

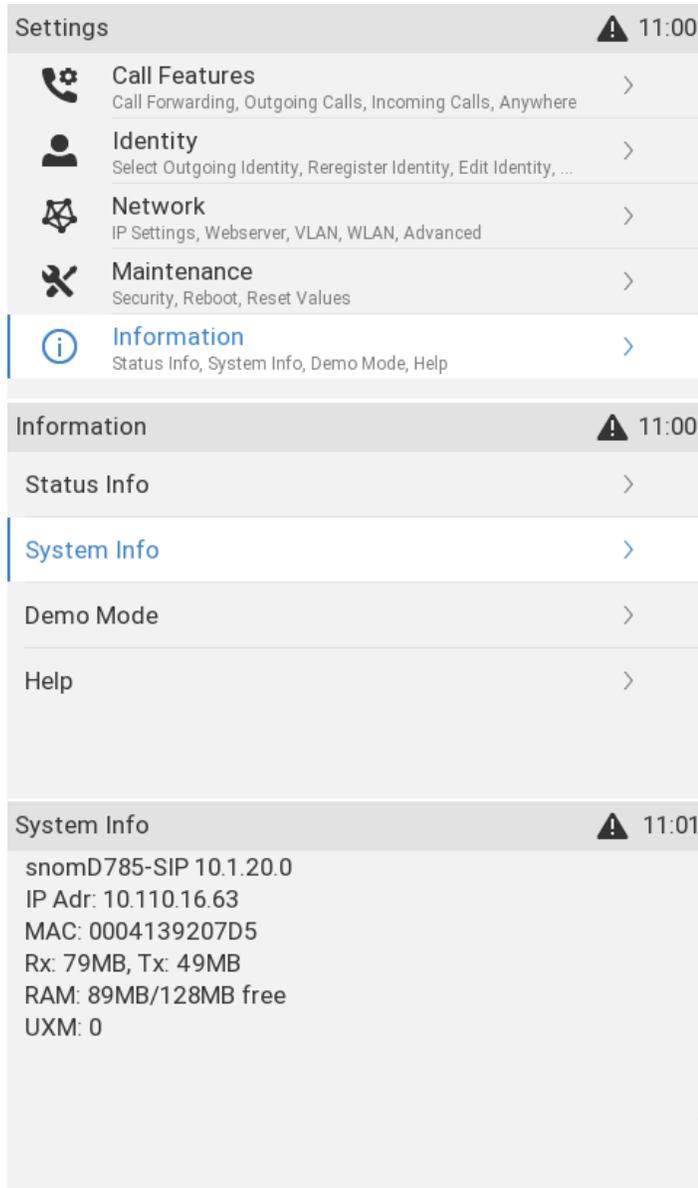
How do I secure my Snom phone

There are a few basic steps to secure your phone from external access.

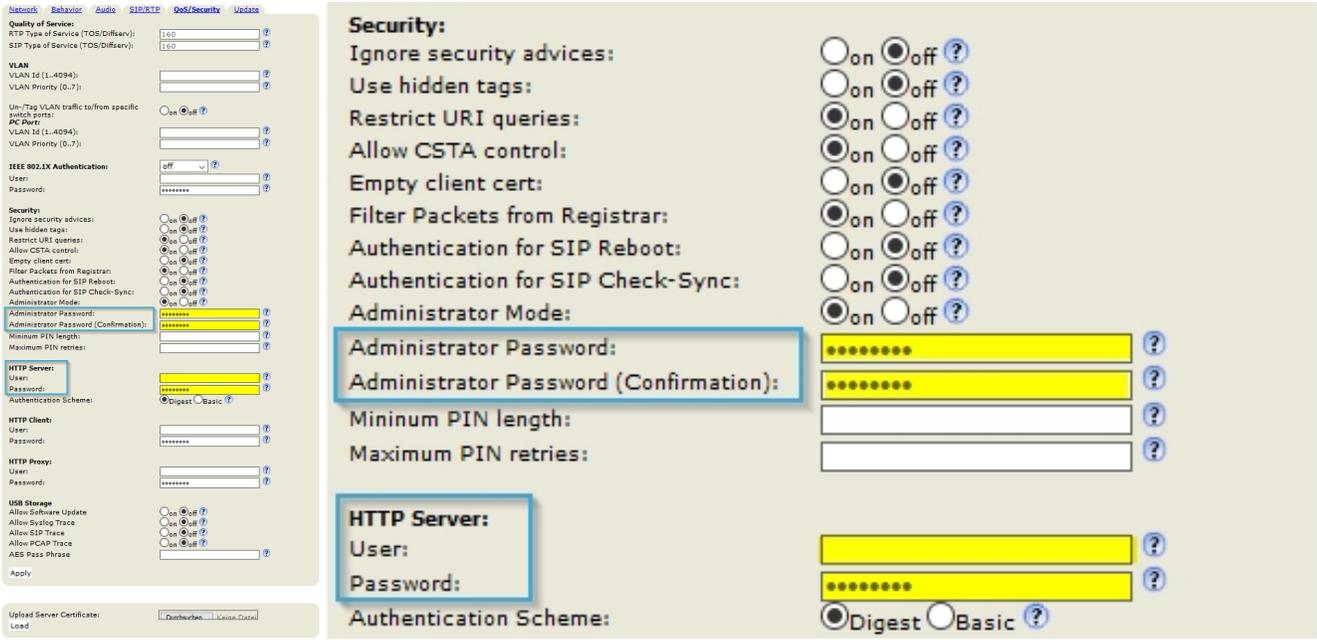
- [Step 1: Set a username and a password for the web user interface \(WUI\)](#)
- [Step 2: Disable admin mode and change the administrator password](#)
- [Step 3: Set the web server to HTTPS only type](#)
- [Step 4: Set a PIN code and keyboard locking to prevent physical abuse](#)

Step 1: Set a username and a password for the web user interface (WUI)

Look up the IP address of your phone in the phone's **Settings** menu, submenu **Information** -> **System Info**.



- Open a web browser on a PC in the same subnet as your phone and enter the **phone's IP address** in the address bar.
- On a new phone or on a phone that has been reset to factory values you will see the following page:



Advanced Authentication QoS/Security

Make sure you set

1. Administrator password (needs to be confirmed!)
2. HTTP Server User and Password (WebUI)
3. "Hidden Tags" to "on"

and click on the button "Apply".

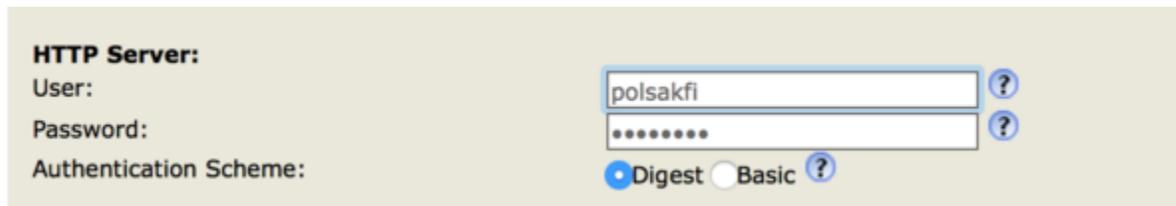
ATTENTION PLEASE:

Please do not forget to click on **save** at the top after every change in the web interface (WUI). Only then will your changes be **permanently retained even after a restart** of the phone.

Some settings are not yet stored permanently. [Save](#) [View Changes](#) [?](#)

You have taken the most important security measures. For an added layer of security, follow the below steps:

- In the vertical menu on the left side of the WUI, select **Advanced** and click the **QoS/Security** tab at the top of the page.
- Scroll down to the "HTTP Server" section and enter a username and a password. Select "Authentication scheme: **Digest**".



Confirm your changes with "Apply". These credentials will now be used to access the phone user interface.

NOTE: If you use remote provisioning and do not need access to the web user interface, you can disable it within your provisioning using [this](#) setting in order to harden your phone even more.

Step 2: Disable admin mode and change the administrator password

Most users do not require the full functionality of either the phone web user interface or the phone menu. In order to prevent users without admin rights from modifying the settings, you need to put the phone in user mode and change the default admin password (0000) on the "QoS/Security" tab.

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

Quality of Service:
RTP Type of Service (TOS/Diffserv): ?
SIP Type of Service (TOS/Diffserv): ?

VLAN
VLAN Id (1..4094): ?
VLAN Priority (0..7): ?

Un-/Tag VLAN traffic to/from 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): ?



Step 3: Set the web server to HTTPS only type

Select the "Network" tab of the **Advanced** page. Scroll down to the HTTP Section and set the "Webserver connection type" to "https only".

HTTP:
HTTP Proxy: ?
HTTP port: ?
HTTPS port: ?
Webserver connection type: ?
Auto Logout (min): ?

Click "Apply" on the bottom of the page to apply the settings.

NOTE: once you press "Apply" the web user interface will no longer be available via http://ip_address_of_phone/ but via https://ip_addresses_of_phone/

Step 4: Set a PIN code and keyboard locking to prevent physical abuse

From the vertical menu on the left side of the WUI, select **Preferences**. Scroll down to "**Lock Keyboard**" and set a [enable_keyboard_lock](#).



Lock Keyboard:
Allow keyboard locking: on off ?
Keyboard lock: on off ?
PIN to lock/unlock: ?



Further Information

- [VoIP Essentials](#)
- [Visit the Snom Forum](#)
- [Open a support ticket](#)
- [Find a local partner](#)

Related articles

- [Configuring VPN on Snom Deskphones](#)
- [Dynamic Blacklist Check](#)
- [EHS - Electronic Hook Switch](#)
- [Entering Snom Deskphone Web Interface - WUI](#)
- [How do I secure my Snom phone](#)
- [How to change phone settings via right-click in the Settings page](#)
- [I'm unable to cancel the Warning messages from the Phone menu](#)
- [Install and configure L2TP on Snom Deskphones](#)
- [Key lock on Snom phones](#)
- [Port Authentication via 802.1x - EAP-TLS](#)
- [Securing Snom phones more effectively](#)
- [Security and Privacy](#)
- [Security FAQ](#)
- [Security How-to](#)
- [Support for OpenVPN redundancy](#)
- [TLS Support](#)
- [Virtual Private Network - VPN](#)
- [VPN-Protocols](#)
- [Where can I find the supported CAs](#)
- [WUI - Advanced](#)
- [WUI - Web User Interface](#)