

Installation & Konfiguration

Installation mit Docker und wichtige Konfigurationen nach der Installation.

- [Installation](#)
- [Arp-Scan](#)
- [Login aktivieren](#)
- [Automatische Up/Down Meldung deaktivieren](#)

Installation

Mit Docker ist Pi.Alert schnell und einfach ausgerollt. Dazu einfach die folgende Compose Config anpassen.

```
services:
  pialert:
    image: jokobsk/pi.alert
    container_name: pialert
    volumes:
      - /pfad/zur/pialert/config:/home/pi/pialert/config
      - /pfad/zur/pialert/db:/home/pi/pialert/db
    environment:
      - TZ=Europe/Berlin
      - HOST_USER_ID=1000
      - HOST_USER_GID=1000
      - PORT=20211
    network_mode: 'host'
    restart: 'unless-stopped'
```

Service Name und Container Name können angepasst werden. Wichtig ist, dass die Volumes angepasst werden, je nachdem in welchem Pfad die Config und DB gespeichert werden sollen.

In der Config werden mit HOST_USER_ID und HOST_USER_GID die ID und Gruppe angepasst, unter der die Dienste in dem Container ausgeführt werden. Deswegen müssen die Berechtigungen/Eigentümer der beiden Ordner, in denen die Config und DB liegen, angepasst werden. Hierzu die beiden folgenden (an die eigenen Pfade angepassten) Befehle ausführen:

```
sudo mkdir /pfad/zur/pialert/config
sudo chown -r 1000 /pfad/zur/pialert/config
sudo mkdir /pfad/zur/pialert/db
sudo chown -r 1000 /pfad/zur/pialert/db
```

Um die Docker Compose Konfiguration auszuführen, kann am besten in das Verzeichnis der YAML Datei gewechselt werden. Danach wird je nach gewählter Installation `sudo docker-compose up` oder `sudo docker compose up -d` (keine Bindestrich zwischen docker und compose) eingegeben, um die Standard Konfiguration `docker-compose.yml` zu starten. Compose erstellt dann die gewünschten Container mit den angegebenen Optionen. Sollten die Container bereits mit dieser Compose Konfiguration erstellt worden sein, so werden die Container in dieser neu erstellt, dessen

Konfiguration geändert wurde.

Nach wenigen Sekunden ist die Weboberfläche unter *http://Server-IP:20211* erreichbar.

Arp-Scan

Nach der Installation sind noch Konfigurationen notwendig, damit gescannt wird. Standardmäßig sind zwar ein paar Scans aktiv, aber gerade der ARP-Scan ist beim Docker Container falsch eingestellt. Außerdem ist die Seite nicht mit einem Login geschützt, sodass jeder im Netzwerk auf diese zugreifen kann. Nach dem 1. Start sieht die Seite wie folgt aus.

Pi.Alert

Devices

Presence

Events

Report

Network

Plugins

Maintenance

Settings

Workflows

System info

Help / FAQ

Donations

Devices

1My Devices

1Connected

0Favorites

0New Devices

0Down Alerts

0Archived

Device presence

My Devices

Showing 1 to 1 of 1 entries

Internet

House

Router

Always on

2021-01-01 00:00:00

2021-01-01 00:00:00

0.0.0.0

Online

Internet

1

0

Orange / Vodafone / Movistar ...

0

Showing 1 to 1 of 1 entries

Previous1Next

Am besten noch ein paar Minuten abwarten, da standardmäßig die ersten Scans laufen. Nach wenigen Minuten sollten dann 2 Geräte in der Liste auftauchen, das Gerät, auf dem Pi.Alert läuft und ein Gerät mit dem Namen *Internet*, der die aktuelle externe IP darstellt. die Ansicht sieht dann in etwa wie folgt aus.

Pi.Alert

Devices

Presence

Events

Report

Network

Plugins

Maintenance

Settings

Workflows

System info

Help / FAQ

Donations

Devices

2My Devices

2Connected

0Favorites

1New Devices

0Down Alerts

0Archived

Device presence

My Devices

Showing 1 to 2 of 2 entries

(name not found)

House

2024-02-23 15:35:54+01:00

2024-02-23 15:35:54+01:00

192.168.178.28

New

70:85:c2:c4:9b:5f

-1062686180

2

X

0

Internet

House

Router

Always on

2021-01-01 00:00:00

2021-01-01 00:00:00

91.97.214.17

Online

Internet

1533138449

1

0

Orange / Vodafone / Movistar ...

0

Showing 1 to 2 of 2 entries

Previous1Next

Arp-Scan

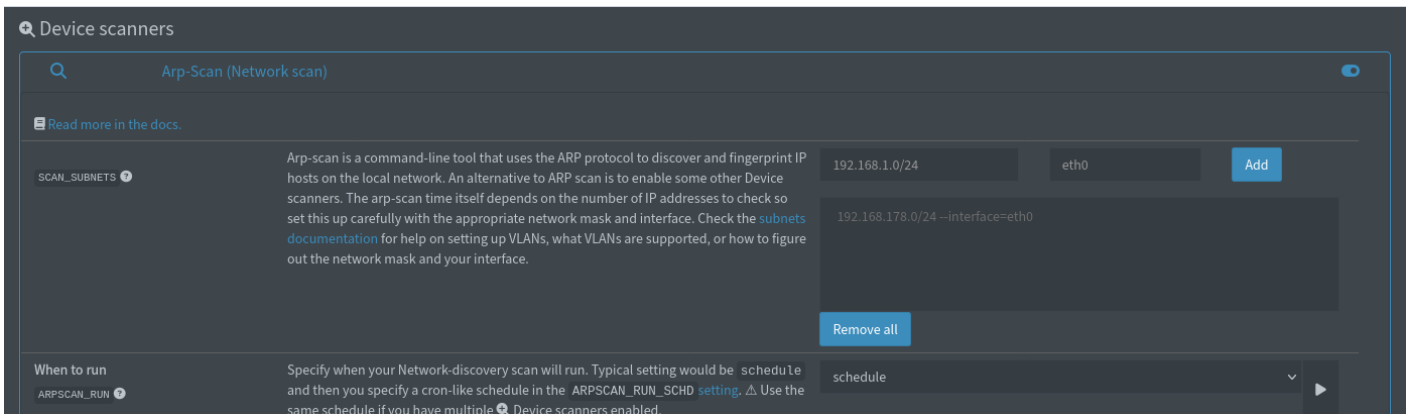
Wie zu sehen ist, werden die Geräte aus dem lokalen Netzwerk nicht angezeigt. Somit wird zuerst der ARP-Scan konfiguriert. Dazu in die *Settings* wechseln. Ganz oben auf der Seite der Einstellungen werden die aktivierten Scans angezeigt.

Leider sind diese aufgrund des Standard Designs schlecht lesbar, dieses lässt sich in den im Menü *Maintenance* anpassen. Daher wird für die nachfolgenden Screenshots das Design in den Dark Mode gewechselt: Maintenance -> Toggle Modes (Dark/Light)

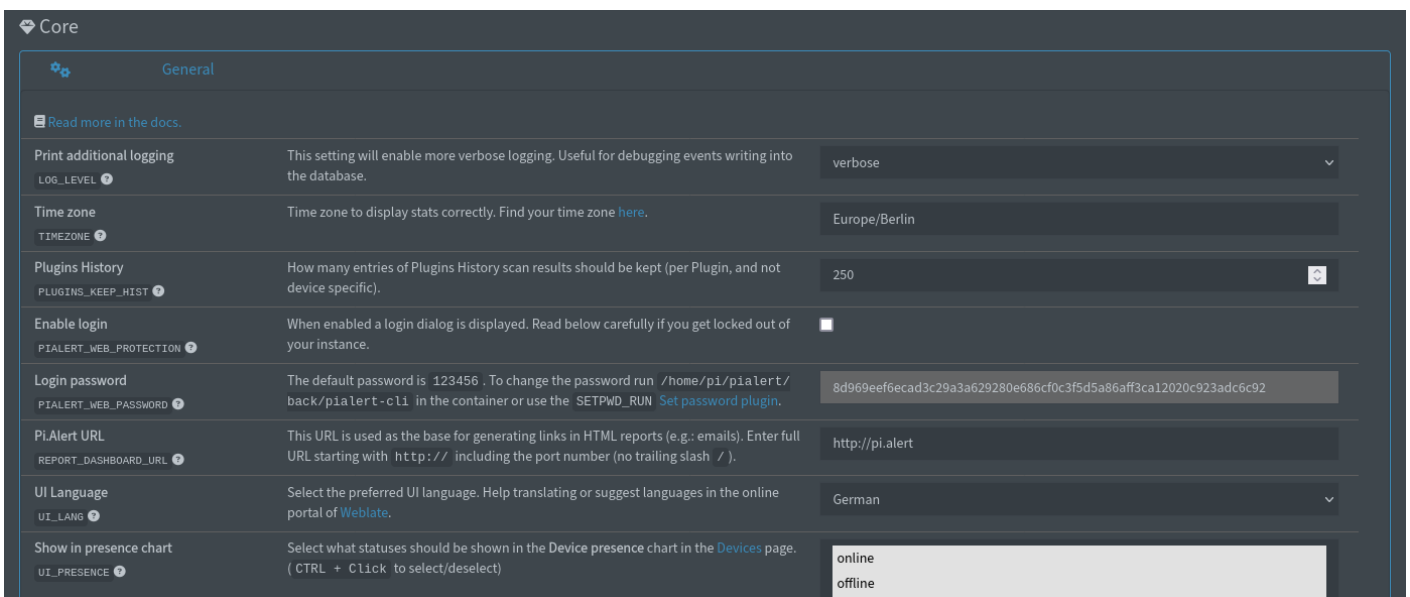
Dort ist bereits der Arp-Scan gelistet. Wenn dieser angeklickt wird, springt der Browser direkt an die passende Stelle in der Konfiguration. Dort ist dann das Problem zu sehen, es wird standardmäßig nur das Netzwerk `192.168.1.0/24` gescannt. Die meisten Heimnetzwerke verwenden häufig `192.168.178.0/24` (Standard FritzBox). Am besten einmal das eigene Netzwerk prüfen z. B. indem die Netzwerk Konfiguration auf dem eigenen Rechner geprüft wird, sofern nicht bereits bekannt. Dann mit *Remove all* das bisherige Netzwerk entfernen. Danach in das Feld darüber die eigene Netzwerk-ID eingeben (in der Regel `192.168.178.0/24` oder `192.168.0.0/24`) und den Namen des Netzwerk Adapters eintragen, über den gescannt werden soll. Dieser ist in der Regel `eth0`.

Der Name des Netzwerk-Adapters lässt sich über die *System info* einsehen. Dort dann nach *Network Hardware* suchen. Neben dem Adapter wird auch die IP von diesem angezeigt, sodass auch direkt die IP ermittelt werden kann, aus der sich dann die Netzwerk-ID ergibt (in der Regel können einfach die Zahlen nach dem letzten Punkt durch eine 0 ersetzt werden, somit wird aus `192.168.178.180/24` -> `192.168.178.0/24`, die `/24` bleibt selbstverständlich

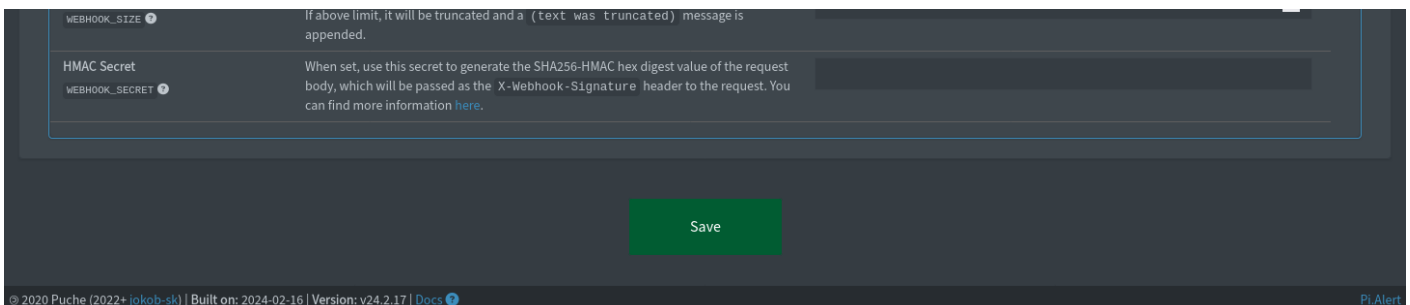
erhalten.



Nachdem die Einstellungen geändert wurden, könnte noch die Sprache angepasst werden, dazu nochmal nach ganz oben scrollen und unter *UI language* die Sprache ändern.



Um die vorgenommen Einstellungen zu speichern nun ans Ende der Seite scrollen und auf **Save** klicken.



Zum Schluss lädt Pi.Alert einmal neu und einige Minuten später sollten die ersten Scan Ergebnisse vorliegen. Wer nicht so lange warten möchte (alle 5 min wird standardmäßig gescannt), kann den Scan in den Einstellungen manuell anstoßen, dazu nochmal in Einstellungen (Settings) wechseln. Wieder zum Menü für den Arp-Scan wechseln und dort auf den kleinen Play-Button klicken.

Device scanners

Arp-Scan (Network scan)

Read more in the docs.

SCAN_SUBNETS

Arp-scan is a command-line tool that uses the ARP protocol to discover and fingerprint IP hosts on the local network. An alternative to ARP scan is to enable some other Device scanners. The arp-scan time itself depends on the number of IP addresses to check so set this up carefully with the appropriate network mask and interface. Check the [subnets documentation](#) for help on setting up VLANs, what VLANs are supported, or how to figure out the network mask and your interface.

192.168.1.0/24

eth0

Add

192.168.178.0/24 --interface=enps6

Remove all

When to run

ARPSCAN_RUN

Specify when your Network-discovery scan will run. Typical setting would be `schedule` and then you specify a cron-like schedule in the `ARPSCAN_RUN_SCHD` setting. Use the same schedule if you have multiple Device scanners enabled.

schedule

▼▶

Command

ARPSCAN_CMD

Command to run. This should not be changed

`python3 /home/pi/pialert/front/plugins/arp_scan/script.py userSubnets={subnets}`

Run timeout

ARPSCAN_RUN_TIMEOUT

Maximum time in seconds to wait for the script to finish. If this time is exceeded the script is aborted.

300

⬇⬆⬇

Schedule

ARPSCAN_RUN_SCHD

Only enabled if you select `schedule` in the `ARPSCAN_RUN` setting. Make sure you enter the schedule in the correct cron-like format (e.g. validate at [crontab.guru](#)). For example entering `* /3 * * *` will run the scan every 3 minutes. Will be run NEXT time the time passes.
It's recommended to use the same schedule interval for all plugins responsible for discovering new devices.

`* /5 * * *`

Watched

ARPSCAN_WATCH

Send a notification if selected values change. Use `CTRL + Click` to select/deselect.

Watched_Value1

• Watched_Value1 is IP

Wenn der Scan abgeschlossen ist bzw. sobald die ersten Geräte gefunden wurden, könnte es so aussehen. Nun können die Geräte bearbeitet werden, um sie mit Details wie Name, Hersteller, Icon usw. zu versehen.

Pi.Alert

← → ↺ + Process: Wait marcel-pc (23/02/2024, 16:31:35) Pi.Alert

Geräte

11

Alle Geräte

9

Verbunden

0

Favoriten

10

Neue Geräte

0

Down Meldungen

0

Archiviert

Geräte

Anwesenheit

Ereignisse

Bericht

Netzwerk

Plugins

Wartung

Einstellungen

Workflows

Systeminfo

Hilfe / FAQ

Donations

Gerätepräsenz im Laufe der Zeit

Online

Offline/Down

Archived

12

10

8

6

4

2

0

15:35

15:40

15:45

15:50

15:55

16:00

16:05

16:10

16:15

16:20

16:25

16:27

16:28

16:30

Alle Geräte

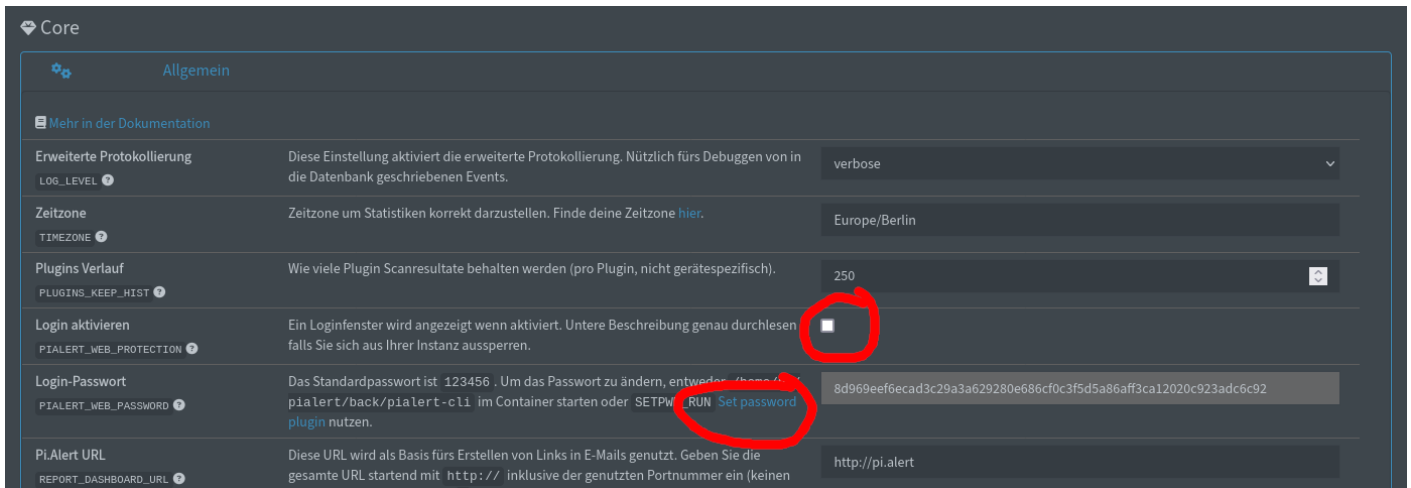
Zeige 50 Einträge

Suche:

Name	Eigentümer	Typ	Icon	Favorit	Gruppe	Erste Sitzung	Letzte Sitzung	Letzte IP	MAC	Status	Gesamte MAC	Last IP Order	Zeilennummer
(name not found)	House					2024-02-23 15:35:54+01:00	2024-02-23 15:35:54+01:00	192.168.178.28		New	70:85:c2:c4:9b:5f	-1062686180	2
(name not found)	House					2024-02-23 16:27:27+01:00	2024-02-23 16:27:27+01:00	192.168.178.20		New	da:31:6c:7d:e1:51	-1062686188	10
(name not found)	House					2024-02-23 16:28:30+01:00	2024-02-23 16:28:30+01:00	192.168.178.38		New	6e:a4:6f:41:f6:11	-1062686170	11
_androidtvremote2	House					2024-02-23 16:27:27+01:00	2024-02-23 16:27:27+01:00	192.168.178.27		New	88:c9:e8:77:9c:76	-1062686181	7
fritz.box (IP match)	House					2024-02-23 16:27:27+01:00	2024-02-23 16:27:27+01:00	192.168.178.1		New	b0:f2:08:21:05:22	-1062686207	3
Internet	House	Router			Always on	2021-01-01 00:00:00	2024-02-23 16:30:44+01:00	91.97.214.17		Online	Internet	1533138449	1

Login aktivieren

Während der Scan läuft ist die perfekte Gelegenheit, um die Seite mit einem Login zu schützen. Dazu wieder in die Einstellungen wechseln. Dort ist dann auch unter *Core* direkt die Checkbox zum Aktivieren des Logins zu sehen. Nachdem setzen des Hakens, auf den Link darunter `Set password plugin` anklicken.



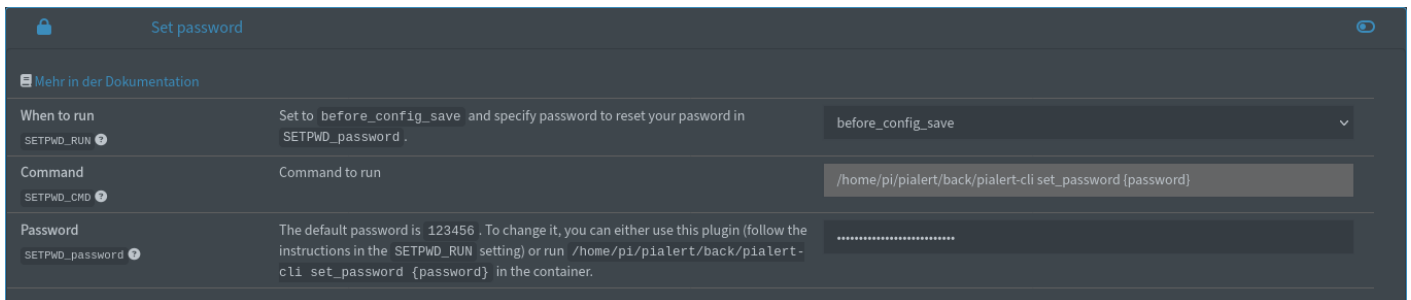
Core

Allgemein

Mehr in der Dokumentation

Erweiterte Protokollierung LOG_LEVEL ⓘ	Diese Einstellung aktiviert die erweiterte Protokollierung. Nützlich fürs Debuggen von in die Datenbank geschriebenen Events.	verbose
Zeitzone TIMEZONE ⓘ	Zeitzone um Statistiken korrekt darzustellen. Finde deine Zeitzone hier .	Europe/Berlin
Plugins Verlauf PLUGINS_KEEP_HIST ⓘ	Wie viele Plugin Scanresultate behalten werden (pro Plugin, nicht gerätespezifisch).	250
Login aktivieren PIALERT_WEB_PROTECTION ⓘ	Ein Loginfenster wird angezeigt wenn aktiviert. Untere Beschreibung genau durchlesen falls Sie sich aus Ihrer Instanz aussperren.	☒
Login-Passwort PIALERT_WEB_PASSWORD ⓘ	Das Standardpasswort ist 123456 . Um das Passwort zu ändern, entweder <code>/home/pi/pialert/back/pialert-cli</code> im Container starten oder <code>SETPWD_RUN</code> Set password plugin nutzen.	8d969eef6ecad3c29a3a629280e686cf0c3f5d5a86aff3ca12020c923adc6c92
PI.Alert URL REPORT_DASHBOARD_URL ⓘ	Diese URL wird als Basis fürs Erstellen von Links in E-Mails genutzt. Geben Sie die gesamte URL startend mit <code>http://</code> inklusive der genutzten Portnummer ein (keinen <code>https://</code> verwenden).	http://pi.alert

Daraufhin springt der Browser zu dem Bereich *Set password*, indem nun oben erstmal *When to run* auf *before_config_save* gestellt wird und in das Feld neben *Password* wird das gewünschte Passwort eingetragen.



Set password

Mehr in der Dokumentation

When to run SETPWD_RUN ⓘ	Set to <code>before_config_save</code> and specify password to reset your password in <code>SETPWD_password</code> .	before_config_save
Command SETPWD_CMD ⓘ	Command to run	/home/pi/pialert/back/pialert-cli set_password {password}
Password SETPWD_PASSWORD ⓘ	The default password is 123456 . To change it, you can either use this plugin (follow the instructions in the <code>SETPWD_RUN</code> setting) or run <code>/home/pi/pialert/back/pialert-cli set_password {password}</code> in the container.	

Zum Schluss wieder ganz unten auf *Save* klicken.

Automatische Up/Down Meldung deaktivieren

Standardmäßig ist eingestellt, dass für alle neuen Geräte Up/Down Meldungen berichtet werden. Das kann stören, wenn es sich um Geräte handelt, die sich regelmäßig trennen und wieder verbinden, besonders wenn Mail-Benachrichtigungen konfiguriert sind. Es wird jedes Mal eine Mail versendet, wenn Geräte sich trennen und wieder verbinden.

Um dies zu ändern, zuerst in die Einstellungen wechseln. Danach zur Rubrik *System* scrollen und dort nach der Unterrubrik *New Devices* suchen. In dieser werden alle Standard-Einstellungen hinterlegt, welche bei neuen Geräten (nicht bei bereits vorhandenen Geräten) gesetzt werden sollen. Dort gibt es eine Einstellung mit dem Namen *Alert Events*. Wenn bei dieser der Haken entfernt wird, wird für alle neuen Geräte die Up/Down Meldung deaktiviert. Trotzdem kann sie bei Bedarf in den Einstellungen der Geräte je Gerät geändert werden, sodass für gewünschte Geräte eine Meldung verschickt wird. Unabhängig von der Meldung werden die Ereignisse weiterhin aktualisiert, um den Online Status von Geräten im Log nachschauen zu können. Im folgenden Foto ist der anzupassen Menüeintrag hervorgehoben.

DB cleanup

Notification Processing

New Devices

Mehr in der Dokumentation

Ignored MACs NEMDEV_ignored_MACs ⓘ	List of MACs to ignore. Use % as a wildcard. Ignored devices will not be shown anywhere in the UI or notifications. For example 02:42:ac:1% to filter out docker containers.	Enter value Add Remove last
Ignored IPs NEMDEV_ignored_IPs ⓘ	List of IPs to ignore. Use % as a wildcard. Ignored devices will not be shown anywhere in the UI or notifications. For example 192.168.3.% to filter out a subnet.	Enter value Add Remove last
Device MAC NEMDEV_dev_MAC ⓘ	The MAC address of the device. Uneditable - Autodetected.	
Device Name NEMDEV_dev_Name ⓘ	The name of the device. Uneditable as internal functionality is dependent on specific new device names.	(unknown)
Device Owner NEMDEV_dev_Owner ⓘ	The owner of the device.	House
Device Type NEMDEV_dev_DeviceType ⓘ	The type of the device.	
Device Vendor NEMDEV_dev_Vendor ⓘ	The vendor of the device. Uneditable - Autodetected.	
Favorite Device NEMDEV_dev_Favorite ⓘ	Indicates whether the device is marked as a favorite.	☐
Device Group NEMDEV_dev_Group ⓘ	The group to which the device belongs.	
Device Comments NEMDEV_dev_Comments ⓘ	Additional comments or notes about the device.	
First Connection NEMDEV_dev_FirstConnection ⓘ	The date and time of the first connection with the device. Uneditable - Autodetected.	
Last Connection NEMDEV_dev_LastConnection ⓘ	The date and time of the last connection with the device. Uneditable - Autodetected.	
Last IP NEMDEV_dev_LastIP ⓘ	The last known IP address of the device. Uneditable - Autodetected.	
Static IP NEMDEV_dev_StaticIP ⓘ	Indicates whether the device has a static IP address.	☐
Scan Cycle NEMDEV_dev_ScanCycle ⓘ	The default value of the Scan device dropdown. Enable if newly discovered devices should be scanned.	✓
Log Events NEMDEV_dev_LogEvents ⓘ	Indicates whether events related to the device should be logged.	✓
Alert Events NEMDEV_dev_AlertEvents ⓘ	Indicates whether events related to the device should trigger alerts. The default value of the Alert All Events checkbox.	✓
Alert Device Down NEMDEV_dev_AlertDeviceDown ⓘ	Indicates whether an alert should be triggered when the device goes down. The default value of the Alert Down checkbox.	☐
Skip Repeated NEMDEV_dev_SkipRepeated ⓘ	The default value of the Skip repeated notifications for dropdown. Enter number of hours for which repeated notifications should be ignored for. If you enter 0 then you get notified on all events.	0
Last Notification NEMDEV_dev_LastNotification ⓘ	The date and time of the last notification sent for the device. Uneditable - Autodetected.	