NETFON
DATENTECHNIK
TELEKOMMUNIKATION

Anleitung

Einrichtung "UPC Trunk - Internet Static IP" für Unify OpenScape Business V2

A. Dokumentklassifikation

Public

B. Versions Kontrolle

Version	Geändert von	Datum	Bemerkungen
1.0	A. Cavegn	04.11.2019	Dokumenterstellung

C. Zweck und Abgrenzung

Im Dokument werden die Schritte für die Verbindung eines UPC SIP Trunk via Internet Registration in Verbindung mit einer Unify OpenScape Business erläutert. Informationen zur benötigten Hardware, Lizenzen sowie System-Grundkonfigurationen entnehmen Sie den entsprechenden System Handbüchern.

D. Produkte

Telefonanlage

Hersteller	Unify
Produkt	OpenScape Business X / S
Version	V2 R7.1.0 oder höher

SIP Trunk

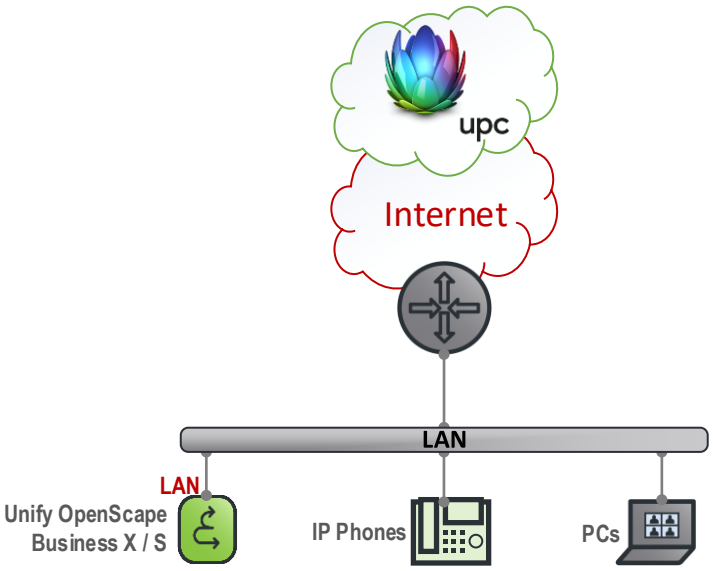
Service Provider	UPC Schweiz GmbH
Produkt	Premium Voice IP
Ausprägung	Internet Static IP

Inhaltsverzeichnis

Netfon Solutions AG
Badenerstrasse 329, Postfach, 8040 Zürich
Telefon 044 497 11 11
Telefax 044 497 11 12
E-Mail info@netfon-solutions.ch
Internet www.netfon-solutions.ch

1 Generelle Angaben

1.1 Lösungsaufbau



1.2 Voraussetzungen

- OpenScape Business hat den SW-Stand V2 R7.1.0 oder höher
- Telefonanlage ist über die LAN Schnittstelle in das Kundennetzwerk integriert und hat transparenten Zugriff auf das Internet
- Port Forwarding wurde auf Router/Firewall für den Port 5060 auf die IP Adresse der Telefonanlage erstellt.
- Erstinstallation- und Basisinstallation-Wizard wurden bereits durchgeführt
- Eine gültige Lizenz wurde bereits in das System geladen
- Die SIP Trunk Informationen stehen zur Verfügung

1.3 Unterstützte Funktionen

Fax	√ Fax over G.711 (empfohlen) √ Fax T.38 (nicht empfohlen)
Codecs	√ G.711 a-law √ G.711 u-law
CLIP	√
CLIP no Screening	√ (Optional, muss vom Service-Provider aktiviert werden)
CLIR	√
COLP	√
Call Forwarding (weiterleiten von A-Nummer zum C-Teilnehmer)	√

Netfon Solutions AG
Badenerstrasse 329, Postfach, 8040 Zürich
Telefon 044 497 11 11
Telefax 044 497 11 12
E-Mail info@netfon-solutions.ch
Internet www.netfon-solutions.ch

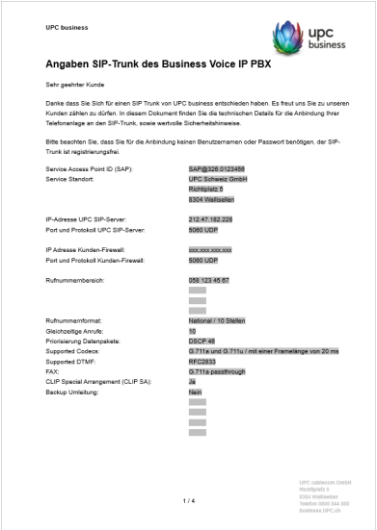
DTMF	√

1.4 Bekannte Einschränkungen

Call Forwarding (SIP Response 302)	- Wird nicht unterstützt

1.5 Für die Konfiguration notwendige Informationen

1.5.1 Angaben SIP-Trunk des Business Voice IP PBX



UPC business

Angaben SIP-Trunk des Business Voice IP PBX

Sehr geehrter Kunde

Danke dass Sie Sich für einen SIP Trunk von UPC business entschieden haben. Es freut uns Sie zu unseren Kunden zählen zu dürfen. In diesem Dokument finden Sie die technischen Details für die Anbindung Ihrer Telefonanlage an den SIP-Trunk, sowie wertvolle Sicherheitshinweise.

Bitte beachten Sie, dass Sie für die Anbindung keinen Benutzernamen oder Passwort benötigen, der SIP-Trunk ist registrierungsfrei.

Service Access Point ID (SAP):	SAP@326.0123456
Service Standort:	UPC Schweiz GmbH Richtistrasse 5 8304 Wallisellen
IP-Adresse UPC SIP-Server:	212.47.182.228
Port und Protokoll UPC SIP-Server:	5060 UDP
IP Adresse Kunden-Firewall:	xxx.xxx.xxx.xxx
Port und Protokoll Kunden-Firewall:	5060 UDP
Rufnummernbereich:	058 123 45 67
Rufnummernformat:	National / 10 Stellen
Gleichzeitige Anrufe:	10
Priorisierung Datenpakete:	DSCP:46
Supported Codecs:	G.711a und G.711u / mit einer Framelänge von 20 ms
Supported DTMF:	RFC2833
FAX:	G.711a passthrough
CLIP Special Arrangement (CLIP SA):	Ja
Backup Umleitung:	Nein

1 / 4

UPC business

Der SIP Trunk von UPC unterstützt folgende Funktionen:

- TCP oder UDP (nach Absprache mit UPC)
- SIP: RFC 3543 und 3261
- SIP Privacy: id, RFC 3323
- P-Asserted-Identity/Remote-Party-ID
- Diversion Header
- SIP OPTIONS (keep-alive)
- DTMF RFC 2833
- Codec
  - 1. Prio G.711a-law (mit einer Framelänge von 20ms)
  - 2. Prio G.711u-law (mit einer Framelänge von 20ms)
- Fax: G.711a pass-through

Folgende Funktionen werden nicht unterstützt:

- Refer
- Update
- Info
- P-Preferred Identity
- TLS/SRTP

Sicherheitseinstellungen

Mit über 1000 SIP Trunks in Betrieb konnten wir viele Erfahrungen sammeln und wir empfehlen Ihnen, dass Sie nur SIP und RTP Pakete von der IP Adresse 212.47.182.228 zulassen.

Wir empfehlen Ihnen folgende Firewall Einstellungen vorzunehmen:

Regel	Quell-IP Adresse	Ziel-IP Adresse / Port
SIP	212.47.182.228 / alle Ports	Lokale IP Adresse Telefonanlage / SIP Port
RTP	212.47.182.228 / alle Ports	Lokale IP Adresse Telefonanlage / RTP Portrange

Um Missbrauch vorzubeugen haben wir ein Informationsblatt zur Sicherheit von Telefonanlagen zusammen gestellt, welches Sie ab Seite 2 finden. Bitte lesen Sie dieses aufmerksam durch.

Bei Fragen, Unklarheiten und Änderungswünschen kontaktieren Sie bitte Ihren technischen Ansprechpartner von dem Sie diese Angaben erhalten haben.

Freundliche Grüsse

UPC – Voice Network und Services

PBX Security Whitepaper DE 20120922 2 / 4 19. September 2012

1.5.2 Informationsblatt zur Sicherheit von Telefonanlagen

UPC Business

Informationsblatt zur Sicherheit von Telefonanlagen

IT-Manager und IT-Fachabteilungen müssen sich vermehrt mit der IT-Sicherheit und im Speziellen auch mit dem Schutz von Telefonanlagen (TK-Anlagen) gegen Missbrauch befassen. Dabei stellt sich die Frage, welche Vorkehrungen getroffen werden müssen, um Schaden abzuwenden. Nachfolgend finden Sie einige wichtige Informationen.

Worum geht es?

PBX-Hacker, Freaks und Shoulder-Surfer - das sind nur ein paar Bezeichnungen für jene Personen, die fremde Telefonanlagen für ihre Zwecke missbrauchen und so die betroffenen Unternehmen weltweit jedes Jahr Millionen kosten. Solche Angriffe wurden unter dem Namen „Toll Fraud» (Gebührenbetrug) bekannt und sind für viele Unternehmen ein echtes Problem. Einige Schweizer Unternehmen beispielsweise wurden in diesem Jahr bei einem Angriff während rund 24 Stunden um insgesamt über 50 000 Schweizer Franken betrogen. Ihre Telefonanlage war manipuliert worden; die Hacker hatten eine Unmenge von Anrufen auf Kosten der nichts ahnenden Unternehmen getätigt.

Was ist «Toll Fraud»?

Toll Fraud ermöglicht Betrügern, sich auf Kosten Anderer zu bereichern: Ein Hacker wählt sich über einen Fernwartungszugang ein und kann so auf eine ungeschützte TK-Anlage zugreifen.
Typischerweise wählt er dann zu Lasten des betroffenen Unternehmens kostenpflichtige Mehrwertnummern im Ausland an, wofür er von den Betreibern der Mehrwertnummern später einen Anteil der aufgelaufenen Gebühren zurück erhält. Manche Hacker haben auch lediglich die Absicht, dem Ruf des Unternehmens zu schaden.

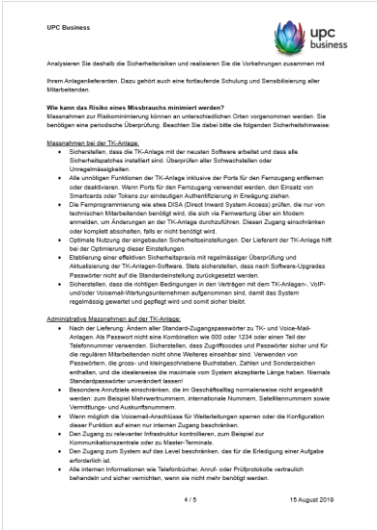
Wer ist betroffen?

Hacker unterscheiden in der Regel nicht zwischen kleinen und grossen Unternehmen. Alle TK-Anlagen ohne geeignete Sicherheitsmassnahmen können zum Ziel werden. Die Angriffe erfolgen bei herkömmlichen, über ISDN- oder E1-Leitungen verbundene TK-Anlagen, aber auch bei neueren, über SIP-Verbindungen angeschlossene IP-TK-Anlagen.
Oft starten die Kriminellen ihre Aktivität am Anfang eines Wochenendes, also zu einem Zeitpunkt, zu dem der Missbrauch mit grosser Wahrscheinlichkeit lange unbemerkt bleibt. Der Angriff dauert meistens an, bis der Missbrauch entdeckt und unterbunden wird. Das kann sich auch über mehrere Tage hinziehen. Wenn Unternehmen die Nutzungsdaten der Telefonanlage nur am Monatsende kontrollieren, kann sich dies sogar über Wochen erstrecken und somit erhebliche Kosten verursachen!

Wer trägt die durch Missbrauch entstandenen Telefonkosten?

Die Verantwortung des Betriebs der Telefonanlage liegt – vorbehältlich einer anderslautenden Servicevereinbarung mit UPC - beim Kunden oder seinem Anlagelieferanten. Anruf- und Gesprächsgebühren, die durch Missbrauch der Telefonanlage entstanden sind, werden wie normale Telefonkosten verrechnet und dem Kunden in Rechnung gestellt. Wichtig ist darum, frühzeitig alle erforderlichen Vorkehrungen gegen einen Missbrauch zu treffen - dies ist Aufgabe des Anlagenlieferanten.
UPC business hat ihrerseits zusätzlich Massnahmen eingriffen, um bei betroffenen Unternehmen allfälligen Schaden zu begrenzen. So werden beispielsweise in den Aufzeichnungen des Telefonie-Verkehrs auffällige Muster automatisch herausgefiltert, damit Kunden frühzeitig auf einen potentiellen Missbrauch aufmerksam gemacht und notwendige Schritte eingeleitet werden können. Dadurch lässt sich ein Schaden im besten Fall begrenzen, aber Missbrauch nicht grundsätzlich verhindern.

3 / 5 15 August 2019



UPC Business

Analysieren Sie deshalb die Sicherheitsrisiken und realisieren Sie die Vorkehrungen zusammen mit

Ihrem Anlagenlieferanten. Dazu gehört auch eine fortlaufende Schulung und Sensibilisierung aller Mitarbeitenden.

Wie kann das Risiko eines Missbrauchs minimiert werden?

Massnahmen zur Risikominimierung können an unterschiedlichen Orten vorgenommen werden. Sie benötigen eine periodische Überprüfung. Beachten Sie dabei bitte die folgenden Sicherheitshinweise:

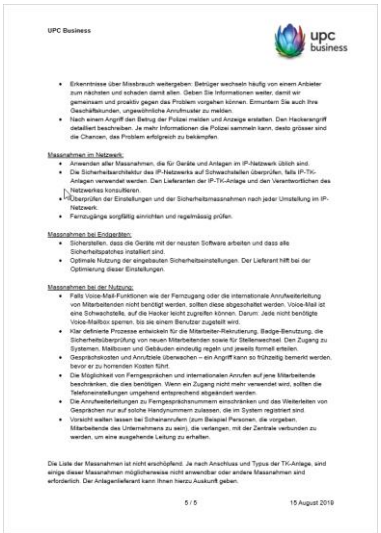
Massnahmen bei der TK-Anlage:

- Sicherstellen, dass die TK-Anlage mit der neusten Software arbeitet und dass alle Sicherheitspatches installiert sind. Überprüfen aller Schwachstellen oder Umsetzmässigkeiten.
- Alle unnötigen Funktionen der TK-Anlage inklusive der Ports für den Fernzugang entfernen oder deaktivieren. Wenn Ports für den Fernzugang verwendet werden, den Einsatz von Smartcards oder Tokens zur eindeutigen Authentifizierung in Erwägung ziehen.
- Die Fernprogrammierung wie etwa DISA (Direct Inward System Access) prüfen, die nur von technischen Mitarbeitenden benötigt wird, die sich via Fernwartung über ein Modem anmelden, um Änderungen an der TK-Anlage durchzuführen. Diesen Zugang einschränken oder komplett abschalten, falls er nicht benötigt wird.
- Optimale Nutzung der eingebauten Sicherheitseinstellungen. Der Lieferant der TK-Anlage hilft bei der Optimierung dieser Einstellungen.
- Etablierung einer effektiven Sicherheitspraxis mit regelmässiger Überprüfung und Aktualisierung der TK-Anlagen-Software. Stets sicherstellen, dass nach Software-Upgrades Passwörter nicht auf die Standardeinstellung zurückgesetzt werden.
- Sicherstellen, dass die richtigen Bedingungen in den Verträgen mit dem TK-Anlagen-, VoIP- und/oder Voicemail-Wartungsunternehmen aufgenommen sind, damit das System regelmässig gewartet und gepflegt wird und somit sicher bleibt.

Administrative Massnahmen auf der TK-Anlage:

- Nach der Lieferung: Ändern aller Standard-Zugangspasswörter zu TK- und Voice-Mail-Anlagen. Als Passwort nicht eine Kombination wie 000 oder 1234 oder einen Teil der Telefonnummer verwenden. Sicherstellen, dass Zugriffscodes und Passwörter sicher und für die regulären Mitarbeitenden nicht ohne Weiteres einsehbar sind. Verwenden von Passwörtern, die gross- und kleingeschriebene Buchstaben, Zahlen und Sonderzeichen enthalten, und die idealerweise die maximale vom System akzeptierte Länge haben. Niemals Standardpasswörter unverändert lassen!
- Besondere Anrufziele einschränken, die im Geschäftsalltag normalerweise nicht angewählt werden: zum Beispiel Mehrwertnummern, internationale Nummern, Satellitennummern sowie Vermittlungs- und Auskunftsnummern.
- Wenn möglich die Voicemail-Anschlüsse für Weiterleitungen sperren oder die Konfiguration dieser Funktion auf einen nur internen Zugang beschränken.
- Den Zugang zu relevanter Infrastruktur kontrollieren, zum Beispiel zur Kommunikationszentrale oder zu Master-Terminals.
- Den Zugang zum System auf das Level beschränken, das für die Erledigung einer Aufgabe erforderlich ist.
- Alle internen Informationen wie Telefonbücher, Anruf- oder Prüfprotokolle vertraulich behandeln und sicher vernichten, wenn sie nicht mehr benötigt werden.

4 / 5 15 August 2019



UPC Business

- Erkenntnisse über Missbrauch weitergeben: Betrüger wechseln häufig von einem Anbieter zum nächsten und schaden damit allen. Geben Sie Informationen weiter, damit wir gemeinsam und proaktiv gegen das Problem vorgehen können. Ermuntern Sie auch Ihre Geschäftskunden, ungewöhnliche Anrufmuster zu melden.
- Nach einem Angriff den Betrug der Polizei melden und Anzeige erstatten. Den Hackerangriff detailliert beschreiben. Je mehr Informationen die Polizei sammeln kann, desto grösser sind die Chancen, das Problem erfolgreich zu bekämpfen.

Massnahmen im Netzwerk:

- Anwenden aller Massnahmen, die für Geräte und Anlagen im IP-Netzwerk üblich sind.
- Die Sicherheitsarchitektur des IP-Netzwerks auf Schwachstellen überprüfen, falls IP-TK-Anlagen verwendet werden. Den Lieferanten der IP-TK-Anlage und den Verantwortlichen des Netzwerkes konsultieren.
- Überprüfen der Einstellungen und der Sicherheitsmassnahmen nach jeder Umstellung im IP-Netzwerk.
- Fernzugänge sorgfältig einrichten und regelmässig prüfen.

Massnahmen bei Endgeräten:

- Sicherstellen, dass die Geräte mit der neusten Software arbeiten und dass alle Sicherheitspatches installiert sind.
- Optimale Nutzung der eingebauten Sicherheitseinstellungen. Der Lieferant hilft bei der Optimierung dieser Einstellungen.

Massnahmen bei der Nutzung:

- Falls Voice-Mail-Funktionen wie der Fernzugang oder die internationale Anrufweiterleitung von Mitarbeitenden nicht benötigt werden, sollten diese abgeschaltet werden. Voice-Mail ist eine Schwachstelle, auf die Hacker leicht zugreifen können. Darum: Jede nicht benötigte Voice-Mailbox sperren, bis sie einem Benutzer zugeteilt wird.
- Klar definierte Prozesse entwickeln für die Mitarbeiter-Rekrutierung, Badge-Benutzung, die Sicherheitsüberprüfung von neuen Mitarbeitenden sowie für Stellenwechsel. Den Zugang zu Systemen, Mailboxen und Gebäuden eindeutig regeln und jeweils formell erteilen.
- Gesprächskosten und Anrufziele überwachen – ein Angriff kann so frühzeitig bemerkt werden, bevor er zu horrenden Kosten führt.
- Die Möglichkeit von Ferngesprächen und internationalen Anrufen auf jene Mitarbeitende beschränken, die dies benötigen. Wenn ein Zugang nicht mehr verwendet wird, sollten die Telefoneinstellungen umgehend entsprechend abgeändert werden.
- Die Anrufweiterleitungen zu Ferngesprächsnummern einschränken und das Weiterleiten von Gesprächen nur auf solche Handynummern zulassen, die im System registriert sind.
- Vorsicht walten lassen bei Sicherannrufern (zum Beispiel Personen, die vorgeben, Mitarbeitende des Unternehmens zu sein), die verlangen, mit der Zentrale verbunden zu werden, um eine ausgehende Leitung zu erhalten.

Die Liste der Massnahmen ist nicht erschöpfend. Je nach Ansichtuss und Typus der TK-Anlage, sind einige dieser Massnahmen möglicherweise nicht anwendbar oder andere Massnahmen sind erforderlich. Der Anlagenlieferant kann Ihnen hierzu Auskunft geben.

5 / 5 15 August 2019

Netfon Solutions AG
Badenerstrasse 329, Postfach, 8040 Zürich
Telefon 044 497 11 11
Telefax 044 497 11 12
E-Mail info@netfon-solutions.ch
Internet www.netfon-solutions.ch

2 Einrichtung

2.1 Netzwerk-Konfigurationen

Damit der SIP-Trunk konfiguriert werden kann, muss vorab der Zugang zum Internet konfiguriert werden. Diese Konfiguration unterscheidet sich bei den Systemen OpenScape Business X und S.

Folgende Punkte sind dabei zu beachten:

- Gültige **IPv4 Adresse** und dazugehörige **Subnetz-Maske**
  OSBiz S: *Suse Yast > Network Devices > Network Services*
  OSBiz X: *OSBiz WBM > Experten-Modus > Netzwerkschnittstellen*
- Korrektes **Default Gateway**
  OSBiz S: *Suse Yast > Network Devices > Network Services*
  OSBiz X: *OSBiz WBM > Experten-Modus > Routing*
- Gültiger **DNS** Server
  OSBiz S: *Suse Yast > Network Devices > Network Services*
  OSBiz X: *OSBiz WBM > Experten-Modus > Routing*
- Gültiger **NTP** Server
  OSBiz S: *Suse Yast > Network Services > NTP Configuration*
  OSBiz X: *OSBiz WBM > Experten-Modus > Grundeinstellungen > Datum und Uhrzeit*

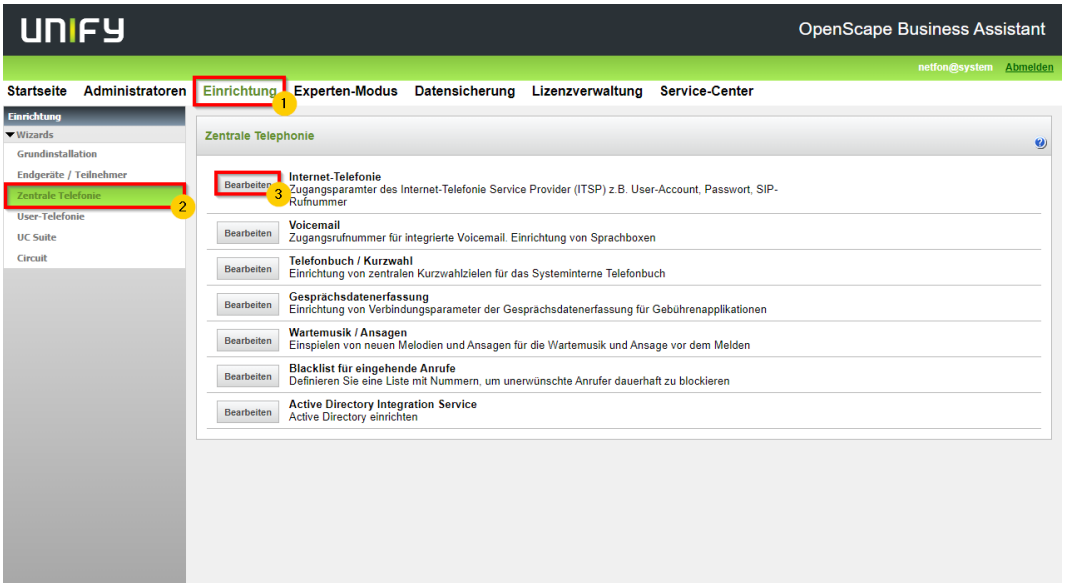
2.2 SIP Trunk Konfiguration mit dem Einrichtungsassistent

Sobald die ‚OpenScape Business' Zugriff auf das Internet hat, kann mit der Einrichtung des SIP Trunks begonnen werden.

Internet –Telefonie Wizard

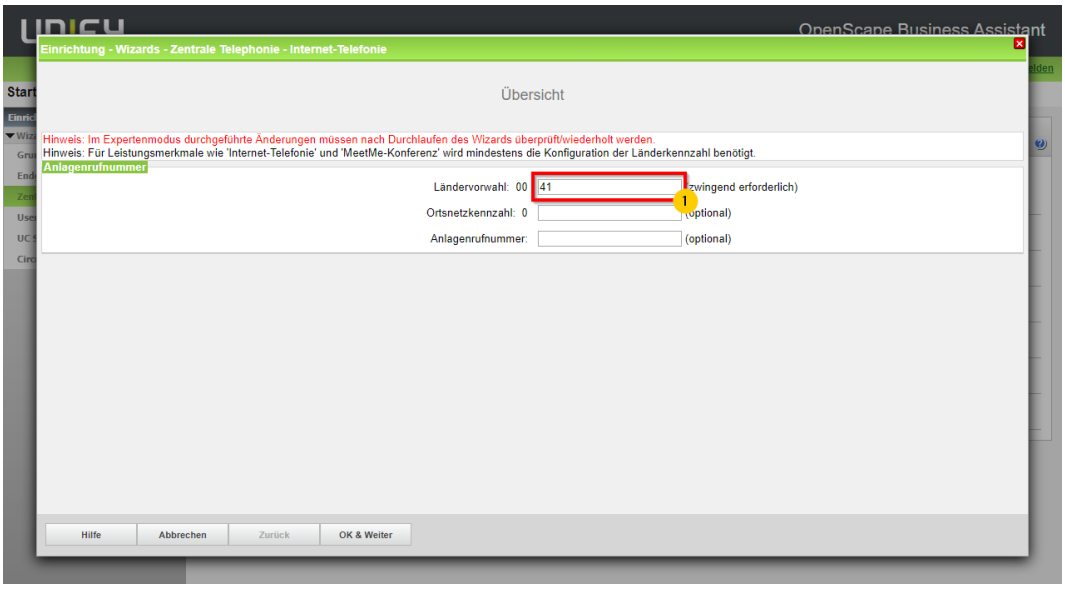
Navigieren Sie zum ‚Internet-Telefonie Wizard' und klicken Sie auf Bearbeiten:

1. Einrichtung
2. Zentrale Telefonie
3. Internet-Telefonie

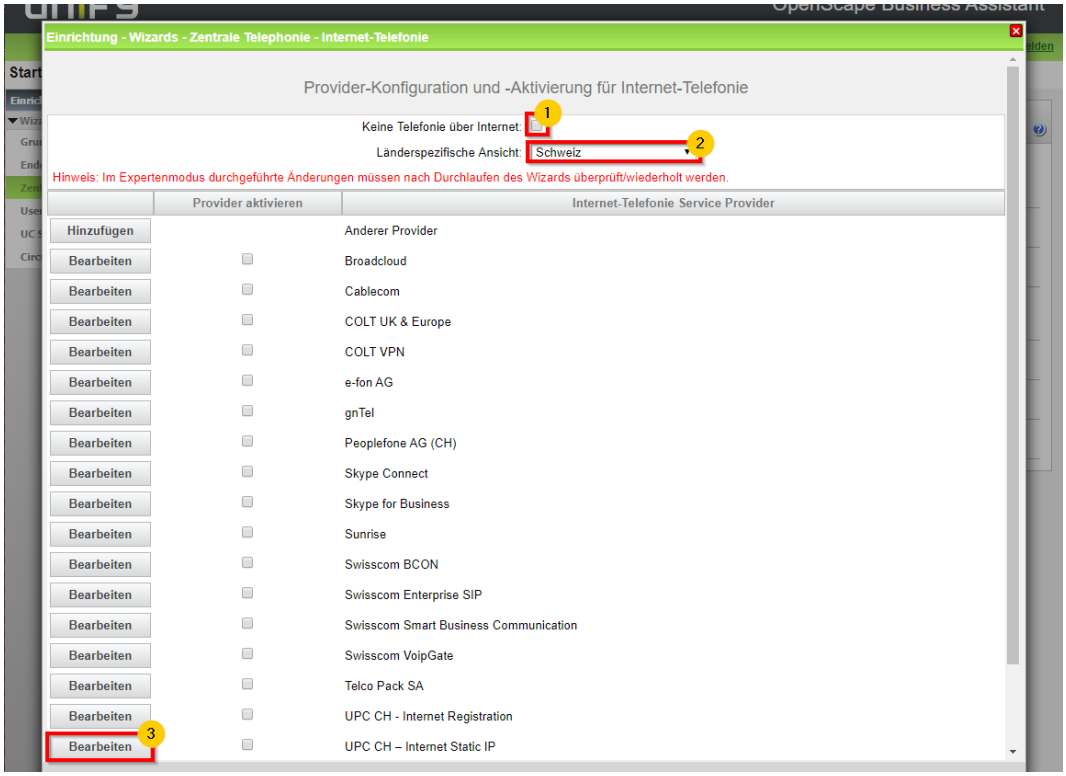


Netfon Solutions AG
Badenerstrasse 329, Postfach, 8040 Zürich
Telefon 044 497 11 11
Telefax 044 497 11 12
E-Mail info@netfon-solutions.ch
Internet www.netfon-solutions.ch

1. Für eine korrekte Funktion muss die **Ländervorwahl** angegeben werden.
   Je nach Einrichtung der Teilnehmer, kann eine **Ortskennzahl** und eine **Anlagenrufnummer** angegeben werden.

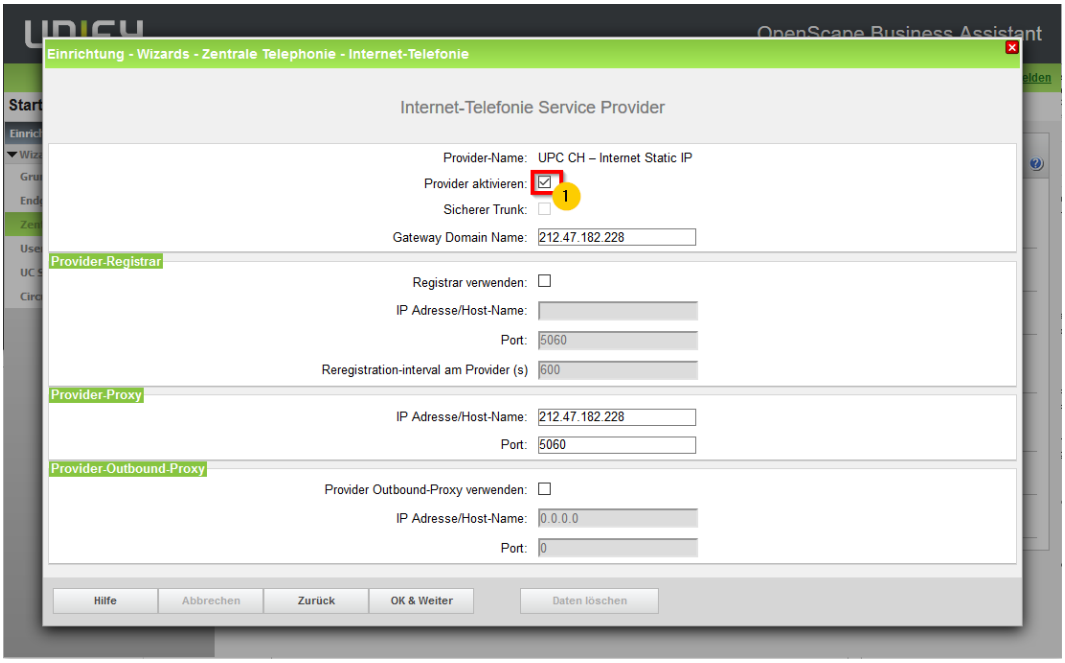


1. Deaktivieren Sie den Punkt ‚**Keine Telefonie über Internet**'.
2. Überprüfen Sie, dass die ‚**Länderspezifische Ansicht**' auf **Schweiz** eingestellt ist.
3. **Scrollen** Sie runter bis zum Punkt ‚**UPC CH – Internet Static IP**'

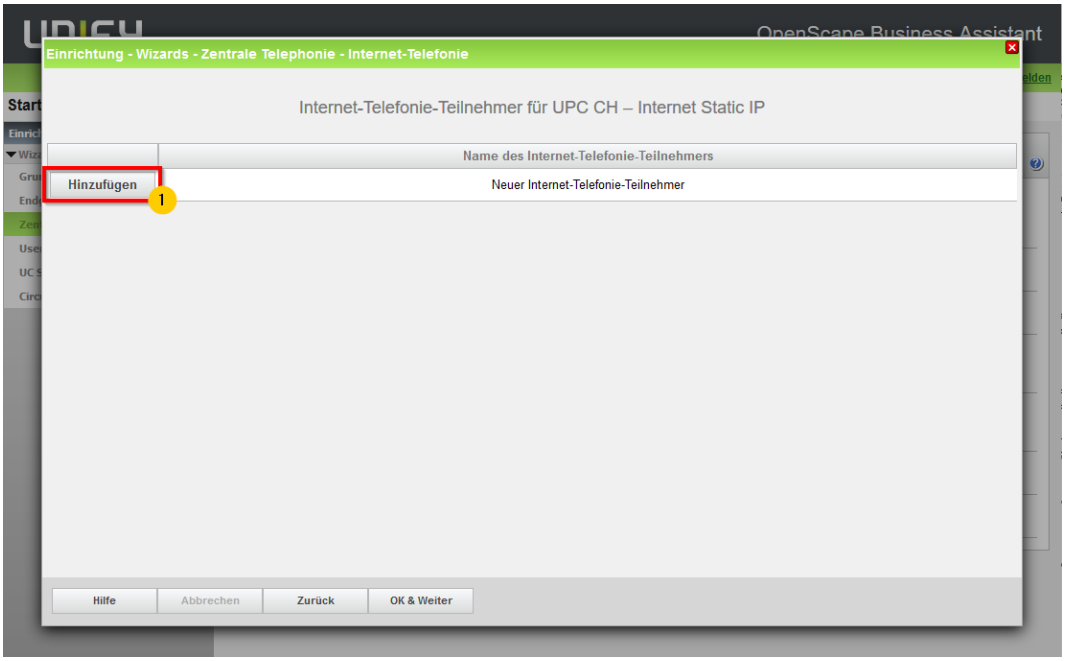


Netfon Solutions AG
Badenerstrasse 329, Postfach, 8040 Zürich
Telefon 044 497 11 11
Telefax 044 497 11 12
E-Mail info@netfon-solutions.ch
Internet www.netfon-solutions.ch

1. Aktivieren Sie den Punkt ‚**Provider aktivieren**‘.

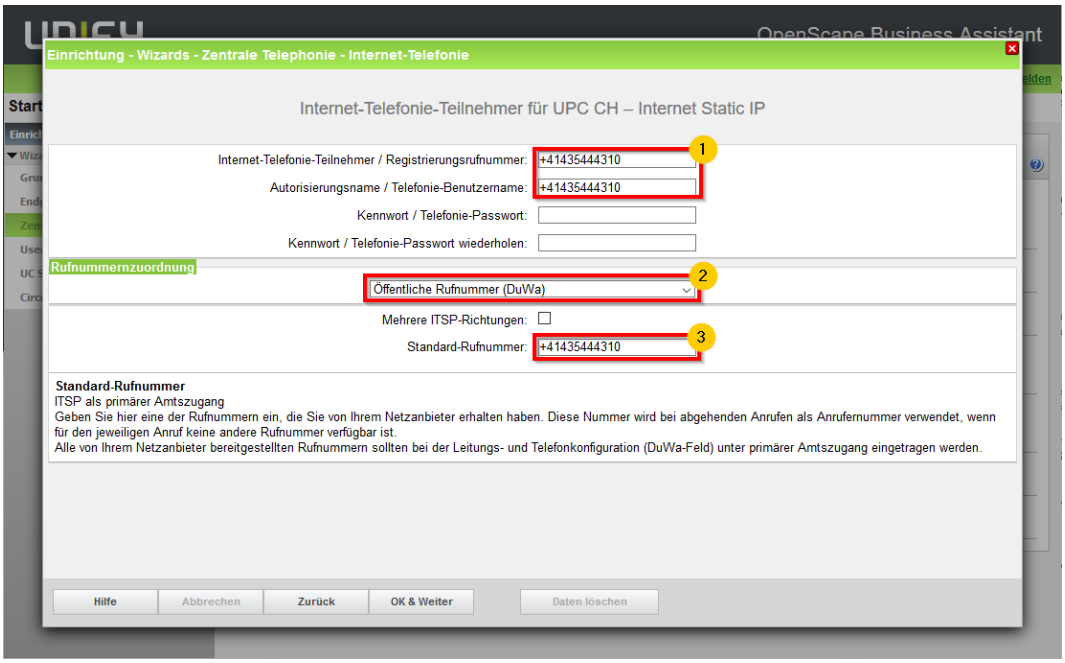


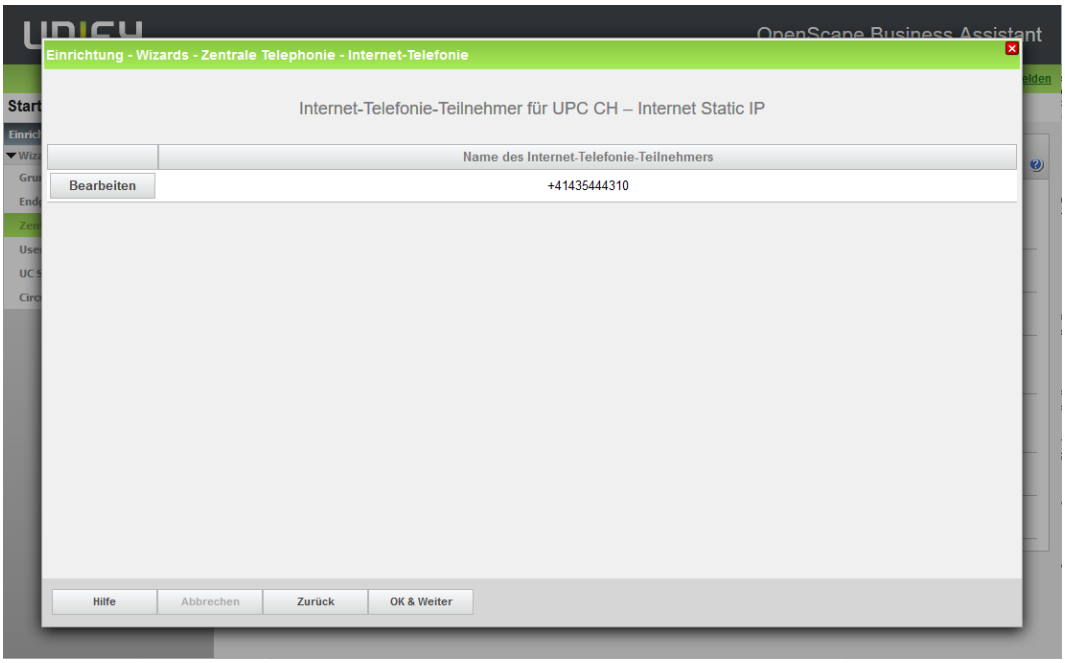
1. Klicken Sie auf den Punkt ‚**Hinzufügen**‘ bei ‚**Neuer Internet-Telefonie Teilnehmer**‘



Netfon Solutions AG
Badenerstrasse 329, Postfach, 8040 Zürich
Telefon 044 497 11 11
Telefax 044 497 11 12
E-Mail info@netfon-solutions.ch
Internet www.netfon-solutions.ch

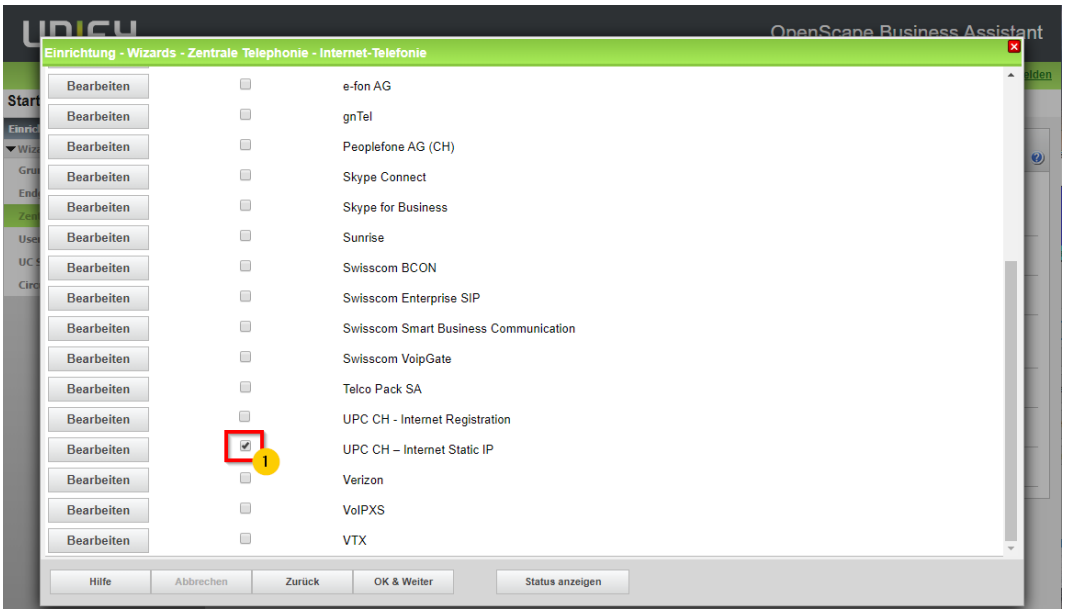
1. Geben Sie die Stamm-Rufnummer im Feld ‚**Internet-Telefonie-Teilnehmer / Registrierungsrufnummer**‘ ein.
   Geben Sie die Stamm-Rufnummer im Feld ‚**Autorisierungsname / Telefonie-Benutzername**‘ ein.
2. Wählen Sie ‚**Öffentliche Rufnummer (DuWa)**‘ in der **Rufnummernzuordnung** aus.
3. Geben Sie die ‚**Stamm-Rufnummer**‘ im Feld ‚**Standard-Rufnummer**‘ ein.



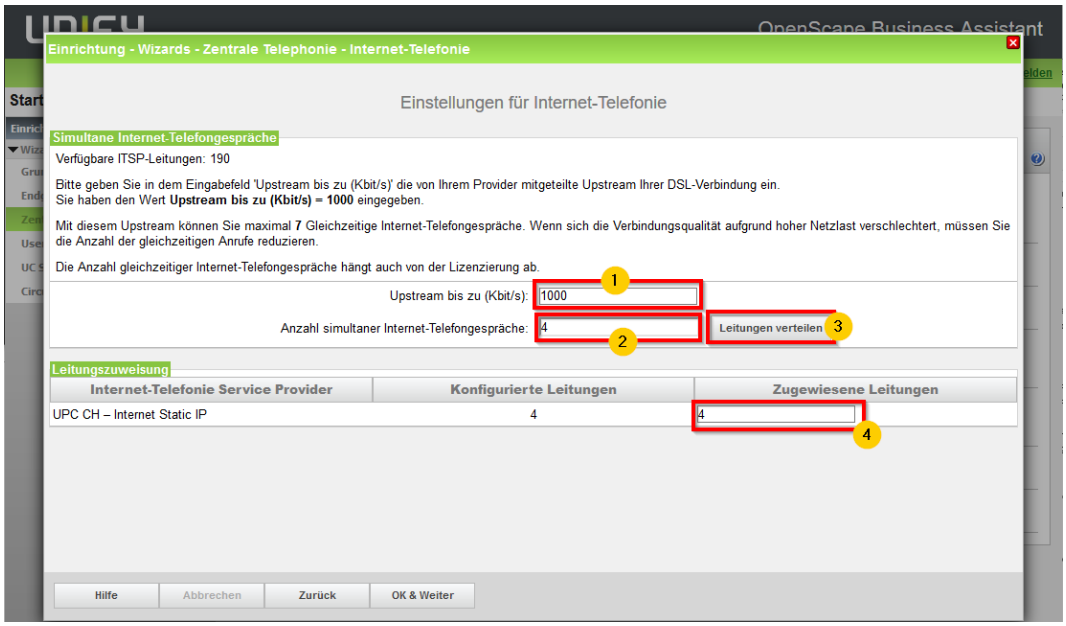


Netfon Solutions AG
Badenerstrasse 329, Postfach, 8040 Zürich
Telefon 044 497 11 11
Telefax 044 497 11 12
E-Mail info@netfon-solutions.ch
Internet www.netfon-solutions.ch

1. Überprüfen Sie, dass der Service Provider ‚**UPC CH – Internet Static IP**‘ **aktiviert** ist.

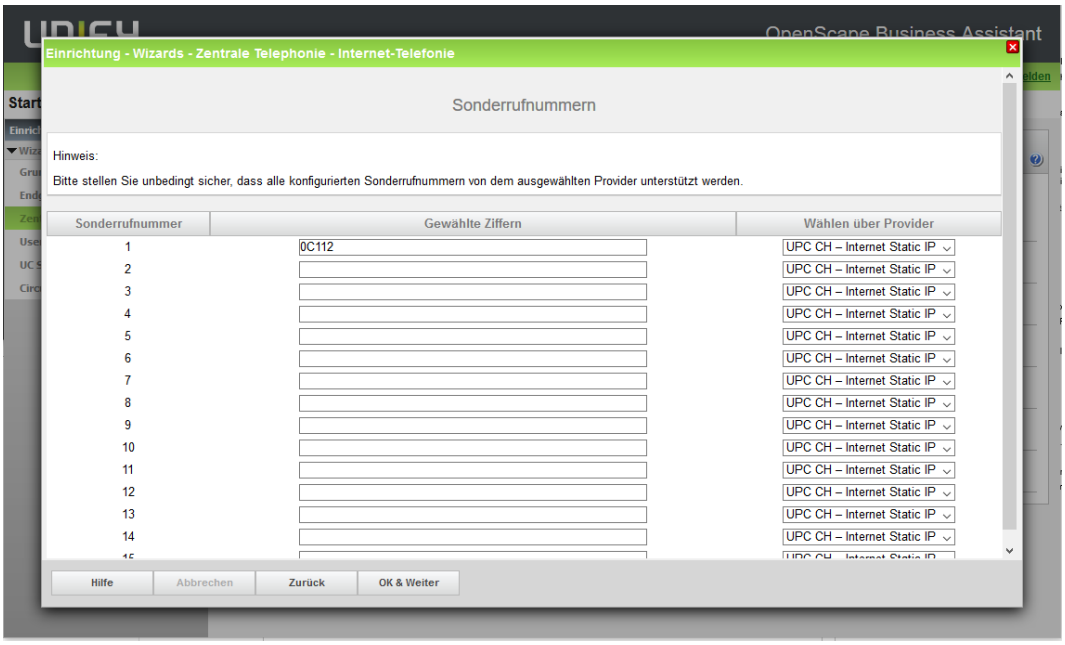


1. Geben Sie den vorhandenen die ‚**verfügbare Upload Bandbreite in kbit/s**‘ im Feld ‚**Upstream bis zu (Kbit/s)**‘ ein.
   Der Wert berechnet sich wie folgt:
   Anzahl Sprachkanäle x 140 kbit/s = notwendiger Upstream
   (Beispiel: 4 Sprachkanäle x 140 kbit/s = 560 kbit/s)
2. Geben Sie die Anzahl vom Provider ‚**abonnierten Sprachkanäle**‘ im Feld ‚**Anzahl simultaner Internet-Gespräche**‘ ein.
3. Klicken Sie auf ‚**Leitungen verteilen**‘
4. Überprüfen Sie den Wert bei ‚**Zugewiesene Leitungen**‘

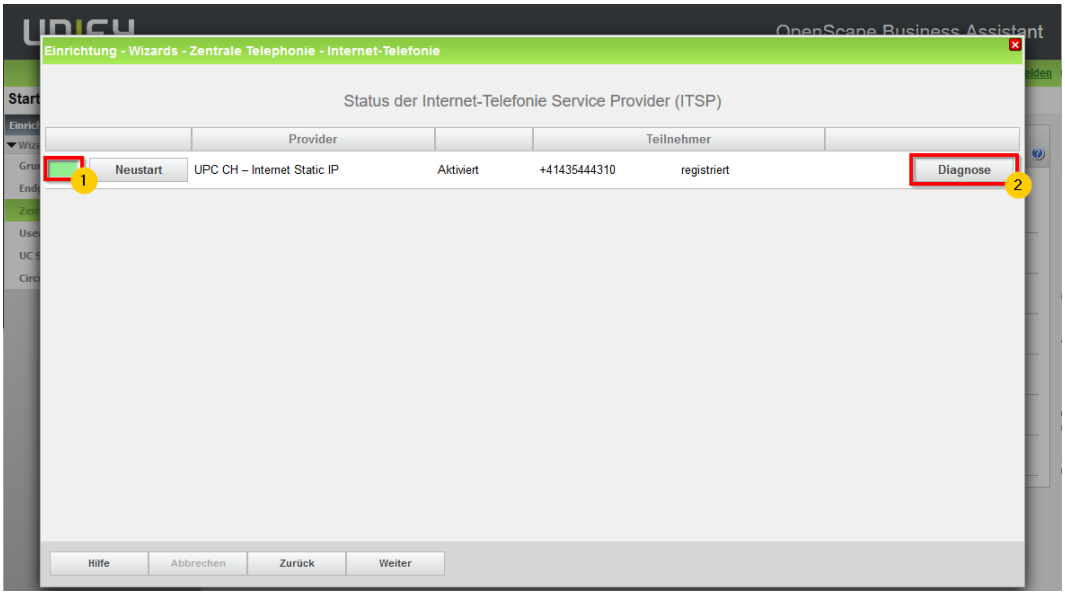


Netfon Solutions AG
Badenerstrasse 329, Postfach, 8040 Zürich
Telefon 044 497 11 11
Telefax 044 497 11 12
E-Mail info@netfon-solutions.ch
Internet www.netfon-solutions.ch

Diese Konfiguration Seite kann übersprungen werden. Die Sondernummern werden in einem späteren Schritt im LCR eingetragen.

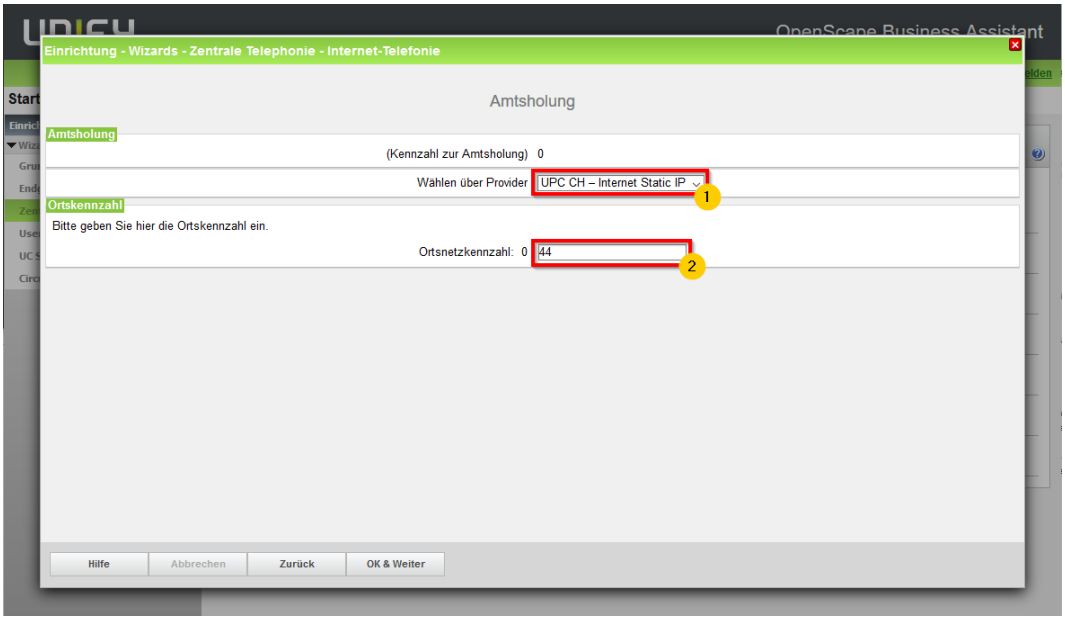


1. Anhand der Farbe erkennen Sie, ob die Registrierung beim Service-Provider erfolgreich war.
   Grün = Registriert
   Rot = Registration nicht erfolgreich
2. Sollte die Registration nicht erfolgreich sein, finden Sie mit der Diagnose bereits erste Indizien über die Gründe.



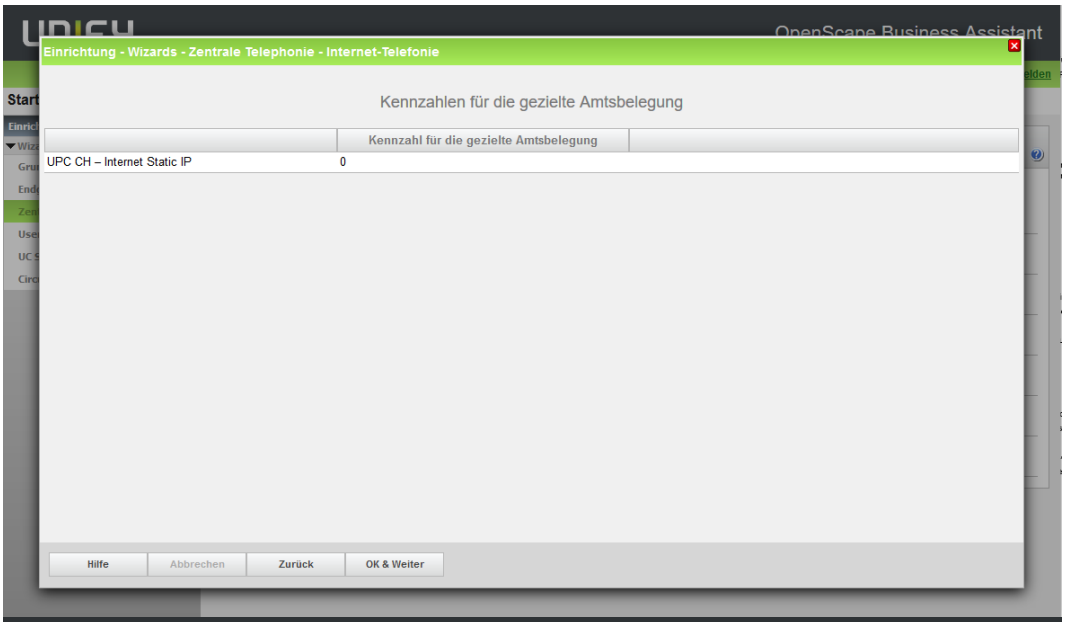
Netfon Solutions AG
Badenerstrasse 329, Postfach, 8040 Zürich
Telefon 044 497 11 11
Telefax 044 497 11 12
E-Mail info@netfon-solutions.ch
Internet www.netfon-solutions.ch

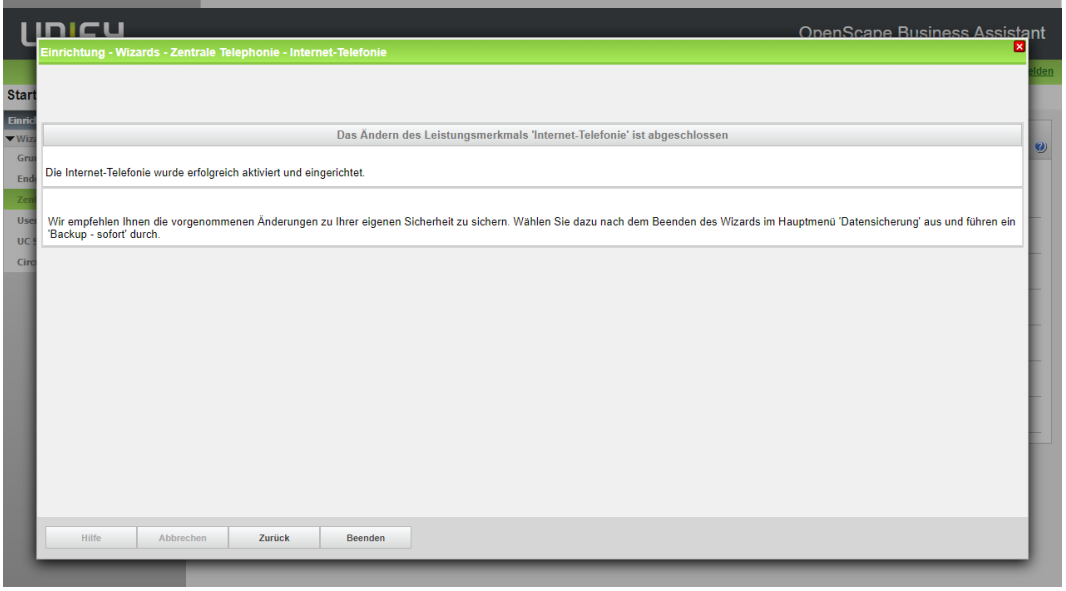
1. Wählen Sie ‚**UPC CH – Internet Registration**‘ im Feld **Wählen über Provider** aus.
2. Tragen Sie die korrekte **Ortsnetzkennzahl** im dafür vorgesehenen Feld ein.



Netfon Solutions AG
Badenerstrasse 329, Postfach, 8040 Zürich
Telefon 044 497 11 11
Telefax 044 497 11 12
E-Mail info@netfon-solutions.ch
Internet www.netfon-solutions.ch

Alle relevanten Konfigurationen wurden durchgeführt. Schliessen Sie den Wizard ab.



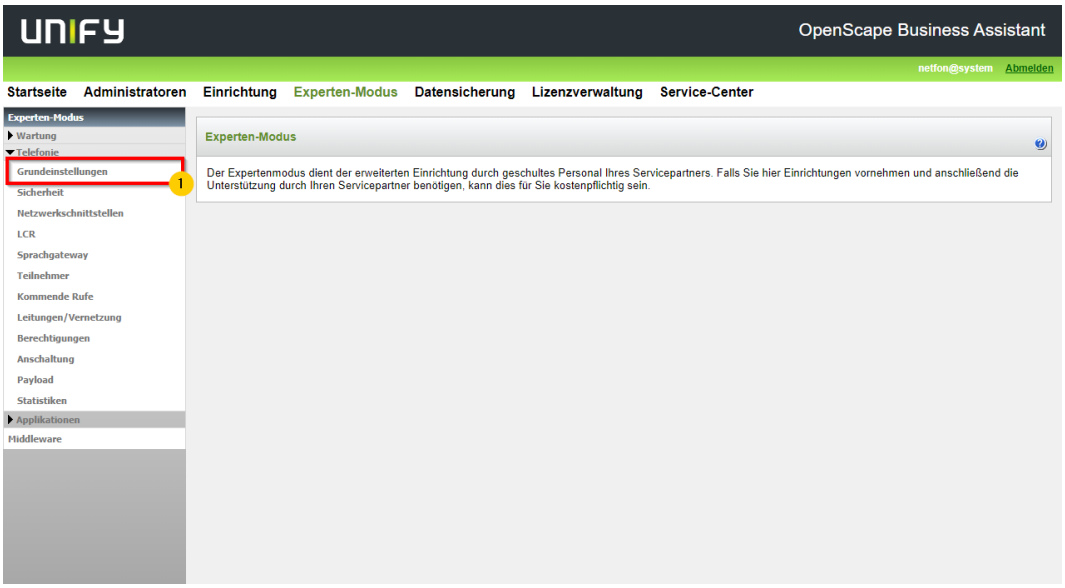


Netfon Solutions AG
Badenerstrasse 329, Postfach, 8040 Zürich
Telefon 044 497 11 11
Telefax 044 497 11 12
E-Mail info@netfon-solutions.ch
Internet www.netfon-solutions.ch

2.3 Grundeinstellungen

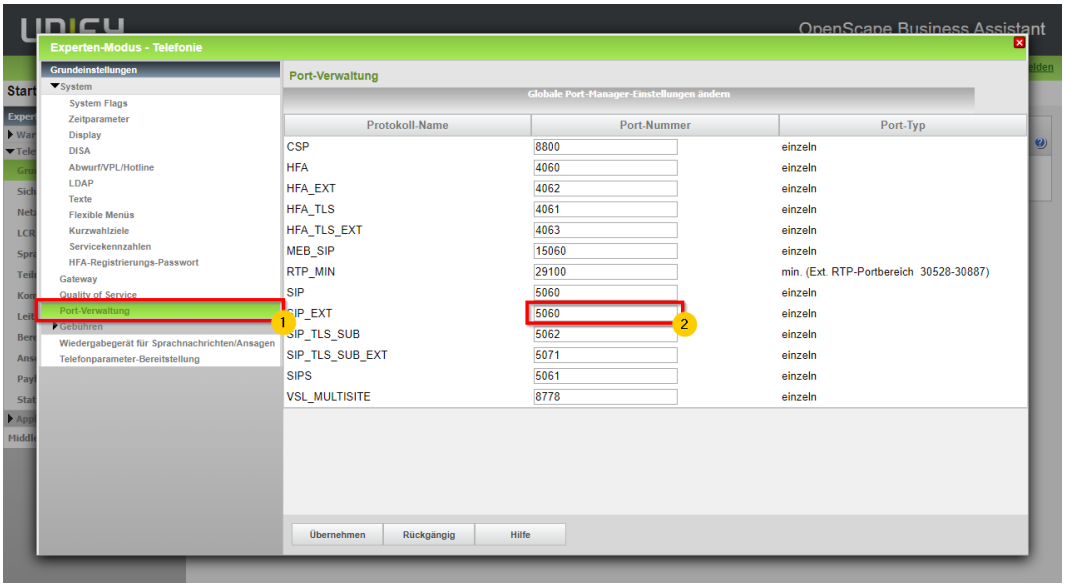
Navigieren Sie zu den ‚Grundeinstellungen':

1. Experten-Modus > Grundeinstellungen



1. Klicken Sie auf Port-Verwaltung
2. Passen Sie im Feld ‚**SIP_EXT**' die Port-Nummer auf **5060** an.

Anmerkung: Der interne SIP Port sollte unbedingt auf einen abweichenden Wert (z.B. 5070) gesetzt werden. Die Konfiguration eines gleichen Wertes für beide Ports ist möglich, hat aber erhebliche Sicherheitsrisiken zur Folge.

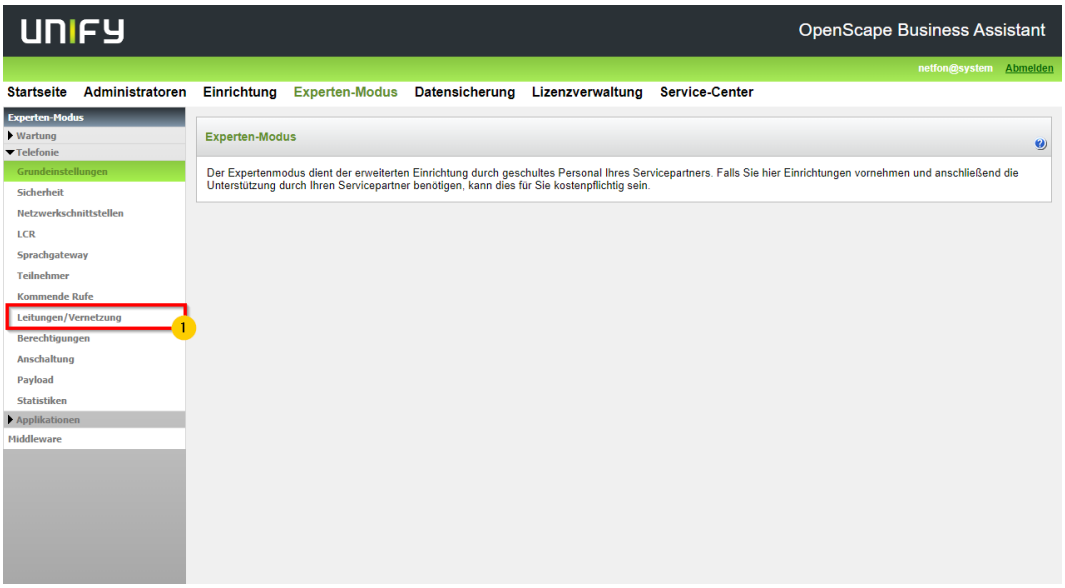


Netfon Solutions AG
Badenerstrasse 329, Postfach, 8040 Zürich
Telefon 044 497 11 11
Telefax 044 497 11 12
E-Mail info@netfon-solutions.ch
Internet www.netfon-solutions.ch

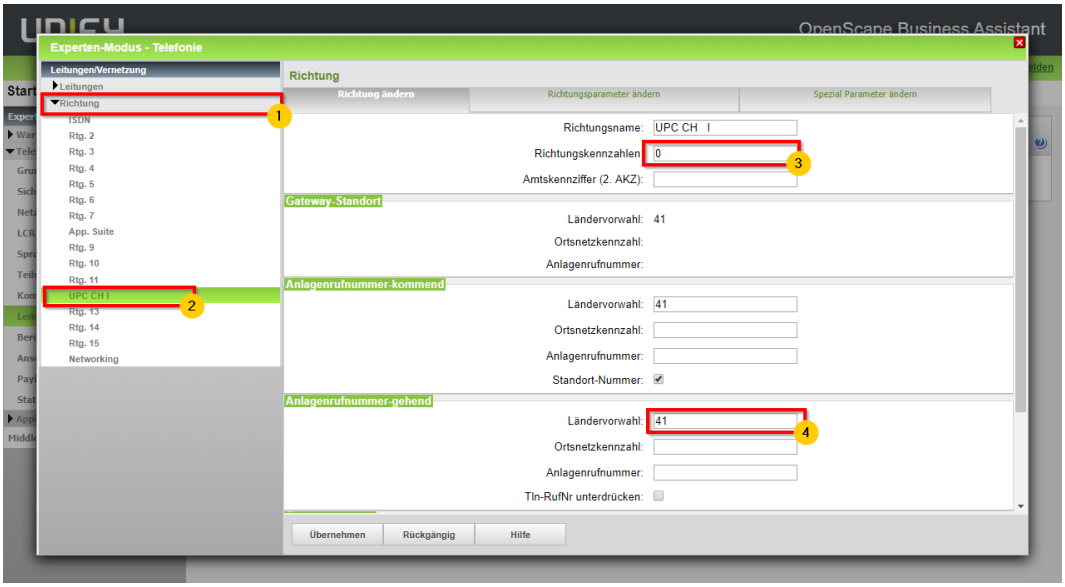
2.4 Leitungen/Vernetzung

Navigieren Sie zu ‚Leitungen/Vernetzung':

1. Experten-Modus > Leitungen/Vernetzung



1. Klicken Sie auf Richtung
2. Klicken Sie auf UPC CH I
3. Passen Sie im Feld ‚**Richtungskennzahlen**' die Kennzahl auf **0** an.
4. Passen Sie im Feld ‚**Ländervorwahl**' die Kennzahl auf **41** an.

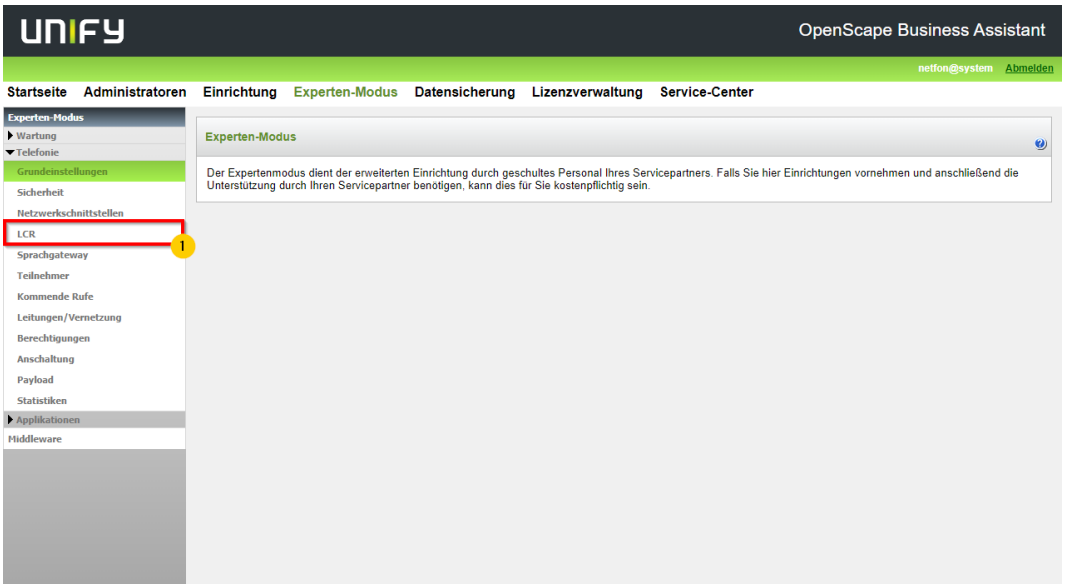


Netfon Solutions AG
Badenerstrasse 329, Postfach, 8040 Zürich
Telefon 044 497 11 11
Telefax 044 497 11 12
E-Mail info@netfon-solutions.ch
Internet www.netfon-solutions.ch

2.5 LCR

Navigieren Sie zum ‚LCR':

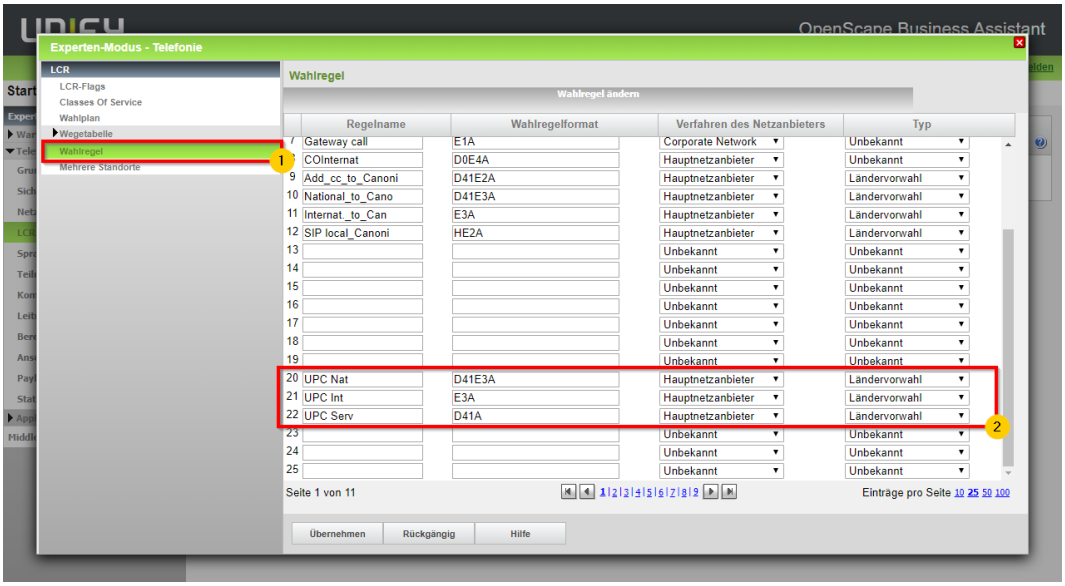
1. Experten-Modus > LCR



2.5.1 Wahlregel

1. Klicken Sie auf Wahlregel
2. Fügen Sie die folgenden Wahlregeln ein

20	UPC Nat	D41E3A	Hauptnetzanbieter	Ländervowahl
21	UPC Int	E3A	Hauptnetzanbieter	Ländervowahl
22	UPC Serv	D41A	Hauptnetzanbieter	Ländervowahl



Netfon Solutions AG
Badenerstrasse 329, Postfach, 8040 Zürich
Telefon 044 497 11 11
Telefax 044 497 11 12
E-Mail info@netfon-solutions.ch
Internet www.netfon-solutions.ch

2.5.2 Wegtabellen

1. Passen Sie die Wegtabellen wie folgt an:

Wegetabelle 80

Wegetabelle ändern

Wegetabelle:80 Blockweise

Index	Dedizierte Richtung	Richtung	Wahlregel	min. Ber.	Warnung	Dediziertes Gateway	GW Knoten-ID
1	☐	UPC CH I	UPC Serv →	15	Keine	Nein	

Wegtabelle 81

Wegetabelle ändern

Wegetabelle:81 Blockweise

Index	Dedizierte Richtung	Richtung	Wahlregel	min. Ber.	Warnung	Dediziertes Gateway	GW Knoten-ID
1	☐	UPC CH I	UPC Nat →	15	Keine	Nein	

Wegtabelle 82

Wegetabelle ändern

Wegetabelle:82 Blockweise

Index	Dedizierte Richtung	Richtung	Wahlregel	min. Ber.	Warnung	Dediziertes Gateway	GW Knoten-ID
1	☐	UPC CH I	UPC Int →	15	Keine	Nein	

Wegtabelle 83

Wegetabelle ändern

Wegetabelle:83 Blockweise

Index	Dedizierte Richtung	Richtung	Wahlregel	min. Ber.	Warnung	Dediziertes Gateway	GW Knoten-ID
1	☐	UPC CH I	UPC Int →	15	Keine	Nein	

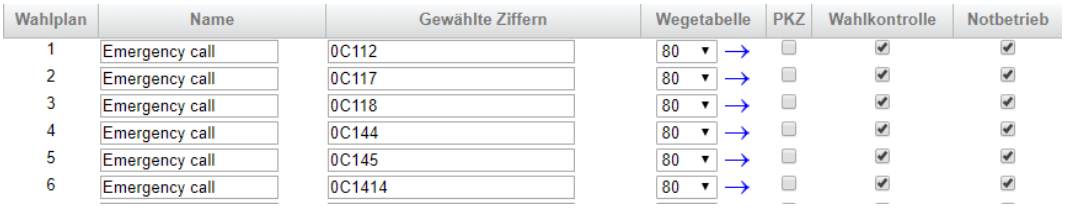
Netfon Solutions AG
Badenerstrasse 329, Postfach, 8040 Zürich
Telefon 044 497 11 11
Telefax 044 497 11 12
E-Mail info@netfon-solutions.ch
Internet www.netfon-solutions.ch

2.5.3 Wahlplan

1. Es empfiehlt sich, denn kompletten Wahlplan mit Ausnahme der Zeilen 31, 33 und 35 zu löschen.
2. Fügen Sie die folgenden Zeilen im Wahlplan ein:

Notrufnummern

Wahl-plan	Name	Gewählte Ziffern	Weg-tabelle	PKZ	Wahl-kontrolle	Not-betrieb
1	Emergency Call	0C112	80	Nein	Ja	Ja
2	Emergency Call	0C117	80	Nein	Ja	Ja
3	Emergency Call	0C118	80	Nein	Ja	Ja
4	Emergency Call	0C144	80	Nein	Ja	Ja
5	Emergency Call	0C145	80	Nein	Ja	Ja
6	Emergency Call	0C1414	80	Nein	Ja	Ja



Allgemeine Rufnummern

Wahl-plan	Name	Gewählte Ziffern	Weg-tabelle	PKZ	Wahl-kontrolle	Not-betrieb
80	Services	0C1Z	80	Nein	Ja	Nein
81	National	0C0-Z	81	Nein	Ja	Nein
82	International	0C00-Z	82	Nein	Ja	Nein
83	COInternat	0C00-41-Z	83	Nein	Ja	Nein

Unify spezifische Dienste sollten <u>nicht</u> angepasst werden

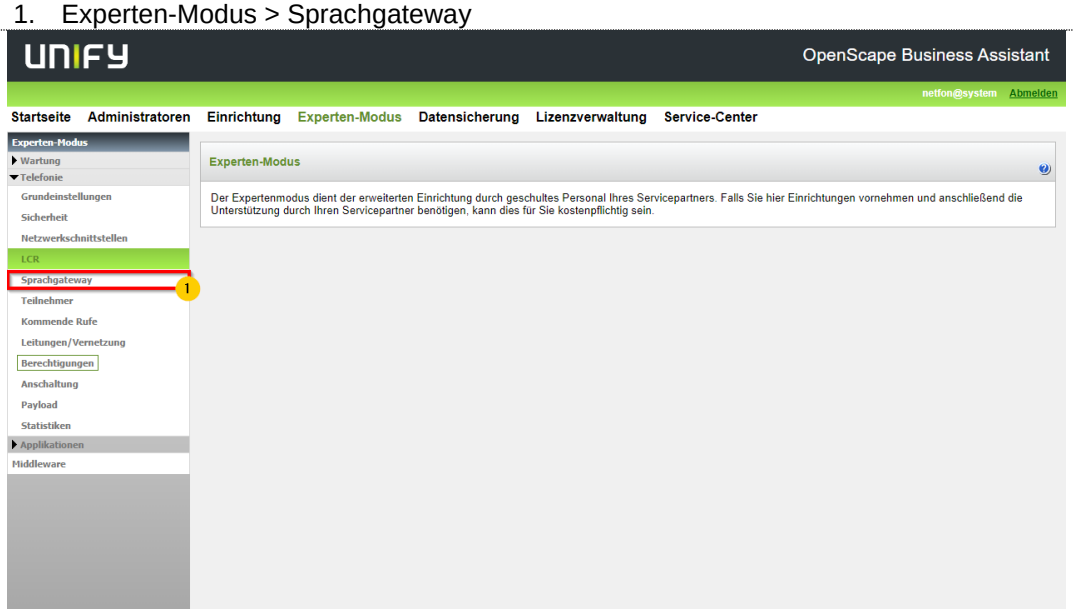
Wahl-plan	Name	Gewählte Ziffern	Weg-tabelle	PKZ	Wahl-kontrolle	Not-betrieb
31	Appl-Suite	-71	12	Nein	Ja	Nein
32			-	Nein	Ja	Nein
33	IP-Network	-Z	13	Nein	Nein	Nein
34			-	Nein	Ja	Nein
35	Ann-Player	-	12	Nein	Ja	Nein

Netfon Solutions AG
Badenerstrasse 329, Postfach, 8040 Zürich
Telefon 044 497 11 11
Telefax 044 497 11 12
E-Mail info@netfon-solutions.ch
Internet www.netfon-solutions.ch

2.6 Sprachgateway

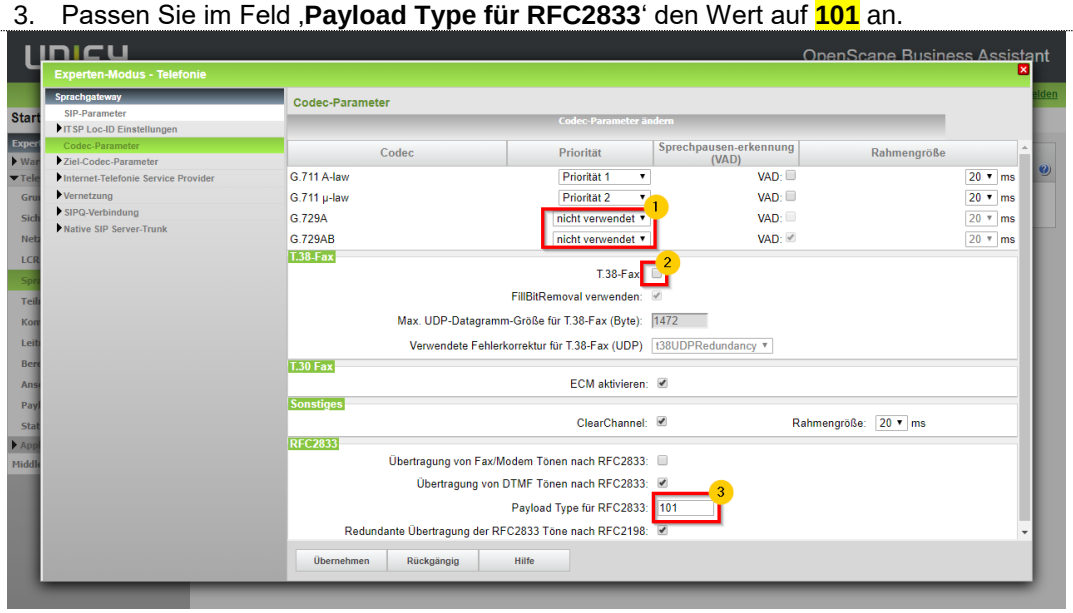
Navigieren Sie zu ‚Sprachgateway':

1. Experten-Modus > Sprachgateway



Passen Sie die Einstellungen im Submenü Codec-Parameter wie folgt an:

1. Der Service-Provider unterstützt ausschliesslich die Codecs G.711 A-law und µ-law. Stellen Sie die Codecs **G.729A und AB** auf ‚**nicht verwendet**'
2. Der Service-Provider empfiehlt auf **T.38-Fax** zu verzichten, die Erfolgsraten ohne T.38 sind höher. **Deaktivieren Sie ‚T.38-Fax**'.
3. Passen Sie im Feld ‚**Payload Type für RFC2833**' den Wert auf **101** an.

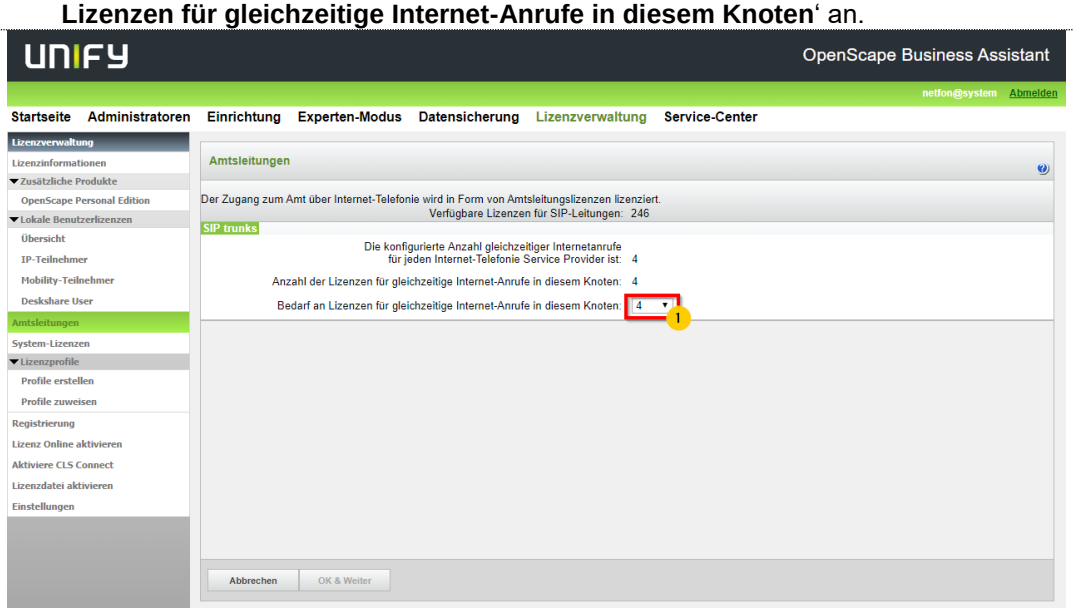


Netfon Solutions AG
Badenerstrasse 329, Postfach, 8040 Zürich
Telefon 044 497 11 11
Telefax 044 497 11 12
E-Mail info@netfon-solutions.ch
Internet www.netfon-solutions.ch

2.7 Lizenzen

Navigieren Sie zu ‚Amtsleitungen' - Lizenzverwaltung > Amtsleitungen

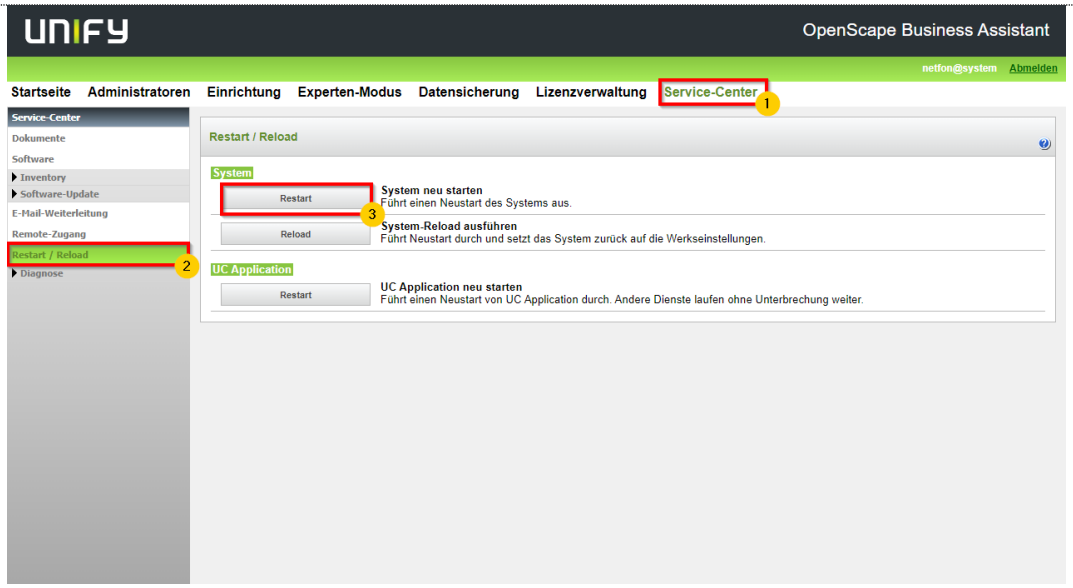
1. Passen Sie die Anzahl gewünschter externer Sprachkanäle im Feld ‚**Bedarf an Lizenzen für gleichzeitige Internet-Anrufe in diesem Knoten**' an.



2.8 Abschluss der Konfiguration

Navigieren Sie zu ‚System Restart':

1. Service-Center
2. Restart / Reload
3. Restart



Netfon Solutions AG
Badenerstrasse 329, Postfach, 8040 Zürich
Telefon 044 497 11 11
Telefax 044 497 11 12
E-Mail info@netfon-solutions.ch
Internet www.netfon-solutions.ch