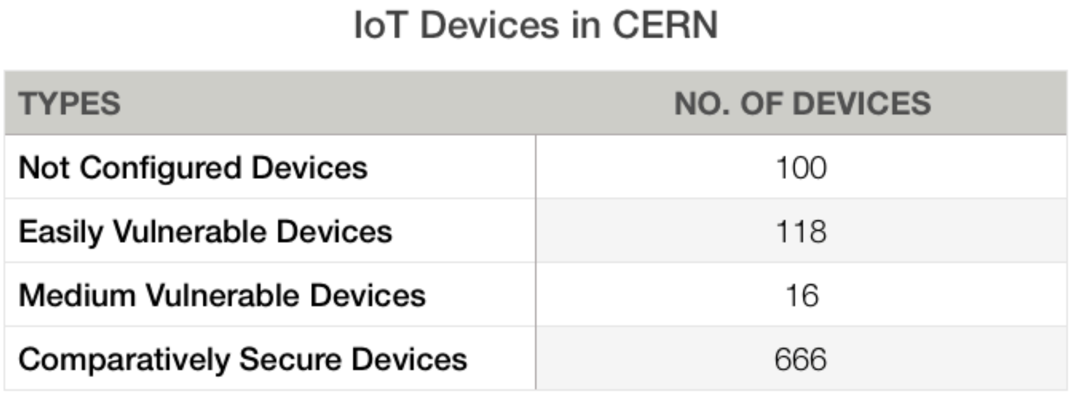
SECURING IOT DEVICES

SHARAD AGARWAL
CERN COMPUTER SECURITY TEAM

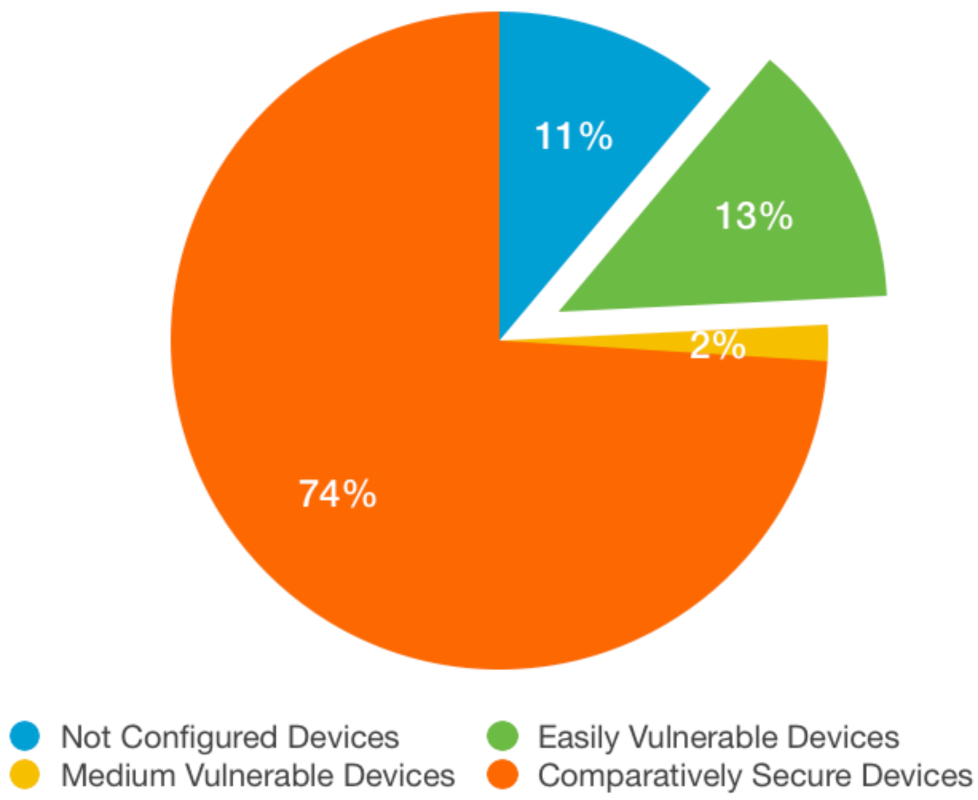
CERN has approximately 900 IoT Devices connected on the General Purpose Network (GPN).



IoT Devices in CERN

TYPES	NO. OF DEVICES
Not Configured Devices	100
Easily Vulnerable Devices	118
Medium Vulnerable Devices	16
Comparatively Secure Devices	666

Overview of Vulnerable IoT Devices

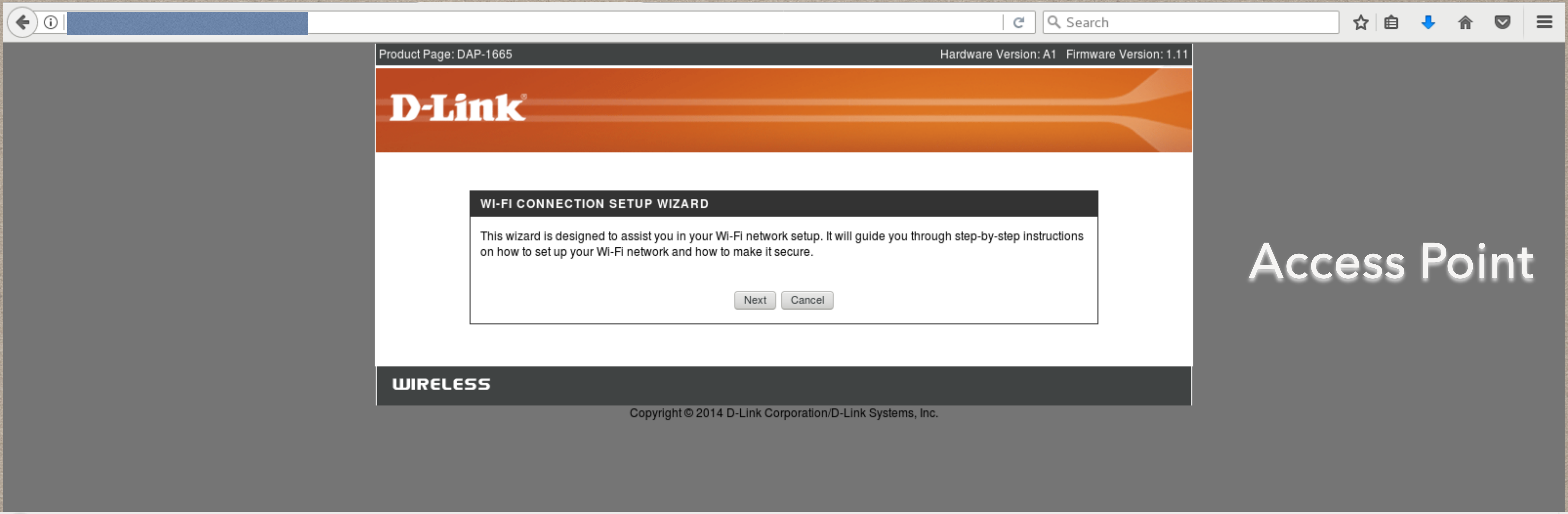


Devices at CERN

1. Switches
2. Routers
3. Thermometers
4. PLCs
5. CCTVs/Webcams
6. Sensors
7. Oscilloscopes
8. IP Phones
9. Anywhere USB
10. NAS
11. Printers
12. Projectors
13. MLCs
14. Conference mics
15. IPMI
16. Infoscreens
17. Power Supply
18. Arduinos
19. Raspberry Pi

and more

Non Configured Devices



[redacted]

Product Page: DAP-1665 Hardware Version: A1 Firmware Version: 1.11

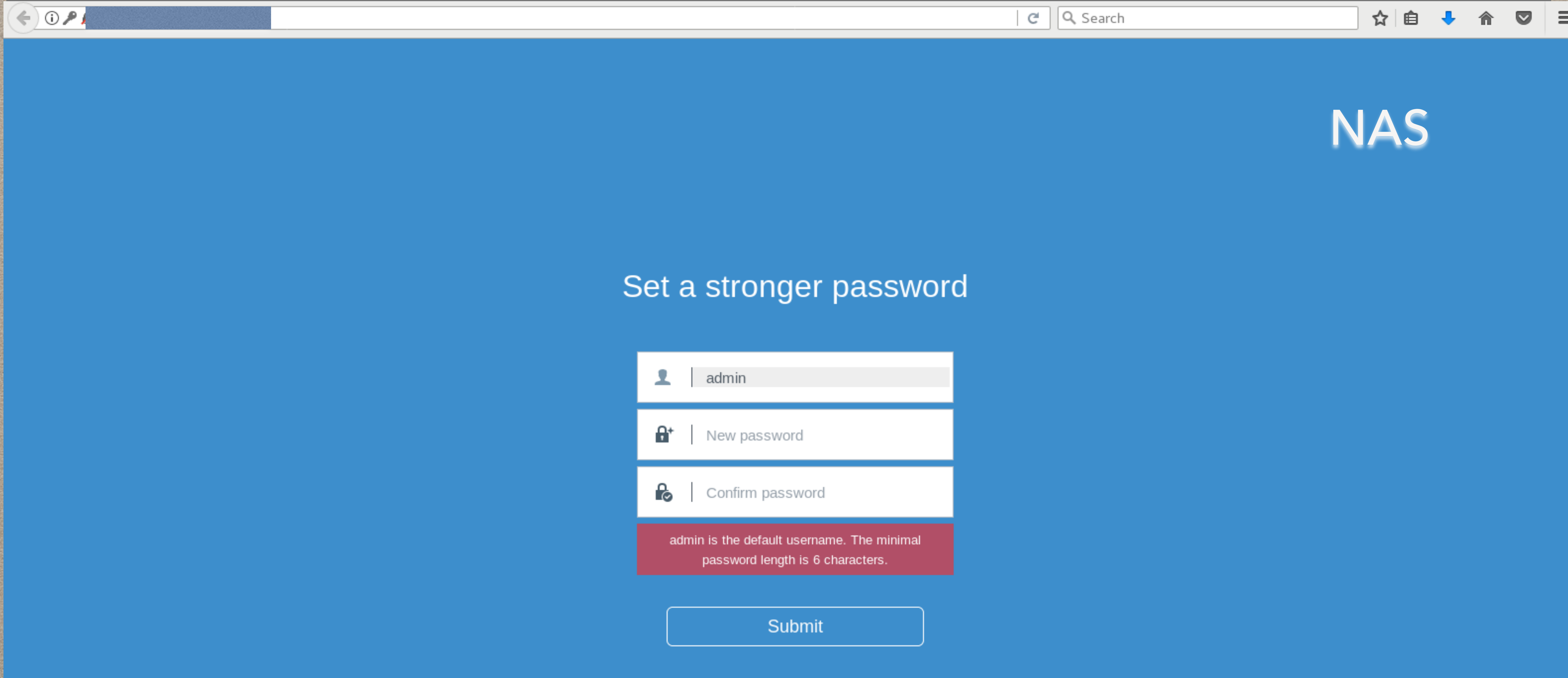
D-Link

WI-FI CONNECTION SETUP WIZARD

This wizard is designed to assist you in your Wi-Fi network setup. It will guide you through step-by-step instructions on how to set up your Wi-Fi network and how to make it secure.

Copyright © 2014 D-Link Corporation/D-Link Systems, Inc.

Access Point



[redacted]

NAS

Set a stronger password

admin

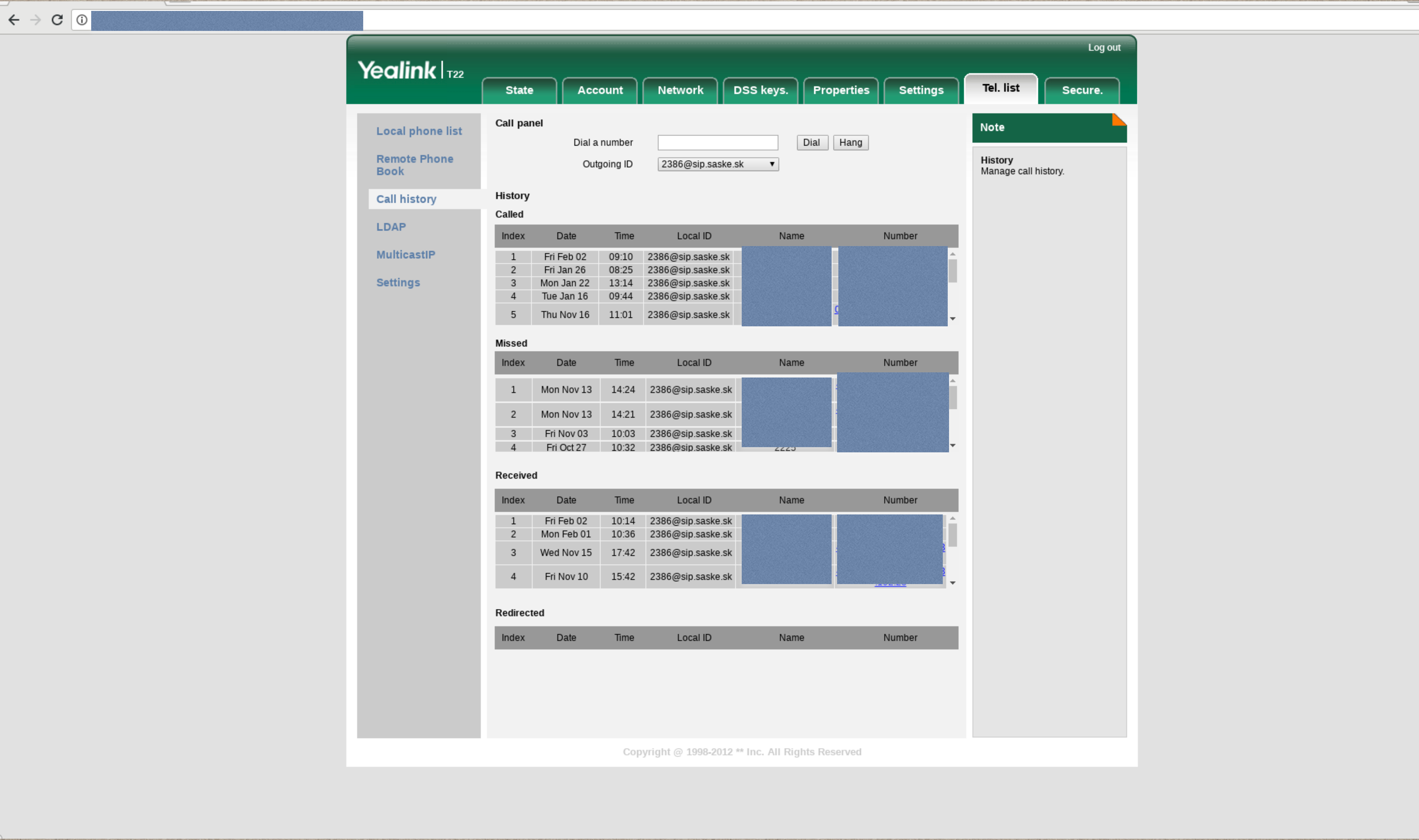
New password

Confirm password

admin is the default username. The minimal password length is 6 characters.

Easily Vulnerable Devices

IP Phone



Call panel

Dial a number

Outgoing ID: 2386@sip.saske.sk

History

Called

Index	Date	Time	Local ID	Name	Number
1	Fri Feb 02	09:10	2386@sip.saske.sk	[redacted]	[redacted]
2	Fri Jan 26	08:25	2386@sip.saske.sk	[redacted]	[redacted]
3	Mon Jan 22	13:14	2386@sip.saske.sk	[redacted]	[redacted]
4	Tue Jan 16	09:44	2386@sip.saske.sk	[redacted]	[redacted]
5	Thu Nov 16	11:01	2386@sip.saske.sk	[redacted]	[redacted]

Missed

Index	Date	Time	Local ID	Name	Number
1	Mon Nov 13	14:24	2386@sip.saske.sk	[redacted]	[redacted]
2	Mon Nov 13	14:21	2386@sip.saske.sk	[redacted]	[redacted]
3	Fri Nov 03	10:03	2386@sip.saske.sk	[redacted]	[redacted]
4	Fri Oct 27	10:32	2386@sip.saske.sk	[redacted]	[redacted]

Received

Index	Date	Time	Local ID	Name	Number
1	Fri Feb 02	10:14	2386@sip.saske.sk	[redacted]	[redacted]
2	Mon Feb 01	10:36	2386@sip.saske.sk	[redacted]	[redacted]
3	Wed Nov 15	17:42	2386@sip.saske.sk	[redacted]	[redacted]
4	Fri Nov 10	15:42	2386@sip.saske.sk	[redacted]	[redacted]

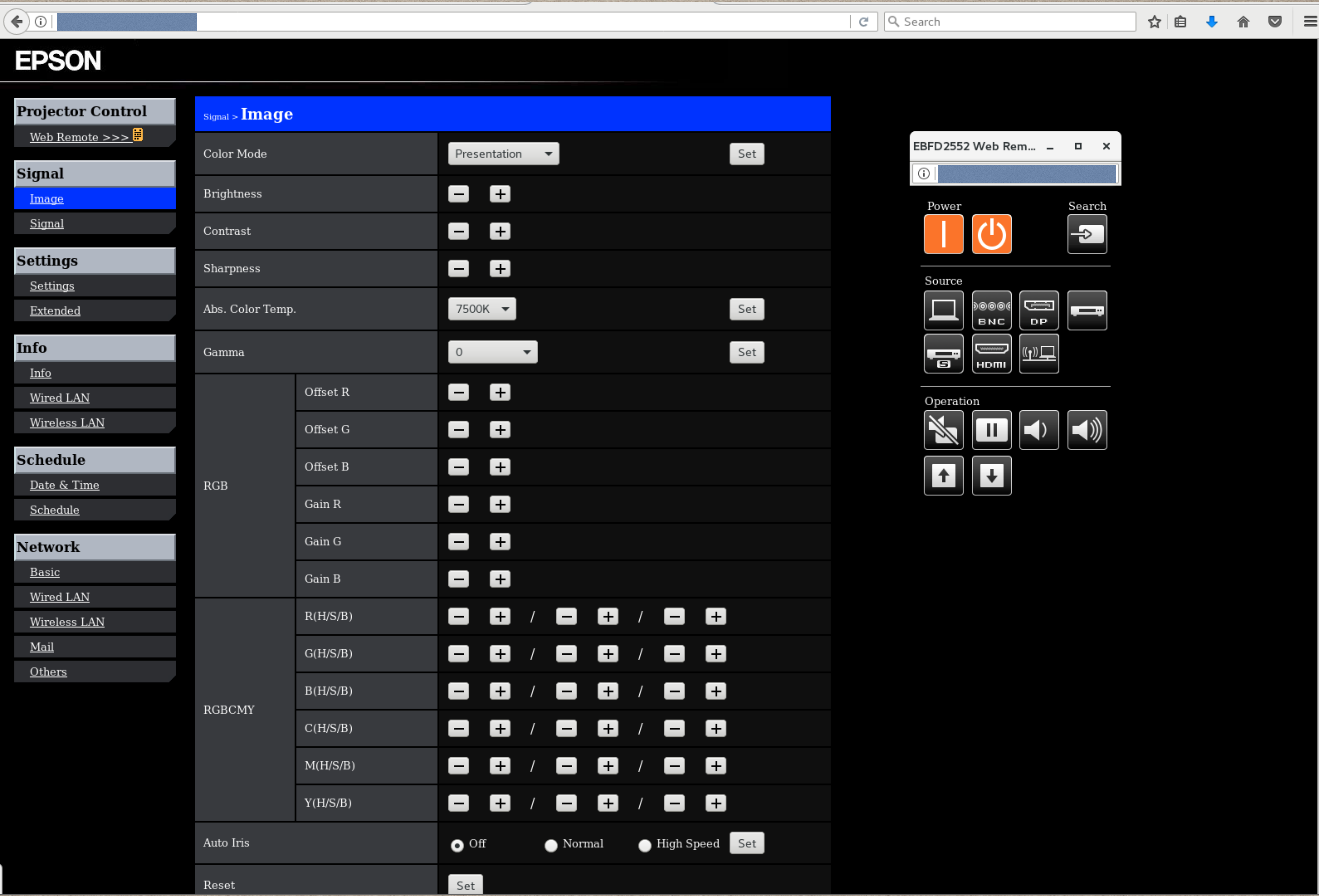
Redirected

Index	Date	Time	Local ID	Name	Number

Note

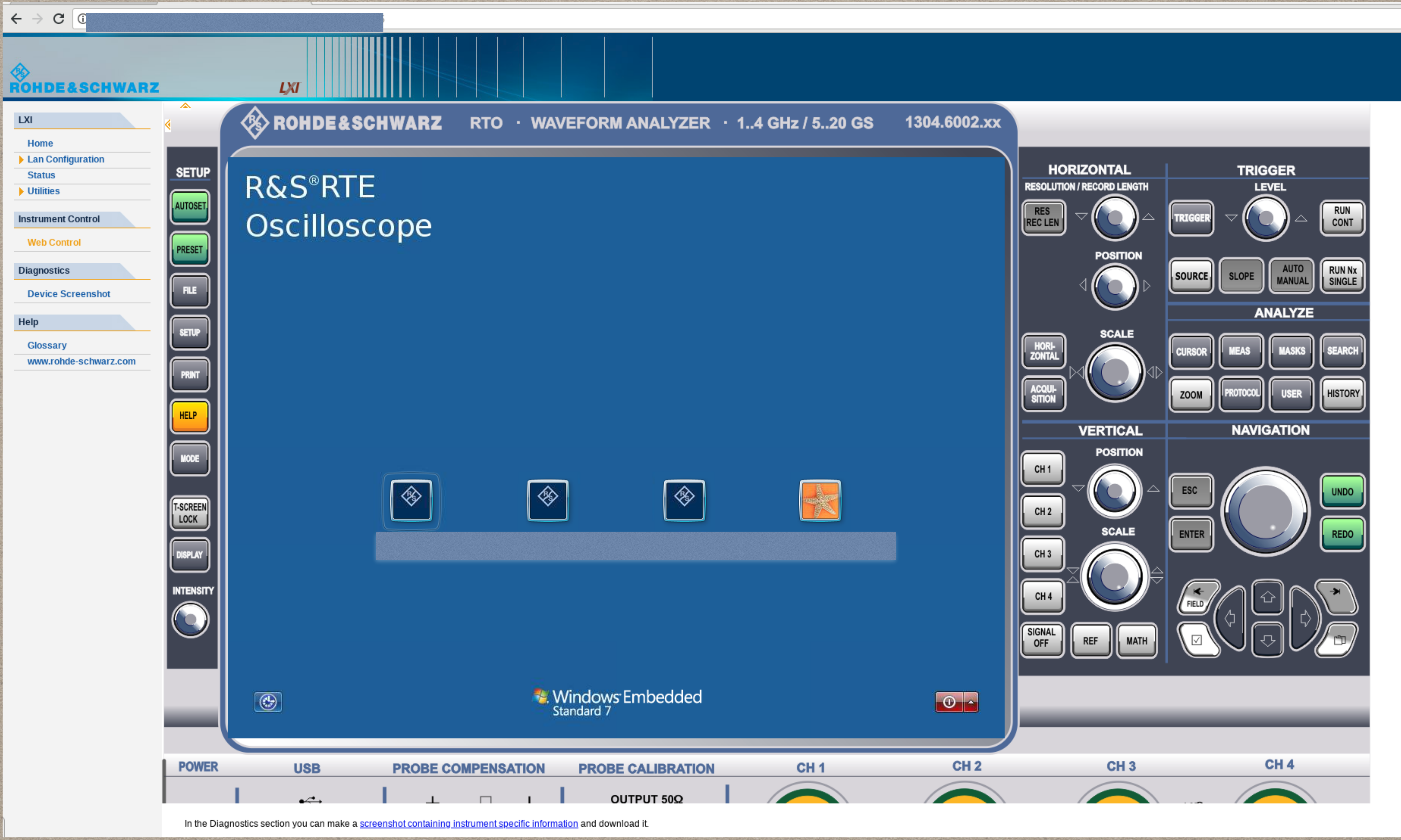
History
Manage call history.

Projector



Signal > Image

Color Mode	Presentation	Set
Brightness	− +	
Contrast	− +	
Sharpness	− +	
Abs. Color Temp.	7500K	Set
Gamma	0	Set
RGB	Offset R	− +
	Offset G	− +
	Offset B	− +
	Gain R	− +
	Gain G	− +
	Gain B	− +
RGBCMY	R(H/S/B)	− + / − + / − +
	G(H/S/B)	− + / − + / − +
	B(H/S/B)	− + / − + / − +
	C(H/S/B)	− + / − + / − +
	M(H/S/B)	− + / − + / − +
	Y(H/S/B)	− + / − + / − +
Auto Iris	● Off ○ Normal ○ High Speed	Set
Reset	Set	

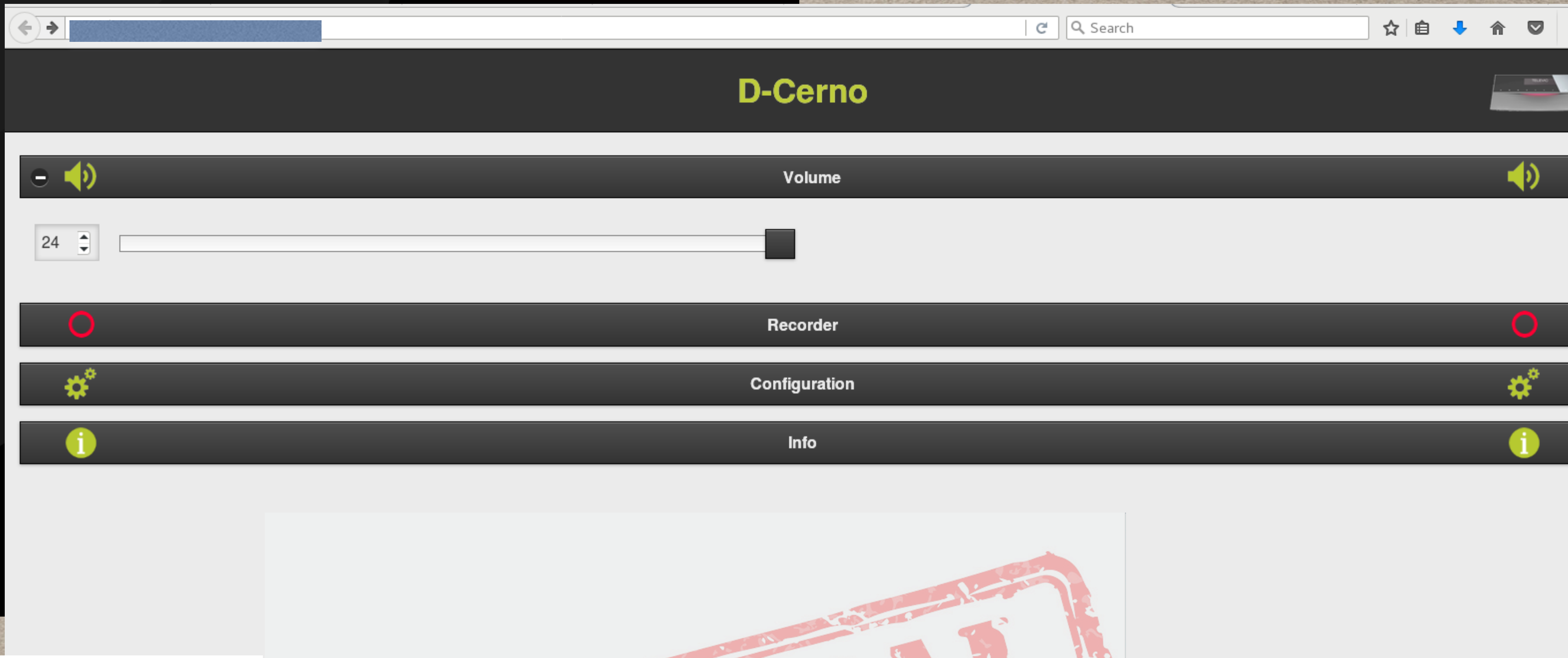


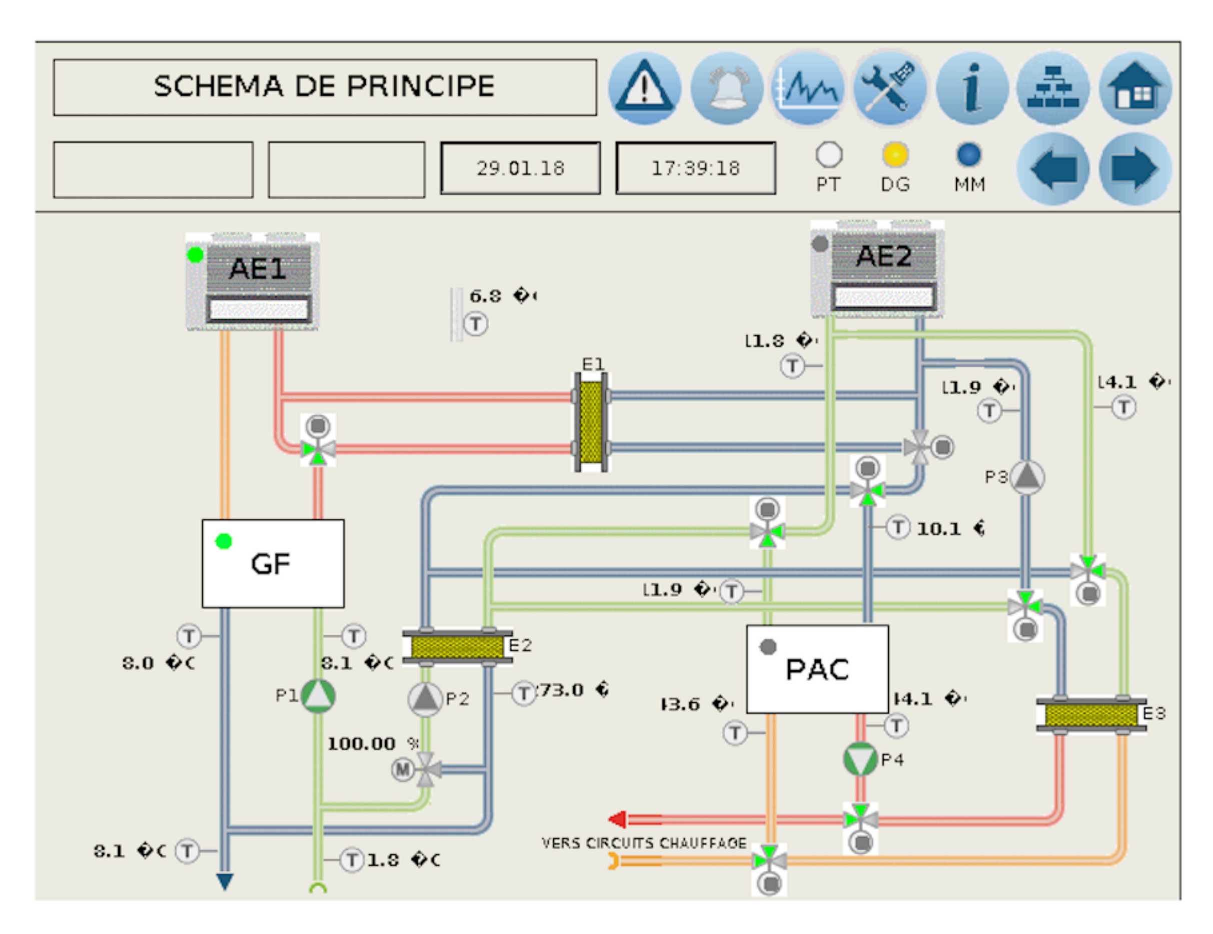
[redacted]

In the Diagnostics section you can make a screenshot containing instrument specific information and download it.

[redacted]

[redacted]


[redacted]



ORIGINAL

[redacted]

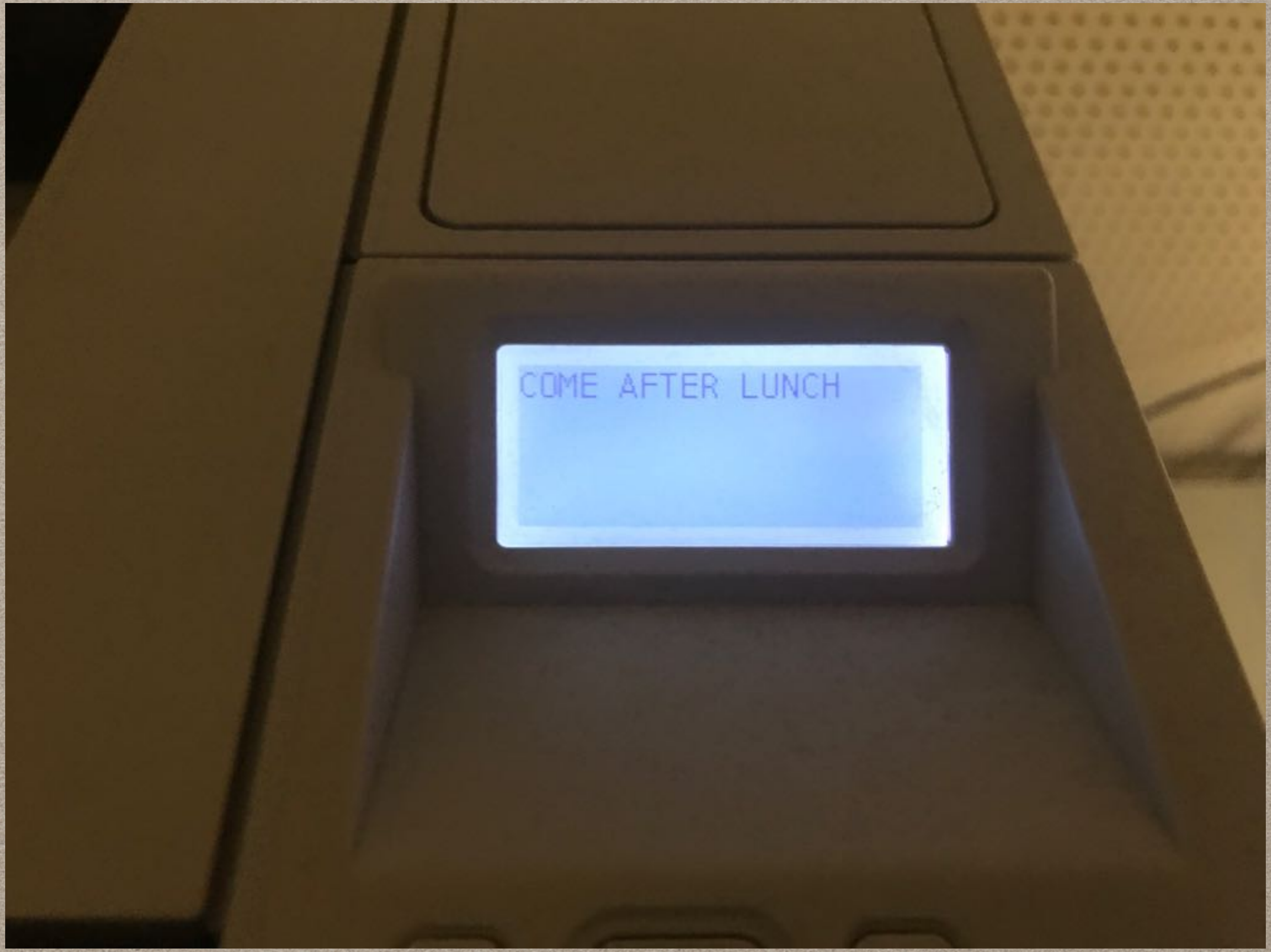
AND MANY MORE

Medium Vulnerable Devices

[redacted]

Number plate readers

Printers



COME AFTER LUNCH

Yes there are no proper standards for IoT security yet

There are only drafts that come out every year
but no proper standards that are finally announced or
security check measures for the companies

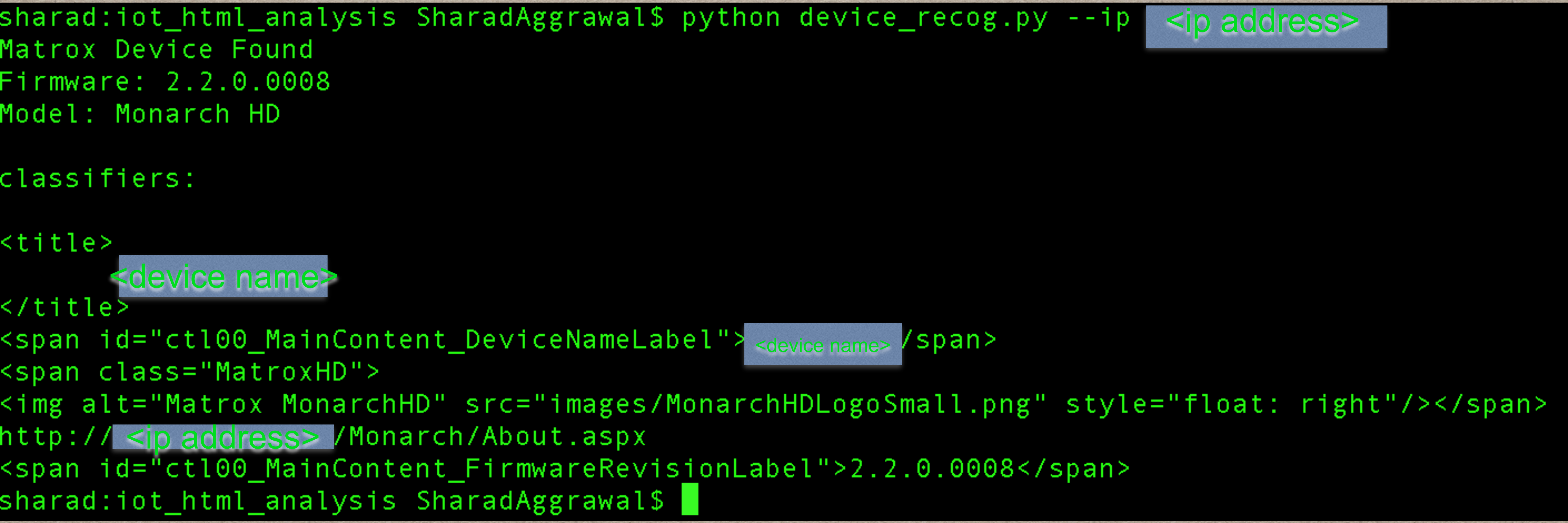
So what else are we doing ?

We are developing an automatic tool that detects IoT devices and provides model and firmware details about them

So how we do this -

1. *Scan the GPN at CERN to detect IoT Devices.*
2. *We tried a lot of tools like scrapy, python requests package, wget, etc but the best outcome was - Selenium with chrome driver.*
3. *Analysing webpages manually.*
4. *Detected different firmwares just using the webpage analysis.*
5. *Constructed tool to automate the output of IoT device detection using beautifulsoup.*

Example for a random CERN IoT device IP



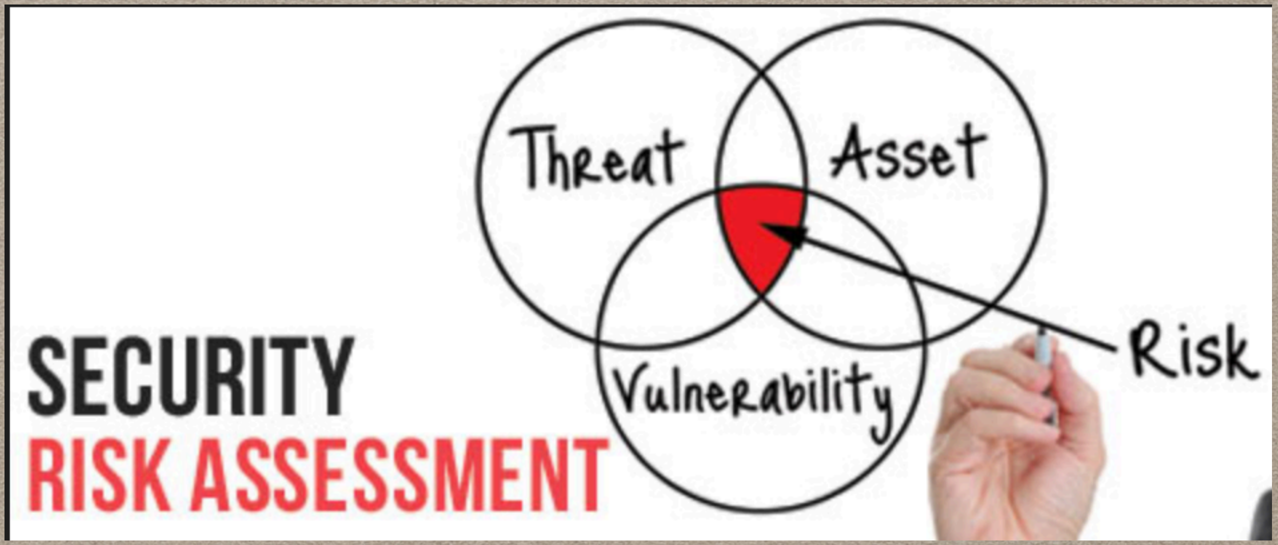
```
sharad:iot_html_analysis SharadAggrawal$ python device_recog.py --ip <ip address>
Matrox Device Found
Firmware: 2.2.0.0008
Model: Monarch HD

classifiers:

<title>
       <device name>
</title>
<span id="ctl00_MainContent_DeviceNameLabel"><device name>/span>
<span class="MatroxHD">
<img alt="Matrox MonarchHD" src="images/MonarchHDLogoSmall.png" style="float: right"/></span>
http://<ip address>/Monarch/About.aspx
<span id="ctl00_MainContent_FirmwareRevisionLabel">2.2.0.0008</span>
sharad:iot_html_analysis SharadAggrawal$
```

What we plan to do with this info -

We will be using this information to show security risks associated with them.



REFERENCES

- http://techomebuilder.com/emagazine-articles-1/security-professionals-find-vulnerabilities-in-most-iot-devices