

Telekom CompanyFlex Integration

Configuration

1. 2N Configuration
2. Telekom Restriction

1. 2N Configuration

- The 2N device must use the Telekom DNS as DNS server.
- Use the new FW 2.42 Version
- PBX Connection Setup

Haupteingang CZ | EN | DE | FR | IT | ES | RU Abmeld

SIP 1 SIP 2 Anrufe Audio Video Lokalanrufe ACS anrufen

Aktivieren eines SIP-Kontos

Identität des Gerätes ▾

Name anzeigen	Haupteingang
Telefonnummer (ID)	→XXXXXXXXXXXXXXX
Domain	tel.t-online.de


Testanruf

Authentifizierung ▾

Authentifizierungs-ID	XXXXXXXXXXXXXXX
Passwort	XXXXXXXXXX

SIP-Proxy ▾

Proxy-Adresse	hpbx.deutschland-lan.de
Proxy-Port	Default
Backup-Proxy-Adresse	

Services 

- Telefon >
- Zugangskontrolle
- Streaming
- E-Mail
- Automatisierung
- HTTP API
- Benutzertöne
- Webserver
- Audio-Test
- SNMP

SIP 1 SIP 2 Anrufe Audio Video Lokalanrufe ACS anrufen

Proxy-Port Default

Backup-Proxy-Adresse

Backup-Proxy-Port Default

SIP-Registrierung

Registrierung aktiviert

Adresse Registrar **hpbx.deutschland-ian.de**

Port Registrar Default


Adresse Backup-Registrierung

Port Backup-Registrierung Default

Registrierung erlischt **600** [s]

Registrierungszustand **ANGEMELDET**

Fehlerursache -

Services 

- Telefon >
- Zugangskontrolle
- Streaming
- E-Mail
- Automatisierung
- HTTP API
- Benutzertöne
- Webserver
- Audio-Test
- SNMP

SIP 1 SIP 2 Anrufe Audio Video Lokalanrufe ACS anrufen

Fehlerursache -

Erweiterte Einstellungen ▾

SIP Transport Protocol TCP ▾

Niedrigste erlaubte TLS Version TLS 1.2 ▾

Serverzertifikat überprüfen

Client-Zertifikat [Vom Gerät signiert] ▾

Lokaler SIP Port 5060

PRACK aktiviert

REFER aktiviert

KeepAlive Pakete absenden

IP-Adressen-Filter aktiviert

Nur verschlüsselte Anrufe empfangen (SRTP)

Verschlüsselte ausgehende Anrufe (SRTP)

MKI in SRTP-Paketen verwenden

Eingehende Early Media nicht abspielen

QoS DSCP Wert 48


Externe IP-Adresse

Ausgangs-RTP-Port 4900

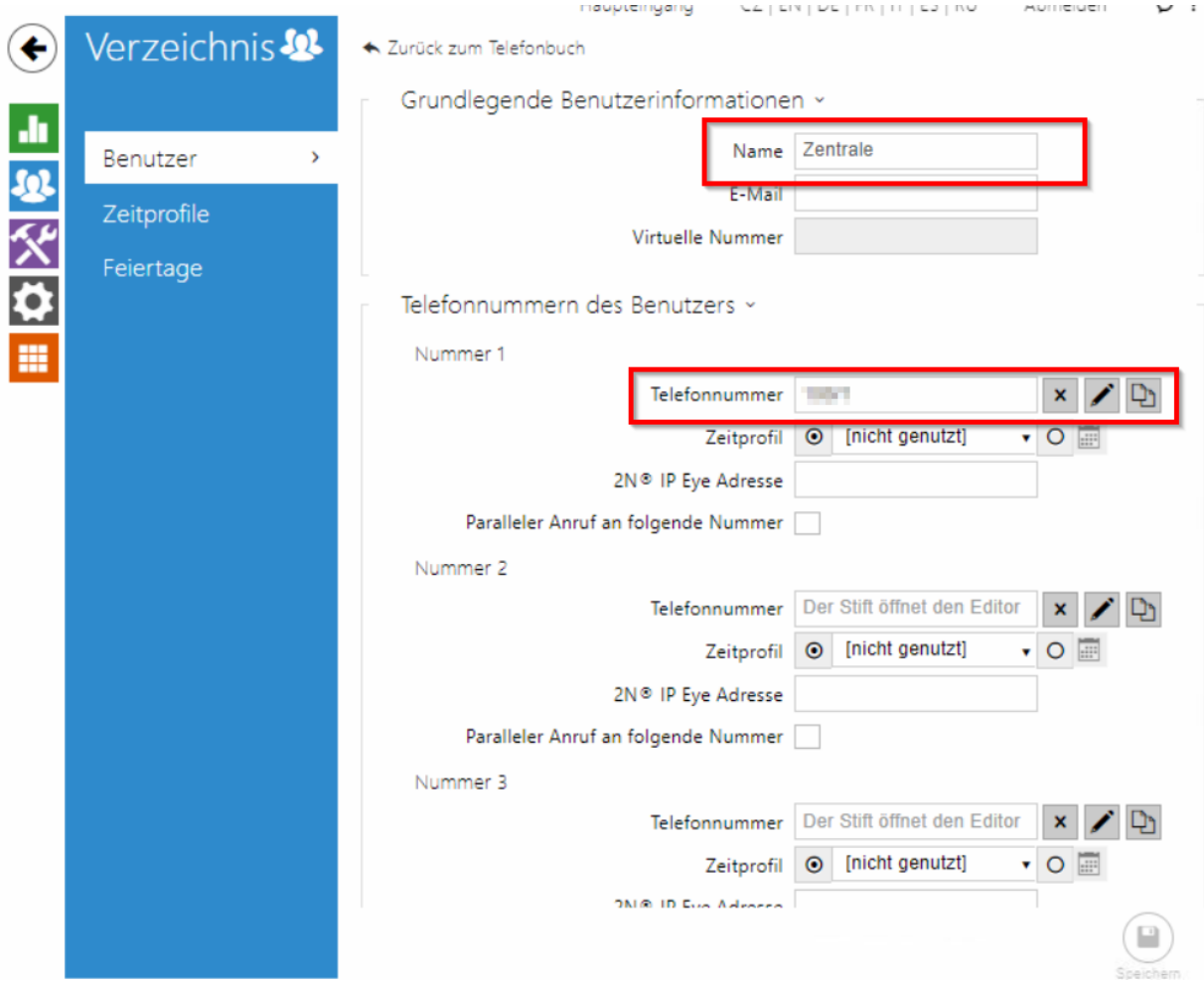
RTP-Zeitüberschreitung 60

Kompatibilität mit Broadsoft-Geräten

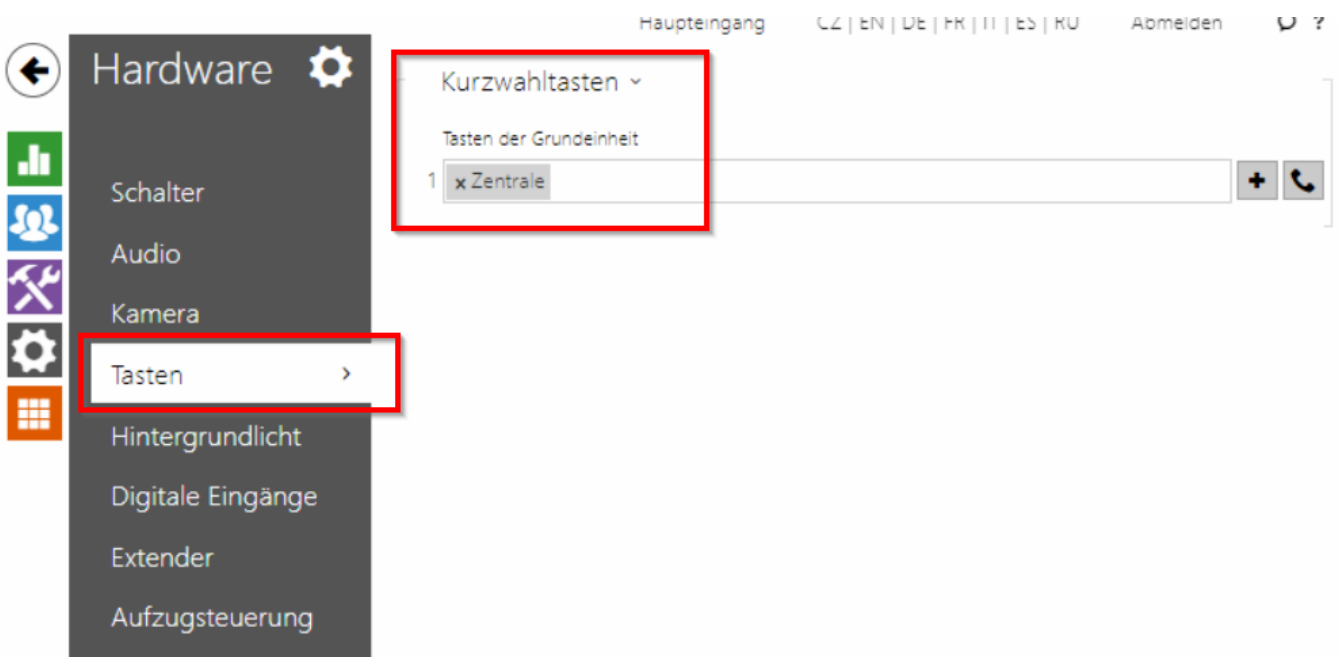
Service records rotieren

 Speichern

- Configure User



- Configure button for calling a destination



- Make sure that you are not taking any security risks when answering incoming calls

The screenshot shows the 'Services' configuration page for SIP settings. The interface includes a navigation menu on the left with options like 'Telefon', 'Zugangskontrolle', 'Streaming', 'E-Mail', 'Automatisierung', 'HTTP API', 'Benutzertöne', 'Webserver', 'Audio-Test', and 'SNMP'. The main content area is divided into sections for 'Allgemeine Einstellungen', 'Eingehende Anrufe', and 'Ausgehende Anrufe'. The 'Eingehende Anrufe' section is highlighted with a red box and contains the following settings:

- Zeitbegrenzung Anruf: 120 [s]
- Antwortmodus (SIP1): Immer besetzt
- Antwortmodus (SIP2): Immer besetzt
- Antwortmodus der Lokalanrufe: Immer besetzt
- Annehmen nach: 0 [s]
- Eingehenden Anruf mit Taste annehmen: Keine

Below the highlighted section, there is a checkbox for 'Beendigung von eingehenden Anrufen zulassen' which is checked. The 'Ausgehende Anrufe' section includes settings for 'Maximale Verbindungszeit' (32 [s]), 'Zeitbegrenzung Klingeln' (32 [s]), 'Begrenzung der Wahlzyklen' (3), a checkbox for 'Gruppengespräche bei der ersten Ablehnung beenden' (unchecked), and a dropdown for 'Tastenfunktion während des ausgehenden Anrufes' set to 'Auflegen'.

2. Telekom Restriction

- Telekom provides incorrect information on the Telekom CompanyFlex for the Universal Basic Profile. SIP Registrar is not the domain, but the proxy server

▲ SIP Accountdaten

Hier können Sie sich detaillierte Anmelde-Informationen zu Ihrem Endgerät anzeigen lassen, um Endgeräte manuell in Betrieb zu nehmen oder um aktivierte Endgeräte mit den SIP-Accountdaten zu überprüfen.

Telefone, die nicht vorkonfigurierbar sind, können Sie mit diesen SIP Accountdaten anmelden. Diese Anmeldung erfolgt durch manuelle Eingabe am Telefon.

Hinweis:

Der SIP-Client muss DNS-Abfragen von NAPTR- und SRV-Einträgen (bzgl. des Proxy-Servers) unterstützen. Für die Kommunikation ist im unverschlüsselten Fall SIP über TCP und RTP, bei Verschlüsselung SIP über TLS und SRTP erforderlich.

Registrierungsanfragen sind an den Proxy-Server zu richten, wobei die SIP-Domain im Benutzernamen übergeben wird.

Authentication Name: 67@tel.t-online.de

Authentication Password:

Benutzername: 9001@tel.t-online.de

SIP-Domain: tel.t-online.de

Proxy-Server: hpbx.deutschland-lan.de (ohne Verschlüsselung, Port 5060)
hpbxsec.deutschland-lan.de (mit Verschlüsselung, Port 5061)

Registrar: tel.t-online.de

- We as 2N are not compatible with the TLS.
 - You have to use Hpbx.deutschland-lan.de and you have to be in the local Telekom network and use Telekom DNS servers.
 - The TLS variant requires MediaSec, which we as 2N do not support.
cpbx-hilfe.deutschland-lan.de/de/ratgeber-zur-konfiguration/spezialkonfigurationen
cpbx-hilfe.deutschland-lan.de/de/ratgeber-zur-konfiguration/spezialkonfigurationen/mediasec

Mediassec (Manuelle Konfiguration von Verschlüsselung)

Für die erfolgreiche Nutzung einer verschlüsselten VoIP-Verbindung sind neben einer TLS Verbindung für die SIP-Signalisierung und SRTP für die Verschlüsselung der Sprache noch weitere zusätzliche SIP Header und SDP Attribute notwendig.

Bei der Registrierung (SIP REGISTER) wird durch die zusätzlichen SIP Header der Plattform die Nutzung der Verschlüsselungsart mitgeteilt. Beim Gesprächsaufbau (SIP INVITE) und bei der Annahme von Gesprächen (SIP Response) muss die Verschlüsselungsart und die Reichweite der Verschlüsselung (Edge zu Access-Edge, Verschlüsselung zwischen TK-Anlage und Registrierungsserver) enthalten sein.

Die SIP Header orientieren sich an einem IETF Draft (<https://tools.ietf.org/html/draft-dawes-sipcore-mediassec-parameter-11>), sind aber als statische Ergänzung der SIP Signalisierung zu sehen.

SIP REGISTER

1) Beim initialen REGISTER ohne Authentication Challenge sind die SIP Header

- Security-Client: sdes-srtp,mediasec
- Proxy-Require: mediassec
- Require: mediassec

erforderlich.

2) Die Plattform antwortet mit 401 UNAUTHORIZED. In dieser SIP Response sind die SIP Header

- Security-Server: msrp-tls,mediasec
- Security-Server: sdes-srtp,mediasec
- Security-Server: dtls-srtp,mediasec

enthalten, welche die möglichen Verschlüsselungsarten wiedergeben.

3) Beim anschließenden REGISTER mit Authentication Challenge müssen neben den ursprünglich im initialen REGISTER geschickten SIP Headern

- Security-Client: sdes-srtp,mediasec
- Proxy-Require: mediassec
- Require: mediassec

zusätzlich die SIP Header

- Security-Verify: msrp-tls,mediasec
- Security-Verify: sdes-srtp,mediasec
- Security-Verify: dtls-srtp,mediasec

ergänzt werden.

Nach RFC 3261 können die Security-Verify Header auch zusammengefasst werden und als