

FusionPBX

Configuration Sip Trunk

1. Dans Accounts > Gateways: rajouter un compte

Gateway

Defines a connections to a SIP Provider or another SIP server.

Gateway	<input type="text" value="OVH"/> <small>Enter the gateway name here.</small>
Username	<input type="text" value="0032"/> <small>Enter the username here.</small>
Password	<input type="password" value="....."/> <small>Enter the password here.</small>
From User	<input type="text"/> <small>Enter the from-user here.</small>
From Domain	<input type="text"/> <small>Enter the from-domain here.</small>
Proxy	<input type="text" value="sip5.ovh.be"/> <small>Enter the hostname or IP address of the proxy. host[:port]</small>
Realm	<input type="text" value="sip5.ovh.be"/> <small>Enter the realm here.</small>
Expire Seconds	<input type="text" value="1800"/> <small>Enter the expire-seconds here.</small>
Register	<input checked="" type="checkbox" value="True"/> <small>Choose whether to register.</small>
Retry Seconds	<input type="text" value="30"/> <small>Enter the retry-seconds here.</small>
⚙️ ADVANCED	
Context	<input type="text" value="public"/> <small>Enter the context here.</small>
Profile	<input type="text" value="external"/> <small>Enter the profile here.</small>

2. Dans Advanced > Access control: rajouter l'IP Wan du serveur SIP Trunk dans la règle Providers

Access Control

Access control list can allow or deny ranges of IP addresses.

Name	<input type="text" value="providers"/>	Enter the name.												
Default	<input type="button" value="deny"/>	Select the default type.												
Nodes	<table border="1"><thead><tr><th>Type</th><th>CIDR</th><th>Description</th><th>Action</th></tr></thead><tbody><tr><td><input type="button" value="allow"/></td><td><input type="text" value="91.121.129.133/32"/></td><td><input type="text" value="OVH"/></td><td><input type="checkbox"/></td></tr><tr><td><input type="button" value=""/></td><td><input type="text" value=""/></td><td><input type="text" value=""/></td><td><input type="checkbox"/></td></tr></tbody></table>	Type	CIDR	Description	Action	<input type="button" value="allow"/>	<input type="text" value="91.121.129.133/32"/>	<input type="text" value="OVH"/>	<input type="checkbox"/>	<input type="button" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>	<input type="checkbox"/>	Enter the description.
	Type	CIDR	Description	Action										
<input type="button" value="allow"/>	<input type="text" value="91.121.129.133/32"/>	<input type="text" value="OVH"/>	<input type="checkbox"/>											
<input type="button" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>	<input type="checkbox"/>											
Description	<input type="text"/>	Enter the description												

3. Dans Status > Sip Status: Relancer les ACL

4. Dans Dialplan > Destination: Ajouter une règle pour le numéro entrant

Destination

Inbound destinations are the DID/DDI, DNIS or Alias for inbound calls.

Type	<input type="button" value="Inbound"/>	Select the type.
Country Code	<input type="text"/>	Enter the country code.
Destination	<input type="text" value="003:"/>	Enter the destination.
Caller ID Name	<input type="text"/>	Enter the caller ID name.
Caller ID Number	<input type="text"/>	Enter the caller ID number.
Context	<input type="text" value="public"/>	Enter the context.
Conditions	<input type="text"/> <input type="text"/>	If the condition matches perform the action.
Actions	<input type="button" value="3000 AppelEntrant"/> <input type="button" value=""/>	Add additional actions.
User	<input type="text"/>	Assign this destination to a user.

Faire une restriction d'appel sur une extension

1. Dans une extension, indiquer une variable qui permettra de définir qui peut appeler l'extérieur. Ici on l'appellera Outside

Toll Allow	<input type="text" value="outside"/>	Enter the toll allow value here. (Examples: domestic,international,local)
-------------------	--------------------------------------	---

2. Dans Dialplan → Outbound Routes: rajouter une condition au début pour n'accepter que les règles toll_allow outside:

Tag	Type	Data	Break	Inline	Group	Order	Enabled	Delete
condition	\$!user_exists)	false			0	10	true	<input type="checkbox"/>
condition	\$!toll_allow)	outside			0	12	true	<input type="checkbox"/>
condition	destination_number	^!d(9,1)\$			0	20	true	<input type="checkbox"/>

Faire une règle pour n'autoriser que certains numéros

1. Dans Dialplan → Outbound rules dupliquer une règle où la destination number correspond à ce pattern:

(^0473349123\$|^0478624123\$|^019544123\$)

Tag	Type	Data	Break	Inline	Group	Order	Enabled	Delete
condition	\$!user_exists)	false			0	10	true	<input type="checkbox"/>
condition	destination_number	(^0473349123\$ ^0478624123\$ ^019544123\$)			0	20	true	<input type="checkbox"/>
action	set	sp_h_accountcode=\${accountcode}			0	30	false	<input type="checkbox"/>

Autoprovision

Snom

1. Dans l'interface du téléphone, choisir Advanced, QOS/Security et introduire le "http client" user et password qui correspond au http_auth_username et http_auth_password que vous avez défini dans les default settings de Fusion Pbx

Logout

Operation

- Home
- Directory

Setup

- Preferences
- Speed Dial
- Function Keys
- Identity 1
- Identity 2
- Identity 3
- Identity 4
- Identity 5
- Identity 6
- Identity 7
- Identity 8
- Identity 9
- Identity 10
- Identity 11
- Identity 12
- Action URI Settings
- Advanced**
- Certificates
- Software Update

Status

- System Information
- Log
- SIP Trace
- DNS Cache
- Subscriptions
- PCAP Trace
- Memory
- Settings
- Manual

snom

© Snom Technology GmbH

Network Behavior Audio SIP/RTP **QoS/Security** Update

Quality of Service

RTP Type of Service (TOS/Diffserv) 160 ?

SIP Type of Service (TOS/Diffserv) 160 ?

VLAN

VLAN Id (1-4094) ?

VLAN Priority (0-7) ?

Un-/Tag VLAN Traffic on Specific Switch Ports on off ?

PC Port

VLAN Id (1-4094) ?

VLAN Priority (0-7) ?

IEEE 802.1X Authentication:

Off ?

User ?

Password ?

Security

Ignore Security Advices on off ?

Use Hidden Tags on off ?

Restrict URI Queries on off ?

Allow CSTA Control on off ?

Empty Client Cert on off ?

Filter Packets from Registrar on off ?

Authentication for SIP Reboot on off ?

Authentication for SIP Check-Sync on off ?

Administrator Mode on off ?

Administrator Password ?

Administrator Password (Confirmation) ?

Minimum PIN Length ?

Maximum PIN Retries ?

HTTP Server

User admin ?

Password ?

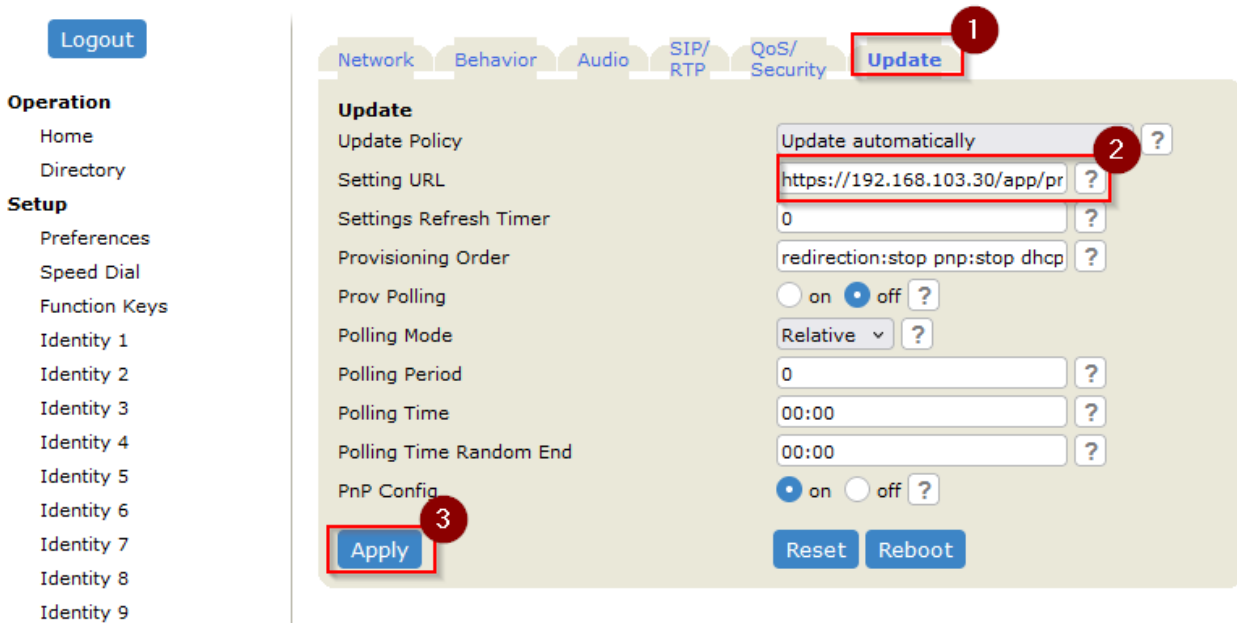
Authentication Scheme Digest Basic ?

HTTP Client

User phone_mgmt ?

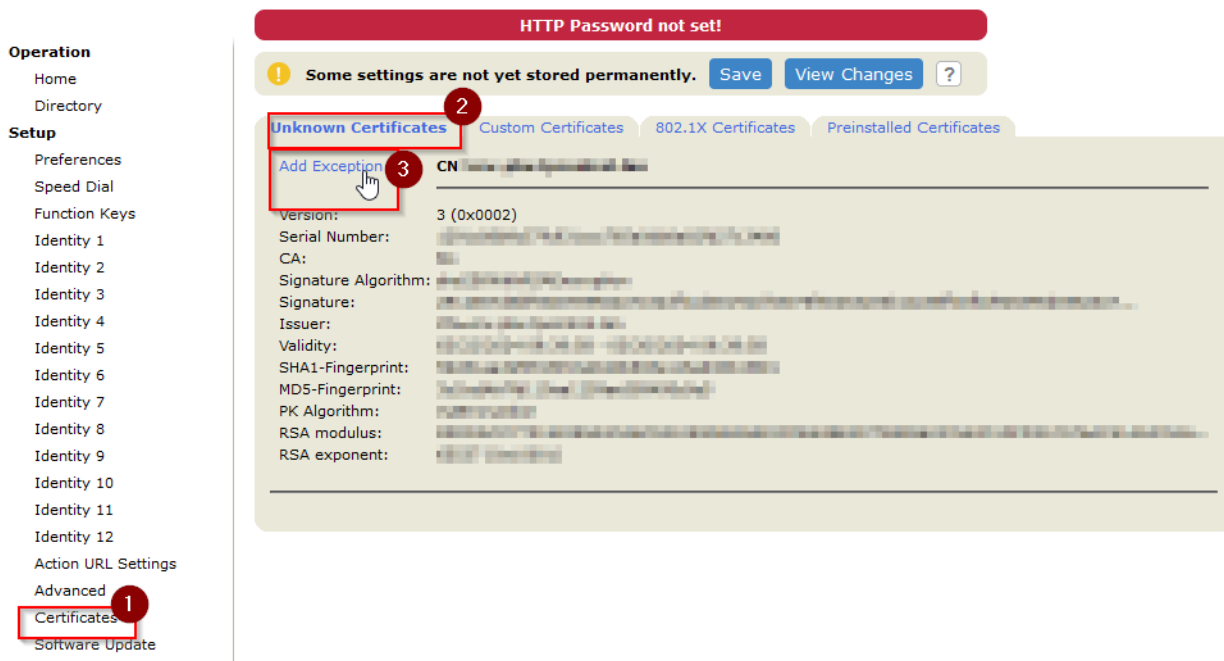
Password ?

2. Ensuite dans l'onglet Update, introduire l'url de provisioning exemple <http://192.168.103.30/app/provision/index.php?mac={mac}> et faire Apply



3. Après un redémarrage, un problème de certificat apparaîtra. Cliquez dans le menu certificats → unknown certificates et acceptez l'exception

Certificates



Debugging

sngrep

sngrep est livré par défaut et permet de voir chaque trace d'une transaction SIP

sngrep - SIP messages flow viewer								
Current Mode: Online [any]		Dialogs: 59						
Match Expression:		BPF Filter:						
Display Filter:								
Idx	Method	SIP From	SIP To	Msgs	Source	Destination	Call State	
[] 1	OPTIONS	keepalive@91.121.129.133	003271115926@sip5.ovh.be	2	91.121.129.133:5060	192.168.103.30:5080		
[] 2	REGISTER	400@192.168.103.30:5060	400@192.168.103.30:5060	4	192.168.103.150:5060	192.168.103.30:5060		
[] 3	REGISTER	400@192.168.103.30:5060	400@192.168.103.30:5060	4	192.168.103.150:5060	192.168.103.30:5060		
[] 4	INVITE	0032467767338@sip5.ovh.be	003271420647@10.7.1.163	8	91.121.129.133:5060	192.168.103.30:5080	CANCELLED	
[] 5	INVITE	0032467767338@192.168.103	301@192.168.103.101:5060	7	192.168.103.30:5060	192.168.103.101:5060	CANCELLED	
[] 6	OPTIONS	keepalive@91.121.129.133	003271115926@sip5.ovh.be	2	91.121.129.133:5060	192.168.103.30:5080		
[] 7	INVITE	0032467767338@192.168.103	302@192.168.103.101:5060	7	192.168.103.30:5060	192.168.103.101:5060	CANCELLED	
[] 8	OPTIONS	keepalive@91.121.129.133	003271115926@sip5.ovh.be	2	91.121.129.133:5060	192.168.103.30:5080		
[] 9	OPTIONS	keepalive@91.121.129.133	003271115926@sip5.ovh.be	2	91.121.129.133:5060	192.168.103.30:5080		
[] 10	OPTIONS	keepalive@91.121.129.133	003271115926@sip5.ovh.be	2	91.121.129.133:5060	192.168.103.30:5080		
[] 11	INVITE	0032495863286@sip5.ovh.be	003271420647@10.7.1.163	8	91.121.129.133:5060	192.168.103.30:5080	COMPLETED	
[] 12	INVITE	0032495863286@192.168.103	301@192.168.103.101:5060	7	192.168.103.30:5060	192.168.103.101:5060	CANCELLED	
[] 13	INVITE	0032495863286@192.168.103	302@192.168.103.101:5060	9	192.168.103.30:5060	192.168.103.101:5060	COMPLETED	
[] 14	OPTIONS	keepalive@91.121.129.133	003271115926@sip5.ovh.be	2	91.121.129.133:5060	192.168.103.30:5080		
[] 15	OPTIONS	keepalive@91.121.129.133	003271115926@sip5.ovh.be	2	91.121.129.133:5060	192.168.103.30:5080		
[] 16	INVITE	400@192.168.103.30	300@192.168.103.30:5060	10	192.168.103.150:5060	192.168.103.30:5060	COMPLETED	
[] 17	OPTIONS	keepalive@91.121.129.133	003271115926@sip5.ovh.be	2	91.121.129.133:5060	192.168.103.30:5080		
[] 18	OPTIONS	keepalive@91.121.129.133	003271115926@sip5.ovh.be	2	91.121.129.133:5060	192.168.103.30:5080		
[] 19	REGISTER	400@192.168.103.30:5060	400@192.168.103.30:5060	12	192.168.103.150:5060	192.168.103.30:5060		
[] 20	REGISTER	400@192.168.103.30:5060	400@192.168.103.30:5060	8	192.168.103.150:5060	192.168.103.30:5060		
[] 21	REGISTER	400@192.168.103.30:5060	400@192.168.103.30:5060	8	192.168.103.150:5060	192.168.103.30:5060		

From:
<https://wiki.makeitsimple.be/> - makeITsimple wiki

Permanent link:
<https://wiki.makeitsimple.be/doku.php?id=linux:fusionpbx&rev=1749377259>

Last update: 2025/06/08 10:07

