

FAQ - CLI access

Valid for:	N610	N670	N870	N870E	Embedded Integrator	Virtual Integrator
------------	------	------	------	-------	---------------------	--------------------

Introduction

It is possible to enable the CLI access and execute commands for different purposes.

When enabled you can access:

- DECT Manager
- Base-stations

Open the web-interface and go to: **SETTINGS - System - Web configurator - CLI access via SSH**

- Enter an CLI password

Connect via SSH using a program like **putty**.

- Username: **cli**
- Password: **What you configured**

CLI access via ssh

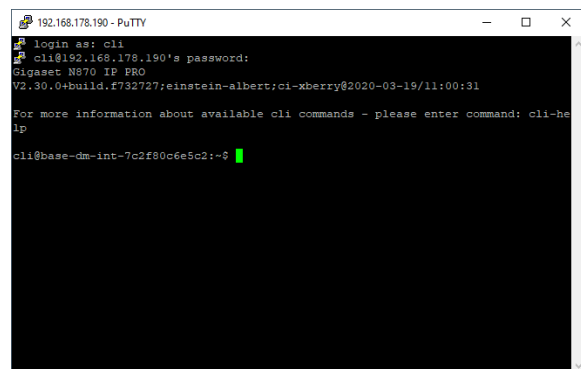
Activated if password is longer than 7 characters ⓘ

✓

CLI password ⓘ

Repeat password

☐ Show password ⓘ



```
192.168.178.190 - PuTTY
login as: cli
cli@192.168.178.190's password:
Gigaset N870 IP PRO
V2.30.0+build.f732727:einstein-albert:ci-xberry@2020-03-19/11:00:31
For more information about available cli commands - please enter command: cli-help
cli@base-dm-int-7c2f80c6e5c2:~$
```

cli-config set scpcd.lan.dm_ip

[Configure the DECT manager IP address via the cli command](#)

DHCP options

Set DHCP options (Example remove DHCP option 66)

cli-config set network.lan.reqopts='114 120 125 43 51 54 58'

network.lan.reqopts='114 66 120 125 43 51 54 58'

Set DHCP options (Example remove DHCP option 66)

cli-config set network.lan.reqopts='114 120 125 43 51 54 58'

ifconfig eth0

[View the configuration of the network interface](#)

measure-dump

[Download of DECT measurement files](#)

measure-dump [<options>]

-h Show this help
-l Lists all sites of which measurement logs are available, with information about number of files
-r <site(s)> Remove the generated measure-dump.tar file (/tmp/pub/measure-dump. tar) and the measurement logs of given site(s) (dfilt: all sites)
<site(s)> Dump measurement of given site(s), if option is not provided, all sites will be dumped

Note: Don't forget to remove your measurement data, if download was successful.
Otherwise you might leave your data on the measurement device.

reset2factory hard	Factory reset device	Needed to remove the N670 upgraded to N870 feature level
set network.lan.release=1	Send DHCP release when rebooting	<code>sudo set network.lan.release=1</code> (Enable the DHCP release) <code>sudo set network.lan.release=0</code> (Disable the DHCP release, default setting)
set-power 1	Set DECT Tx power to a specific value for example to force a handover	Set power to the lowest value <code>sudo set-power 1</code> Set power to the highest value <code>sudo set-power 10</code> Set power to the default value <code>sudo set-power 0</code> Setting per DECT base and does not survive a reboot
scheduled-reboot	Creating a reboot scheduling plan	

USAGE: scheduled-reboot --time=<HH:MM> --dow=<value> --check_intvl=<value>

Creating a reboot scheduling plan
--time=<HH:MM>: Time of day to reboot
--dow=<value>: Comma separated list of days-of-week starting with 0
e.g. "1" only on Mo
"0,1,2,3,4,5,6" daily
"0,2,4,6" Su,Tu,Th,Sa

--check-intvl=<value>: 0 Means no check for any active call - reboot is executed as planned.
--check-intvl=<value>: >0 Means how often an outstanding reboot call is suppressed if an call is active
on that device and adding a delay of 5 min before next check-interval.
When reaching the maximum check_intvl iteration while a call is still active, the current reboot job is skipped and shifted to the next reboot-job execution based on the scheduling plan. Default value is 0 -> no check.

scheduled-reboot --time=clear
Clearing the reboot scheduling plan

scheduled-reboot --time=now
reboots now without touching the scheduling plan

scheduled-reboot --show
show current reboot crontab-based entry

sysdump-all

Sysdump via CLI

Usage: sysdump-all [<options>]
-h Show this help
-c add core dump
-s add css_ramdump
-x exclude rotated /var/log/messages*.gz
-b add sysdumps from all external bases
-i exclude last incident sysdump
-e exclude database dump
-d define output directory of the generated sysdump-all.tar file (dflt: /tmp/pub/sysdump-all.tar)

tcpdump

dump traffic on a network

Example:

Dump all packets (except ssh) and pipe it to wireshark on Linux

bash -c 'ssh -o StrictHostKeyChecking=no cli@192.168.2.183 sudo tcpdump -n -i any -U port !22 -w - | wireshark -k -i -'

whereami 10

Flashing the LEDs of the current device for 10s

whoami

Print the user name associated with the current effective user id