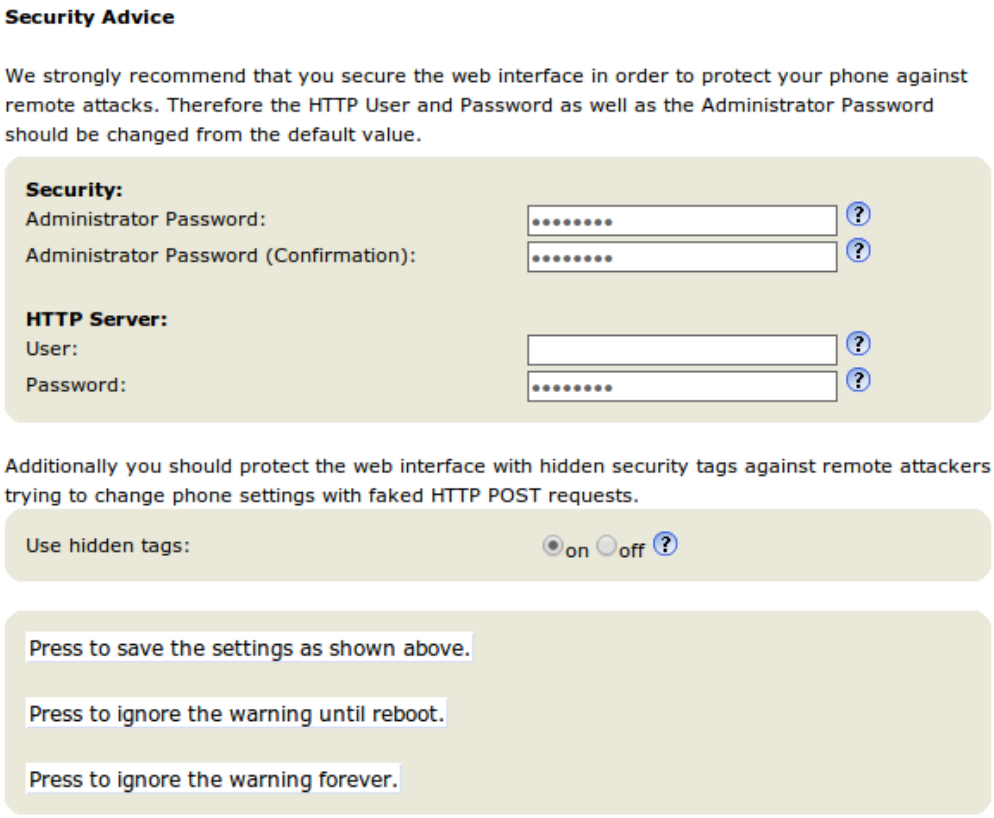
SNOM-300 SNOM-320 SNOM-820 Configuration Manual. Firmware version 8.7.3.19

How to set HTTP User and Password as well as Administrator Password

On first run of Snom we strongly recommend that you secure the web interface in order to protect your phone against remote attacks. Therefore the HTTP User and Password as well as the Administrator Password should be changed from the default value.



Setting-Up the phone for TLS

Server Authentication

Your phone also acts as a client in a couple of cases. E.g. if you register to a secure SIP proxy or if you open a Action URL over HTTPS. Normally, you do not need to worry about the server identification. Snom phones do not verify server identities by default. From FW version 8.2.30 you can explicitly state to verify server certificates though. You can activate the feature on the certificates page of the web interface:

Please carefully enable the feature. The phone will reject all secure connections of peers offering an unknown certificate that could not be verified by one of build-in CA's of the snom phone. Please refer to the Certificate Authorities tab to see which authorities are supported by the phone. Due to security concerns, you can only disable the feauture by resetting the phone to the factory defaults.

Certificates Management

A known issue in SNOM products is that they cannot follow the key chain. So you will always manage new remote certificates as exceptions, no matter if their issuer's CA is loaded in SNOM or not. We can examine some everyday cases in certificates management.

Adding Unknown Certificates

This is the most generic case you can get, as every new certificates got by your SNOM would be flagged as "unknown", thus requiring your explicit approval (which is not such a bad thing). You'll notice something is wrong eith your SNOM phone because it would reject connection to your PrivateServer if it could not verify its identification by its certificate. A notify would appears on the screen:

A certificate is trusted if its signature is signed by a certificate authority. Snom has pre-installed a couple of CA's which are listed on the *Certificate Authorities* tab of the *Certificates* page:

All rejected certificates are listed in the *Unknown Certificates* tab. If you persist on trusting the identification you can add it as an exception:

Henceforward, the certificate is listed in the *Server Certificates* tab and a connection to this identification is no longer rejected. Currently, this is the only way to add unknwon server certificates to the phone.

When a certificate is upgraded on Privateserver

If one certificate upgraded or change was performed on your PrivateServer , then you got into the case explained in this section introduction: new certificate needs to be accepted as exception. Since this is a server side change with no explicit notification to SNOM client, in order to update the client's certification setup you need to force it connecting again. This can be done using "Re-register" button shown in first image of "Basic configuration" paragraph below (which shows identity tab setup), action that forces your SNOM phone to re-register and thus negotiate server's certificate. After that action has been taken, the upgraded certificate will be listed as "Unknown" and since SNOM phone cannot follow the certificate chain, then it wouldn't be able to connect to PrivateServer . Please follow "Adding unknow certificate" section above to accept it and make your SNOM client re-register again. Now it should connect all right.

Manually Uploading Certificates

In admin mode, you can manually upload certificates in the *Unknown Certificates* tab. Every attempt to upload a unknown certificate will fail. Please refer to the log and assure your certificate is in DER format and is either signed by one of phone's authorities or server certificates.

Procedure for upgrade firmware

> The latest official firmware supported by PrivateWave Italia S.r.l. is 8.7.3.19

a. Open the Web User Interface of the snom and navigate to the Software Update page.

b. Copy and paste this URL:

http://provisioning.snom.com/download/fw/snom300-8.7.3.19-SIP-f.bin

into the Firmware field and press load

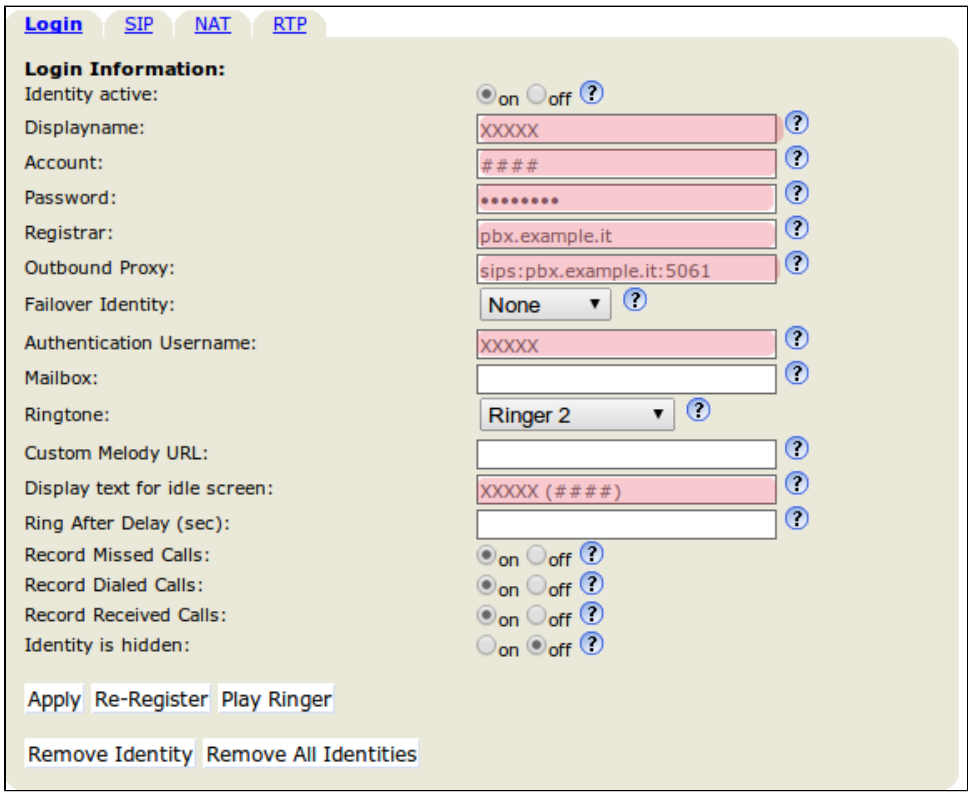
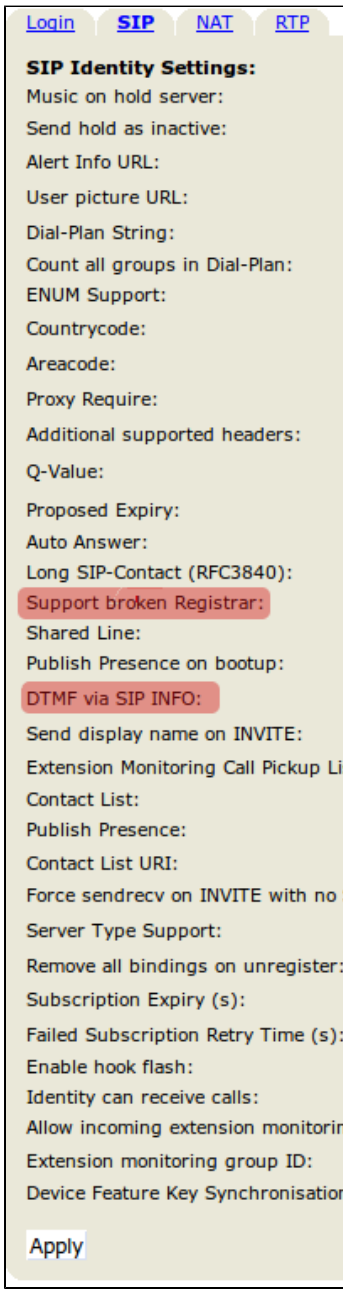
c. The phone reboots and may ask you to perform the update, click ‘Yes’.

> Do not disconnect the power at anytime!

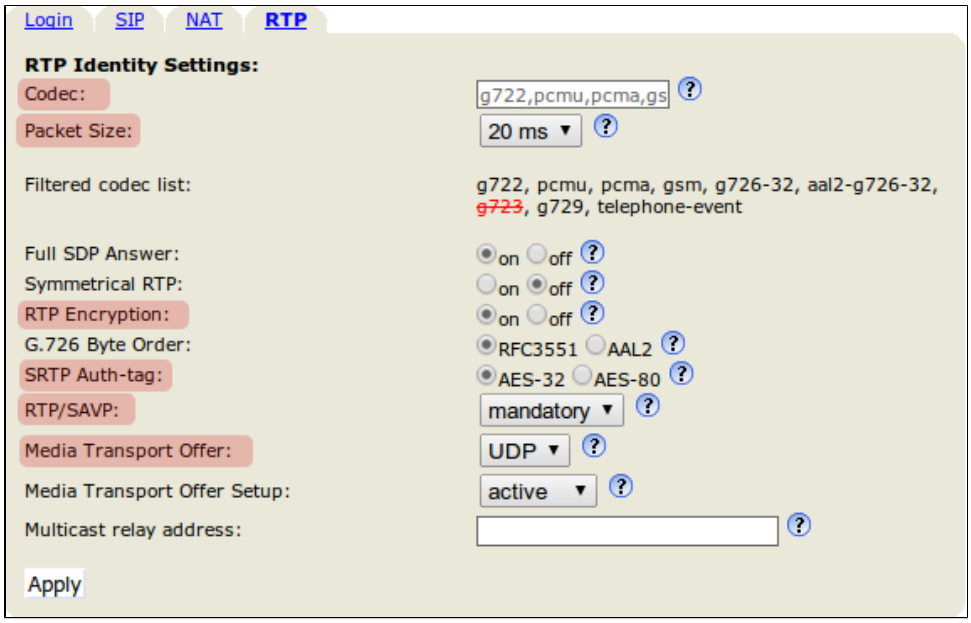
After that, the phone is upgraded to version 8.7.3.19.

Basic Configuration of the SNOM 300/320:

Open the Web User Interface of the SNOM

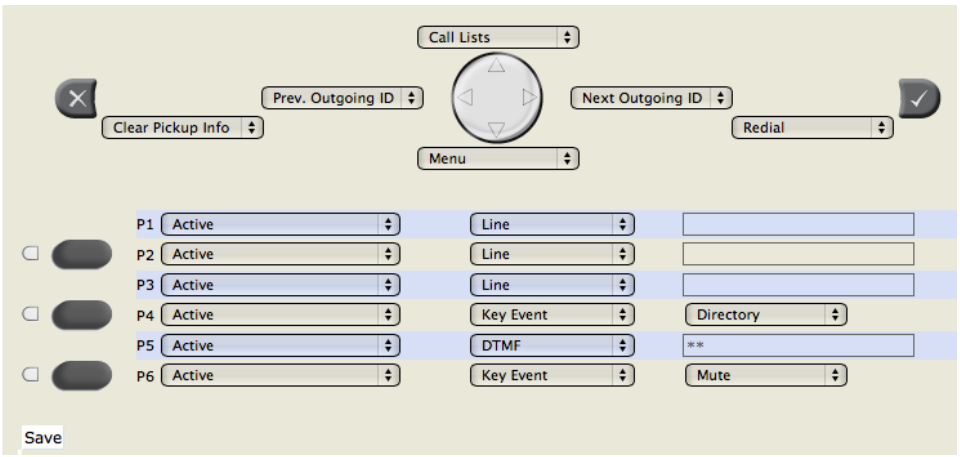
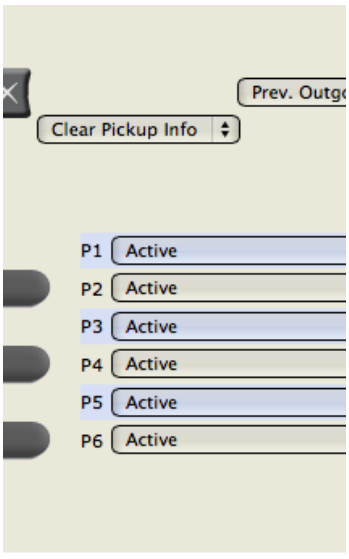
Step 1	Step 2
Navigate to the Setup/Identity1 page, login tab: • Set Account, Authentication Username and password with the correct data that you have. • Set Registrar with the IP Address (or DNS) of Server Sip. • Set Outbound Proxy in this form : 'sips:ip_of_the_srv(or dns):5061'	Goto in the Setup/Identity1 page, SIP t • Set Support Broken registrar to O • DTMF via SIP Info set to ON.
	

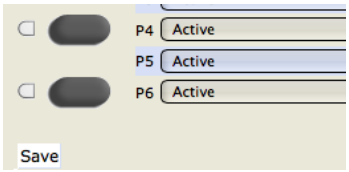
Step 3	Step 4
Goto in the Setup/Identity1 page, RTP tab: • Set Codec: g722,pcmu,pcma,gsm,g726-32,aal2-g726-32,g723,g729,telephone-event • Set RTP Encryption to ON. • Set SRTP Auth-tag to AES-32. • Set RTP/SAVP to Mandatory. • Set Packet Size to 20ms. • Set Media Transport Offer to UDP.	Goto in the Certificates: • Enable the server identity check in TLS connection by pushing the "TLS" button in "Unknown Certificates".



Advanced Configuration of the SNOM 300/320:

With the Advanced configuration we enable on the SNOM phone the "3-way call" and the "call transfer" functions.

Step 1	Step 2
Navigate to the Setup/Function Keys page: • Choose a dial pad button to edit (in the example it's P5) • Click on the drop-down menu of the "Action" (i.e. the second column)	• Choose "DTMF" • Save by pushing the "Save" butto
	

Step 3	Step 4
Insert the "*1*" string in the third column: These DTMF activate the transfer mode.	Act the same way for another dial butto train: this one activates the "3-way call'
 P5 Active DTMF *1*	 P4 Active P5 Active P6 Active Save