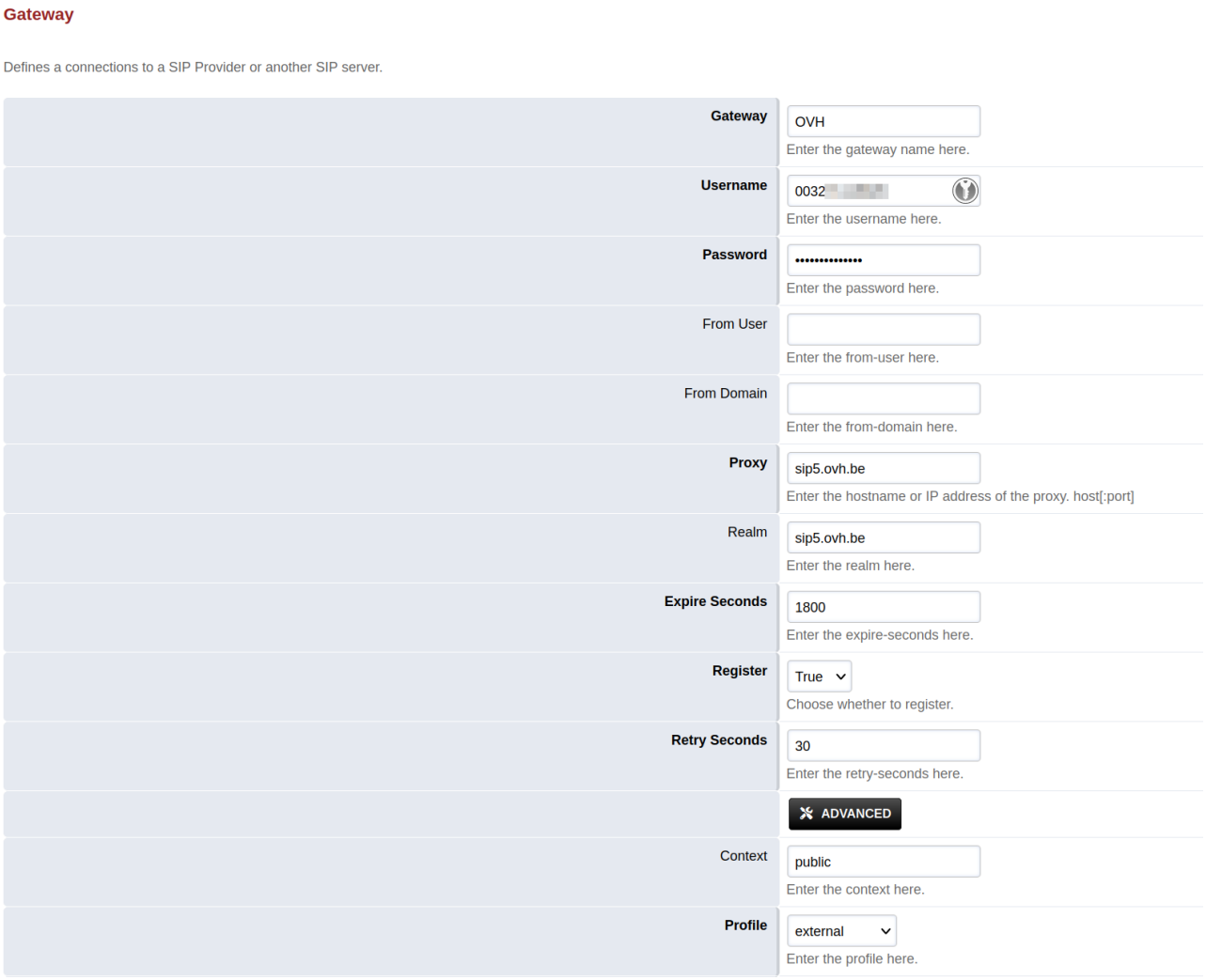
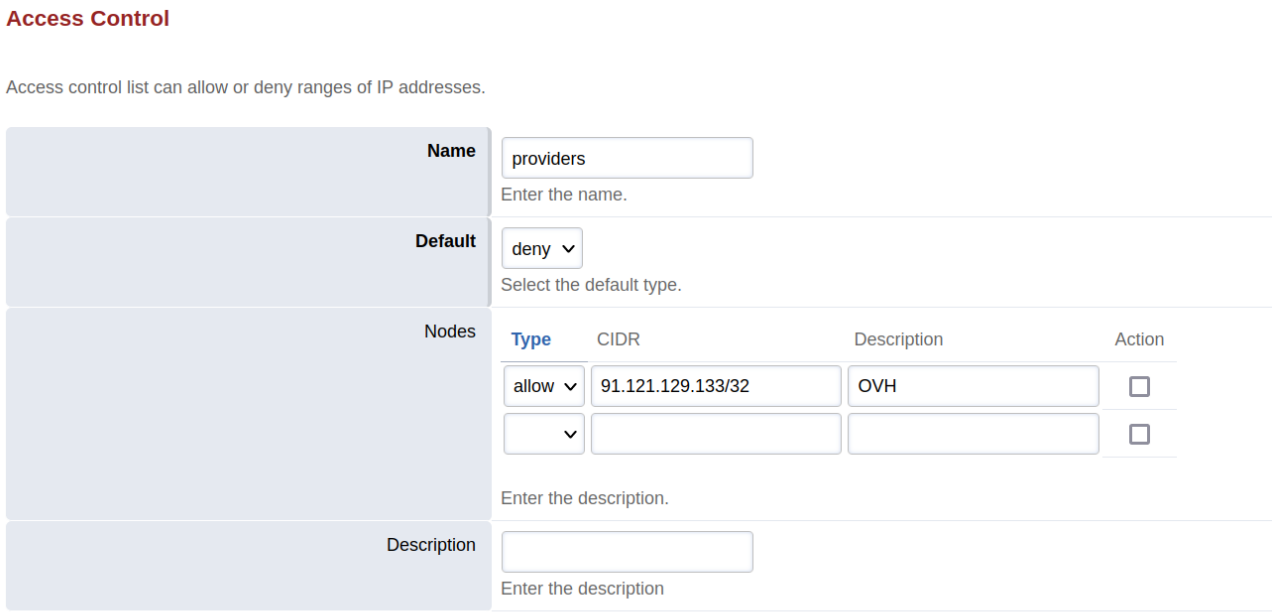
FusionPBX

Configuration Sip Trunk

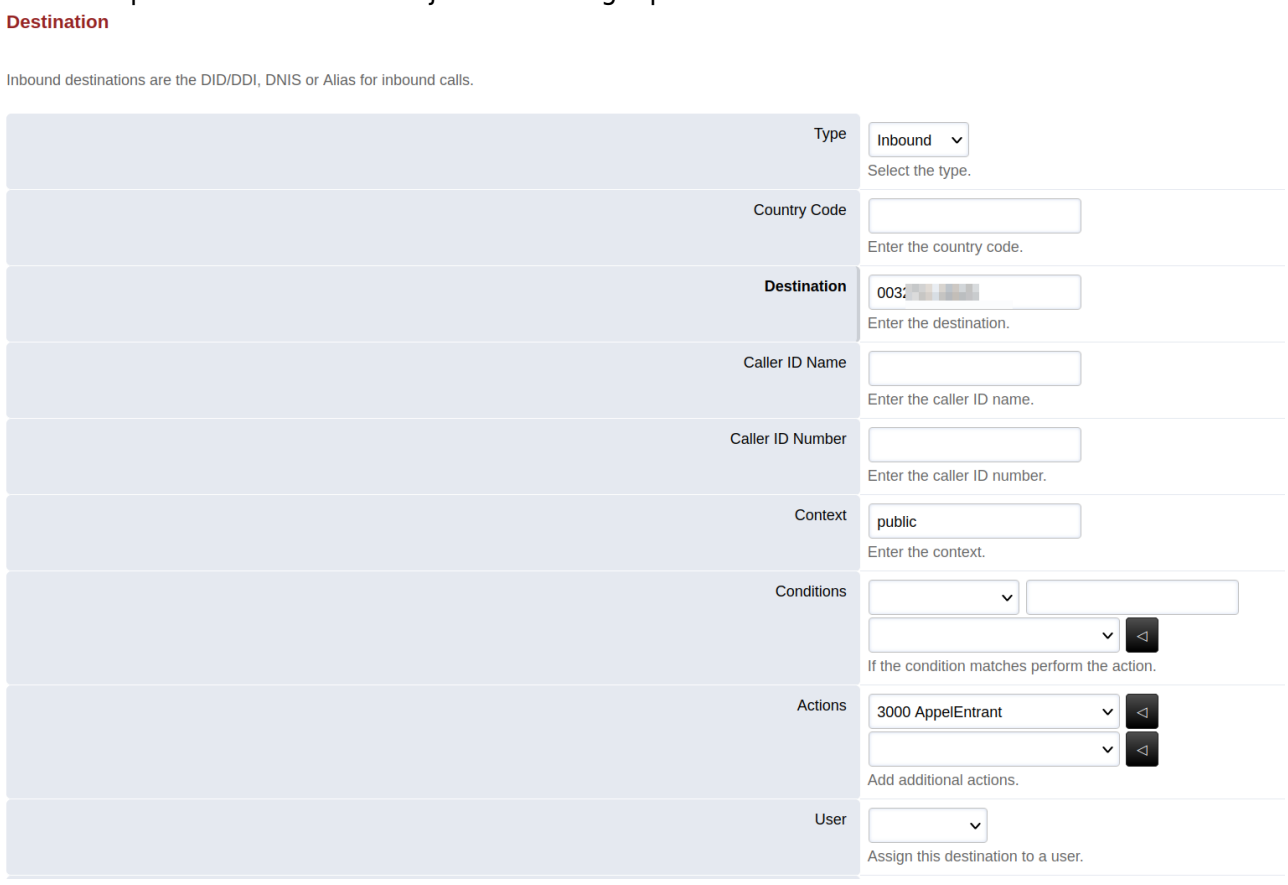
1. Dans Accounts > Gateways: rajouter un compte



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

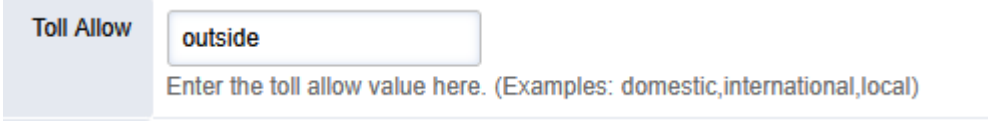


3. Dans Status > Sip Status: Relancer les ACL
4. Dans Dialplan > Destinantion: Ajouter une règle pour le numéro entrant

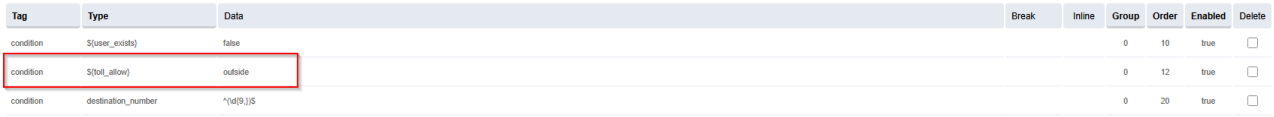


Faire une restriction d'appel sur une extension

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



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	
condition	${toll_allow}	outside			0	12	true	
condition	destination_number	^(\d{9,})$			0	20	true	

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:

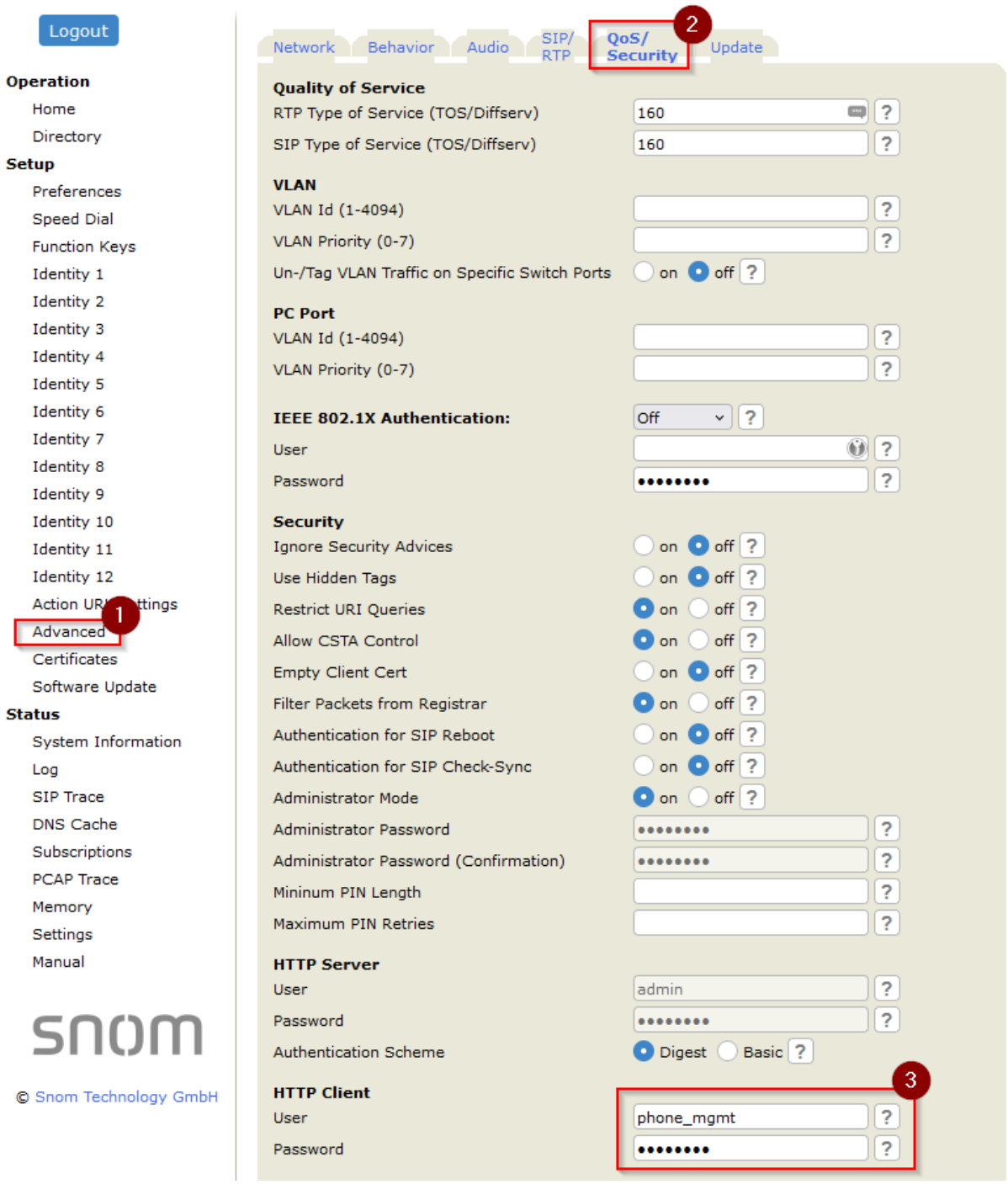
(^0473349123$|^0478624123$|^019544123$)

Tag	Type	Data	Break	Inline	Group	Order	Enabled	Delete
condition	${user_exists}	false			0	10	true	
condition	destination_number	(^0473349[redacted]$|^0478624[redacted]^019544[redacted]			0	20	true	
action	set	sip_h_accountcode=${accountcode}			0	30	false	

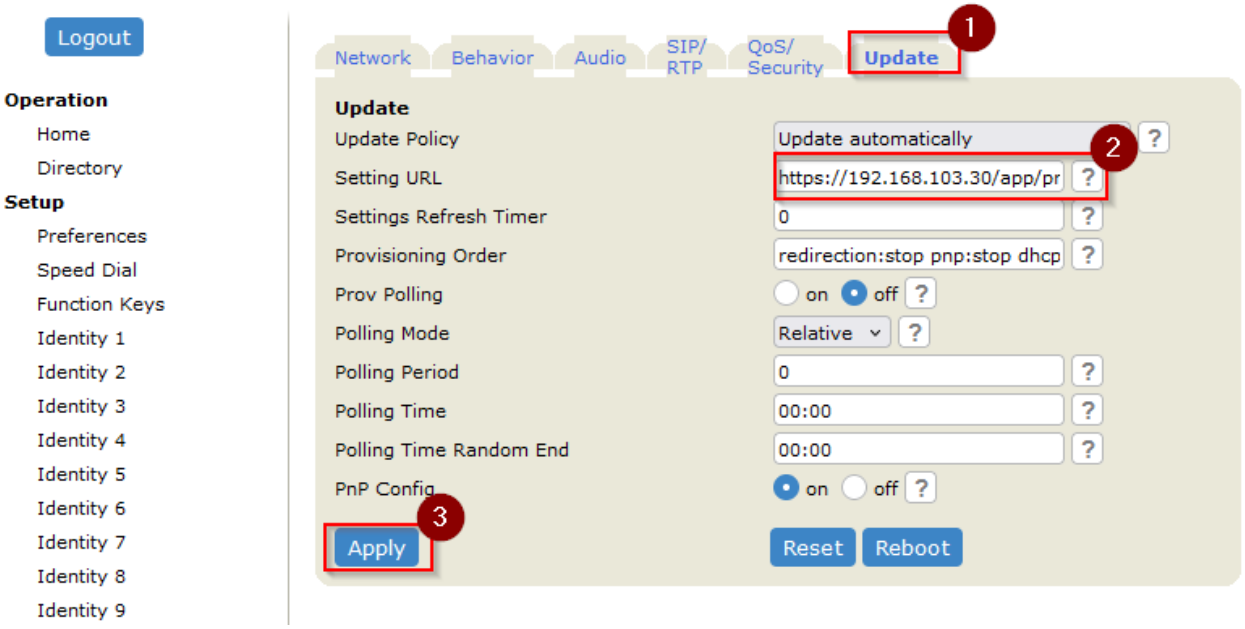
Autoprovision

Snom

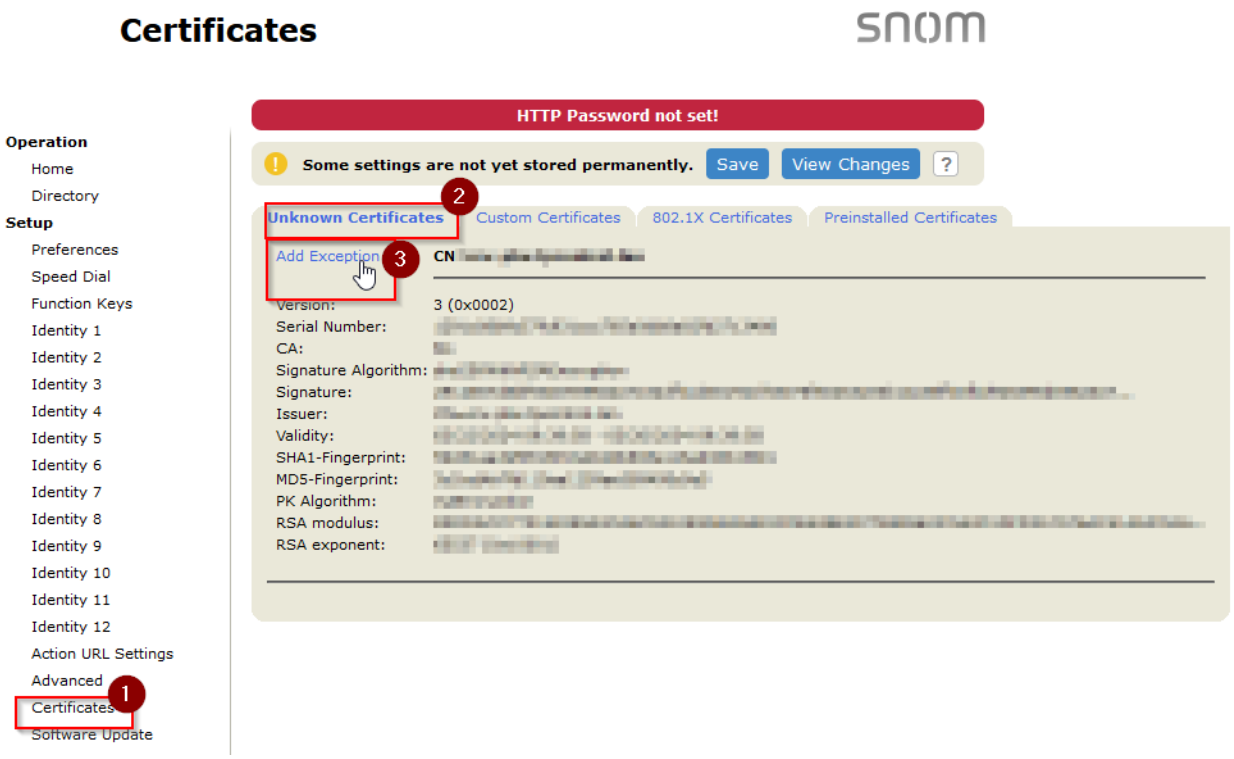
1. Dans l'interface du téléphone, choisir Advanced, QOS/Security et introduire le “http client” user et password qui correspond au http_auth_username et http_auth_password que vous avez défini dans les defautl settings de Fusion Pbx



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 apparaitra. Cliquez dans le menu certificates → unknown certificates et acceptez l'exception



Debugging

sngrep

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