

Guide - UniFi Gateway



**Til opsætning af UniFi Gateway
(Router) og Wireless Access Points til
Trådløse netværk.**

Kasper Henneberg Madsen /

Kim Donnerborg

RTS – Data og kommunikation GF2 og
Elektriker HF

30-06-2026

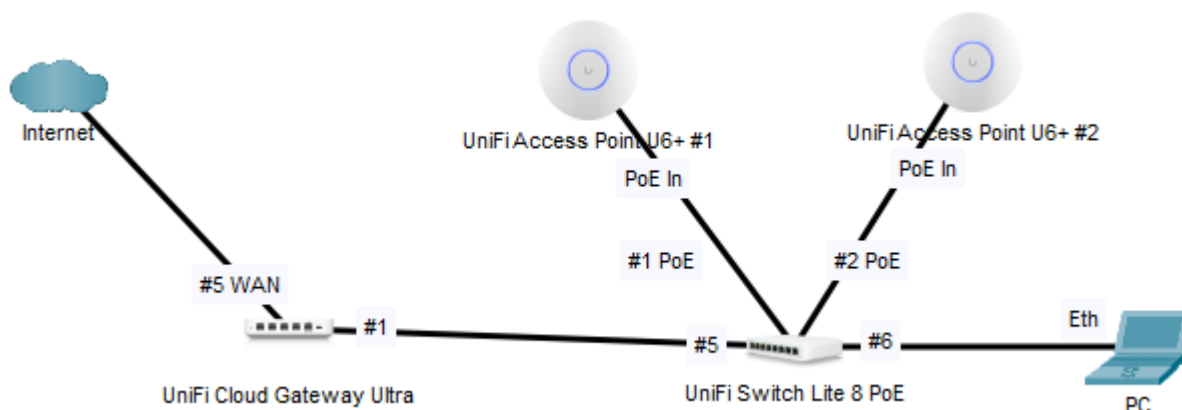
Indholdsfortegnelse

TILSLUT ENHEDER EFTER TEGNING	2
NULSTILLING AF CLOUD GATEWAY	2
<i>Kontroller PC har fået IP-adresse fra Gateway</i>	<i>2</i>
START OPSÆTNING AF UNIFI GATEWAY FRA PC	3
KONFIGURER NETVÆRK (VALGFRI).....	7
OPRET DHCP RESERVATIONER (VALGFRI)	8
KONFIGURER ENHEDER.....	8
KONFIGURER TRÅDLØSE NETVÆRK	10
OPRET ISOLERET NETVÆRK PÅ ANDET VLAN (VALGFRI).....	13
BLOKER ADGANG TIL ISOLERET NETVÆRK (VALGFRI)	14
OPRET WIFI TIL ISOLERET NETVÆRK	15
PORT FORWARDING	16
SIKKERHED	17
OPRET VPN-ADGANG TIL DIT NETVÆRK	19
OPDATERINGER	19
BACKUP & RESTORE.....	20
SYSTEMINDSTILLINGER	21
LOG OG NOTIFIKATIONER	21

UniFi officiel vejledning: <https://dl.ui.com/qig/ucg-ultra/#index>

Tilslut enheder efter tegning

Tilslut PC du vil bruge til konfiguration af Gateway og 1-2 Access Points til en PoE (Power over Ethernet) Switch eller PoE injektor og tilslut Switch/injektor til en af LAN-porte (1-4) på Gateway.



Nulstilling af Cloud Gateway

Tænd enheden: Sørg for, at din Cloud Gateway er tilsluttet strøm og startet helt op.

Hold Reset inde: Brug en papirclips eller lignende til at trykke **forsigtigt** på Reset-knappen (placeret i det lille hul på bagsiden). Hold den inde i ca. 10 sekunder.

Hold øje med skærmen: Slip knappen, når skærmen på forsiden viser, at nulstillingen er i gang.

Genstart: Enheden genstarter automatisk. Når skærmen viser "Ready for Setup", er den klar til at blive sat op på ny.

Kontroller PC har fået IP-adresse fra Gateway

Åbn Kommandoprompt på PC og indtast "**ipconfig**" og tjek PC har fået IPv4-adresse: 192.168.1.x og Default Gateway: **192.168.1.1**.

Hvis ikke kan du frigive IP på PC ved at indtaste "**ipconfig /release**" og forny IP-adressen herefter med "**ipconfig /renew**"

```
Kommandoprompt
Microsoft Windows [Version 10.0.26200.7840]
(c) Microsoft Corporation. Alle rettigheder forbeholdes.

C:\Users\rts-admin>ipconfig

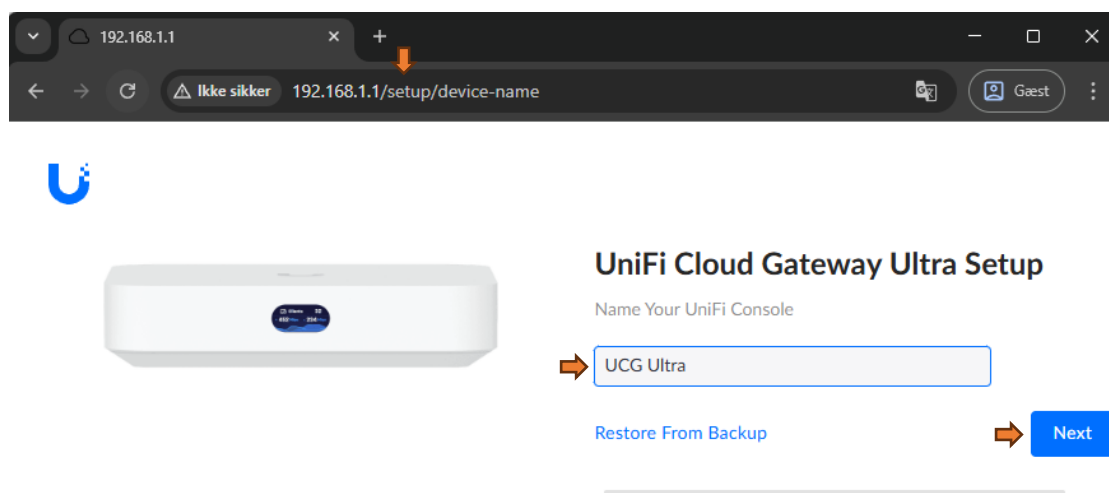
Windows IP Configuration

Ethernet adapter Ethernet:

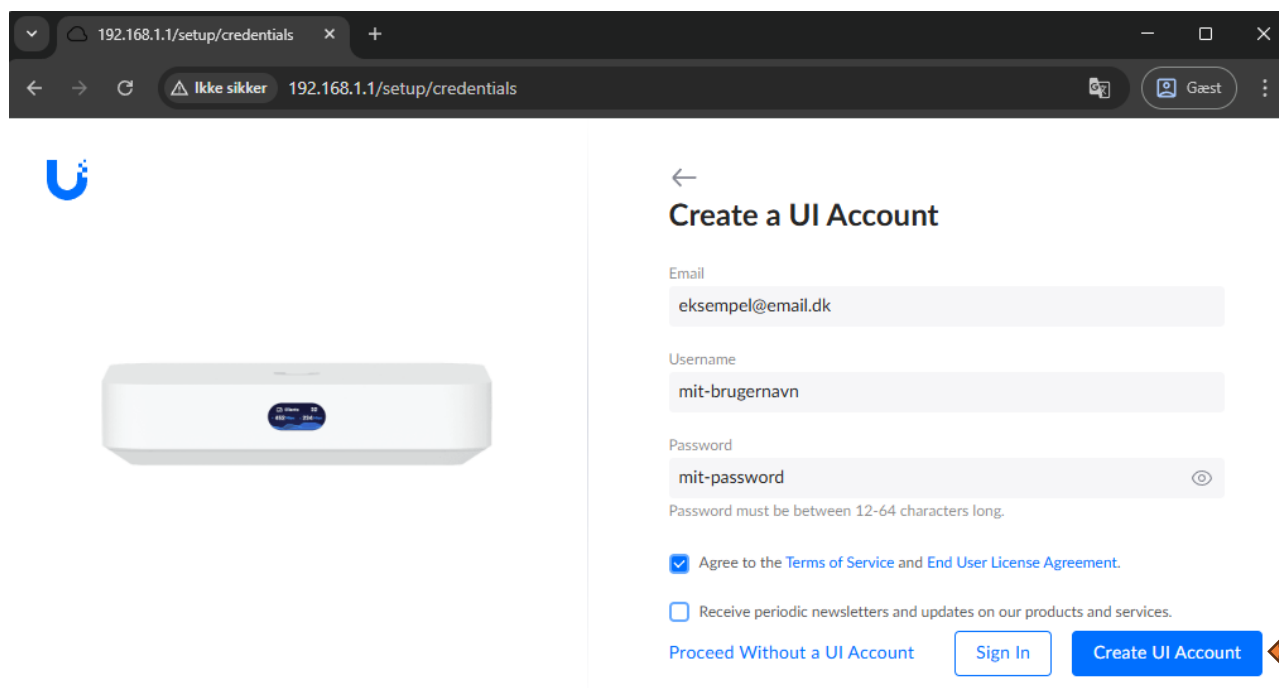
    Connection-specific DNS Suffix  . : localdomain
    Link-local IPv6 Address . . . . . : fe80::b1de:49b5:16d0:4bc0%14
    IPv4 Address. . . . . : 192.168.1.113
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1
```

Start opsætning af UniFi Gateway fra PC

1. Åben Browser på PC for at tilgå Gateway via dens IP-adresse 192.168.1.1 Vælg et beskrivende navn til Gateway og klik "Next"

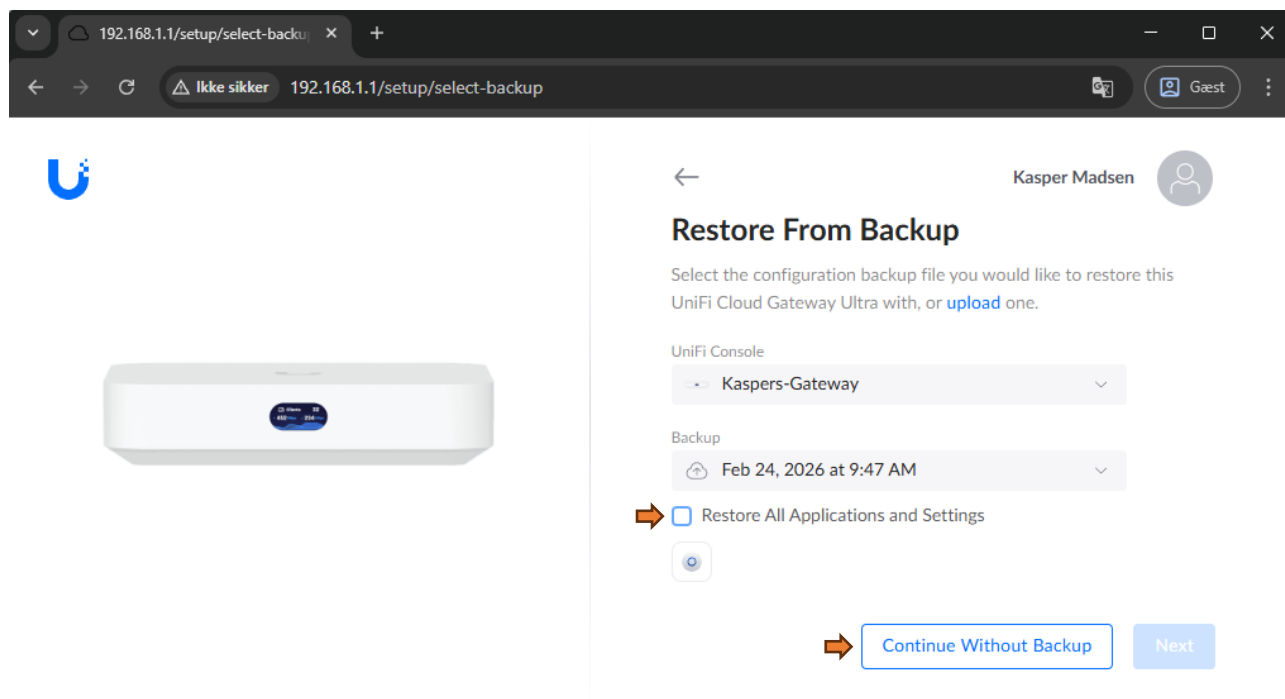


2. Opret gratis Unifi konto eller login hvis du allerede har en. Det er samme konto der bruges til UniFi Design Center.

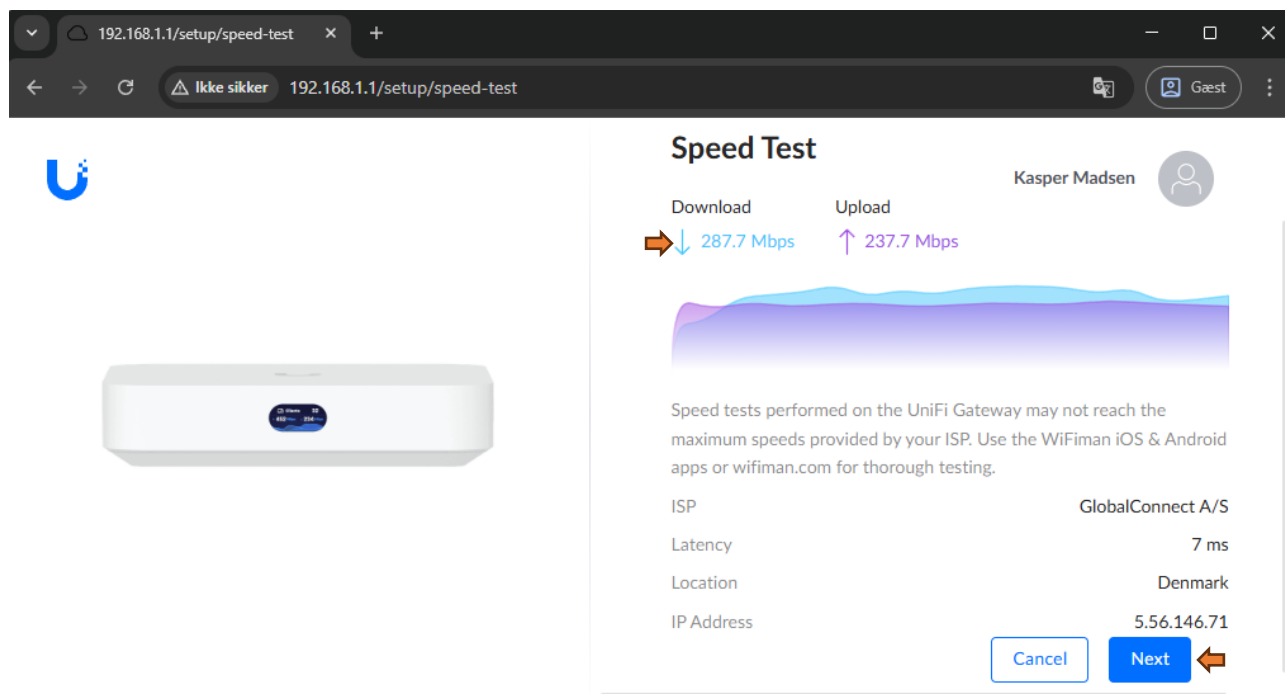


Fortsættes på næste side...

3. Genskab evt. Backup, hvis du tidligere har haft anden Gateway fra UniFi. Her fjerner jeg flueben i **"Restore All Applications and Settings"** og klikker **"Continue Without Backup"**, for at opsætte Gateway fra ny.

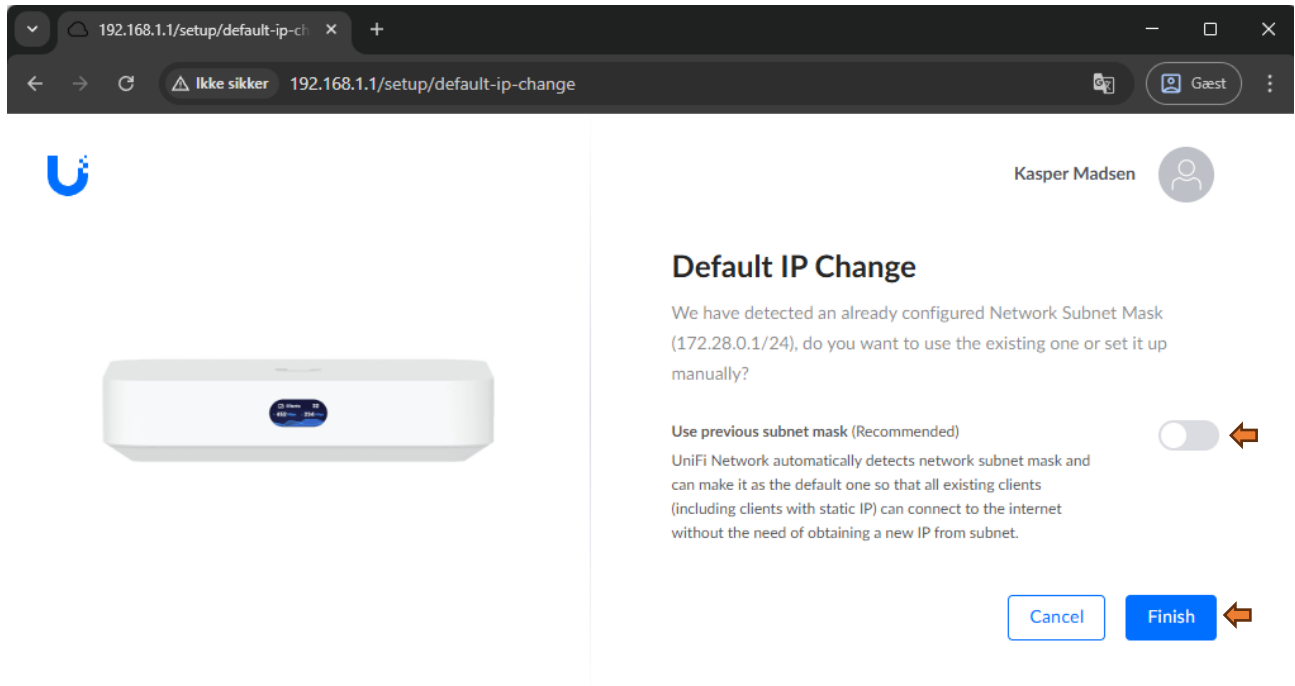


4. Gateway laver herefter speedtest af Internet-forbindelsen. Når den er gennemført, klikker man Next.

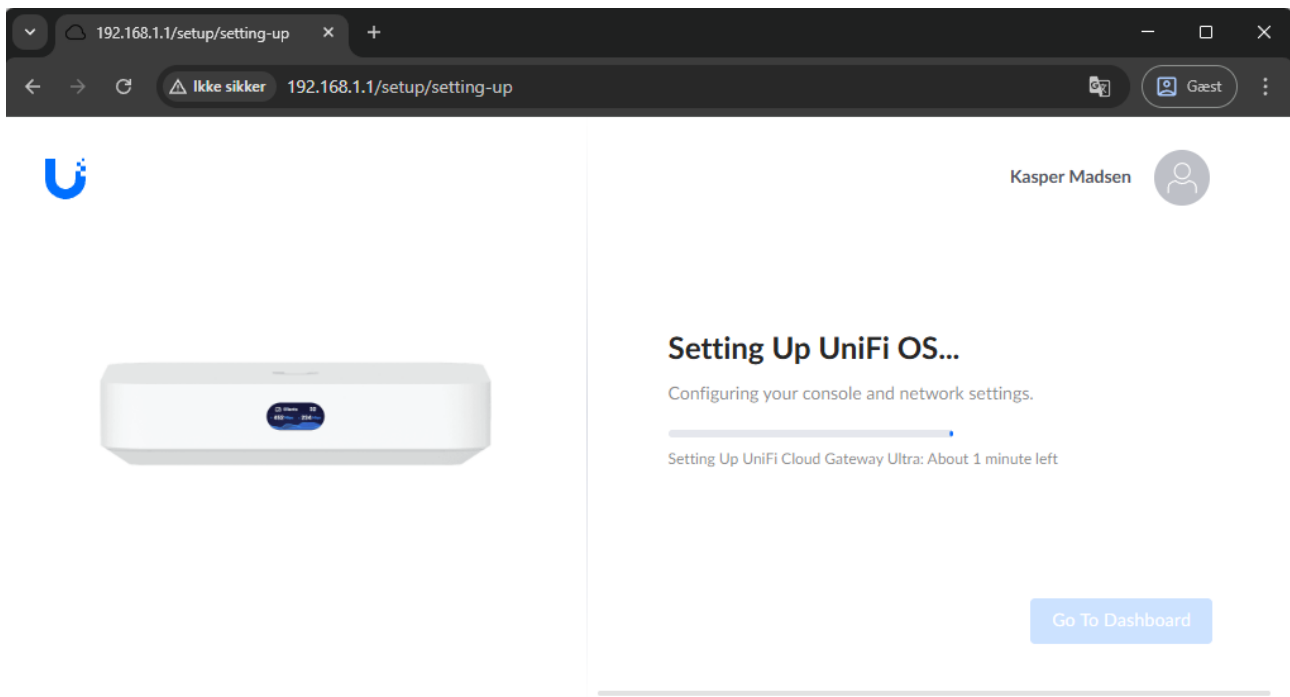


Fortsættes på næste side...

5. Deaktiver forslag **"Use previous subnet mask"**. Vi ønsker ikke at skifte IP-adressen på Subnet lige nu. Klik **"Finish"**.

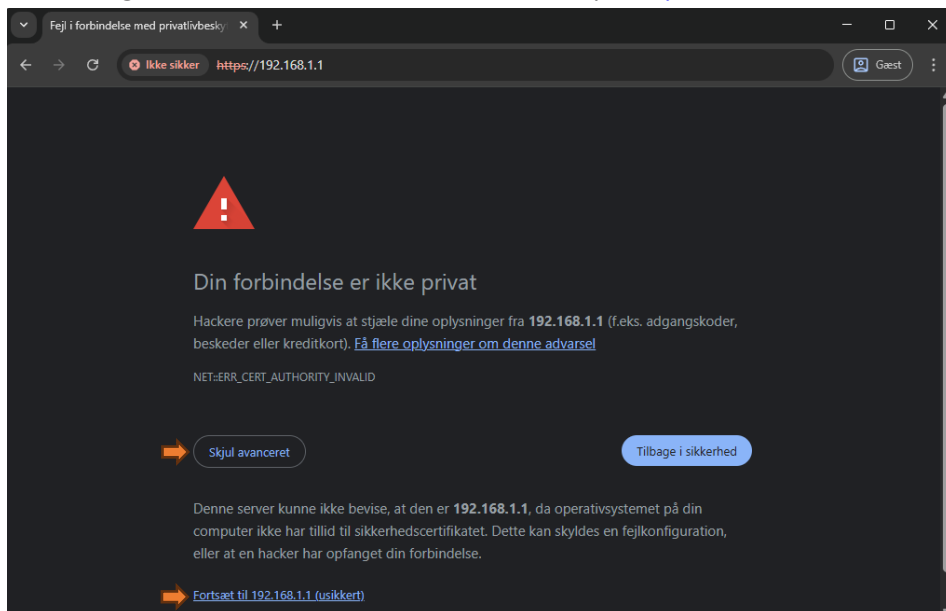


6. Afvent færdiggørelse af opsætning og klik herefter på **"Go To Dashboard"**.

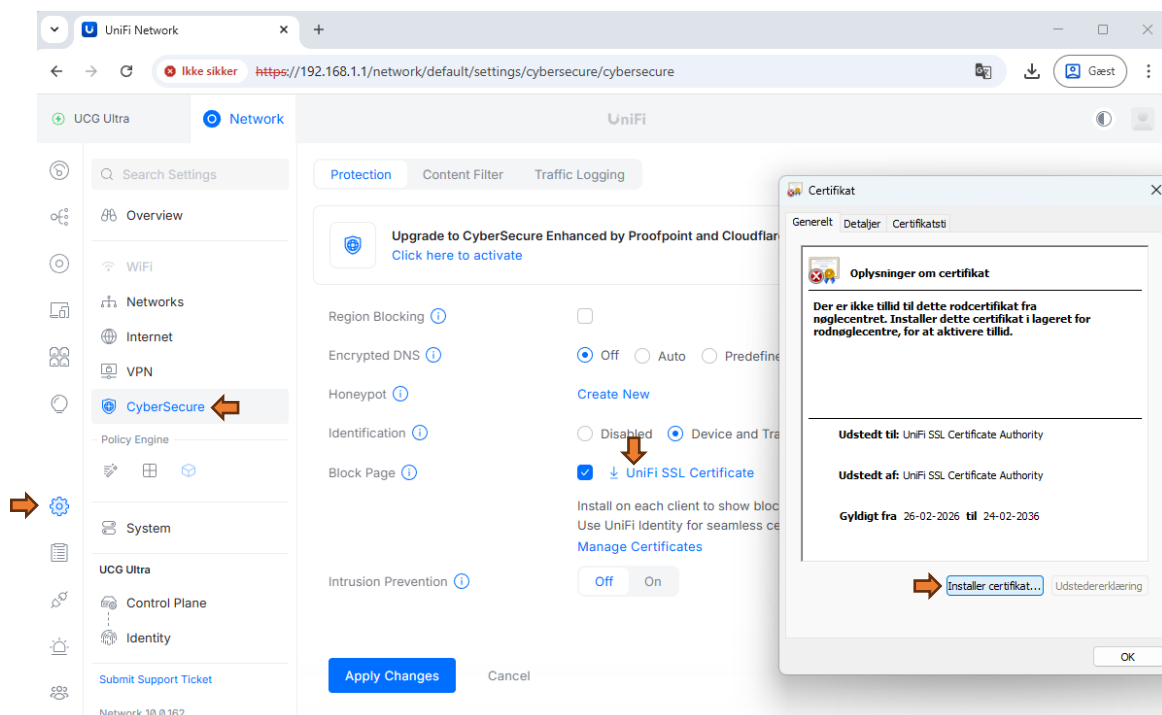


Fortsættes på næste side...

7. Hvis du bliver mødt advarsel som nedenfor, klikker du blot Avanceret nederst til venstre og herefter på **"Fortsæt til 192.168.1.1 (usikkert)"**. Det er blot manglende SSL Certifikat til HTTPS og der er intet usikkert når al kommunikation foregår lokalt. Du kan også administrere netværk via din konto på <https://unifi.ui.com/>



8. Installér evt. SSL Certifikat under **Settings -> CyberSecure -> Block Page** for at undgå browser blokerer siden. Klik på **UniFi SSL Certificate** og kørs **"UniFi-SSL-Certificate.cer"** der downloades.
- Klik **"Installer certifikat"**
 - Vælg **"Aktuel bruger"** og **Næste**.
 - Vælg **"Placer alle certifikater i følgende certifikatlager"** og klik **Gennemse** og vælg **"Rodnøglecentre, der er tillid til"** og klik **OK** og **Næste** og **Udfør**.
 - Klik **Ja** til Sikkerhedsvarsel for at installere certifikat. Genstart Enhed.

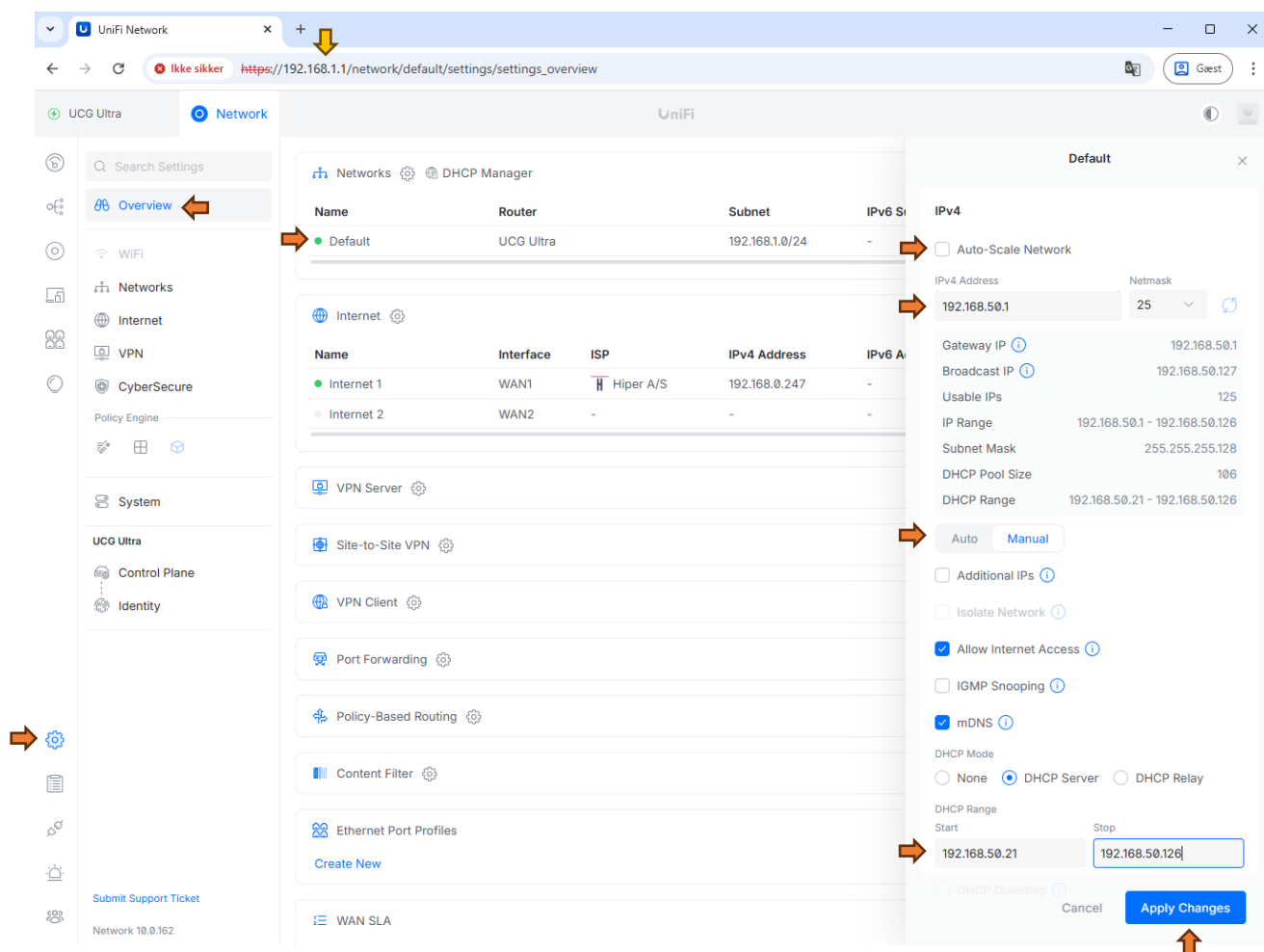


Konfigurer Netværk (valgfri)

Hvis ikke brugerfladen helt matcher det på skærbilleder, kan enhed og Network App være ældre/nyere. Start evt. med at opdatere, se s. 19 hvordan.

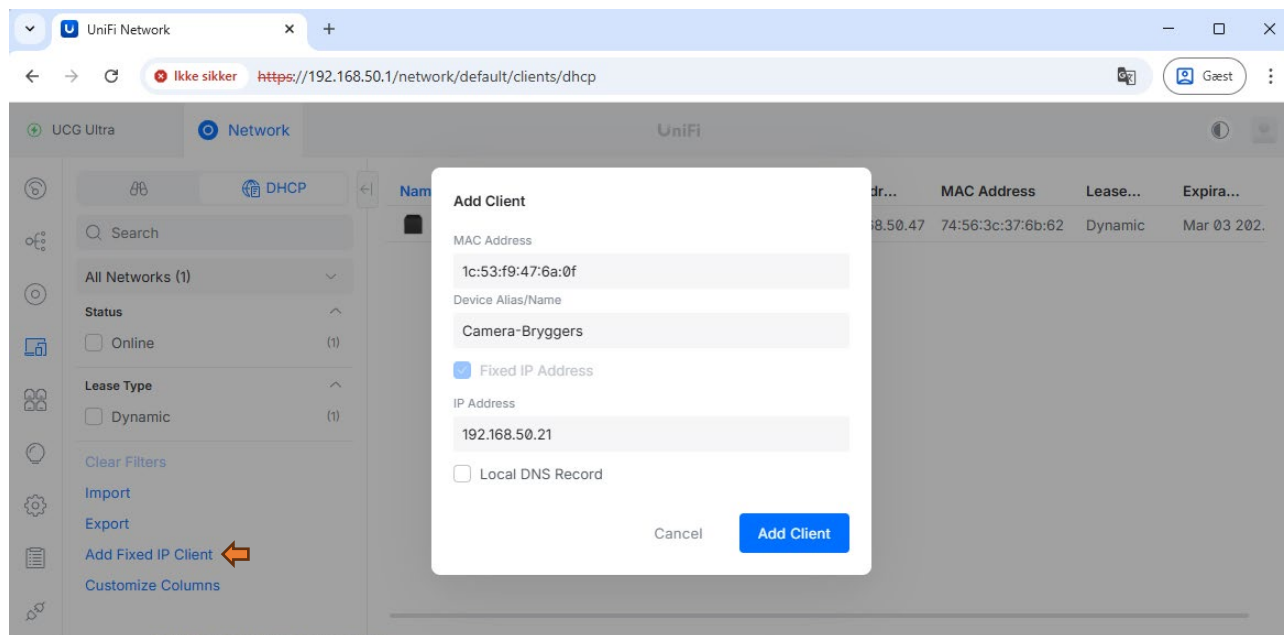
Hvis standard-netværket til LAN ønskes ændret fra **192.168.1.1 /24** gøres følgende:

1. Klik **Settings** -> **Overview**. Klik **"Default"** under **Networks** og dialogboks til højre åbner.
2. Fjern flueben i **"Auto-Scale Network"**. Indtast ønsket **IPv4 Address** til Router (Default Gateway) og vælg **Netmask** (Subnet Mask) efter ønsket størrelse på subnet. **Husk adresse** til trin 5!
3. Ændre fra Auto til **Manual** og indtast **Start** og **Stop** adresse på DHCP Puljen. Jeg starter her på .21 for at have nogle ledige adresser fra .2-20 til statiske enheder.
4. Klik **Apply Changes** for at gemme ændringer.
5. Efter ændring af IP til Router, skal du huske at skrive den nye IP i adresselinjen i Browser.
6. Hvis du stadig ikke kan få forbindelse til Router igen, så har din PC stadig den gamle 192.168.1.x adresse og skal fornyes. Brug **"ipconfig /release"** og **"ipconfig /renew"** i Kommandoprompt som på side 2. Bekræft PC har fået en 192.168.50.x adresse eller fra det subnet du har valgt.



Opret DHCP Reservationer (valgfri)

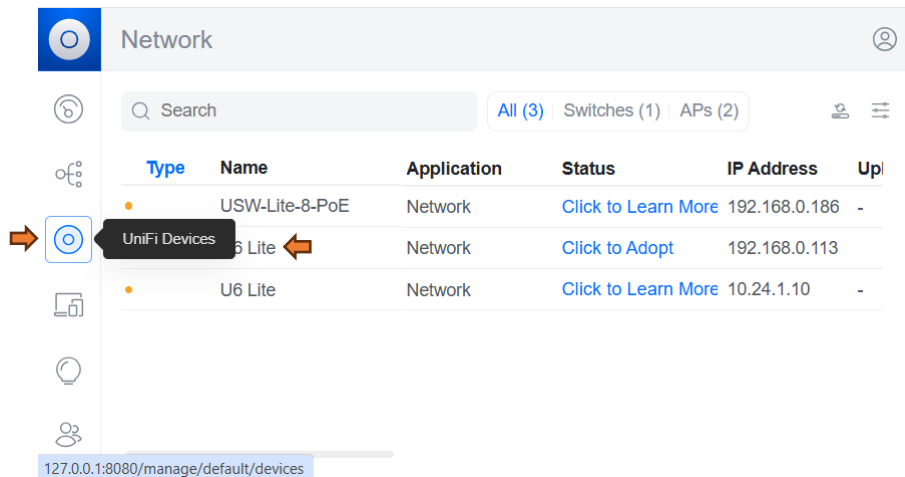
1. Klik på **DHCP Manager** eller **IP Table** ved **Networks** på **Overview** i **Settings**.
2. På oversigt over DHCP kan du se alle Clients og under kolonnen **Lease...** se om IP er **Dynamic** (Automatisk tildelt) eller **Fixed** (Fast adresse reserveret til enhed).
Tryk på **Add Fixed IP Client** for at oprette en DHCP Reservation.



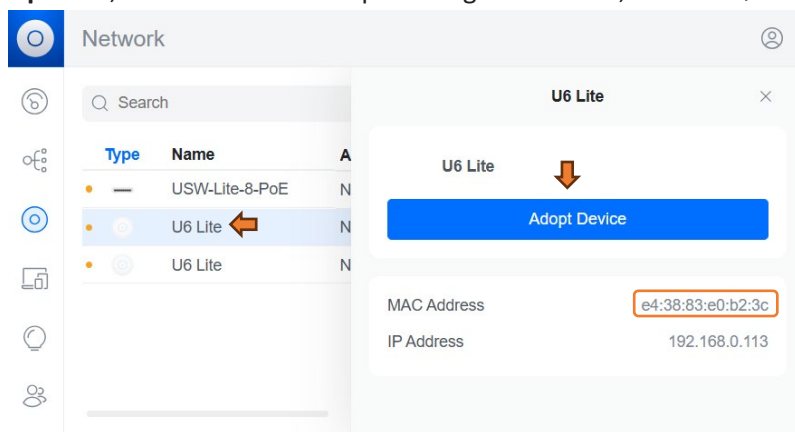
3. Udfyld **MAC Adresse** på enhed, et beskrivende **navn** og den faste **IP** du ønsker til enhed.
Tryk herefter **Add Client** og reservation tilføjes. Hvis ikke enheden er tilsluttet netværk endnu, vil den fremgå som Offline.

Konfigurer enheder

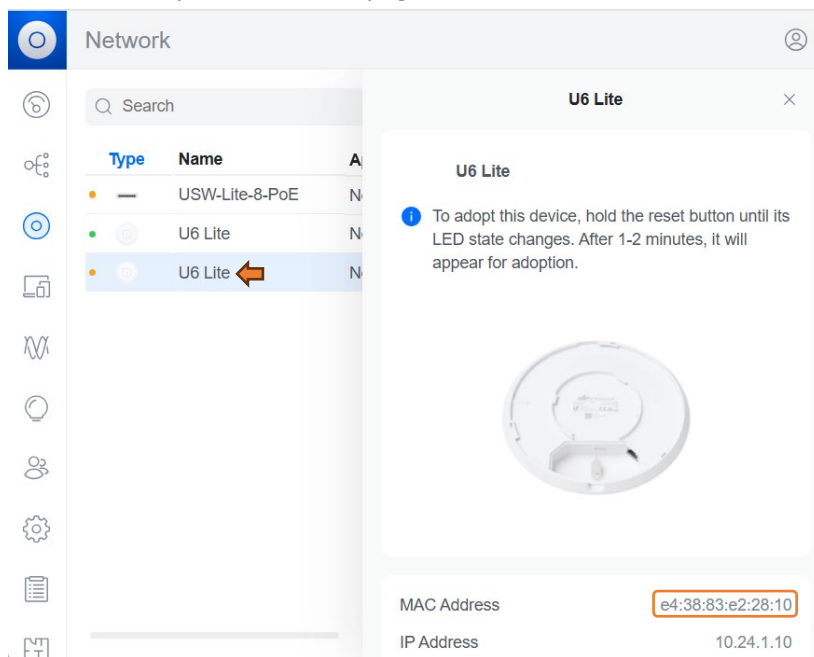
1. Vælg **UniFi Devices** i menuen til venstre og du bør kunne se en oversigt over alle UniFi enheder på samme netværk. Her er der 1x PoE Switch og 2x U6 Lite Access Points. Hvis der står **Click to Adopt** er enheden nulstillet og klar til adoption af Gateway. Hvis der står **Click to Learn More**, skal enheden nulstilles. Hvis ikke enheden fremgår, så tjek [status på LED-lys](#) på enheden.



2. Tjek enhedens MAC-adresse, for at tjekke det er den rigtige enhed, som du adopterer. Hvis der er Access Points i nærheden, vil de også kunne ses trådløst. Klik på en enhed og sammenlign MAC-adressen med den i strekkoden på bagsiden af din enhed. Klik så **"Adopt Device"**. Det tager 1-2 min. at adoptere enheden. Hvis status efterfølgende er **"Click to Update"**, er der kommet en opdatering til enheden, som du bør installere.

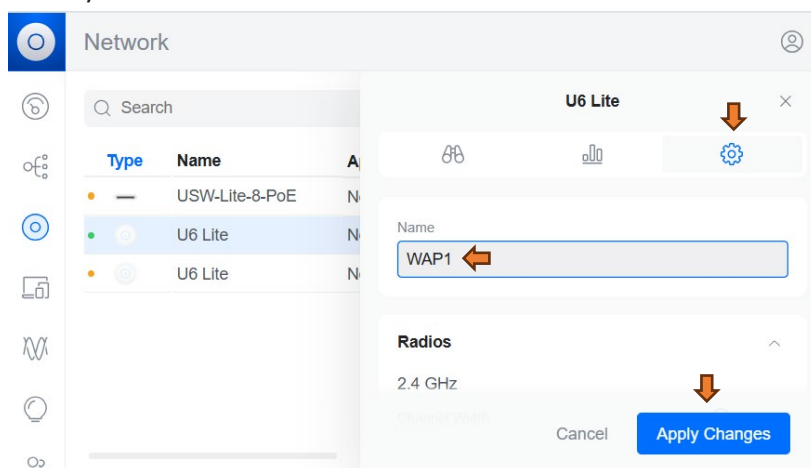


3. Klik på enhed hvor der står **"Click to Learn More"**. Tjek MAC-adresse og find den fysiske enhed. Nulstil enhed ved at holde reset-knap nede med spidsen af en papir-clips indtil lys ændrer sig. Vent 1-2 min. på den starter op igen. Hvis den er nulstillet korrekt, bør den kunne adopteres nu.



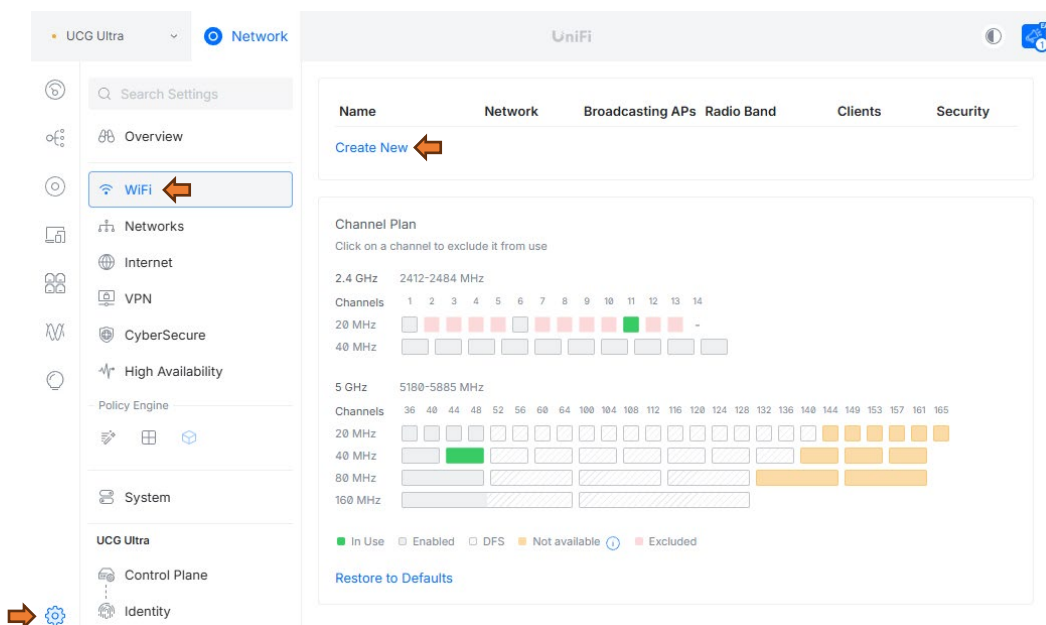
Fortsættes på næste side...

4. Navngiv enheden og opmærk evt. Access Point med Dymo, så du kan holde styr på dem når du har flere. Klik på enheden, vælg **Settings** og angiv et beskrivende navn og klik herefter **Apply Changes**. Nederst i Settings, kan du også aktivere **"Locate"**, hvor den valgte Access Point, så blinker hurtigt blå, så du kan se hvilken du konfigurer. Husk at trykke "Stop Locating" herefter. I disse indstillinger kan du også angive en statisk IP-adresse, hvis ikke den skal køre dynamisk eller har en DHCP Reservation.



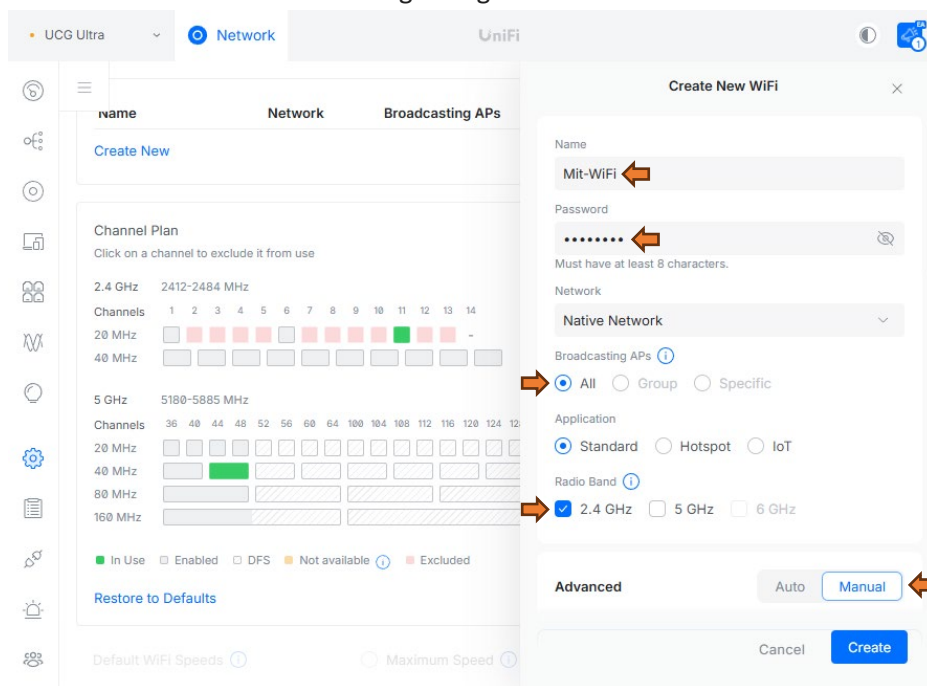
Konfigurer Trådløse netværk

1. Klik på **Settings** og derefter **WiFi** i menuen til venstre. Her ses de trådløse netværk. Tryk på **"Create New"** for at oprette et nyt trådløst netværk (Det kræver en WAP tilsluttet).

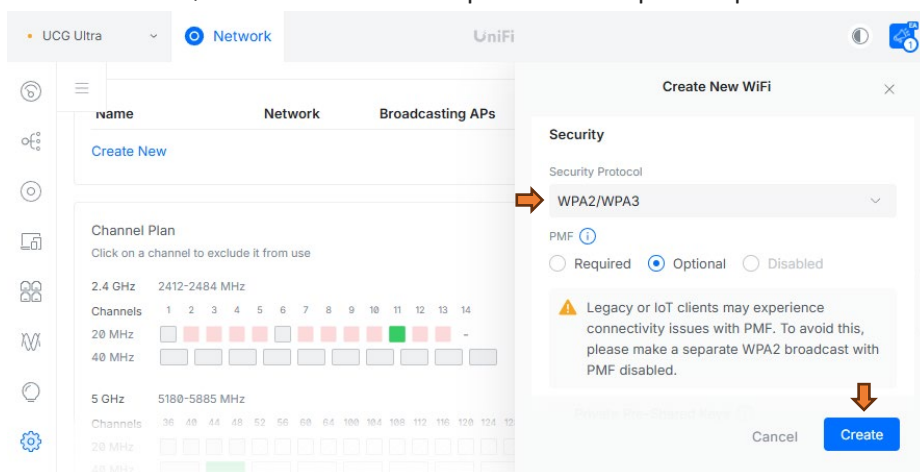


Fortsættes på næste side...

2. Angiv et **navn** (SSID) til det trådløse netværk og en ønsket **kode**. Brug kun A-Z, 0-9, punktum, bindestreg og bundstreg. Undgå æøå. Vælg alle Access Points og ønsket **Radio Band**, så du kan oprette et trådløst netværk på hver sin frekvens.. Vælg **Manual** ved **Advanced** for at få flere indstillingsmuligheder.

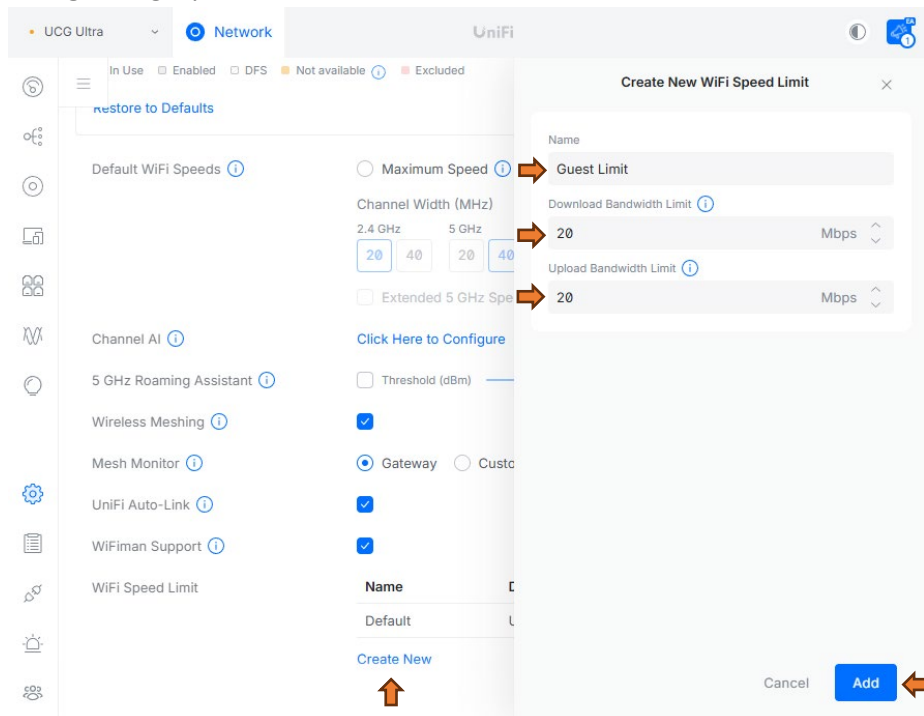


3. Under **Advanced** kan du vælge "**Security Protocol**". Nyeste og sikreste protokol er WPA3, men ældre enheder understøtter kun op til WPA2, så vælg denne eller kombination som her. Klik til sidst **Add WiFi Network**, hvorefter du kommer tilbage til oversigten og kan se det nye netværk. Gentag for hvert trådløst netværk du ønsker. Tilføj "**_5G**", "**_6G**" til det valgte WiFi navn på andre frekvenser end standard 2.4 GHz. Tilføj "**_Guest**" til gæste-WiFi og "**_MLO**" hvis du har et WiFi 7 AP med understøttelse for Multi Link Operation der opererer på flere frekvenser samtidigt.



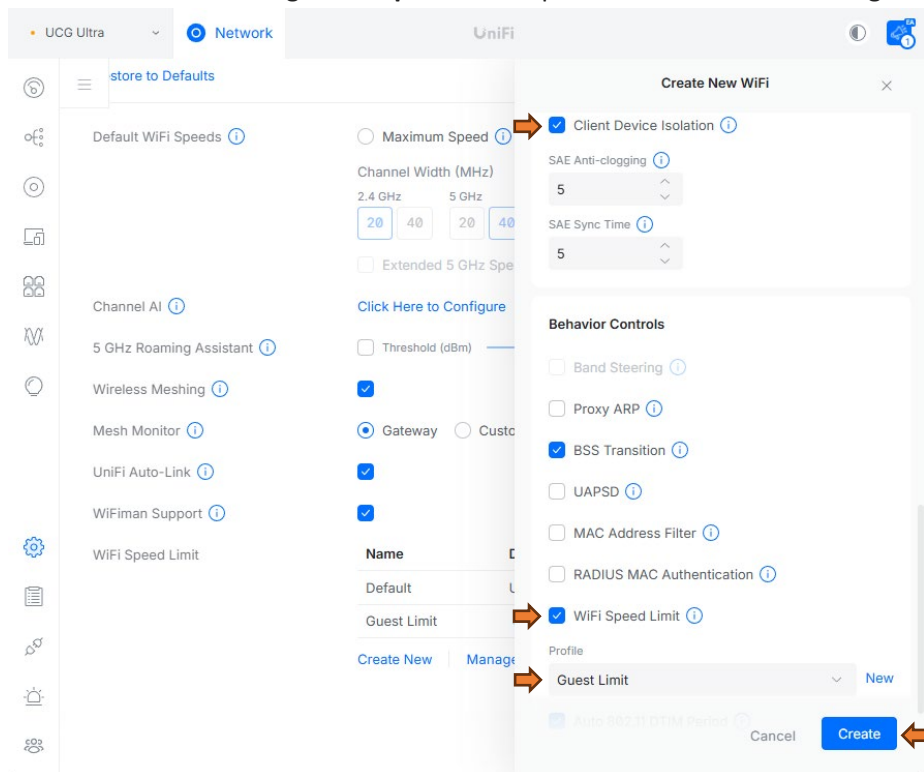
Fortsættes på næste side...

4. Hvis du vil begrænse den enkelte brugers hastighed og sikre kapacitet nok til alle, kan du oprette profiler med **"WiFi Speed Limit"**. De oprettes i bunden af siden i **Settings -> WiFi**. Klik **Create New**. Angiv et beskrivende **navn** og ønsket **Download/Upload hastighed** og tryk herefter **Add**.



The screenshot shows the UniFi Gateway settings interface. On the left, the 'WiFi Speed Limit' option is selected under the 'Settings' tab. The main panel displays the 'Create New WiFi Speed Limit' dialog. The 'Name' field is set to 'Guest Limit'. The 'Download Bandwidth Limit' is set to 20 Mbps, and the 'Upload Bandwidth Limit' is also set to 20 Mbps. The 'Add' button is highlighted with a red arrow.

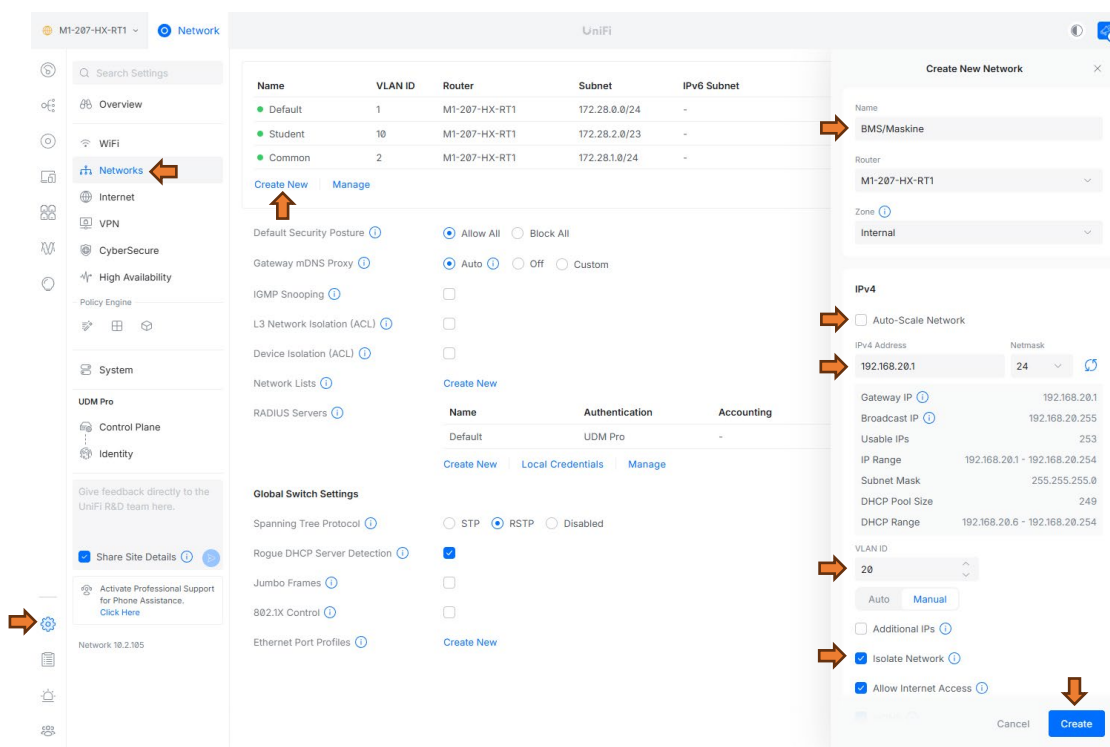
5. Hvis ikke enheder skal kunne se hinanden på netværk (f.eks. gæste-wifi), så sæt flueben i **Client Device Isolation**. Tilvælg **"WiFi Speed Limit"** på ønskede WiFi-netværk og vælg relevant profil.



The screenshot shows the UniFi Gateway settings interface. On the left, the 'WiFi Speed Limit' option is selected under the 'Settings' tab. The main panel displays the 'Create New WiFi' dialog. The 'Client Device Isolation' checkbox is checked. The 'SAE Anti-clogging' is set to 5, and the 'SAE Sync Time' is set to 5. Under 'Behavior Controls', the 'BSS Transition' checkbox is checked. The 'WiFi Speed Limit' checkbox is also checked. The 'Profile' dropdown is set to 'Guest Limit'. The 'Create' button is highlighted with a red arrow.

Opret isoleret netværk på andet VLAN (valgfri)

1. Klik på **Create New** under **Settings -> Networks**
2. Navngiv netværket, f.eks. **"BMS/Maskine"** eller **"IoT"**
3. Fjern flueben i **"Auto-Scale Network"**
4. Angiv ønsket IPv4-adresse, f.eks. **"192.168.20.1 /24"**
5. Angiv ønsket VLAN ID, f.eks. **"20"**
6. Under **Manual** tilvælges **Isolate Network** for at der ikke kan kommunikeres med andre netværk, men stadig have Internet-adgang.
7. Klik **Create**



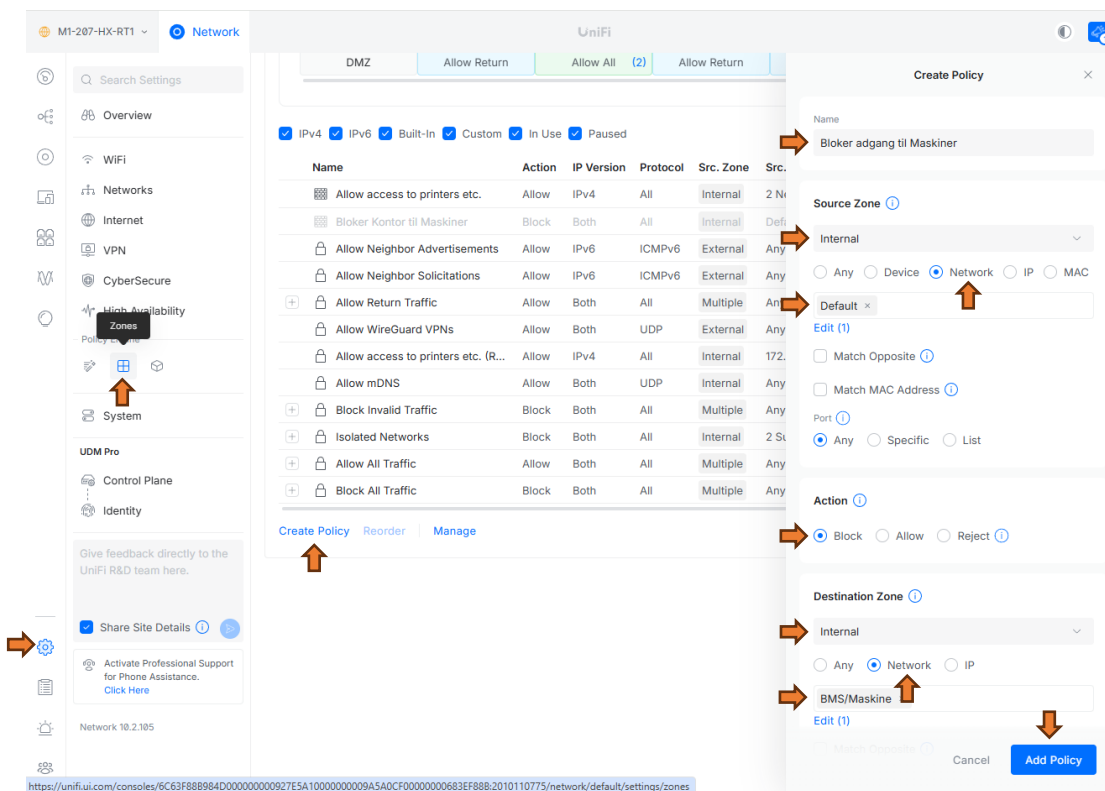
The screenshot shows the UniFi Gateway settings interface. On the left, the 'Networks' tab is selected in the sidebar. The main panel displays a table of existing networks and a 'Create New Network' dialog. The dialog is open to the 'Manual' tab, where the following settings are visible:

- Name:** BMS/Maskine
- Router:** M1-207-HX-RT1
- Zone:** Internal
- IPv4:**
 - ☐ Auto-Scale Network
 - IPv4 Address:** 192.168.20.1
 - Netmask:** 24
 - Gateway IP:** 192.168.20.1
 - Broadcast IP:** 192.168.20.255
 - Usable IPs:** 253
 - IP Range:** 192.168.20.1 - 192.168.20.254
 - Subnet Mask:** 255.255.255.0
 - DHCP Pool Size:** 249
 - DHCP Range:** 192.168.20.6 - 192.168.20.254
- VLAN ID:** 20
- Auto:** Manual
- ☐ Additional IPs
- ☒ Isolate Network
- ☒ Allow Internet Access

The 'Create' button is highlighted with an orange arrow.

Bloker adgang til isoleret netværk (valgfri)

1. Klik på **Create Policy** under **Settings -> Zones**
2. Giv regel et beskrivende navn, som f.eks. **"Bloker adgang til Maskiner"**
3. **Source Zone:** Vælg **Internal** og herunder **Network** og tilvæl **Default** og evt. andre netværk der ikke må få adgang
4. **Action:** Vælg **Block**
5. **Destination Zone:** Vælg **Internal** og herunder **Network** og vælg dit **BMS/Maskine** netværk
6. Klik på **Add Policy**

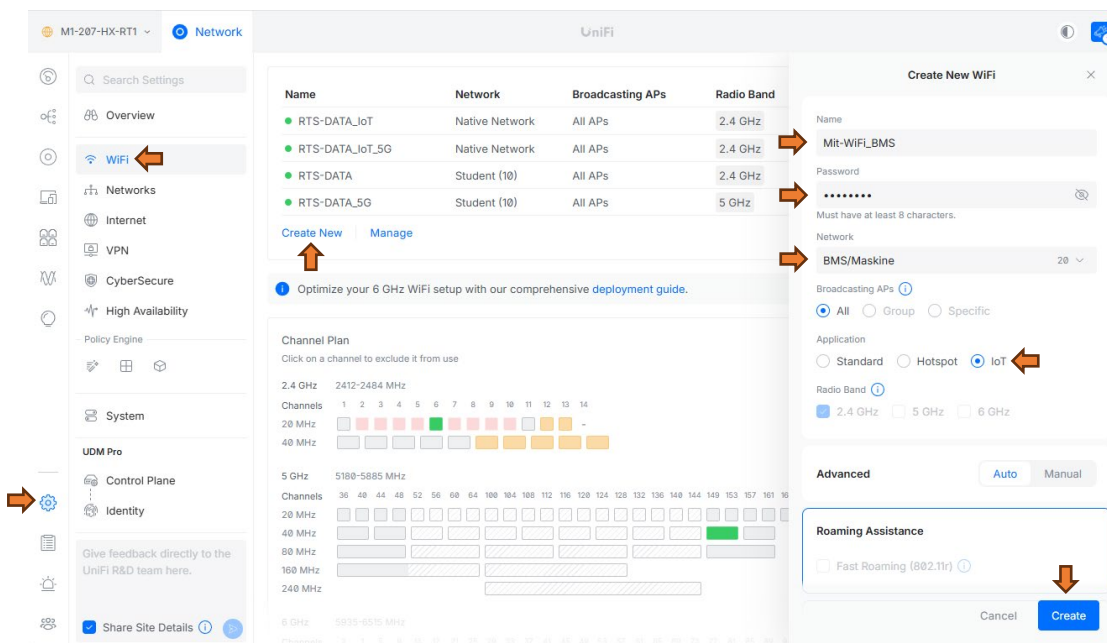


The screenshot shows the UniFi Gateway web interface. On the left sidebar, the 'Zones' menu item is highlighted with an orange arrow. The main panel displays a list of existing policies, including 'Allow access to printers etc.', 'Blocker Kontor til Maskiner', and 'Allow Neighbor Advertisements'. The 'Create Policy' dialog is open on the right, showing the configuration for a new policy named 'Bloker adgang til Maskiner'. The 'Source Zone' is set to 'Internal' and the 'Destination Zone' is set to 'Internal'. The 'Action' is set to 'Block'. The 'Add Policy' button is highlighted with an orange arrow.

Name	Action	IP Version	Protocol	Src. Zone	Src.
Allow access to printers etc.	Allow	IPv4	All	Internal	2 N
Bloker Kontor til Maskiner	Block	Both	All	Internal	Def
Allow Neighbor Advertisements	Allow	IPv6	ICMPv6	External	Any
Allow Neighbor Solicitations	Allow	IPv6	ICMPv6	External	Any
Allow Return Traffic	Allow	Both	All	Multiple	Any
Allow WireGuard VPNs	Allow	Both	UDP	External	Any
Allow access to printers etc. (R...	Allow	IPv4	All	Internal	172.
Allow mDNS	Allow	Both	UDP	Internal	Any
Block Invalid Traffic	Block	Both	All	Multiple	Any
Isolated Networks	Block	Both	All	Internal	2 S
Allow All Traffic	Allow	Both	All	Multiple	Any
Block All Traffic	Block	Both	All	Multiple	Any

Opret WiFi til isoleret netværk

1. Klik på **Create New** under **Settings -> WiFi**
2. Angiv et **navn** (SSID) til det trådløse netværk og en ønsket **kode**. Brug suffiks der beskriver netværket som f.eks. "**_BMS**" eller "**_IoT**"
3. Vælg det isolerede netværk som f.eks. her "**BMS/Maskine**"
4. Vælg **IoT** for at WiFi er kompatibelt med så mange enheder som muligt. Dette ændrer Radio Band til **2.4 GHz**, Security Protocol til **WPA2** og deaktiverer **BSS Transition**
5. Klik **Create**



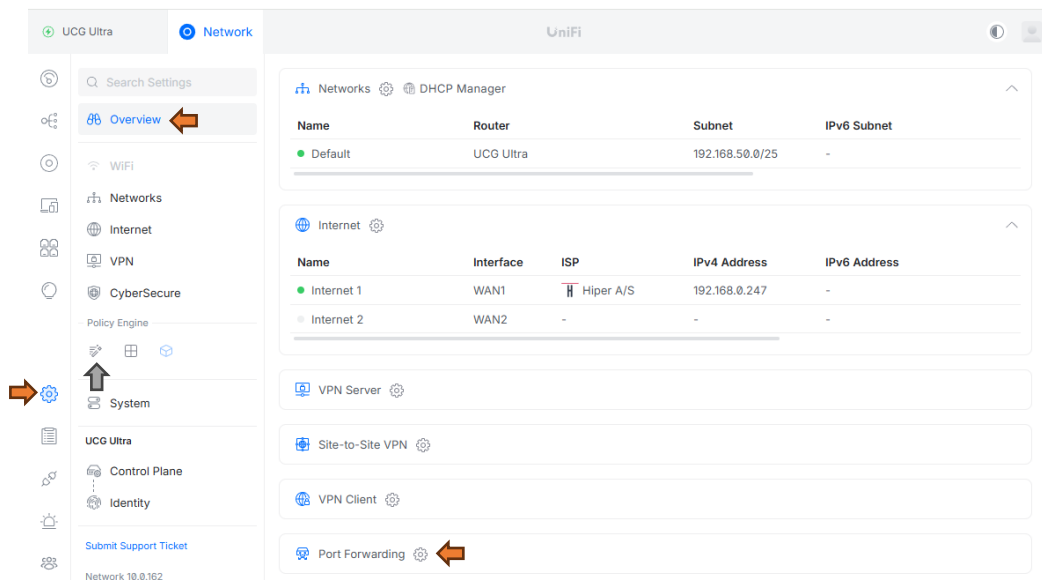
The screenshot shows the UniFi Gateway settings interface. On the left, the 'WiFi' tab is selected in the sidebar. The main content area displays a table of existing WiFi networks and a 'Channel Plan' section. The 'Create New WiFi' dialog box is open, showing the following fields:

- Name:** Mit-WiFi_BMS
- Password:** *****
- Network:** BMS/Maskine
- Broadcasting APs:** All
- Application:** IoT
- Radio Band:** 2.4 GHz

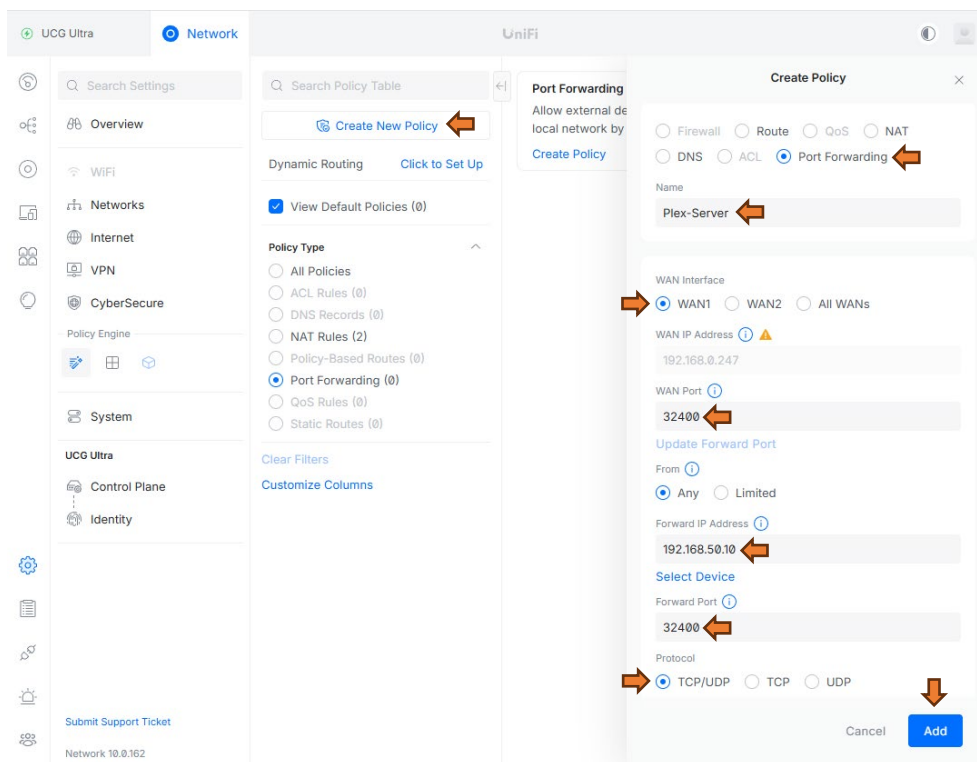
The 'Create' button is highlighted with an orange arrow.

Port Forwarding

1. Gå til **Settings -> Overview** og klik på tandhjul ud for **"Port Forwarding"** eller ikonet **"Policy Table"**



2. Her kan du åbne porte, hvis du skal have adgang til en enhed på det lokale netværk fra andre netværk (f.eks. når du ikke er hjemme). Dette eksempel åbner adgang til en Plex Server. Husk enhed skal have fast IP, da port henviser til specifik IP. Tryk **Create New Policy**.



- a. i dialogboks til højre, sikrer du **Port Forwarding** er valgt
- b. Angiv valgfrit navn på service
- c. WAN Interface (fysisk port) som Internet er tilsluttet din Gateway
- d. WAN- og Forward Port (logisk port) som service bruger
- e. Forward IP (IP-adresse til din server)
- f. Den protokol service bruger (TCP/UDP).
- g. Tryk **Add**.

Bemærk udråbstegn

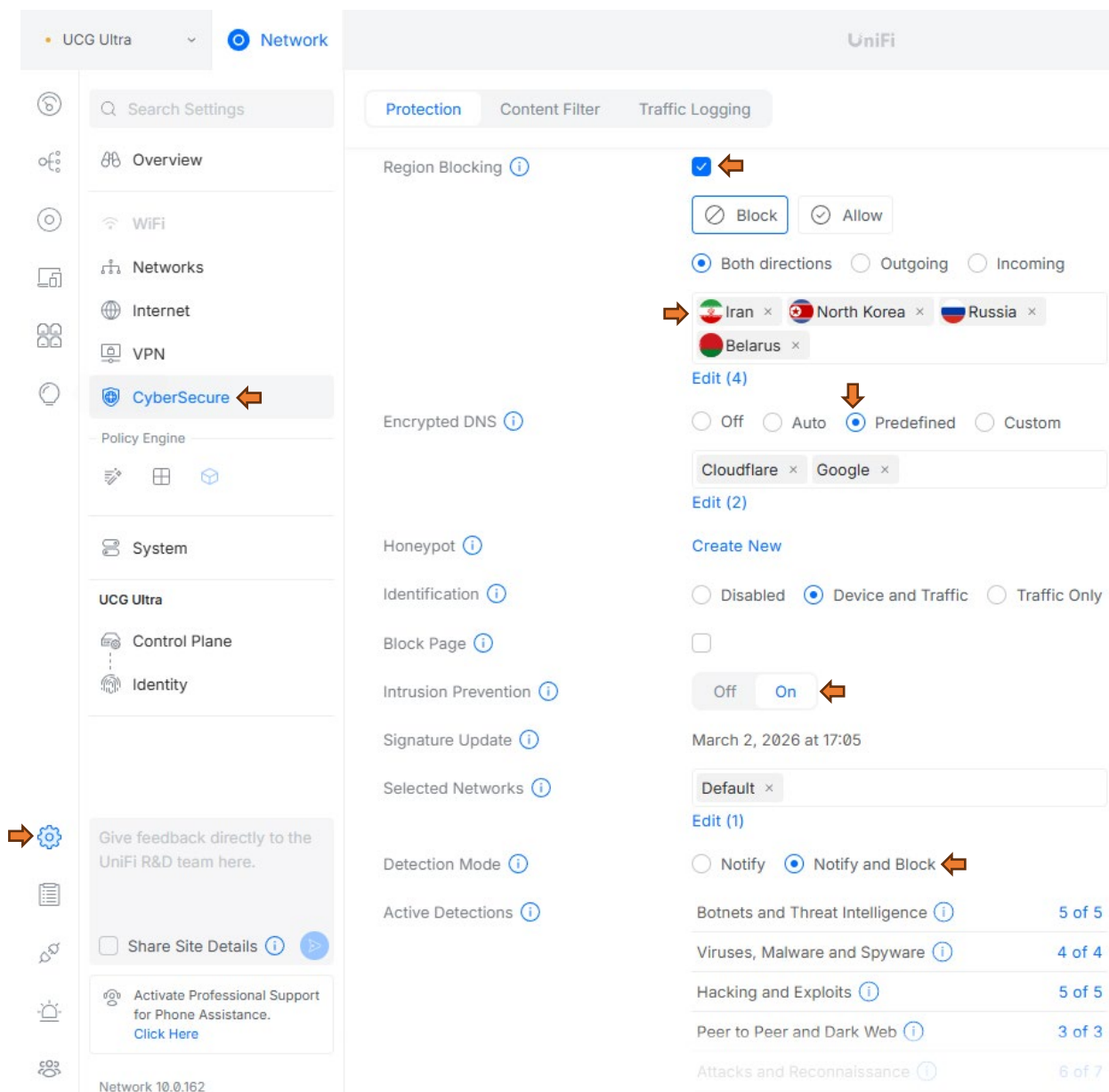
ved WAN IP her, da jeg ikke er direkte forbundet til Internet med offentlig IP. Derfor vil det ikke fungere i praksis, da der er endnu en Router/Firewall på netværket.

Sikkerhed

Gateway har både SPI (Stateful Packet Inspection - Layer 4) og DPI (Deep Packet Inspection - Layer 7) indbygget, men nogle funktioner kræver opgradering til CyberSecure Enhanced (89€/år).

Der er understøttelse for både [Intrusion Detection and Prevention \(IDS/IPS\)](#) som er noget af den bedste sikkerhed der tilbydes på Gateways. Gå til **Settings -> CyberSecure**:

1. Aktiver **Region Blocking** (Both directions) og tilføj f.eks. Iran, Nord Korea, Rusland og Hvide Rusland for at begrænse al trafik med de regioner.
2. Aktiver **Encrypted DNS** til Cloudflare og Googles DNS, så alle DNS-opslag igennem Router bliver krypteret igennem HTTPS (DoH). Husk at alle enheder skal bruge Router som primær DNS-server.
3. Aktiver **Intrusion Prevention** og sæt **Detection Mode** til **Notify and Block**, så evt. Trusler også bliver blokeret af Router.



The screenshot displays the UniFi Gateway's CyberSecure settings. The left sidebar contains a 'CyberSecure' menu item with an arrow pointing to it. The main panel is divided into several sections:

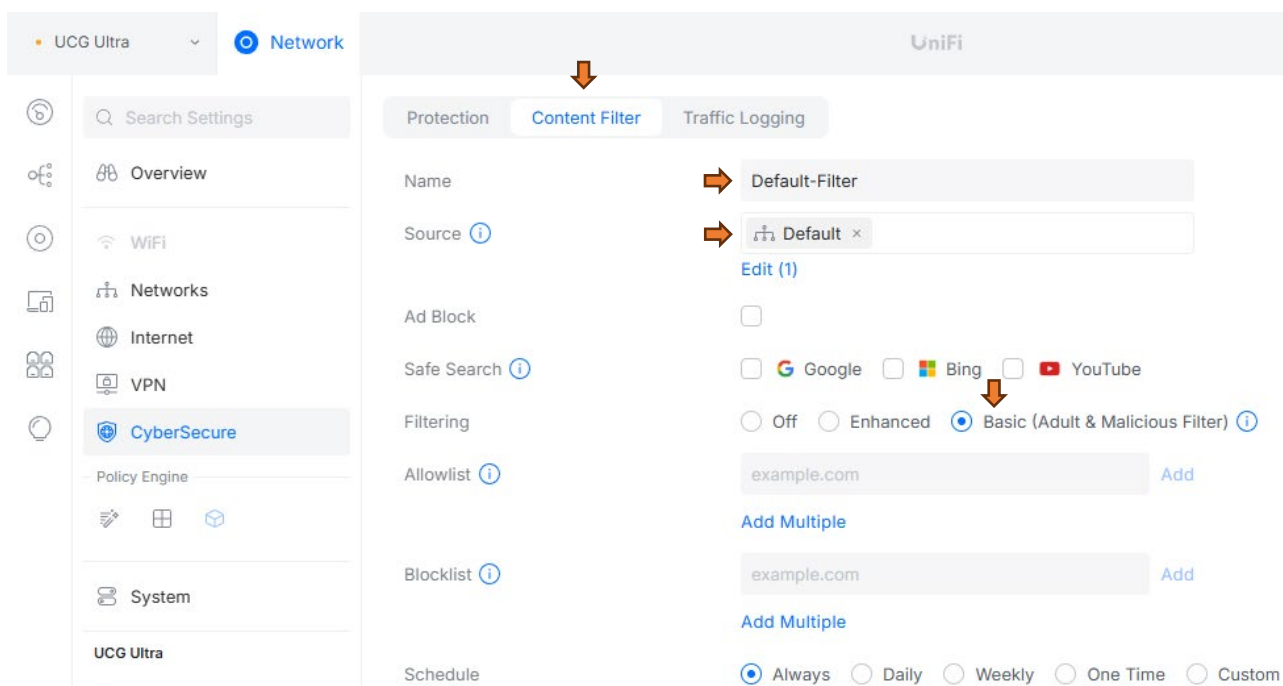
- Region Blocking:** A checkbox is checked, and the 'Block' button is selected. The 'Both directions' radio button is chosen. A list of regions includes Iran, North Korea, Russia, and Belarus.
- Encrypted DNS:** The 'Predefined' radio button is selected. The 'Cloudflare' and 'Google' DNS providers are listed.
- Intrusion Prevention:** The 'On' button is selected.
- Detection Mode:** The 'Notify and Block' radio button is selected.

At the bottom of the main panel, a table lists various threat categories and their status:

Threat Category	Status
Botnets and Threat Intelligence	5 of 5
Viruses, Malware and Spyware	4 of 4
Hacking and Exploits	5 of 5
Peer to Peer and Dark Web	3 of 3
Attacks and Reconnaissance	6 of 7

6. Aktiver evt. **Content Filter**

- Angiv **Navn**, "f.eks. Default-Filter" som her
- Vælg **Source**, f.eks. dit LAN navngivet "**Default**" medmindre du har ændret det.
- Tjek "**Basic (Adult & Malicious Filter)**" er valgt for at blokere voksen-indhold og ondsindede sider efter pre-konfigurerede lister. **Enhanced** er noget bedre og bruger CloudFlare, men det kræver abonnement. Det er også muligt at tilføje sider på **Allowlist**, hvis en side bliver blokeret som en falsk-positiv og du ved den er sikker, eller der er enkelte Voksen-sider du gerne ville kunne tilgå. Omvendt kan du tilføje sider på **Blocklist**, hvis enkelte sider ikke fanges.
- Sæt evt. Ad Block og Safe Search til, hvis ikke du har andet Software til dette, som er lettere at administrere. F.eks. Windows Defender/MalwareBytes' Browser Guard eller andre Browser Udvidelser.
- Brug **Altid**, eller ændre **Schedule** til hvornår denne filtrering skal gælde.

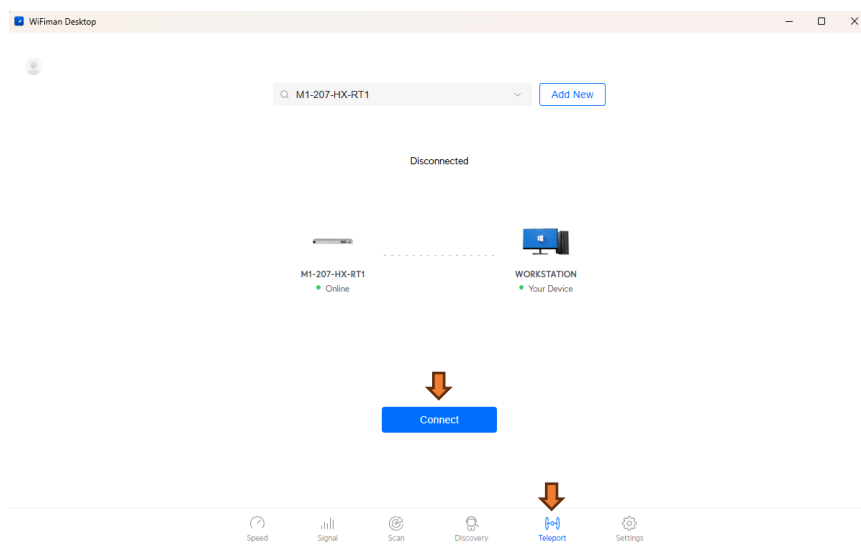


The screenshot shows the UniFi Gateway web interface. On the left is a sidebar with navigation icons and labels: Search Settings, Overview, WiFi, Networks, Internet, VPN, CyberSecure (highlighted), Policy Engine, System, and UCG Ultra. The main content area is titled 'UniFi' and has three tabs: Protection, Content Filter (selected), and Traffic Logging. Under the 'Content Filter' tab, there are several settings: 'Name' is set to 'Default-Filter'; 'Source' is set to 'Default' with a dropdown arrow; 'Ad Block' is unchecked; 'Safe Search' is unchecked; 'Filtering' has three radio buttons: 'Off', 'Enhanced', and 'Basic (Adult & Malicious Filter)' (selected); 'Allowlist' and 'Blocklist' each have an input field with 'example.com' and an 'Add' button; 'Schedule' has five radio buttons: 'Always' (selected), 'Daily', 'Weekly', 'One Time', and 'Custom'. There are also links for 'Edit (1)', 'Add Multiple', and 'Add' for the lists.

Opret VPN-adgang til dit netværk

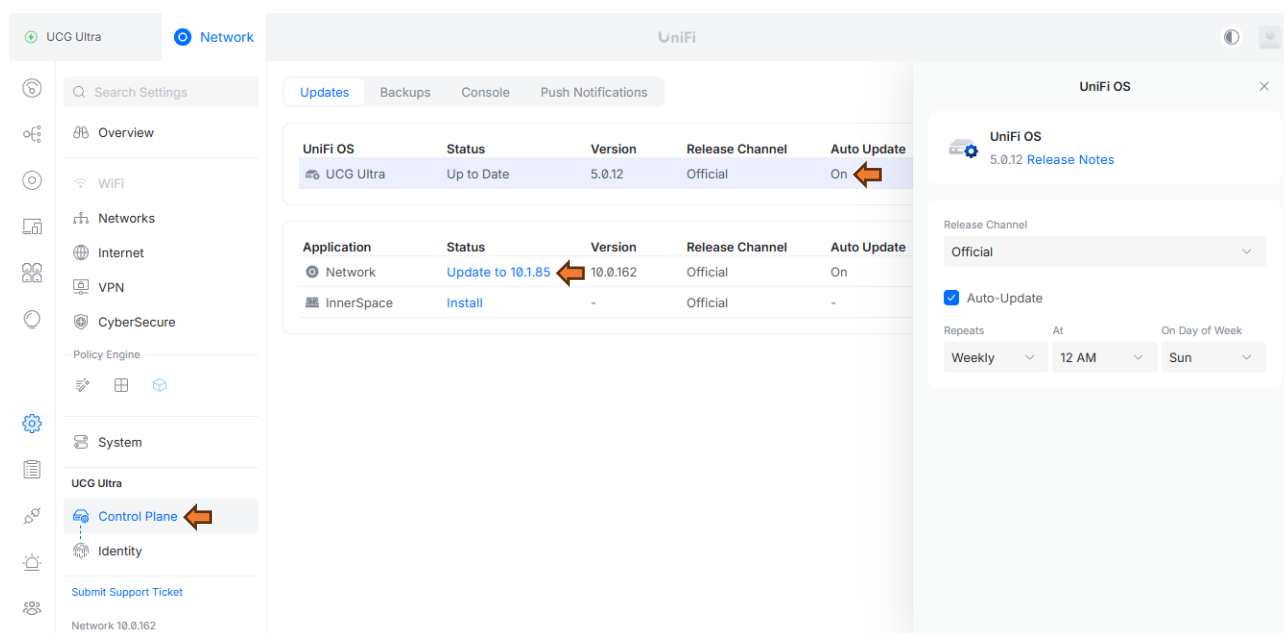
Den hurtigste og nemmeste løsning er at hente [WiFiman](#).

1. Klik på **Teleport** og **Connect**. Så kommunikerer du igennem dit UniFi netværk uanset hvor du er i verden. Fordelen ved denne løsning kontra alternativer som WireGuard, OpenVPN eller L2TP, er at de kræver der åbnes porte i Gateway.



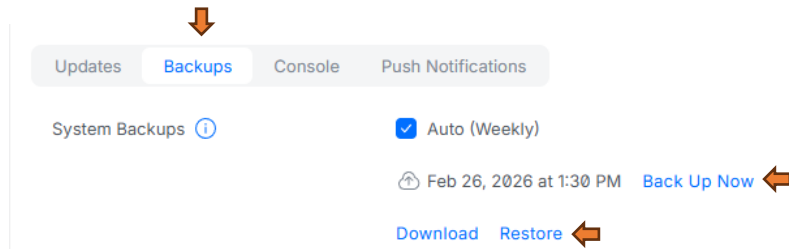
Opdateringer

1. Der kan være opdateringer til både enhed og Softwaren på, så tjek under **Settings -> Control Plane**. Her er enheden opdateret, men der er en opdatering til Network-softwaren på den. Automatiske opdateringer er dog aktiveret, så jeg kan vente og lade den gøre det automatisk eller tvinge opdatering igennem nu.



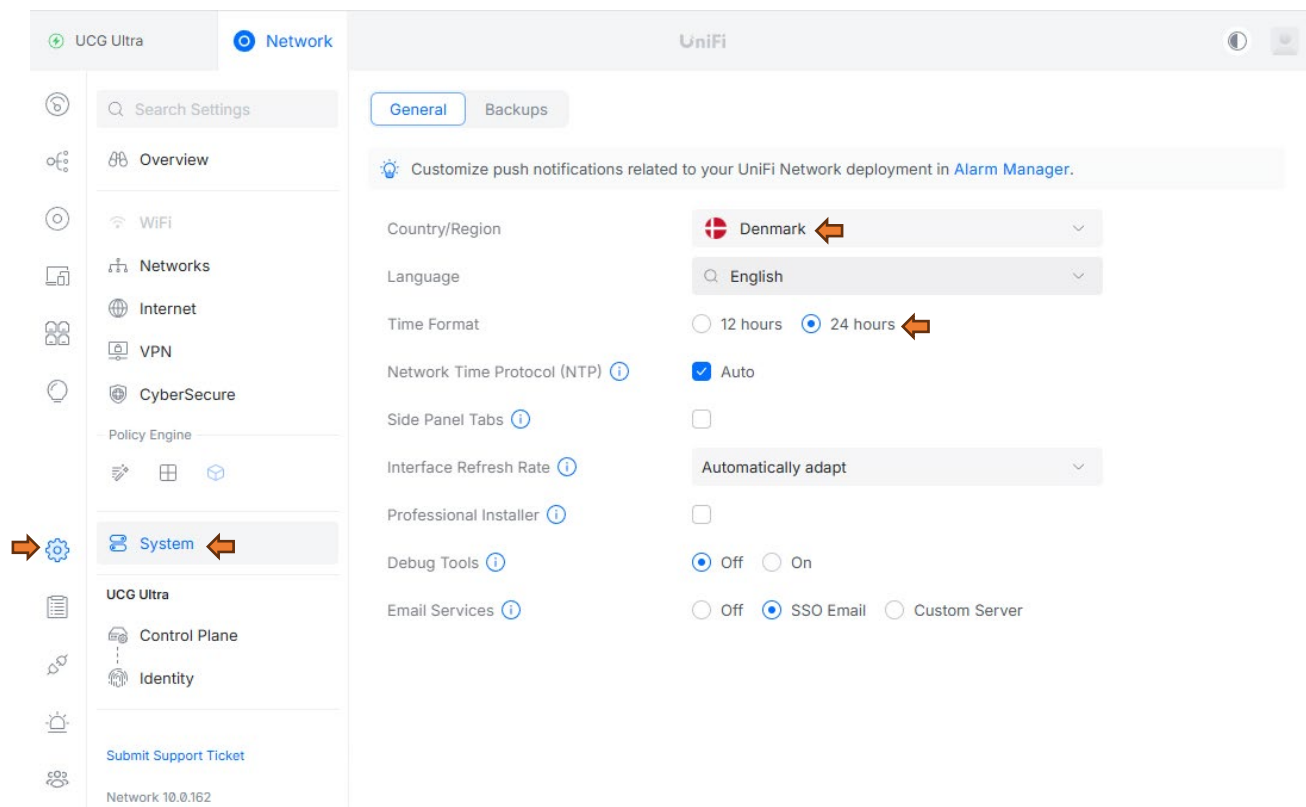
Backup & Restore

1. Findes under **Backups** i **Settings** -> **Control Plane**. Der laves automatisk cloud backup ugentligt af alle indstillinger. Du kan også gennemtvinge backup hvis du lige har lavet en masse ændringer. Omvendt kan du også genskabe en backup her, hvis fået lavet noget rod og ting ikke virker optimalt mere.



Systemindstillinger

1. Tjek korrekt **Country/Region** og **Time Format** er indstillet i **Settings -> System**



UCG Ultra Network UniFi

Search Settings

Overview

WiFi

Networks

Internet

VPN

CyberSecure

Policy Engine

System

UCG Ultra

Control Plane

Identity

Submit Support Ticket

Network 10.0.162

General Backups

Customize push notifications related to your UniFi Network deployment in [Alarm Manager](#).

Country/Region: Denmark

Language: English

Time Format: 12 hours 24 hours

Network Time Protocol (NTP): Auto

Side Panel Tabs

Interface Refresh Rate: Automatically adapt

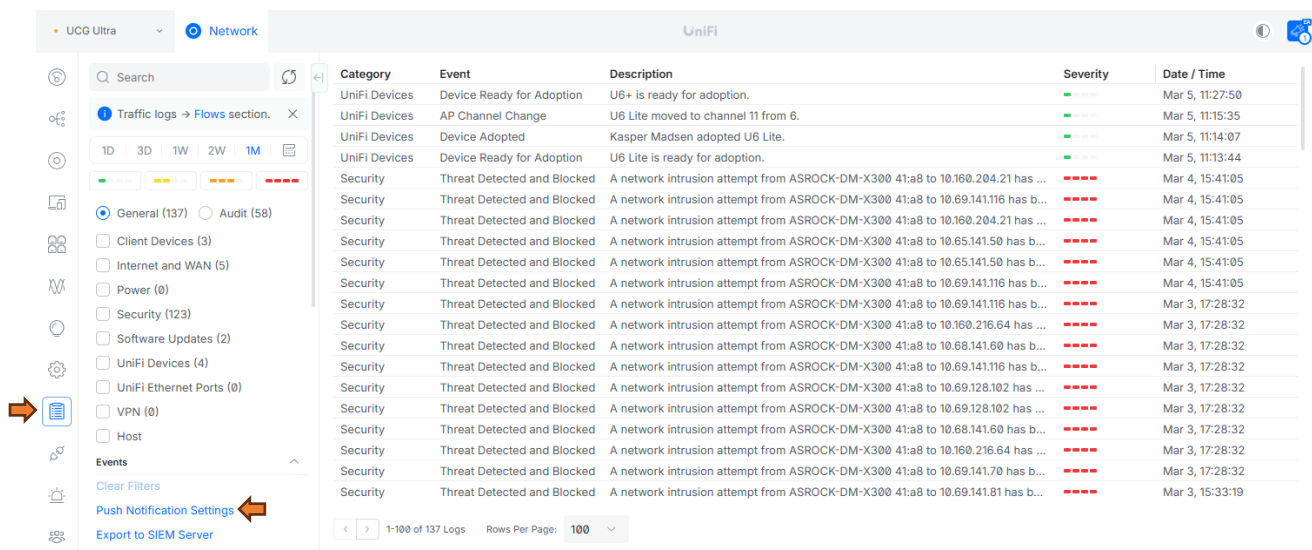
Professional Installer

Debug Tools: Off On

Email Services: Off SSO Email Custom Server

Log og notifikationer

Tjek log for trafik løbende for at overvåge netværk/hændelser og indstil hvad du ønsker notifikationer på og hvordan, f.eks. Push notifikation fra [UniFi App](#) eller Email.



UCG Ultra Network UniFi

Search

Traffic logs → [Flows section](#)

1D 3D 1W 2W 1M

General (137) Audit (58)

Client Devices (3)

Internet and WAN (5)

Power (0)

Security (123)

Software Updates (2)

UniFi Devices (4)

UniFi Ethernet Ports (0)

VPN (0)

Host

Events

Clear Filters

Push Notification Settings

Export to SIEM Server

Category	Event	Description	Severity	Date / Time
UniFi Devices	Device Ready for Adoption	U6+ is ready for adoption.	Info	Mar 5, 11:27:50
UniFi Devices	AP Channel Change	U6 Lite moved to channel 11 from 6.	Info	Mar 5, 11:15:35
UniFi Devices	Device Adopted	Kasper Madsen adopted U6 Lite.	Info	Mar 5, 11:14:07
UniFi Devices	Device Ready for Adoption	U6 Lite is ready for adoption.	Info	Mar 5, 11:13:44
Security	Threat Detected and Blocked	A network intrusion attempt from ASROCK-DM-X300 41:a8 to 10.160.204.21 has b...	High	Mar 4, 15:41:05
Security	Threat Detected and Blocked	A network intrusion attempt from ASROCK-DM-X300 41:a8 to 10.69.141.116 has b...	High	Mar 4, 15:41:05
Security	Threat Detected and Blocked	A network intrusion attempt from ASROCK-DM-X300 41:a8 to 10.160.204.21 has b...	High	Mar 4, 15:41:05
Security	Threat Detected and Blocked	A network intrusion attempt from ASROCK-DM-X300 41:a8 to 10.65.141.50 has b...	High	Mar 4, 15:41:05
Security	Threat Detected and Blocked	A network intrusion attempt from ASROCK-DM-X300 41:a8 to 10.65.141.50 has b...	High	Mar 4, 15:41:05
Security	Threat Detected and Blocked	A network intrusion attempt from ASROCK-DM-X300 41:a8 to 10.69.141.116 has b...	High	Mar 4, 15:41:05
Security	Threat Detected and Blocked	A network intrusion attempt from ASROCK-DM-X300 41:a8 to 10.69.141.116 has b...	High	Mar 3, 17:28:32
Security	Threat Detected and Blocked	A network intrusion attempt from ASROCK-DM-X300 41:a8 to 10.160.216.64 has b...	High	Mar 3, 17:28:32
Security	Threat Detected and Blocked	A network intrusion attempt from ASROCK-DM-X300 41:a8 to 10.68.141.60 has b...	High	Mar 3, 17:28:32
Security	Threat Detected and Blocked	A network intrusion attempt from ASROCK-DM-X300 41:a8 to 10.69.141.116 has b...	High	Mar 3, 17:28:32
Security	Threat Detected and Blocked	A network intrusion attempt from ASROCK-DM-X300 41:a8 to 10.69.128.102 has b...	High	Mar 3, 17:28:32
Security	Threat Detected and Blocked	A network intrusion attempt from ASROCK-DM-X300 41:a8 to 10.69.128.102 has b...	High	Mar 3, 17:28:32
Security	Threat Detected and Blocked	A network intrusion attempt from ASROCK-DM-X300 41:a8 to 10.68.141.60 has b...	High	Mar 3, 17:28:32
Security	Threat Detected and Blocked	A network intrusion attempt from ASROCK-DM-X300 41:a8 to 10.68.141.60 has b...	High	Mar 3, 17:28:32
Security	Threat Detected and Blocked	A network intrusion attempt from ASROCK-DM-X300 41:a8 to 10.160.216.64 has b...	High	Mar 3, 17:28:32
Security	Threat Detected and Blocked	A network intrusion attempt from ASROCK-DM-X300 41:a8 to 10.69.141.70 has b...	High	Mar 3, 17:28:32
Security	Threat Detected and Blocked	A network intrusion attempt from ASROCK-DM-X300 41:a8 to 10.69.141.81 has b...	High	Mar 3, 15:33:19

1-100 of 137 Logs Rows Per Page: 100