not the domain controller.

### Software requirements

- .NET framework 3.51 (can be activated as a feature within server administration)
- .NET framework 4.0 (http://www.microsoft.com/download/en/details.aspx?id=17718)
- UCMA Runtime (http://www.microsoft.com/download/en/details.aspx?id=20958)

### Permissions

Local admin rights or more are required for the installation of the SIP2Lync components. Later on, a membership in the domain group RTCUniversalServerAdmins is required as well. It is therefore advisable to begin the installation process with an account that already meets both requirements.

### Installation of the SIP2Lync components

Start the installation via the OfficeMaster-SIP2Lync-Setup.exe. The following installation either occurs manually or automatically via the in SIP2Lync integrated assistant.

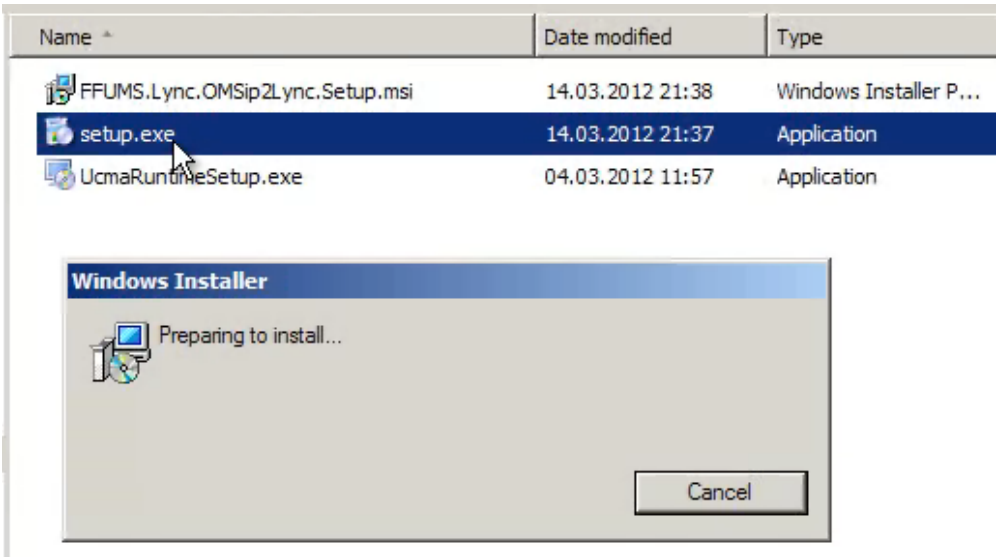


Image 2.1: Install SIP2Lync

## 2.2 Installation and Provisioning

First, the SIP2Lync Configurator has to be executed. Maximizing the window can improve visibility.

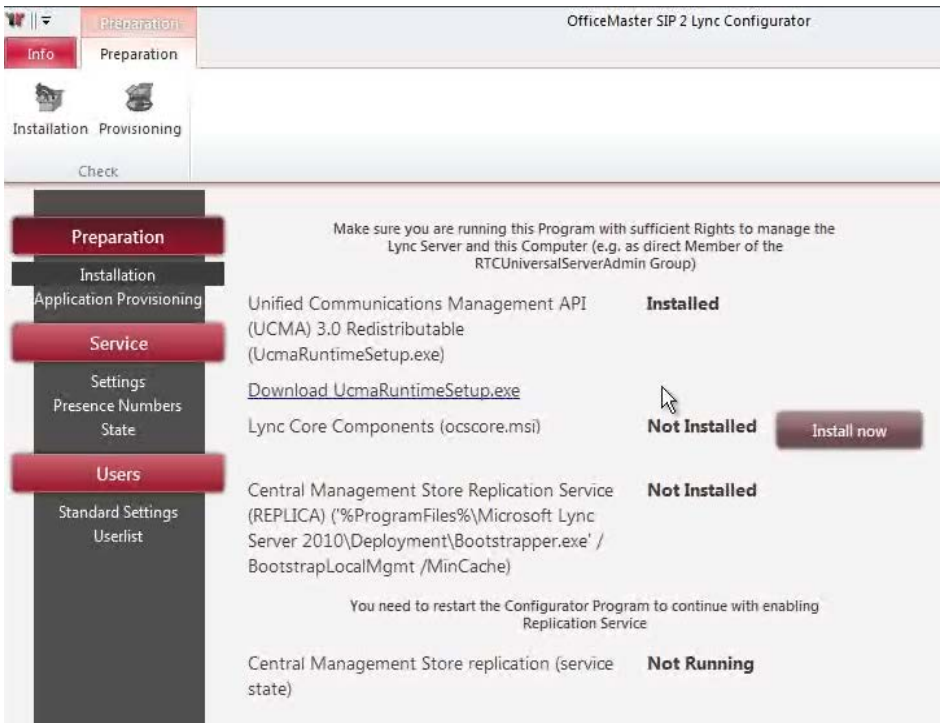


Image 2.2: Installation Dialog

This dialog will appear if Unified Communications Management API 3.0 has already been installed. Otherwise, an option will allow for the download and installation of UCMA 3.0. Install now installs the Lync Core Components.

This is followed by the installation of SQL Express together with a replication service.

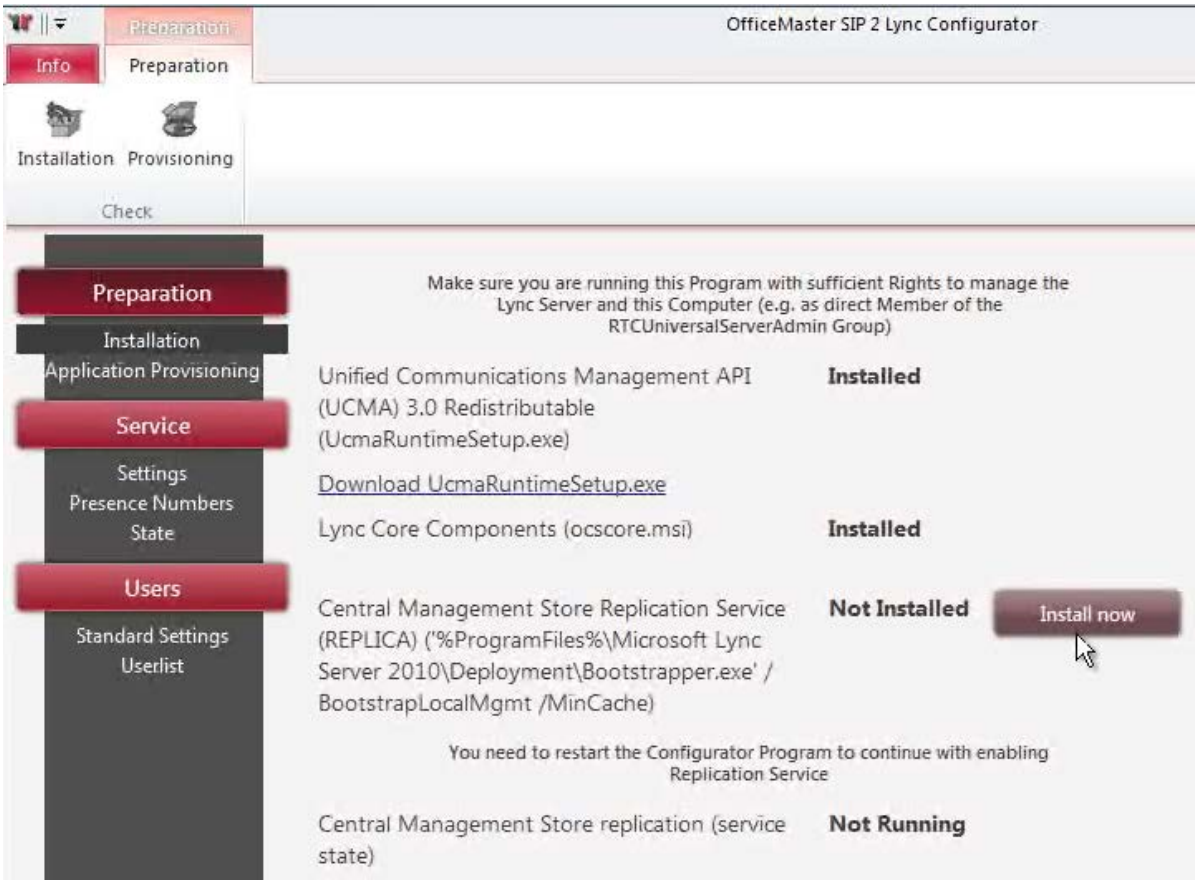


Image 2.3: Installing SQL and Replication Service

The installation will take a few minutes.

▼Note! The configuration program will, as also indicated within the program itself, need to be restarted for the now-installed Powershell components to be loaded properly.

After the restart, the replication service has to be activated (Enable now).

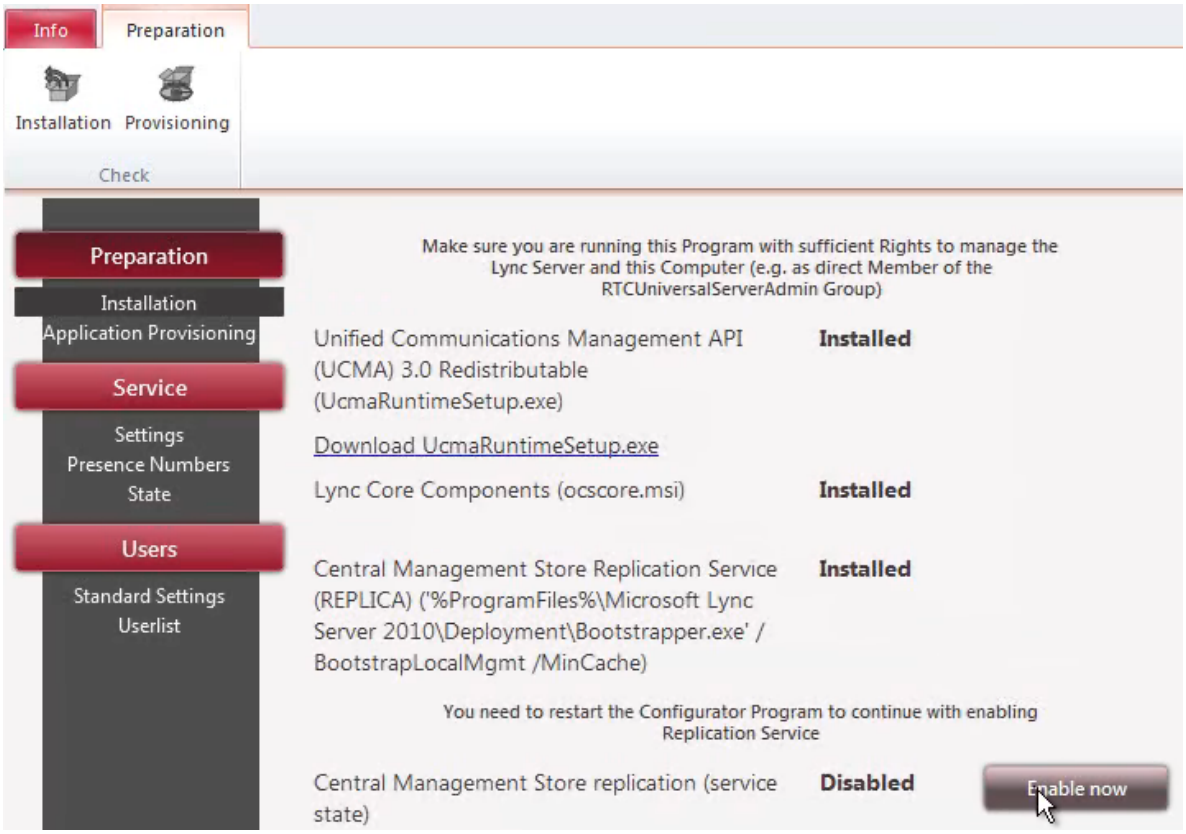


Image 2.4: Activate Replication

This concludes the installation process. The next step is to integrate the application into Lync.

## Application Provisioning

▼Note! The Lync environment is in most cases recognized automatically. It can also be declared within the service settings.

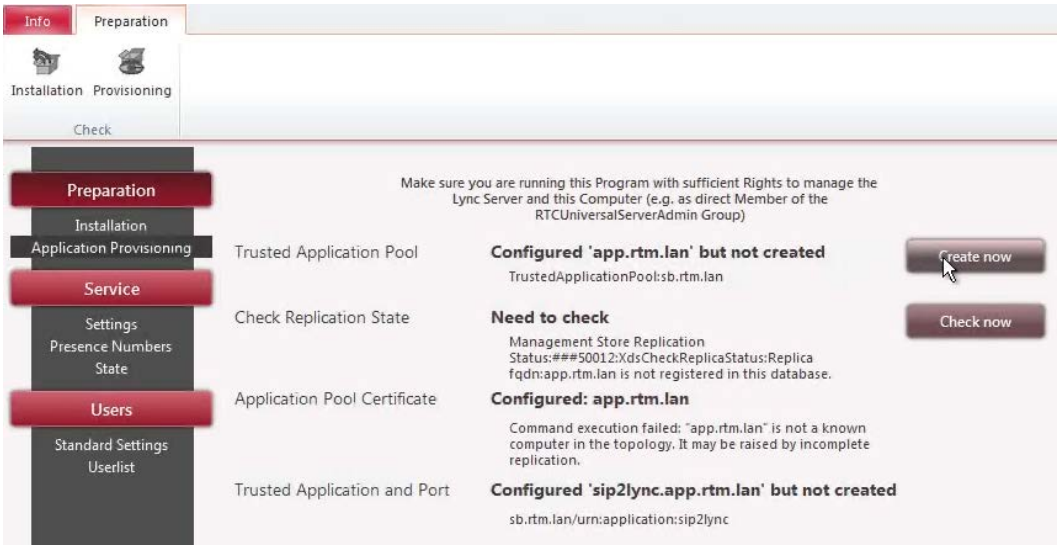


Image 2.5: Application Provisioning



Ferrari electronic

Pressing Create now will create the Trusted Application Pool in the Lync environment that was detected either automatically or specified in the service settings.

▼Note! The replication of the Management Store has to occur before continuing. Press Check now until the replication status shows Is up to date: True.

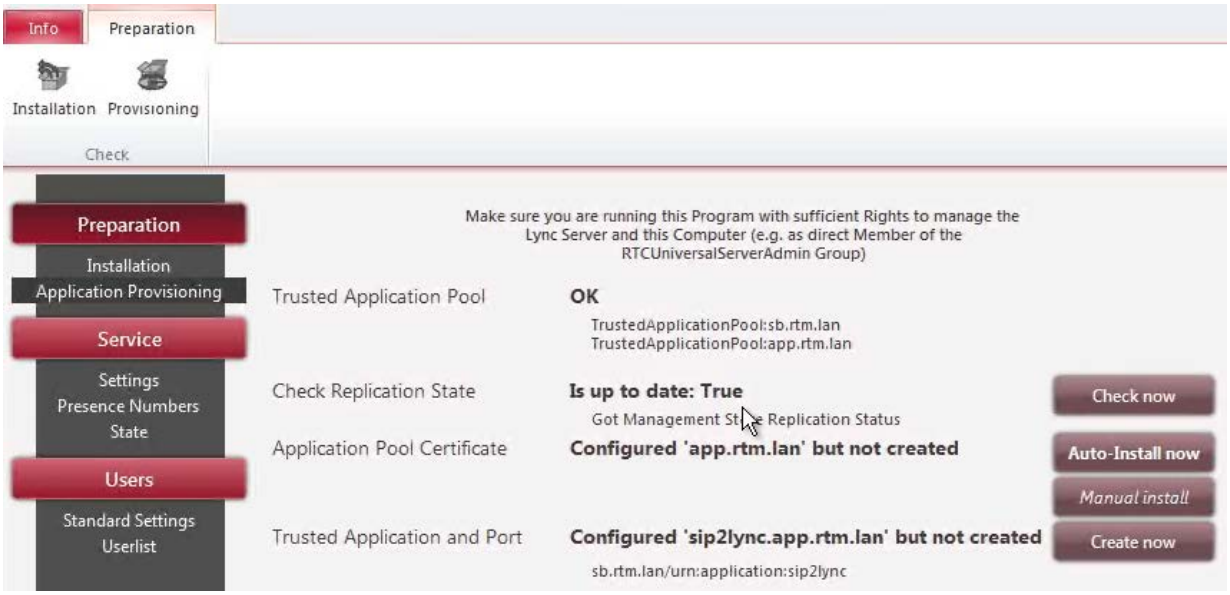


Image 2.6: Replication Status

Now a certificate has to be requested and installed for the secure communication with the Lync Server via TLS. The simplest way of achieving this is by pressing the Auto-Install now button. This is however only possible if an Enterprise-Certificate-Authority is available and the signed-in user possesses the Enroll-Permission onto the template Webserver.

Alternatively, a certificate can be requested by pressing Manual install. The certificate can then be installed into the appropriate master-certificate.

Lastly, the Trusted Application needs to be created and the port for TLS communication needs to be declared.

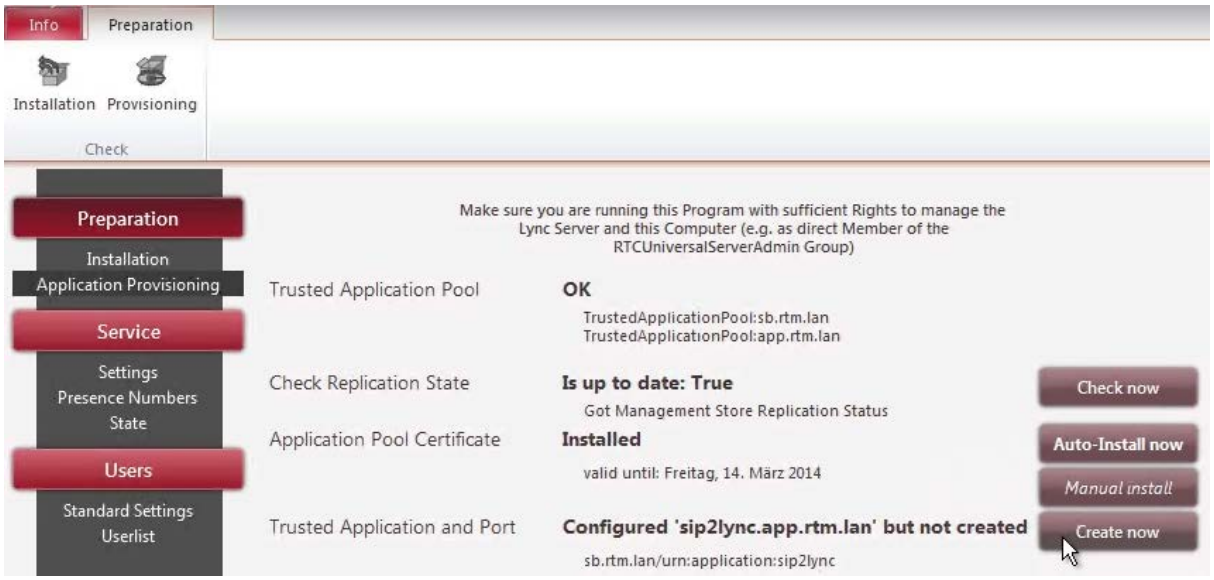


Image 2.7: Create Trusted Application

▼Note! On occasion, the display of the current status needs to be updated by pressing Provisioning in the ribbon bar. The desired status for Trusted Application and Port is OK.

## Service Settings

The DNS-Name ("FQDN") of the active OfficeMaster Gate has to be entered and applied by pressing Apply.

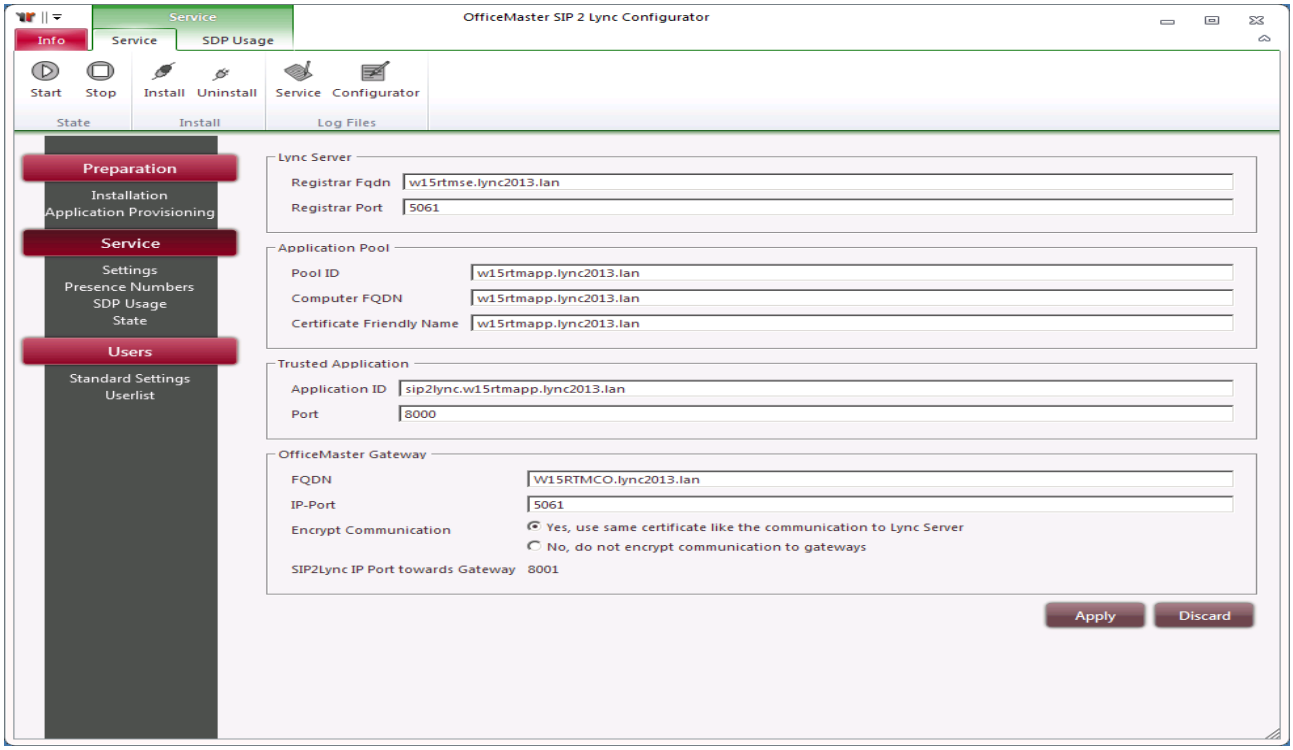


Image 2.8: Entering OfficeMaster Gate



Ferrari electronic

▼Note! In the lower part the Port on which SIP2Lync expects the SIP communication from the Gateway is shown. This later becomes important during the Gateway configuration within respective rules. The default is 8001; the communication should take place via TLS. Additionally, the Port on which the Gateway is waiting for a connection has to be tested. The default for TLS, in most cases, is 5061 – this can be verified in the Gateway's VoIP settings.

## ▶ Lync Server

### ▶ Registrar FQDN:

DNS name of the Lync Server on which the user is configured

### ▶ Registrar Port

TLS port on which the Lync Server waits for incoming connections

## ▶ Application Pool

### ▶ Pool ID

### ▶ Computer FQDN

DNS name of the computer

### ▶ Certificate Friendly Name

Name of a certificate on the local computer which is used to encode the communication with the Lync Server. The locale certificate and the certificate on the Lync Server should at least be issued by the same certificate authority (CA). Should the communication between the Lync Server and SIP2Lync Application not be encoded (not advised) this field needs to be left empty.

## ▶ Trusted Application

### ▶ Application ID

### ▶ Port

## ▶ OfficeMaster Gate

### ▶ FQDN

Fully Qualified Domain Name of the OfficeMaster Gate that is to be used

### ▶ IP-Port

TLS Port of the OfficeMaster Gate, on which it waits for encoded incoming connections

### ▶ Encrypt Communication

If the communication between OfficeMaster Gate and SIP2Lync should be encrypted, the same certificate that is used for the communication with the Lync Server will be used with the Gateway.

▼Note! SIP2Lync IP Port towards Gateway is always one number higher than the Trusted Application Port (e.g. 8001). This has to be configured in OfficeMaster Gate.

Pressing Apply concludes the configuration. This also concludes the installation of SIP2Lync. Afterwards, the users for the Gateway have to be configured.

## 2.3. Manual Installation and Provisioning

### Installation of required components

Manual installation of the components is possible as an alternative to using the installation assistant.

Firstly all requirements listed under preparations have to be fulfilled. All other required components can be installed manually or via the SIP2Lync configuration program SIP2Lync Configurator.

### Order of installation

(The Microsoft components can, for example, be found on a Lync installation disc or online)

1. Unified Communication Managed API 3.0 (UCMA) Runtime
2. OCSCore.msi
3. Search and install Windows Updates
4. Reboot
5. Installation of the CMS replication service: start Bootstrapper.exe: ("%ProgramFiles%\Microsoft Lync Server 2013\Deployment\Bootstrapper.exe" /BootstrapLocalMgmt / MinCache)
6. Replication and execution of the Central Management Store via the configuration program or Lync Server Management Shell:
   - Enable-CSReplica
   - Start-CsWindowsService replica
   - Review: Get-CsManagementStoreReplicationStatus (can take up to 5 minutes until it is "true")
   - If the above step takes too long: start Invoke-CsManagementStoreReplication

### Provisioning (Setting up a „Trusted Application Pool" and „Trusted Application")

After the installation is complete and the Central Management Store has been started, an Application Pool has to be set up and a trusted application has to be set up in this pool. Both have to then be made known in the Lync Server. This is called Provisioning. For this, settings have to be created that declare the identity of the pool and the application as well as how the Lync Server can be reached:

1. Registrar FQDN: DNS name of the Lync Server for whom the application is configured
2. Registrar Port: TLS Port of the Lync Server
3. Pool ID: Unique name (within the Lync Server System) of the Application Pool, which needs to be created unless it already exists
4. Computer FQDN: DNS name of the computer on whom the SIP2Lync Application is run
5. Certificate Friendly Name: Name of the certificate used for the encrypted communication with the Lync Server. The certificate is, if necessary, requested and installed during the Provisioning stage.

▼Note! It is beneficial if Pool ID, Computer FQDN and the certificate name are identical, especially if only one application is run on only one computer in the Pool

6. Application ID: unique name of the SIP2Lync Application within the Application Pool, which needs to be created unless it already exists

7. (first) Port: TCP/IP Port which the application provides in order to receive messages from the Lync Server

8. Changes have to be saved via the Apply button. The settings are then saved in the registry database under the key HKLM\Software\Ferrari\Lync\OMSip2Lync.

9. Via Create Now, the Application Pool, certificate and trusted application (have to be executed in this exact order) are created. Alternatively, these steps can also be done via the Lync Server Management Shell. The commands for this have to be executed in the following order:

10. New-CsTrustedApplicationPool -Identity lyncapp.company.net -Registrar lyncserver.company.net -Site 1 (Example) -ComputerFqdn lyncapp.company.net -Verbose

11. Enable-CsTopology -Verbose

12. Request-CsCertificate -New -Type Default -FriendlyName lyncapp.company.net -CA ca.company.net\CompanyCA -ComputerFqdn lyncapp.company.net -Verbose

13. Note: The Request-CsCertificate command provides details of the newly created certificate, which are needed in the next step

14. Set-CsCertificate -Type Default -Thumbprint CertificateTumbprint (as it was issued after Request) -Verbose

15. New-CsTrustedApplication -TrustedApplicationPoolFqdn lyncapp.company.net -Port 8000 – ApplicationId Sip2LyncApp.company.net -Verbose

16. Enable-CsTopology -Verbose

# 3. Configuration

In order to make SIP2Lync fully operational, settings need to be adjusted at three different points:

- OfficeMaster Gate Settings
- SIP2Lync User Settings
- External SIP devices

## 3.1 OfficeMaster Gate Settings

The communication between SIP2Lync and third-party telephone devices is handled via OfficeMaster Gate. The differing communication protocols are translated here.

### Basic settings

First, the connection between the configuration program (“OfficeMaster Gate Configuration”) and the gateway has to be established.

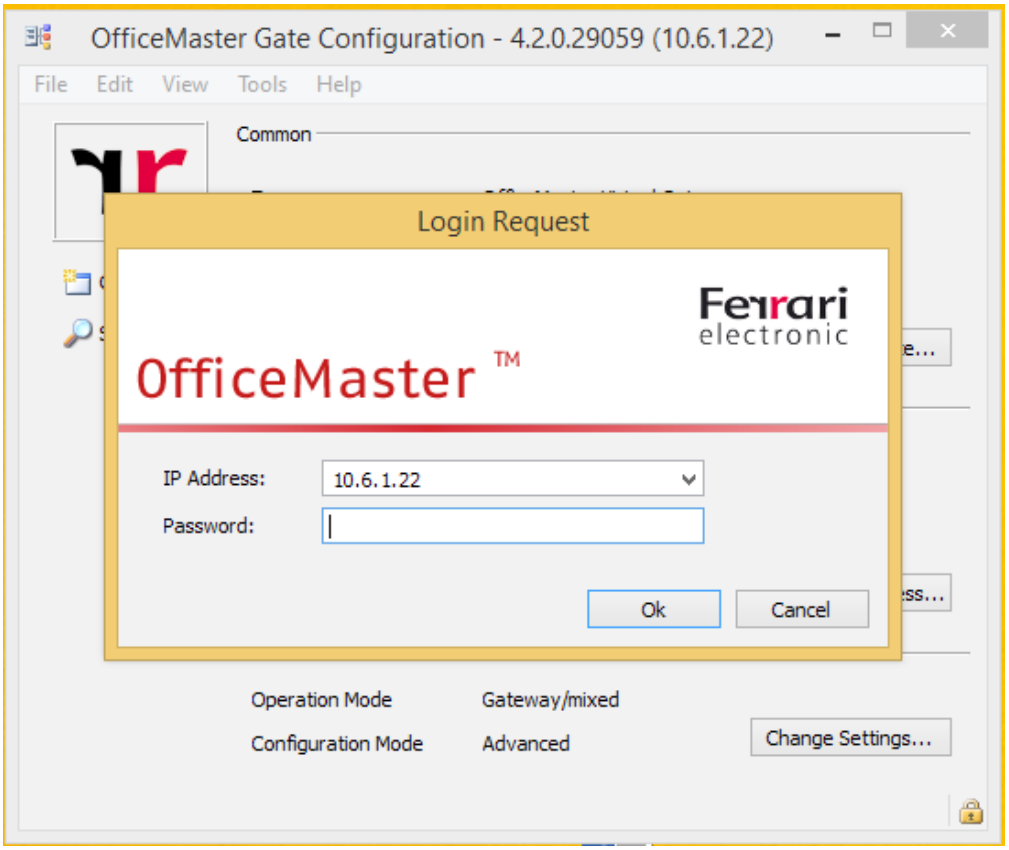


Image 3.1: Connecting to OfficeMaster Gate

The Gateway can be found and selected via the search function. Alternatively it can be accessed by entering the FQDN. The default password for the login is “omc”.

Edit and SIP2Lync Settings (only visible with the appropriate license) lead to the configuration for the connection to the SIP2Lync application.

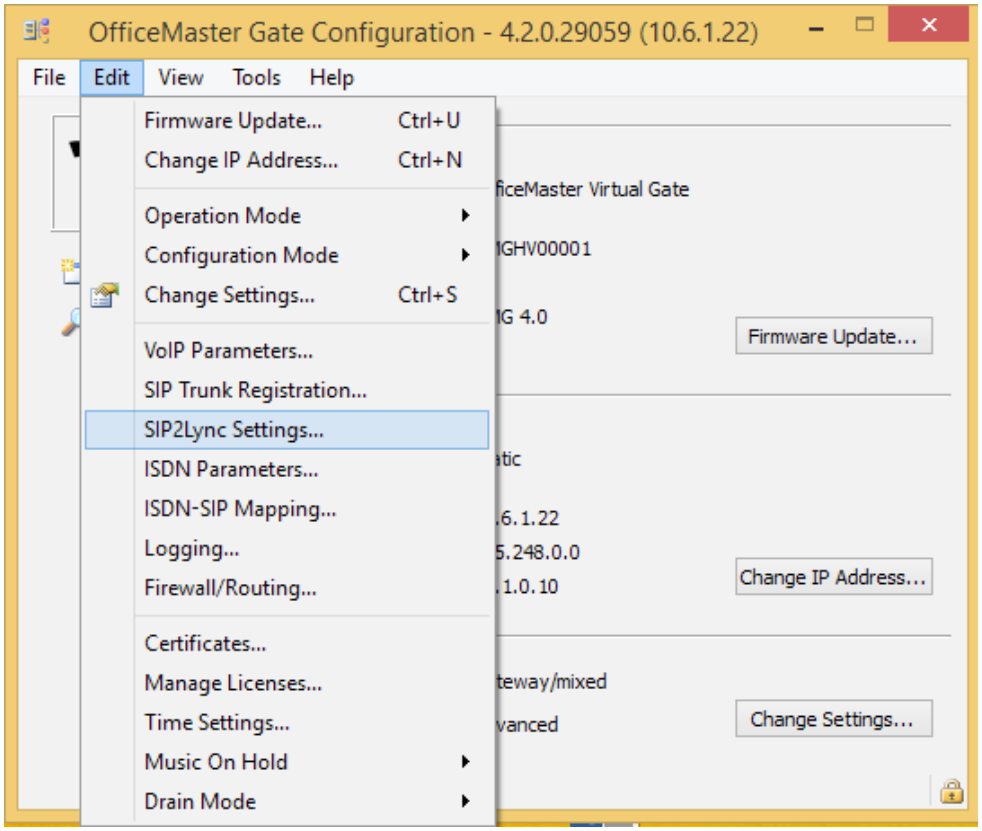


Image 3.2: Selecting SIP2Lync Settings

The connection to SIP2Lync can be activated here. The address of the application server as well as the SIP-Port-Number can also be declared.

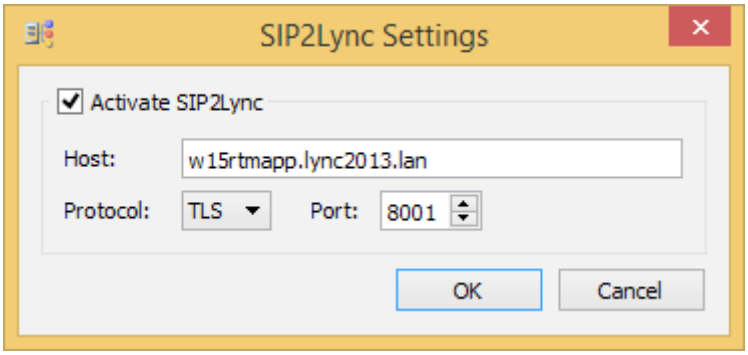


Image 3.3: SIP2Lync Settings in OfficeMaster Gate

## B2BUA Settings

The Back to Back User Settings can be accessed by pressing Change Settings ...

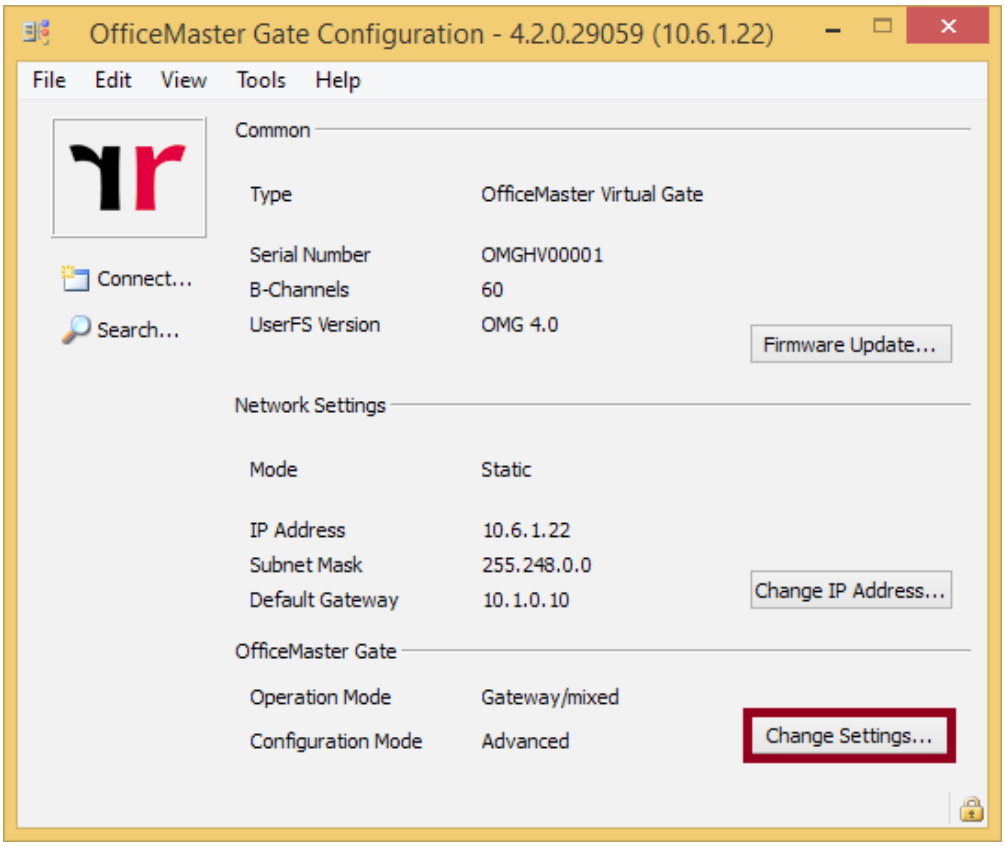


Image 3.4: Open Interface Configuration

One of the two virtual ports has to simulate the ISDN PSTN because of the ISDN protocol being asymmetrical and on Layer 2 behaving either as NT or as participant (TE). As displayed in Image 3.5, NT – Network Termination Mode has been selected for PCM2, which is highlighted and marked with a small checkmark.

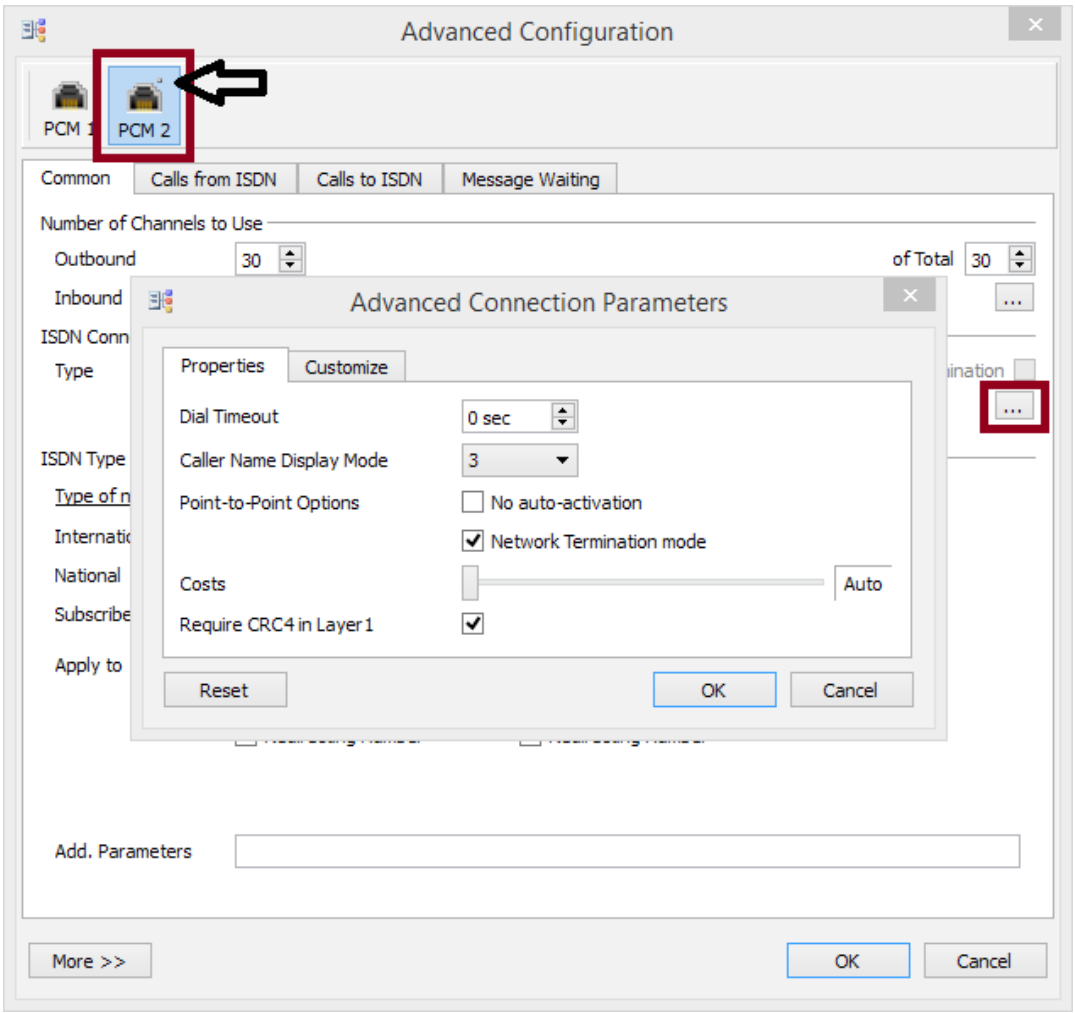


Image 3.5: Network Termination Mode Active

To change these settings (in older Firmware Versions it is not set by default) the dialog displayed can be accessed by pressing "..." in the section ISDN Connection.

▼Note! The value of Caller Name Display Mode should, on both ports, be the same in order to enable the display of Caller Name on external telephones as well.

## Declaring rules for the SIP connection

Rules which initiate the connection between internal and external have to be declared within the gateway. In the following example, connections from SIP2Lync are directed into the interface PCM2. They therefore automatically appear at PCM1 as incoming calls, which are then (again via a declared rule) redirected towards the external devices.

Vice versa, calls from external devices are received on PCM1 and redirected, as incoming calls, to PCM2 and then redirected to SIP2Lync. This allows for in- and outbound calls.

▼Note! The rules have to be created in a way that makes sure that the ways described above are the only ones possible. In some cases rules blocking certain other possibilities can be useful.

## Outbound Calls Step 1: Receiving calls from SIP2Lync

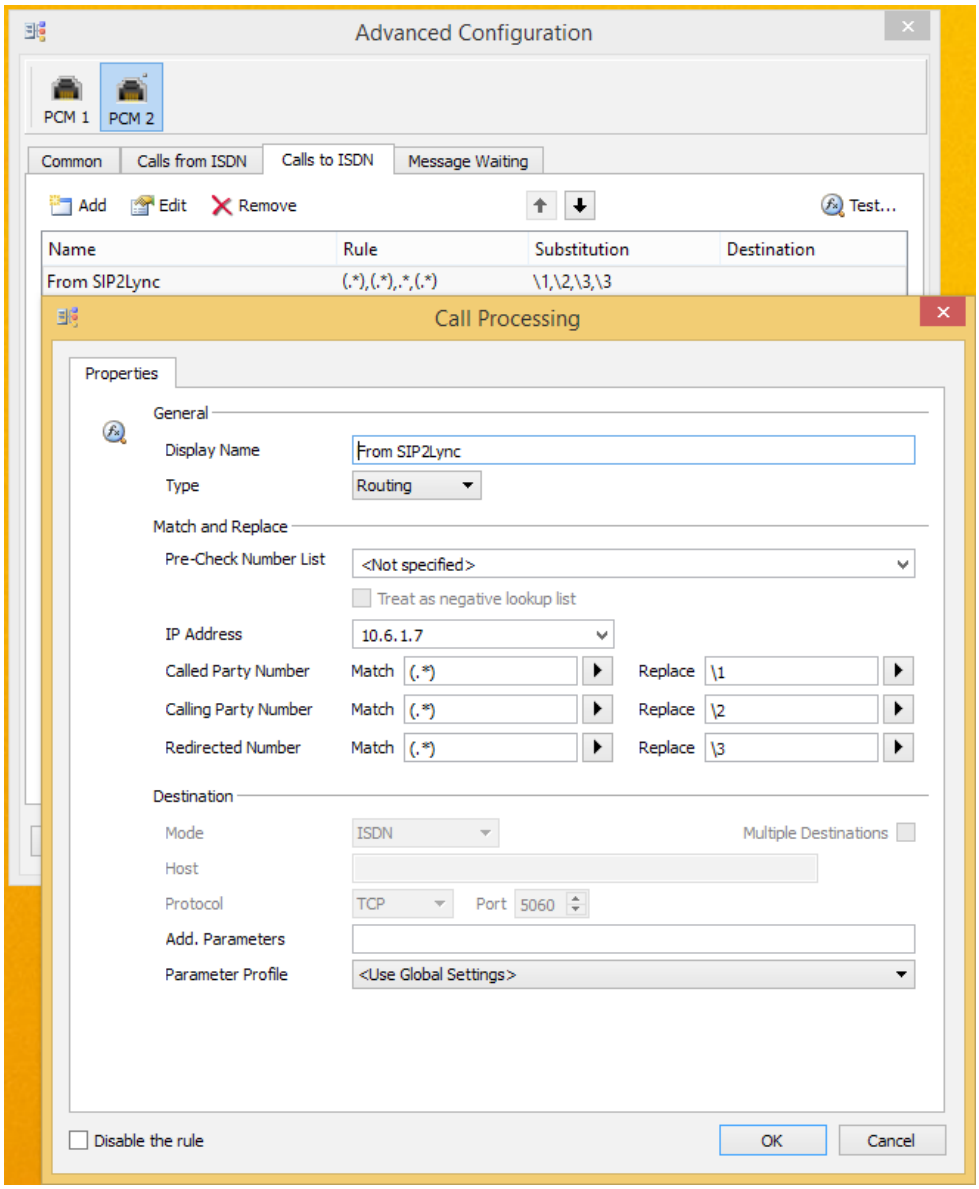


Image 3.6: Calls from SIP2Lync

This rule responds to all calls from host with IP 10.6.1.7 (SIP2Lync is installed on that host). The calls will be forwarded into the loopback device.

## Outbound Calls Step 2: Forwarding calls to external devices

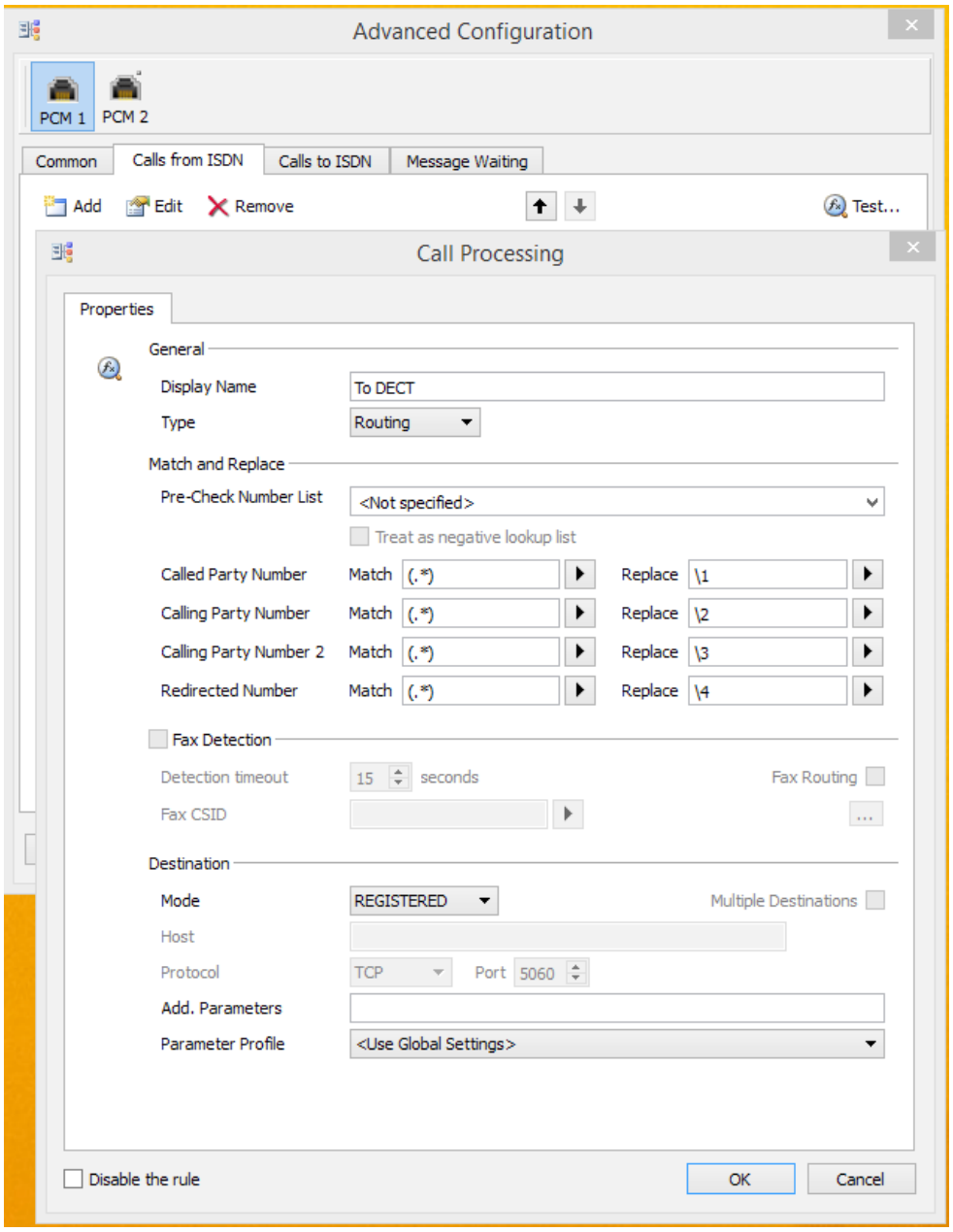


Image 3.7: Forwarding Calls to External Devices

No additional filtering is needed as PCM1 solely receives calls for external devices because of the first rule created. The type REGISTERED can be selected, meaning that the destination number will be searched for within the table of currently registered devices. If all devices are reached via SIP on the same IP address and the same port (like for example with Aastra SIP-DECT-Stations), SIP can be chosen as destination type (protocol, IP address and port need to be declared).

## Inbound Calls Step 1: Reception of calls from external devices

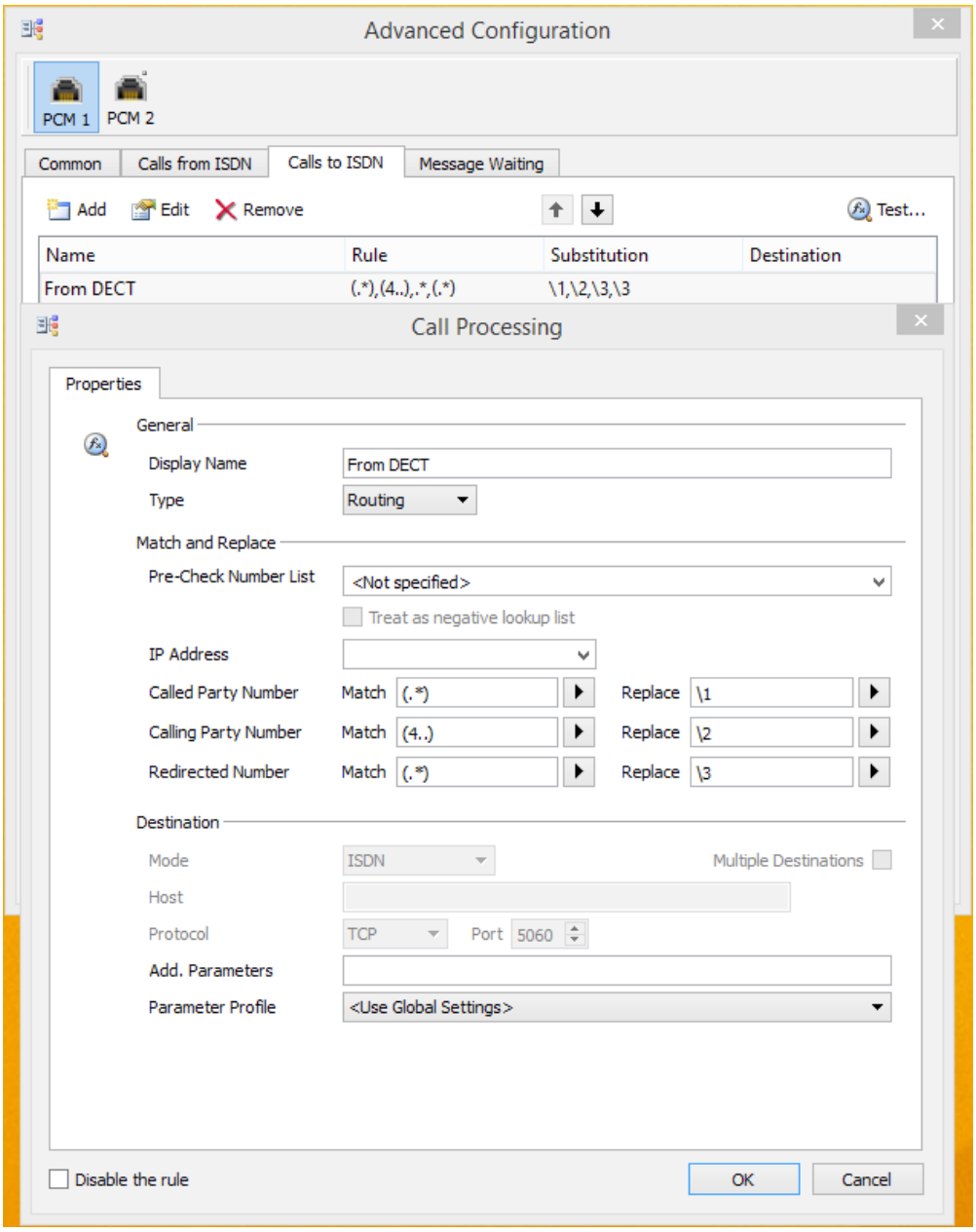


Image 3.8: Calls from External Devices

These connections are identified based on the Calling Party Number, which in this example is three digits long and begins with the number 4. The calls are redirected to PCM1 and therefore appear automatically in PCM2 as an inbound call.

## Inbound Calls Step 2: Redirecting calls to SIP2Lync

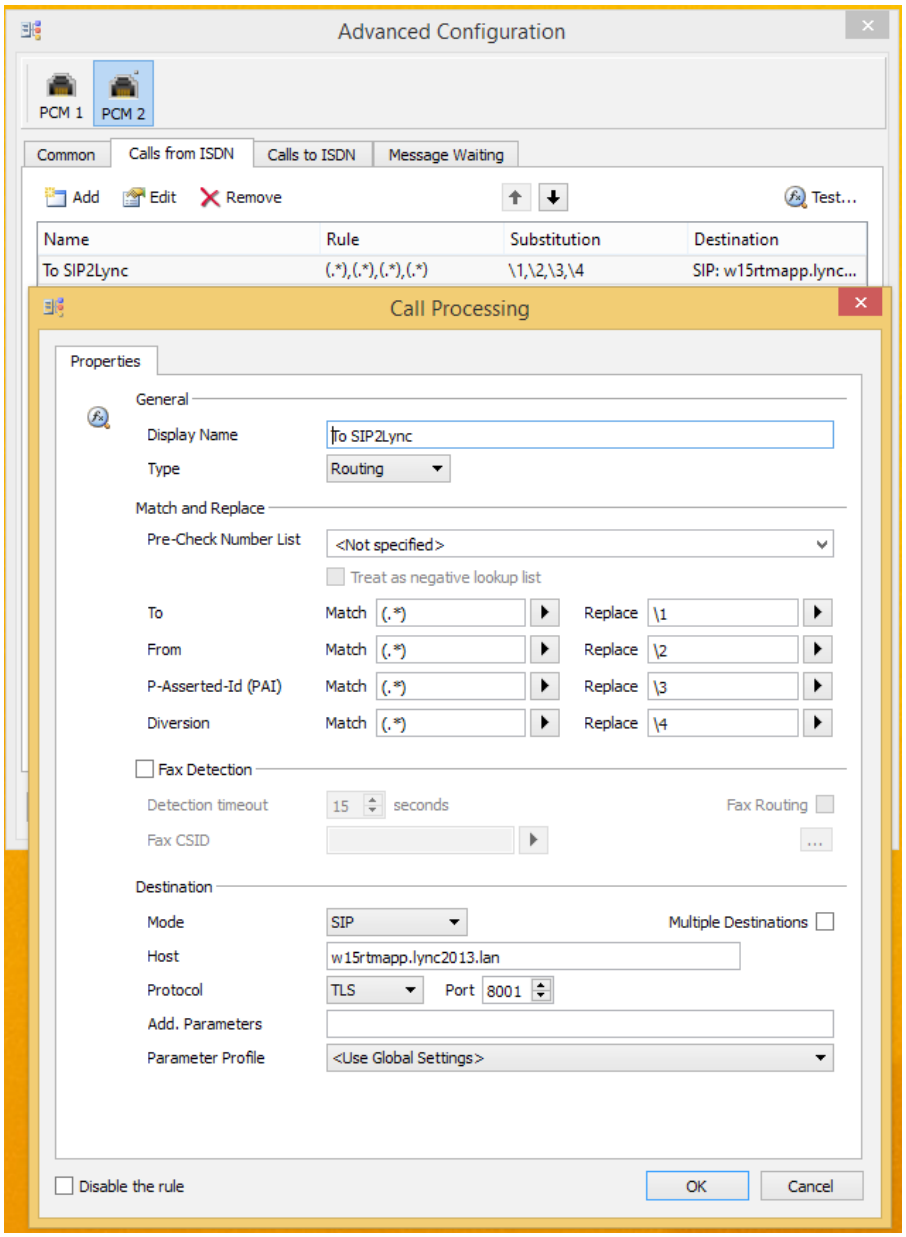


Image 3.9: Redirecting Calls to SIP2Lync

Again, no selection is required as PCM2 solely receives calls from external devices. Declare the address of the SIP2Lync server including the configured port number as destination.

▼Note! The gateway has to have the appropriate certificates for TLS installed as the communication is commonly handled via TLS. More information can be found within the OfficeMaster Gate Manual which can be found on http://www.ferrari-electronic.com.

## 3.2. User Configuration

For the use of SIP2Lync, users that are already managed in “Enterprise Voice” have to be configured in SIP2Lync as well. These users usually use a common extension on the side of the third-party phones that are to be integrated, while possessing a complete E.164 number within Lync.

### Users

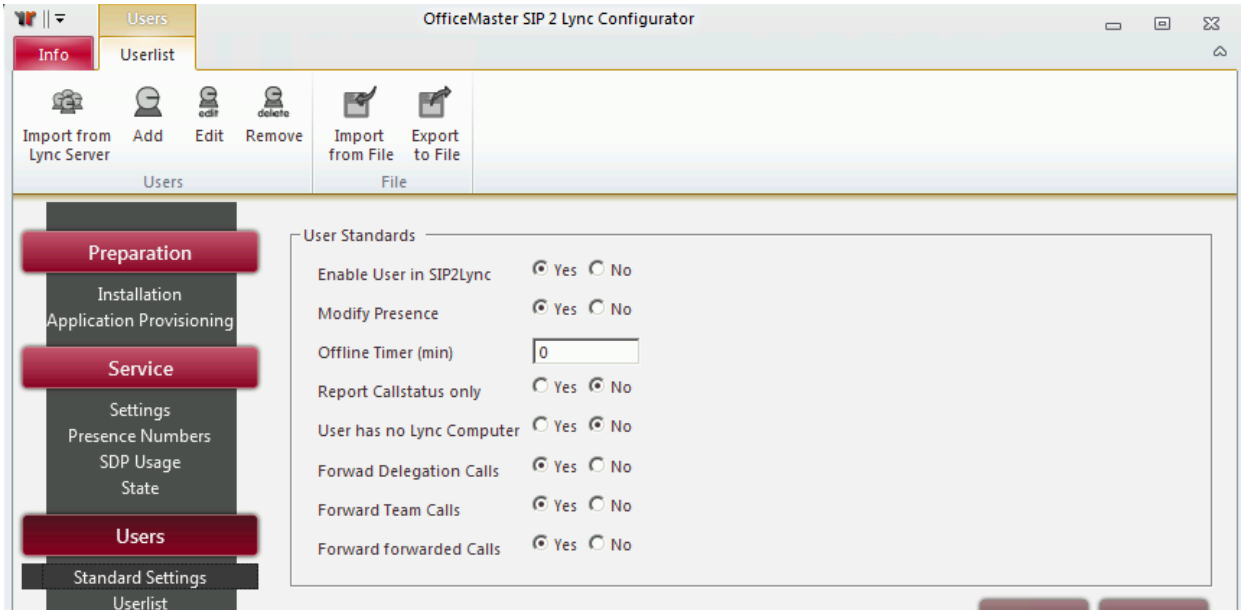


Image 3.10: Standard User Settings

► User Standards

► Enable User in SIP2Lync

Defines whether or not the user is activated for SIP2Lync

► Modify Presence

If selected SIP2Lync modifies the users presense in Microsoft Lync

► Offline Timer (min)

► Report Call status only

► User has no Lync Computer

DECT device is the only phone client for the user

► Forward Delegation Calls

DECT user receives delegation calls

▶ Forward Team Calls

DECT user receives team calls

▶ Forward forwarded Calls

DECT user receives forwarded calls

### 3.2.1 Importing Users from Lync

User can either import previously exported SIP2Lync users from Lync or add them via Add/Edit.

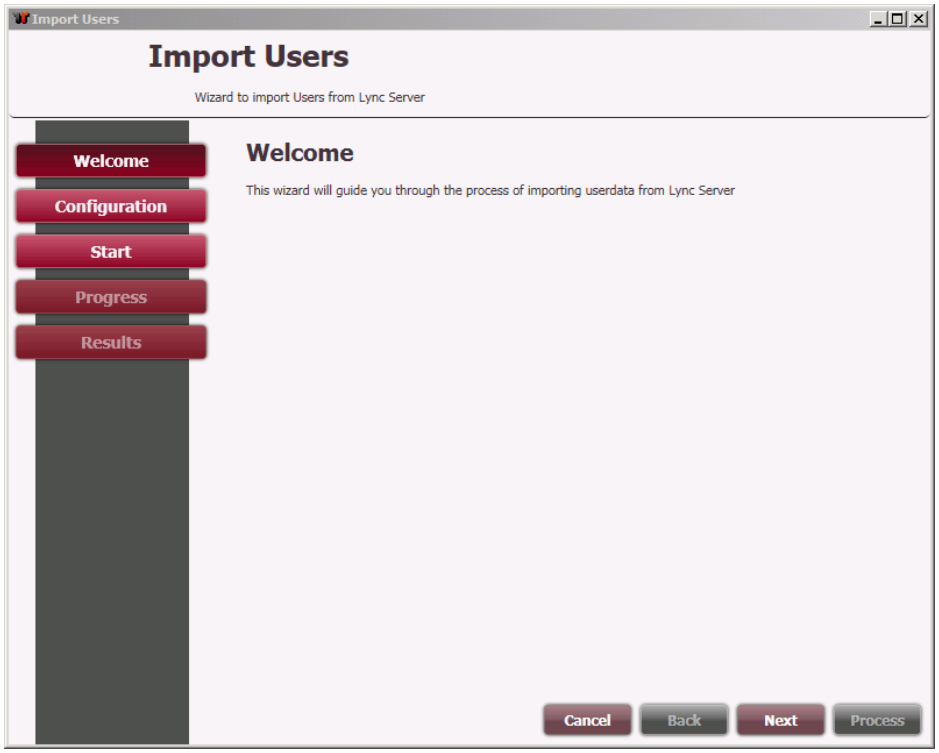


Image 3.11: Importing Users from Lync

Initially, all found users are displayed and marked for import.

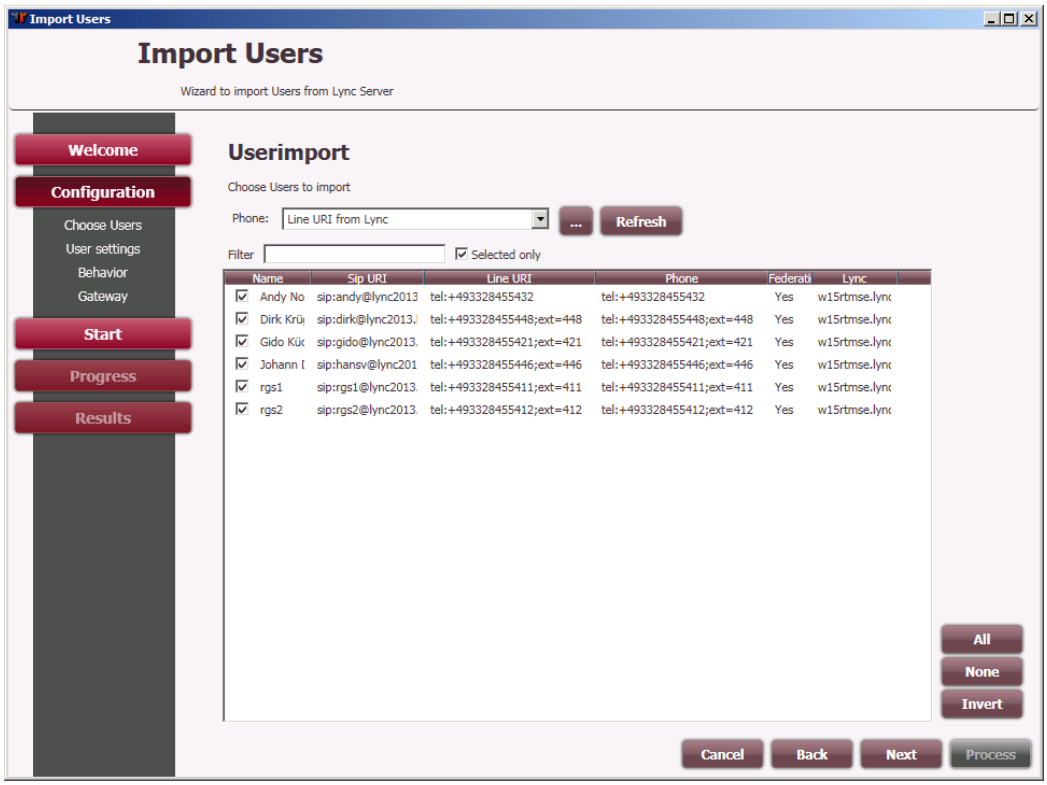


Image 3.12: Import Users by Line URI from Lync (default)

To specify the phone number of the selected users press the More (...) Button.

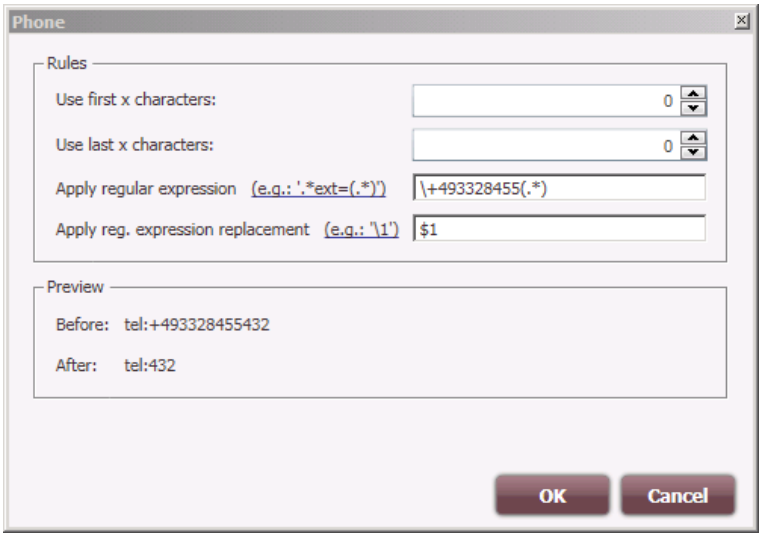


Image 3.13: Import Rules

Use last x characters: for example defines, that the last x digits of the E.164 telephone number represent the extension. The number can also be extracted with the help of a regular expression. The appropriate expression for the migration of extensions, which are already in the ";ext=xxx" format, can be preconfigured for the use as reference for the selection (".*ext=(.*)") as well as for the content of the bracket ("\1") by selecting the template.

▼Note! After applying the rules, only one number shows the desired format. The others still show an extension number. They have to be deselected.

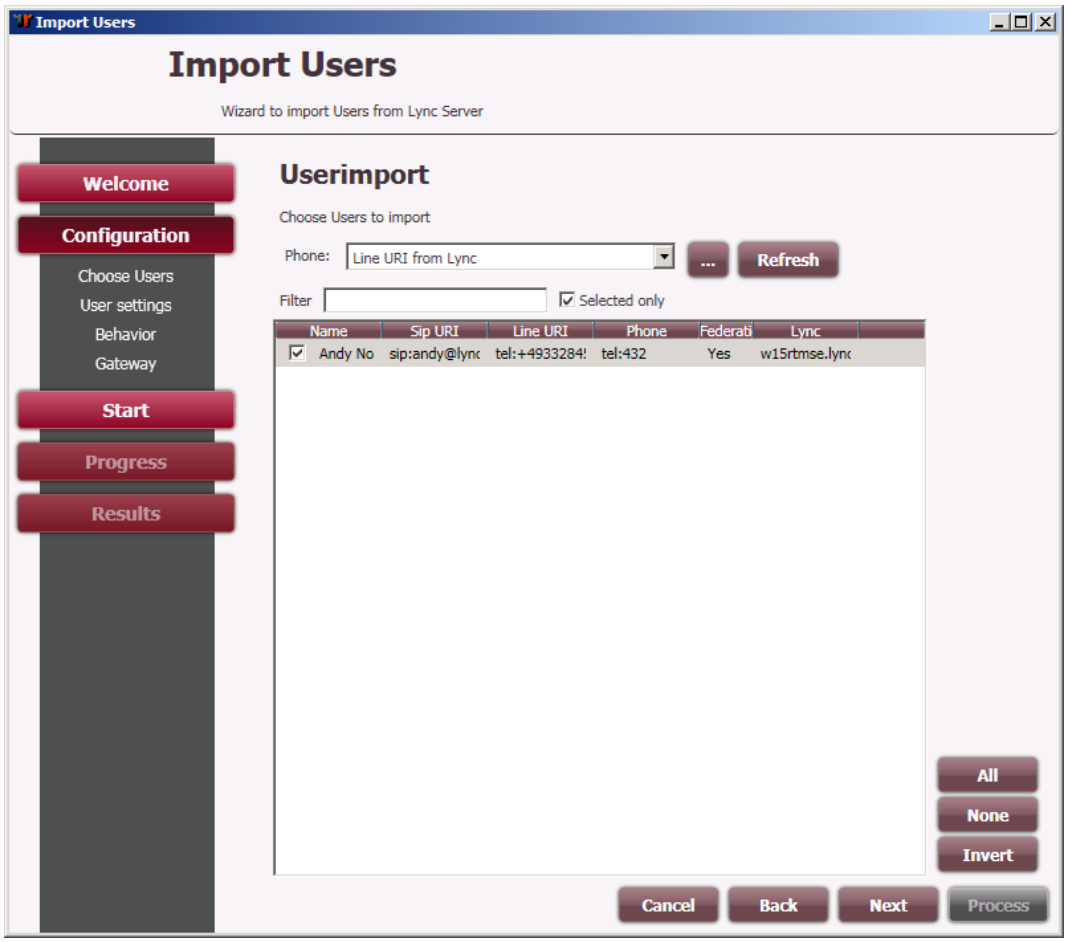


Image 3.14: Preview with Used Rules

Click Next and follow the wizard with standard settings, as described under Users on page 20.

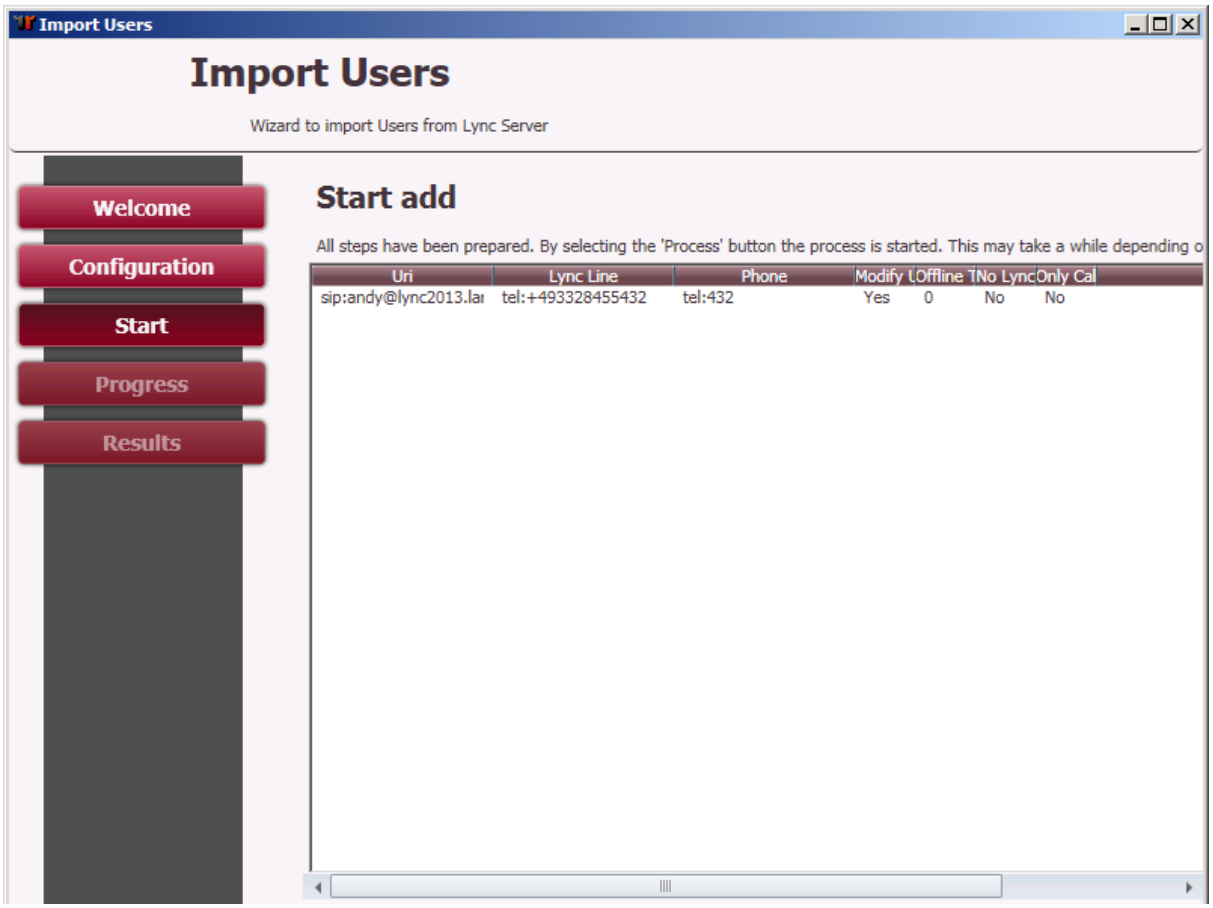


Image 3.15: Click Process

Press Process to finalize the import.

▼Note! “tel:” is required by OfficeMaster Gate to route the call correctly and will, at the end of the import, be added automatically.

To add the previously deselected users, start the import wizard again. In our example we need the following

import rule.

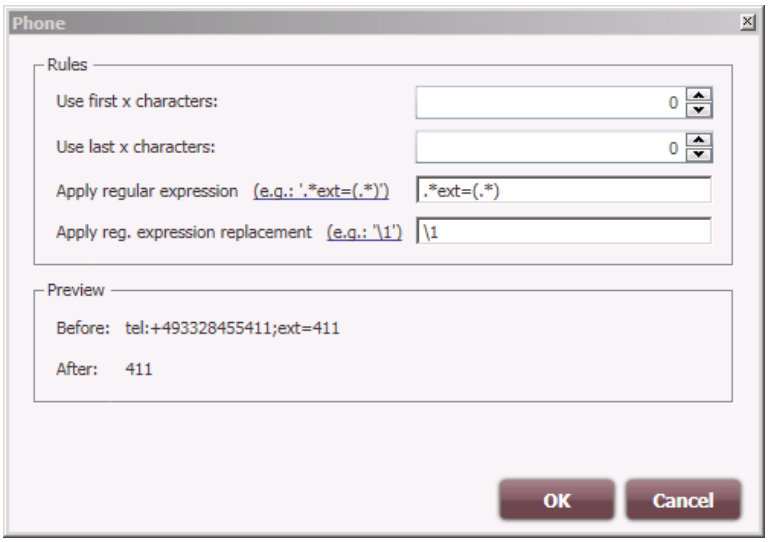


Image 3.16: Second Rule

### 3.2.2 Assisted Creating/Editing of Users

The procedure is started via "Add" respectively "Edit".

### 3.2.3 Import Users from File

Press „Import Users from File" to select users that have already be configured and saved within a file.

### 3.2.4 Export to File

Press "Export to File" in order to export configured users to a file for later use. This allows for creating files that can later be imported again. This option is helpful when for example setting up a new installation.

## 3.3 Configuration of SIP devices

**SIP registration or fixed SIP connection (="Trunk")?**

External SIP devices can register themselves at OfficeMaster Gate to be reachable as "REGISTERED" within the outbound rule. This is mainly necessary for devices where every participant uses a different port number. In cases where all phones are reached on the same SIP port and only differentiated by telephone number, registration is not necessarily required. The outbound rule in that case has to be changed to "SIP" instead of "REGISTERED".

# 4. Using SIP2Lync

## Managing ones presence status from a telephone

Under “Presence Numbers” in the SIP2Lync Configurator, number sequences can be defined with which ones presence status can be managed from telephones.

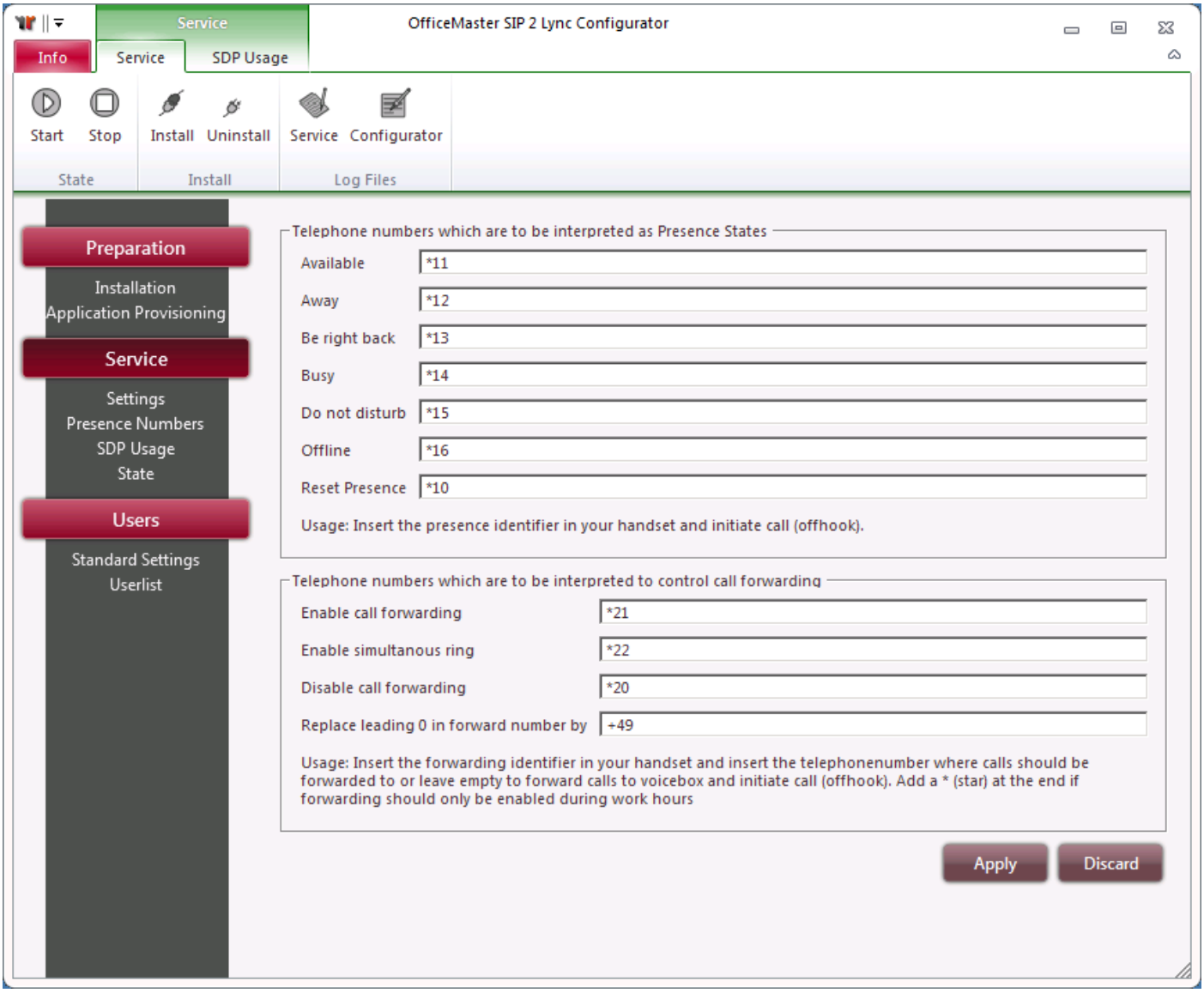


Image 4.1: Managing ones Presence

SIP2Lync can be executed, once the installation is complete and all related components have been configured.

## Execute as Console-Application

SIP2Lync can be executed directly as an application, provided that it is not registered as a service (Display in section “State”: “Service not installed”). By pressing Start, a console window is opened in which the application runs. This is helpful for a first test run - during normal operation however, the application should be run as a Windows service.

## Setting up and executing as service

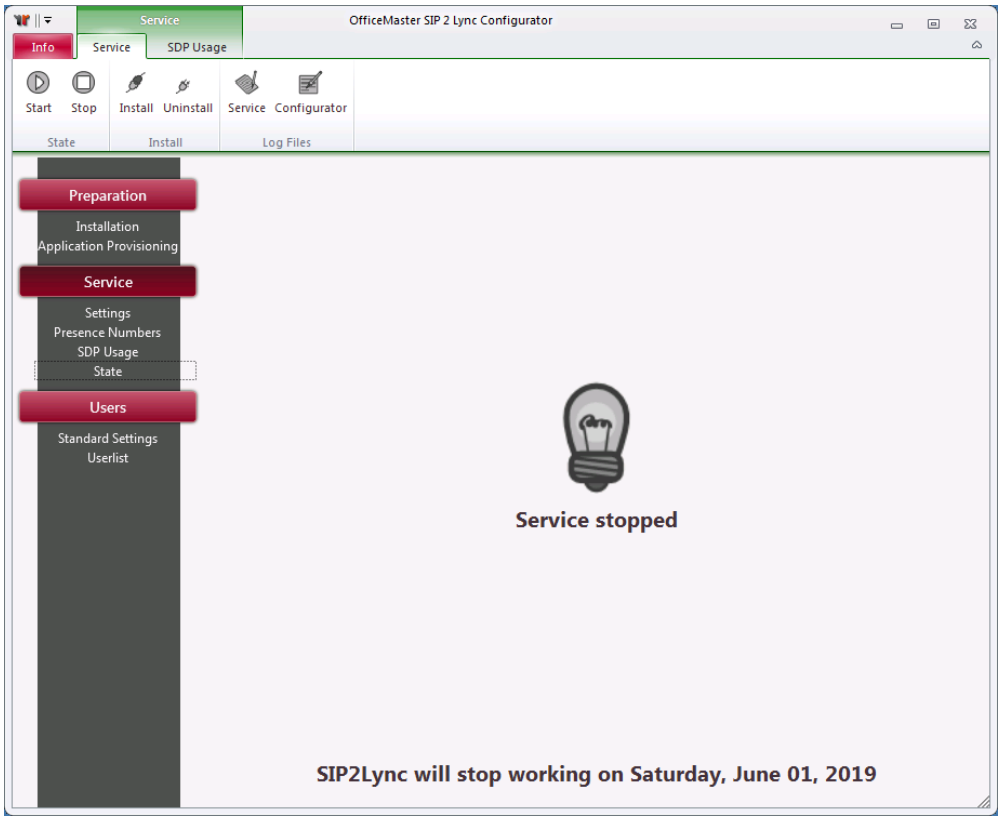


Image 4.2: Default: The Service is Stopped

Install installs SIP2Lync as a service - Uninstall accordingly removes the installation. Pressing Start initializes

the service. The following status is shown after a successful initialization:

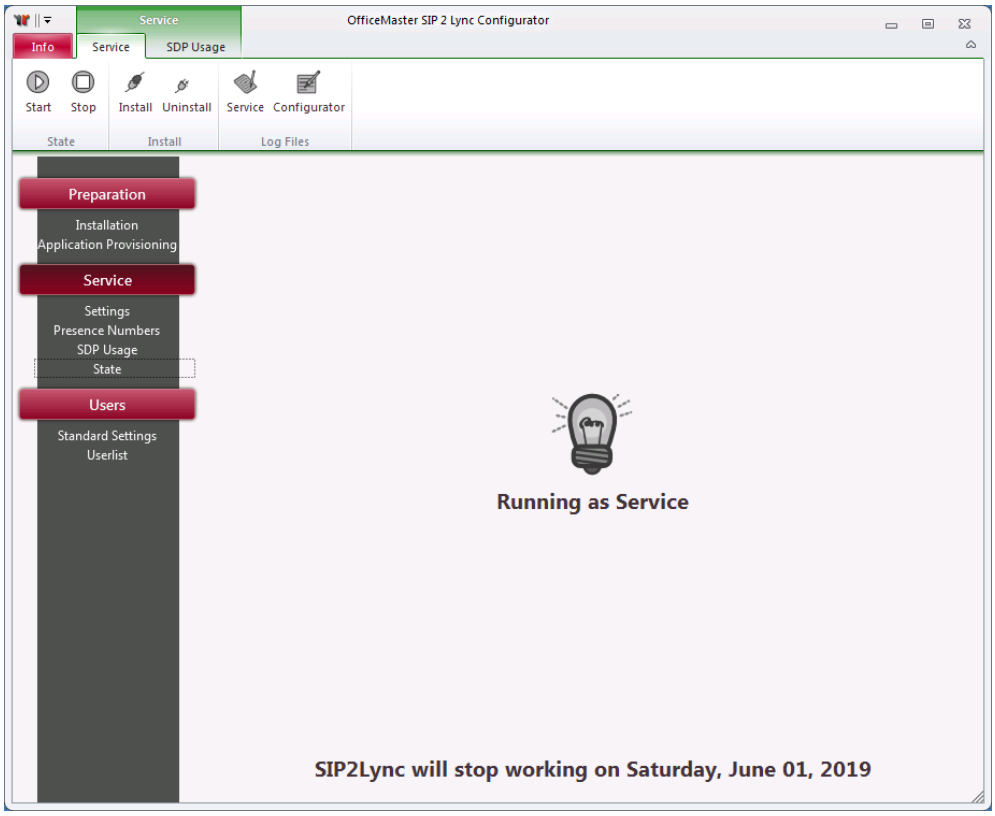


Image 4.3: Running SIP2Lync as a Service

## Displaying log files

Pressing Service or Configurator shows the log files of the SIP2Lync program respectively those of the installation process for diagnostics.

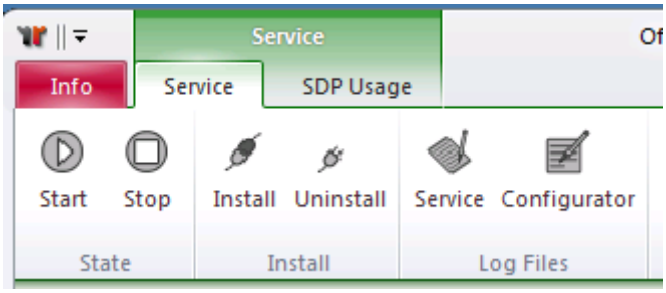


Image 4.4: Open Logfiles in Section Service

# 5. Troubleshooting

## The configuration program is not working as expected:

- Log files in %programdata%\ffums\omsip2lync\log
- Manually execute the installation of required third party components
- Execute configuration steps for Application Provisioning via the Lync Server Management shell

## SIP2Lync is not working as expected:

- Log files in %programdata%\ffums\omsip2lync\log
- Use Lync Server Logging Tool to analyze the communication between the application, the Lync Server and OfficeMaster Gateway
- Stop the SIP2Lync service
- Start SIP2Lync as console application

Activate OfficeMaster Gate Syslog Service to analyze the communication between OfficeMaster Gateway and Gateway.