OpenScape Business

VoIP Provider Data Collection

Unify | NOW PART OF Mitel

Content

History of change

Date	Version	Change
2020-05-06	V3.0	Document update for V3 • Support 100rel made visible in WBM / new SDP filter
2021-03-15	V3.1	Document update for V3R1 • rebranding • History-Info added • Check Redirection added
2021-12-13	V3.1.2	new parameter for CLIP no Screening (CLIP in From / DID in PAI)
2023-10-06	V3.3	Document update for V3R3 • WBM refresh • STUN: hint for publicIPAddr
2024-03-11	V3.3.1	Document update for V3R3.1

Comments and corrections are welcome, please contact: osbiz-certification@mitel.com.

1 Scope

This document shall guide you through the certification process of a new ITSP. The certification is needed to ensure error free connections between OpenScape Business and the ITSP. The general procedures on how to configure an ITSP are described in a separate document available in Wiki.

After successful certification you can use the OpenScape Business Certified ITSP Logo:

For new ITSP certifications and all questions about certification please contact the certification team osbiz-certification@mitel.com.

After approval by PM a member of the UNIFY certification team will be named to support you during the process and the certification can start.

The following information will be gathered during this process:

1. Basic configuration: information how to connect to the SIP infrastructure of the ITSP. (e.g. server addresses)
2. Extended SIP Provider Data: information on specific needs inside the SIP protocol. These parameters are configured to meet the specific requirements of a certain provider and should not be changed by the end user. (e.g., call number formats and SIP header content)
3. General Information about ITSP (e.g., supported features)
4. Configuration guide to help users to establish the ITSP connection

The Basic configuration (1) and Extended SIP Provider Data (2) are stored in an ITSP profile. This profile will be stored in the OpenScape business system and provides the configuration for the SIP stack in the system. Thus, defining the profile is the most important step in releasing a new ITSP.

2 Certification process

The certification always starts with

- **Collect information about ITSP**
  Collect as much information about the SIP interface and provide this information in the questionnaire you received together with this document. Deliver the questionnaire to the certification team.

- **Create a new profile for the ITSP**
  All ITSP specific configuration data is stored in a profile. Before starting the test, you must Export the profile and send it together with the ITSP questionnaire for review with the UNIFY certification team. If you need support to create a profile based on the available information, contact the UNIFY certification team partner.

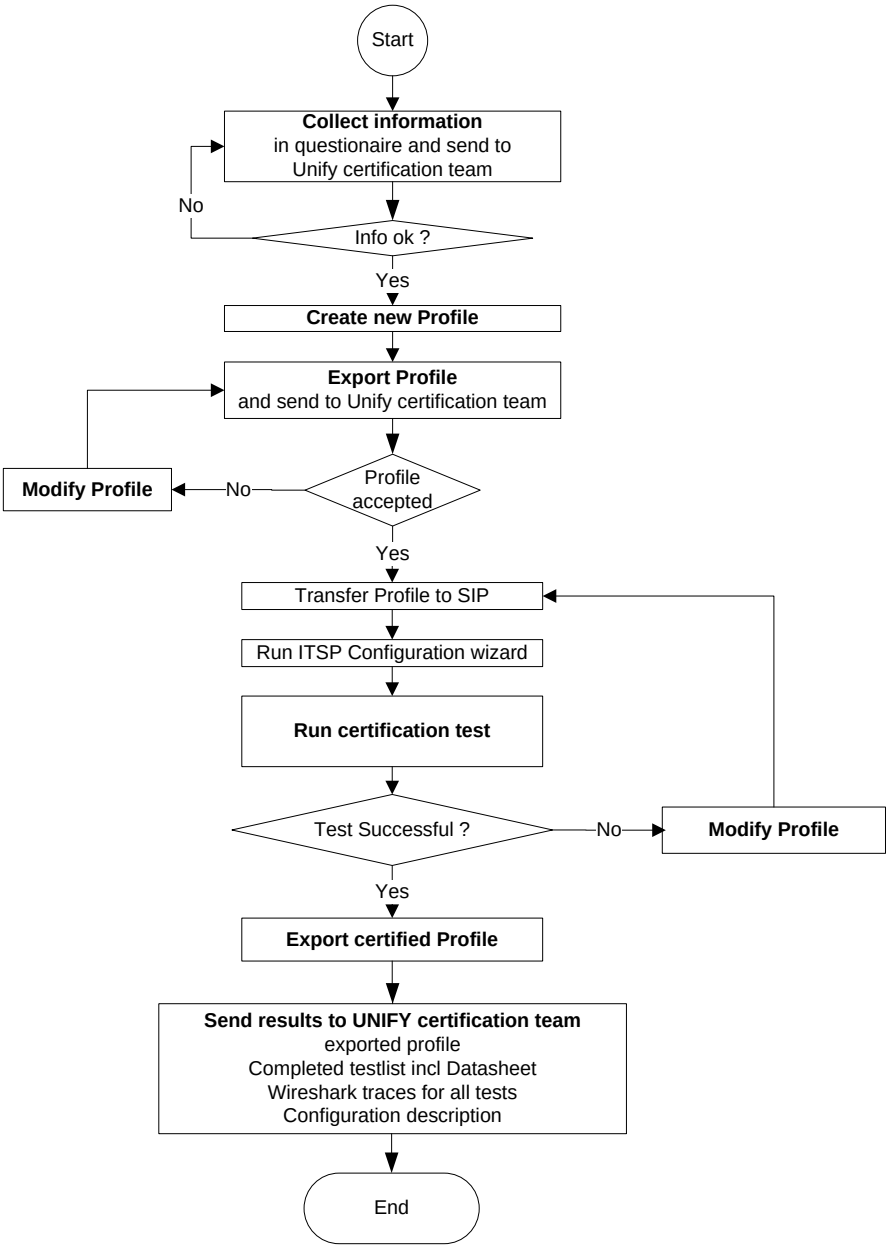
After review and during certification it may be necessary to

- **Modify the profile**
  You may need to change certain parameters to comply with all test cases.

At the end, when all tests have been passed successfully, you need to

- **Export the profile**
  If all certification tests have been passed successfully the created profile must be exported and sent to the Unify certification team together with the test documentation.

These steps are described in the following sections.

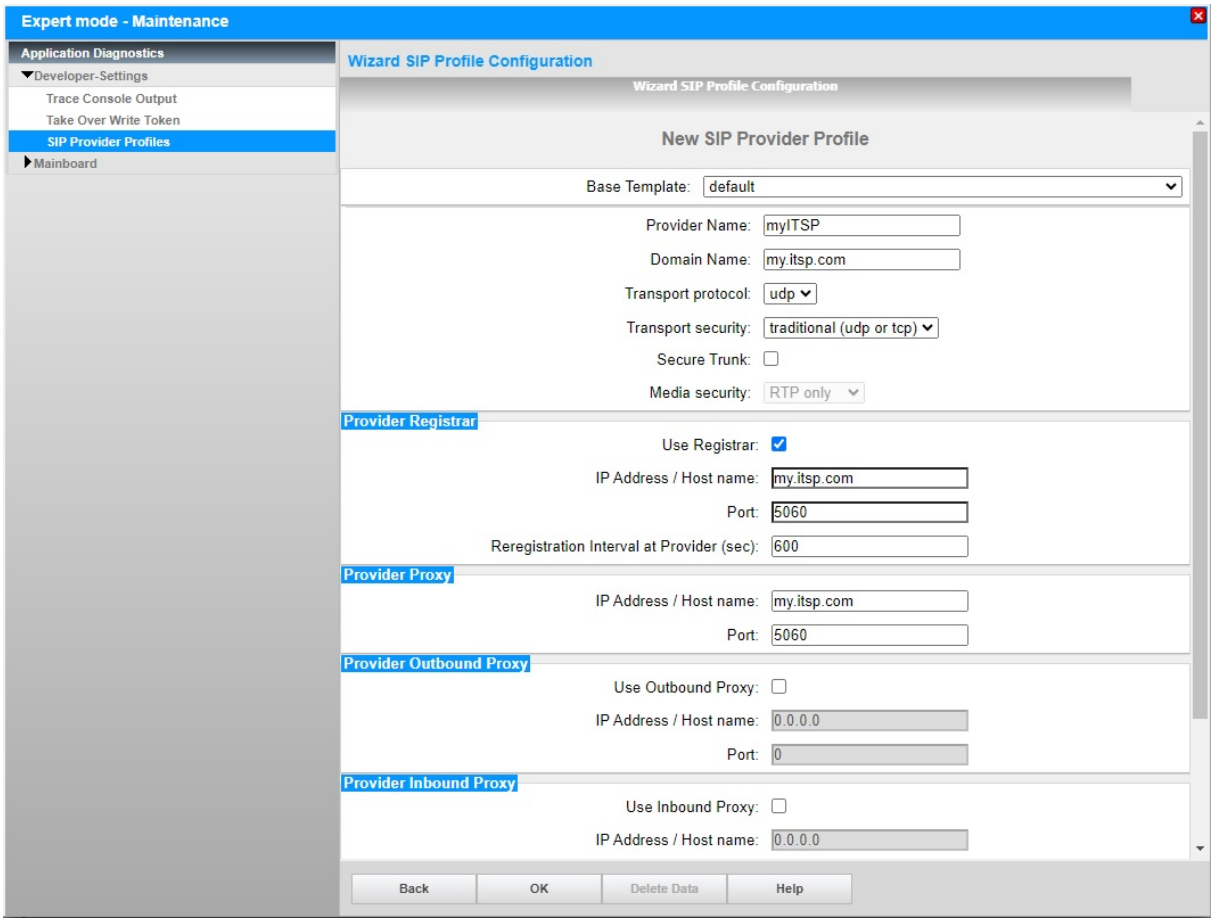

Start
Collect information
in questionaire and send to
Unify certification team
No
Info ok ?
Yes
Create new Profile
Export Profile
and send to Unify certification team
Modify Profile
No
Profile
accepted
Yes
Transfer Profile to SIP
Run ITSP Configuration wizard
Run certification test
Test Successful ?
No
Modify Profile
Yes
Export certified Profile
Send results to UNIFY certification team
exported profile
Completed testlist incl Datasheet
Wireshark traces for all tests
Configuration description
End

2.1 Create profile

Open **Expert mode->Maintenance->Application Diagnostic->Developer Settings**

➢ Press [Add] to create a new profile.

	This page MUST be used for all profile related steps during a certification. Expert mode->Voice Gateway->Internet Telephony MUST not be used.



In general, the default "base template" can be used to start the tests. You can select an already existing profile if the new ITSP is like an existing one (e.g., the new ITSP is a reseller of lines of a certified ITSP)

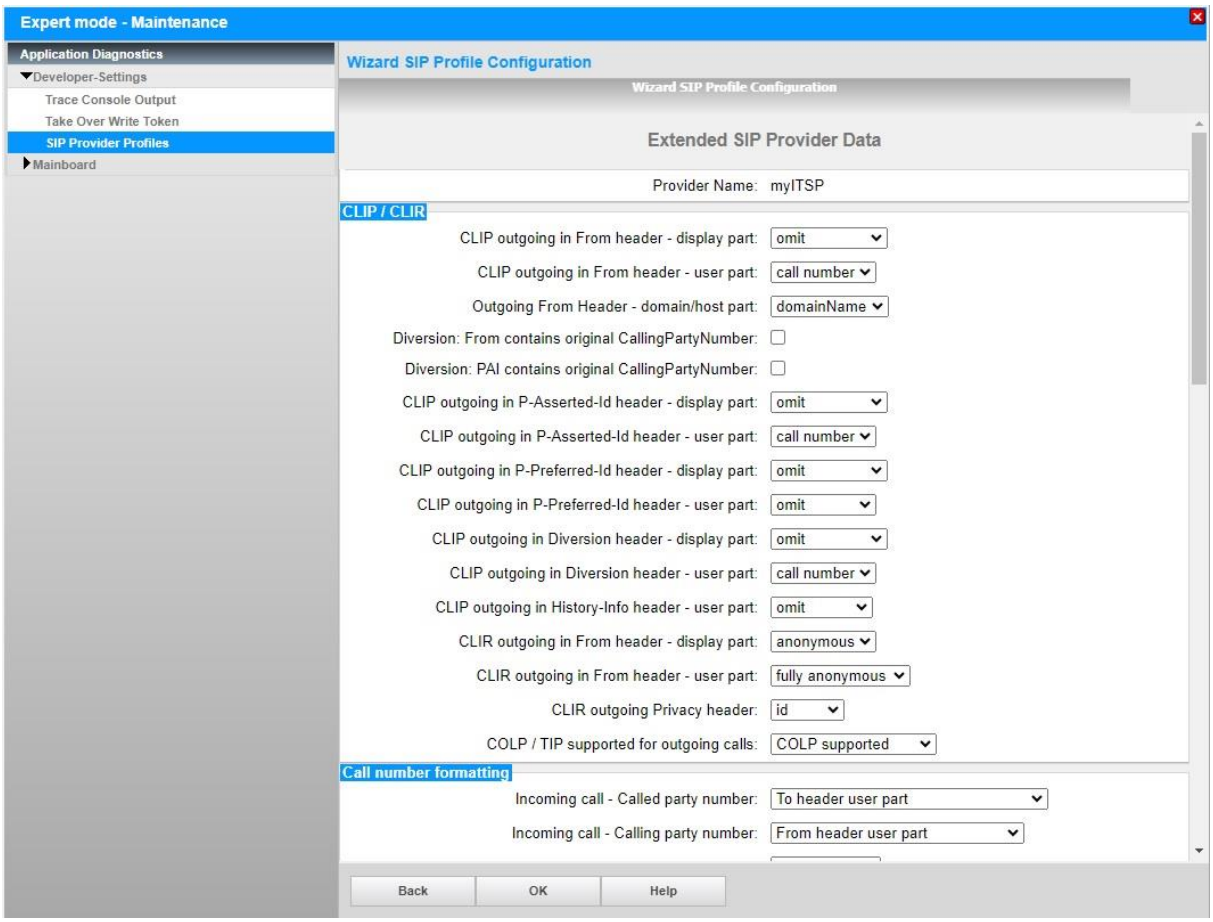
You must provide the mandatory values:

- Provider name
- Domain name
- Provider proxy

All other data are optional and may be filled out according to the needs of the new provider.

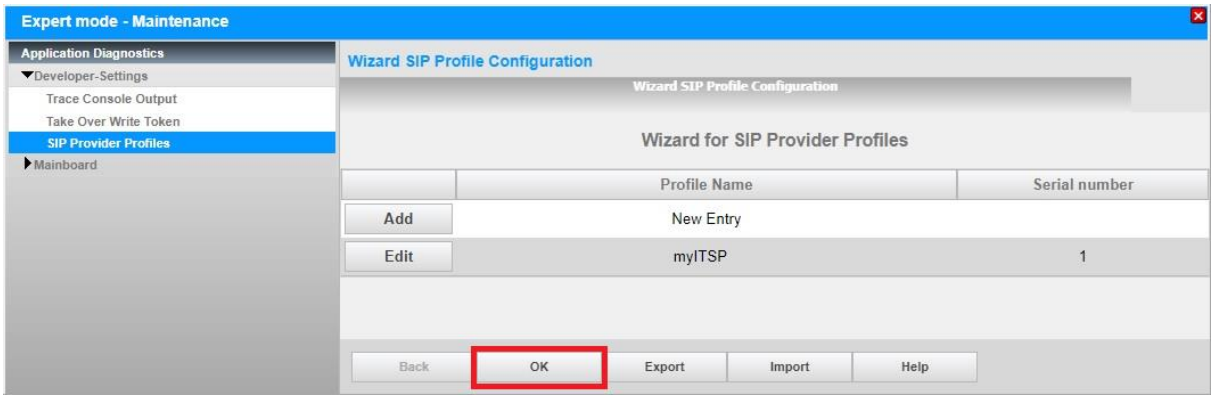
➢ Press [OK] when you are done with the page.

Every new created ITSP profile comes with default values which are the most common used among the providers already certified. The next page allows changing these values to comply with the provider's requirements.



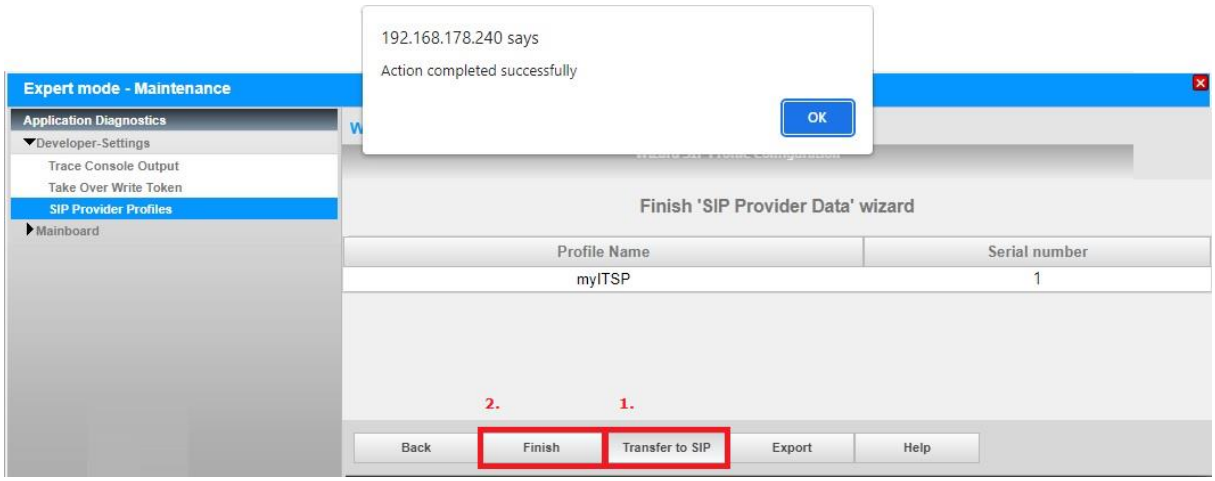
	Please be careful in providing the entries. Creating a profile with wrong entries may cause malfunctions (e.g., provider may not go into service or calls will fail).

➢ Press [OK] when you are done with the page.



Now the new profile is created and can be used for the certification tests.

- Press [OK] to go to the next page.

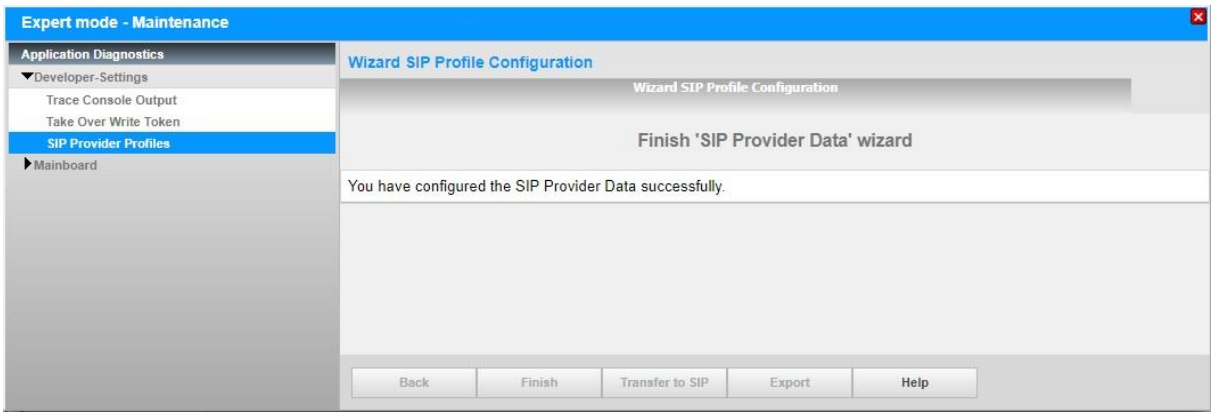


After successful creation of the new profile, it must be transferred to the SIP stack of the system.

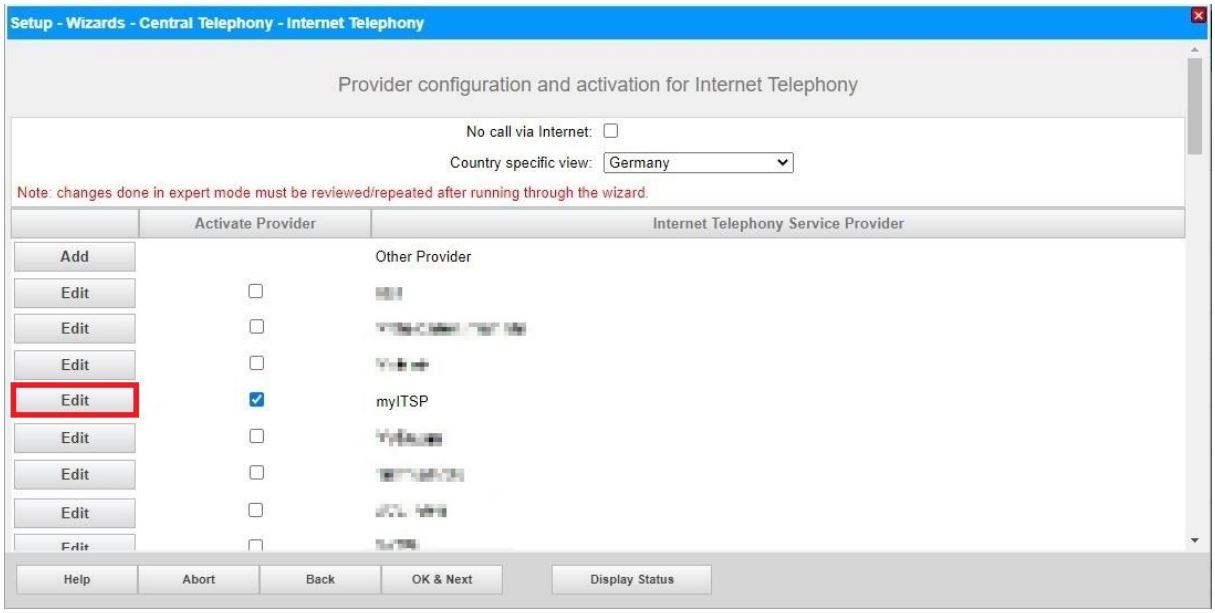
- Press [Transfer to SIP]

When the popup "Action completed successfully appears

- Press [Finish]



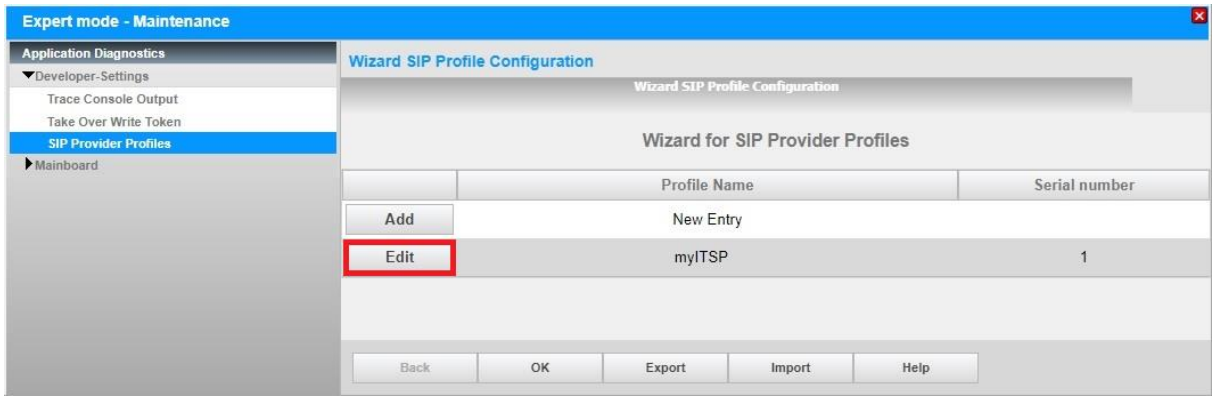
Now you can run through the ITSP configuration wizard, select the new profile, and configure the ITSP for the certification test.



2.2 Modify profile

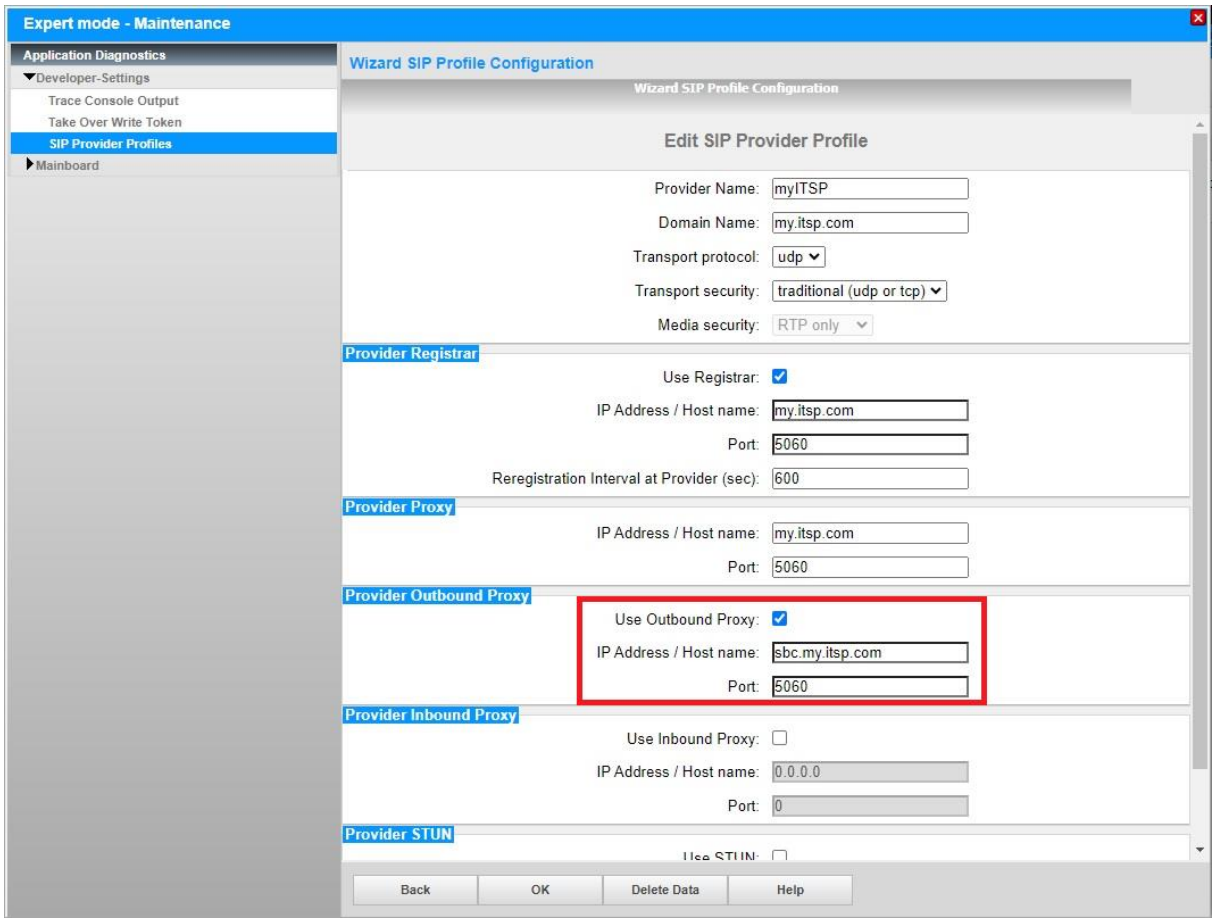
It is important that all changes for the certification are done in:

Expert mode->Maintenance->Application Diagnostic->Developer Settings



	Do not use the **Expert mode->Voice Gateway->Internet Telephony** page for changes during certification.

Change the data (e.g., outbound proxy in the example)



➢ Press [OK] when you are done with the page.

	Now please follow the same steps as for initial creation: Press [OK] on the edit pages and at the end [Transfer to SIP] when you are finished. After you transferred the data to SIP you must run through the ITSP wizard to activate the changes.

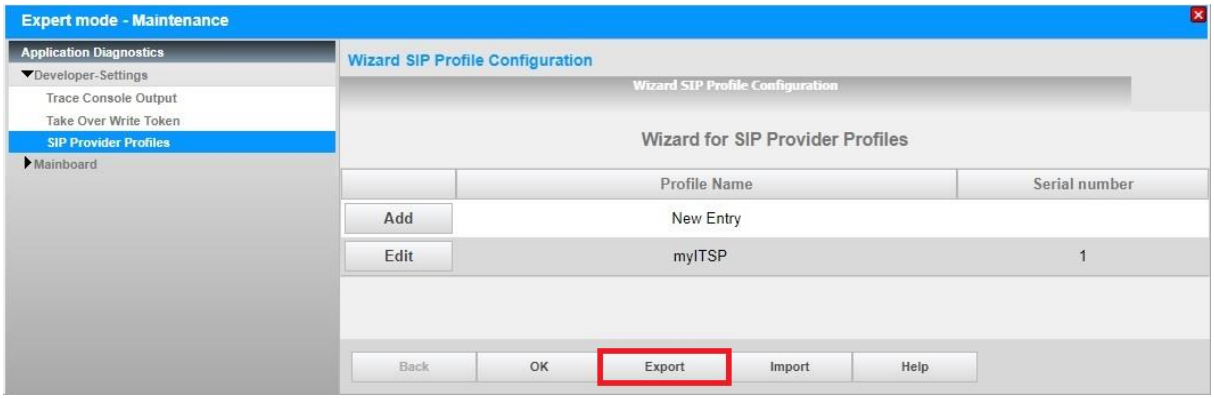
2.3 Export profile

Expert mode->Maintenance->Application Diagnostic->Developer Settings

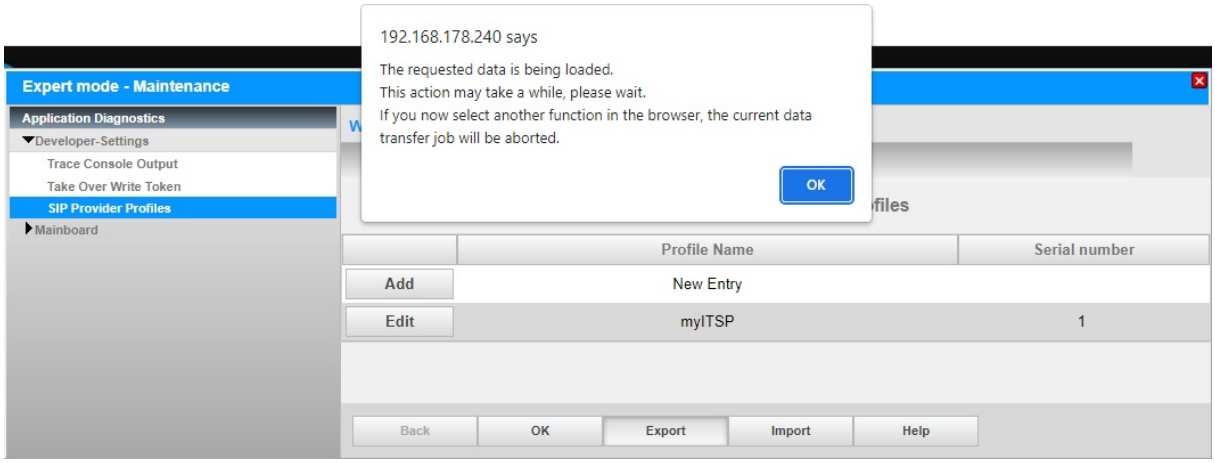
When all changes during certification have been done using the ITSP profile wizard under "Developer Settings" and the settings of the certification are like the productive environment of the ITSP this profile can be used without change in each OpenScape Business system.

In some cases, the certification is performed in a test environment and the server names need to be changed or the SIP servers need individual configuration at the customer site. In such cases the profile needs a final update using the "Edit" function described in chapter **Fehler! Verweisquelle konnte nicht gefunden werden.**.

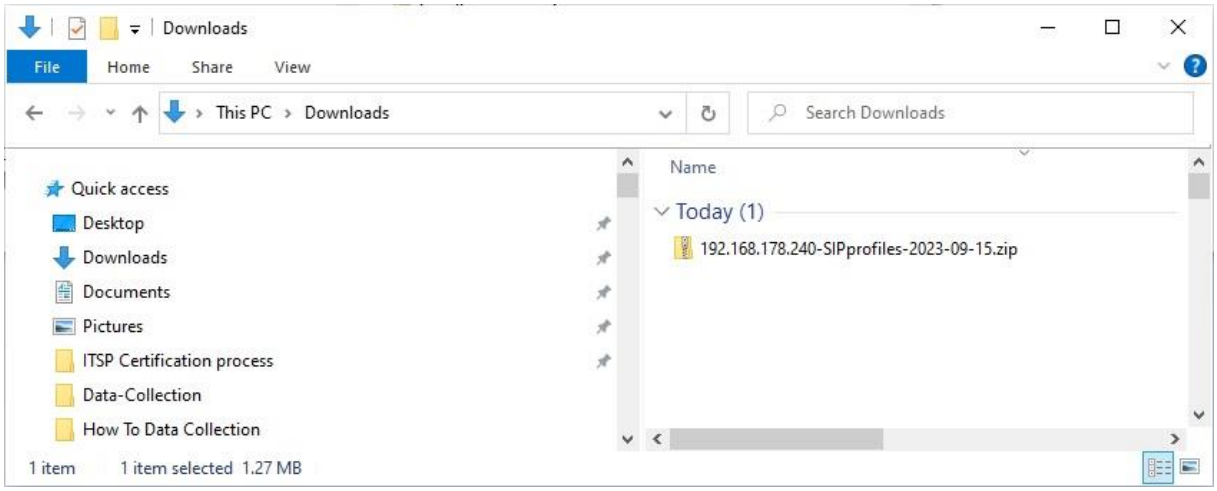
In case of individual servers (see chapter **Fehler! Verweisquelle konnte nicht gefunden werden.**) use a descriptive text (e.g. "*please.enter.ip.address*") instead of a dummy address. This text will be displayed during configuration.



➢ Press [Export]



The Export function will create a .zip file containing the XML representation of the profile.



Attach the .zip to the certification documents.

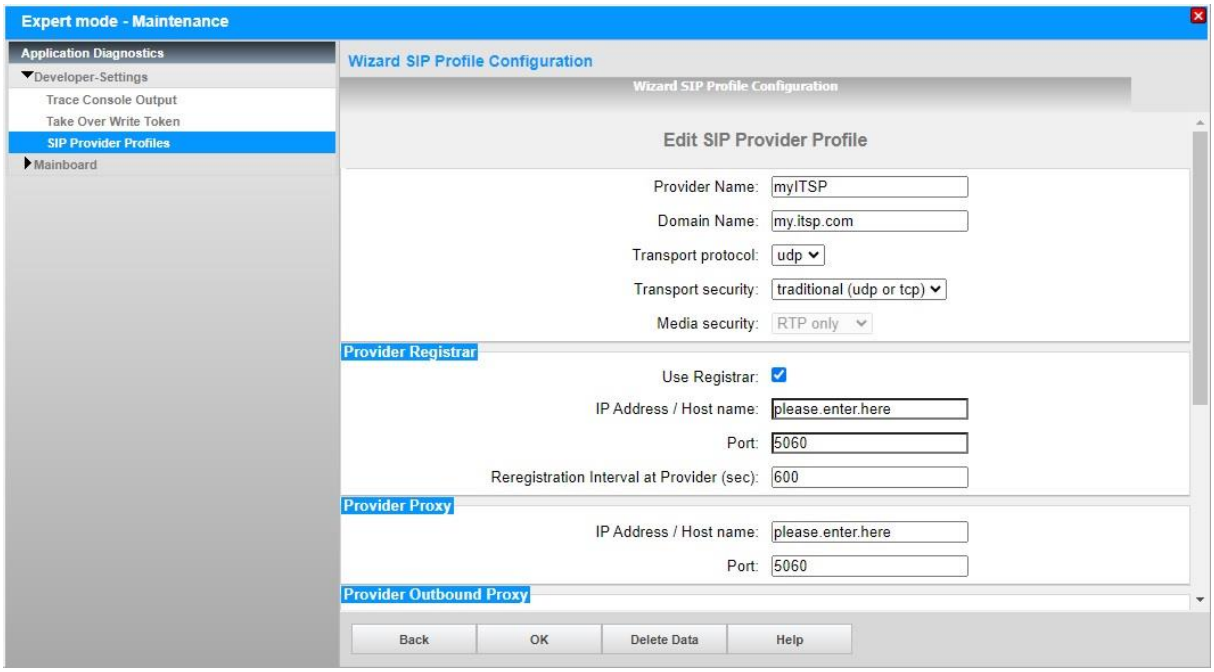
2.4 Profile needs “customer specific” data

In some cases, the ITSP infrastructure makes use of dedicated servers for a certain customer. In this case it is not possible to provide a complete template which can be used at every customer without additional entries.

For this case an additional step is needed to create the template which will be delivered with the system software.

After saving the profile used for the certification, go to the step “Modify profile” and exchange all the fields which need to be filled at the customer side (proxy, registrar, outbound proxy) with a text like “*please.enter.here*” or “*please.enter.ip.address*”

	The characters “0-9”, “a-z”, “A-Z”, “.” and “-” are allowed in these fields only.



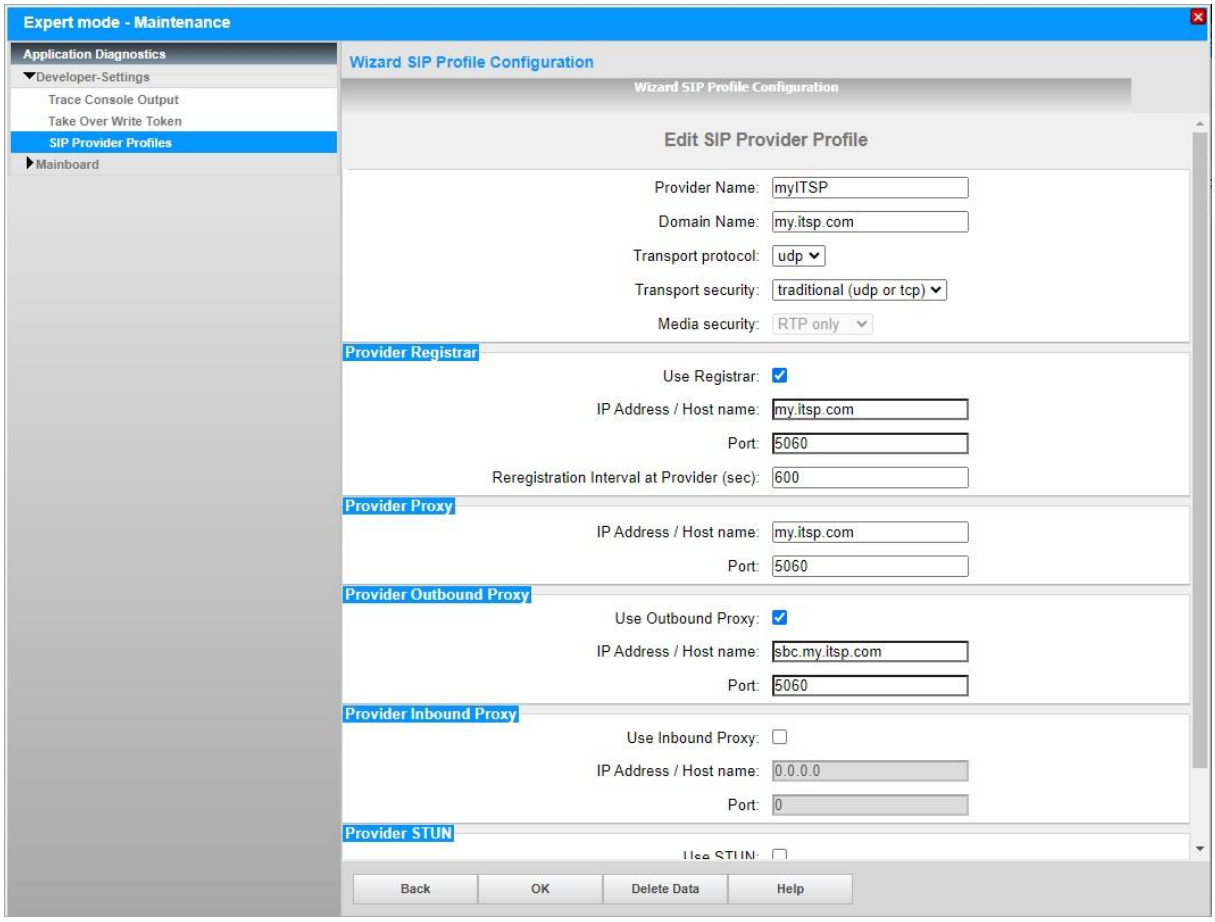
3 ITSP configuration parameters

The following chapter explains all parameters for basic configuration, user account configuration and special configuration in detail.

In the SIP examples the following placeholders for call numbers or accounts are used:

```
Calling party number     +4923026672695
Calling party account    sip-acc1
Called party number      +498970070
Called party account     sip-acc2
```

3.1 Basic ITSP configuration



3.1.1 Provider Identification / Domain

Provider Name

This is a unique name which is used in the WBM of the system to identify the ITSP. The name has no effect on the SIP protocol. If an ITSP has several product offerings, the name should include the product name.

Domain Name

The domain name is provided by the ITSP. It can contain a name or an IP-address.

Usage examples:

The configured Domain Name is used in the Host part of e.g. From: and PAI/PPI-header fields

```
From: sip:+4923026672695@DomainName
P-Asserted-Identity: sip: +4923026672695@DomainName
```

3.1.2 Transport protocol / security

Transport protocol **default: UDP**

Select the transport protocol used by the ITSP for traditional connections. Possible transports are UDP (default) or TCP.

Because of the fixed protocol selection NAPTR DNS queries are not supported as the OpenScape Business requires to trigger it and therefore no transport (udp/tcp/tls) should be configured (among other prerequisites).

Transport security **default: traditional**

Select the desired transport security level. If the ITSP offers a secure trunk as an option traditional should be used.

Please note that for use of TLS you MUST import a valid Root certificate provided by your ITSP to authenticate the TLS connection.

Secure Trunk **default: false**

If the ITSP offers a secure trunk, this flag must be set to true. This allows enabling the secure trunk in the wizard.

Media security **default: RTP-only**

Select the desired media security level. The system supports either RTP-only (unencrypted media) or SDES-only (encrypted media) mode.

If the ITSP offers a secure trunk, SDES-only MUST be selected.

3.1.3 Provider Registrar

Registration is used by ITSP for two different purposes.

1. *Addressing:* With the registration the ITSP's Registrar is informed about the IP-Address and port of the system. This is useful if the system is located behind an internet access using a dynamic IP address.
2. *Monitoring:* Registrations must be repeated periodically. The ITSP's Registrar will monitor the registrations and thus knows about availability of the system.

If ITSP provide an infrastructure with static IP addresses and availability is monitored by other means a Registration might not be necessary. Thus, using a Registrar is configurable with the following parameters:

Use Registrar	**Default: true**

With this flag registration for an ITSP is activated.
If the ITSP works without registration this flag is set to *false* and the following data are ignored.

IP Address / Host name	**Default: 0.0.0.0**

The address of the ITSP's registrar server. This can be an IP-address or the host name.

For a better flexibility ITSP's usually provide a FQDN here (e.g., sip.provider.com). If your ITSP provides you with a fixed IP address, please clarify if this is an intermediate solution or if they intend to stick to this server address.

If your provider is using geographically separated servers, each to be used in a certain location (e.g., sip-south.provider.com, sip-north.provider.com) please list all possible servers in the questionnaire contained in the test list.

Port	**Default: 5060**

Port of the ITSP registrar.

If **DNSSRV** shall be used to query IP `address:port` of the registrar, the port MUST be set to 0. (Provider proxy port must be configured with 0 as well)

In case of DNSSRV the registrar host name is usually the same as the ITSP domain name.

ReRegistration Interval at Provider (sec)	**Default(sec): 600**

Registrations must be repeated in regular intervals. The system proposes the configured interval which is sent in the expires header field. The ITSP can accept this value or answers with a different one which will be used instead.
Note: The configuration of this timer will affect the number of messages sent periodically and the time in which a loss of connection is detected. A short registration interval has the advantage that a loss of connection to the ITSP is detected after a short time, but this needs more messages to send on the interface. If a long interval is configured it takes a long time to detect the connection loss.

Note that if STUN is used it monitors the connection to the STUN server (and thus the internet connection in general). If it detects an IP address change (e.g., due to DSL reconnect) or loss of connection, it unregisters the old IP address and registers the new one at the ITSP.

Usage examples:

The configured data will be used to perform the registration of the user accounts (see also user account data 3.2)

```
REGISTER sip:RegistrarIp/HostName:RegistrarPort;transport=udp SIP/2.0
Via: SIP/2.0/UDP SystemIp:SystemPort;rport;branch=z9hG4bK122b40148b4a2d146
...
Contact:
<sip:UserAccount@SystemIp:SystemPort>;expires=Reregistrationinterval
```

The values of **SystemIp** and **SystemPort** depend on the deployment of the system. They are taken either from the IP configuration or will be determined using the STUN protocol. Other configuration parameters (see 3.3.3) will affect the message contents as well.

3.1.4 Provider Proxy

IP Address / Host name	**Default: 0.0.0.0**

The address of the ITSP's proxy server. This can be an IP-address or the host name. Please see the comments for IP Address listed for Provider Registrar too.

Port	**Default: 5060**

Port of the ITSP proxy.

If **DNSSRV** shall be used to query IP address:port of the proxy server, the port MUST be set to 0 (provider registrar must be configured with 0 as well)

In case of DNSSRV the proxy host name is usually the same as the ITSP domain name.

Usage examples:

The configured data will be used to address the ITSP's SIP server:

```
INVITE sip:+498970070@ProviderProxyIp/HostName:ProviderProxyPort SIP/2.0
To: sip: +4923026672695@ProviderProxyIp/HostName:ProviderProxyPort
```

3.1.5 Provider Outbound Proxy

In some deployments an outbound proxy is used. This is the case, when the ITSP requires for a certain domain part in the SIP headers (which is taken from the proxy configuration), but the messages must be sent to a different outbound proxy. Thus, the addresses/names in proxy and outbound proxy SHOULD be different.

Please provide additional information if you require the same addresses/names in proxy and outbound proxy.

Use Outbound Proxy	**Default: false**

With this flag usage of an outbound proxy is activated.

IP Address / Host name	**Default: 0.0.0.0**

The address of the ITSP's outbound proxy server. This can be an IP-address or the host name.

Port	**Default: 0**

Port of the ITSP outbound proxy server.
If **DNSSRV** shall be used to query the IP address of the proxy server port MUST be set to port 0.

Usage examples:

If an outbound proxy is used, all SIP messages are sent via this proxy.
Note: The SIP Request-URI and the header fields contain the data configured for SIP proxy. In addition, a Route: header field containing the outbound proxy is sent.

```
INVITE sip:+498970070@ProviderProxyIp/HostName:ProviderProxyPort SIP/2.0
Route: sip:ProviderOutboundProxyIp/HostName:ProviderOutboundProxyPort
```

3.1.6 Provider Inbound Proxy

In some rare cases an ITSP use additional server(s) for inbound traffic, which are not resolved via DNS or DNS-SRV. As the system does not allow traffic from unknown servers, such server(s) must be configured here.

The configuration of inbound proxies has no effect on the SIP protocol, they are needed to configure the "whitelist".

Use Inbound Proxy	**Default: false**

With this flag usage of an inbound proxy is activated.

IP Address / Host name	**Default: 0.0.0.0**

The address of the ITSP's inbound server. This is usually an IP-address but can be a host name as well.

A list of serves can be configured using ";" as separation character.

Usage examples:

Single inbound proxy: 10.255.241.100

multiple inbound proxy: 10.255.241.100;10.255.241.116

Port	**Default: 0**

Port of the ITSP inbound proxy server, in case of IP-addresses port should be configured (e.g., 5060) only a single port is supported.

3.1.7 Provider STUN

STUN may be needed if the system is connected via an external router. It depends on the deployment of the ITSP if STUN must be used. Some ITSP's provide so called "far end NAT traversal" where STUN is not needed to traverse the router. Thus, it must be checked with the ITSP if STUN is required and/or if a STUN server is provided.

If STUN is required for a certain provider, you MUST have a valid entry for the STUN server. A certification is NOT possible without having the information about the STUN server to be used. This STUN server might be provided by the provider itself or by a cooperation partner.

For details see Background information about STUN and Network configuration.

Use STUN	**Default: false**

With this flag the use of STUN for an ITSP is activated.

IP Address / Host name	**Default: 0.0.0.0**

The address of the STUN server. This can be an IP-address or the host name.

Port	**Default: 3478**

Port of the STUN server.

3.2 Account configuration

If an ITSP uses registration, one or more user accounts must be configured.

Two different access types are supported by OpenScape Business

- **DID / SIP Connect access**

  This type of access needs only one registration for all numbers served at the access. For this type of access one account needs to be configured. This access type is offered by most ITSPs for the SME business.

- **MSN access**

  This type of access needs a single registration for each call number. Up to 30 accounts of this access type can be configured for an ITSP. This access type is offered by most ITSPs for Home users.

	The account configuration data is provided by the ITSP. As these data are part of the registration process it is important to document the correct format of the data during the certification. Please make sure that an example of the ITSPs customer documentation is available and explain which data out of this documentation needs to be entered in the system

If an ITSP does not use registration the internal logic requires a "User" to maintain the interface parameters. Thus a "default user" must be created without any authentication information. Usually, the first call number is used to configure the User.

The following data must be entered and will be used as described in the SIP protocol.

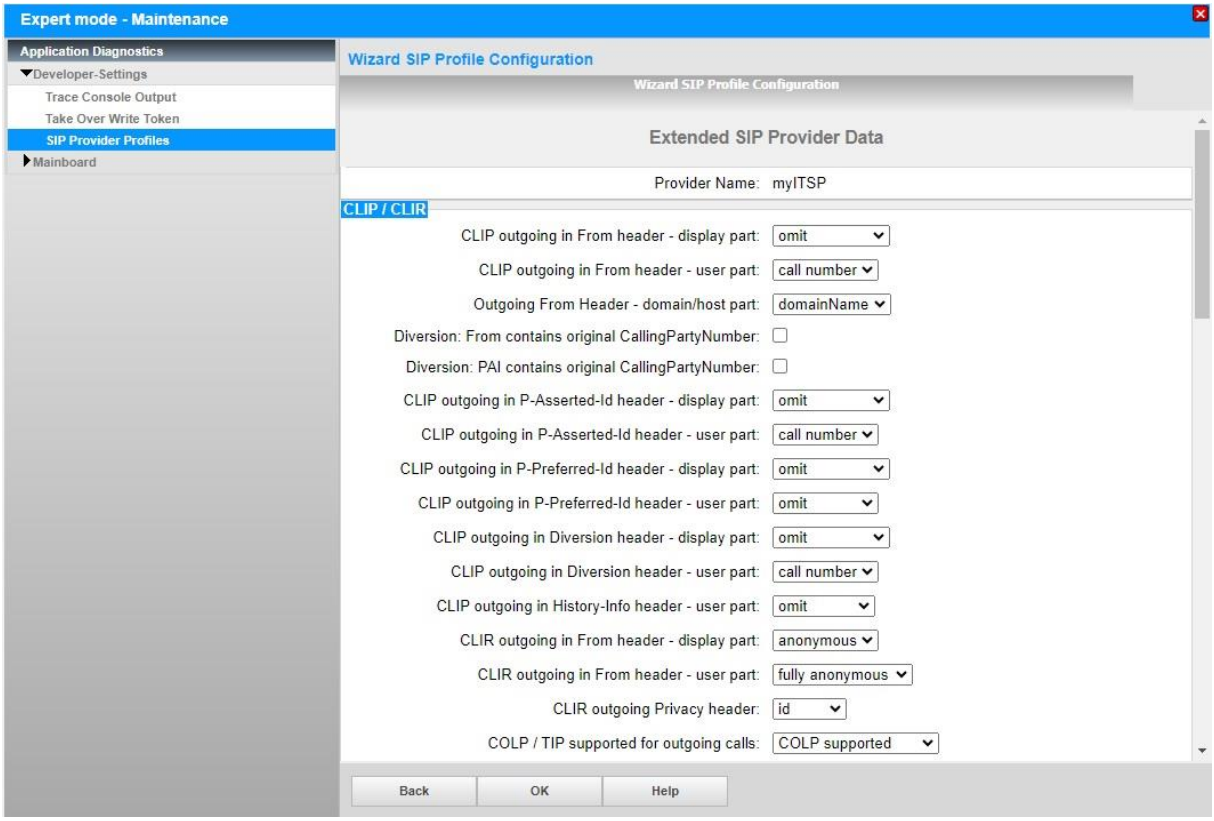
Field in WBM/Wizard	**Used in**
Internet telephony station	UserAccount Sip URI in From, To and Contact
Authorization name	UserAuthorizationName in Authorization: *Leave empty, if no extra name is needed*
Password	Used to calculate the response=CalculatedHash in Authorization

If no "Authorization name" is given, the value of "Internet telephony station" is used as username. These values must be provided by the ITSP.

Example:

```
REGISTER sip:RegistrarIp/HostName:RegistrarPort;transport=udp SIP/2.0
Via: SIP/2.0/UDP SystemIp:SystemPort;rport;branch=z9hG4bK...
From: <sip: UserAccount@RegistrarIp/HostName:RegistrarPort
To: <sip: UserAccount@RegistrarIp/HostName:RegistrarPort>
...
Contact:
<sip:UserAccount@SystemIp:SystemPort>;expires=Reregistrationinterval
Authorization: Digest username="UserAuthorizationName",
realm="ReceivedIn401", nonce="ReceivedIn401",uri="R-
URI",response="CalculatedHash",algorithm=MD5
```

3.3 Extended SIP Provider Data



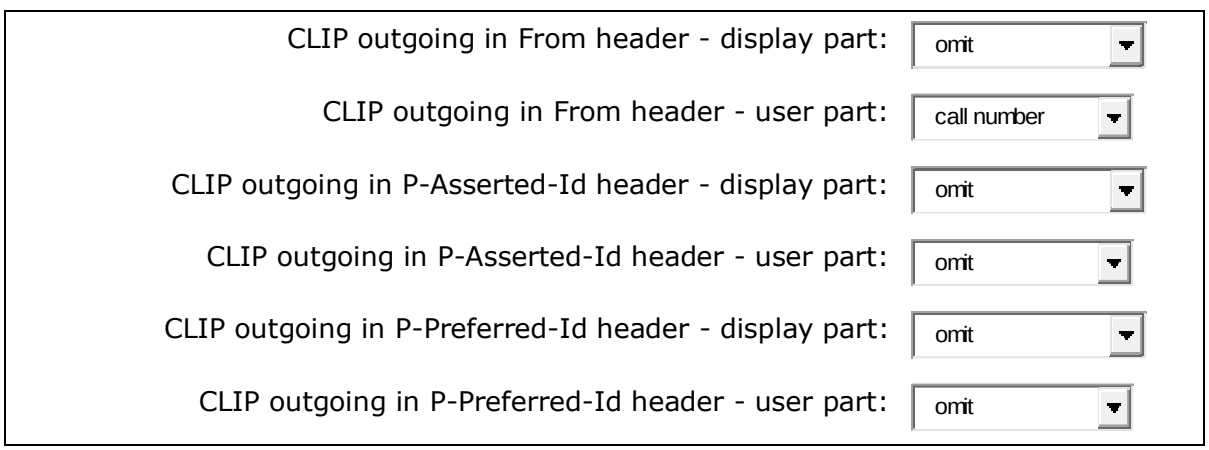
3.3.1 CLIP / CLIR

3.3.1.1 Format of From, PAI and PPI Headers for Basic Call

The system provides various profile parameters to control format of SIP header fields according to the needs of the ITSP.The contents of the following header fields which describe the source of a call can be controlled:

```
From: DisplayPart <sip:UserPart@HostPart>
P-Asserted-Identity: DisplayPart <sip:UserPart@HostPart>
P-Preferred-Identity: DisplayPart <sip:UserPart@HostPart>
```

Each header field has an own parameter to set the "display part" and the "user part" independently.



Possible settings for "display part" are:

- ***"call number"*** – the number configured in the stations CLIP/LIN field (or in the User Account data under MSN for MSN mode accounts). If stations CLIP/LIN field is not configured the station DID will be used instead.
- ***"account"*** – the user name assigned by the ITSP is sent in the format as configured in the User Account data under "Internet telephony station"
- ***"omit"*** – field is omitted
- ***"display name"*** - the string configured in the stations "Display" field

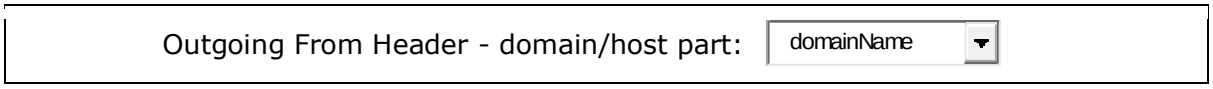
Possible settings for "user part" are:

- ***"call number"*** – the number configured in the stations CLIP/LIN field (or in the User Account data under MSN for MSN mode accounts). If stations CLIP/LIN field is not configured the station DID will be used instead.
- ***"account"*** – the user name assigned by the ITSP is sent in the format as configured in the User Account data under "Internet telephony station"

As the From header field is mandatory the "user part" cannot be omitted.

	OpenScape Business support one name for a certain station which is used internally and on the ITSP interface when display name is configured. Thus, the default setting for "display part" in ALL header fields is "omit". If you enable the "display part" in one of the header fields to provide number or account information, please provide additional information about the use case.

For some rare configurations it's possible to set the host part with the system's IP address (local IP address ***"localIPaddr"*** or public IP address ***"publicIPaddr"***). If this parameter is set it will affect the host part of all three header fields From, PAI and PPI, the default setting is: ***"domainName"***.



PPI is disabled by default. Usage of PPI is unusual, but as it is requested by some providers the system can make use of this header field too.

If the ITSP does NOT support the PAI or PPI, both "display part" AND "user part" MUST be set to **"omit"** for the header field concerned.

	Even if your provider might work with the configured default, please check carefully which options are supported. Only a correct usage of the header fields will enable the usage of the transferred addressing information for features (e.g. caller list).

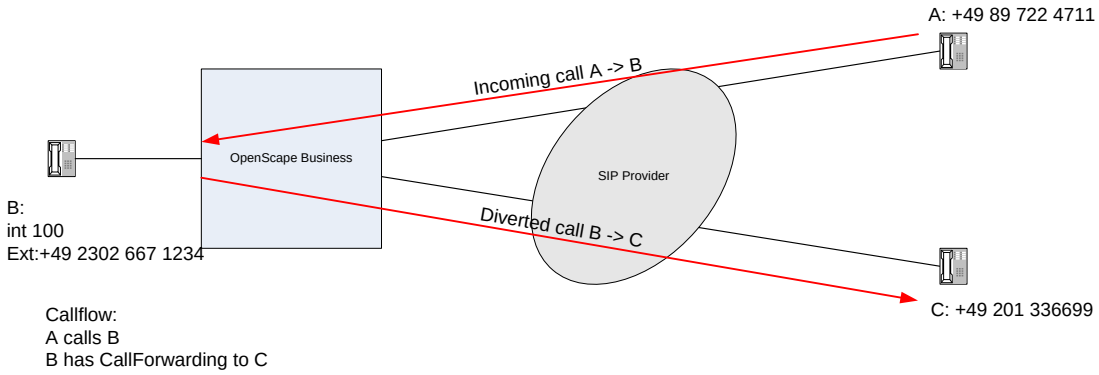
3.3.1.2 Diverted Calls: Format of From, PAI and PPI Headers

For regular outgoing calls the ITSP usually checks if the caller is allowed to place outgoing calls. This is done by means of account information provided in the outgoing INVITE as configured in 3.3.1.1.

If an outgoing call is established due to call forwarding, the system can provide information about the original calling party. Thus, two profile parameters are provided to control the contents of the From and the PAI/PPI header fields for diverted calls.

Diversion: From contains original CallingPartyNumber: ☐
Diversion: PAI contains original CallingPartyNumber: ☐

Note: The second parameter will affect the PPI header field as well



In default the From header field contains information which represents the B-Ext. (Redirecting party) and is known by the ITSP (call number/account).

Setting "From contains original CallingPartyNumber" = true causes the system to send the original calling party (A-Ext) in the From header field.

	Note: If "From contains original CallingPartyNumber" is set to true the From header format settings must be set to call number as well.

Setting "Diversion: PAI contains original CallingPartyNumber" = true causes the system to send the original calling party (A-Ext) in the P-Asserted_ID and P-Preferred-ID header field.

3.3.1.3 Diverted Calls: Format of Diversion Header

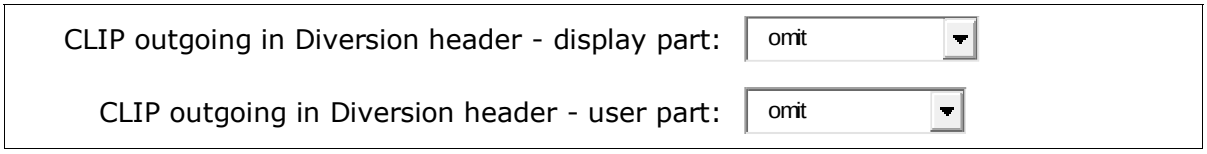
By default, the outgoing INVITE for diverted calls contains a Diversion header field. The Diversion header field always represents the Redirecting party. In default the call number is used in the "user part" and NO "display part" is sent.

```
Diversion: Display <sip:UserPart@Domainname>;reason=unconditional;counter=1
```

Example:

```
Diversion: <sip:+4923026672695@Domainname>;reason=unconditional;counter=1
```

"display part" and "user part" may be configured



If the ITSP does NOT support the diversion header field both "display part" AND "user part" MUST be set to 'omit'.

If B has invoked call number suppression (presentation restricted) the "display part" and "user part" of the diversion-header field are formatted in the same way as specified in 3.3.1.5 for the From header field in Anonymous calls.

3.3.1.4 Diverted Calls: Format of History-Info Header

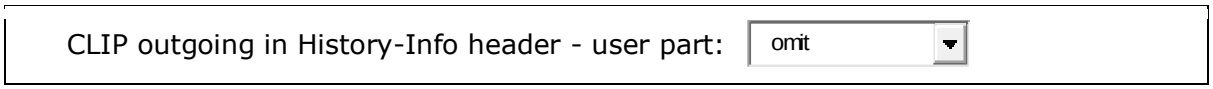
The History-Info header field represents the Redirecting party. By default the outgoing INVITE for diverted calls does not contain a History-Info header field.

```
History-Info: <sip:UserPart@Domainname;user=phone>;index = 1
```

Example:

```
History-Info: <sip:+4923026672695@Domainname;user=phone>;index = 1
```

"user part" may be configured



Possible settings for "user part" are:

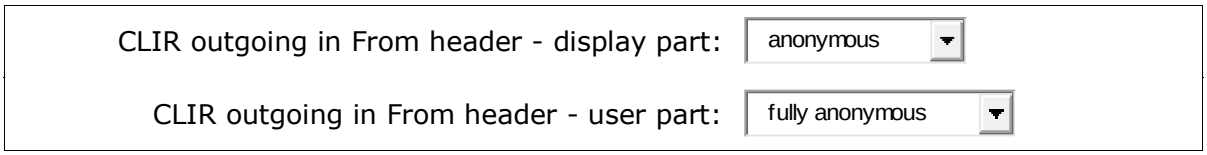
"call number"
The number configured in the stations DID field (or in the User Account data under MSN for MSN mode accounts). If stations CLIP/LIN field is configured it will be used instead of stations DID.

"omit" (default)
The History-Info field is omitted. If the ITSP does NOT support the History-Info header field "user part" MUST be set to 'omit'.

3.3.1.5 Anonymous Calls

If a user has activated call number suppression this can be signaled either in "anonymous" From header or with a privacy header when PAI is supported

The format of the anonymous From is configured:



Possible settings for "display part" are:

"omit" / ***"call number"*** / ***"account"*** / ***"anonymous"***

Possible settings for "user part" are:

"call number" / ***"account"*** / ***"fully anonymous"*** / ***"user anonymous"***

Example:

```
From: <sip:023026672695@...
From: Anonymous <sip:sip-acc1@...
From: Anonymous <sip:anonymous@anonymous.invalid
From: sip-acc1 <sip:anonymous@...
```

Another means of providing the information about call number suppression can be signaled by the presence of the Privacy header.

Possible tag-values of the Privacy Header are:

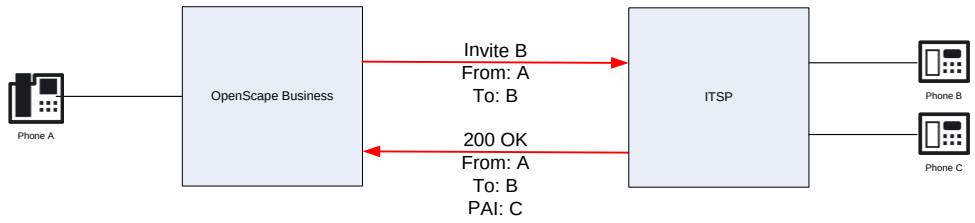
"omit" / ***"id"*** / ***"user"*** / ***"user;id"***

Example:

```
Privacy: id
Privacy: user;id
```

3.3.1.6 COLP / TIP supported

In ISDN the feature COLP (Connect Line Identification Presentation) was introduced. In SIP this feature is sometimes referred to as TIP (Termination Identification Presentation).

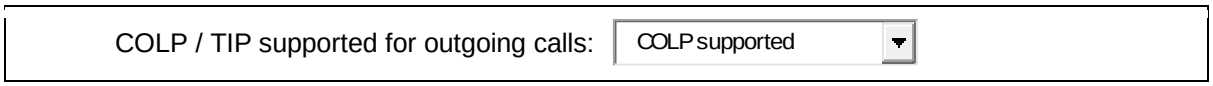


Callflow:
A calls B
C answers the call (e.g. Pickup)

RFC3324(section 5.) defines a mechanism to transport the identity of the accepting party (C) in the P-Asserted-Identity header field of the 200 OK response:

```
200 OK
   From: A
   To: B
   P-Asserted-Identity: C
```

If an ITSP does not support this feature or cannot guarantee useful information in the PAI of the 200 OK this feature should be deactivated.



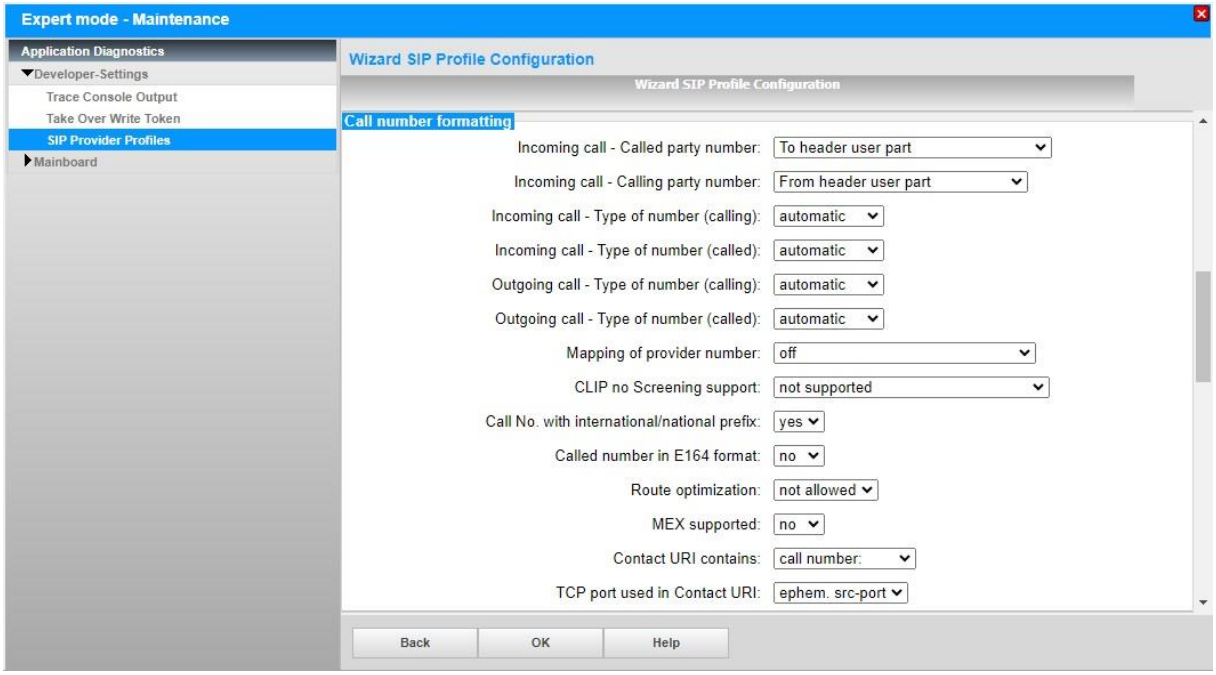
3.3.2 Call number formatting

3.3.2.1 Call numbers

As addressing of endpoints is done by call numbers, it is important to know the call number format used by the ITSP and in which format the number must be presented in the SIP messages.

OpenScape Business supports the following formats:

	Number format	Example (based on German numbering plan)
1	international E.164	+49 89 7007 4711
2	international with prefix	0049 89 7007 4711
3	implicit international without prefix	49 89 7007 4711
4	national with prefix	089 7007 4711
5	implicit national without prefix	89 7007 4711
6	unknown dialable format	089 7007 4711 **or** 0049 89 7007 4711 (no specific format is required)



3.3.2.2 Incoming calls

Various parameters are provided to control the treatment of header fields on **incoming** INVITE messages.

Incoming call – Called party number:

With this parameter it is determined where the destination address of a call is derived from. With this information the target in the system will be addressed. Depending on the "mapping mode" this must be correlated to the entries either in

- Internet telephony call number table (mapping ITSP) or
- Station DID number and corresponding route entries for prefixes

In default this is taken from the **"user part"** of the **To header** field.

```
To: +498970070 <sip:+498970070@sip.provider.de>
```

Other possible settings are:

"display part" of the **To** header field

```
To: +498970070 <sip:+498970070@sip.provider.de>
```

request line

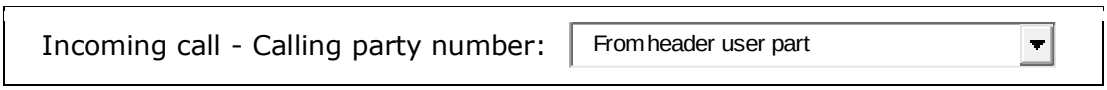
```
INVITE sip:+498970070@80.144.242.235:61901 SIP/2.0
```

"user part" or **"display part"** of **P-Called-Party-Id** header field:

```
P-Called-Party-ID: <sip:+498970070@sip.provider.de>
P-Called-Party-ID: +498970070<sip:+498970070@sip.provider.de>
```

Incoming call – Calling party number:

With this parameter it is determined where the source address is derived from.



In default the system takes the calling party out of the From header "user part".

```
INVITE sip:+498970070@80.144.242.235:61901 SIP/2.0
From: <sip:+4923026672695@sip.provider.de>
P-Asserted-Identity: <sip:+4923026672695@sip.provider.de>
```

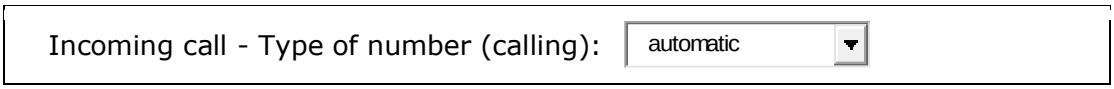
If the provider requires a special treatment here it can be determined which part of the P-Asserted-Identity or From header field should be used to derive the caller's identity.

In automatic mode the system searches first in the "user part" of the P-Asserted-Identity, if present. If no P-Asserted-Identity is present the "user part" of the From header field is taken.

For best interoperability this parameter SHALL be set to ***"From header user part"***.

Incoming call –Type of Number (calling):

With this parameter the treatment of the calling party number format is controlled.



"*automatic*" *(default)*

Used if ITSP provides the calling party number in a "dialable" format (national or international prefix is included) like 089700712345, 004989700712345 or as E.164 with leading "+" (e.g.+4989700712345).

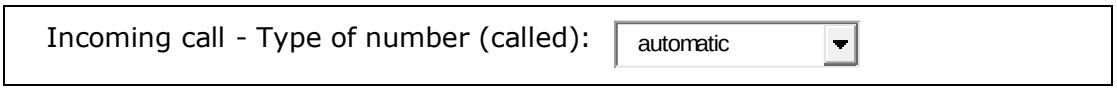
"*international*"

Used if ITSP provides an implicit international number format without international prefix (e.g. 4989700712345).

Other settings are not supported.

Incoming call –Type of Number (called):

With this parameter the treatment of the called party number format is controlled.



"*automatic*" *(default)*

Used if ITSP provides the called party number including national or international prefix (e.g. 00498970070 or 08970070) or as E.164 with leading "+" (e.g. +498970070).

"*international*"

Used if ITSP provides an implicit international number format without international prefix (e.g. 498970070).

"*national*"

Used if ITSP provides an implicit national number format without national prefix (e.g. 8970070).

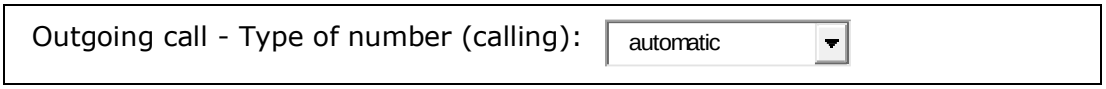
Other settings are not supported.

Tip: *Please mind that national prefix is not existing in some countries (e.g.: Greece). In case "national type of number" is preferred then "automatic" is the most appropriate choice.*

3.3.2.3 Outgoing calls

Outgoing call –Type of Number (calling):

This parameter is used for "non mapping" ITSP's only and describes the number format expected by the ITSP. If the number cannot be provided by the system in this format, the default access number is sent instead.



"*automatic*" *(default)*

Used if ITSP expects the calling party number including national or international prefix (e.g. 00498970070 or 08970070 = dialable format) or as E.164 with leading "+" (e.g. +498970070).

"*international*"

Used if ITSP expects an implicit international number format (international number without international prefix, e.g.: 4989700712345)

"*national*"

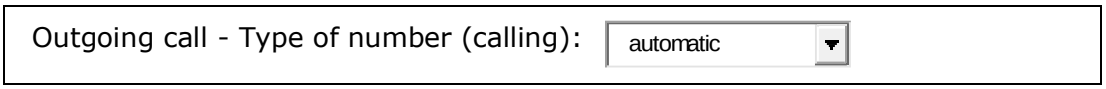
Used if ITSP expects an implicit national number format (national format without national prefix, e.g.: 89700712345)

Other settings are not supported.

Tip: *Please mind that national prefix is not existing in some countries (e.g.: Greece). In case were "national type of number" is preferred then "automatic" is the most appropriate choice.*

Outgoing call –Type of Number (called):

This parameter describes the number format of the called party number expected by the ITSP.



"*automatic*" *(default)*

Used if ITSP expects the called party number including national or international prefix (e.g. 00498970070 or 08970070 = dialable format) or as E.164 with leading "+" (e.g. +498970070).

"*international*"

Used if ITSP expects an implicit international number format (international number without international prefix, e.g.: 4989700712345)

Tip: *Please mind that national prefix is not existing in some countries (e.g.: Greece). In case "national type of number" is preferred then "automatic" is the most appropriate choice.*

Summary on call number formats and appropriate profile settings:

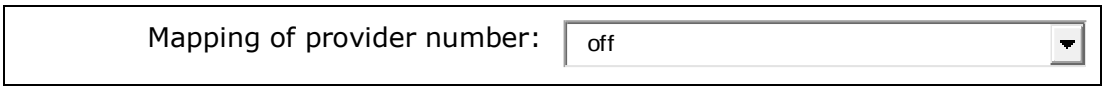
Incoming call: call number format		Incoming call Type of number (called)	Incoming call Type of number (calling)
international E.164	+49 89 7007 4711	automatic	automatic
international with prefix	0049 89 7007 4711	automatic	automatic
international without prefix	49 89 7007 4711	international	international
national with prefix	089 7007 4711	automatic	automatic
national without prefix	89 7007 4711	national	not supported

Outgoing call: calling number format		Outgoing call Type of number (calling)	Call No. With international / national prefix	E.164 Format
international E.164	+49 89 7007 4711	automatic	no	Don't care
international without prefix	49 89 7007 4711	international	no	
national without prefix	89 7007 4711	national	no	
national with prefix	089 7007 4711	automatic	yes	
international with prefix	0049 89 7007 4711	automatic	yes	

Outgoing call: called number format		Outgoing call Type of number (called)	Call No. With international / national prefix	E.164 Format
international E.164	+49 89 7007 4711	automatic	no	yes
international without prefix	49 89 7007 4711	international	no	yes
national without prefix	89 7007 4711	not supported	don't care	don't care
national with prefix	089 7007 4711	automatic	yes	no
international with prefix	0049 89 7007 4711	automatic	yes	no

3.3.2.4 Incoming and Outgoing calls

Mapping of provider call numbers:



With this parameter the use of the mapping table is controlled for incoming and outgoing direction:

"in any case"

call number is "mapped"

- incoming: received called number will be mapped
- outgoing: calling number will be mapped

"incoming called only (if configured)"

This is a special mode for the SIP-MEX feature

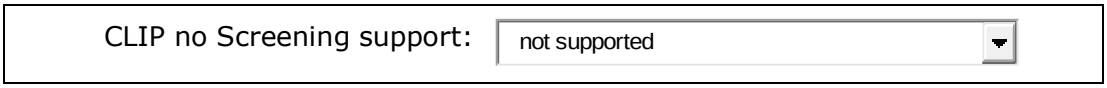
- incoming: received called number will be mapped if a matching entry exists, otherwise original (received) number will be used.
- outgoing: no call number mapping at all

"off" *(default)*

Call number will not be mapped. Use DID table instead.

CLIP no Screening support:

Providers may allow sending an "arbitrary call number" in the From header field. This feature is often named as *CLIP no screening* (CNS) and used to signal e.g. a toll-free number (0800-4711) or the A-number in case of diversion. As some providers need a call number associated with the access in the outgoing INVITE this can be configured with:



"Not supported"

ITSP does not support CLIP no Screening. In group call / ringing group scenarios the "default number" is put into the PAI and/or PPI header field.

"CLIP in From / trusted number in PAI"

ITSP allow for an arbitrary *"call number"* in the From header field if the *"default number"* is put into the PAI and/or PPI header field.

"Supported - No special treatment"

If ITSP allows for an arbitrary *"call number"* in the From header field. In group call / ringing group scenarios the "default number" is put into the PAI and/or PPI header field.

"CLIP in From / DID in PAI"

If ITSP allows for an arbitrary *"call number"* in the From header field, the DID number is put into the PAI and/or PPI header field.

	Emergency calls Emergency calls fall into the category of basic call. Providing the DID of the station in PAI/PPI by specifying the actual number of the caller must be configured according to the ITSP requirements.

Prerequisites:

- ITSP MUST be configured with "Mapping of provider number" = "off"
- A "default number" MUST be present for the ITSP
- The DID/CLIP tables as well as the route parameters MUST be configured consistently.

	Note: If "*CLIP no Screening support*" is set to "*CLIP in From / trusted number in PAI*" the From, PAI and/or PPI header format settings MUST be set to "*call number*". The parameter "*Diversion: PAI contains original CallingPartyNumber*" MUST not be set.

Example:

A subscriber is configured with

DID number: +498970074711
CLIP number: **+498001234567** (the toll-free service group number)
ITSP Default number: +498970071111

With ***"CLIP in From / trusted number in PAI"*** the following INVITE will be sent:

```
INVITE sip:123456@provider SIP/2.0
From: <sip:+498001234567@provider>;tag=6a05084..
To: sip:123456@provider
P-Asserted-Identity: sip:+498970071111@provider
```

This INVITE will be processed by the provider, as he can check the validity of the call based on the contents of the PAI header.

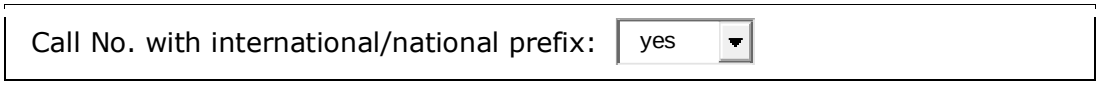
With ***"not supported"*** the following INVITE will be sent:

```
INVITE sip:123456@provider SIP/2.0
From: <sip:+498001234567@provider>;tag=6a05084..
To: sip:123456@provider
P-Asserted-Identity: sip:+498001234567@provider
```

(Note: Header contents depends on other format settings as well)

Call Number with international/national prefix:

This parameter used by the ITSP wizard to set the corresponding Route parameter in the ITSP route.



"yes"

call number includes the configured prefix value (e.g. 00492302… or 02302…)

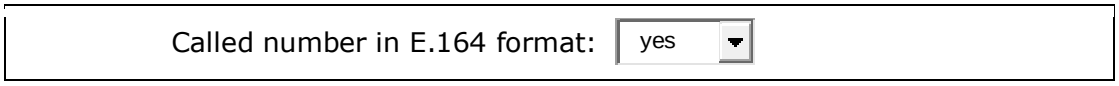
"no"

call number does NOT include the configured prefix value (e.g. +492302… or 492302 or 2302…)

	Changing this parameter in the ITSP profile itself has no immediate effect on the route. This parameter needs to be defined in the profile to allow automatic route configuration when running through the ITSP wizard.

Called number in E164 format:

More and more ITSP expect to receive the called party number in canonical E.164 format. With the flexible and powerful LCR configuration OpenScape Business is prepared for this requirement. To avoid manual configuration, this parameter is used by the ITSP wizard to setup the corresponding LCR rules.



"yes"

LCR is configured with dialing rules for canonical E.164 format (default, local, national and international rules provided)

e.g.	dial	sent to ITSP
local number	230798	+4989230798
national number	089230798	+4989230798
international number	004989230798	+4989230798

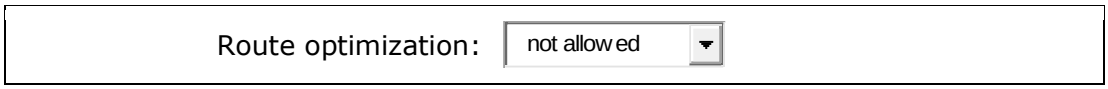
"no"

LCR is configured with default dialing rules (default and local rule is provided).

	Changing this parameter in the ITSP profile itself has no immediate effect on the LCR. This parameter needs to be defined in the profile to allow automatic LCR configuration when running through the ITSP wizard.

Route optimization:

This parameter is used by the Setup-Wizard to activate call deflection with a 302 response sent on the SIP trunk.

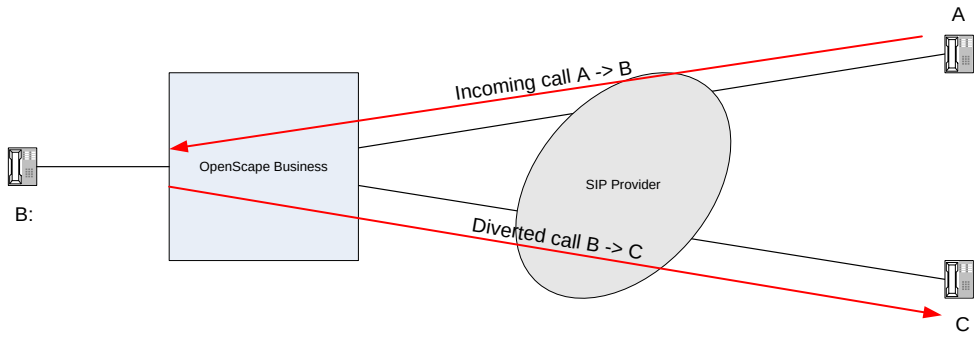


"not allowed"

In default call forwarding is performed by initiating a new call (Forward switching)

+ call management can be used after call forwarding is initiated

- two ITSP channels are used when call is active

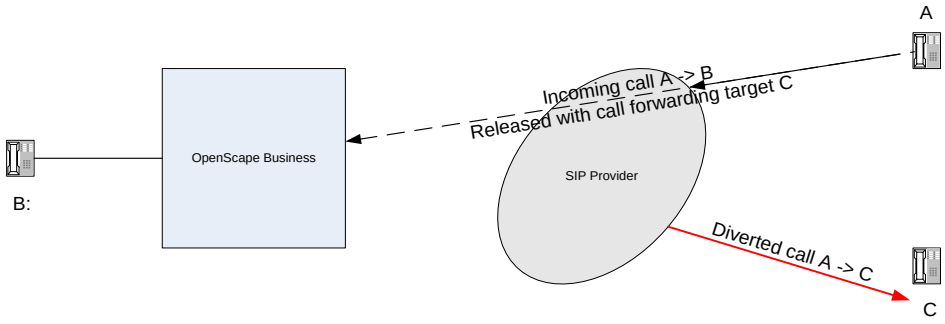


"allowed"

When Route optimization is allowed call forwarding is performed by sending a 302 response.

+ no ITSP channel used when call is active

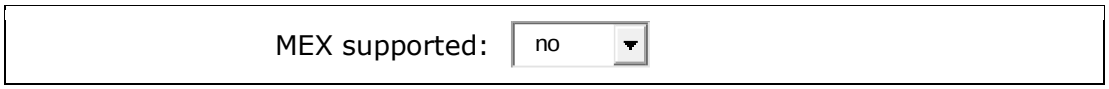
- no control of the call when call deflection is initiated



	Changing this parameter in the ITSP profile itself has no immediate effect. This parameter needs to be defined in the profile to allow the selection or rerouting in the ITSP wizard.

MEX supported:

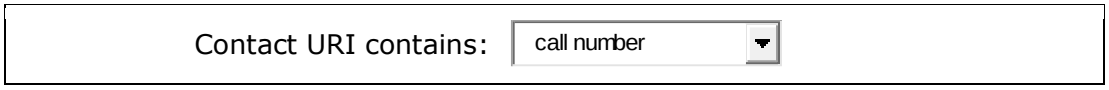
This parameter is used by the Setup-Wizard to display the configuration of the MEX numbers.



Contact URI contains:

This parameter is used to configure the "user part" content of the contact-URI

```
Contact: sip:UserPart@HostPart
```



"Call number"

In default the "user part" of the Contact URI contains the call number.

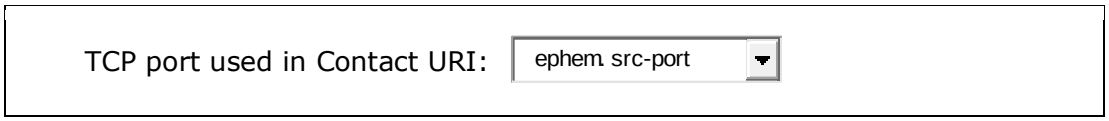
"Registration AOR"

As an alternative the Contact URI can be configured to include the Registration AOR (account=user part for registration) regardless of the configuration of the content of the From header field.

TCP port used in Contact URI

This parameter is used to configure the tcp-port used in the host part of the contact-URI

```
Contact: sip:UserPart@HostPart:port
```



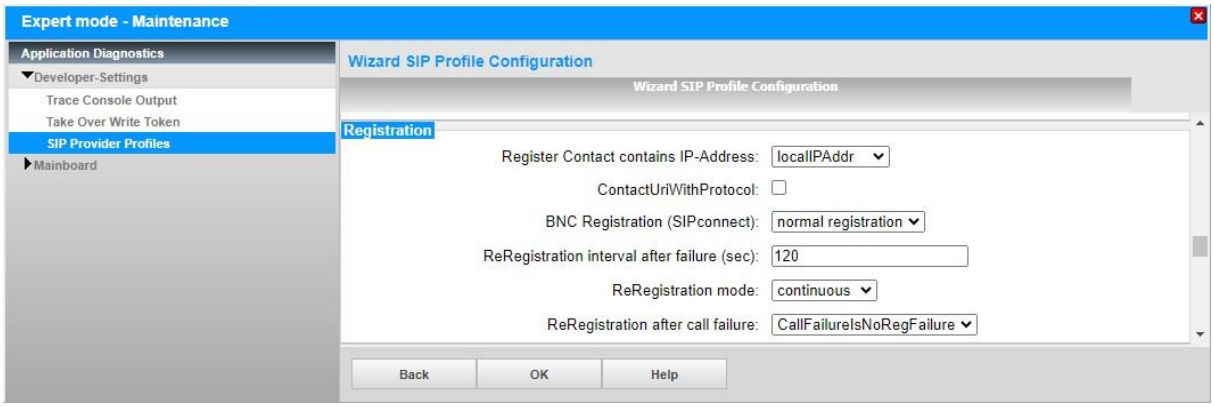
"ephem. src-port"

In default the ephemeral tcp src port is used. As the connection to the ITSP is established by the OpenScape Business system it is expected that all SIP signaling traffic is transported on this connection.

"SIP server port"

Some ITSP want to have the OpenScape Business SIP server port listed in the contact-URI. If ITSPs need this kind of signaling, it must be assured that the SIP Server port is reachable (e.g. firewall needs to be opened)

3.3.3 Registration



Used Contact Address in REGISTER

Register Contact contains IP-Address:	localIPAddr

IP-Address (localIPAddr) or domain name (domainName) may be set in the hostPart of the sipUri in the Contact header in REGISTER.

```
Contact: <sip:…@192.168.138.1:5060>;…
Contact: <sip:…@sip.provider.de>;…
```

For ITSPs this parameter MUST be set to IP-Address if the ITSP uses the contact address for addressing purposes. If the ITSP does not use the contact address (e.g., works without STUN) both settings are valid and should be set to the needs of the ITSP.

	If STUN is activated the publicIPAddr is used for the Contact header instead of the localIPAddr.

Additional parameters in contact-URI

ContactUriWithProtocol: ☐

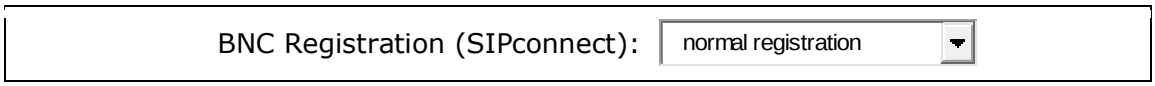
Used to add the 'OwnSecurity' parameter in the Contact header of REGISTER. This is propriatary information used in the UNIFY networking protocol.

```
Contact: <sip:..@..>;transport=tcp;+u.www.siemens.com/icn/en/oscar/…
```

	For ITSPs this parameter SHOULD be set to false. If it is needed for enhancements in the networking protocol this parameter may change without any notice to external partners.

If you need to set this parameter, please provide additional information about the use of this header field parameter.

BNC registration (SIPconnect1.1)



With this parameter the format of the REGISTER will be set to the format specified for SIP-Connect1.1 including two new header fields included in the REGISTER message:

```
Require: gin
Proxy Require: gin
```

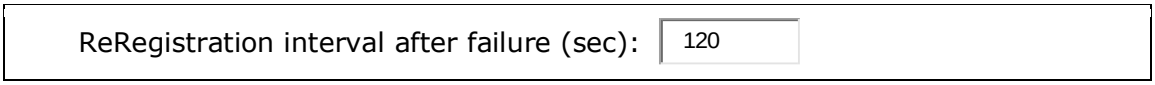
The supported header field must include the path option tag:

```
Supported: path
```

In addition the contact header field has to include a URI without a "user part" and the IP-Address of the PBX and the "bnc" parameter

```
Contact: <IP-Addr;bnc>
```

ReRegistration interval after failure

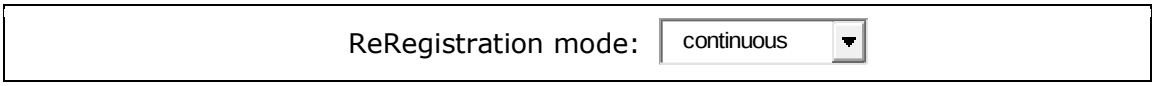


With this parameter the time between detection of a registration failure and the next registration attempt is controlled.

The timerinterval should be 30 sec < reregtime < 3600 sec

The default timeout is 120 sec (= 2 min)

Reregistration behaviour (SIPconnect 1.1)



"Continuous"

Reregistration is started after expiry of the Reregistration timer specified above. (default 120 sec)

"SIPConnect"

SIPConnect 1.1 requires the following behavior: If no SP-SSE is reachable, or no alternates are available, the SIP-PBX MUST delay reattempting Registration for 30 seconds and increasing this delay value by doubling it for each successive delivery failure until delivery succeeds, up to a maximum value of 960 seconds. (30 – 60 – 120 – 240 – 480 – 960)

With this parameter the time between detection of a registration failure and the next registration attempt is controlled.

ReRegistration after call failure (SIPconnect 1.1)

ReRegistration after call failure: CallFailureIsNoRegFailure

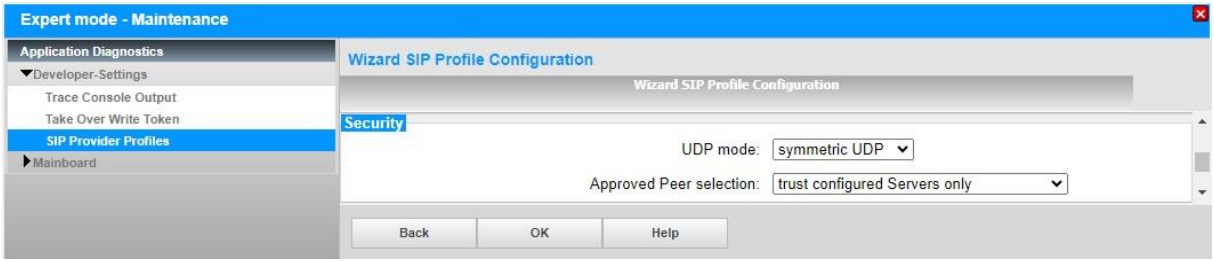
With this parameter the registration behaviour after a detection of a failure in call signaling is controlled:

If set to "CallFailureIsRegFailure" the following will be triggered:

On timer expiry (408) or receiving a 403 response for any non-REGISTER request, the system must assume that the SIP-PBX's registration is no longer active at the SP-SSE and has to start a re-registration.

In default the system will treat a call signaling failure not as a registration failure.

3.3.4 Security related



For security reasons OpenScape Business has an integrated *Session Border Controller* https://wiki.unify.com/wiki/OpenScape_Business#Integrated_Session_Border_Controller

which controls the access to the system. One of the filter functions is based on IP addresses and port numbers. The following configuration settings may be used to adapt the security measures.

UDP mode of operation:

When using UDP transport an IP port filter is used to discard unwanted traffic

UDP mode: symmetric UDP

"symmetric UDP"

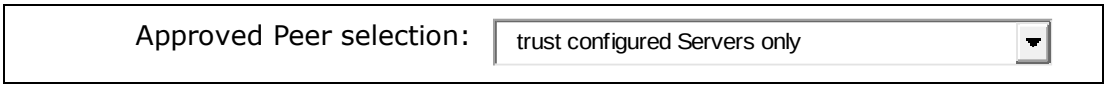
In symmetric mode of operation all received SIP are checked for the correct source-port. E.g. SIP server is configured with port 5060. In symmetric mode of operation only messages with source-port 5060 are accepted.

"asymmetric UDP"

In asymmetric mode of operation the port number is not checked. Received SIP messages are accepted from the any port.

Approved Peer selection:

The IP address filter function uses a table with all configured SIP servers (whitelist). This table is filled by the configured IP addresses or in case of DNS or DNS-SRV with the addresses retrieved from the DNS server responses.



"trust configured Servers only"

fill address filter table with configured IP addresses and DNS/DNS-SRV responses only (proxy, registrar, outbound proxy, inbound proxy)

"trust Servers received in SIP responses"

In addition to configured IP addresses and DNS/DNS-SRV responses the address filter table is filled with server addresses received in contact: and/or Record-Route: header fields from trusted proxies.

Example:

Proxy is configured and resolved to **90.158.44.243:5060**.

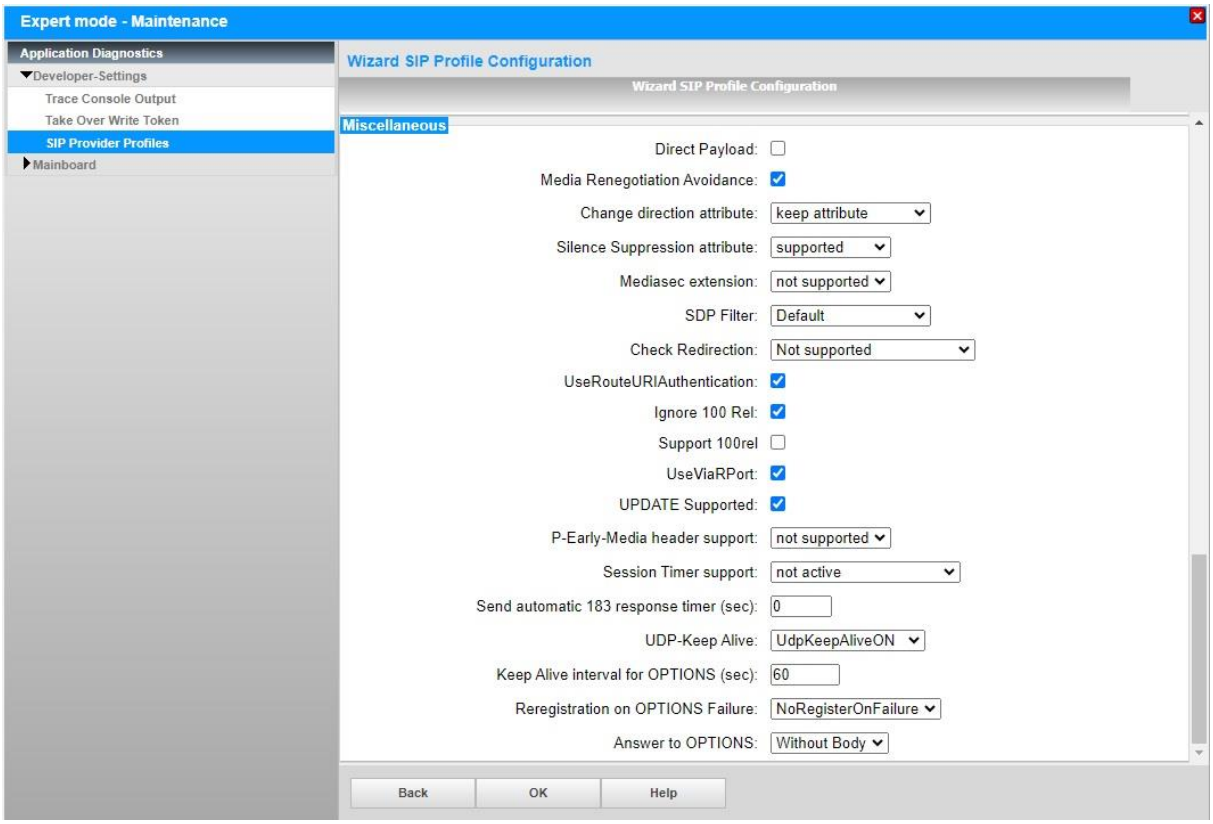
Outgoing Invite is sent to ITSP. ITSP answers with a response including a contact header with a different address:

```
INVITE sip:902523110601@90.158.44.243:5060 SIP/2.0
Via: SIP/2.0/UDP 62.134.46.4:53460;branch=z9hG4bK0755.ce..

SIP/2.0 200 OK
From:..
Contact: <sip:902123663900@90.158.44.233:5067>
```

The system will now sent requests (e.g. reINVITE, BYE) to the server addressed in the contact header. If this server is not resolved via DNS, the parameter "Approved Peer selection" MUST be set to "trust Servers received in SIP responses" to allow receiving messages from this address.

3.3.5 Miscellaneous



3.3.5.1 Media handling

Direct Payload

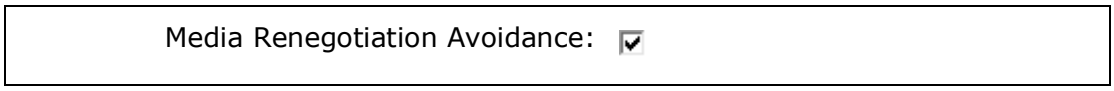
Direct Payload: ☐

Usually in SIP networks payload is transported end-to-end. ITSP's are usually located in the public internet whereas the OpenScape Business is located in a private local network. Thus, routing of the payload between public and local addresses needs SBC functionality. For this purpose, OpenScape Business uses the integrated SBC function to manage the media exchanged with the ITSP.

For a direct ITSP connection this parameter MUST be set to false.

If an external SBC is used in front of the OpenScape Business this parameter is set to true.

Media Renegotiation Avoidance



During feature invocation media renegotiation is used to establish a new media path if necessary. A lot of ITSP do not like to be exposed with such reInvite messages. The internal SBC function is able to avoid sending media renegotiations if only `IP-Addresses:Ports` are changed.

For a direct ITSP connection this parameter MUST be set to true.

If the media handling parameter **Direct Payload** is set to true, this parameter has NO effect. (e.g., in cases where an external SBC is used in front of the OpenScape business system)

Change direction attribute

This is a parameter to adapt the MOH signaling to specific ITSP requirements which do provide MOH in their own platform regardless of received MOH from the PBX.

This parameter is used to manipulate the SDP direction attribute when a reInvite is sent to the ITSP in case of MOH.

"keep attribute"

If a reInvite needs to be sent, the direction attribute is sendonly for MOH. This is the recommended default setting

"change to sendrecv"

If a reInvite needs to be sent, the direction attribute is sendrecv for MOH. With this setting the ITSP does not get a "HOLD-indication".

Silence Suppression attribute

Some ITSPs do not allow the presence of the `a=silenceSupp` attribute in SDP.

The following parameter is used to control the processing of the SDP attribute line `a=silenceSupp:off - - - -`

"supported" *(default)*

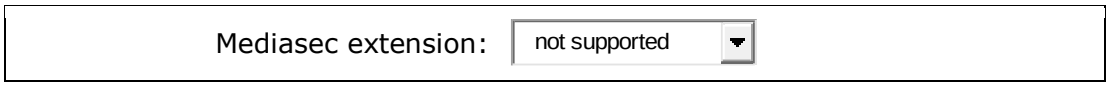
attribute line is kept unchanged in SDP

"not supported"

attribute line is deleted from SDP before sending it to ITSP

Mediasec extension

With this parameter the mediasec extensions are enabled. These extensions are required by Deutsche Telekom to establish secure calls. The extensions are defined in the 1TR119 specification. If this value is set to supported additional mediasec parameters are used in REGISTER and INVITE requests. The SDP for secure calls includes the `a=3ge2ae:requested` attribute.



"not supported" *(default)*

mediasec extensions are disabled

"supported"

mediasec extensions are enabled

SDP Filter

Due to the increasing complexity of networks, we have observed interoperability issues with different ITSPs. To avoid issues related to SDP handling a filter is implemented in the integrated SBC function. In default all ITSPs are restricted to the use of the codecs supported by the system endpoints (G7.11, G.729 and G.722).

Available profiles are:

- Default G.711, G.729, G.722, CLEARMODE
- Compatibility G.711, CLEARMODE
- open no SDP filtering

Ignore received 100 Rel in INVITE

Ignore 100 Rel: ☑

Ignore a 'Supported: 100rel' header field if received in INVITE.

Because 100rel may interfere with interworking to non-SIP subscribers, this parameter SHOULD be set to true.

Support 100 Rel

If a provider requires to change media addresses during call establishment phase reliable provisional responses must be used.

Support 100 Rel: ☐

When setting this flag, the system will add a supported 100rel header in the outgoing invite. This will allow the ITSP to send reliable provisional responses followed by UPDATE messages.

	Note: When using reliable provisional responses, the system does NOT support a change of media capabilities in the early dialog phase other the IP-Address and port.

Currently the system does not fully support a media change in the call establishment phase. Consequently, in default no 100rel tag is included in the Supported header field.

	Please contact the Atos Unify representative to clarify the exact needs.

3.3.5.2 Parameter for Authentication

UseRouteURIAuthentication

UseRouteURIAuthentication: ☑

True sets the behavior for using the Route URI instead of the request URI in the (Proxy-) Authorization header for INVITE or INFO (not for REGISTER). The request URI will be used when no Route URI is present.

For ITSPs this parameter MUST be set to true.

3.3.5.3 Routing parameter

UseViaRPort

Add rport-parameter in Via header field.

UseViaRPort: ☑

If set to true, the rport parameter is added to Via-Header.

```
Via: SIP/2.0/UDP 192.168.138.1:5060;rport;
```

If set to false, no rport parameter is added to Via-Header.

```
Via: SIP/2.0/UDP 192.168.138.1:5060;
```

RFC3581 defines a 'rport' parameter for the Via header:

" .. When used with UDP, responses to requests are returned to the source address the request came from, and to the port written into the topmost Via header field value of the request. This behavior is not desirable in many cases, most notably, when the client is behind a Network Address Translator (NAT). … "rport" allows a client to request that the server send the response back to the source IP address and port from which the request originated."

3.3.5.4 Supported methods and procedures

With the parameters in this section the used methods on the SIP interface can be controlled.

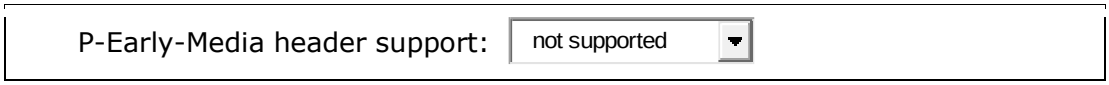
UPDATE Supported

If set to true UPDATE is used depending on the contents of the Allow header field. If UPDATE is not set in the Allow header field received, the SIP stack never sends an UPDATE.

If set to false, the UPDATE method will never be used (a re-INVITE is used instead of this)

For ITSP this parameter SHALL be set to true (default)

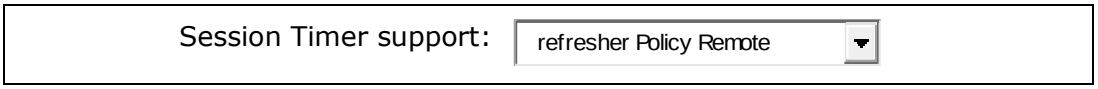
P-Early-Media header supported



If set to supported, the system will add a "P-Early-Media: supported" header field in outgoing initial INVITE requests.

When receiving 18x provisional responses containing a P-Early-Media: header field this is processed and used to control rendering early media.

Session Timer support



"not active"

If set to "not active" the system will not request for session timer actively.

"refresher Policy Remote"

If set to "refresher Policy Remote" the system will request for session refreshes performed by the ITSP. The "session limit" can be configured in the global SIP settings (default is 1800 sec = 30 min)

It depends on the ITSP if SessionTimer should be supported or not.

3.3.5.5 Special procedures

Check redirection

"not supported" (default)

If set to "not supported" the system will not check for History-Info and Referred-By header.

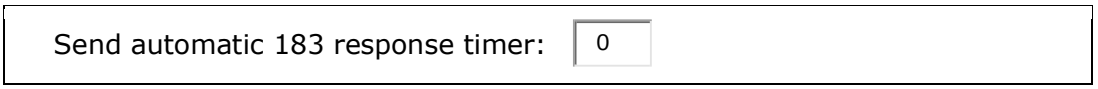
"History-Info + Referred-By"

If set to "History-Info + Referred-By" the system will check for History-Info and Referred-By header.

"History-Info"

If set to "History-Info" the system will check for History-Info and Referred-By header.

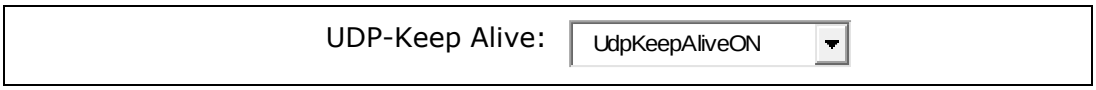
Automatic 183 responses to initial INVITE request



With this timer a provisional response (183) is triggered after timeout if no progress information is available from the system. This is necessary because some platforms do not stop supervision timers when receiving a 100 trying (e.g., Broadsoft)

0	no automatic response is sent; all responses are triggered by the system
1-10	timeout in sec, timer is started on receiving an INVITE request from the ITSP. On timer expiry a 183 is sent out by the SIP stack.

Send UDP-Keep alive packets



With this parameter the Keep Alive functionality of the system is controlled. Keep alive can be used for different purposes:

If the system is located behind a firewall, special measures are needed to keep the firewall open, so that the external SIP server can reach the OpenScape business system from the internet.

If no registration is used a different means of checking the path to the server may be necessary.

"UdpKeepAliveOFF"

If set to "*UdpKeepAliveOFF*" the system will not send UDP packets on the SIP signaling port.

"UdpKeepAliveON"

If set to "UdpKeepAliveON" the system will send "empty" UDP packets to the SIP signaling port of the SIP server (one or many depending on DNS results) in regular intervals (15 sec) from the SIP signaling port.

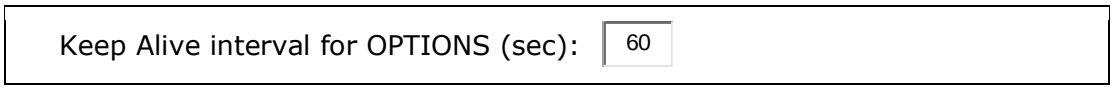
Some ITSP treat these empty packets as a SIP error or SIP attack. In such a case the UDP keep alive must be switched of and the firewall has to be opened by configuration

This option has no effect if TCP/TLS transport is used.

"SendAliveOptions"

If set to "SendAliveOptions" the system will send SIP OPTIONS messages in regular intervals defined with the Keep Alive Interval. This option is primarily used for ITSP using TCP transport.

Keep Alive interval for OPTIONS (sec)



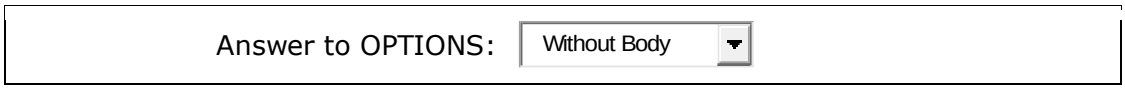
With this parameter the interval for sending SIP OPTIONS is defined.

ReRegistration on OPTIONS Failure

When OPTIONS are used for Keep Alive these checks can be used to trigger a reregistration.

If set to "RegisterOnFailure" a re-registration is triggered when OPTIONS are not answered. This mechanism is used for UPD transport only.

Answer to OPTIONS



If the system receives an OPTIONS request the content of the body in the response is controlled with this parameter

"Without Body"

The 200 OK response is sent without the SDP body.

"Full Answer"

The 200 OK response is sent including the SDP body.

4 Restrictions

Due to different reasons, OpenScape Business does not support some features, which may be offered by an ITSP.

Please check the **OpenScape Business V3 General Configuration Guides for ITSP** documents in Wiki for known restrictions:

https://wiki.unify.com/index.php/Collaboration_with_VoIP_Providers#General_Configuration_guides

5 References

Further related information can be found under the following links:

Reference		Hyperlink
[1]	Administration Documentation	Online Help in OpenScape Business Assistant
[2]	Diagnostic hints	Administration Documentation
[3]	Experts Wiki	https://wiki.unify.com/index.php/OpenScape_Business
[4]	OpenScape Business Security Checklist	https://nuxeo.unify.com/nuxeo/site/proxy/nxdoc/view/raw/b2efab60-4ba8-491c-988d-870077267c4a
[5]	How To connect Unify Phone	https://wiki.unify.com/images/7/7f/How_To_connect_Unify_Phone_to_OpenScape_Business.pdf
[6]	How To MS Teams Interworking	https://wiki.unify.com/images/4/4f/How_To_Configure_OSBiz_MS_Teams_Interworking.pdf
[7]	How To Skype for Business Teams Interworking	https://wiki.unify.com/images/3/31/How_To_Configure_OSBiz_Skype_for_Business_Interworking.pdf
[8]	"How to collection" for H4k and OSV networking	https://wiki.unify.com/wiki/How_to_collection_and_tutorials_for_OpenScape_Business#Networking
[9]	Device@Home – configuration	https://wiki.unify.com/images/d/de/How_To_Configure_System_Device%40Home.pdf
[10]	SIP@Home – configuration	https://wiki.unify.com/images/8/8c/OSBiz_V2_SIP_Endpoint_Configuration_for_SIP%40Home.pdf