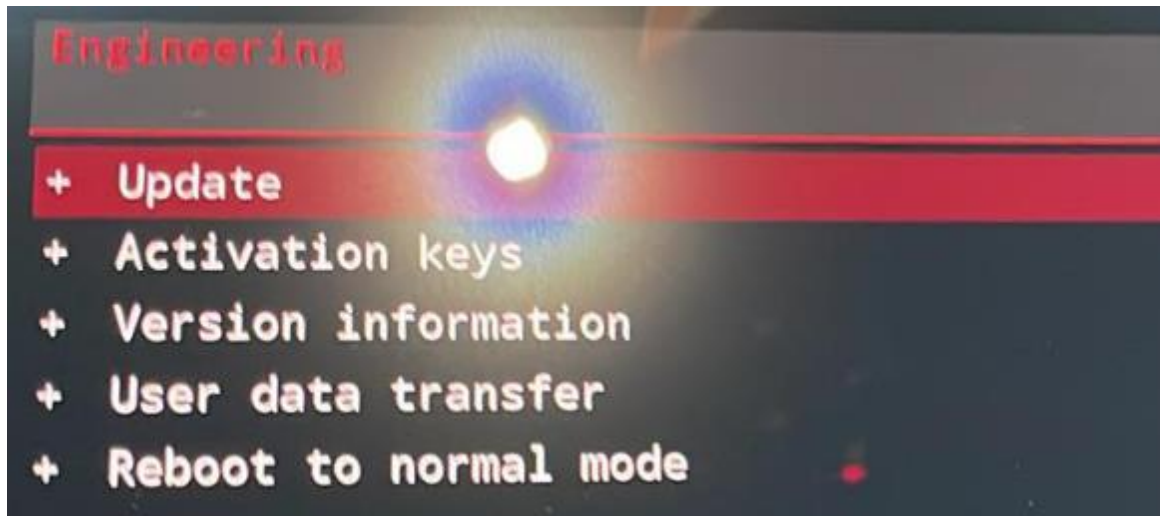


Shell access via challenge method

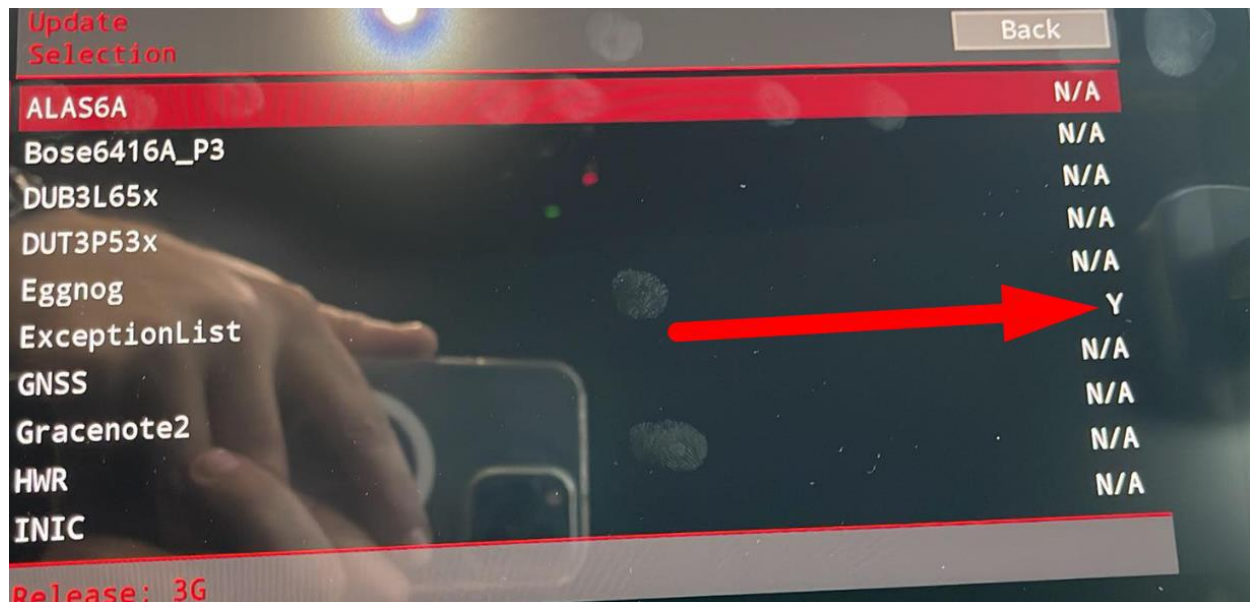
Update with “Special firmware” which changes public key of challenge. To do that. Hold two fingers in top right corner to enter **SWUP (RED)** Mode. Press +



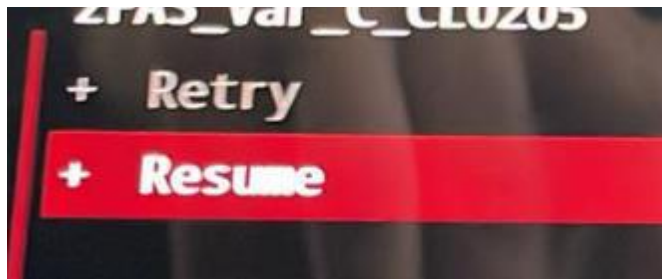
Press + **Update**



Everything should say **N/A** except **ExceptionList**. It is normal, just scroll down and press **Start update**.



After update finished, press + **Resume**



**NOTE: ALL CHANGES ON UNIT SHOULD BE DONE IN RED MENU !!!
HOLD 2 FINGERS IN TOP RIGHT CORNER, UNIT WILL GO TO RED
MENU, ONLY THEN YOU CAN CONTINUE WITH FECS/CONVERSION.**

When unit is in **red** menu, connection to unit can be done via D-Link DUB-E100. You need to change IPv4 address and mask to same as Harman uses

When unit is in **red** menu, connection to unit can be done via D-Link DUB-E100. You need to change IPv4 address and mask to same as Harman uses.

☐ Получить IP-адрес автоматически
☒ Использовать следующий IP-адрес:

IP-адрес:
 Маска подсети:
 Основной шлюз:

☐ Получить адрес DNS-сервера автоматически
☒ Использовать следующие адреса DNS-серверов:

Предпочитаемый DNS-сервер:
 Альтернативный DNS-сервер:

Challenge is on telnet **172.16.250.2.48:22111**

 PuTTY Configuration ✕

Category:

- Session
 - Logging
- Terminal
 - Keyboard
 - Bell
 - Features
- Window
 - Appearance
 - Behaviour
 - Translation
 - Selection
 - Colours
- Connection
 - Data
 - Proxy
 - SSH
 - Serial
 - Telnet
 - Rlogin
 - SUPDUP

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address) Port

Connection type:
☐ SSH ☐ Serial ☒ Other: Telnet

Load, save or delete a stored session

Saved Sessions

Default Settings

Close window on exit:
☐ Always ☐ Never ☒ Only on clean exit

Copy **CHALLENGE KEY** and send

```
172.16.250.248 - PuTTY
320A423835333039333235313932304539410A4445565F4D4D5832505F41555F45525F4733355F35
313150524F440A313566663034383032343030303030303030373430383935633930303030303030310A
4150552D30303133312E30332E313932415031303131300A
```

Copy **mmx_response.**, CTRL + A (Select all), CTRL + C (Copy all) and paste response with right click into **same** putty window!

CHALLENGE

RESPONSE

```
172.16.250.248 - PuTTY
320A423835333039333235313932304539410A4445565F4D4D5832505F41555F45525F4733355F35
313150524F440A31356666303438303234303030303030303030373430383935633930303030303030310A
4150552D30303133312E30332E313932415031303131300A^C
```

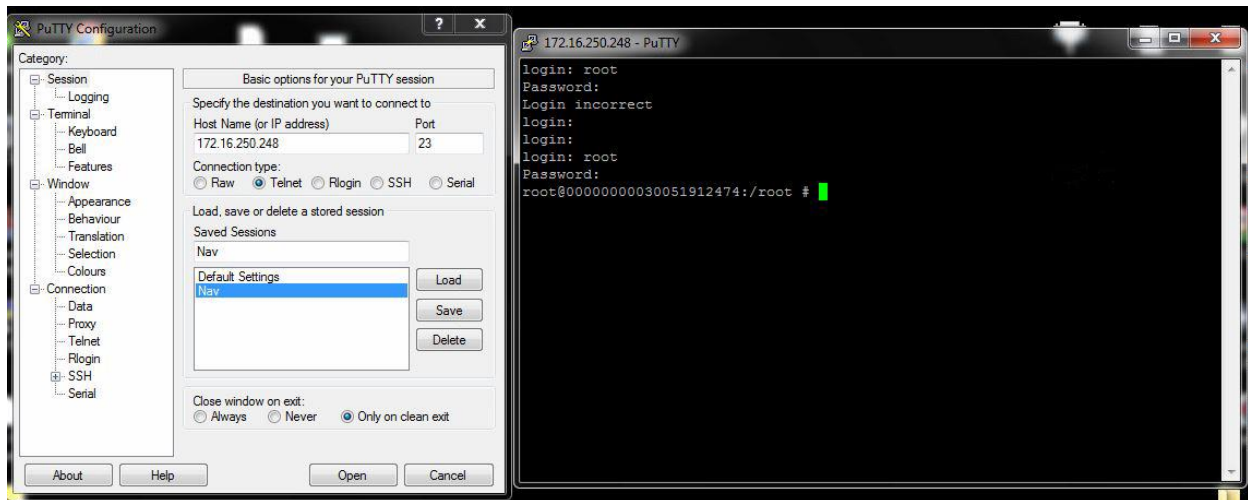
Press Enter. Putty should close.

MMX console
Challenge

Telnet: 172.16.250.248:23
Telnet:172.16.250.248:22111

Now you have opened telnet access and can connect with port 23.

Note: If you can't login, you are probably in normal, not in red menu. Go to red menu, and try to login then.



**To disable password you need to run these commands:
RUN ALL COMMANDS ONLY FROM RED MENU !!)**

```
mount -t qnx6 /dev/mnanda0t177.2 /mnt/swup
cp /mnt/swup/etc/nopasswd /mnt/swup/etc/passwd
sync
```

Now, even after reboot, your unit will have no password.

backup before modifying or patching any files

mount -a

mount -uw /fs/sdb0/

cat /dev/fs0 > /fs/sdb0/fs0_mib2p

cat /eso/bin/apps/fecmanager > /fs/sdb0/fecmanager

cat /eso/bin/apps/componentprotection > /fs/sdb0/componentprotection

mkdir /fs/sdb0/fec_backup/

cp -f /mnt/persist_new/fec/* /fs/sdb0/fec_backup/

FEC keys Edit on hex:

granted.fecs																ANSI ASCII	
Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
00000000	B6	78	3D	4C	02	00	00	00	00	C3	11	07	FF	FF	FF	FF	ix=L Å ýýýý
00000016	03	2B	99	34	A9	96	57	41	31	46	56	41	46	31	34	4B	+™4@-WAlFVAF14K
00000032	44	30	30	37	37	35	32	00	5B	98	9D	D3	08	00	04	01	D007752 [~Ó
00000048	00	02	61	00	F0	00	05	00	00	00	07	02	00	00	03	00	a ð
00000064	00	00	06	08	00	00	06	09	00	00	06	0F	00	0E	AB	77	«w
00000080	7C	CF	49	CE	A7	92	11	F9	AD	70	20	70	D2	E2	08	D5	İİİs' ù-p pòá Œ
00000096	90	75	67	2F	A6	D5	DC	2B	CA	90	89	AA	FB	5A	FF	13	ug/;ŒŬ+Ê %*ûZý
00000112	69	6B	43	FA	C4	64	E5	5E	9F	26	E3	B5	3B	DC	29	AB	ikCúÄdâ^Ÿ&âµ;Ŭ)«
00000128	4B	DA	6A	31	73	28	E8	D6	EC	B2	EE	4A	09	1A	C6	3F	KŬj1s(èŒi*îŬ Æ?
00000144	45	A5	39	13	90	20	2D	49	8C	D9	47	7F	80	D2	C2	65	E¥9 -İŒŬG èŒâe
00000160	8D	F6	80	72	9E	5E	67	07	E9	6F	D1	AB	21	94	94	2F	öErž^g éoŒ«!""/
00000176	79	14	6F	83	55	E4	77	89	61	2A	16	AB	50	38	7B	77	y ofUâwka* «P8{w
00000192	51	94	AB	E0	1A	28	39	3E	D9	93	BC	4B	A2				Q"«â (9>Ŭ"4Kc

Put fecmanager and granted.fecs to SD, then login to unit and use commands:

mount -t qnx6 /dev/mnanda0t177.1 /tmp/177.1

mount -t qnx6 /dev/mnanda0t177.2 /tmp/177.2

mount -t qnx6 /dev/mnanda0t177.3 /tmp/177.3

mount -uw /tmp/177.1

mount -uw /tmp/177.2

mount -uw /tmp/177.3

/fs/sdb0/fecmanager

cp -Vf /fs/sdb0/fecmanager /tmp/177.1/eso/bin/apps/fecmanager

```
chmod 777 /tmp/177.1/eso/bin/apps/fecmanager  
cp -Vf /fs/sdb0/fecmanager /tmp/177.2/eso/bin/apps/fecmanager  
chmod 777 /tmp/177.2/eso/bin/apps/fecmanager  
cp -Vf /fs/sdb0/fecmanager /tmp/177.3/eso/bin/apps/fecmanager  
chmod 777 /tmp/177.3/eso/bin/apps/fecmanager
```

Fec:

```
rm -f /mnt/persist_new/fec/*.hist  
rm -f /mnt/persist_new/fec/*.fecs  
cd /mnt/persist_new/fec  
cp -Vf /fs/sdb0/granted.fecs /mnt/persist_new/fec/  
restart unit hold Power button
```

