

Anleitung

UPC - Internet Static IP für OpenScape Business

A. Dokumentklassifikation

Klassifizierung: **Public**

B. Versions Kontrolle

Dokumentstatus: **Final – 1.2**

Version	Geändert von	Datum	Bemerkungen
1.0	Andrea Cavegn	19.04.2020	Dokumenterstellung
1.1	Andrea Cavegn	01.04.2024	Rebranding
1.2	Mitel	24.09.2024	redaktionelle Änderungen

C. Zweck und Abgrenzung

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

D. Produkte

Telefonanlage

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

Die Basis für dieses Dokument ist die zum Zeitpunkt der Zertifizierung aktuelle OpenScape Business. Da die OpenScape Business ständig weiterentwickelt wird, können sich künftig Eingabemasken und Oberflächen als auch die Anforderungen ändern. Die hier beschriebenen Einstellungen und Eingaben gelten dann sinngemäß.

SIP-Trunk

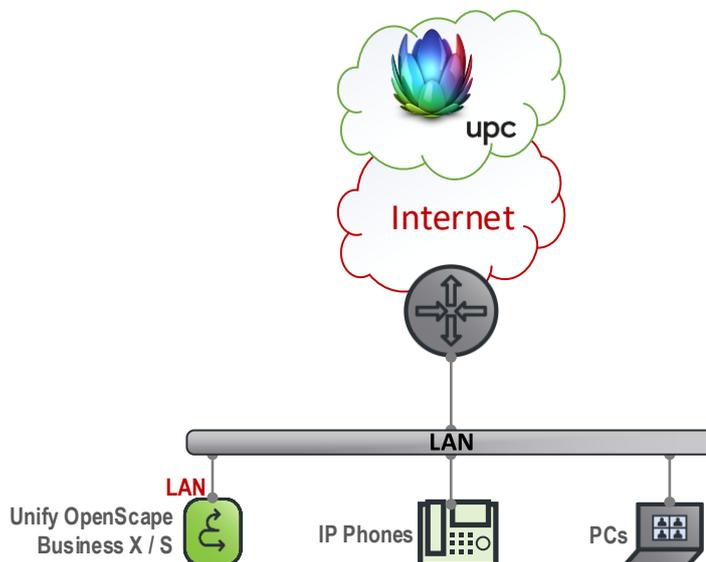
Service Provider	UPC Schweiz GmbH
Produkt	Premium Voice IP
Ausprägung	Internet Static IP

Inhaltsverzeichnis

A.	Dokumentklassifikation	A
B.	Versions Kontrolle	A
C.	Zweck und Abgrenzung	A
D.	Produkte.....	A
1	Generelle Angaben	1
2	Einrichtung	3

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)	√
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 weitere Sicherheits Hinweise.

Bitte beachten Sie, dass Sie für die Anbindung keine Benutzername oder Passwort benötigen, der SIP-Trunk ist zugangslos.

Service Access Point ID (SAFI): **SAP@202.012445**
 UPC Schwach-Sicher: **UPC@202.012445**
 Service Standort: **0000000000000000**

IP-Adresse UPC SIP-Server: **212.47.182.228**
 Port und Protokoll UPC SIP-Server: **5060 UDP**

IP-Adresse Kunden-Firewall: **192.168.1.1**
 Port und Protokoll Kunden-Firewall: **5060 UDP**

Rufnummernbereich: **000 102 48 87**

Rufnummernformat: **0000000000000000**
 Dienstleistungs-Anbieter: **00**
 Priorisierung Datenpakete: **0**
 Supported Codes: **07716 und 07716 / mit einer Framelänge von 20ms**
 Supported DTMF: **00000000**
 FAX: **07716 0000000000**
 CLIP Special Arrangement (CLIP SA): **00**
 Backup-Verbindung: **0000000000000000**

UPC business

Der SIP Trunk von UPC unterstützt folgende Funktionen:

- TSP oder U2P (nach Absprache mit UPC)
- SIP RFC 2843 und 3381
- SIP Privacy (RFC 3325)
- Pushed-Identity/Rendez-Party-ID
- Overseas-Header
- SIP OPTIONS (Reaktiv)
- OTM-RFC 3333
- Codecs:
 - G.711a (mit einer Framelänge von 20ms)
 - G.711u (mit einer Framelänge von 20ms)
 - Far. G.711a pass-through

Folgende Funktionen werden nicht unterstützt:

- Relay
- Update
- Info
- P-Header Identity
- TLSDTMF

Sicherheitsbestimmungen

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: Qualität-Anfrage 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 oder Änderungswünschen kontaktieren Sie bitte Ihren technischen Hauptansprechpartner von dem Sie diese Angaben erhalten haben.

Freundliche Grüsse

UPC - Voice Network und Services

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 in speziellen auch mit dem Schutz von Telefonanlagen (TK-Anlagen) gegen Missbrauch befassen. Dabei stellt sich die Frage, welche Vorkehrungen getroffen werden müssen, um Schäden abzuwehren. Nachfolgend finden Sie einige wichtige Informationen.

Warum geht es?

IP-Header, Freizeite und Shoutbox-Surfer, die sind nur ein paar Bezeichnungen für jene Personen, die heimlich Telefonanlagen für ihre Zwecke missbrauchen und so die betroffenen Unternehmen weltweit jedes Jahr Millionen kosten. Solche Angriffe wurden oder werden im Teil Freizeite (Dialerhacking) bekannt und sind für viele Unternehmen ein tolles Problem. Einige Schweizer Unternehmen beispielsweise wurden in diesem Jahr bei einem Angriff schmerzlich von 24 Stunden im insgesamt über 50 000 Schweizer Franken bestraft. Ihre Telefonanlage war manipuliert worden: die Header hatten eine Umleitung von Anrufen auf Kosten der nicht-erlaubten Unternehmen gelangt.

Was ist ein Freizeite?

Teil Freizeite ermöglicht Betrugern, sich auf Kosten Anderer zu bereichern. Ein Hacker wählt sich über einen Fernanrufangriff ein und kann so auf eine ungeschützte TK-Anlage zugreifen. Typischerweise wählt er dann zu Leuten des betroffenen Unternehmens kostengünstige Mehrnummern im Ausland an, wofür er von den Betreibern der Mehrnummern später einen Anteil der erzielten Erlöse zurück erhält. Manche Hacker haben auch lediglich die Absicht, den Ruf des Unternehmens zu schaden.

Wer ist betroffen?

Heimliche Unternehmen in der Regel nicht zwischen kleinen und grossen Unternehmen. Alle TK-Anlagen ohne geeignete Sicherheitsmassnahmen können zum Ziel werden. Die Angriffe erfolgen bei heimlichen, über SIP- oder IP-Verbindungen verbundenen TK-Anlagen, aber auch bei klassischen, über SIP-Verbindungen angeschlossene IP-TK-Anlagen.

Die Absicht der heimlichen ist Absicht ein Angriff eines Mittelstandes, also zu einem Zeitpunkt, zu dem die Mitarbeiter mit grosser Mehrzahl nicht länger unterrichtet bleibt. Der Angriff dauert meistens an, bis der Missbrauch entdeckt und unterbunden wird. Das kann sich auch über mehrere Tage hinziehen. Wenn Unternehmen die Nutzungsdauer der Telefonanlage nur am Monatsende kontrollieren, kann sich das sogar über Wochen erstrecken und somit erhebliche Kosten verursachen!

Wer trägt die durch Missbrauch entstehenden Teilkosten?

Die Verantwortung des Schutzes der Telefonanlage liegt - vornehmlich unter einer anwenderbezogenen Servicevereinbarung mit UPC - beim Kunden oder seinen Anlagenspezialisten. Anrufe und Gesprächsgebühren, die durch Missbrauch im Telefonanlage entstehen sind, werden wie normale Teilkosten verrechnet und dem Kunden in Rechnung gestellt. Wichtig ist darum, frühzeitig alle erforderlichen Vorkehrungen gegen einen Missbrauch zu treffen - dies ist Aufgabe des Anlagenbetreibers.

UPC business hat innerhalb zusätzlicher Massnahmen ergreifen, um bei betroffenen Unternehmen erhebliche Schäden zu begrenzen. So werden beispielsweise in den Aufzeichnungen des Telefonverkehrs auffällige Muster automatisch herausgefiltert, damit Kunden frühzeitig auf einen unerwarteten Missbrauch aufmerksam gemacht und notwendige Schritte eingeleitet werden können. Dadurch lässt sich ein Schaden im besten Fall begrenzen, aber Missbrauch nicht grundsätzlich verhindern.

UPC business

Analysieren Sie deshalb die Sicherheitsrisiken und realisieren Sie die Vorkehrungen zusammen mit Ihrem Anlagenspezialisten. Dazu gehört auch eine fortlaufende Schulung und Sensibilisierung aller Mitarbeiter.

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 Sicherheitsmassnahmen:

Massnahmen bei TK-Anlagen

- Sicherstellen, dass die TK-Anlage mit der neuesten Software arbeitet und dass alle Sicherheitspatches installiert sind. Überprüfen aller Schwachstellen oder Unregelmäßigkeiten.
- 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 Schwachstellen oder Ports zur eingehenden Authentifizierung in Erwägung ziehen.
- Die Fernzugangsmethode wie etwa Direct Inward System Access prüfen, da nur von technischen Mitarbeitern benötigt wird, die sich via Fernzugang 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 eingebundenen Sicherheitsbestimmungen. Der Lieferant der TK-Anlage hilft bei der Optimierung dieser Einstellungen.
- Etablierung einer effektiven Sicherheitsprozess mit regelmässiger Überprüfung und Aktualisierung der TK-Anlagen-Software. Dazu sicherstellen, dass nach Software-Updates Patches nicht auf die Standardlieferung zurückgesetzt werden.
- Sicherstellen, dass die nötigen Bedingungen in den Verträgen mit dem TK-Anlagen-Verpflichteter (Vollständiger Überprüfungsmaßnahmen aufgenommen sind, dass das System regelmässig gewartet und gepatcht wird und somit sicher bleibt.

Massnahmen bei SIP-Verbindungen

- Wenn die Verbindung, sondern alle Standard-Zugangsparameter zu TK- und Voice-Mail-Anlagen als Passwort nicht eine Kombination von 8 bis 128 oder einem Teil der Telefonnummer verwendet. Sicherstellen, dass Zugangsdaten und Passwörter sicher und für die regulären Mitarbeiter nicht ohne Weiteres erkennbar sind. Verwenden von Passwörtern, die gross- und kleingeschriebene Buchstaben, Zahlen und Sonderzeichen enthalten, und die mindestens die maximale von System abhängige Länge haben. Merkmale Sonderzeichen unverändert lassen!
- Besondere Anordnungen einhalten, die in Geschäftsblättern normalerweise nicht angegeben werden zum Beispiel Mehrnummern, internationale Nummern, Satellitennummern sowie Vertriebsnummern und Kundennummern.
- Wenn möglich die Voicemail-Anrufe für Mitarbeiter sperren oder die Konfiguration dieser Funktion auf einen nur internen Zugang beschränken.
- Den Zugang zum System auf ein Level beschränken, das für die Erfassung einer Aufgabe erforderlich ist.
- Alle internen Informationen wie Telefonbücher, Anruf- oder Rufprotokolle vertraulich behandeln und sicher verwahren, wenn sie nicht benötigt werden.

UPC business

- Einerkennung über Missbrauch vorzubeugen. Betrüger wechseln häufig von einem Anbieter zum nächsten und schaden damit einem. Geben Sie Informationen weiter, damit wir gemeinsam und proaktiv gegen das Problem vorgehen können. Erklären Sie auch Ihre Geschäftsmodelle, ungewöhnliche Anrufmuster zu melden.
- Nach einem Angriff den Betrag der Forderung melden und Anzeige erstatten. Den Hackerangriff dokumentieren. Je mehr Informationen die Polizei sammeln kann, desto grösser sind die Chancen, den Forderungserfolg zu bekommen.

Massnahmen bei Internet

- Anfragen aller Massnahmen, die für Geräte und Anlagen in IP-Netzwerke üblich sind.
- Die Sicherheitsrisiken des IP-Netzwerks auf Schwachstellen überprüfen. Alle IP-TK-Anlagen verwenden werden. Den Lieferanten der IP-TK-Anlage und dem Verantwortlichen des Netzwerkes kontaktieren.
- Überprüfen der Einstellungen und der Sicherheitsmassnahmen nach jeder Umstellung im IP-Netzwerk.
- Fernzugänge sorgfältig einstellen und regelmässig prüfen.

Massnahmen bei Firewalls

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

Massnahmen bei der Nutzung

- Falls Voice-Mail-Funktionen wie der Fernzugang oder die internationale Anrufweiterleitung von Mitarbeitern nicht benötigt werden, sollten diese abgeschaltet werden. Voice-Mail ist eine Schwachstelle, auf die Hacker nicht zugreifen können. Wenn, nicht benötigte Voice-Mailbox sperren, bis sie einen Benutzer zugewiesen wird.
- Viele definierte Prozesse einhalten für die Mitarbeiter-Beurteilung. Regelmässige, die Sicherheitsüberprüfung von neuen Mitarbeitern sowie für Stellenwechsel. Den Zugang zu Systemen, Modulen und Codebooks einseitig richtig und jeweils formal einholen.
- Geprüfte Mitarbeiter und Anwohler (überwachen) - ein Angriff kann so frühzeitig bemerkt werden, bevor er zu normalen Kosten führt.
- Die Möglichkeiten von Ferngesprächen und internationalen Anrufen auf jene Mitarbeiter beschränken, die dies benötigen. Wenn ein Zugang nicht mehr verwendet wird, sollten die Telefonnummern umgehend entsprechend gesperrt werden.
- Die Anwesenheitsnummern zu Ferngesprächennummern einschliessen und das Weiterleiten von Gesprächen nur auf solche Nummernnummern zulassen, die im System registriert sind.
- Vorsicht walten lassen bei Softwareupdates (zum Beispiel Personal, die vorgaben. Mitarbeitende des Unternehmens zu sein, die verlangen, mit der Zentrale verbunden zu werden, um eine angelegte Leitung zu erhalten).

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

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

The screenshot shows the Netfon administration interface. The top navigation bar includes 'Startseite', 'Administratoren', 'Einrichtung', 'Experten-Modus', 'Datensicherung', 'Lizenzverwaltung', and 'Service-Center'. The 'Einrichtung' menu is highlighted with a red box and a yellow '1'. The left sidebar shows 'Zentrale Telefonie' highlighted with a red box and a yellow '2'. The main content area shows the 'Zentrale Telefonie' configuration page with several options, each with a 'Bearbeiten' button. The 'Internet-Telefonie' option is highlighted with a red box and a yellow '3'. The 'Internet-Telefonie' configuration details include: 'Zugangsparameter des Internet-Telefonie Service Provider (ITSP) z.B. User-Account, Passwort, SIP-Rufnummer'.

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

Einrichtung - Wizards - Zentrale Telephonie - Internet-Telefonie

Übersicht

Hinweis: Im Expertenmodus durchgeführte Änderungen müssen nach Durchlaufen des Wizards überprüft/wiederholt werden.
Hinweis: Für Leistungsmerkmale wie 'Internet-Telefonie' und 'MeetMe-Konferenz' wird mindestens die Konfiguration der Länderkennzahl benötigt.

Anlagenrufnummer:

Ländervorwahl: 00 (zwingend erforderlich)

Ortskennzahl: 0 (optional)

Anlagenrufnummer: (optional)

Hilfe Abbrechen Zurück OK & Weiter

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'**

Einrichtung - Wizards - Zentrale Telephonie - Internet-Telefonie

Provider-Konfiguration und -Aktivierung für Internet-Telefonie

Keine Telefonie über Internet: 1

Länderspezifische Ansicht: Schweiz 2

Hinweis: Im Expertenmodus durchgeführte Änderungen müssen nach Durchlaufen des Wizards überprüft/wiederholt werden.

	Provider aktivieren	Internet-Telefonie Service Provider
Hinzufügen		Anderer Provider
Bearbeiten	<input type="checkbox"/>	Broadcloud
Bearbeiten	<input type="checkbox"/>	Cablecom
Bearbeiten	<input type="checkbox"/>	COLT UK & Europe
Bearbeiten	<input type="checkbox"/>	COLT VPN
Bearbeiten	<input type="checkbox"/>	e-fon AG
Bearbeiten	<input type="checkbox"/>	gnTel
Bearbeiten	<input type="checkbox"/>	Peoelfone AG (CH)
Bearbeiten	<input type="checkbox"/>	Skype Connect
Bearbeiten	<input type="checkbox"/>	Skype for Business
Bearbeiten	<input type="checkbox"/>	Sunrise
Bearbeiten	<input type="checkbox"/>	Swisscom BCON
Bearbeiten	<input type="checkbox"/>	Swisscom Enterprise SIP
Bearbeiten	<input type="checkbox"/>	Swisscom Smart Business Communication
Bearbeiten	<input type="checkbox"/>	Swisscom VoipGate
Bearbeiten	<input type="checkbox"/>	Telco Pack SA
Bearbeiten	<input type="checkbox"/>	UPC CH - Internet Registration
Bearbeiten 3	<input type="checkbox"/>	UPC CH – Internet Static IP

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

Einrichtung - Wizards - Zentrale Telephonie - Internet-Telefonie

Internet-Telefonie Service Provider

Provider-Name: UPC CH – Internet Static IP
 Provider aktivieren: **1**
 Sicherer Trunk:
 Gateway Domain Name: 212.47.182.228

Provider-Registrar

Registrar verwenden:
 IP Adresse/Host-Name:
 Port: 5060
 Reregistration-interval am Provider (s): 600

Provider-Proxy

IP Adresse/Host-Name: 212.47.182.228
 Port: 5060

Provider-Outbound-Proxy

Provider Outbound-Proxy verwenden:
 IP Adresse/Host-Name: 0.0.0.0
 Port: 0

Hilfe Abbrechen Zurück OK & Weiter Daten löschen

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

Einrichtung - Wizards - Zentrale Telephonie - Internet-Telefonie

Internet-Telefonie-Teilnehmer für UPC CH – Internet Static IP

	Name des Internet-Telefonie-Teilnehmers
Hinzufügen 1	Neuer Internet-Telefonie-Teilnehmer

Hilfe Abbrechen Zurück OK & Weiter

1. Geben Sie die Stamm-Rufnummer im Feld, **Internet-Telefonie-Teilnehmer / Registrierungsnummer** 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.

Einrichtung - Wizards - Zentrale Telephonie - Internet-Telefonie

Internet-Telefonie-Teilnehmer für UPC CH – Internet Static IP

Internet-Telefonie-Teilnehmer / Registrierungsnummer: +41435444310 **1**

Autorisierungsname / Telefonie-Benutzername: +41435444310

Kennwort / Telefonie-Passwort:

Kennwort / Telefonie-Passwort wiederholen:

Rufnummernzuordnung **2**

Öffentliche Rufnummer (DuWa)

Mehrere ITSP-Richtungen:

Standard-Rufnummer: +41435444310 **3**

Standard-Rufnummer
ITSP als primärer Amtszugang
Geben Sie hier eine der Rufnummern ein, die Sie von Ihrem Netzanbieter erhalten haben. Diese Nummer wird bei abgehenden Anrufen als Anrufernummer verwendet, wenn für den jeweiligen Anruf keine andere Rufnummer verfügbar ist.
Alle von Ihrem Netzanbieter bereitgestellten Rufnummern sollten bei der Leitungs- und Telefonkonfiguration (DuWa-Feld) unter primärer Amtszugang eingetragen werden.

Hilfe Abbrechen Zurück OK & Weiter Daten löschen

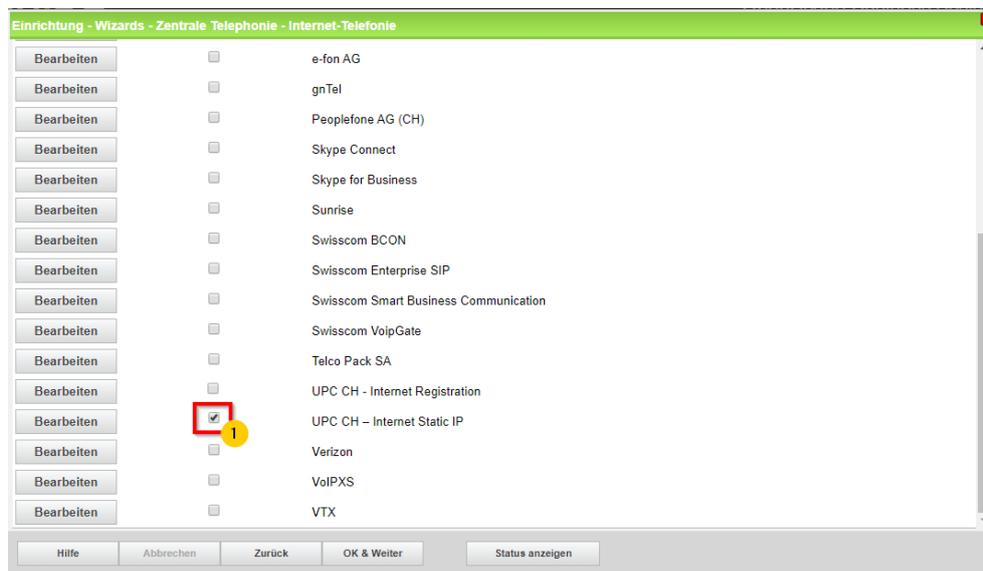
Einrichtung - Wizards - Zentrale Telephonie - Internet-Telefonie

Internet-Telefonie-Teilnehmer für UPC CH – Internet Static IP

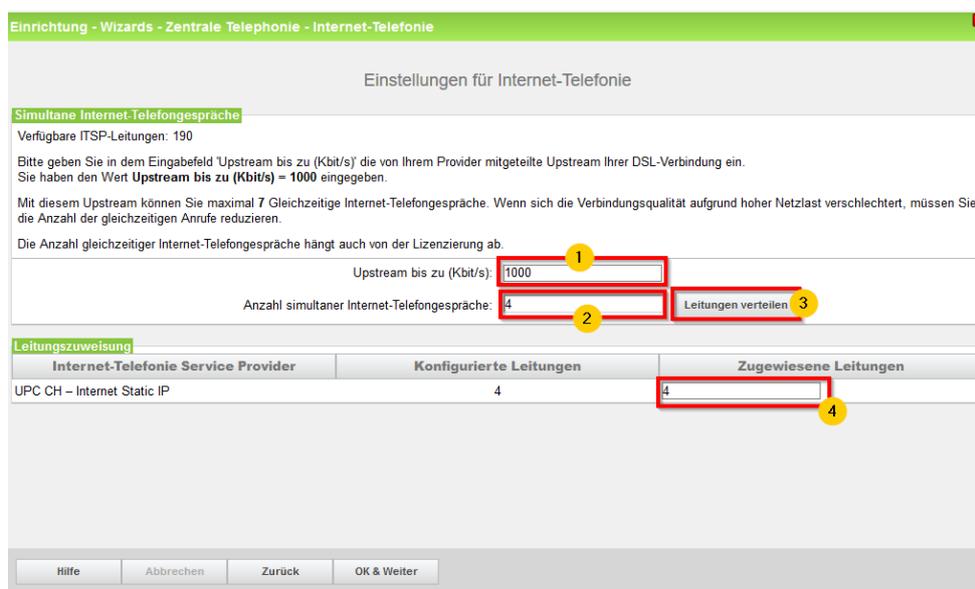
	Name des Internet-Telefonie-Teilnehmers
Bearbeiten	+41435444310

Hilfe Abbrechen Zurück OK & Weiter

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



- 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:
 $\text{Anzahl Sprachkanäle} \times 140 \text{ kbit/s} = \text{notwendiger Upstream}$
(Beispiel: $4 \text{ Sprachkanäle} \times 140 \text{ kbit/s} = 560 \text{ kbit/s}$)
- Geben Sie die Anzahl vom Provider **'abonnierten Sprachkanäle'** im Feld **'Anzahl simultaner Internet-Gespräche'** ein.
- Klicken Sie auf **'Leitungen verteilen'**
- Überprüfen Sie den Wert bei **'Zugewiesene Leitungen'**



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

Sonderrufnummer	Gewählte Ziffern	Wählen über Provider
1	0C112	UPC CH - Internet Static IP
2		UPC CH - Internet Static IP
3		UPC CH - Internet Static IP
4		UPC CH - Internet Static IP
5		UPC CH - Internet Static IP
6		UPC CH - Internet Static IP
7		UPC CH - Internet Static IP
8		UPC CH - Internet Static IP
9		UPC CH - Internet Static IP
10		UPC CH - Internet Static IP
11		UPC CH - Internet Static IP
12		UPC CH - Internet Static IP
13		UPC CH - Internet Static IP
14		UPC CH - Internet Static IP
15		UPC CH - Internet Static IP

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

	Provider		Teilnehmer		
1	UPC CH - Internet Static IP	Aktiviert	+41435444310	registriert	2 Diagnose

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

Einrichtung - Wizards - Zentrale Telephonie - Internet-Telefonie

Amtsholung

Amtsholung (Kennzahl zur Amtsholung) 0

Wählen über Provider: UPC CH – Internet Static IP 1

Ortsnetzkenzahl

Bitte geben Sie hier die Ortsnetzkenzahl ein.

Ortsnetzkenzahl: 0 44 2

Hilfe Abbrechen Zurück OK & Weiter

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

Einrichtung - Wizards - Zentrale Telephonie - Internet-Telefonie

Kennzahlen für die gezielte Amtsbelegung

	Kennzahl für die gezielte Amtsbelegung
UPC CH - Internet Static IP	0

Hilfe Abbrechen Zurück OK & Weiter

Einrichtung - Wizards - Zentrale Telephonie - Internet-Telefonie

Das Ändern des Leistungsmerkmals 'Internet-Telefonie' ist abgeschlossen

Die Internet-Telefonie wurde erfolgreich aktiviert und eingerichtet.

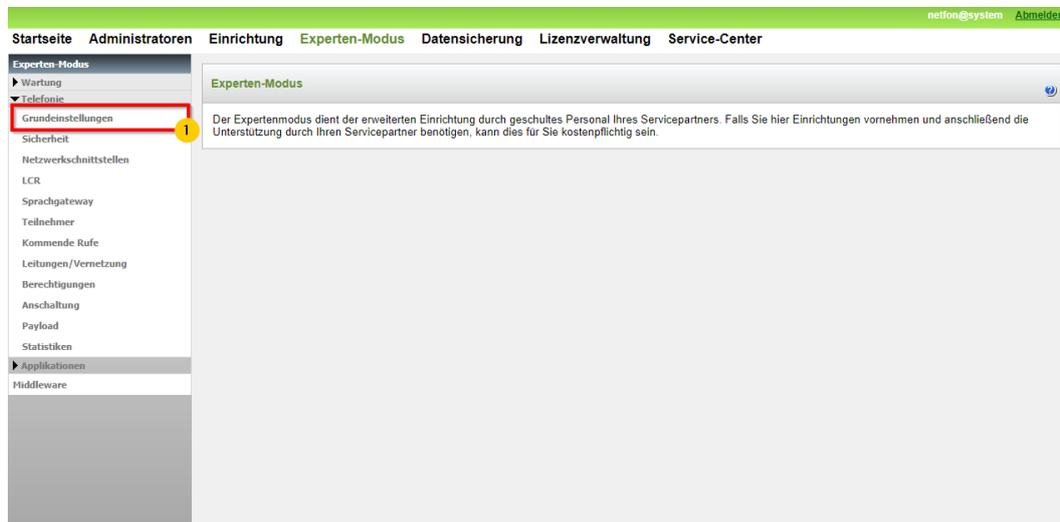
Wir empfehlen Ihnen die vorgenommenen Änderungen zu Ihrer eigenen Sicherheit zu sichern. Wählen Sie dazu nach dem Beenden des Wizards im Hauptmenü 'Datensicherung' aus und führen ein 'Backup - sofort' durch.

Hilfe Abbrechen Zurück Beenden

2.3 Grundeinstellungen

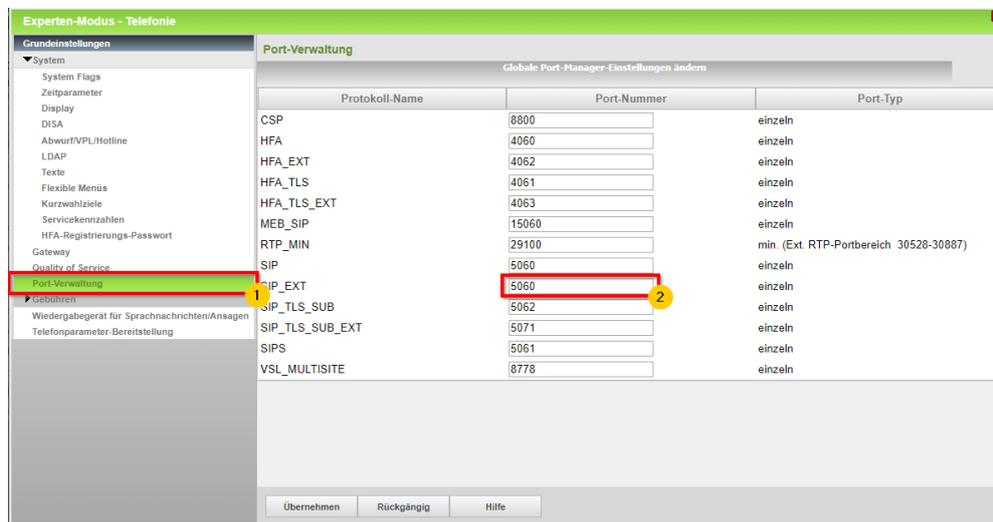
Navigieren Sie zu den ‚Grundeinstellungen‘:

1. Experten-Modus > Grundeinstellungen



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

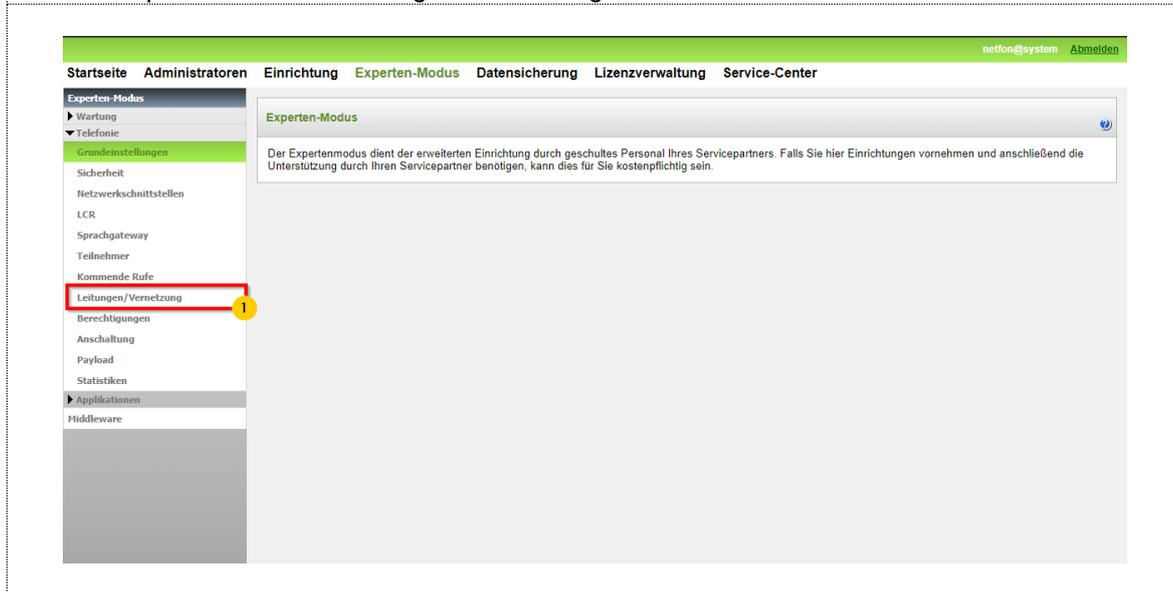
Anmerkung: Der interne SIP Port sollte unbedingt auf einen abweichenden Wert (z.B. 5070) gesetzt werden. Die Konfiguration eines gleichen Wertes für beide Ports ist möglich, hat aber erhebliche Sicherheitsrisiken zur Folge.



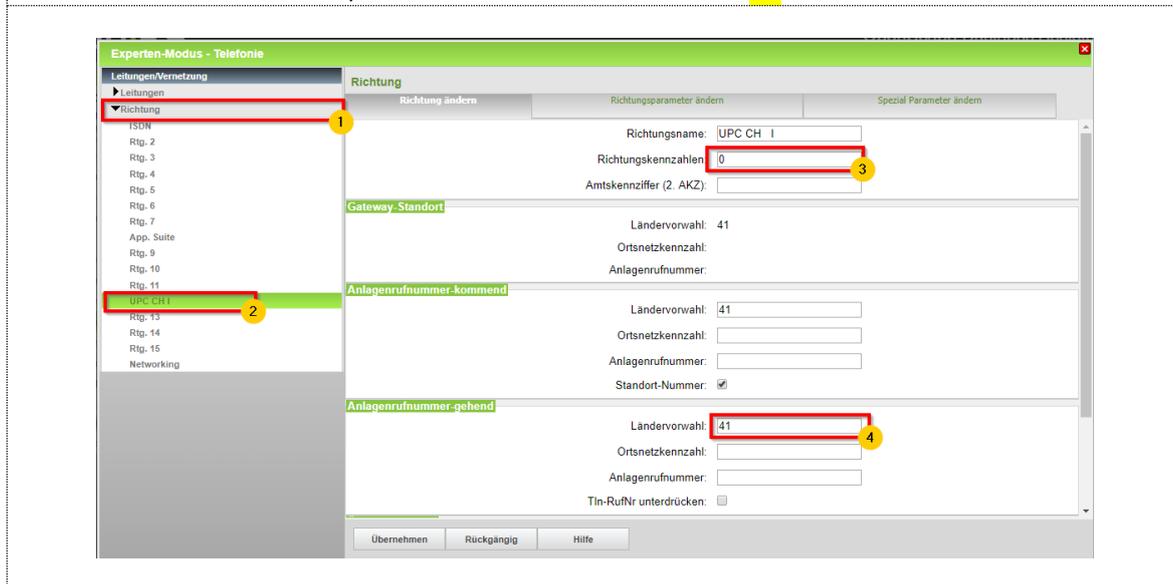
2.4 Leitungen/Vernetzung

Navigieren Sie zu ‚Leitungen/Vernetzung‘:

1. Experten-Modus > Leitungen/Vernetzung



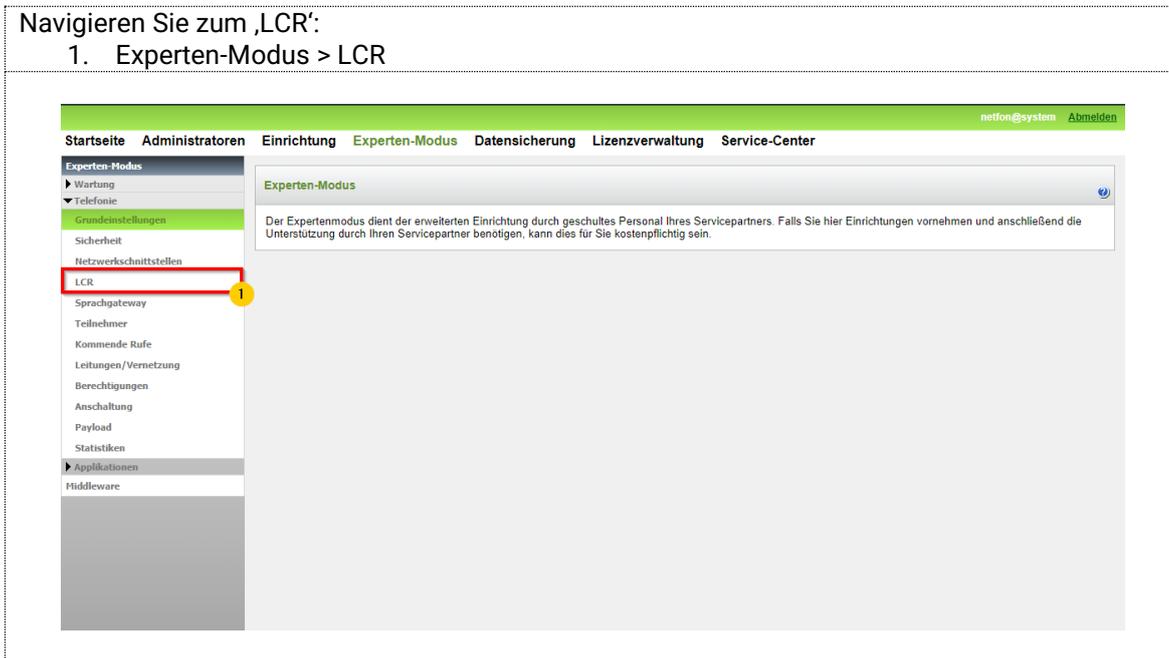
1. Klicken Sie auf Richtung
2. Klicken Sie auf UPC CH I
3. Passen Sie im Feld ‚Richtungskennzahlen‘ die Kennzahl auf **0** an.
4. Passen Sie im Feld ‚Ländervorwahl‘ die Kennzahl auf **41** an.



2.5 LCR

Navigieren Sie zum ‚LCR‘:

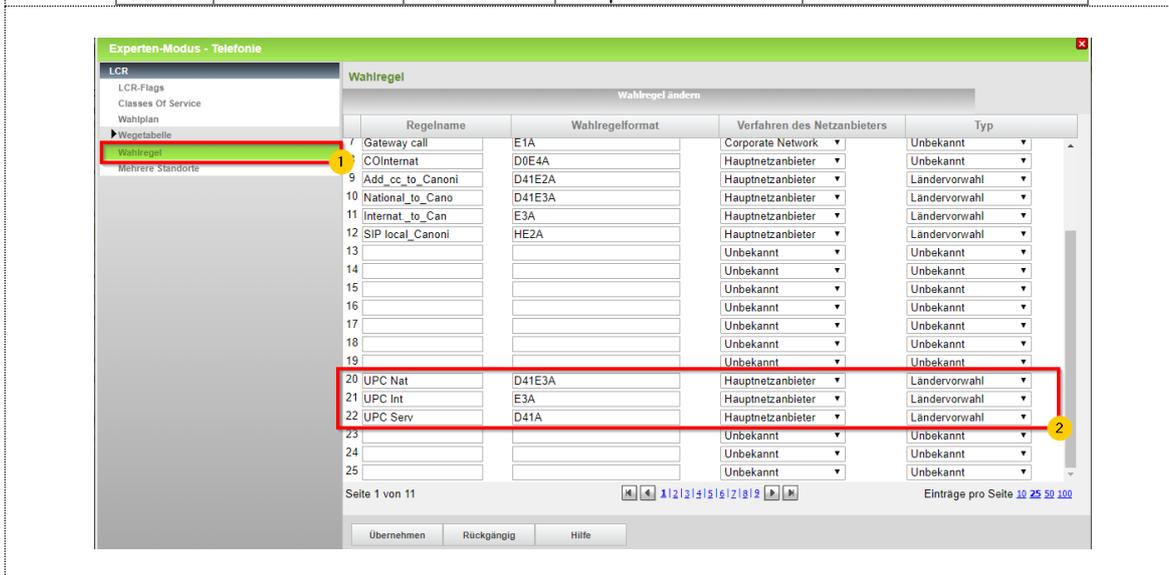
1. Experten-Modus > LCR



2.5.1 Wahlregel

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

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



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	<input type="checkbox"/>	UPC CHI	UPC Serv →	15	Keine	Nein	

Wegetabelle 81

Wegetabelle ändern							
Wegetabelle: 81							
Blockweise							
Index	Dedizierte Richtung	Richtung	Wahlregel	min. Ber.	Warnung	Dediziertes Gateway	GW Knoten-ID
1	<input type="checkbox"/>	UPC CHI	UPC Nat →	15	Keine	Nein	

Wegetabelle 82

Wegetabelle ändern							
Wegetabelle: 82							
Blockweise							
Index	Dedizierte Richtung	Richtung	Wahlregel	min. Ber.	Warnung	Dediziertes Gateway	GW Knoten-ID
1	<input type="checkbox"/>	UPC CHI	UPC Int →	15	Keine	Nein	

Wegetabelle 83

Wegetabelle ändern							
Wegetabelle: 83							
Blockweise							
Index	Dedizierte Richtung	Richtung	Wahlregel	min. Ber.	Warnung	Dediziertes Gateway	GW Knoten-ID
1	<input type="checkbox"/>	UPC CHI	UPC Int →	15	Keine	Nein	

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

Wahlplan	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

Wahlplan	Name	Gewählte Ziffern	Wegetabelle	PKZ	Wahlkontrolle	Notbetrieb
1	Emergency call	0C112	80 ▾ →	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2	Emergency call	0C117	80 ▾ →	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
3	Emergency call	0C118	80 ▾ →	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
4	Emergency call	0C144	80 ▾ →	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
5	Emergency call	0C145	80 ▾ →	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
6	Emergency call	0C1414	80 ▾ →	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Allgemeine Rufnummern

Wahlplan	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

Wahlplan	Name	Gewählte Ziffern	Wegetabelle	PKZ	Wahlkontrolle	Notbetrieb
80	Services	0C1Z	80 ▾ →	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
81	National	0C0-Z	81 ▾ →	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
82	International	0C00-Z	82 ▾ →	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
83	COInternat	0C00-41-Z	83 ▾ →	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

OpenScope Business spezifische Dienste sollten nicht angepasst werden

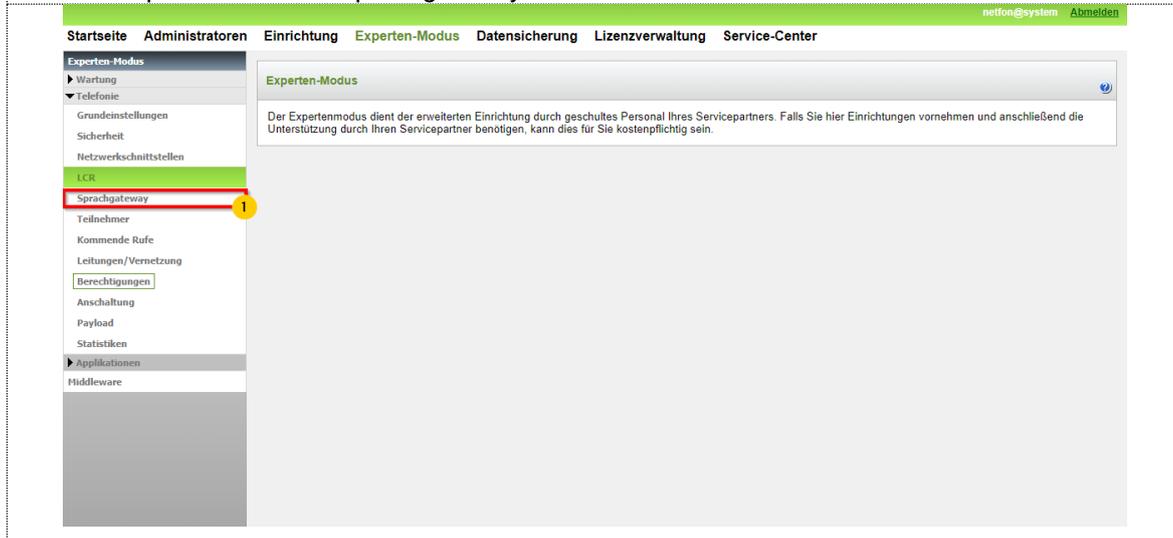
Wahlplan	Name	Gewählte Ziffern	Weg-tabelle	PKZ	Wahl-kontrolle	Not-betrieb
31	Appl-Suite	-71	12	Nein	Ja	Nein
32			-	Nein	Ja	Nein
33	IP-Network	-Z	13	Nein	Nein	Nein
34			-	Nein	Ja	Nein
35	Ann-Player	-	12	Nein	Ja	Nein

31	Appl-Suite	-71	12 ▾ →	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
32			- ▾ →	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
33	IP-Network	-Z	13 ▾ →	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
34			- ▾ →	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
35	Ann-Player	-	12 ▾ →	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

2.6 Sprachgateway

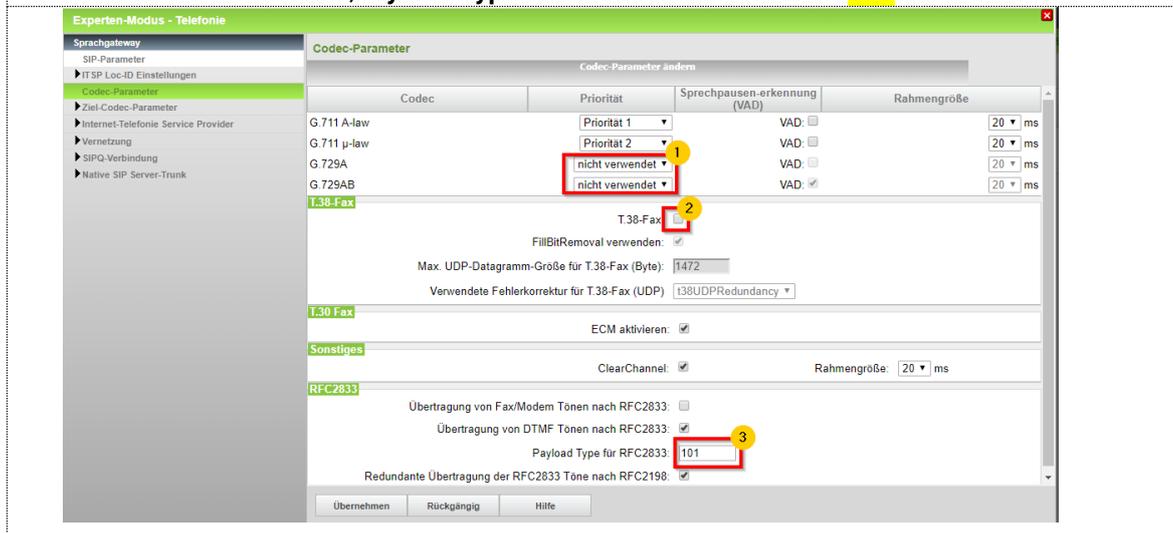
Navigieren Sie zu ‚Sprachgateway‘:

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.



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