IP-COM



# Manual utilizare interfață web de gestionare

pentru punctele de acces Wi-Fi 7, modele **Pro-7-LR** și **Pro-7-Lite**,

destinate utilizării în spații interioare cu montare pe plafon

Funcțiile disponibile ale AP-urilor pot varia în funcție de model și de versiunea software. Toate imaginile, pașii și descrierile din acest ghid au caracter orientativ și este posibil să nu reflecte în totalitate experiența reală de utilizare a dispozitivului.

## Declarație privind drepturile de autor

**Copyright © 2026 IP-COM Networks Co., Ltd. Toate drepturile rezervate.**

IP-COM este o marcă înregistrată a IP-COM Networks Co., Ltd. Celelalte mărci și denumiri de produse menționate în acest document sunt mărci comerciale sau mărci înregistrate ale deținătorilor lor respectivi. Drepturile de autor asupra produsului, ca ansamblu, inclusiv asupra accesoriilor și software-ului aferent, aparțin IP-COM Networks Co., Ltd. Nicio parte a acestei publicații nu poate fi reprodusă, transmisă, transcrisă, stocată într-un sistem de stocare și regăsire sau tradusă în nicio limbă, sub nicio formă și prin niciun mijloc, fără acordul prealabil, exprimat în scris, al IP-COM Networks Co., Ltd.

## Declinare de responsabilitate

Imaginile și specificațiile produsului prezentate aici au caracter informativ. Pentru îmbunătățirea designului intern, a funcționalității și/sau a fiabilității, IP-COM își rezervă dreptul de a modifica produsele descrise în acest document, fără obligația de a notifica în prealabil vreo persoană sau organizație. IP-COM nu își asumă nicio răspundere pentru eventualele consecințe rezultate din utilizarea sau aplicarea produsului ori a schemelor de circuit prezentate. La elaborarea acestui document au fost depuse toate eforturile pentru a asigura acuratețea informațiilor; cu toate acestea, declarațiile, informațiile și recomandările incluse nu constituie o garanție de niciun fel, expresă sau implicită.

# Prefață

Acest ghid descrie cum se configurează fiecare funcție, din interfața locală web de gestionare, a următoarelor puncte de acces de la IP-COM pentru montare în spații interioare acoperite. Montarea se poate face pe o suprafață plană, pe un perete sau pe un tavan.

- **Pro-7-LR**
- **Pro-7-Lite**

Note

Funcțiile disponibile ale AP-urilor pot varia în funcție de model și de versiunea software. Toate imaginile, pașii și descrierile din acest ghid au caracter orientativ și este posibil să nu reflecte în totalitate experiența reală de utilizare a dispozitivului.

## Convenții

În acest manual, termenii tehnici uzuali proveniți din engleză sunt scrișI românizat — adică așa cum sunt pronunțați și declinați în limba română, de exemplu, *ruter* în loc de *router*, *a seta* în loc de *to set* etc.

Figurile și capturile de ecran din acest ghid sunt prezentate cu titlu informativ. Acestea pot diferi de produsul real achiziționat, fără a afecta utilizarea normală.

Dacă o funcție sau un parametru apare afișat cu gri în interfața web a produsului, înseamnă că nu este disponibil pentru modelul respectiv sau nu poate fi modificat.

Elementele tipografice utilizate în acest document sunt definite după cum urmează.

| Articol | Prezentare | Exemplu |
|---|---|---|
| Meniuri în cascadă | > | **Wireless** > **SSID** |
| Parametru și valoare | Aldin, cu valoarea uneori cursiv | La **Nume utilizator** introduceți ***Albert***. |
| Variabilă | Cursiv și aldin | Format adresă MAC: ***XX:XX:XX:XX:XX:XX*** |
| Controlul interfeței utilizator | Aldin | Pe pagina **Politică**, faceți clic pe butonul **OK**. |
| Mesaj | Cursiv | Apare mesajul **Succes**. |

Simbolurile care pot fi găsite în acest document sunt definite după cum urmează.

| Simbol | Descriere |
| --- | --- |
|  | Notă: Este folosit pentru a evidenția informații importante sau de interes special. Ignorarea acestui tip de notă poate duce la configurații ineficiente, pierderi de date sau deteriorarea dispozitivului. |
|  | Sfat: Este folosit pentru a evidenția o procedură care va economisi timp sau resurse. |

## Pentru mai multe informații

Pentru a obține mai multe documente sau informații despre dispozitiv, vizitați pagina https://www.ip-com.com.cn/ro și căutați modelul dorit și accesați secțiunea **Descărcări** de pe pagina de prezentare a produsului.

## Suport tehnic

Contactați-ne dacă aveți nevoie de mai mult ajutor. Vom fi bucuroși să vă ajutăm cât mai curând posibil.

Adresă de e-mail: support.ro@ip-com.com.cn

Pagină web: https://www.ip-com.com.cn/ro

## Istoricul reviziilor

IP-COM caută în permanență modalități de a-și îmbunătăți produsele și documentația. Tabelul următor indică orice modificări care ar fi putut fi făcute de la lansarea ghidului de utilizare.

| Versiune | Data | Descriere |
| --- | --- | --- |
| V1.0 | 2026.05.26 | Prima publicare în limba română. |

# Cuprins


1 NOȚIUNI INTRODUCTIVE ȘI CONFIGURARE INIȚIALĂ ..... 1

1.1 Ce este acest echipament ..... 1

1.2 Moduri de gestionare ..... 1

1.3 Configurarea inițială din interfața locală web ..... 3

1.4 Setare mod conectare la rețeaua locală din amonte, prin Wi-Fi sau cablu Ethernet, din configuratorul inițial ..... 5

1.4.1 Conectare prin cablu Ethernet la rețeaua din amonte ..... 5

1.4.2 Conectare prin Wi-Fi la rețeaua din amonte ..... 9

2 ACCES INTERFAȚĂ WEB GESTIONARE, DUPĂ CONFIGURAREA INIȚIALĂ ..... 13

2.1 Conectare la interfața web ..... 13

2.2 Deconectare din interfața web ..... 16

2.3 Aspect interfață web ..... 16

2.4 Butoane comune găsite în interfața web ..... 17

2.5 Schimbare limbă interfață web ..... 17

3 MENIUL STATUS (STARE) ..... 18

3.1 Submeniul System Status (Stare sistem) ..... 18

3.2 Submeniul Wireless Status (Stare wireless) ..... 22

3.3 Submeniul Traffic Statistics (Statistici trafic) ..... 24

3.4 Submeniul Client List (Listă clienți) ..... 25

4 MENIUL QUICK SETUP (CONFIGURARE RAPIDĂ) ..... 27

4.1 Prezentare generală a meniului ..... 27

4.2 Mod de lucru AP ..... 28

4.3 Configurarea primului SSID de pe fiecare bandă, în modul de lucru AP ..... 29

**4.4 Mod de lucru Client+AP ..... 30**

**5 MENIUL INTERNET SETTINGS (SETĂRI INTERNET) ..... 32**

**5.1 Submeniul LAN Setup (Configurare LAN) ..... 32**
5.1.1 Fila LAN Setup (Configurare LAN) ..... 32
5.1.2 Fila Management IP (IP de gestionare) ..... 35

**5.2 Submeniul Intelligent DHCP Service (Serviciu DHCP inteligent) ..... 36**
5.2.1 Fila Intelligent DHCP Service (Serviciu DHCP inteligent) ..... 37
5.2.2 Fila DHCP Clients (Clienți DHCP) ..... 38

**6 MENIUL WIRELESS ..... 40**

**6.1 Submeniul SSID ..... 40**
6.1.1 Prezentare generală ..... 40
6.1.2 Protocoale de securitate Wi-Fi de la opțiunea Security Mode (Mod securitate) ..... 44
6.1.3 Exemplu configurare rețea Wi-Fi deschisă, fără parolă ..... 48
6.1.4 Exemplu configurare rețea Wi-Fi criptată cu PSK ..... 50
6.1.5 Exemplu de configurare a unei rețele Wi-Fi cu autentificare RADIUS și a unui server RADIUS pe Windows ..... 51

**6.2 Submeniul RF Settings (Setări radiofrecvențe) ..... 62**

**6.3 Submeniul RF Optimization (Optimizare radiofrecvențe) ..... 66**

**6.4 Submeniul Load Balancing (Echilibrare încărcare) ..... 73**
6.4.1 Echilibrare încărcare între AP-uri ..... 73
6.4.2 Echilibrare încărcare între benzi ..... 76

**6.5 Submeniul Frequency Analysis (Analiză frecvențe) ..... 78**
6.5.1 Afișare utilizare spectru ..... 78
6.5.2 Detalii rețele Wi-Fi din zonă ..... 79

**6.6 Submeniul Access Control (Control acces) ..... 80**
6.6.1 Adăugarea unei adrese MAC la Blacklist (Listă neagră), din meniul Access Control (Control acces) ..... 80
6.6.2 Adăugarea unei adrese MAC la Blacklist (Listă neagră), din meniul Client List (Listă clienți) ..... 81
6.6.3 Adăugare unei adrese MAC la Whitelist (Listă albă) ..... 82
6.6.4 Eliminarea unei adrese MAC din Blacklist (Listă neagră) sau din Whitelist (Listă albă) ..... 83

**6.7 Submeniul Advanced Settings (Setări avansate) ..... 84**
6.7.1 Prezentare generală ..... 84
6.7.2 Activare identificare tip client conectat ..... 87
6.7.3 Limitare rată trafic broadcast și multicast prin Wi-Fi ..... 87
6.7.4 Utilizare AP ca un controler virtual de AP-uri ..... 88

**6.8 Submeniul QVLAN Settings (Setări QVLAN) ..... 89**
6.8.1 Prezentare generală ..... 89
6.8.2 Exemplu de configurare a setărilor QVLAN ..... 90

**6.9 Submeniul WiFi Schedule (Orar Wi-Fi) ..... 92**

**6.10 Submeniul Roaming Settings (Setări roaming) ..... 94**

**7 MENIUL ADVANCED (AVANSAT) ..... 97**

**7.1 Submeniul Traffic Control (Control trafic) ..... 97**

**7.2 Submeniul Cloud Maintenance (Mentenanță cloud) ..... 100**
7.2.1 Prezentare generală ..... 100
7.2.2 Selectarea modului de gestionare ..... 102
7.2.3 Moduri de adăugare echipament în IP-COM ProFi Cloud ..... 103

**7.3 Submeniul Remote Management (Gestionare de la distanță) ..... 111**
7.3.1 Prezentare generală ..... 111
7.3.2 Exemplu de configurare a accesului la interfața web de gestionare din afara rețelei locale ..... 112

**8 MENIUL TOOLS (INSTRUMENTE) ..... 115**

**8.1 Submeniul Date & Time (Dată și oră) ..... 115**
8.1.1 Sincronizare dată și oră automată ..... 115
8.1.2 Setare manuală dată și oră ..... 116
8.1.3 Deconectare automată de la interfața de gestionare după o perioadă de inactivitate ..... 117

**8.2 Submeniul Maintenance (Mentenanță) ..... 118**
8.2.1 Repornire manuală ..... 118
8.2.2 Repornire periodică automată ..... 119
8.2.3 Resetare ..... 121
8.2.4 Salvare și restaurare setări echipament ..... 122
8.2.5 Control indicator led de pe echipament ..... 125

**8.3 Submeniul System Software Upgrade (Actualizare software sistem) ..... 126**
8.3.1 Actualizare locală de firmware ..... 127
8.3.2 Actualizare online de firmware ..... 127

**8.4 Submeniul System Account (Cont sistem) ..... 128**

**8.5 Submeniul System Log (Jurnal sistem) ..... 129**

**8.6 Submeniul Diagnostic Tool (Instrument diagnosticare) ..... 130**

**8.7 Submeniul Uplink Detection (Detectare legătură amonte) ..... 131**

**9 ANEXE ..... 134**

**9.1 Setări implicite ..... 134**

**9.2 Acronime și abrevieri ..... 135**

# 1 Noțiuni introductive și configurare inițială

Funcțiile pot varia în funcție de model și de versiunea software instalată. Imaginile, pașii și descrierile prezentate în acest manual au caracter orientativ și pot diferi de interfața sau funcționarea reală. În acest manual, denumirile meniurilor și ale opțiunilor sunt prezentate în limba engleză, iar echivalentul în limba română este indicat între paranteze. Manualul este adaptat utilizatorilor cunoscători de limba română.

## 1.1 Ce este acest echipament

În literatura de specialitate și în practică se folosesc, adesea interschimbabil, mai mulți termeni: *punct de acces la rețea locală prin Wi-Fi*, *punct de acces Wi-Fi*, *punct de acces fără fir*, *punct de acces*, *access point*, *wireless access point* sau, prescurtat, *AP*. Toți denumesc același lucru: un dispozitiv de rețea care permite echipamentelor wireless (telefon, laptop, cameră IP etc.) să se conecteze la o rețea locală (LAN).

Conexiunea cu rețeaua din amonte se face în două moduri, în funcție de configurație: prin cablu Ethernet către un switch sau ruter — caz în care echipamentul funcționează în modul de lucru **Access Point**. Sau prin Wi-Fi, conectându-se la rețeaua emisă de un alt ruter ori punct de acces — caz în care funcționează în modul **Bridge** (sau **Client+AP**).

Din punct de vedere al traficului, AP-ul se comportă ca un switch: direcționează cadrele pe baza adreselor MAC. Diferența față de un switch obișnuit este că, pe lângă porturile Ethernet, oferă și conectivitate Wi-Fi pentru dispozitivele din proximitate. AP-ul nu furnizează el însuși acces la internet — această funcție revine ruterului sau gateway-ului din rețeaua locală.

Pe parcursul acestui manual, termenii *AP*, *punct de acces* și *punct de acces Wi-Fi* sunt folosiți alternativ, cu sau fără ghilimele, pentru același echipament.

## 1.2 Moduri de gestionare

Aparatul poate fi gestionat prin mai multe moduri simultane sau complementare.

- **Din interfața web locală a AP-ului**

  Aparatul poate fi administrat direct din interfața web locală, accesând adresa IP LAN a dispozitivului, folosind un browser. Această interfață oferă acces la setul complet de funcții și este cea detaliată în **prezentul manual de utilizare**.

- **Din interfața web a unui ruter multi-WAN cu funcție de controler AP, de la IP-COM**

  Gestionarea AP-ului se poate realiza centralizat din interfața web a unui ruter multi-WAN cu funcție de controler AP integrat, din seria M de la IP-COM — modele compatibile fiind, de exemplu, IP-COM M20-PoE, IP-COM M20-8G-PoE, IP-COM M50-F, IP-COM M80-F etc. Ca principiu de funcționare, setările efectuate în interfața ruterului sunt propagate local către toate AP-urile adoptate, ceea ce permite o configurare uniformă a întregii rețele wireless dintr-un singur punct. Procedura de adăugare a unui AP în controler este simplă:

1. Asigurați-vă că ruterul multi-WAN este actualizat la ultima versiune de firmware.
2. Apoi AP-ul trebuie actualizat la cea mai recentă versiune de firmware.
3. Resetați AP-ul la setările din fabrică, indiferent dacă ați făcut actualizare de firmware sau nu.
4. Conectați AP-ul în aceeași rețea locală, fizică și logică, cu ruterul multi-WAN. Asigurați-vă că celelalte AP-uri neconfigurate și neadoptate nu sunt pornite. Efectuați adoptarea pe rând, unul câte unul.
5. După aproximativ 2–10 minute, AP-ul trebuie să apară automat detectat în meniul **AP > AP List and Maintenance (Listă AP-uri și mentenanță)** din interfața ruterului multi-WAN. Apoi, toate configurările, inclusiv cele de roaming, SSID, securitate sau optimizare radio, se aplică centralizat din submeniurile din meniul **AP** al interfeței web de gestionare a ruterului, fiind împinse către toate punctele de acces controlate.

  Note

  Dacă aveți mai multe AP-uri ce trebuie adoptate, conectați-le în rețea și adoptați-le pe rând, unul câte unul.

- **Cu controlerul software IP-COM ProFi Software Controller (Windows)**

  **IP-COM ProFi Software Controller** este un controler software instalabil pe Windows, utilizat pentru gestionarea și monitorizarea AP-urilor IP-COM și a switch-urilor din seria ProFi. Poate fi implementat on-premises, fără dependență de cloud, necesitând resurse hardware minime. Interfața este bine structurată, cu funcții automate, statistici și capabilități de raportare, facilitând configurarea, monitorizarea și depanarea. Controlerul permite roaming rapid și fără întreruperi, eliminând necesitatea unui controler hardware dedicat. În caz de defecțiuni, reinstalarea este simplă. Dacă se dorește ulterior, prin integrarea cu o platformă online denumită **IP-COM ProFi SDN**, se poate activa accesul remote din afara rețelei locale, de pe internet. Ca principiu, setările efectuate din interfața controlerului software sunt împinse local către AP-uri.

- **Din serviciul de gestionare unificată din cloud IP-COM ProFi Cloud**

  Platforma web **IP-COM ProFi Cloud** oferă gestionare și mentenanță unificată de la distanță pentru echipamentele IP-COM. Dispozitivele instalate în locații diferite pot fi centralizate într-un singur proiect, permițând monitorizarea și administrarea rețelei din orice locație. Interfața este intuitivă și orientată spre funcțiile uzuale ale administratorilor. Pentru funcționalitate completă, se poate accesa în paralel și interfața locală a dispozitivului. Gestionarea este disponibilă și prin aplicația mobilă **IP-COM ProFi** (Android și iOS), utilizând aceleași date securizate din cloud, fără costuri

suplimentare. Ca principiu, setările efectuate din interfața aplicației sau platformei web sunt împinse local către AP-uri. Modul de adoptare este explicat în acest manual la subcapitolul 7.2 Submeniul Cloud Maintenance (Mentenanță cloud).

## 1.3 Configurarea inițială din interfața locală web

Acest subcapitol descrie configurarea inițială a echipamentului direct din interfața web — pagina locală de administrare a punctului de acces — folosind expertul de configurare rapidă. Procedura se poate aplica atunci când punctul de acces este utilizat autonom: la prima punere în funcțiune, după o resetare la setările din fabrică, sau în orice altă situație în care AP-ul nu este gestionat de un alt echipament de rețea, de exemplu, un ruter multi-WAN cu funcție de control AP din seria *M* de la IP-COM ori de o platformă cloud precum IP-COM ProFi Cloud.

În unele scenarii de utilizare acest configurator pas cu pas nu e necesar a fi urmat, în altele e nevoie. Însă, pentru a accesa setările și meniurile din interfața web explicată în acest manual, e nevoie de parcurgerea configurării inițiale pas cu pas.

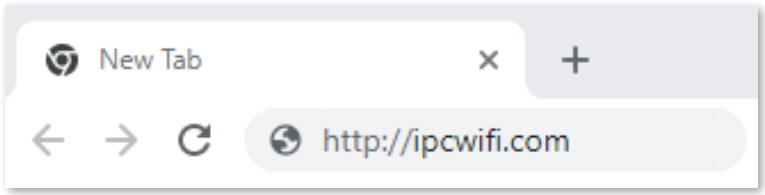
Expertul vă permite să configurați rapid conexiunea la rețeaua din amonte și parametrii de bază ai rețelei Wi-Fi și parola de acces la interfața de gestionare. Pentru opțiuni avansate, consultați capitolele corespunzătoare din acest ghid.

1. Cu un cablu Ethernet conectați portul marcat **PoE/LAN** de pe AP la un port Ethernet cu PoE de pe un switch PoE, sau, conectați la portul marcat **AP** (sau **Access Point**) de pe injectorul PoE inclus în pachet.
2. Așteptați câteva momente pornirea echipamentului. Obligatoriu citiți instrucțiunile din **Quick Installation Guide (Ghid de instalare rapidă)** pentru cum anume se alimentează echipamentul, cum se face cablarea, montarea și alte instrucțiuni.
3. Conectați un dispozitiv client la Wi-Fi-ul emis de AP sau conectați prin cablu Ethernet. Apoi accesați pagina web de gestionare și efectuați configurarea rapidă a AP-ului.

Tip

- Dacă punctul de acces nu este gestionat de niciun ruter multi-WAN sau platformă cloud, atunci rețelele Wi-Fi emise de AP sunt cele implicite, anume **IP-COM_*XXXXXX*** pentru rețeaua ce emite pe 2,4 GHz și **IP-COM_*XXXXXX*_5G** pentru 5 GHz. Iar ***XXXXXX*** reprezintă ultimele șase cifre ale adresei MAC de pe eticheta punctului de acces după îndepărtarea capacului frontal. Numele rețelelor Wi-Fi se află scrise pe eticheta de pe AP.
- Dacă vă conectați la rețeaua Wi-Fi utilizând un telefon sau o tabletă și apare o notificare de tip *Rețea nesecurizată*, ignorați acest mesaj și continuați cu conectarea la rețeaua Wi-Fi emisă de AP.

4. După o conexiune reușită la Wi-Fi, pe dispozitivul client se va deschide automat o pagină web cu procesul de configurare pas cu pas a AP-ului. Această pagină e denumită **Quick Setup (Configurare rapidă)**. Dacă nu se deschide automat, atunci deschideți un browser și introduceți **http://ipcwifi.com** în bara de adrese pentru a vă conecta. Nu introduceți în câmpul de adresă al browserului, indiferent că folosiți un computer sau un telefon inteligent.




5. La primul pas trebuie să setați modul de conectare la rețeaua locală din amonte, fie prin Wi-Fi, fie prin Ethernet. Pentru mai multe detalii citiți subcapitolul următor 1.4 Setare mod conectare la rețeaua locală din amonte, prin Wi-Fi sau Ethernet, din configuratorul inițial pas cu pas. Apoi setați rețelele Wi-Fi emise de AP inclusiv setarea parolei de autentificare la interfața de gestionare.

**---Continuați cu secțiunea următoare**

Tip

Dacă pagina de configurare rapidă nu se deschide, atunci încercați următoarele soluții:

- Asigurați-vă că punctul de acces funcționează corect și că dispozitivul client este conectat la rețeaua Wi-Fi corectă.
- Când vă conectați folosind un telefon inteligent, asigurați-vă că rețeaua celulară (datele mobile) este dezactivată.
- Încercați să utilizați adresa IP pentru a vă conecta la interfața web de gestionare a punctului de acces.
  - Conectare cu o nouă adresă IP: Dacă punctul de acces (AP-ul) este conectat într-o rețea unde există un server DHCP (de regulă e un server DHCP pe ruterul din rețeaua locală), acesta poate primi automat o adresă IP nouă. Accesați interfața de gestionare a ruterului și identificați lista de dispozitive conectate, uneori denumită DHCP Client List. Căutați AP-ul în listă și notați adresa IP atribuită. Introduceți această adresă IP în browser pentru a accesa interfața web. Dacă nu reușiți să identificați adresa IP, încercați adresa implicită, astfel, accesați **http://192.168.0.254**. Se presupune că adaptorul de rețea al dispozitivului client (PC, laptop, telefon) este setat implicit pe obținerea automată a unei adrese IP (DHCP), conform configurației standard din majoritatea sistemelor de operare (Windows, macOS, Linux, Android, iOS).
  - Conectare cu **10.16.16.169:** În acest caz, setați manual pe telefon sau laptop o adresă IP din același subnet, de exemplu: **10.16.16.X (unde X** este între 1 și 254, dar diferit de 169 și neutilizat). Subnet mask: **255.255.255.0**. Nu este necesar un gateway. După configurare, deschideți browserul și accesați adresa: **http://10.16.16.169**. Această metodă este utilă în special pentru configurare inițială sau în situații în care dispozitivul nu este integrat într-o rețea locală existentă.
- Dacă în rețea există mai multe AP-uri IP-COM, este recomandat să le configurați pe rând, nu simultan. Conectați și accesați fiecare AP individual, apoi modificați adresa IP astfel încât fiecare AP să aibă o adresă IP unică. Acest lucru previne conflictele de IP și problemele de acces la interfața de gestionare.
- Ștergeți memoria cache a browserului sau folosiți un alt browser și încercați să vă conectați din nou.
- Resetați AP-ul și reîncercați.

# 1.4 Setare mod conectare la rețeaua locală din amonte, prin Wi-Fi sau cablu Ethernet, din configuratorul inițial

În configuratorul inițial pas cu pas, trebuie să stabiliți modul prin care echipamentul se conectează la rețeaua din amonte. Există două variante: prin cablu Ethernet între AP și un switch sau ruter din amonte — mod de lucru denumit **Access Point** sau denumit **AP**, sau prin Wi-Fi, conectând AP-ul la rețeaua Wi-Fi emisă de un alt ruter Wi-Fi sau punct de acces — mod de lucru denumit **Bridge** sau denumit alternativ în interfață ca **Client+AP**. După ce accesați pagina de configurare rapidă, puteți seta modul de lucru și parametrii wireless.

În ambele moduri de lucru se accesează o rețea locală (LAN), redirecționarea făcându-se pe baza adreselor MAC, exact ca un switch. Iar internetul e partajat efectiv de un ruter sau gateway din rețeaua locală (LAN), nu de echipamentul IP-COM.

Tip

Ulterior, după finalizarea configuratorului inițial pas cu pas, vă puteți conecta la interfața web de gestionare a punctului de acces și:

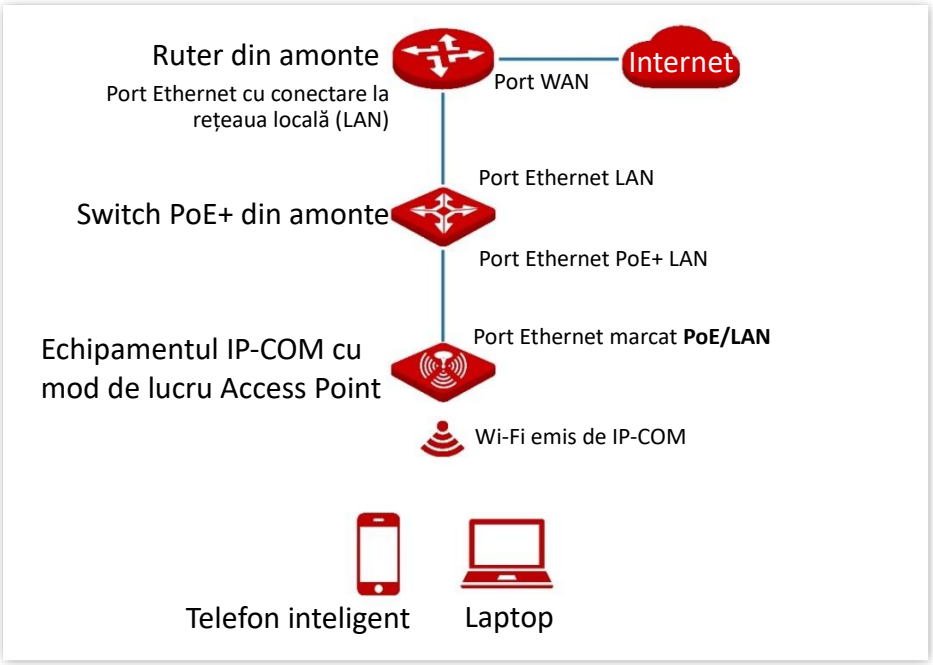
- Puteți naviga la meniul **Quick Setup (Configurare rapidă)** pentru a modifica modul de lucru al echipamentului.
- Dacă nu puteți detecta rețeaua Wi-Fi a dispozitivului din amonte atunci când modul de funcționare al punctului de acces este setat pe modul **Bridge** (sau **Client+AP),** atunci navigați la **Wireless** > **RF Settings (Setări RF),** asigurați-vă că este activată opțiunea **Wireless Network (Rețea wireless)** pentru banda de frecvență corespunzătoare (din filele **2,4 GHz** sau **5 GHz**) și încercați din nou.

## 1.4.1 Conectare prin cablu Ethernet la rețeaua din amonte

În modul de lucru **Access Point** (sau denumit **AP**) punctul de acces se conectează la rețeaua din amonte prin cablu Ethernet. Schema de mai jos ilustrează echipamentul IP-COM conectat direct la un switch PoE+, fără injectorul PoE inclus în pachet.

Alternativ, poate fi folosit injectorul PoE din pachet, astfel:

- Conectați AP-ul la portul marcat **AP** de pe injector.
- Conectați celălalt port (marcat **Switch**) al injectorului la un switch obișnuit sau direct la ruter.
- Alimentați injectorul de la priză, prin adaptorul de curent inclus.

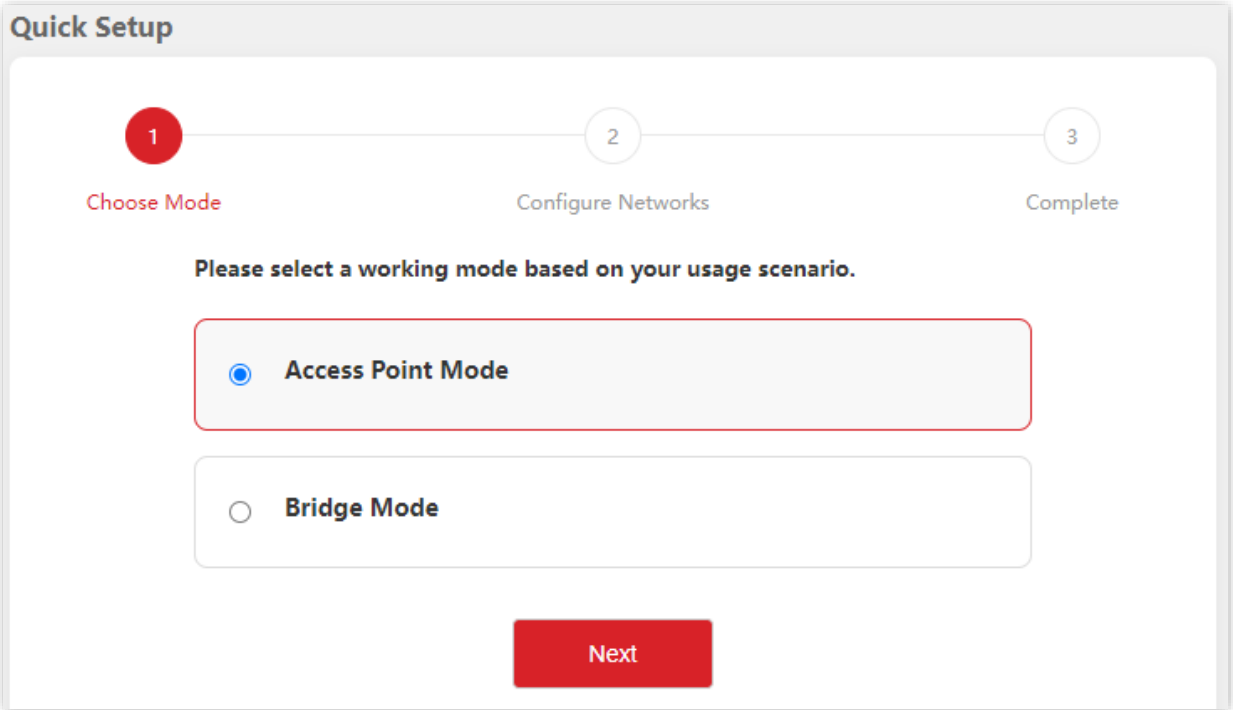



**Procedură pentru configurarea modului de lucru Access Point**

Tip

Asigurați-vă că prin echipamentul din amonte se poate accesa rețeaua locală și internetul.

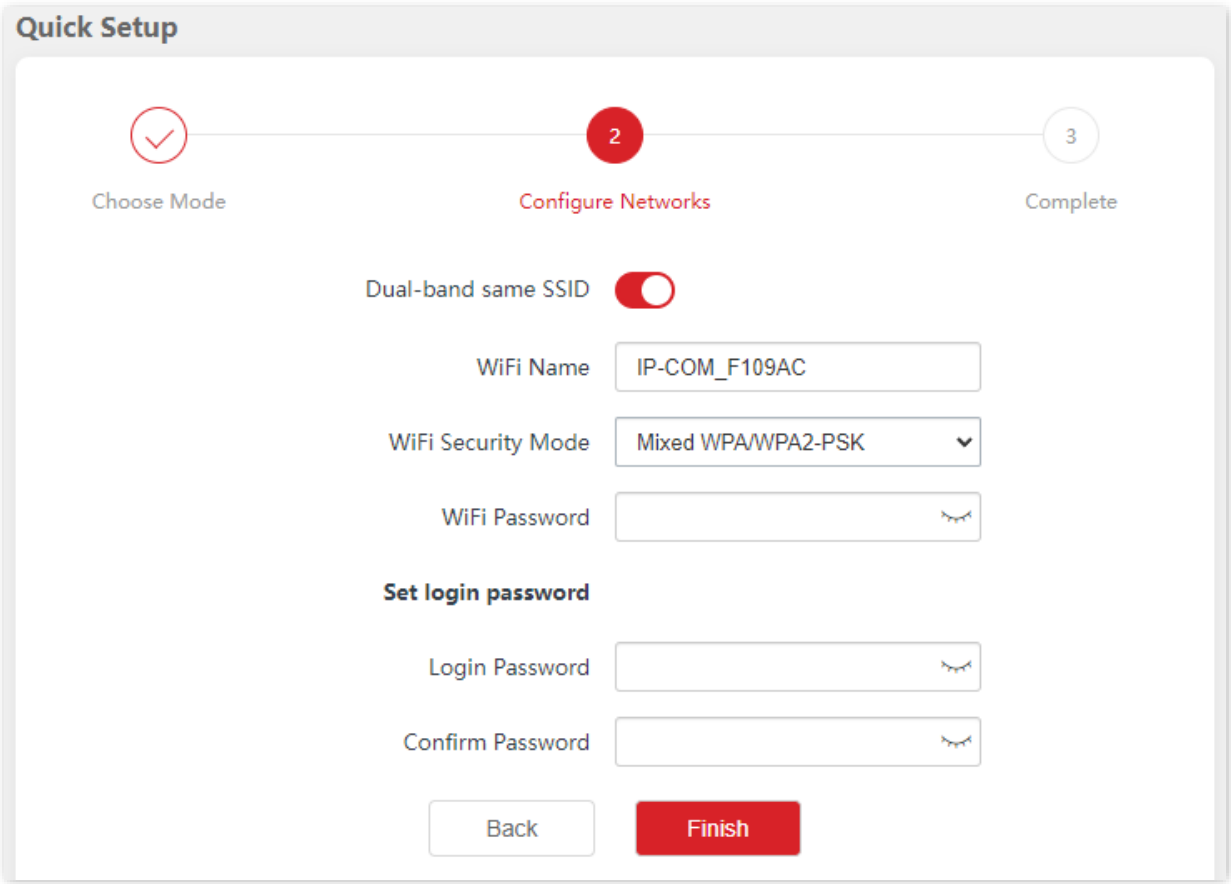
1. La pasul **1** din configuratorul pas cu pas, setați modul de funcționare al punctului de acces la **Access Point Mode (Mod AP)** și faceți clic pe **Next (Următorul).**




2. La pasul **2**, activați sau dezactivați **Dual-band same SSID (Același SSID pe ambele benzi)** după cum e explicat mai jos. Următoarea figură exemplificatoare prezintă această funcție activă.

- Activare **Dual-band same SSID (Același SSID pe ambele benzi):** Numele, parola Wi-Fi și modul de securitate sunt identice pentru ambele benzi, 2,4 GHz și 5 GHz, astfel încât rețeaua apare sub un singur nume. Când vă conectați la această rețea, se comută automat pe banda cu cel mai bun semnal pentru client. A se reține că opțiunea se aplică unui singur SSID — primul din listă pe fiecare bandă. Acest echipament profesional poate emite simultan mai multe rețele Wi-Fi cu SSID-uri distincte, iar restul rețelelor rămân independente pe fiecare bandă. Pentru a vedea lista de SSID-uri pe fiecare bandă puteți accesa meniul **Wireless > SSID**, după finalizarea acestui proces.
- Dezactivare **Dual-band same SSID (Același SSID pe ambele benzi):** Rețelele Wi-Fi sunt separate, diferite pe fiecare bandă, 2,4 GHz și 5 GHz. Va apărea un câmp separat pe fiecare bandă, pentru denumire Wi-Fi, parolă Wi-Fi dar și protocoalele de securitate Wi-Fi permise. A se reține că opțiunea se aplică unui singur SSID — primul din listă pe fiecare bandă. Acest echipament profesional poate emite simultan mai multe rețele Wi-Fi cu SSID-uri distincte. Pentru a vedea lista de SSID-uri pe fiecare bandă puteți accesa meniul **Wireless > SSID**, după finalizarea acestui proces.

3. Apoi, introduceți pentru rețeaua Wi-Fi principală emisă de punctul de acces, denumirea rețelei (SSID) la **WiFi Name (Nume Wi-Fi)**, selectați protocoalele de securitate Wi-Fi permise de la WiFi Security Mode și parola rețelei la **WiFi Password (Parolă Wi-Fi)** parametri specifici, după cum este necesar.



4. Mai jos în aceeași fereastră de la pasul **2**, setați parola de autentificare la interfața locală web a echipamentului, adică accesul la această interfață explicată în acest manual. Introduceți aceeași parolă la **Login Password (Parolă autentificare)** și la **Confirm Password (Confirmare parolă)**.

Note

- La prima configurare sau după o resetare la setările din fabrică, alegeți parole noi atât pentru rețeaua Wi-Fi, cât și pentru accesul la interfața web — pentru confidențialitate și securitate. Cu cât parola este mai lungă, cu atât protecția este mai puternică. Lungimea minimă și caracterele permise sunt indicate în mesajele și sfaturile din interfața web, în momentul introducerii.

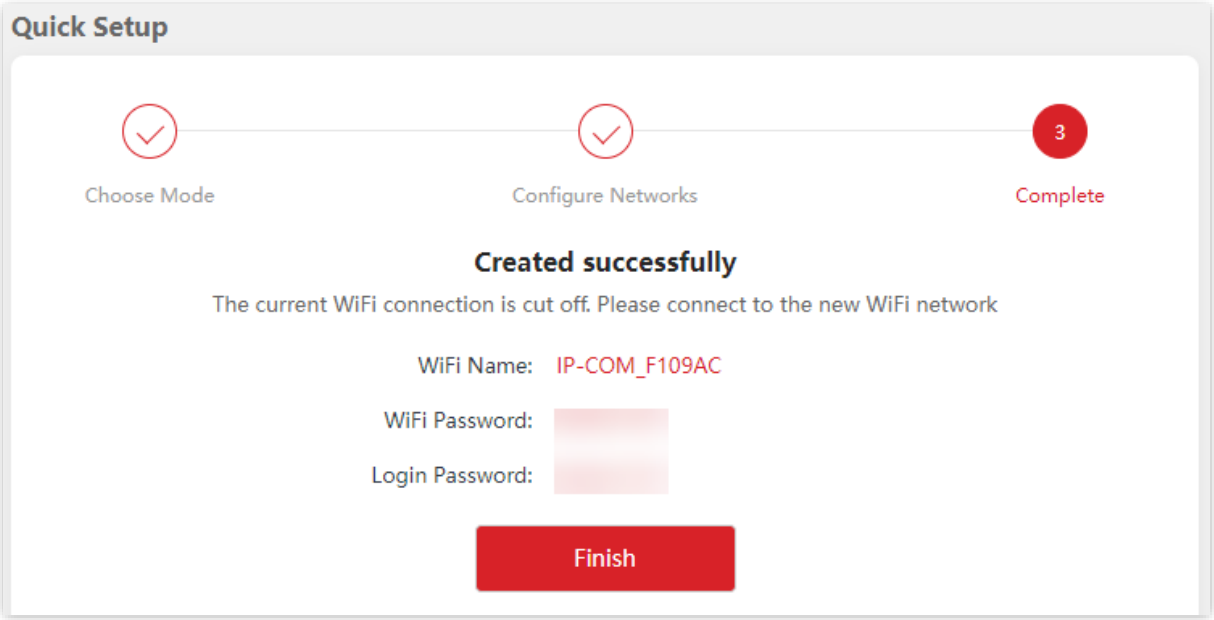
5. Faceți clic pe **Finish (Finalizare)**. În funcție de versiunea de firmware, o bară de progres va fi afișată. Așteptați.

6. La pasul **3**, în funcție de versiunea de firmware, puteți vedea denumirile Wi-Fi și parolele în clar. Apăsați **Finish (Finalizare)**.

7. După finalizarea configurării, puteți utiliza dispozitive compatibile Wi-Fi (cum ar fi telefonul inteligent sau tableta) pentru a vă reconecta la punctul de acces Wi-Fi pe care l-ați configurat pentru accesarea rețelei locale și implicit a internetului partajat de un ruter din rețea.

Tip

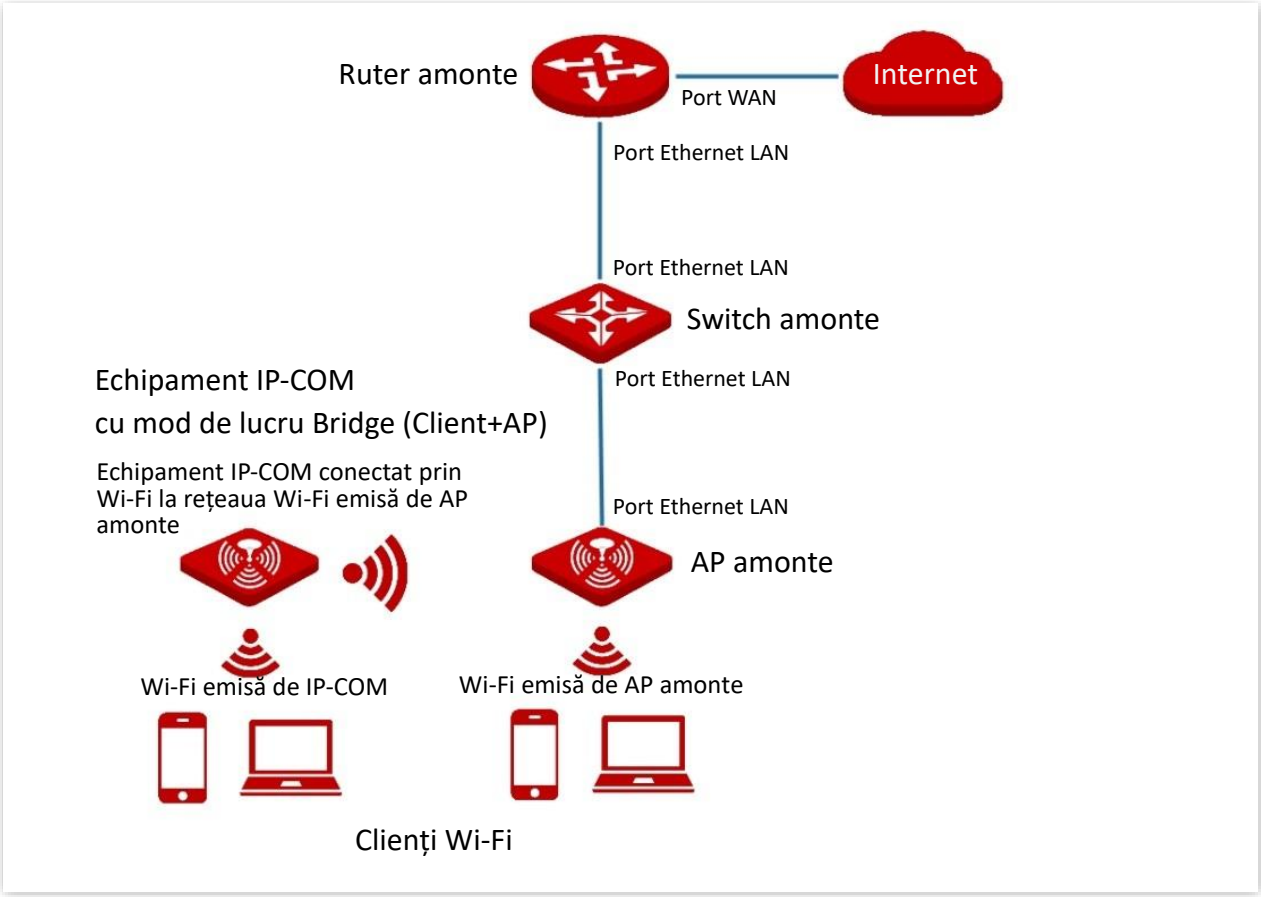
Conectați-vă la interfața web de gestionare a punctului de acces și navigați la **Wireless** > **SSID** pentru a accesa pagina unde puteți vizualiza numele Wi-Fi (SSID), parola Wi-Fi (cheia), protocoalele de securitate Wi-Fi permise dar și alte setări avansate.




**---Sfârșit**

## 1.4.2 Conectare prin Wi-Fi la rețeaua din amonte

În modul de lucru **Bridge** (sau sub denumirea **Client+AP**), punctul de acces este conectat prin Wi-Fi la o altă rețea Wi-Fi emisă de un echipament din rețeaua locală din amonte, cum ar fi un punct de acces ca în figura următoare. Echipamentul IP-COM e alimentat prin PoE.

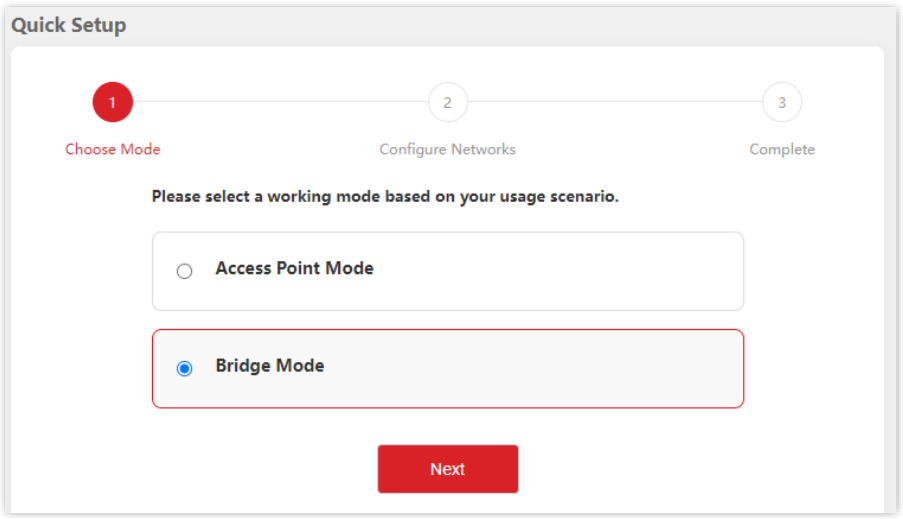



**Procedură pentru configurarea modului Bridge**

Tip

Asigurați-vă că prin echipamentul din amonte se poate accesa rețeaua locală și internetul.

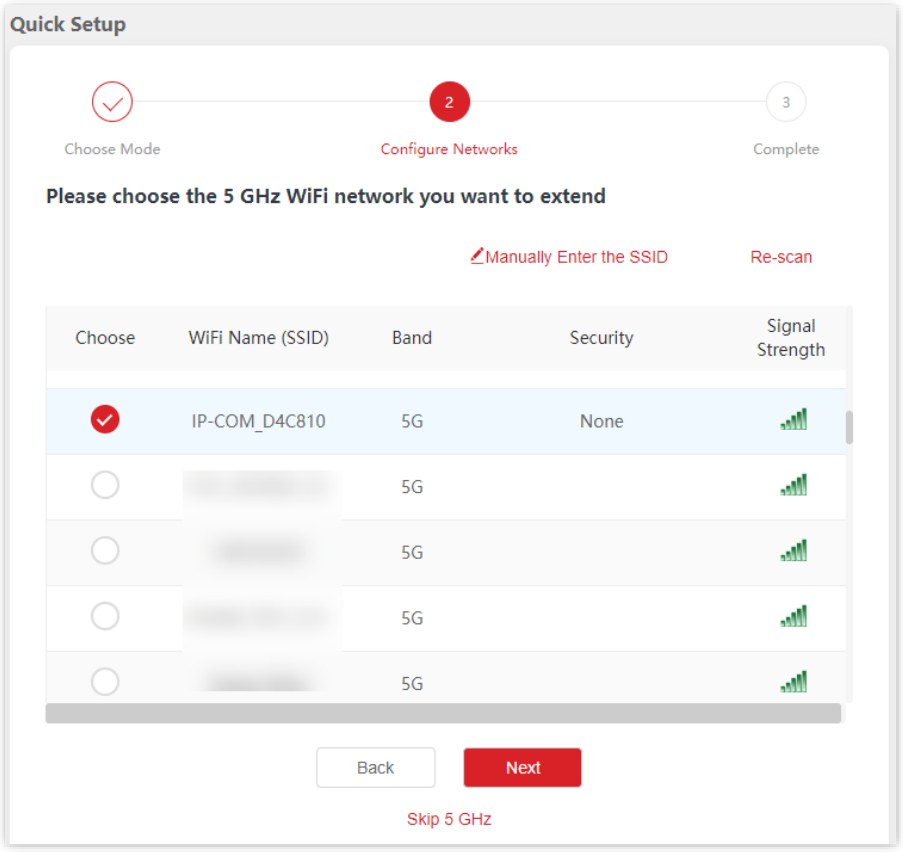
1. Setați modul de funcționare al punctului de acces la **Bridge Mode (Mod Bridge)** și faceți clic pe **Next (Următorul).**




2. La pasul **2** se va cere să vă conectați la rețeaua Wi-Fi emisă de echipamentul din amonte. O să fie afișate rețele Wi-Fi care emit pe **5 GHz**. Alternativ, apăsați butonul de jos **Skip 5 GHz (Omitere 5 GHz)** dacă doriți conectarea la rețeaua din amonte pe 2,4 GHz. Selectați rețeaua Wi-Fi din amonte. Dacă are o parolă, introduceți parola acesteia la câmpul **Security (Securitate)**. Apoi faceți clic pe **Next (Următorul).** Așteptați conectarea.

Tip

Dacă rețeaua Wi-Fi din amonte emite doar pe banda de 2,4 GHz, sau dacă doriți ca echipamentul IP-COM să se conecteze la rețeaua din amonte numai pe banda de 2,4 GHz, atunci apăsați butonul **Skip 5 GHz (Omitere 5 GHz)** din partea de jos a paginii.



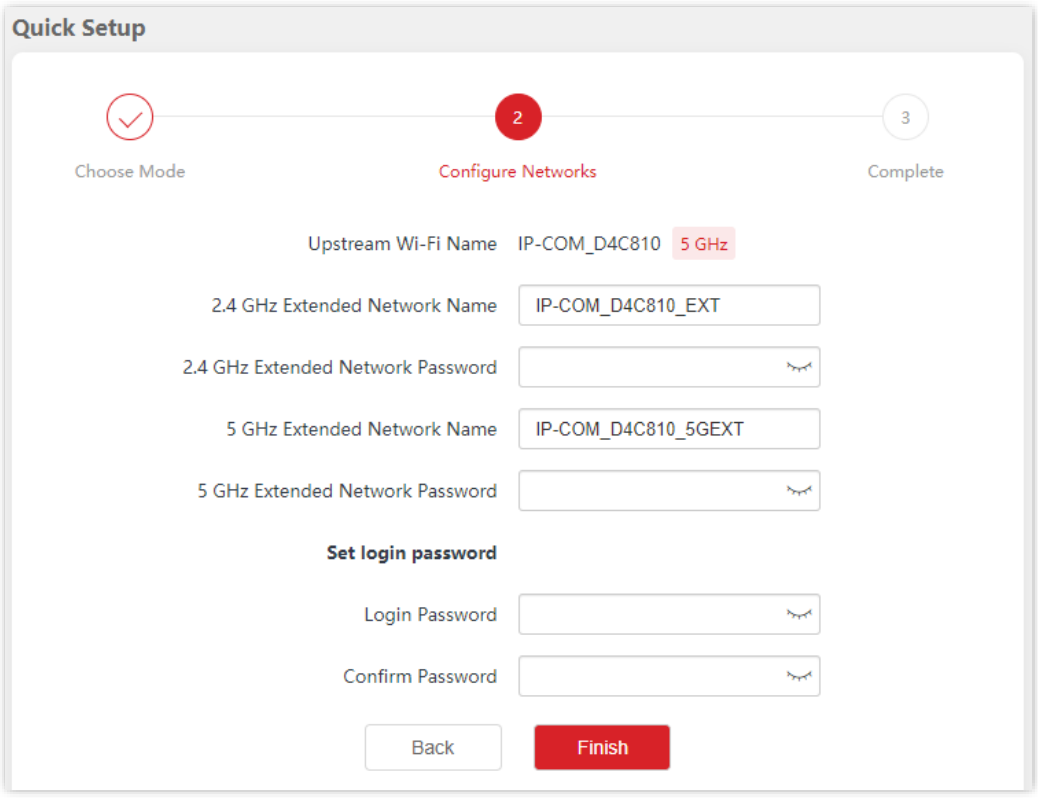
3. Apoi, în următoarea fereastră după o conectare reușită la o rețea Wi-Fi din amonte, fie pe 5 GHz, fie pe 2,4 GHz, o să vedeți la câmpul **Upstream Wi-Fi Name (Nume Wi-Fi amonte)** rețeaua la care echipamentul IP-COM s-a conectat.

4. La câmpurile **2,4 GHz Extended Network Name (Nume Wi-Fi 2,4 GHz emisă)**, **5 GHz Extended Network Name (Nume Wi-Fi 5 GHz emisă)** sunt denumirile rețelelor Wi-Fi emise de echipamentul IP-COM, la care clienții se vor conecta. Și, bineînțeles, parolele Wi-Fi corespondente la câmpurile **2,4 GHz Extended Network Password (Parolă Wi-Fi 2,4 GHz emisă)** și **5 GHz Extended Network Password (Parolă Wi-Fi 5 GHz emisă)**.

   Se observă că inițial parolele rețelelor Wi-Fi emise de echipamentul IP-COM sunt identice cu parola rețelei din amonte, iar denumirile acestora preiau ca prefix numele rețelei Wi-Fi din amonte, urmat de sufixul **_EXT** pentru banda de 2,4 GHz și **_5GEXT** pentru banda de 5 GHz. Toate acestea pot fi modificate.

5. Mai jos în aceeași fereastră setați parola de autentificare la interfața web de gestionare a echipamentului IP-COM. Introduceți aceeași parolă la **Login Password (Parolă autentificare)** și la **Confirm Password (Confirmare parolă)**.

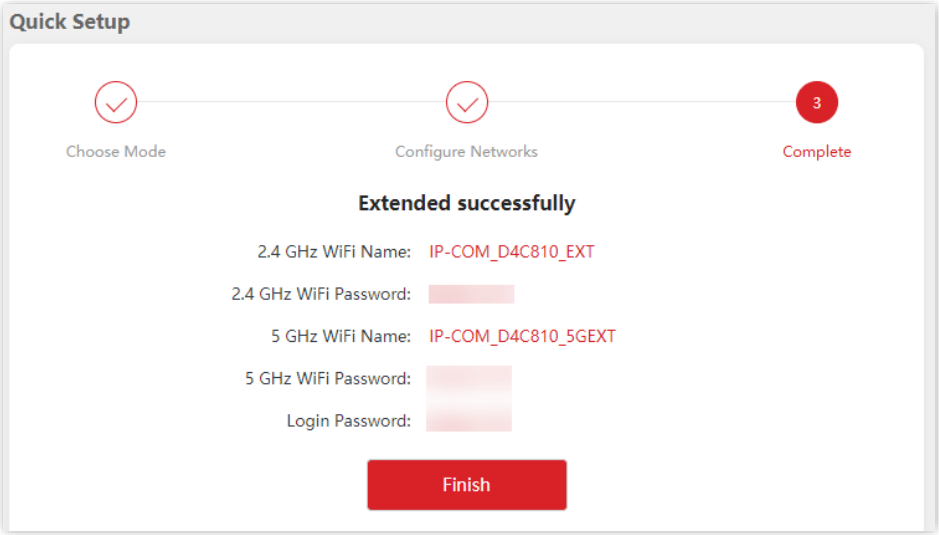
6. Faceți clic pe **Finish (Finalizare)**. Așteptați finalizarea procesului.




7. După finalizarea configurării o să vedeți denumirile Wi-Fi și parolele în clar, inclusiv parola de autentificare la interfața web de gestionare. Reconectați dispozitivele client la noile rețele emise de echipamentul IP-COM.

Tip

Conectați-vă la interfața web de gestionare a punctului de acces și navigați la **Wireless** > **SSID** pentru a accesa pagina unde puteți vizualiza numele Wi-Fi (SSID), parola Wi-Fi (cheia), protocoalele de securitate Wi-Fi permise dar și alte setări avansate.




**---Sfârșit**

# 2 Acces interfață web gestionare, după configurarea inițială

Funcțiile pot varia în funcție de model și de versiunea software instalată. Imaginile, pașii și descrierile prezentate în acest manual au caracter orientativ și pot diferi de interfața sau funcționarea reală. În acest manual, denumirile meniurilor și ale opțiunilor sunt prezentate în limba engleză, iar echivalentul în limba română este indicat între paranteze. Manualul este adaptat utilizatorilor cunoscători de limba română.

## 2.1 Conectare la interfața web

Dacă configurați punctul de acces pentru prima dată sau l-ați restaurat la setările din fabrică și punctul de acces nu este gestionat de niciun controler de AP-uri precum un ruter multi-WAN IP-COM sau de o platformă cloud precum **IP-COM ProFi Cloud**, atunci consultați secțiunea 1.3 Configurarea inițială din interfața locală web, din capitolul anterior.

Dacă punctul de acces este deja configurat și doriți doar să accesați interfața web locală de gestionare, urmați instrucțiunile de aici.

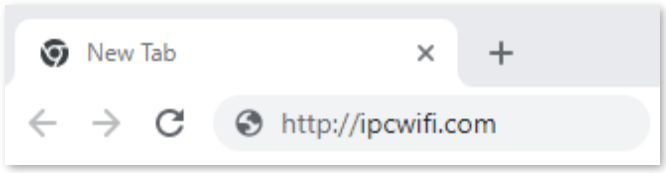
**Procedură pentru conectarea la Interfața web de gestionare a punctului de acces**

1. Conectați un dispozitiv compatibil Wi-Fi, cum ar fi un telefon inteligent sau un computer, la rețeaua Wi-Fi emisă de punctul de acces.

   Tip

   - Dacă punctul de acces este gestionat de un controler (inclusiv de un ruter cu funcții de gestionare a punctelor de acces, precum ruterele din seria M de la IP-COM) sau de o platformă cloud, precum **IP-COM ProFi Cloud**, conectați-vă la interfața web a controlerului ori la platforma cloud pentru a verifica numele și parola rețelei Wi-Fi emisă de acest punct de acces.

2. Porniți un browser și accesați **http://ipcwifi.com/** în bara de adrese pentru a vă conecta la interfața web a punctului de acces.

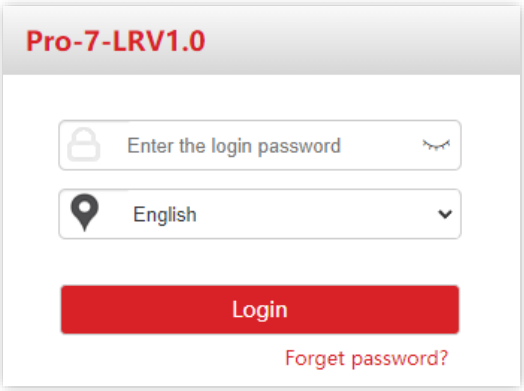



Puteți accesa interfața și folosind și IP-ul implicit al AP-ului http://192.168.0.254/ sau folosind IP-ul atribuit de un server DHCP din rețea sau folosind IP-ul secundar de gestionare http://10.16.16.169/.

Tip

- Încercați să utilizați adresa IP din rețeaua locală (LAN) a punctului de acces pentru a vă conecta la interfața web a acestuia, în loc de adresa **http://ipcwifi.com**.
  - **Metoda 1:** Dacă punctul de acces obține automat o adresă IP de la serverul DHCP din rețeaua locală, verificați mai întâi noua adresă IP alocată de serverul DHCP și folosiți-o pentru conectare. În caz contrar, accesați interfața web a punctului de acces tastând adresa implicită http://192.168.0.254/ în bara de adrese a browserului. Acest IP se poate seta și manual direct pe echipament din fila **LAN Setup (Configurare LAN)** din meniul **Internet Settings (Setări internet) > LAN Setup (Configurare LAN)**.
  - **Metoda 2**: Conectare prin IP-ul secundar de management **10.16.16.169**, accesând http://10.16.16.169/. Setați manual pe dispozitivul Wi-Fi (telefon sau laptop) o adresă IP din același segment de rețea ca punctul de acces, de forma **10.16.16.X** (unde **X** este un număr între **1** și **254**, neutilizat de un alt dispozitiv din rețea). Aceasta este o adresă IP secundară, care permite accesul la interfața web și printr-un IP alternativ și se poate modifica din fila **Management IP (IP de gestionare)** din meniul **Internet Settings (Setări internet) > LAN Setup (Configurare LAN)**.
- Dacă în rețea există două sau mai multe puncte de acces neconfigurate, toate vor avea inițial aceeași adresă IP implicită, ceea ce generează un conflict. Pentru a evita acest lucru, conectați-vă pe rând la fiecare punct de acces și modificați-i adresa IP, astfel încât fiecare să aibă o adresă IP unică în rețea. Inclusiv pentru IP-ul de la **Management IP (IP de gestionare)** dar și IP-ul de la **LAN Setup (Configurare LAN)**, din meniul **Internet Settings (Setări internet) > LAN Setup (Configurare LAN)**.
- Dacă funcția **QVLAN** este activată din **Wireless > QVLAN Settings (Setări QVLAN)**, conectarea la interfața de gestionare se poate face numai dintr-o rețea Wi-Fi al cărei **VLAN ID** coincide cu cel din câmpul **Management VLAN (VLAN gestionare)** sau printr-un cablu Ethernet conectat la un port al cărui VLAN membru corespunde aceluiași VLAN de gestionare. În caz contrar, dispozitivul nu va fi accesibil prin browser. ID-urile VLAN pentru rețelele Wi-Fi (SSID) emise de echipament se configurează tot din meniul **Wireless > QVLAN Settings (Setări QVLAN).**
- Dacă nu puteți accesa interfața web, atunci ștergeți memoria cache a browserului sau folosiți un alt browser și încercați să vă conectați din nou.
- Dacă nu puteți accesa interfața web, atunci resetați AP-ul la setările din fabrică și reconfigurați.
- Asigurați-vă că punctul de acces funcționează corect și că dispozitivul client este conectat la rețeaua Wi-Fi corectă.
- Când vă conectați folosind un telefon inteligent, asigurați-vă că datele mobile sunt dezactivate.

3. Introduceți parola de autentificare la interfața de gestionare și faceți clic pe **Login (Autentificare).**

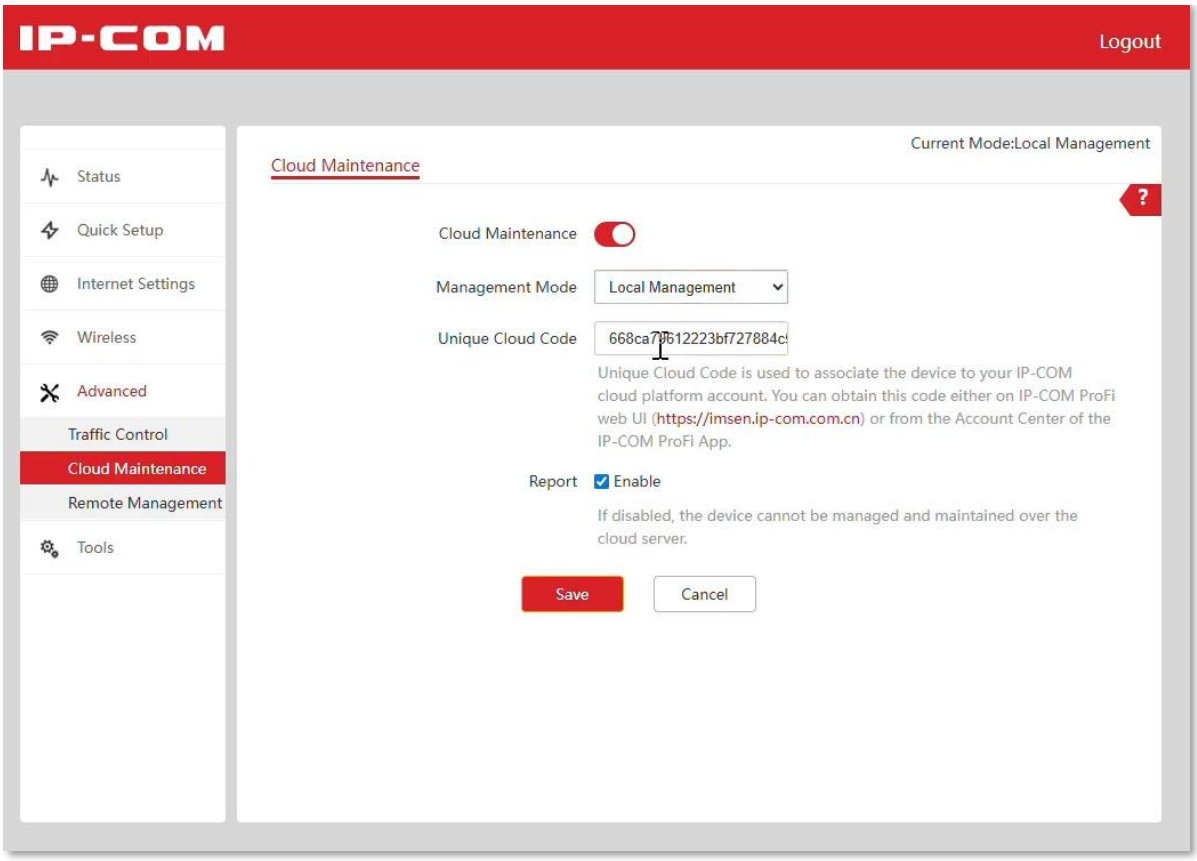



4. După conectarea la interfața web a punctului de acces, modul de gestionare al fiecărui AP poate fi schimbat individual din meniul **Advanced (Avansat) >** Cloud Maintenance (Mentenanță cloud), de la opțiunea **Management Mode (Mod gestionare)**, alegând **Local Management (Gestionare locală)** sau **Cloud Management (Gestionare cloud)**, urmat de **Save (Salvare)**.

   Modul activ este afișat și în colțul din dreapta-sus la **Current Mode (Mod curent)**, astfel:

   – Când este afișat **Cloud Management (Gestionare cloud)**, opțiunile granulare și avansate dispar din interfața locală a AP-ului, acesta fiind gestionat din **IP-COM ProFi Cloud**, dacă a fost adoptat în acest serviciu, bineînțeles.

   – Când este afișat **Local Management (Gestionare locală)** toate setările avansate redevin disponibile, și acesta poate fi gestionat și de un controler de AP-uri, precum un ruter multi-WAN seria M de la IP-COM. În imaginea următoare e activ acest mod.



## 2.2 Deconectare din interfața web

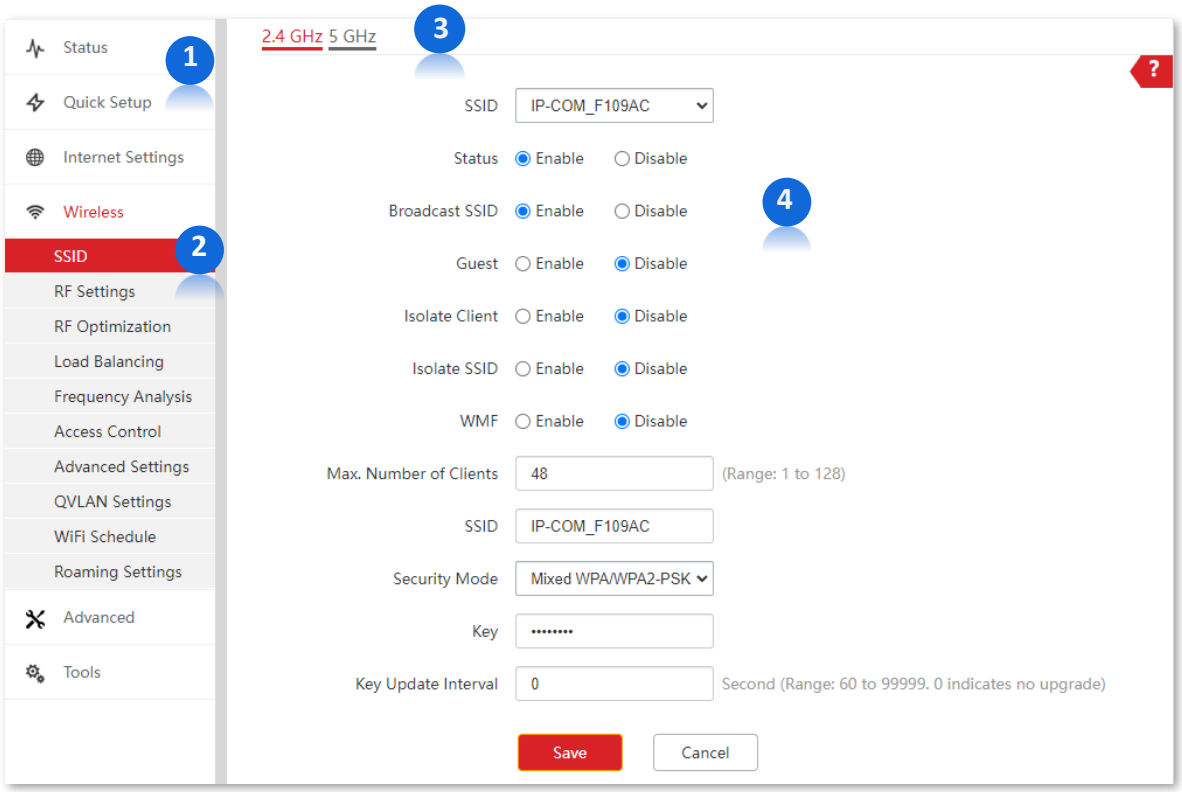
După conectarea la interfața web de gestionare, dacă nu se efectuează nicio operațiune în intervalul de timp setat la **Login Timeout Interval (Interval expirare autentificare)** din meniul **Tools (Instrumente)** > **Date & Time (Dată și oră)**, atunci sistemul se va deconecta automat. Intervalul implicit de deconectare e de 5 minute, dar poate fi modificat între 1 și 60 de minute.

În plus, puteți face clic pe **Logout (Deconectare)** în colțul din dreapta sus pentru a ieși în siguranță din interfața web.

După deconectare trebuie să introduceți din nou parola de autentificare la interfața de gestionare.

## 2.3 Aspect interfață web

Interfața web este compusă din patru părți: bara de navigare principală laterală cu meniurile principale (1) și submeniurile (2), filele (3) și zona (4) cu funcțiile pentru configurare. Următoarea figură este doar pentru exemplificare.




Tip

Opțiunile, câmpurile sau butoanele afișate cu text gri (estompat) în interfața web sunt indisponibile în contextul curent — fie funcția corespunzătoare nu este activată, fie depind de alte setări care nu sunt încă configurate, fie nu pot fi modificate în modul de funcționare ales. Pentru a le activa, verificați dacă funcția-părinte este pornită și dacă sunt îndeplinite condițiile prealabile (de exemplu, activarea unei opțiuni superioare).

| Nu. | Nume | Descriere |
|---|---|---|
| 1 | Bară laterală de navigare cu meniurile principale de nivel I | Structură de meniuri pentru a ajunge la funcția dorită a fi configurată. |
| 2 | Submeniuri de nivel II de pe bara laterală principală | |
| 3 | Submeniuri de nivel III sub formă de file (taburi) | |
| 4 | Zona de configurare | Zona în care efectuați sau verificați configurațiile, setările efective. |

## 2.4 Butoane comune găsite în interfața web

Butoanele găsite în mod curent în interfața web sunt ilustrate mai jos.

| Buton comun | Descriere |
|---|---|
| Refresh | Butonul **Refresh (Reîmprospătare)** e utilizat pentru reîmprospătarea paginii de setări. Uneori AP-ul poate fi modificat în același timp din cloud sau de un ruter cu control de AP-uri și pentru a vedea ultimele modificări e nevoie a fi apăsat acest buton. |
| Save | Butonul **Save (Salvare)** e utilizat pentru salvarea configurațiilor de pe pagina curentă și a face ca acestea să aibă efect. |
| Cancel | Butonul **Cancel (Anulare)** anulează configurațiile nesalvate de pe pagina curentă și restaurează configurațiile anterioare. |
| ? | Butonul sub forma unui semn de întrebare, **?**, va afișa într-o nouă pagină informații concise despre opțiunile, funcțiile și valorile permise din submeniul curent. Apăsând acest buton găsiți mai rapid informații despre diverse funcții din pagina curentă, aducând o economie de timp majoră; însă se recomandă și parcurgerea manualului. |

## 2.5 Schimbare limbă interfață web

Pentru a schimba limba interfeței web, în pagina de autentificare, faceți clic pe meniul derulant, situat sub câmpul de parolă, afișând implicit **English** și selectați din listă limba dorită, după care introduceți parola și apăsați butonul **Login (Autentificare)** pentru a accesa interfața de administrare în limba aleasă.

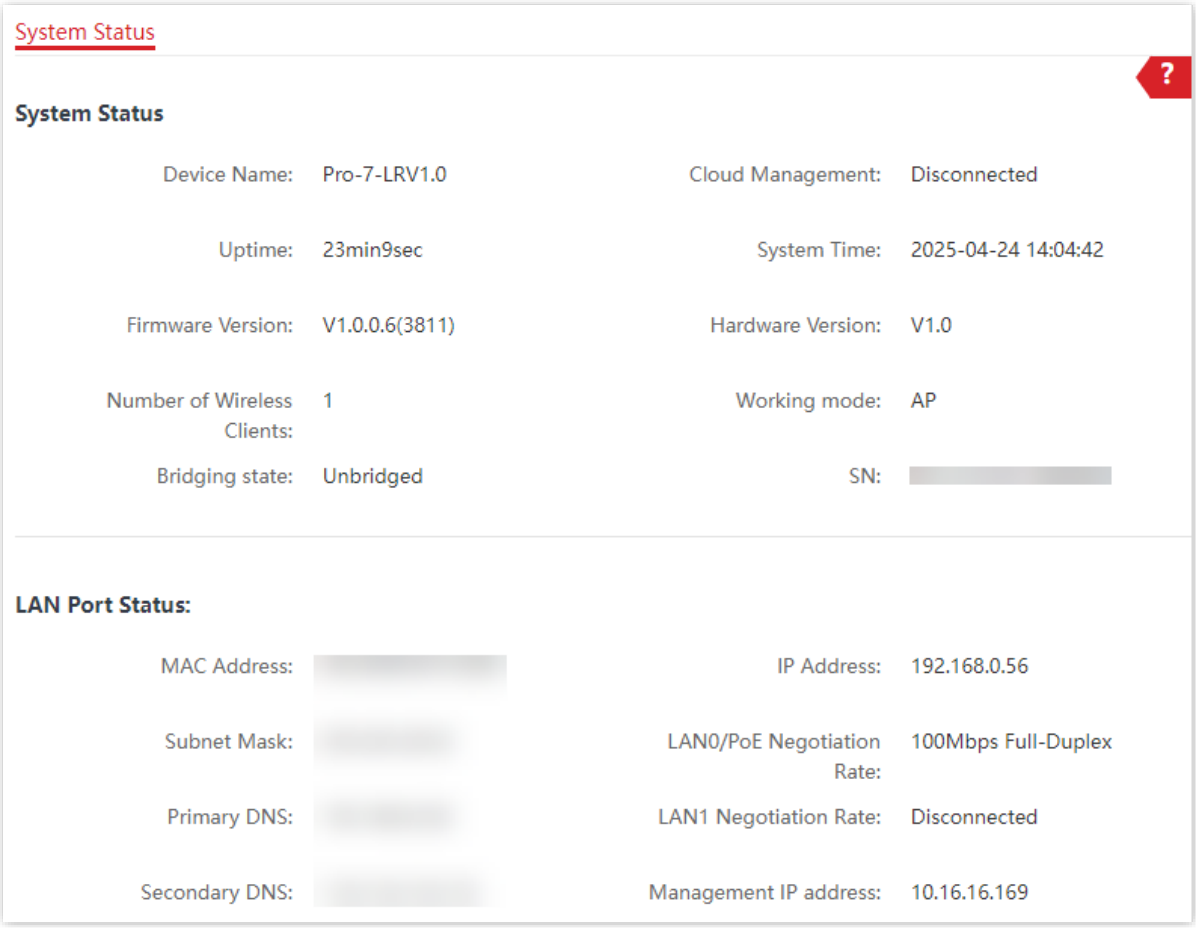
# 3 Meniul Status (Stare)

Funcțiile pot varia în funcție de model și de versiunea software instalată. Imaginile, pașii și descrierile prezentate în acest manual au caracter orientativ și pot diferi de interfața sau funcționarea reală. În acest manual, denumirile meniurilor și ale opțiunilor sunt prezentate în limba engleză, iar echivalentul în limba română este indicat între paranteze. Manualul este adaptat utilizatorilor cunoscători de limba română.

## 3.1 Submeniul System Status (Stare sistem)

Pentru a accesa informațiile de la **System Status (Stare sistem)**, conectați-vă la interfața web a punctului de acces și navigați la **Status (Stare)** > **System Status (Stare sistem).**

În această secțiune puteți consulta informațiile generale despre echipament și starea sa de funcționare, precum și starea porturilor Ethernet și datele aferente acestora. Aceste informații sunt utile atunci când e nevoie să depanați echipamentul și să trimiteți informații echipei de suport tehnic **IP-COM**. Figura de mai jos este prezentată doar cu titlu de exemplu.



### Descriere parametri Status (Stare) > System Status (Stare sistem)

| Parametru | | Descriere |
|---|---|---|
| Secțiune<br>**System Status (Stare sistem)** | **Device Name**<br>**(Nume dispozitiv)** | Specifică numele punctului de acces. Puteți schimba numele echipamentului din fila **LAN Setup (Configurare LAN)** de la meniul **Internet Settings (Setări internet) > LAN Setup (Configurare LAN)**.<br>Se recomandă să schimbați numele punctului de acces pentru a indica locația acestuia, astfel încât să puteți identifica cu ușurință pe teren echipamentul când gestionați mai multe puncte de acces.<br>Această denumire e și cea afișată în rețeaua logică. |
| | **Cloud Management (Gestionare cloud)** | Specifică starea conexiunii dintre punctul de acces și platforma de gestionare unificată din cloud **IP-COM ProFi Cloud**. |
| | **Uptime**<br>**(Timp funcționare)** | Specifică timpul scurs de la pornirea echipamentului. |
| | **System Time**<br>**(Timp sistem)** | Specifică data și ora setată pe echipament. |
| | **Firmware Version (Versiune firmware)** | Specifică versiunea de firmware a echipamentului. |
| | **Hardware Version (Versiune hardware)** | Specifică versiunea hardware a echipamentului.<br>Când căutați manual o nouă versiune de firmware pe pagina https://www.ip-com.com.cn/ro/ este important să cunoașteți versiunea hardware a echipamentului, de obicei notată cu v1.0, v2.0 etc. |
| | **Number of Wireless Clients**<br>**(Număr clienți wireless)** | Specifică numărul de clienți conectați prin punctul de acces. |
| | **Working mode**<br>**(Mod de lucru)** | Specifică modul de lucru al punctului de acces, care poate fi **AP** (sau cunoscut ca **Access Point**) sau **Client+AP** (sau cunoscut ca **Bridge**), moduri de lucru ce pot fi schimbate din meniul **Quick Setup (Configurare rapidă)**. |
| | **Bridging state**<br>**(Stare conexiune Wi-Fi amonte)** | Specifică starea de conectare la rețeaua Wi-Fi din amonte, dacă echipamentul e în modul de lucru **Client+AP** (sau **Bridge**). |

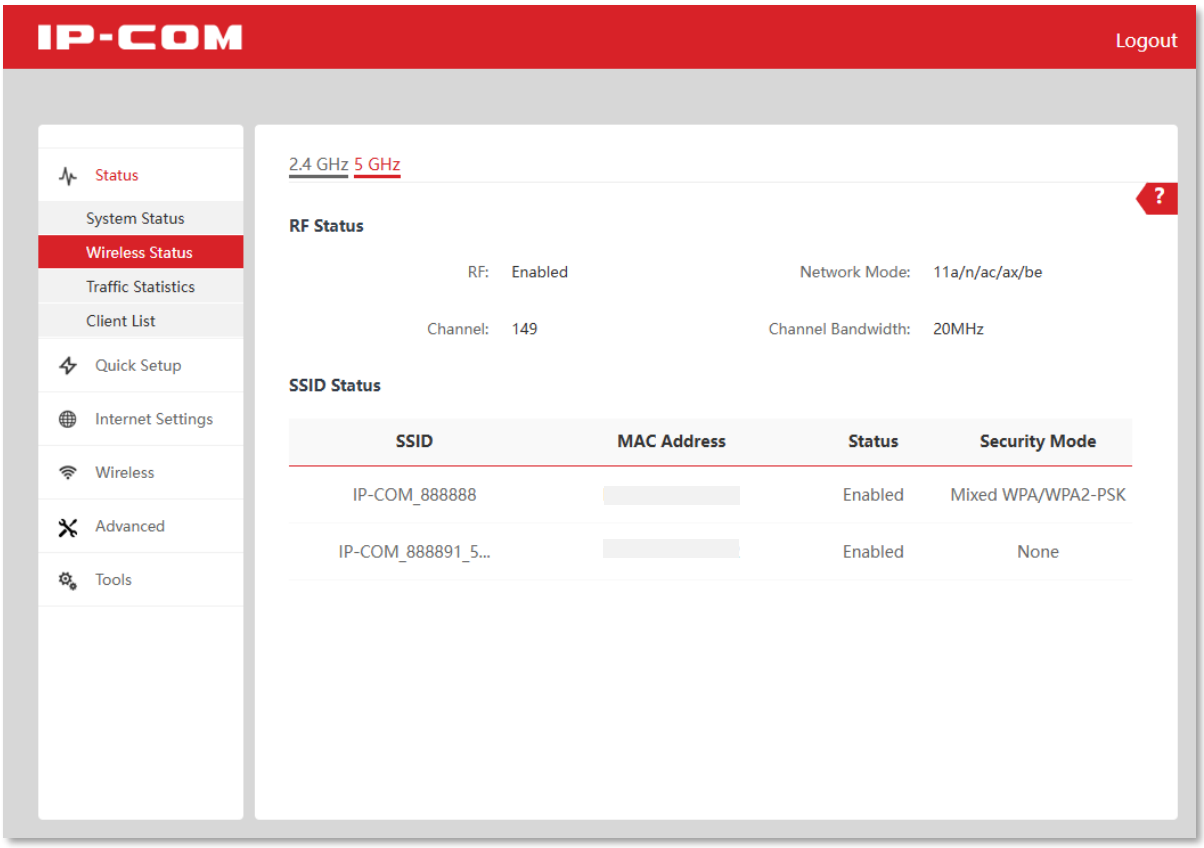
| Parametru | | Descriere |
|---|---|---|
| | **Bridging SSID**<br>**(SSID amonte)** | Specifică denumirea rețelei Wi-Fi (SSID-ul) emisă de dispozitivul din amonte, la care echipamentul IP-COM se conectează dacă e în modul de lucru **Client+AP** (sau cunoscut ca **Bridge**).<br><br>Tip<br><br>Această informație este disponibilă pe unele puncte de acces. Produsul real prevalează. |
| | **SN** | Specifică numărul de serie unic al echipamentului. |
| Secțiune<br>**LAN Port Status (Stare port LAN)** | **MAC Address**<br>**(Adresă MAC)** | Specifică identificatorul unic MAC de pe portul Ethernet. |
| | **IP Address**<br>**(Adresă IP)** | Indică adresa IP din rețeaua locală (LAN) a punctului de acces. Utilizatorii din rețeaua locală se pot conecta la interfața web de gestionare a punctului de acces folosind această adresă IP.<br><br>Această adresă IP este obținută în mod implicit de la serverul DHCP al rețelei locale (LAN). Dacă nu există un server DHCP în rețeaua locală unde se află punctul de acces, adresa IP implicită va fi **192.168.0.254**. Puteți schimba adresa IP din fila **LAN Setup (Configurare LAN)** de la meniul **Internet Settings (Setări internet) > LAN Setup (Configurare LAN)**.<br><br>Această adresă IP nu influențează conexiunile clienților conectați prin acest echipament, fie că sunt prin cablu Ethernet, fie că sunt prin Wi-Fi. Aceasta e folosită exclusiv pentru accesul la interfața web de gestionare, pentru accesul echipamentului la internet și comunicarea cu **IP-COM ProFi Cloud**. Indiferent de IP-ul configurat, echipamentul continuă să funcționeze ca un switch transparent pentru traficul clienților, transmiterea datelor între aceștia și restul rețelei făcându-se la nivel de Layer 2, conform modelului OSI.<br><br>Tip<br><br>– Înainte de a utiliza această adresă IP pentru a vă conecta la interfața web de gestionare a punctului de acces, asigurați-vă că adresa IP a dispozitivului client se află în aceeași subrețea ca și adresa IP a punctului de acces.<br>– Dacă funcția **QVLAN** este activată din **Wireless > QVLAN Settings (Setări QVLAN)**, conectarea la interfața de gestionare se poate face numai dintr-o rețea Wi-Fi al cărei **VLAN ID** coincide cu cel din câmpul **Management VLAN (VLAN gestionare)** sau printr-un cablu Ethernet conectat la un port al cărui VLAN membru corespunde aceluiași VLAN de gestionare. În caz contrar, dispozitivul nu va fi accesibil prin browser. ID-urile VLAN pentru rețelele Wi-Fi (SSID) emise de echipament se configurează tot din meniul **Wireless > QVLAN Settings (Setări QVLAN)**. |

| Parametru | | Descriere |
|---|---|---|
| | **Subnet Mask**<br><br>**(Mască subrețea)** | Indică masca de subrețea corespunzătoare adresei IP a portului LAN al punctului de acces.<br><br>Puteți schimba din fila **LAN Setup (Configurare LAN)** de la meniul **Internet Settings (Setări internet) > LAN Setup (Configurare LAN)**. |
| | **Primary DNS**<br><br>**(DNS principal)** | Indică adresa IP a serverului DNS principal al punctului de acces.<br><br>Puteți schimba din fila **LAN Setup (Configurare LAN)** de la meniul **Internet Settings (Setări internet) > LAN Setup (Configurare LAN)**. |
| | **Secondary DNS**<br><br>**(DNS secundar)** | Indică adresa IP a serverului DNS secundar al punctului de acces.<br><br>Puteți schimba din fila **LAN Setup (Configurare LAN)** de la meniul **Internet Settings (Setări internet) > LAN Setup (Configurare LAN)**. |
| | **LAN0/PoE Negotiation Rate (Rată negociere LAN0/PoE)** | Afișează modul de negociere și rata (viteza) maximă a legăturii Ethernet pe portul **LAN0/PoE** — același port fizic prin care punctul de acces primește alimentarea PoE și transmite datele către echipamentul din amonte (switch, ruter sau injector PoE).<br><br>De exemplu pot fi afișate valori precum **100 Mbps Full-Duplex, 1000 Mbps Full-Duplex** etc. |
| | **Management IP address**<br><br>**(Adresă IP de gestionare)** | Indică adresa IP secundară (alternativă) de accesare a interfeței de gestionare a echipamentului, pe lângă cea setată din fila **LAN Setup (Configurare LAN)**, din meniul **Internet Settings (Setări internet) > LAN Setup (Configurare LAN)**. Așadar, utilizatorii din rețeaua locală pot utiliza o adresă secundară de gestionare precum cea implicită **10.16.16.169**. Se poate modifica din fila **Management IP (IP de gestionare)** din meniul **Internet Settings (Setări internet) > LAN Setup (Configurare LAN)**.<br><br>Tip<br><br>– Înainte de a utiliza această adresă IP pentru a vă conecta la interfața web de gestionare a punctului de acces, asigurați-vă că adresa IP a dispozitivului client se află în aceeași subrețea ca și adresa IP a punctului de acces.<br><br>– Dacă funcția **QVLAN** este activată din **Wireless > QVLAN Settings (Setări QVLAN)**, conectarea la interfața de gestionare se poate face numai dintr-o rețea Wi-Fi al cărei **VLAN ID** coincide cu cel din câmpul **Management VLAN (VLAN gestionare)** sau printr-un cablu Ethernet conectat la un port al cărui VLAN membru corespunde aceluiași VLAN de gestionare. În caz contrar, dispozitivul nu va fi accesibil prin browser. ID-urile VLAN pentru rețelele Wi-Fi (SSID) emise de echipament se configurează tot din meniul **Wireless > QVLAN Settings (Setări QVLAN)**. |

# 3.2 Submeniul Wireless Status (Stare wireless)

Pentru a accesa informațiile de la **Wireless Status (Stare wireless)**, conectați-vă la interfața web a punctului de acces și navigați la **Status (Stare)** > **Wireless Status (Stare wireless)**.

Puteți vizualiza starea benzilor pe 2,4 GHz și 5 GHz și starea fiecărui SSID emis de echipament. În mod implicit este afișată fila **2,4 GHz** cu informații despre starea conexiunilor wireless pe banda de 2,4 GHz. Pentru a vizualiza starea conexiunilor wireless pe 5 GHz, faceți clic pe fila **5 GHz**.




**Descriere parametri Status (Stare) > Wireless Status (Stare wireless)**

| Parametru | | Descriere |
|---|---|---|
| Filele<br>**2,4 GHz**<br>și<br>**5 GHz** | | Apăsați fila **2,4 GHz** pentru informații despre starea conexiunilor wireless pe banda de 2,4 GHz.<br>Apăsați fila **5 GHz** pentru informații despre starea conexiunilor wireless pe banda de 5 GHz.<br>Opțiunile de mai jos pot fi diferite în funcție de fila apăsată. |
| Secțiune | **RF (Radiofrecvență)** | Indică dacă banda, fie că e 2,4 GHz, fie că e 5 GHz, e activă sau nu. |

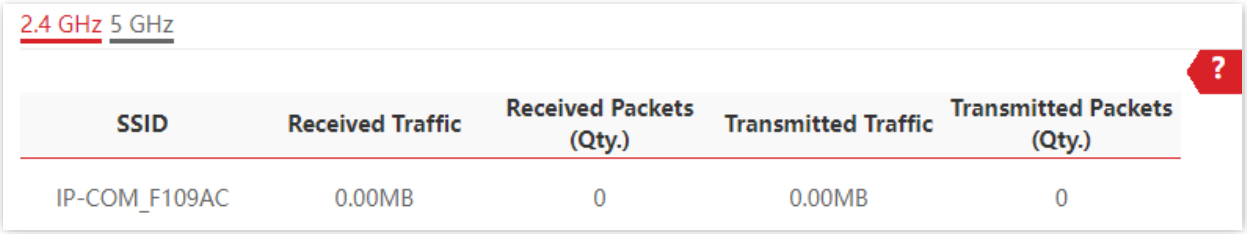
| Parametru | | Descriere |
|---|---|---|
| **RF Status (Stare radiofrecvență)** | **Network Mode (Mod rețea)** | Indică protocoalele Wi-Fi utilizate pe banda respectivă. Prefixul **11** e prescurtarea pentru IEEE 802.11, standardul care reglementează rețelele Wi-Fi.<br>Literele indică generațiile compatibile **b** — 802.11b, **g** — 802.11g, **n** — 802.11n (Wi-Fi 4), **ac** — 802.11ac (Wi-Fi 5), **ax** — 802.11ax (Wi-Fi 6), **be** — 802.11be (Wi-Fi 7).<br>Se aplică pentru toate SSID-urile din listă. |
| | **Channel (Canal)** | Indică numărul canalului din bandă pe care se emit.<br>Se aplică pentru toate SSID-urile din listă. |
| | **Channel Bandwidth (Lățime canal)** | Indică lățimea canalului radio, exprimată în **MHz**; aceasta nu trebuie confundată cu frecvența benzii pe care funcționează rețeaua Wi-Fi.<br>Se aplică pentru toate SSID-urile din listă. |
| Tabelul **SSID Status (Stare SSID)** | **SSID** | Se indică numele rețelelor Wi-Fi emise de echipamentul IP-COM.<br>Denumirile, activarea, dar și alte setări pentru aceste SSID-uri se face din meniul **Wireless > SSID**. |
| | **MAC Address (Adresă MAC)** | Specifică MAC-ul corespunzător unui SSID din listă. |
| | **Status (Stare)** | Specifică dacă sunt activate acele SSID-uri. |
| | **Security Mode (Mod securitate)** | Specifică protocoalele de securitate Wi-Fi standardizate setate pe fiecare SSID de la opțiunea **Security Mode (Mod securitate)** din meniul **Wireless > SSID.**<br>În funcție de modelul de echipament se afișează diverse moduri de securitate pentru criptarea Wi-Fi, precum WPA-PSK, **WPA2-PSK**, **WPA**, **WPA2**, **WPA3-SAE**, moduri mixte precum WPA-PSK **& WPA2-PSK, WPA/WPA2-PSK** și **WPA2-PSK & WPA3-SAE**, inclusiv fără parolă și criptare dacă e afișat **None (Fără)**.<br>Modurile de securitate pot diferi în funcție de modele și benzi radio. Prevalează produsul real. Vă rugăm să verificați specificațiile tehnice ale echipamentului sau contactați suportul tehnic IP-COM. |

# 3.3 Submeniul Traffic Statistics (Statistici trafic)

Pentru a accesa informațiile de la **Traffic Statistics (Statistici trafic)**, conectați-vă la interfața web a punctului de acces și navigați la **Status (Stare)** > **Traffic Statistics (Statistici trafic)**.

Puteți vizualiza statisticile pentru datele trimise și primite pe fiecare SSID.

În mod implicit, pagina afișează informații statistice despre traficul pe banda de 2,4 GHz. Pentru a vizualiza informații despre 5 GHz, faceți clic pe fila **5 GHz.**




**Descriere parametri Status (Stare) > Traffic Statistics (Statistici trafic)**

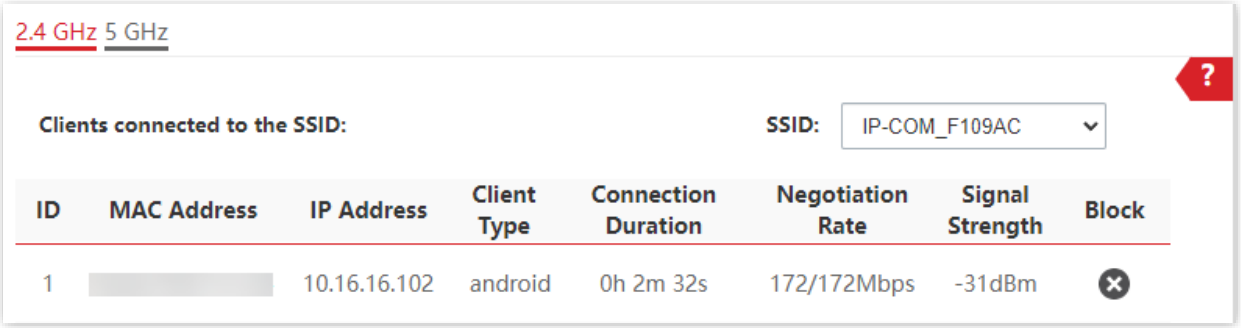
| Parametru | Descriere |
|---|---|
| Filele<br>**2,4 GHz**<br>și<br>**5 GHz** | Apăsați fila **2,4 GHz** pentru informații despre traficul wireless pe banda de 2,4 GHz.<br>Apăsați fila **5 GHz** pentru informații despre traficul wireless pe banda de 5 GHz. |
| SSID | Se indică numele rețelelor Wi-Fi emise de echipamentul IP-COM.<br>Denumirile, activarea, dar și alte setări pentru aceste SSID-uri se face din meniul **Wireless > SSID.** |
| **Received Traffic**<br>**(Trafic primit)** | Specifică numărul total de octeți primiți de o rețea Wi-Fi (SSID). |
| **Received Packets (Qty.)**<br>**(Pachete primite (cantitate))** | Specifică numărul total de pachete primite de o rețea Wi-Fi. |
| **Transmitted Traffic**<br>**(Trafic trimis)** | Specifică numărul total de octeți transmiși de o rețea Wi-Fi (SSID). |
| **Transmitted Packets (Qty.)**<br>**(Pachete transmise (cantitate))** | Specifică numărul total de pachete transmise de o rețea Wi-Fi (SSID). |

Note

- Toate statisticile sunt șterse când funcția wireless este dezactivată sau AP-ul este repornit.
- Toate statisticile unui SSID sunt șterse atunci când SSID-ul este dezactivat.

# 3.4 Submeniul Client List (Listă clienți)

Pentru a accesa informațiile despre clienții conectați prin rețelele Wi-Fi emise de echipament, conectați-vă la interfața web a punctului de acces și navigați la **Status (Stare)** > **Client List (Listă clienți)**. În mod implicit, pagina afișează clienții wireless conectați pe banda de 2,4 GHz, asociați primului SSID din listă, din fila **2,4 GHz**. Pentru a vedea clienții altui SSID, alegeți-l din lista derulantă din colțul dreapta-sus denumită **SSID**, iar pentru a comuta pe banda de 5 GHz apăsați fila **5 GHz**.




**Descriere parametri Status (Stare) > Client List (Listă clienți)**

| Parametru | Descriere |
|---|---|
| Filele **2,4 GHz** și **5 GHz** | Apăsați fila **2,4 GHz** pentru informații despre clienții wireless pe banda de 2,4 GHz. Apăsați fila **5 GHz** pentru informații despre clienții wireless pe banda de 5 GHz. |
| **SSID** | Se folosește pentru a selecta un nume Wi-Fi (SSID) din meniul derulant pentru a vizualiza clienții conectați la rețeaua respectivă. |
| **ID** | Numărul de ordine al clientului wireless din lista SSID-ului selectat. |
| **MAC Address (Adresă MAC)** | Specifică adresa MAC a adaptorului Wi-Fi din dispozitivul client conectat la acel SSID. Adresa MAC (Media Access Control) este un identificator unic, alocat din fabrică fiecărei interfețe de rețea (placă Ethernet, modul Wi-Fi etc.). Are 48 de biți și se scrie ca 6 perechi hexazecimale separate prin **:** sau **-** (ex. A4:2B:B0:F1:09:AC). Spre deosebire de adresa IP, care se schimbă în funcție de rețea, adresa MAC rămâne în general aceeași și este folosită pentru identificarea dispozitivului la nivelul legăturii de date. |
| **IP Address (Adresă IP)** | Specifică adresa IP din rețeaua locală (LAN) a clientului wireless. |
| **Client Type (Tip client)** | Specifică tipul de sistem de operare al clientului wireless.<br><br>Tip<br><br>Echipamentul poate identifica corect tipul de sistem de operare al clientului conectat numai atunci când este activată funcția **Identify Client Type (Identificare tip client)** din meniul **Wireless > Advanced Settings (Setări avansate)** și clientul a accesat un site web HTTP. |

| Parametru | Descriere |
| --- | --- |
| **Connection Duration (Durată conexiune)** | Specifică durata de conectare online, neîntreruptă, a clientului wireless. |
| **Negotiation Rate (Rată negociere)** | Specifică rata de transmisie și rata de recepție, maximă, dintre client și SSID-ul respectiv. |
| **Signal Strength (Putere semnal)** | Specifică puterea semnalului Wi-Fi dintre client și echipamentul IP-COM. Valorile sunt întotdeauna negative, iar cu cât numărul este mai aproape de zero, cu atât semnalul este mai puternic: −30 dBm reprezintă un semnal excelent (client foarte aproape de AP), −60…−70 dBm un semnal bun, iar sub −80 dBm un semnal slab, cu pierderi de pachete și viteze reduse. |
| **Block (Blocare)** | Prin apăsarea butonului , de sub coloana **Block (Blocare)**, adăugați adresa MAC a dispozitivului din listă la **Blacklist (Listă neagră)** și acesta nu mai are acces la rețeaua Wi-Fi.<br>Pentru a verifica lista și debloca dacă e necesar, atunci accesați meniul **Wireless >** Access Control (Control acces). |

# 4 Meniul Quick Setup (Configurare rapidă)

Funcțiile pot varia în funcție de model și de versiunea software instalată. Imaginile, pașii și descrierile prezentate în acest manual au caracter orientativ și pot diferi de interfața sau funcționarea reală. În acest manual, denumirile meniurilor și ale opțiunilor sunt prezentate în limba engleză, iar echivalentul în limba română este indicat între paranteze. Manualul este adaptat utilizatorilor cunoscători de limba română.

## 4.1 Prezentare generală a meniului

Meniul **Quick Setup (Configurare rapidă)** permite stabilirea rapidă a modului de lucru al echipamentului, ceea ce determină implicit și modul în care acesta se conectează la rețeaua din amonte.

Din câmpul **Working Mode (Mod de lucru)** puteți alege una dintre cele două variante disponibile:

- **AP**: Funcționează ca punct de acces clasic, conectat prin cablu Ethernet la un switch sau ruter din rețeaua din amonte și apoi emite Wi-Fi pentru clienți. În configuratorul inițial acest mod e denumit **Access Point**.
- **Client+AP:** Se conectează prin Wi-Fi la o rețea Wi-Fi existentă (ca un client Wi-Fi) și apoi emite o rețea Wi-Fi proprie. Util când nu se poate trage cablu până la AP. În configuratorul inițial acest mod e denumit **Bridge**.

În ambele moduri de lucru se accesează o rețea locală (LAN), redirecționarea făcându-se pe baza adreselor MAC, exact ca un switch. Iar internetul e partajat efectiv de un ruter sau gateway din rețeaua locală (LAN), nu de echipamentul IP-COM.

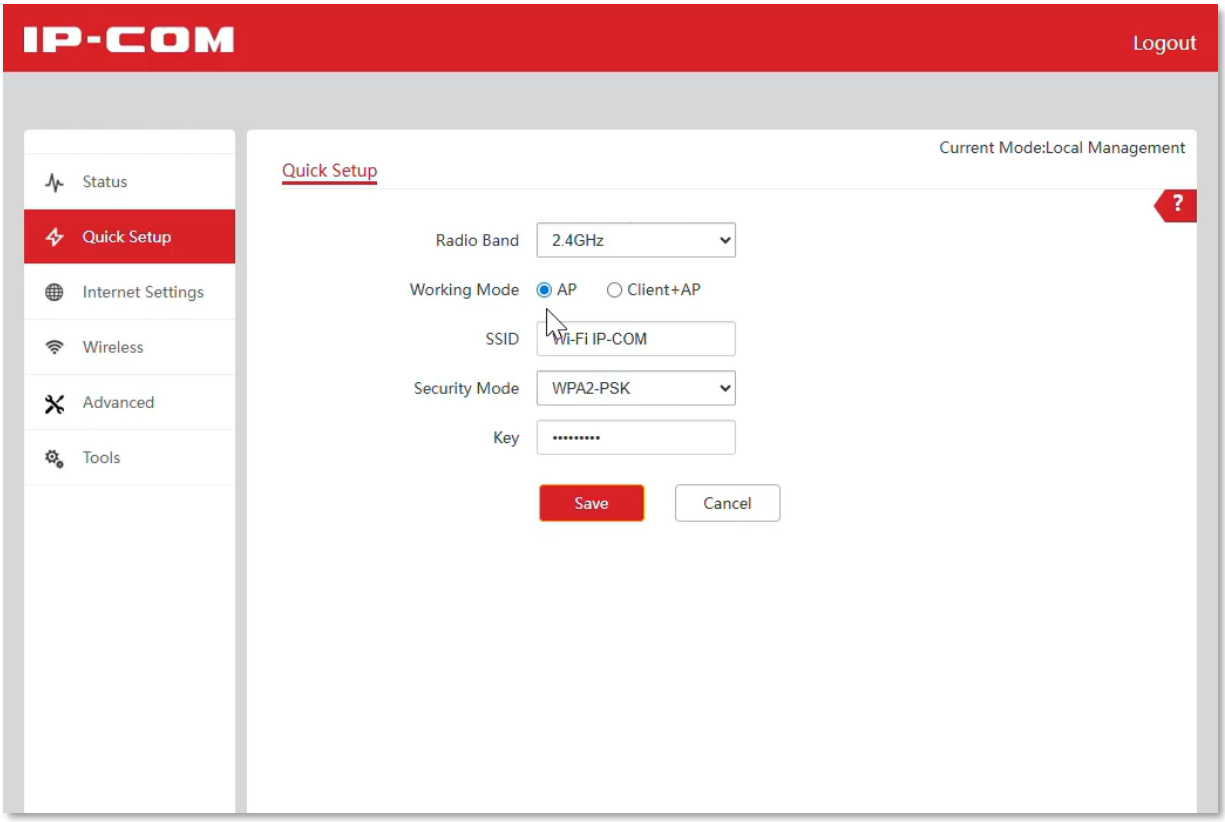
Câmpurile **SSID**, **Security Mode (Mod de securitate)** și **Key (Cheie)** din meniul **Quick Setup (Configurare rapidă)** își schimbă rolul în funcție de modul de lucru selectat:

- În modul **AP**: Ele descriu rețeaua Wi-Fi pe care echipamentul o emite — mai exact primul SSID de pe banda aleasă (2,4 GHz sau 5 GHz). Astfel se introduce numele rețelei Wi-Fi (**SSID**), tipul de criptare aplicat clienților la **Security Mode (Mod securitate**) și parola de acces la **Key (Cheie**). De reținut că echipamentul poate emite mai multe SSID-uri pe fiecare bandă; toate pot fi activate și modificate ulterior din meniul **Wireless > SSID**.

- În modul **Client+AP**: Aceleași câmpuri descriu rețeaua Wi-Fi din amonte la care AP-ul se conectează ca un client — adică numele rețelei existente la **SSID**, tipul de criptare al acesteia la **Security Mode (Mod securitate)** și parola ei la **Key (Cheie)**. Datele pot fi reintroduse manual sau preluate automat printr-o rescanare a rețelelor Wi-Fi disponibile în jur.

## 4.2 Mod de lucru AP

Cel mai rapid și facil este să setați echipamentul în modul de lucru **AP**. Echipamentul e conectat prin cablu Ethernet la un switch sau ruter din rețeaua din amonte și apoi emite Wi-Fi pentru clienți. Mai jos e o captură din interfață cu modul **AP** selectat la **Working Mode (Mod de lucru)**.




**Procedură comutare la modul de lucru AP**

1. Se conectează echipamentul la rețeaua din amonte prin cablu Ethernet — fie direct la un switch PoE+, fie prin injectorul PoE din pachet, conectând echipamentul IP-COM la portul marcat **AP** al injectorului, celălalt port marcat **Switch** la un switch ori direct la ruter, iar injectorul la priză prin adaptorul de curent inclus.
2. Conectați-vă la interfața web de gestionare.
3. Accesați meniul din stânga **Quick Setup (Configurare rapidă)**.
4. La **Working Mode (Mod de lucru)** selectați **AP**.

   Se presupune că setările Wi-Fi sunt corecte și nu trebuie modificate informațiile de la **SSID**, **Security Mode (Mod securitate)** și **Key (Cheie)**.

5. Apăsați **Save (Salvare)**.
6. Așteptați reconfigurarea și repornirea. Vă puteți reconecta la un Wi-Fi emis de echipament.

**---Sfârșit**

## 4.3 Configurarea primului SSID de pe fiecare bandă, în modul de lucru AP

Tot din meniul **Quick Setup (Configurare rapidă)** se poate configura rețeaua Wi-Fi principală emisă de echipamentul IP-COM, mai exact primul SSID de pe fiecare bandă (2,4 GHz și 5 GHz) dacă acesta e în modul de lucru **AP**. A se reține faptul că acest echipament poate emite mai multe SSID-uri, toate pot fi activate și modificate ulterior din meniul **Wireless > SSID.**

1. Conectați-vă la interfața web de gestionare.
2. Accesați meniul din stânga **Quick Setup (Configurare rapidă)**.
3. La **Working Mode (Mod de lucru)** asigurați-vă că e deja selectat **AP**. Dacă este selectat modul Client+AP, nu mai urmați această procedură, ci urmați instrucțiunile de la secțiunea 4.4 Mod de lucru Client+AP.
4. Selectați pe rând banda dorită din câmpul Radio Band **(Bandă radio)**, pentru început selectați **2,4 GHz.**
5. Introduceți denumirea rețelei Wi-Fi în câmpul **SSID**.
6. Alegeți tipul de criptare din **Security Mode (Mod securitate)** și introduceți și parola Wi-Fi dacă e cazul la câmpul **Key (Cheie)**. La modelele e posibil să fie afișat și câmpul **Encryption Algorithm (Algoritm criptare)** de selectare a algoritmului de criptare, oferindu-se posibilitatea de a selecta dintre **AES**, **TKIP** și **TKIP & AES**.
7. Apăsați **Save (Salvare)** pentru a aplica modificările. Toate setările făcute la aceste câmpuri se vor reflecta la prima intrare din lista **SSID** din meniul **Wireless > SSID**, fila **2,4 GHz**.
8. Apoi, pentru a modifica și pe banda de 5 GHz, selectați **5 GHz** la câmpul **Radio Band (Bandă radio) și urmați** pașii **1**-**7**. Puteți introduce aceleași valori ca la **2,4 GHz**, la câmpurile **SSID**, **Security Mode (Mod securitate)** și **Key (Cheie)** pentru a avea o conectare unificată pe ambele benzi.

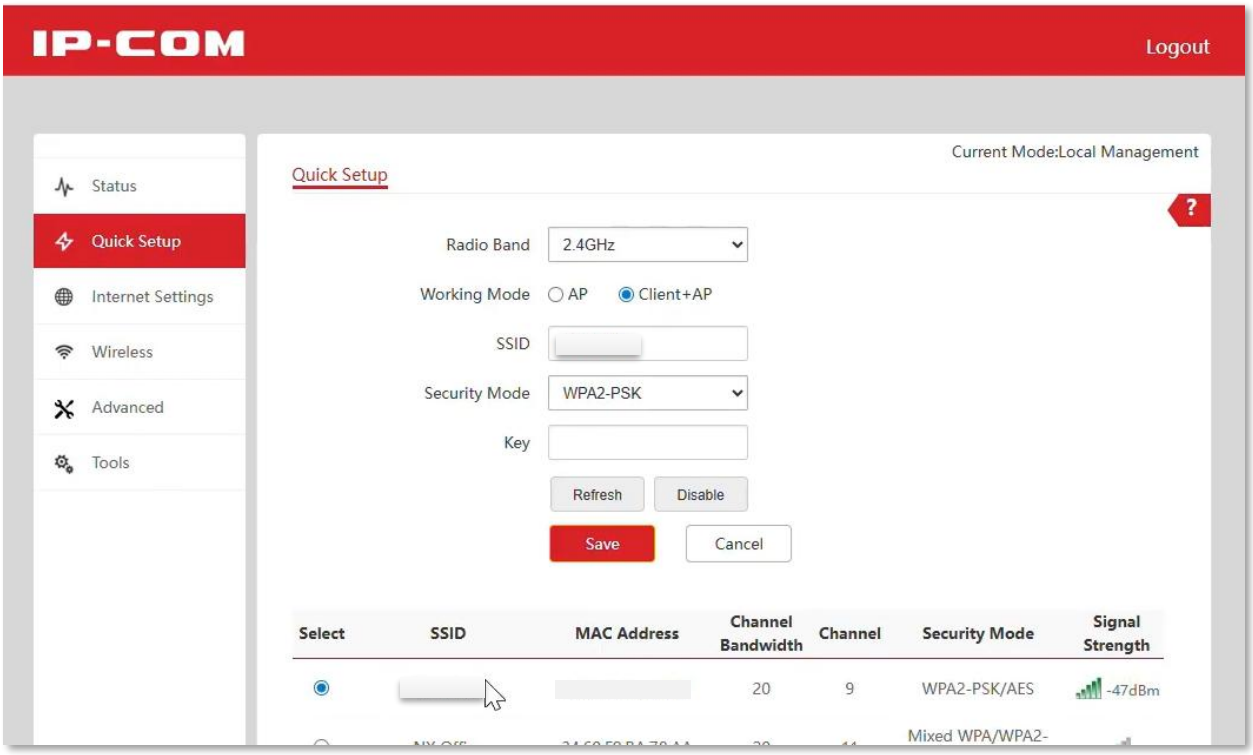
   La fel, după salvare, toate setările făcute la aceste câmpuri se vor reflecta la prima intrare din lista **SSID** din meniul **Wireless > SSID**, dar de data asta fila **5 GHz**.

**---Sfârșit**

# 4.4 Mod de lucru Client+AP

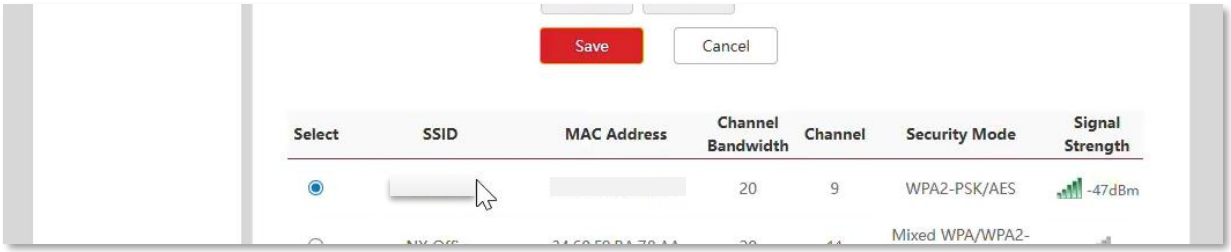
În modul de lucru **Client+AP**, echipamentul nu se mai conectează prin cablu Ethernet la rețeaua din amonte, ci se conectează prin Wi-Fi la o rețea Wi-Fi existentă (comportându-se ca un client Wi-Fi) și emite propria rețea Wi-Fi pentru clienții din jur. Modul este util atunci când nu se poate trage cablu până la echipament. În configuratorul inițial, acest mod este denumit **Bridge** și mai este cunoscut și ca *extender*, uneori *range extender* sau *repetor Wi-Fi*.

Mai jos este prezentată o captură cu modul **Client+AP** selectat la **Working Mode (Mod de lucru)**.



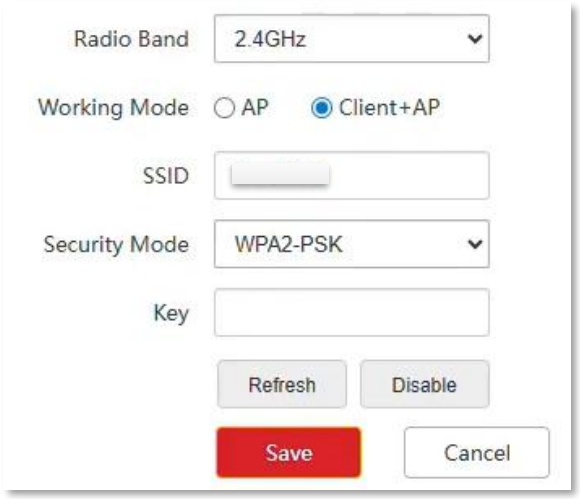

**Procedură comutare la modul de lucru Client+AP**

1. Pentru alimentarea echipamentului, conectați portul **LAN/PoE** al acestuia, printr-un cablu Ethernet, la portul **AP** al injectorului PoE inclus în pachet. Alternativ, echipamentul poate fi conectat direct la un switch PoE.
2. Conectați-vă la interfața web de gestionare.
3. Accesați meniul din stânga **Quick Setup (Configurare rapidă)**.
4. La **Working Mode (Mod de lucru)** selectați **Client+AP**.
5. Din câmpul **Radio Band (Bandă radio)** selectați banda de frecvență pe care doriți să vă conectați la rețeaua Wi-Fi din amonte: **2,4 GHz** sau **5 GHz**. Banda de 5 GHz oferă rată (viteză) de comunicare mai mare, dar o rază de acoperire mai mică, în timp ce banda de 2,4 GHz are o rază de acoperire mai mare, însă rată (viteză) mai redusă.
6. Apăsați butonul **Scan (Scanare)** și așteptați detectarea rețelelor Wi-Fi pe banda selectată.
7. Din listă selectați rețeaua Wi-Fi din amonte, urmăriți coloana **SSID**.




8. Odată ce selectați rețeaua, denumirea va fi completată la câmpul **SSID** și selectat protocolul de securitate la **Security Mode (Mod securitate)**. Mai trebuie doar să introduceți parola rețelei Wi-Fi din amonte la câmpul **Key (Cheie)**. Tot aici puteți conecta echipamentul la o rețea Wi-Fi ascunsă, completând manual aceste trei câmpuri.

   La unele modele e posibil să fie afișat și câmpul **Encryption Algorithm (Algoritm criptare)** de selectare a algoritmului de criptare, oferindu-se posibilitatea de a selecta dintre **AES**, **TKIP** și **TKIP & AES**.




9. Apăsați **Save (Salvare)** și așteptați conectarea echipamentului la rețeaua Wi-Fi din amonte. De reținut că, în acest mod de lucru, rețeaua Wi-Fi emisă mai departe de echipamentul IP-COM nu mai poate fi configurată din acest meniu **Quick Setup (Configurare rapidă)**; vizualizarea și modificarea SSID-urilor pe fiecare bandă se fac din meniul **Wireless > SSID**.

**---Sfârșit**

# 5 Meniul Internet Settings (Setări internet)

Funcțiile pot varia în funcție de model și de versiunea software instalată. Imaginile, pașii și descrierile prezentate în acest manual au caracter orientativ și pot diferi de interfața sau funcționarea reală. În acest manual, denumirile meniurilor și ale opțiunilor sunt prezentate în limba engleză, iar echivalentul în limba română este indicat între paranteze. Manualul este adaptat utilizatorilor cunoscători de limba română.

## 5.1 Submeniul LAN Setup (Configurare LAN)

### 5.1.1 Fila LAN Setup (Configurare LAN)

Configurările IP din fila **LAN Setup (Configurare LAN)** au rol strict administrativ și nu influențează traficul clienților conectați la acest punct de acces, indiferent dacă aceștia utilizează o conexiune prin cablu sau Wi-Fi. Aceste setări sunt utile pentru:

- Accesarea interfeței web de gestionare locală.
- Permiterea accesului echipamentului la internet (pentru actualizări sau sincronizare timp).
- Comunicarea cu platforma de management **IP-COM ProFi Cloud**.

Din punct de vedere tehnic, indiferent de adresa IP configurată, dispozitivul funcționează ca un switch transparent pentru traficul utilizatorilor. Transmisia datelor între clienți și restul rețelei se realizează la nivel de Layer 2, conform modelului OSI. Câteva detalii importante de conectare:

- Adresa IP implicită: În mod nativ, echipamentul poate fi accesat la adresa **192.168.0.254**.
- Alocare dinamică: Dacă în rețeaua locală există un server DHCP activ, punctul de acces va obține automat o adresă IP de la acesta.
- Personalizare: În această secțiune, puteți vizualiza adresa MAC a portului LAN și puteți modifica adresa IP, numele dispozitivului și alți parametri de rețea asociați.

**Procedură pentru configurarea setărilor din rețeaua locală (LAN), pentru acest echipament**

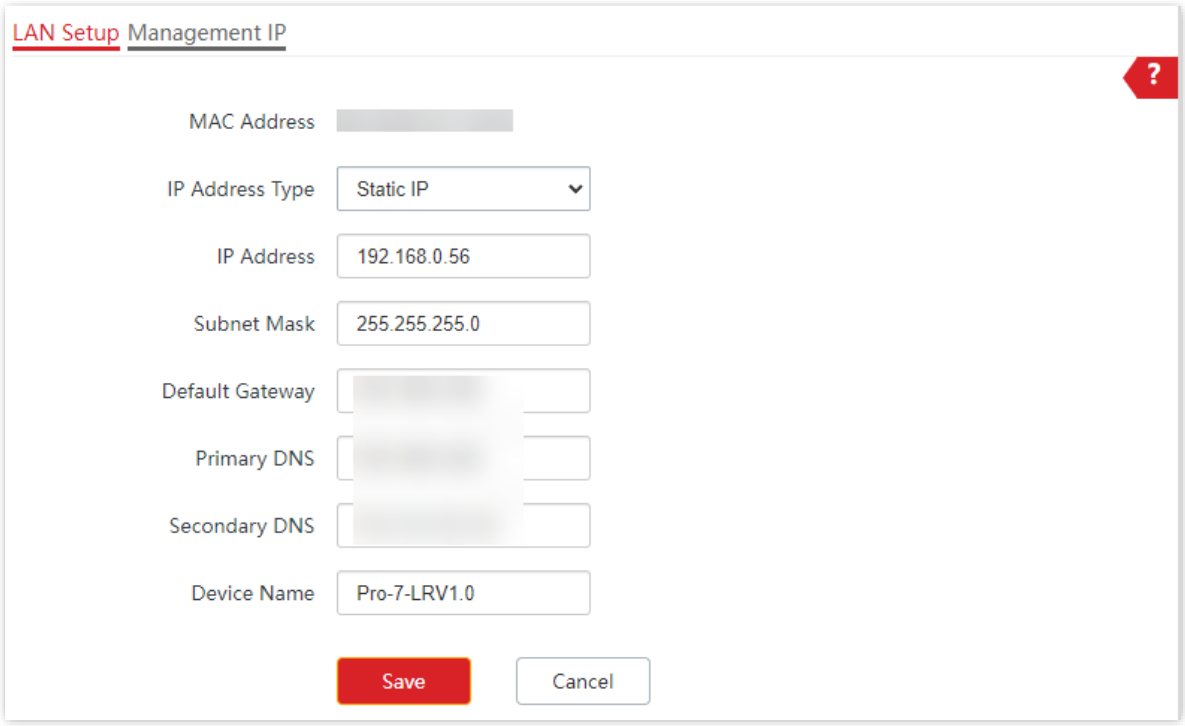
1. Conectați-vă la interfața web a punctului de acces.
2. Navigați la **Internet Settings (Setări internet)** > **LAN Setup (Configurare LAN)** > fila **LAN Setup (Configurare LAN)**.

3. La **IP Address Type (Tip adresă IP)** selectați modul în care punctul de acces obține informațiile IP. Fie selectați **Static IP (IP static)** și completați manual toate câmpurile de mai jos, fie selectați **DHCP (Dynamic IP Address) (DHCP (Adresă IP dinamică))** pentru a obține automat informațiile IP de la un server DHCP din rețeaua locală.

Tip

Dacă este selectată opțiunea **Static IP (IP static),** specificați manual adresa IP, masca de subrețea, gateway-ul implicit și serverul DNS.

4. Faceți clic pe **Save (Salvare).** Următoarea figură este doar pentru referință.




**---Sfârșit**

Tip

Dacă ați modificat adresa IP de internet a punctului de acces, trebuie să utilizați noua adresă IP pentru a vă conecta la interfața web.

**Descriere parametri din meniul Internet Settings (Setări internet) > LAN Setup (Configurare LAN) > LAN Setup (Configurare LAN)**

| Parametru | Descriere |
|---|---|
| **MAC Address (Adresă MAC)** | Specifică adresa MAC a portului LAN al punctului de acces. |

| Parametru | Descriere |
| --- | --- |
| **IP Address Type**<br>**(Tip adresă IP)** | Specifică modul de obținere a adresei IP a punctului de acces.<br>– **Static IP (IP static):** Indică faptul că adresa IP, masca de subrețea, gateway-ul și serverul DNS sunt setate manual.<br>– **DHCP (Dynamic IP Address) (DHCP (Adresă IP dinamică)):** Indică faptul că informațiile despre adresa IP, masca de subrețea, gateway-ul și serverul DNS al punctului de acces sunt obținute de la un server DHCP din rețeaua locală.<br><br>Când este selectat **DHCP (Dynamic IP Address) (DHCP (Adresă IP dinamică))** adresa IP a punctului de acces se poate modifica. Înainte de a vă conecta la interfața web a punctului de acces, verificați lista de clienți de pe serverul DHCP din rețea pentru a găsi adresa IP atribuită punctului de acces, apoi utilizați acea adresă IP pentru a vă conecta. |
| **IP Address**<br>**(Adresă IP)** | Specifică adresa IP din rețeaua locală (LAN) a punctului de acces. Interfața web a punctului de acces este accesibilă la această adresă IP.<br><br>– Înainte de a utiliza această adresă IP pentru a vă conecta la interfața web a punctului de acces, asigurați-vă că adresa IP a dispozitivului client ce va accesa interfața se află în aceeași subrețea.<br>– Dacă funcția QVLAN este activată din **Wireless > QVLAN Settings (Setări QVLAN)**, conectarea la interfața de gestionare se poate face numai dintr-o rețea Wi-Fi al cărei **VLAN ID** coincide cu cel din câmpul **Management VLAN (VLAN gestionare)** sau printr-un cablu Ethernet conectat la un port al cărui VLAN membru corespunde aceluiași VLAN de gestionare. În caz contrar, dispozitivul nu va fi accesibil prin browser. ID-urile VLAN pentru rețelele Wi-Fi (SSID) emise de echipament se configurează tot din meniul **Wireless > QVLAN Settings (Setări QVLAN)**. |
| **Subnet Mask**<br>**(Mască subrețea)** | Specifică masca de subrețea corespunzătoare adresei IP. Este utilizată pentru a defini intervalul de adrese al segmentului de rețea al dispozitivului. |
| **Default Gateway**<br>**(Gateway implicit)** | Specifică IP-ul de comunicare cu un ruter (sau gateway) pentru a avea acces la internet (sau la o rețea externă).<br>De obicei acest IP este cel al ruterului din amonte ce partajează internetul. |

| Parametru | Descriere |
| --- | --- |
| **Primary DNS**<br>**(DNS primar)** | Specifică serverul DNS principal. DNS reprezintă un sistem care traduce numele de domenii (de exemplu, ip-com.com.cn) în adrese IP numerice (de exemplu, 110.190.233.155), utilizate de calculatoare pentru a se identifica între ele în rețea. Serverele DNS funcționează asemenea unei agende telefonice.<br>Serverele DNS publice, precum cele oferite de Google (8.8.8.8) sau Cloudflare (1.1.1.1), sunt baze de date globale ce pot fi interogate pentru a găsi rapid adresele IP ale site-urilor accesate.<br>În acest câmp, în multe cazuri, puteți introduce adresa IP LAN a ruterului din amonte. Ruterul care partajează conexiunea la internet va rezolva sau va redirecționa corespunzător interogările DNS, inclusiv în situația în care este configurat un proxy DNS. |
| **Secondary DNS**<br>**(DNS secundar)** | Specifică adresa IP a serverului DNS secundar al punctului de acces. Acest parametru este opțional.<br>Dacă există două adrese IP de server DNS, puteți introduce adresa IP secundară în acest câmp. |
| **Device Name**<br>**(Nume dispozitiv)** | Specifică numele punctului de acces, acesta fiind utilizat pentru identificarea în rețea.<br>Se recomandă modificarea numelui pentru a indica locația dispozitivului, permițând astfel identificarea rapidă a acestuia atunci când gestionați mai multe puncte de acces în aceeași rețea. |

### 5.1.2 Fila Management IP (IP de gestionare)

Pe lângă adresa IP principală setată la fila **LAN Setup (Configurare LAN)**, punctul de acces poate fi configurat cu o adresă IP secundară de gestionare. Aceasta permite accesul la interfața web a dispozitivului din subrețele diferite, facilitând administrarea chiar și atunci când adresa IP principală nu este accesibilă direct. Acest IP mai e cunoscut și ca IP-ul secundar de management.

Orice dispozitiv conectat la rețea poate accesa această adresă secundară, cu condiția ca setările adaptorului de rețea (placa de rețea) să fie modificate corespunzător. Mai exact, utilizatorul trebuie să configureze manual o adresă IP statică pe calculatorul său, care să facă parte din aceeași clasă (subrețea) cu IP-ul secundar al punctului de acces. Această metodă este utilă în mod special pentru depanare sau pentru izolarea traficului de administrare de cel de date.

Tip

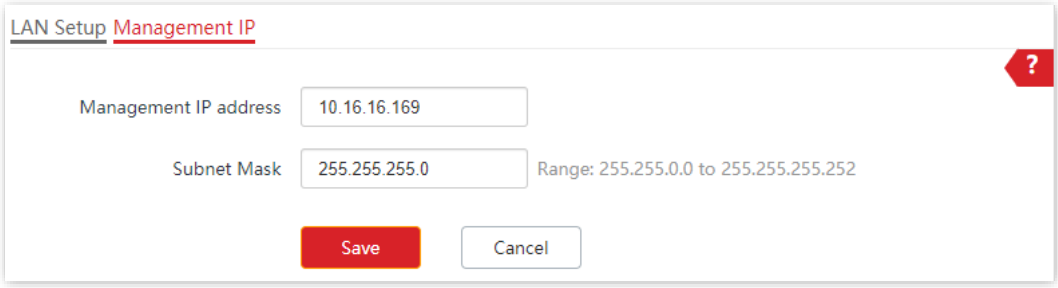
Înainte de a utiliza această adresă IP pentru a vă conecta la interfața web a punctului de acces:

- Înainte de a utiliza această adresă IP pentru a vă conecta la interfața web a punctului de acces, asigurați-vă că adresa IP a dispozitivului client ce va accesa interfața se află în aceeași subrețea.
- Dacă funcția QVLAN este activată din **Wireless > QVLAN Settings (Setări QVLAN)**, conectarea la interfața de gestionare se poate face numai dintr-o rețea Wi-Fi al cărei **VLAN ID** coincide cu cel din câmpul **Management VLAN (VLAN gestionare)** sau printr-un cablu Ethernet conectat la un port al cărui VLAN membru corespunde aceluiași VLAN de gestionare. În caz contrar, dispozitivul nu va fi accesibil prin browser. ID-urile VLAN pentru rețelele Wi-Fi (SSID) emise de echipament se configurează tot din meniul **Wireless > QVLAN Settings (Setări QVLAN)**.

Adresa IP implicită este **10.16.16.169** și dacă aveți mai multe echipamente IP-COM se recomandă să schimbați pe fiecare echipament acest IP, măcar valoarea de la ultimul octet.

**Procedură pentru configurarea IP-ului de gestionare:**

1. Conectați-vă la interfața web a punctului de acces.
2. Navigați la **Internet Settings (Setări internet)** > **LAN Setup (Setare LAN)** > fila **Management IP (IP de gestionare).**
3. Modificați **Management IP address (Adresă IP gestionare)** și **Subnet Mask (Mască subrețea)** după cum este necesar.
4. Faceți clic pe **Save (Salvare).** După finalizarea configurării, trebuie să utilizați noua adresă IP de administrare pentru a vă conecta la interfața web a punctului de acces.




**---Sfârșit**

# 5.2 Submeniul Intelligent DHCP Service (Serviciu DHCP inteligent)

**Intelligent DHCP Service (Serviciu DHCP inteligent)** este utilizat atunci când nu există niciun alt server DHCP în rețeaua locală în care se află punctul de acces. În acest caz, AP-ul acționează ca un server DHCP și atribuie automat adrese IP dispozitivelor din rețeaua locală.

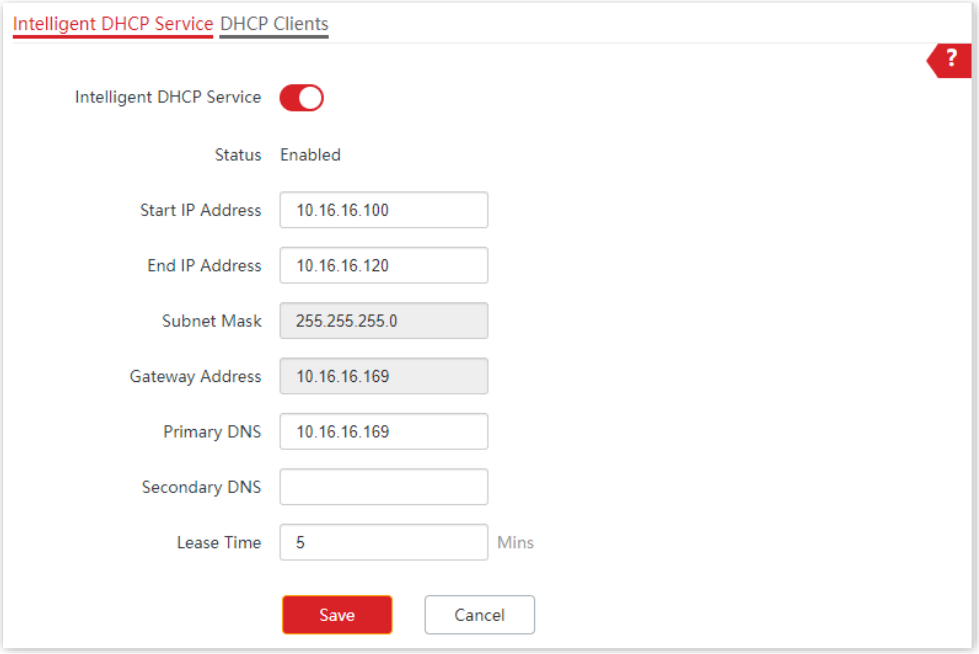
Funcția de serviciu DHCP inteligent este activată în mod implicit. Când există alte servere DHCP în rețeaua locală unde se află punctul de acces sau când punctul de acces este gestionat de un

controler de AP-uri IP-COM sau de un ruter multi-WAN cu control de AP-uri, seria M de la IP-COM, atunci această funcție va fi dezactivată automat.

Dacă funcția **Intelligent DHCP Service (Serviciu DHCP inteligent)** a fost dezactivată automat, iar la câmpul **Status (Stare)** apare mesajul **Disabled (Dezactivat)**, reactivarea manuală ar putea fi restricționată. În cazul în care, trecând cu mausul peste comutatorul funcției, apare simbolul de interzis, singura modalitate de a reactiva această opțiune este resetarea punctului de acces la setările din fabrică.

## 5.2.1 Fila Intelligent DHCP Service (Serviciu DHCP inteligent)

1. Conectați-vă la interfața web a punctului de acces.
2. Navigați la **Internet Settings (Setări internet)** > **Intelligent DHCP Service (Serviciu DHCP inteligent)** > fila **Intelligent DHCP Service (Serviciu DHCP inteligent).**
3. Asigurați-vă că e activă funcția **Intelligent DHCP Service (Serviciu DHCP inteligent).**
4. Ca la orice alt server DHCP, modificați parametrii după cum este necesar.
5. Faceți clic pe **Save (Salvare).**




**---Sfârșit**

**Descriere parametri Internet Settings (Setări internet) > Intelligent DHCP Service (Serviciu DHCP inteligent) > Intelligent DHCP Service (Serviciu DHCP inteligent)**

| Parametru | Descriere |
|---|---|
| **Intelligent DHCP Service (Serviciu DHCP inteligent)** | Specifică dacă se activează funcția de serviciu inteligent DHCP a punctului de acces. |

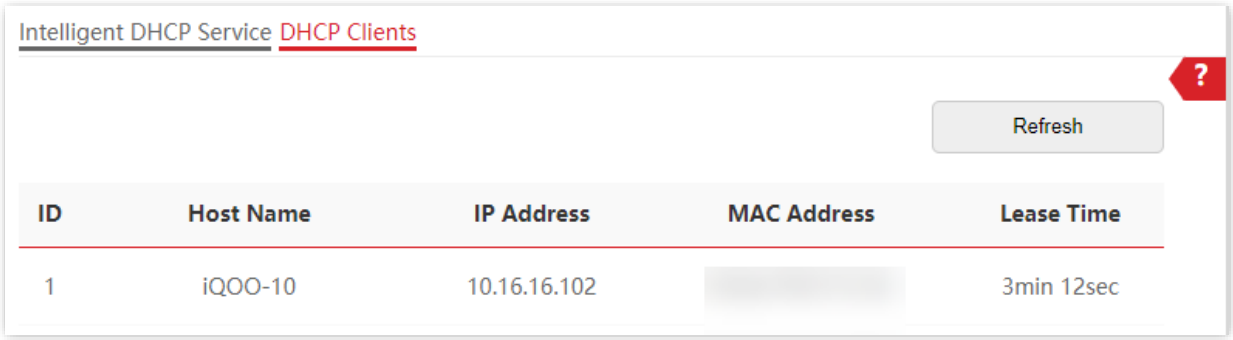
| Parametru | Descriere |
|---|---|
| **Status**<br>**(Stare)** | Specifică starea funcției de serviciu inteligent DHCP a punctului de acces. |
| **Start IP Address**<br>**(Adresă IP de început)** | Specificați intervalul de adrese IP din care vor fi oferite IP-uri clienților conectați.<br><br>După modificarea adresei IP de la **Management IP (IP de gestionare)** din meniul **Internet Settings (Setări internet) > LAN Setup (Setare LAN)**, sistemul verifică și setările de aici, de la **Intelligent DHCP Service (Serviciu DHCP inteligent)**. Astfel, dacă noua adresă de la **Management IP (IP de gestionare)** nu face parte din aceeași subrețea cu cea din acest interval, sistemul va ajusta automat intervalul de adrese DHCP pentru a corespunde noii subrețele. |
| **End IP Address**<br>**(Adresă IP de sfârșit)** | |
| **Subnet Mask**<br>**(Mască subrețea)** | Specifică masca de subrețea atribuită clienților de către serverul DHCP al punctului de acces. În mod implicit, este masca de subrețea corespunzătoare câmpului Subnet Mask (Mască subrețea) de la Management IP. |
| **Gateway Address**<br>**(Adresă gateway)** | Specifică adresa IP a gateway-ului atribuită clienților de serverul DHCP al punctului de acces. În mod implicit, aceasta este adresa IP de la **Management IP (IP de gestionare)**. |
| **Primary DNS**<br>**(DNS primar)** | Specifică adresa IP a serverului DNS principal atribuit clienților de către serverul DHCP. |
| **Secondary DNS**<br>**(DNS secundar)** | Specifică adresa IP a serverului DNS secundar atribuit clienților. Acest parametru este opțional, ceea ce indică faptul că îl puteți lăsa necompletat dacă serverul DHCP nu atribuie acest parametru. |
| **Lease Time**<br>**(Durată închiriere)** | Specifică perioada de valabilitate a unei adrese IP atribuite unui client. La expirarea acestui interval, se aplică următoarele reguli:<br>– Dacă un client este încă conectat la punctul de acces, acesta va reînnoi automat perioada și va păstra aceeași adresă IP.<br>– Dacă un client nu mai este conectat la punctul de acces, adresa IP ocupată anterior va fi eliberată. Astfel, dacă un alt dispozitiv solicită o adresă IP, punctul de acces poate atribui adresa eliberată noului client.<br>Durata poate fi configurată manual sau prin selectarea unei valori predefinite: 30 de minute, 1, 6, 12 ore ori 1, 3 sau 7 zile. |

## 5.2.2 Fila DHCP Clients (Clienți DHCP)

Atunci când punctul de acces acționează ca server DHCP, datorită activării funcției **Intelligent DHCP Service (Serviciu DHCP inteligent)**, puteți vizualiza informații despre clienți, precum numele și adresele IP ale dispozitivelor care au obținut informații IP de la serverul DHCP.

**Procedură pentru vizualizarea clienților DHCP**

1. Conectați-vă la interfața web a punctului de acces.
2. Navigați la **Internet Settings (Setări internet)** > **Intelligent DHCP Service (Serviciu DHCP inteligent)** > fila **DHCP Clients (Clienți DHCP).**
3. Opțional, faceți clic pe **Refresh (Reîmprospătare)** pentru a vizualiza cea mai recentă listă de clienți DHCP.
4. Apoi în listă vedeți la coloana **Host Name (Nume gazdă)** numele dispozitivului client, la **IP Address (Adresă IP)** adresa IP atribuită, la **MAC Address (Adresă MAC)** identificatorul MAC al adaptorului de rețea prin care se conectează la rețea și la **Lease Time (Durată închiriere)** durata alocării adresei IP.




**---Sfârșit**

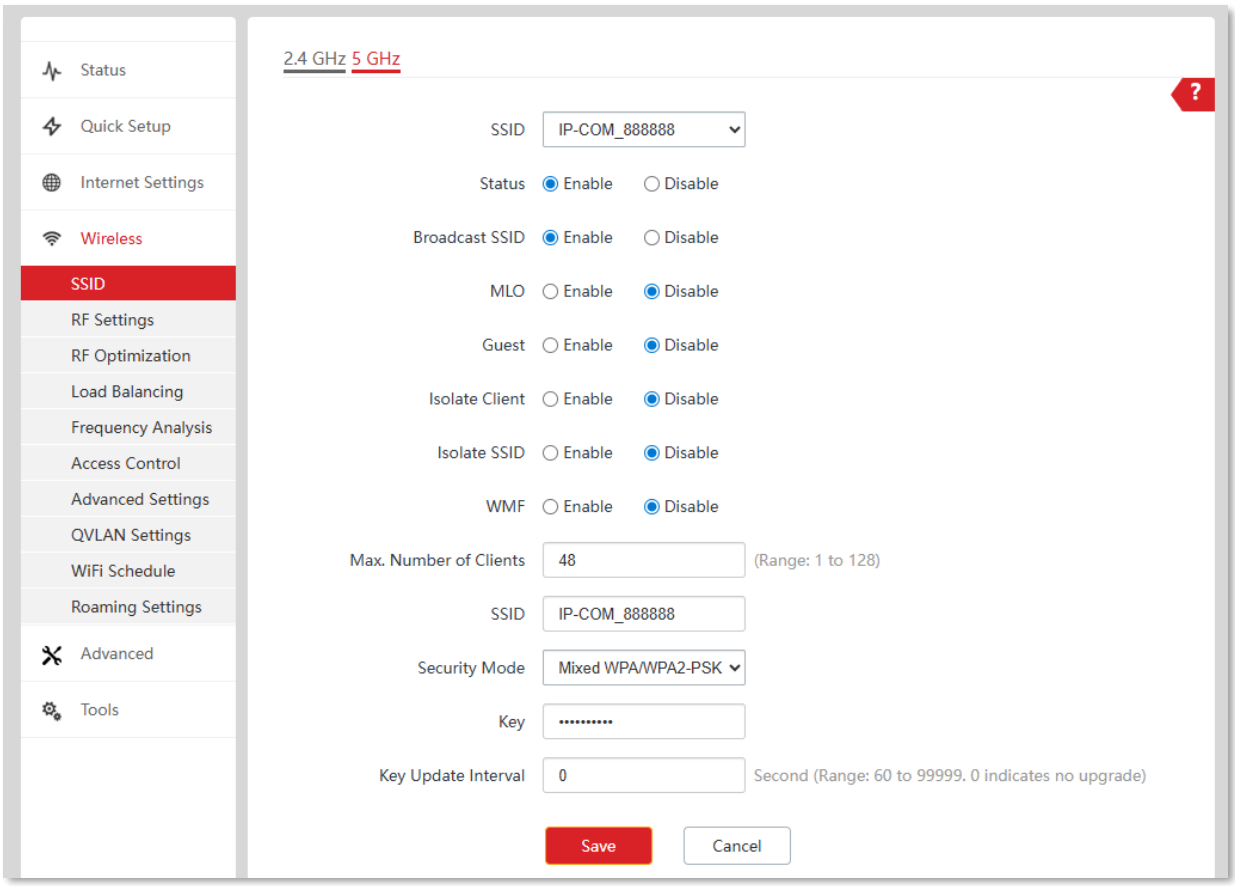
# 6 Meniul Wireless

Funcțiile pot varia în funcție de model și de versiunea software instalată. Imaginile, pașii și descrierile prezentate în acest manual au caracter orientativ și pot diferi de interfața sau funcționarea reală. În acest manual, denumirile meniurilor și ale opțiunilor sunt prezentate în limba engleză, iar echivalentul în limba română este indicat între paranteze. Manualul este adaptat utilizatorilor cunoscători de limba română.

## 6.1 Submeniul SSID

### 6.1.1 Prezentare generală

Pentru a accesa pagina unde puteți modifica mai multe opțiuni pentru toate SSID-urile, conectați-vă la interfața web a punctului de acces și navigați la **Wireless** > **SSID.** Puteți seta parametrii avansați pentru fiecare SSID, de pe fiecare bandă. Modelele din manual suportă 8 SSID-uri pe banda de 2,4 GHz și 4 SSID-uri pe banda de 5 GHz.



### Descriere parametri Wireless > SSID

| Parametru | Descriere |
|---|---|
| Fila **2,4 GHz**<br>Fila **5 GHz** | Apăsați pe unul dintre aceste două file pentru a selecta banda pe care se vor face configurările SSID-urilor. |
| **SSID** | Se selectează SSID-ul care va fi configurat.<br>Primul SSID afișat pe pagină, sub fila benzii radio, este SSID-ul principal al benzii radio.<br>Se permite configurarea unui număr de 8 SSID-uri pe fila **2,4 GHz** și 4 SSID-uri pe **5 GHz**. |
| **Status**<br>**(Stare)** | Se activează sau dezactivează SSID-ul selectat.<br>Primul SSID este activat în mod implicit, în timp ce celelalte SSID-uri sunt dezactivate în mod implicit. Le puteți activa după cum este necesar. |
| **Broadcast SSID**<br>**(Difuzare SSID)** | Ascunde sau afișează numele rețelei Wi-Fi — funcție cunoscută la alte echipamente comerciale și ca *ascundere rețea Wi-Fi* sau *Hide Wi-Fi*.<br>Când această opțiune este dezactivată, punctul de acces nu mai face vizibil SSID-ul, astfel că dispozitivele wireless din apropiere nu îl vor mai detecta automat. Pentru conectarea la rețeaua Wi-Fi respectivă, va trebui să introduceți manual numele SSID pe dispozitivul client.<br>Dezactivarea difuzării contribuie la îmbunătățirea securității rețelei Wi-Fi. |
| **Guest**<br>**(Invitați)** | Politicile aplicate rețelei pentru invitați (oaspeți) elimină traficul broadcast și multicast în sensul LAN către WLAN pentru toate dispozitivele, cu excepția gateway-ului implicit, și blochează propagarea traficului broadcast provenit de la stațiile wireless spre rețeaua locală. Această configurație îmbunătățește securitatea și performanța rețelei, izolând invitații (oaspeții) de restul infrastructurii.<br>După activarea acestei funcții, clienții wireless conectați la rețeaua pentru invitați pot accesa doar internetul, fără a avea acces la resursele din rețeaua locală LAN (inclusiv la interfața web a punctului de acces). Astfel, rețeaua pentru invitați răspunde nevoilor de acces la internet ale acestora, păstrând în același timp securitatea rețelei principale.<br>Note<br>– Dacă este necesară și izolarea clienților invitați între ei, se recomandă activarea suplimentară a opțiunii **Client Isolation (Izolare client)**.<br>– În rețelele de dimensiuni reduse, fără switch-uri cu interfață de gestionare, activarea acestei funcții poate oferi o separare funcțională a traficului similară unui VLAN dedicat, direct la nivelul punctului de acces. Totuși, această opțiune nu înlocuiește complet un VLAN configurat corect în infrastructură, deoarece izolarea se aplică exclusiv la nivel wireless, fără a afecta segmentarea la nivel de switch sau uplink. |

| Parametru | Descriere |
| --- | --- |
| **MLO** | MLO (Multi-Link Operation) este o funcționalitate introdusă în standardul Wi-Fi 7 (802.11be) care permite unui dispozitiv client și unui access point să comunice simultan pe mai multe benzi de frecvență (2,4 GHz și 5 GHz) în cadrul aceleiași conexiuni.<br><br>În Wi-Fi 6 și versiunile anterioare, un client se conecta la o singură bandă la un moment dat. Dacă banda respectivă era congestionată sau avea interferențe, performanța scădea, iar trecerea pe altă bandă implica o reconectare.<br><br>Cu **MLO**, clientul stabilește legături paralele pe mai multe benzi simultan, iar traficul este coordonat între aceste legături. Practic, dispozitivul „vede" mai multe canale ca pe o singură conexiune logică.<br><br>Funcționează doar dacă rețelele de 2,4 GHz și 5 GHz au același nume Wi-Fi aceeași parolă la și sunt configurate în modul wireless **802.11be.** |
| **Isolate Client**<br><br>**(Izolare client)** | Specifică dacă se activează funcția de izolare a clienților wireless.<br><br>După activarea acestei funcții, clienții conectați la același SSID nu pot comunica direct între ei. Fiecare client poate accesa în continuare internetul și resursele din rețeaua cu fir conectată la punctul de acces, însă traficul dintre stațiile wireless este blocat la nivelul AP-ului.<br><br>Această funcție este recomandată în scenarii publice sau semi-publice — hoteluri, aeroporturi, săli de conferință, cafenele — unde utilizatorii partajează aceeași rețea Wi-Fi, dar nu ar trebui să aibă vizibilitate reciprocă. Activarea izolării clienților reduce semnificativ riscul de scanare a rețelei, acces neautorizat la dispozitivele altor utilizatori sau atacuri de tip *lateral movement*.<br><br>Note<br><br>Izolarea clienților acționează exclusiv la nivelul SSID-ului selectat. Dacă dispozitivele sunt conectate atât prin Wi-Fi, cât și prin cablu, izolarea nu se aplică traficului dintre acestea pe traficul cu cablu. |
| **Isolate SSID**<br><br>**(Izolare SSID)** | Specifică dacă se activează funcția de izolare între SSID-uri.<br><br>După activarea acestei funcții, clienții wireless conectați la SSID-uri diferite ale aceluiași punct de acces nu pot comunica direct între ei la nivel wireless, chiar dacă se află în același segment de rețea. Traficul dintre SSID-uri este blocat la nivelul AP-ului, fiecare rețea Wi-Fi funcționând independent față de celelalte.<br><br>Această funcție este utilă în scenarii în care același punct de acces difuzează mai multe SSID-uri cu scopuri diferite — de exemplu, o rețea pentru angajați și una pentru invitați, sau SSID-uri dedicate unor departamente separate — și se dorește prevenirea comunicării laterale între acestea fără a recurge la o segmentare VLAN completă.<br><br>Note<br><br>Izolarea SSID acționează exclusiv la nivel wireless. Pentru o separare completă a traficului, inclusiv pe traficul prin cablu, se recomandă utilizarea VLAN-urilor dedicate per SSID, configurate atât pe punctul de acces, cât și pe switch-ul și ruterul din infrastructură. |

| Parametru | Descriere |
| --- | --- |
| **WMF** | Specifică dacă se activează *Wireless Multicast Forwarding (Redirecționare multicast wireless)*.<br><br>În mod implicit, pachetele multicast sunt transmise în rețelele Wi-Fi la cea mai mică rată de date suportată (de exemplu, 1 Mbps), pentru a fi recepționate de toți clienții, ceea ce duce la o eficiență scăzută a transmisiei și la consum ridicat de timp pe canalul radio.<br><br>După activarea **WMF**, punctul de acces convertește traficul multicast în trafic unicast și îl transmite individual către fiecare client abonat la fluxul respectiv. Astfel, fiecare client primește pachetele la rata de date negociată automat pentru conexiunea sa și beneficiază de mecanismul de confirmare (ACK) și retransmisie specific traficului unicast.<br><br>Activarea **WMF** este recomandată în rețelele unde există trafic multicast frecvent, cum ar fi: streaming video sau IPTV, transmisii live, sisteme de videoconferință, aplicații VoIP multicast, supraveghere video pe IP cu camere care transmit fluxuri multicast.<br><br>Note<br><br>Funcția este utilă în rețelele cu trafic multicast frecvent. În rețelele fără surse multicast active, activarea ei nu aduce un beneficiu vizibil, dar nici nu afectează performanța. |
| **Max. Number of Clients**<br><br>**(Număr maxim de clienți)** | Stabilește câți clienți se pot conecta simultan la rețeaua Wi-Fi a unui SSID.<br><br>Odată atinsă această limită, clienții noi nu se mai pot conecta la SSID până când alți clienți nu se deconectează.<br><br>Numărul maxim e indicat în interfață. Se acceptă maximum **128** de clienți per SSID. |
| **SSID** | Folosit pentru a schimba numele SSID-ului selectat.<br><br>Mai exact, e numele rețelei Wi-Fi. |
| **Security Mode**<br><br>**(Mod securitate)** | Se aleg protocoalele de securitate Wi-Fi pentru SSID-ul selectat.<br><br>Opțiunile includ: **None (Fără)**, **WPA-PSK, WPA2-PSK, Mixed WPA/WPA2-PSK (Mixt WPA/WPA2-PSK)**, **WPA, WPA2**, **WPA3-SAE** și **WPA2-PSK&WPA3-SAE**.<br><br>Modurile de securitate cu toate sub-opțiunile afișate sunt prezentate începând cu secțiunea următoare.<br><br>Note<br><br>Modurile de securitate pot diferi în funcție de modele și benzile radio (2,4 GHz și 5 GHz). Prevalează produsul real. |

## 6.1.2 Protocoale de securitate Wi-Fi de la opțiunea Security Mode (Mod securitate)

Rețelele Wi-Fi transmit datele prin unde radio, un mediu accesibil oricui se află în raza de acoperire. În lipsa unor măsuri de protecție, oricine se poate conecta la rețea pentru a-i accesa resursele sau pentru a intercepta datele care circulă prin ea. De aceea, traficul Wi-Fi trebuie criptat, astfel încât doar utilizatorii autorizați să poată accesa rețeaua, iar comunicațiile să rămână confidențiale.

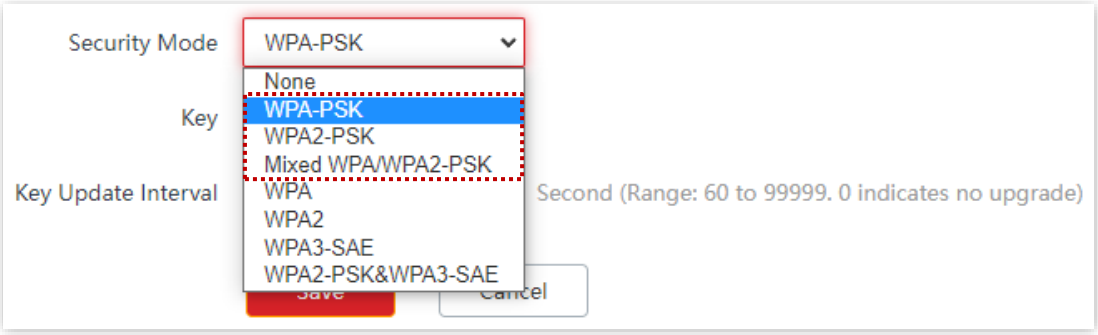
Echipamentul acceptă diverse moduri de securitate pentru criptarea rețelei, anume: **None (Fără)**, **WPA-PSK**, **WPA2-PSK**, **Mixed WPA/WPA2-PSK (Mix WPA/WPA2-PSK)**, **WPA**, **WPA2**, **WPA3-SAE** și **WPA2-PSK&WPA3-SAE**. Modurile pot diferi în funcție de modelul de echipament și bandă selectată.

- **None (Fără)**

  Indică faptul că orice client wireless se poate conecta la rețeaua Wi-Fi, fără nicio restricție de autentificare, fără parolă Wi-Fi. Această opțiune nu este recomandată, deoarece lasă rețeaua deschisă și expusă accesului neautorizat, afectând semnificativ securitatea acesteia.

- **WPA-PSK**

  Reprezintă prima generație a standardului WPA (Wi-Fi Protected Access), introdusă ca soluție tranzitorie pentru a înlocui protocolul WEP, considerat nesigur. Utilizează autentificarea cu cheie partajată (Pre-Shared Key) și algoritmul de criptare **TKIP** (Temporal Key Integrity Protocol). Deși a reprezentat un progres față de WEP, **WPA-PSK** este astăzi considerat învechit și vulnerabil la mai multe tipuri de atacuri (printre care atacurile de tip dicționar și exploiturile asupra **TKIP**). Nu este recomandat pentru rețele active și ar trebui utilizat doar pentru compatibilitate cu dispozitive foarte vechi care nu suportă WPA2.




- **WPA2-PSK**

  Este standardul introdus prin certificarea IEEE 802.11i, care înlocuiește TKIP cu algoritmul de criptare AES-CCMP, considerabil mai sigur și mai eficient. Folosește, de asemenea, autentificarea cu cheie partajată (Pre-Shared Key), dar oferă o protecție criptografică modernă, fiind ani de zile standardul de facto pentru rețelele Wi-Fi. **WPA2-PSK** rămâne o opțiune sigură pentru majoritatea scenariilor, deși este vulnerabil în general la atacuri de tip dicționar. Pentru securitate maximă, se recomandă utilizarea **WPA3-SAE** acolo unde este suportat.

- **Mixed WPA/WPA2-PSK (Mix WPA/WPA2-PSK)**

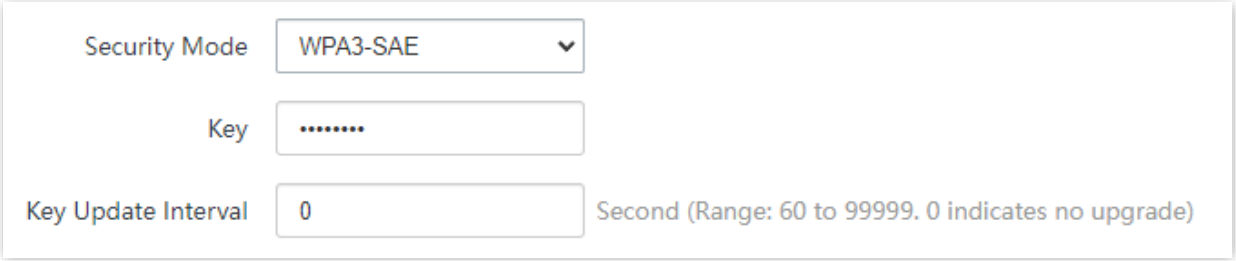
  Permite conectarea simultană a clienților care suportă **WPA-PSK** și a celor care suportă **WPA2-PSK**. Punctul de acces negociază automat cu fiecare client cel mai bun protocol suportat. Această opțiune este utilă în rețelele cu dispozitive eterogene, unde coexistă echipamente vechi alături de unele moderne. Dezavantajul este că nivelul general de securitate al rețelei este limitat de cel mai slab protocol acceptat.

- **WPA3-SAE**

  WPA3-SAE utilizează mecanismul de autentificare SAE (Simultaneous Authentication of Equals), care înlocuiește handshake-ul PSK (Pre-Shared Key) din WPA2 cu un schimb criptografic mai bun. Spre deosebire de WPA2, în care cheia de sesiune derivă direct din parola rețelei, SAE negociază o cheie de sesiune unică pentru fiecare conexiune, fără a transmite parola sau derivate ale acesteia prin aer. Aceasta elimină vulnerabilitatea la atacurile de tip dicționar offline — chiar dacă un atacator captează handshake-ul, nu poate recupera parola prin forță brută ulterior. În plus, cu **WPA3-SAE** activat, chiar dacă parola rețelei este compromisă la un moment dat, traficul capturat anterior nu poate fi decriptat.

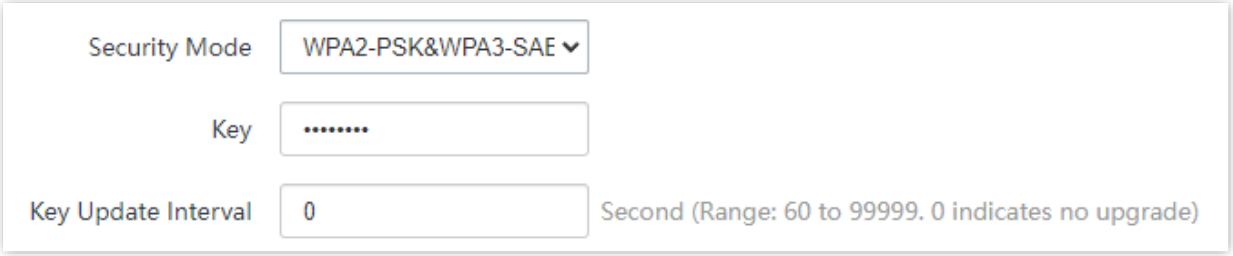
  Tip

  Dacă clienții dumneavoastră wireless nu acceptă **WPA3-SAE** sau dacă experiența Wi-Fi este nesatisfăcătoare, vă recomandăm să setați modul de securitate la **WPA2-PSK**.

- **WPA2-PSK&WPA3-SAE**

  Indică faptul că rețeaua Wi-Fi adoptă modul de criptare mixt WPA2-PSK/AES și WPA3-SAE/AES pentru a asigura siguranța, dar și compatibilitatea.

**Descriere parametri de la Wireless > SSID**

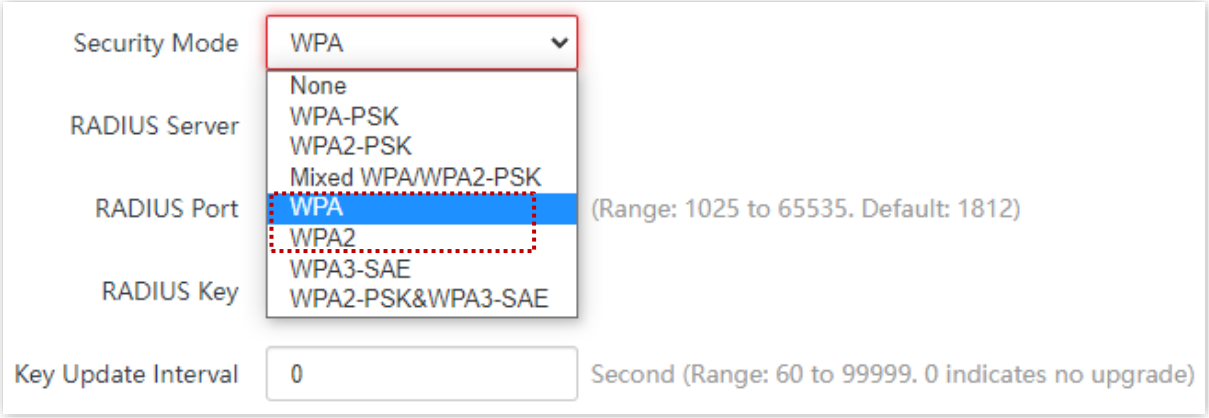
| Parametru | Descriere |
|---|---|
| **Security Mode**<br>**(Mod securitate)** | Specifică modul de securitate cu cheie personală sau pre-partajată, inclusiv **WPA-PSK, WPA2-PSK, Mixed WPA/WPA2-PSK (Mixt WPA/WPA2-PSK), WPA3-SAE** și **WPA2-PSK&WPA3-SAE.**<br>– **WPA-PSK:** Indică faptul că rețeaua Wi-Fi corespunzătoare SSID-ului selectat este criptată cu WPA-PSK.<br>– **WPA2-PSK:** Indică faptul că rețeaua Wi-Fi corespunzătoare SSID-ului selectat este criptată cu WPA2-PSK.<br>– **WPA-PSK&WPA2-PSK** sau afișat **Mixed WPA/WPA2-PSK (Mixt WPA/WPA2-PSK):** Indică faptul că clienții wireless se pot conecta la rețeaua Wi-Fi corespunzătoare SSID-ului selectat utilizând fie WPA-PSK, fie WPA2-PSK.<br>– **WPA3-SAE:** Indică faptul că rețeaua Wi-Fi corespunzătoare SSID-ului selectat este criptată cu WPA3-SAE.<br>– **WPA2-PSK&WPA3-SAE:** Rețeaua Wi-Fi adoptă modul de criptare mixt WPA2-PSK/AES și WPA3-SAE/AES pentru a asigura siguranța. |
| **Key**<br>**(Cheie)** | Specifică o cheie pre-partajată, adică parola pe care clienții o utilizează pentru a se conecta la rețeaua Wi-Fi. |
| **Key Update Interval**<br>**(Interval actualizare cheie)** | Reprezintă intervalul de timp, în secunde, la care punctul de acces regenerează automat cheile de criptare de grup GTK (Group Temporal Key) utilizate pentru traficul broadcast și multicast din rețeaua Wi-Fi.<br>În rețelele criptate există două tipuri de chei de criptare, adică tipuri de parole:<br>– PTK (Pairwise Transient Key) e cheia (parola) individuală, unică pentru fiecare client, folosită pentru traficul unicast (între AP și client).<br>– GTK (Group Temporal Key) e cheia (parola) comună, partajată de toți clienții conectați la același SSID, folosită însă doar pentru traficul broadcast sau multicast.<br>Parametrul **Key Update Interval (Interval actualizare cheie)** controlează frecvența cu care GTK este regenerată și redistribuită clienților conectați.<br>Valoarea **0** indică faptul că nu este actualizată. |

- **WPA** și **WPA2**

Pentru a remedia slăbiciunile de gestionare a cheilor din **WPA-PSK** și **WPA2-PSK**, Wi-Fi Alliance a introdus **WPA** și **WPA2**. Acestea folosesc standardul 802.1x pentru autentificarea clienților și pentru generarea unor chei rădăcină dedicate criptării datelor, înlocuind cheile pre-partajate setate manual, dar păstrând același proces de criptare ca **WPA-PSK** și **WPA2-PSK**.

Deoarece **WPA** și **WPA2** folosesc 802.1x pentru autentificare, datele de conectare ale fiecărui client sunt gestionate individual de către acesta, ceea ce reduce semnificativ riscul de scurgere a informațiilor. În plus, de fiecare dată când un client se conectează la un punct de acces în mod **WPA** sau **WPA2**, serverul **RADIUS** generează o cheie unică de criptare și o atribuie clientului, ceea ce îngreunează interceptarea ei de către atacatori. Aceste caracteristici cresc semnificativ

securitatea rețelei, motiv pentru care **WPA** și **WPA2** sunt modurile de securitate preferate pentru rețelele Wi-Fi care necesită un nivel ridicat de protecție.

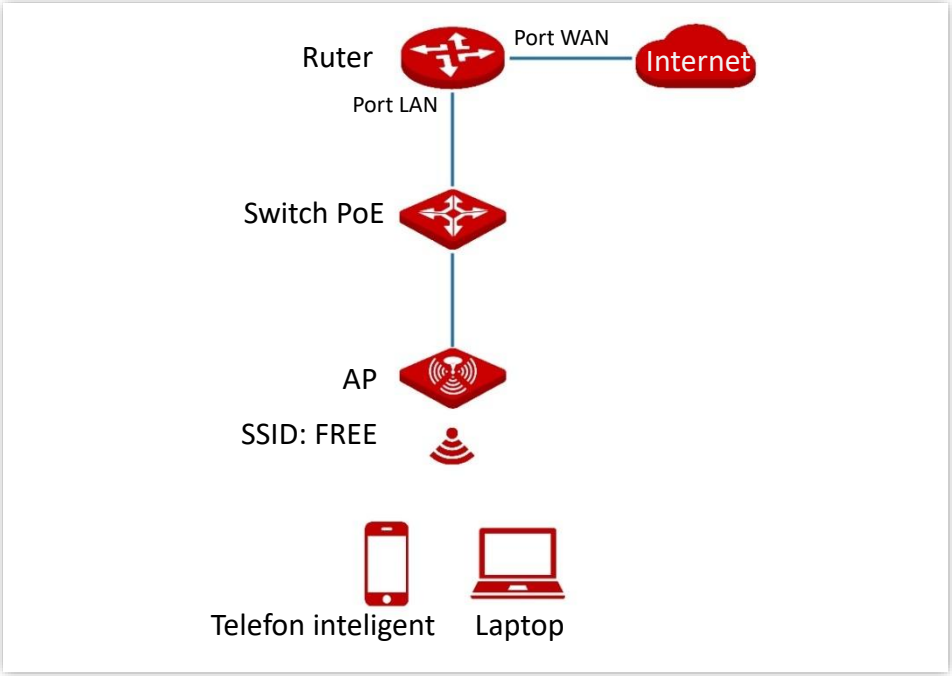



### Descriere parametri de la Wireless > SSID

| Parametru | Descriere |
|---|---|
| **Security Mode**<br>**(Mod securitate)** | Opțiunile **WPA** și **WPA2** sunt disponibile pentru protecția rețelei cu un server RADIUS.<br>– **WPA:** Indică faptul că rețeaua Wi-Fi corespunzătoare SSID-ului selectat este criptată cu WPA.<br>– **WPA2:** Indică faptul că rețeaua Wi-Fi corespunzătoare SSID-ului selectat este criptată cu WPA2. |
| **RADIUS Server**<br>**(Server RADIUS)** | Specifică adresa IP a serverului RADIUS pentru autentificarea clientului.<br>Un server *RADIUS (Remote Authentication Dial-In User Service)* este un serviciu extern de autentificare, autorizare și contorizare *(AAA — Authentication, Authorization, Accounting)* la care punctul de acces deleagă verificarea identității utilizatorilor care încearcă să se conecteze la rețeaua Wi-Fi. |
| **RADIUS Port**<br>**(Port RADIUS)** | Specifică numărul de port logic UDP al serverului RADIUS pentru autentificarea clientului.<br>Portul UDP folosit pentru autentificare poate fi în general **1812**. |
| **RADIUS Key**<br>**(Cheie RADIUS)** | Cheia (parola) comună între AP și serverul RADIUS, folosită pentru autentificarea reciprocă a celor două dispozitive. |

## 6.1.3 Exemplu configurare rețea Wi-Fi deschisă, fără parolă

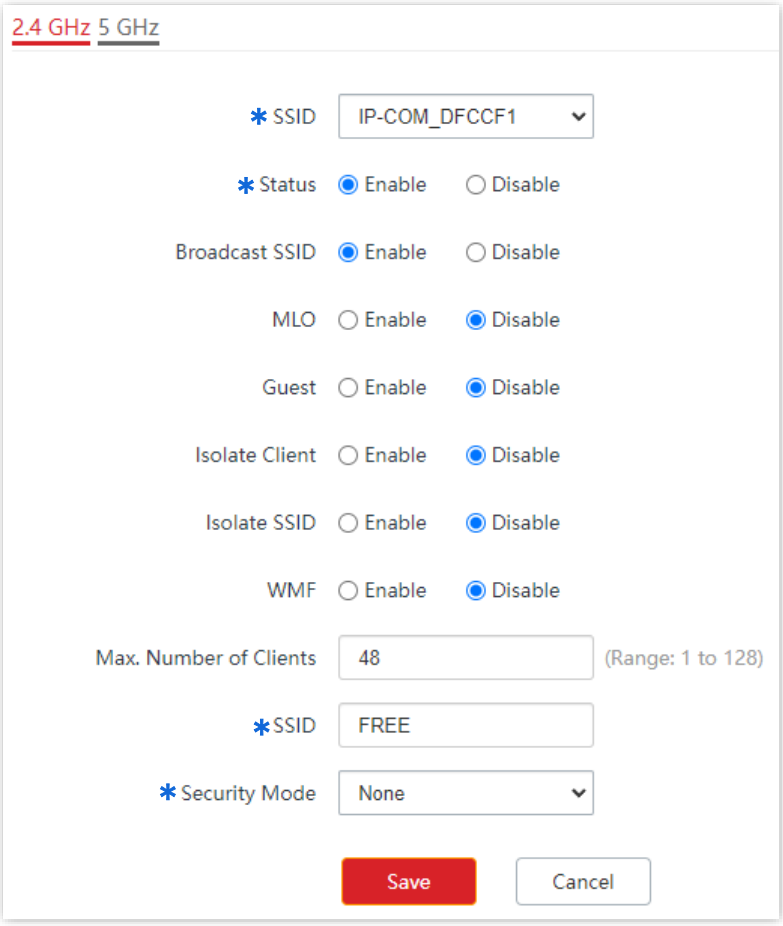
Să presupunem că într-un hotel, se dorește ca invitații să se poată conecta la rețeaua Wi-Fi fără parolă și să poată accesa internetul prin intermediul rețelei Wi-Fi.




**Procedură pentru configurarea unei rețele Wi-Fi fără parolă**

Presupunem că urmează să fie configurat un al doilea SSID pe banda de 2,4 GHz.

1. Conectați-vă la interfața web a punctului de acces.
2. Navigați la **Wireless** > **SSID.**
3. Asigurați-vă că sunteți în fila **2,4 GHz**.
4. Selectați al doilea SSID din lista derulantă **SSID.**
5. Setați **Status (Stare)** pe **Enable (Activare)**.
6. La câmpul editabil **SSID** introduceți textul **FREE.**
7. La **Security Mode (Mod securitate)** selectați **None (Fără)** din listă.
8. Faceți clic pe **Save (Salvare).**



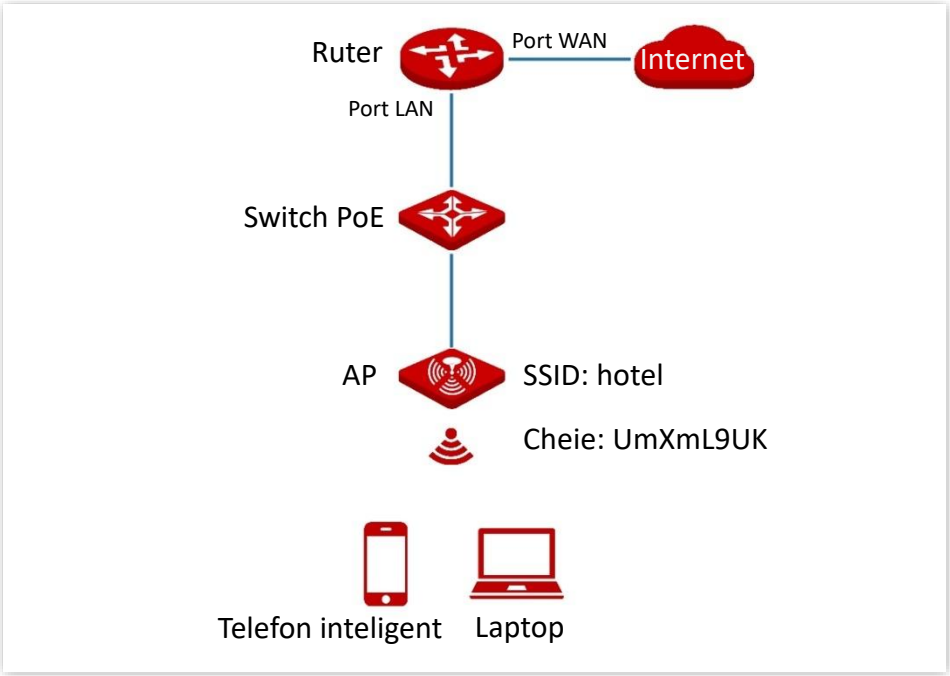

9. Verificați dacă dispozitivele compatibile Wi-Fi se pot conecta la rețeaua Wi-Fi cu denumirea **FREE** fără parolă.

**---Sfârșit**

## 6.1.4 Exemplu configurare rețea Wi-Fi criptată cu PSK

Se presupune că se dorește o rețea Wi-Fi separată într-un hotel cu un anumit nivel de securitate ce trebuie configurată printr-o procedură simplă și care să asigure securitate și compatibilitate extinsă. În acest caz, se recomandă modul de securitate WPA-PSK, WPA2-PSK sau un mix între cele două WPA/WPA2-PSK.

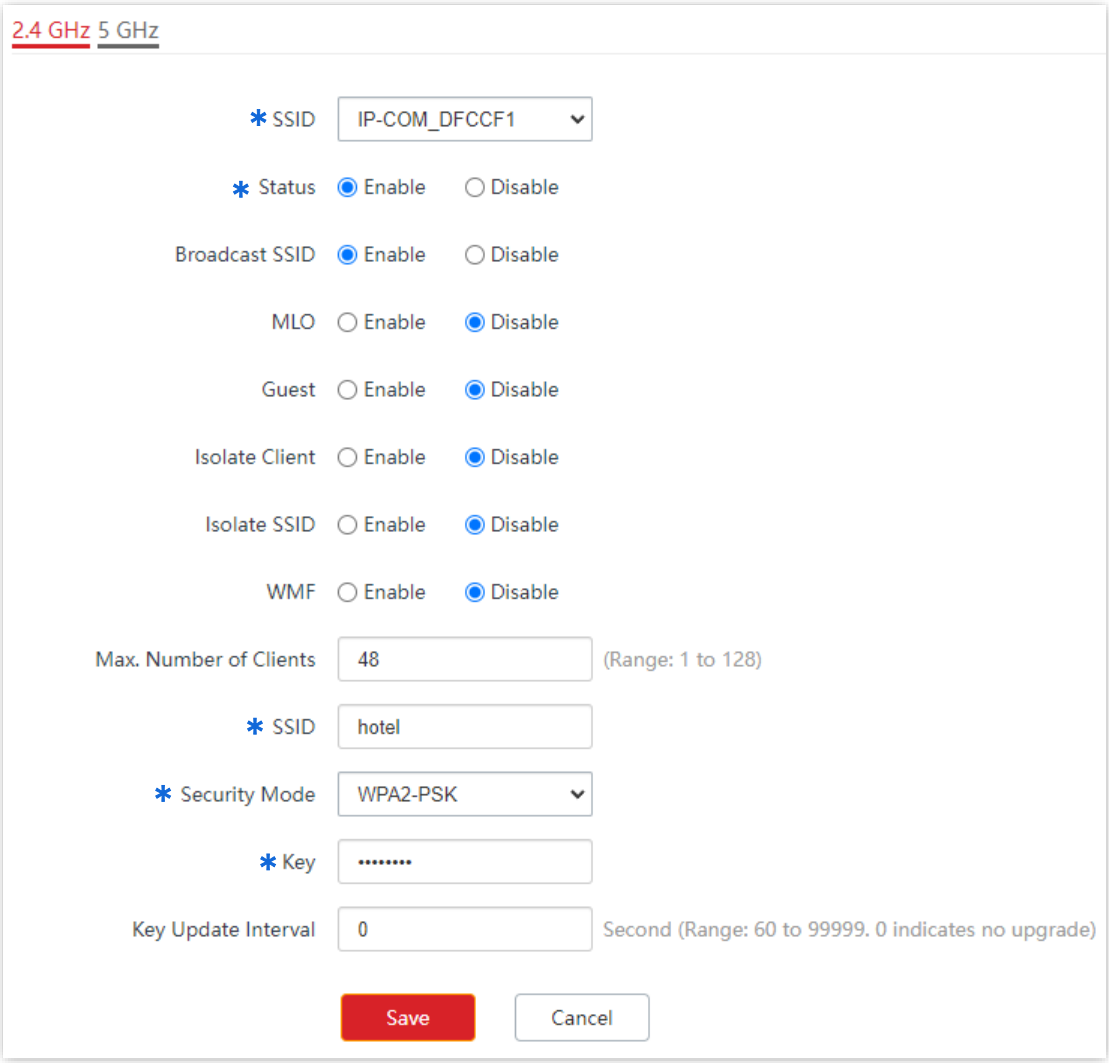
Presupunem că denumirea rețelei Wi-Fi (SSID) va fi **hotel** și parola Wi-Fi (cheia) va fi **UmXmL9UK.** Vedeți următoarea topologie.




**Procedură pentru configurarea unei rețele Wi-Fi criptate PSK**

Presupunem că urmează să fie configurat al doilea SSID de pe banda 2,4 GHz a punctului de acces.

1. Conectați-vă la interfața web a punctului de acces.
2. Navigați la **Wireless** > **SSID.**
3. Asigurați-vă că sunteți în fila **2,4 GHz**.
4. Selectați al doilea SSID din lista derulantă **SSID**.
5. Setați **Status (Starea)** pe **Enable (Activare).**
6. La câmpul **SSID** introduceți textul **hotel**.
7. Din lista de la **Security Mode (Mod securitate)**, selectați **WPA2-PSK**.
8. La **Key (Cheie)** introduceți textul **UmXmL9UK**.
9. Faceți clic pe **Save (Salvare).**




10. Verificați dacă dispozitivele compatibile Wi-Fi se pot conecta la rețeaua Wi-Fi numită **hotel** cu parola **UmXmL9UK.**

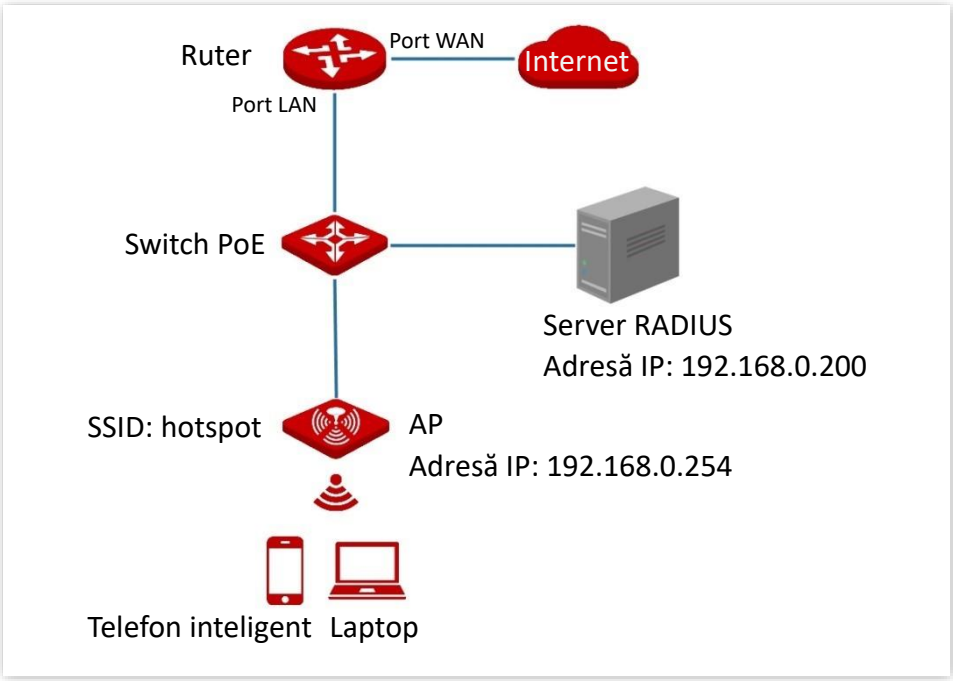
**---Sfârșit**

## 6.1.5 Exemplu de configurare a unei rețele Wi-Fi cu autentificare RADIUS și a unui server RADIUS pe Windows

Se presupune că este necesară o rețea Wi-Fi extrem de sigură și este disponibil un server RADIUS în rețeaua locală (LAN). Din diverse motive ce țin de logistica infrastructurii, se recomandă modurile de criptare WPA sau WPA2. Consultați topologia următoare.

Se presupune că:

- Denumire rețea Wi-Fi (SSID): ***hotspot***
- Adresă IP a serverului RADIUS: ***192.168.0.200***
- Port RADIUS: ***1812***
- Cheie RADIUS: ***UmXmL9UK***

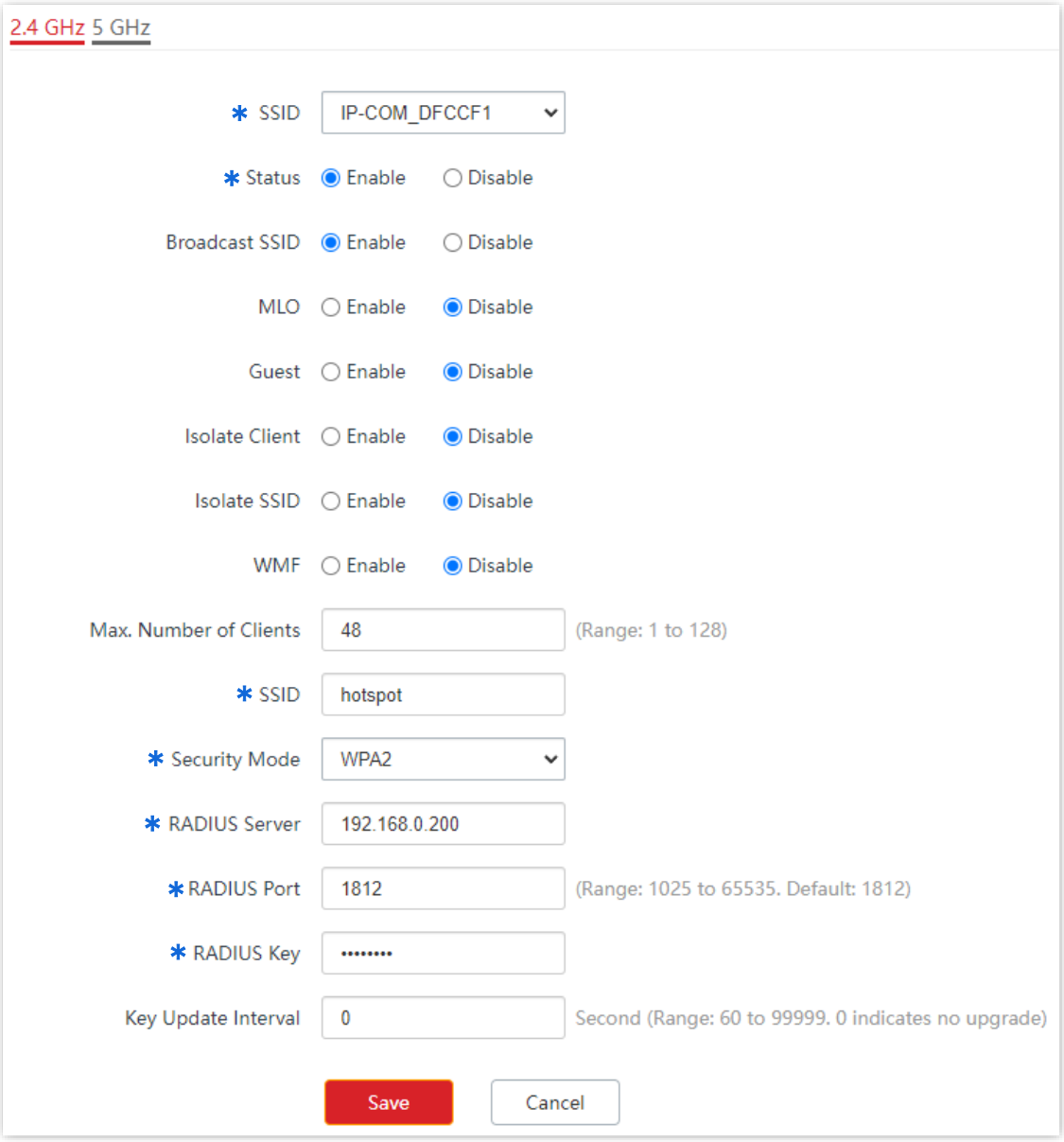



**Procedură pentru configurarea unei rețele Wi-Fi cu autentificare prin RADIUS și a serverului aferent**

**I. Configurați punctul de acces IP-COM**

Presupunem că urmează să fie configurat al doilea SSID din banda de 2,4 GHz a punctului de acces.

1. Conectați-vă la interfața web a punctului de acces.
2. Navigați la **Wireless** > **SSID.**
3. Asigurați-vă că sunteți pe fila **2,4 GHz**.
4. Selectați al doilea SSID din lista derulantă **SSID.**
5. Setați **Status (Starea)** pe **Enable (Activat).**
6. Introduceți la câmpul **SSID** textul ***hotspot*.**
7. Setați **Security Mode (Mod securitate)** pe **WPA2**.
8. La **RADIUS Server (Server RADIUS)** introduceți IP-ul serverului ***192.168.0.200***.
9. La **RADIUS Port (Port RADIUS)** introduceți portul UDP tipic, anume ***1812***.
10. La **RADIUS Key (Cheie RADIUS)** introduceți parola ***UmXmL9UK***.
11. Faceți clic pe **Save (Salvare).**




## II. Acum trebuie să configurați serverul RADIUS plus alte politici pe un server Windows

În exemplul de mai jos, configurarea serverului RADIUS și a politicilor aferente este ilustrată pe Microsoft Windows Server 2016. Pe alte versiuni de Windows, pașii concreți și denumirile opțiunilor pot diferi, însă principiul de configurare rămâne același.

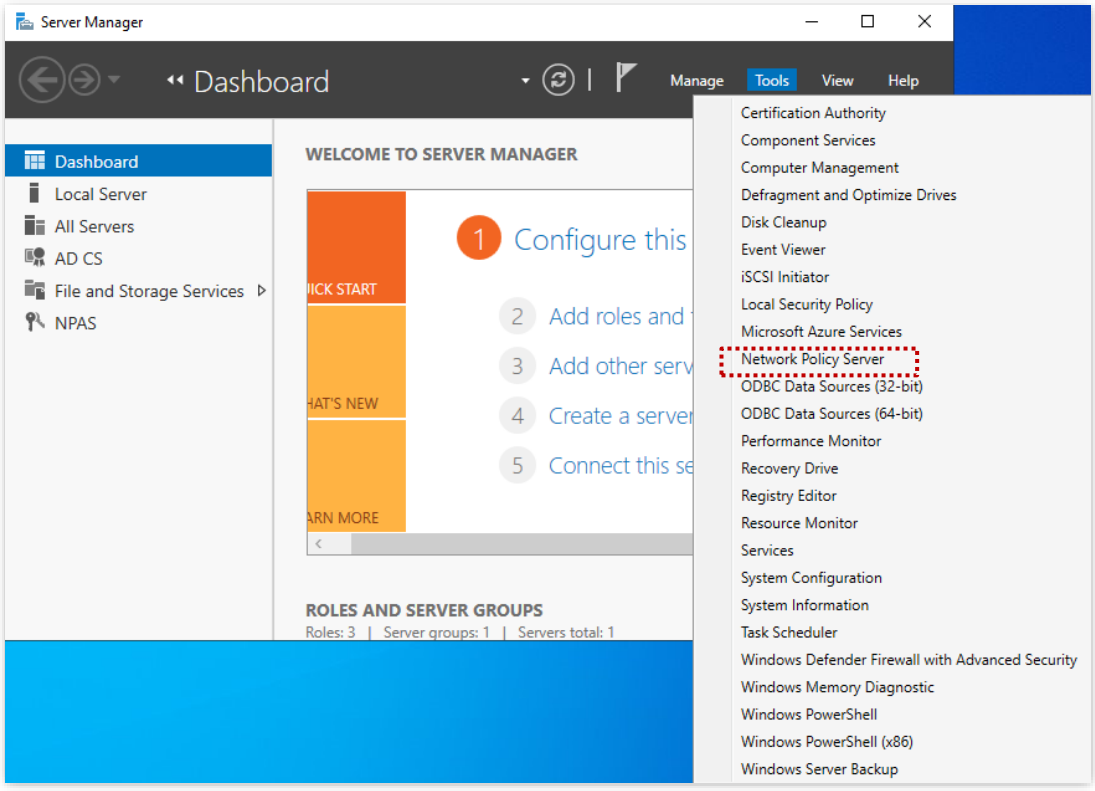
1. Trebuie să instalați serviciile **Active Directory Certificate Services** și **Network Policy and Access Services** și să implementați un certificat. Din meniul de **Start** din Windows Server căutați și deschideți **Server Manager**.

2. Din **Server Manager** accesați **Dashboard** > **Add roles and features** > **Installation Type** > selectați **Role-based or feature-based installation** > **Server Selection** > selectați serverul > **Server Roles** > bifați **Active Directory Certificate Services.**

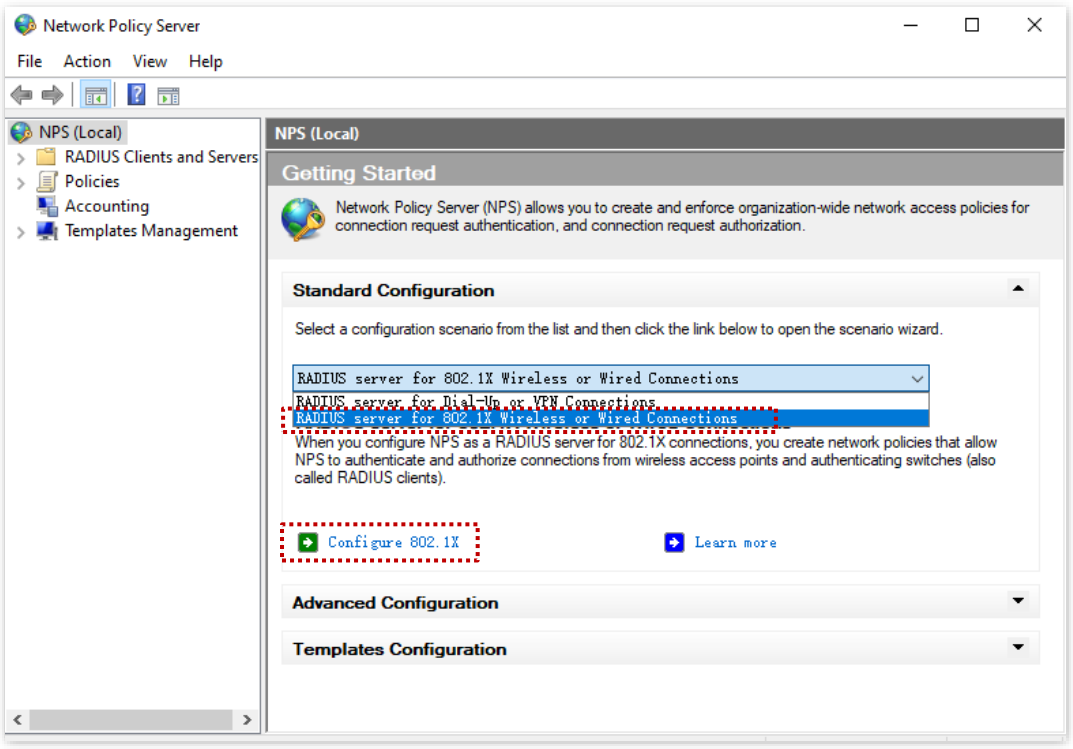
3. Conform expertului pas cu pas, instalați **Certification Authority** pentru **Active Directory Certificate Services** și **Network Policy and Access Services**.

4. După finalizarea instalării serviciului, faceți clic pe butonul din colțul din dreapta sus și urmați instrucțiunile pentru a implementa certificatul.

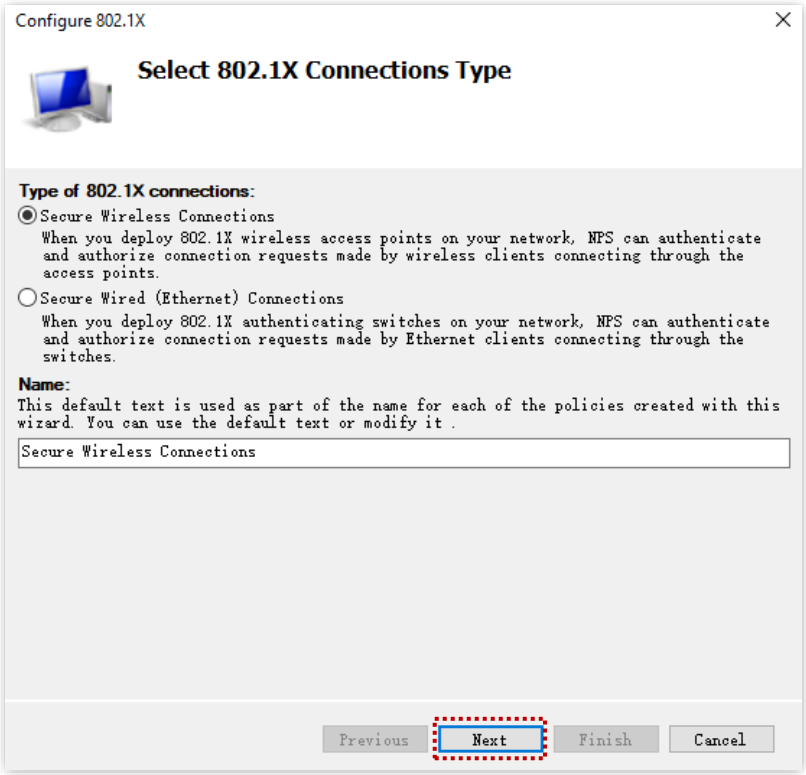
5. Acum trebuie să configurați serviciul 802.1X. În primă instanță navigați la **Start** > **Server Manager** > **Dashboard** și faceți clic pe meniul **Tools** de sus. Apoi clic pe **Network Policy Server**.




6. Selectați **RADIUS server for 802.1X Wireless or Wired Connection** de la secțiunea **Standard Configuration** și mai jos faceți clic pe **Configure 802.1X**.

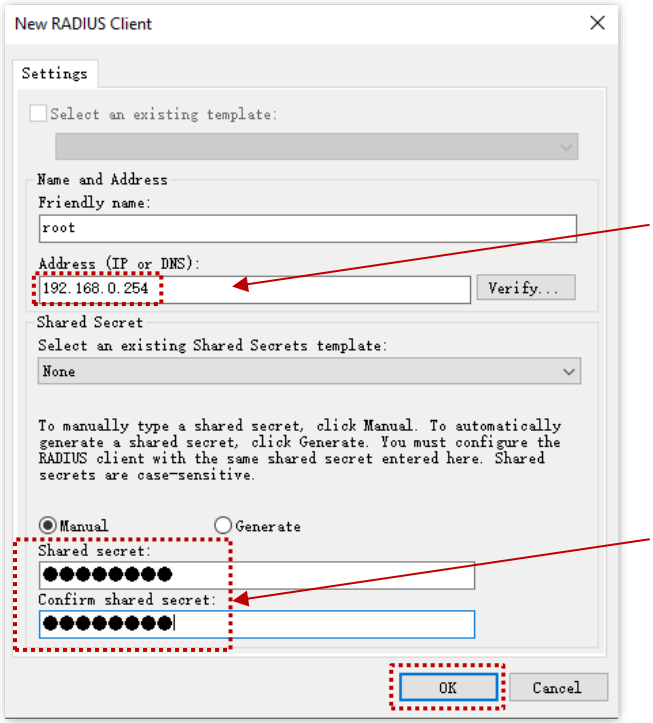



7. Selectați **Secure Wireless Connections** pentru **Type of 802.1X connections**. Modificați numele după cum este necesar, care în acest exemplu este *Secure Wireless Connections*, și faceți clic pe **Next**.




8. În fereastra **Specify 802.1X Switches**, faceți clic pe **Add (Adăugare).**

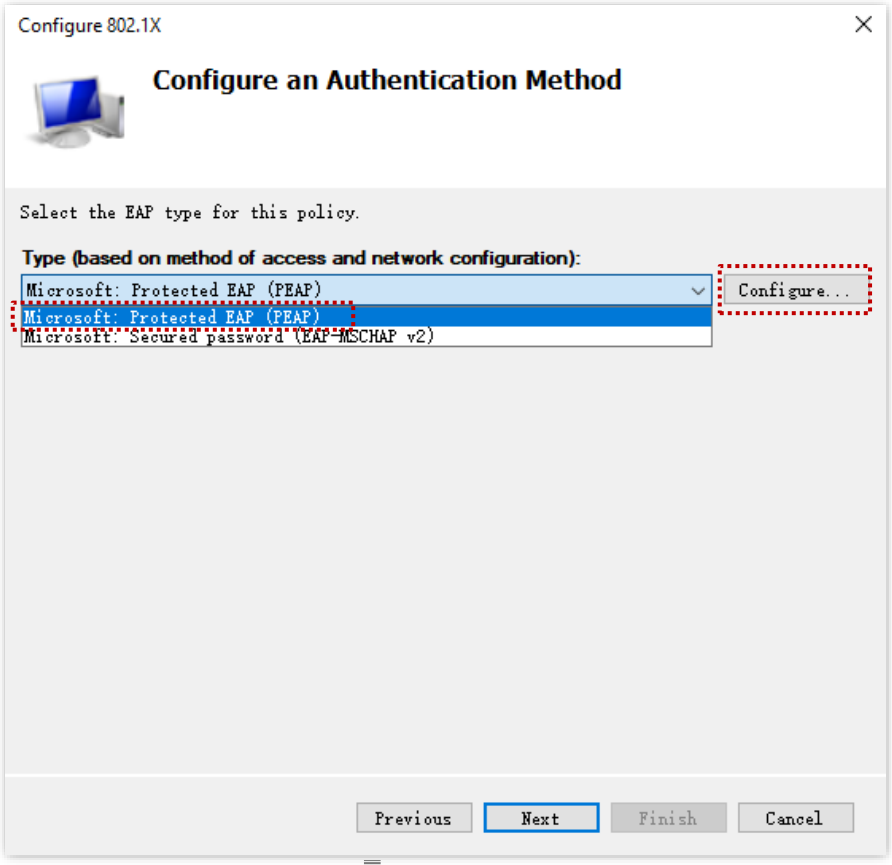
9. Introduceți un nume la **Friendly name** și adresa IP a punctului de acces IP-COM. Introduceți parola *UmXmL9UK* în casetele text **Shared secret** și **Confirm shared secret**. Apoi faceți clic pe **OK**.

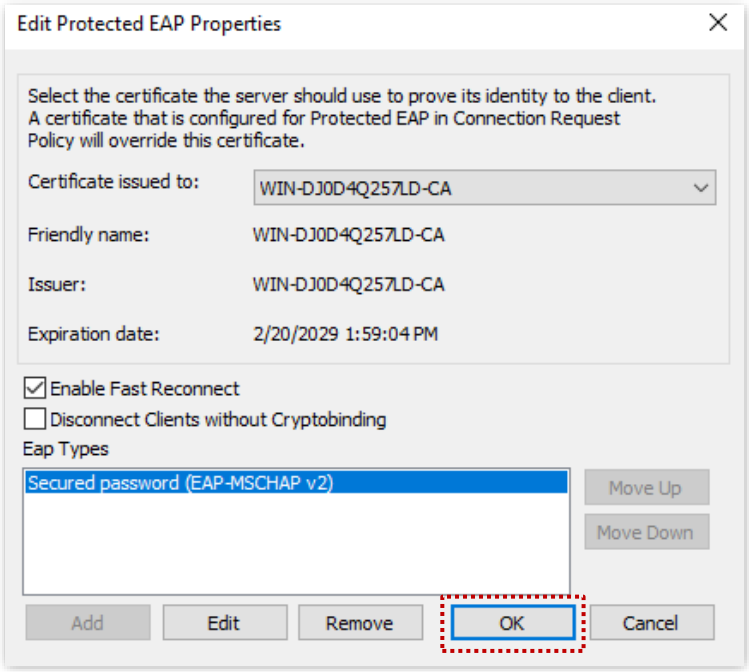



Adresa IP a punctului de acces.

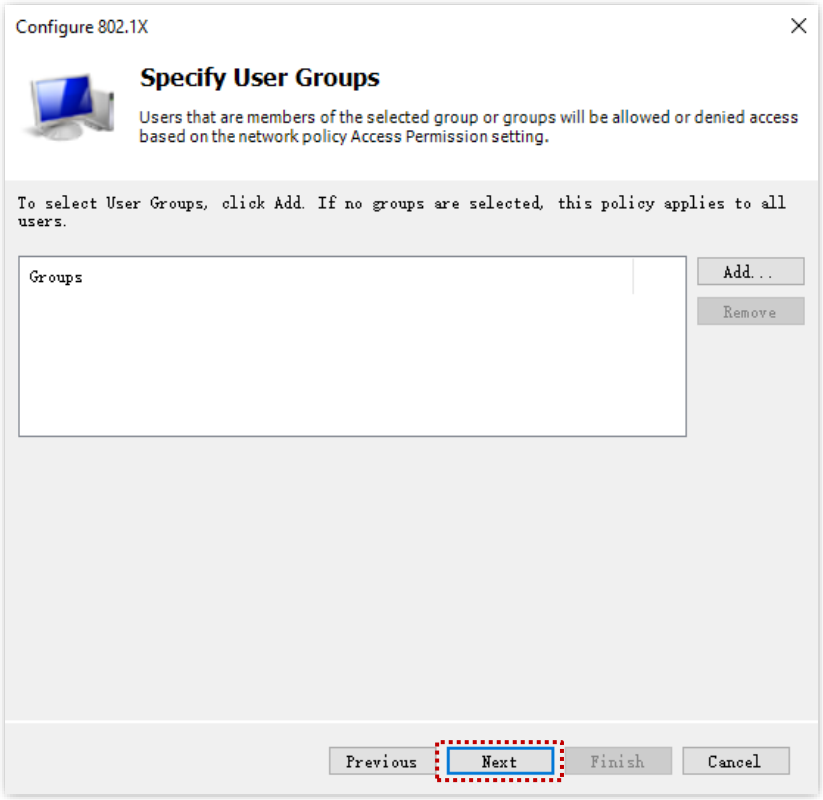
Același cu cel specificat la câmpul **RADIU Key (Cheie RADIUS)** din interfața punctului de acces IP-COM.

10. Selectați **Microsoft: Protected EAP (PEAP)** din lista de la **Type** și faceți clic pe butonul Configure. Selectați certificatul implementat în autoritatea de certificare din pașii anteriori. Apoi faceți clic pe **OK** și pe **Next** după finalizarea configurării.

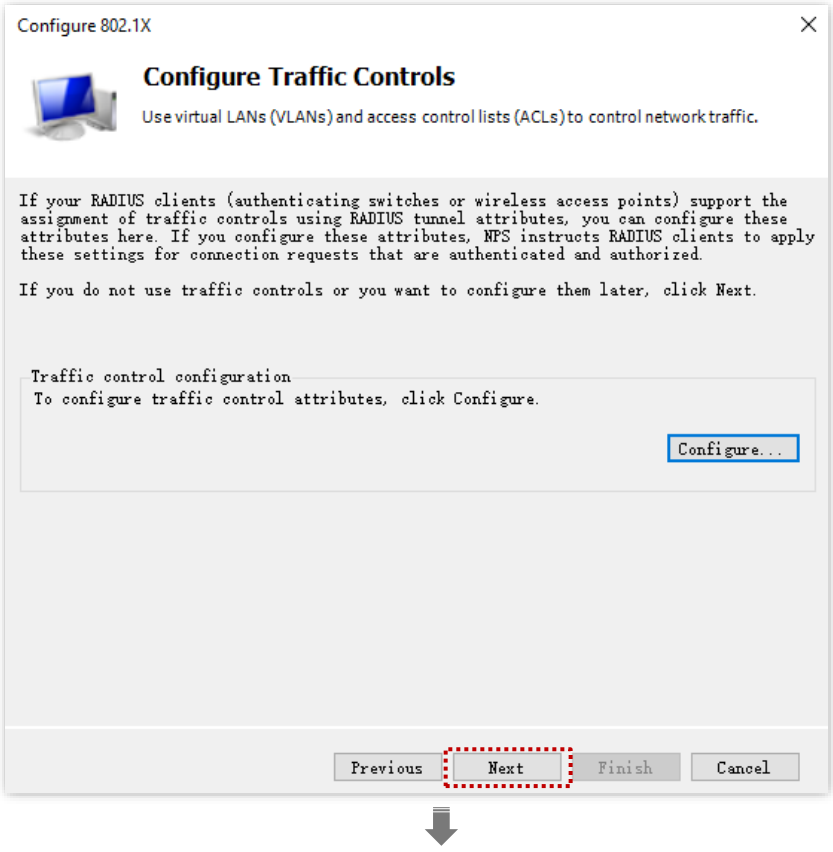


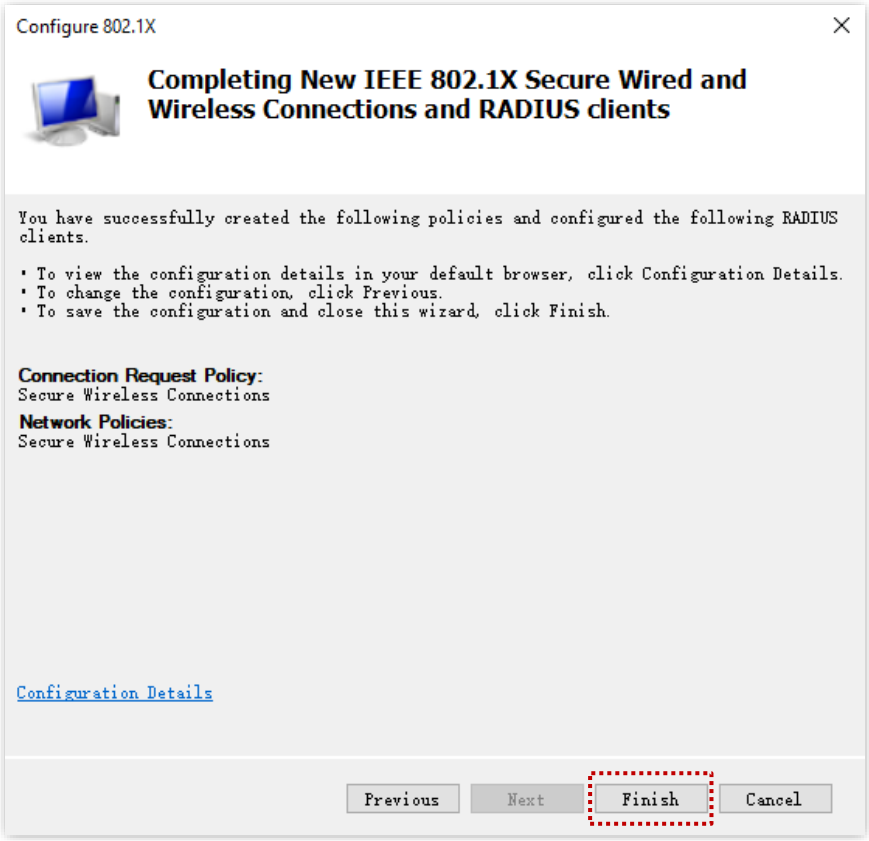




**11.** Faceți clic pe **Next** din fereastra **Specify User Groups.**




**12.** Pe pagina **Configure Traffic Controls** configurați parametrii după cum este necesar și recomandat de politica implementată de administratorul de rețea, faceți clic pe **Next** și apoi pe **Finish**.

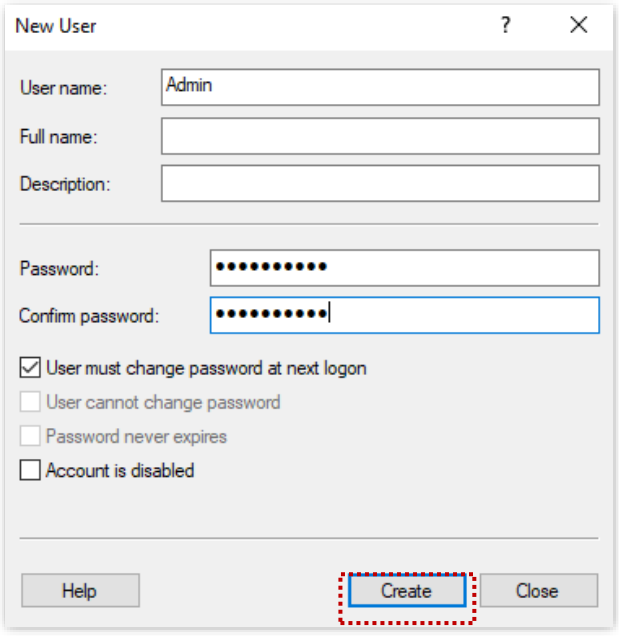





### III. Creați conturile de autentificare și unele politici

1. Acum trebuie să configurați utilizatorul (sau utilizatorii dacă doriți mai mulți) și grupul de utilizatori în care trebuie adăugat. Pentru început creați un utilizator, astfel, navigați la **Start** > **Server Manager** > **Dashboard**. Faceți clic pe **Tools** de sus, faceți clic pe **Computer Management** și faceți dublu clic pe **Local Users and Groups**.

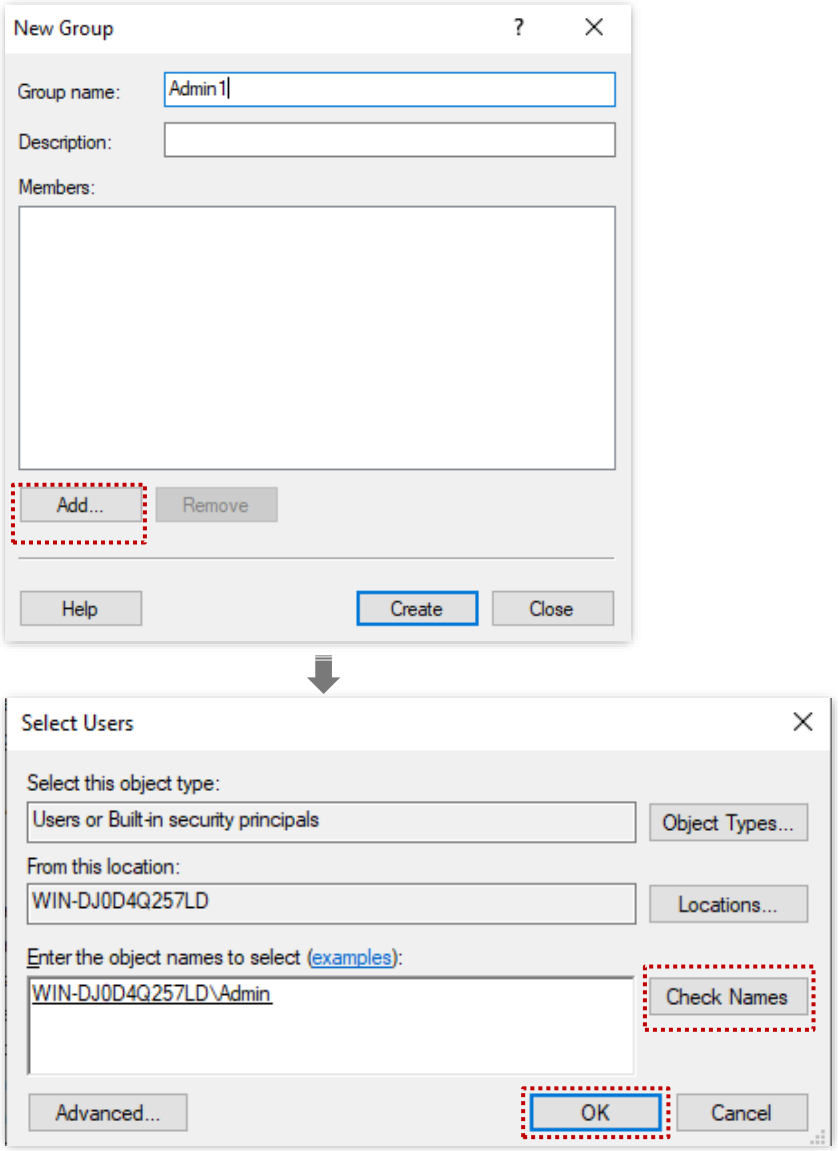
2. Faceți clic dreapta pe **Users** și clic pe **New User**. Introduceți numele de utilizator și parola, care în acest exemplu sunt ***Admin*** ca nume de utilizator și ***JohnDoe123*** pentru parolă. Apoi faceți clic pe **Create**.



3. Acum creați un grup de utilizatori în care va fi adăugat acest cont nou creat. Pentru asta, faceți clic dreapta pe **Groups** și selectați **New Group**. La **Group name** introduceți ca exemplu ***Admin1 și faceți*** clic pe **Add.**

4. În noua fereastră în câmpul **Enter the object names to select**, tastați numele de utilizator creat și faceți clic pe butonul din dreapta **Check Names** și apoi pe **OK**.

5. La final, în fereastra **New Group** faceți clic pe butonul **Create**.



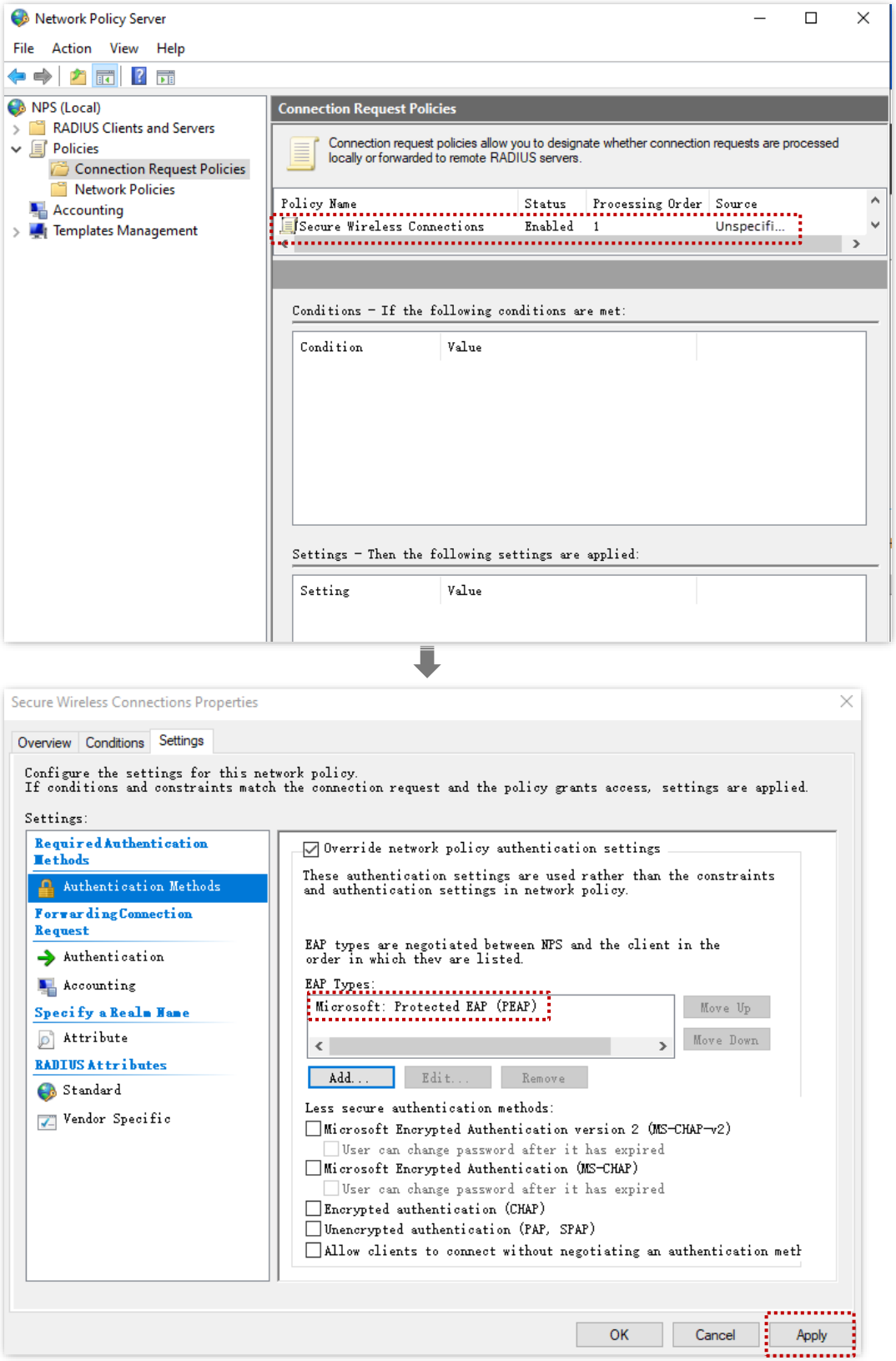

6. Acum trebuie să configurați politicile de rețea pe Windows Server. Navigați din nou la **Start** > **Server Manager** > **Dashboard** și faceți clic pe meniul de sus **Tools**.

7. Faceți clic pe **Network Policy Server** și faceți dublu clic pe **Policies.**

8. Faceți clic pe **Connection Request Policies** și faceți dublu clic pe **Secure Wireless Connections**.

9. În fereastra **Secure Wireless Connections Properties** faceți clic pe **Settings** și bifați **Override network policy authentication settings.**

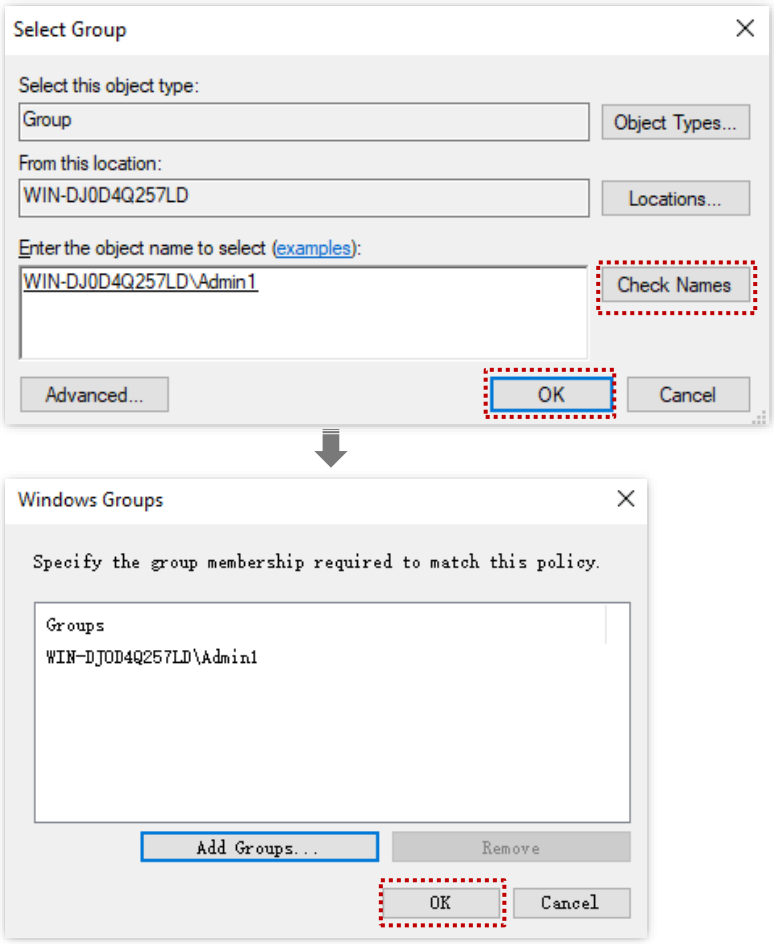
10. Faceți clic pe **Add**, adăugați **Microsoft: Protected EAP (PEAP)** în secțiunea **EAP Types** și faceți clic pe **Apply**.




11. Apoi faceți clic pe **Network Policies**, de unde faceți dublu clic pe **Secure Wireless Connections**.

12. În fereastra **Secure Wireless Connections Properties**, faceți clic pe fila **Conditions** și apoi pe butonul **Add**. Din fereastra **Select condition**, selectați **Windows Groups** și faceți clic pe **Add**. Introduceți numele grupului de utilizatori creat anterior și faceți clic pe **Check Names** pentru a valida.

13. Faceți clic pe butonul **OK**, apoi din nou pe **OK** și la final pe **Apply**.



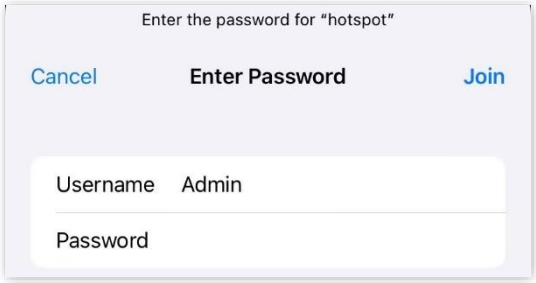

## IV. Acum configurați dispozitivul client care se va conecta prin RADIUS la rețeaua Wi-Fi

Un telefon inteligent cu sistem iOS este folosit ca exemplu.

1. Atingeți pictograma de setări de pe telefon.
2. Atingeți **WLAN** și conectați telefonul inteligent la rețeaua Wi-Fi a punctului de acces, care în acest exemplu este denumită ***hotspot*.**
3. O fereastră ce vă cere un utilizator și o parolă este afișată. Introduceți numele de utilizator și parola create anterior pe serverul Windows, apoi atingeți butonul **Join.**

Tip

Dacă apare o fereastră pop-up care întreabă dacă certificatul este de încredere, atingeți **Trust.**



4. La final verificați dacă telefonul se poate conecta la rețeaua Wi-Fi numită ***hotspot*** și are acces la internet.




Tip

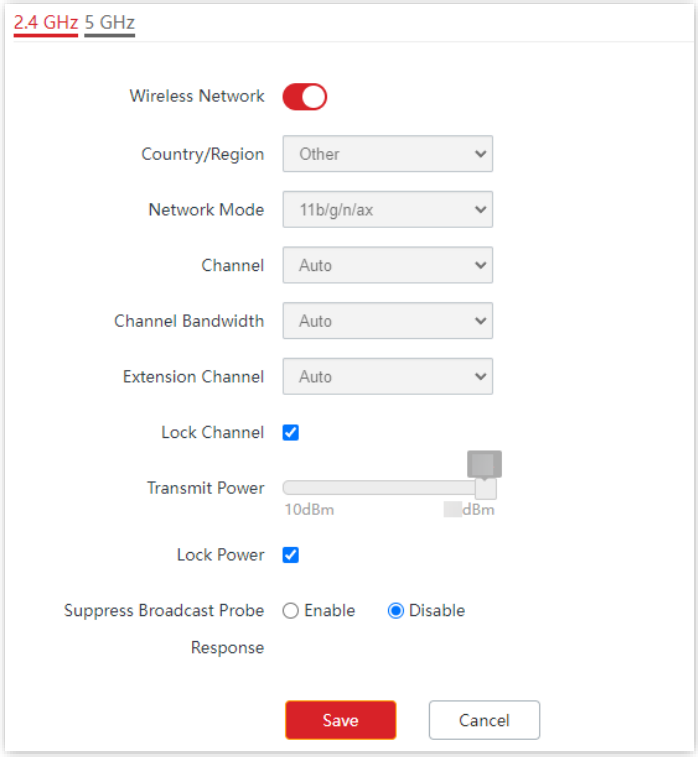
Dacă conexiunea eșuează, vă rugăm:

- Asigurați-vă că serverul RADIUS și punctul de acces pot comunica normal. Trimiteți comenzi ping unul către celălalt.
- Încercați să modificați setările de firewall de pe serverul unde e instalat serviciul RADIUS. Adăugați reguli de intrare și ieșire pentru a permite conectarea porturilor logice *1812, 1813, 1645, 1646* pe TCP și UDP.

**---Sfârșit**

# 6.2 Submeniul RF Settings (Setări radiofrecvențe)

Pentru a accesa **RF Settings (Setări radiofrecvențe)**, conectați-vă la interfața web și navigați la **Wireless** > **RF Settings (Setări radiofrecvențe)**. Puteți modifica parametrii radio de bază pe fiecare bandă.



### Descriere parametri Wireless > RF Settings (Setări radiofrecvențe)

| Parametru | Descriere |
|---|---|
| Fila **2,4 GHz**<br>Fila **5 GHz** | Utilizat pentru a selecta banda radio pentru care urmează să fie modificate setările. |
| **Wireless Network**<br>**(Rețea wireless)** | Specifică dacă se activează funcția de rețea Wi-Fi pe banda respectivă. Această setare se aplică pentru toate SSID-urile din bandă. |
| **Country/Region (Țară/Regiune)** | Specifică țara sau regiunea în care este utilizat punctul de acces. Acest parametru ajută la respectarea reglementărilor privind canalele radio din țara sau regiunea respectivă.<br>În listă găsiți majoritatea țărilor și regiunilor, inclusiv România.<br>Acest parametru poate fi setat dacă nu este selectată opțiunea **Lock Channel (Blocare canal)**. |
| **Network Mode**<br>**(Mod rețea)** | Specifică protocoalele Wi-Fi ce pot fi utilizate pe banda respectivă și se aplică pentru toate SSID-urile de pe bandă. Acest parametru poate fi setat dacă nu este selectată opțiunea **Lock Channel (Blocare canal)**.<br>Opțiunile disponibile pentru **2,4 GHz** sunt **11b, 11g, 11b/g, 11b/g/n, 11b/g/n/ax** și **11b/g/n/ax/be, , iar opțiunile** disponibile pentru **5 GHz** sunt **11a, 11ac, 11a/n, 11a/n/ac/ax** și **11a/n/ac/ax/be.**<br>– **11b:** AP-ul emite pe banda respectivă rețea Wi-Fi conformă standardului IEEE 802.11b.<br>– **11g:** AP-ul emite pe banda respectivă rețea Wi-Fi conformă standardului IEEE 802.11g.<br>– **11b/g:** AP-ul emite pe banda respectivă rețea Wi-Fi conformă standardelor IEEE 802.11b și 802.11g.<br>– **11b/g/n:** AP-ul emite pe banda respectivă rețea Wi-Fi conformă standardelor IEEE 802.11b, 802.11g și 802.11n.<br>– **11b/g/n/ax:** AP-ul emite pe banda respectivă rețea Wi-Fi conformă standardelor IEEE 802.11b, 802.11g, 802.11n și 802.11ax.<br>– **11b/g/n/ax/be**: AP-ul emite pe banda respectivă rețea Wi-Fi conformă standardelor IEEE 802.11b, 802.11g, 802.11n, 802.11ax și 802.11be.<br>– **11a:** AP-ul emite pe banda respectivă rețea Wi-Fi conformă standardului IEEE 802.11a.<br>– **11ac:** AP-ul emite pe banda respectivă rețea Wi-Fi conformă standardului 802.11ac.<br>– **11a/n:** AP-ul emite pe banda respectivă rețea Wi-Fi conformă standardelor IEEE 802.11a și 802.11n.<br>– **11a/n/ac/ax:** AP-ul emite pe banda respectivă rețea Wi-Fi conformă standardelor IEEE 802.11a, 802.11n, 802.11ac și 802.11ax.<br>– **11a/n/ac/ax/be**: AP-ul emite pe banda respectivă rețea Wi-Fi conformă standardelor IEEE 802.11a, 802.11n, 802.11ac, 802.11ax și 802.11be. |

| Parametru | Descriere |
| --- | --- |
| **Channel**<br><br>**(Canal)** | Specifică canalul de operare pe banda selectată și se aplică pentru toate SSID-urile de pe bandă. Acest parametru poate fi setat dacă nu este selectată opțiunea **Lock Channel (Blocare canal)**.<br><br>**Auto (Automat):** Indică faptul că punctul de acces își ajustează automat canalul de operare în funcție de rețelele din jur sau diverși algoritmi.<br><br>Puteți selecta manual un **număr identificator de canal** standardizat. Acesta reprezintă o subdiviziune a benzii de frecvență, adică un interval specific în cadrul benzii de 2,4 GHz sau 5 GHz pe care punctul de acces îl folosește pentru transmisie. De exemplu, banda de 2,4 GHz are 13 canale disponibile (în Europa), iar banda de 5 GHz are un număr mult mai mare. Canalele pot diferi în funcție de model. De exemplu la *IP-COM Pro-7-Lite*, pe banda de 5 GHz se regăsesc canalele **36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161, 165**.<br><br>Dacă întâmpinați frecvent deconectări, întârzieri sau rate reduse, atunci încercați să schimbați canalul. Puteți utiliza funcția de analiză a canalelor de la rețelele Wi-Fi vecine, pe fiecare bandă, de la meniul **Wireless > Frequency Analysis (Analiză frecvențe)**, pentru a detecta canalele mai puțin utilizate și care au mai puține interferențe. |
| **Channel Bandwidth (Lățime canal)** | Specifică lățimea canalului de la **Channel (Canal)** și se aplică pentru toate SSID-urile de pe bandă. Acest parametru poate fi setat dacă nu este selectată opțiunea **Lock Channel (Blocare canal)**.<br><br>Lățimea canalului, măsurată în **MHz**, reprezintă cât de „lat" este acel interval de frecvență. Valorile uzuale sunt **20 MHz**, **40 MHz**, **80 MHz** sau **160 MHz** și influențează direct viteza și stabilitatea conexiunii: un canal mai lat permite transferuri mai rapide, dar este mai susceptibil la interferențe. Este important de reținut că lățimea canalului (MHz) nu este același lucru cu banda de frecvență (2,4 GHz sau 5 GHz), unde banda indică domeniul general de frecvențe folosit.<br><br>Lățimea unui canal poate fi:<br><br>– **20 MHz:** Indică faptul că punctul de acces poate utiliza o lățime a canalului de 20 MHz.<br>– **40 MHz:** Indică faptul că punctul de acces poate utiliza o lățime a canalului de 40 MHz.<br>– **80 MHz:** Indică faptul că punctul de acces poate utiliza o lățime a canalului de 80 MHz.<br>– **160 MHz:** Indică faptul că punctul de acces poate utiliza o lățime a canalului de 160 MHz.<br>– **Automat:** AP-ul ajustează automat lățimea canalului în funcție de interferențele din jur și în funcție de diverși algoritmi.<br><br>Tip<br><br>Lățimile pot diferi în funcție de modelele de puncte de acces. Prevalează produsul real. |

| Parametru | Descriere |
|---|---|
| **Extension Channel**<br>**(Canal extindere)** | Selectați canalul de extindere utilizat pentru a determina banda de frecvență de operare a dispozitivului atunci când se folosește o lățime de canal de **40 MHz** în modul **11n**. La o lățime de canal de **40 MHz**, dispozitivul combină canalul principal cu un canal secundar (de extensie) de câte 20 MHz fiecare. În funcție de canalul principal selectat, canalul de extensie poate fi poziționat deasupra sau dedesubtul acestuia — de exemplu, pentru canalul principal **5**, opțiunile disponibile sunt **1** (dedesubt) sau **9** (deasupra).<br><br>Această setare este relevantă doar în modul **11n**, adică când se emite o rețea Wi-Fi conformă IEEE 802.11n, pe banda de 2,4 GHz și cu lățime de canal de **40 MHz** — în celelalte moduri sau la lățimi de canal de 20 MHz, opțiunea nu are efect.<br><br>Se aplică pentru toate SSID-urile de pe banda de 2,4 GHz. Acest parametru poate fi setat dacă nu este selectată opțiunea **Lock Channel (Blocare canal)**. Această opțiune se găsește doar la fila **2,4 GHz**. |
| **Lock Channel**<br>**(Blocare canal)** | Bifați pentru a bloca modificarea setărilor **Country/Region (Țară/Regiune)**, **Network Mode (Mod rețea)**, **Channel (Canal)**, **Channel Bandwidth (Lățime canal)** și **Expansion Channel (Canal extindere)**. |
| **Transmit Power**<br>**(Putere transmisie)** | Specifică puterea de transmisie radio, a punctului de acces, pe banda selectată. Acest parametru poate fi setat dacă nu este selectată opțiunea **Lock Power (Blocare putere)**.<br><br>O putere de transmisie mai mare a punctului de acces oferă o acoperire mai largă a rețelei, însă puteți reduce ușor puterea de transmisie pentru a îmbunătăți performanța și securitatea rețelei Wi-Fi.<br><br>A se reține faptul că o putere de transmisie mai redusă prezintă mai multe avantaje: semnalul Wi-Fi nu va depăși perimetrul instituției sau spațiului deservit, reducând astfel riscul ca persoane neautorizate din exterior să detecteze rețeaua și să încerce accesarea acesteia; interferențele cu alte rețele wireless din vecinătate sunt diminuate, ceea ce îmbunătățește calitatea și stabilitatea conexiunii; consumul de energie al echipamentului este ușor redus; iar în medii cu mai multe puncte de acces, o putere mai mică previne suprapunerea excesivă a semnalelor, asigurând o distribuție mai echilibrată a clienților între acestea.<br><br>În funcție de regiune și versiune puterea maximă permisă poate varia. |
| **Lock Power**<br>**(Blocare putere)** | Specifică dacă setările curente de la **Transmit Power (Putere transmisie)** pot fi modificate. Dacă este selectată, setările nu pot fi modificate. |

| Parametru | Descriere |
| --- | --- |
| **Suppress Broadcast Probe Response**<br><br>**(Suprimare răspuns probe broadcast)** | Atunci când această opțiune este activată, punctul de acces nu mai răspunde dispozitivelor care scanează „la general" după rețele Wi-Fi disponibile, răspunzând doar clienților care solicită în mod explicit conectarea la un anumit SSID — ceea ce face rețeaua mai dificil de detectat de către scanările automate.<br><br>În mod normal, dispozitivele compatibile Wi-Fi trimit continuu pachete *Probe Request* pentru a identifica rețelele din apropiere, iar punctul de acces răspunde fiecăruia cu pachete *Probe Response* conținând toți parametrii rețelei — un proces care consumă resurse wireless considerabile, mai ales în medii cu multe dispozitive.<br><br>După activarea funcției, punctul de acces ignoră solicitările de tip broadcast (cele fără un SSID specificat) și răspunde doar dispozitivelor care cunosc deja numele rețelei, reducând astfel traficul inutil și economisind resursele wireless.<br><br>Această funcție este deosebit de utilă în medii aglomerate precum școli, hoteluri sau birouri, unde numeroase dispozitive scanează permanent rețelele disponibile. |
| **Save**<br><br>**(Salvare)** | Apăsați acest buton pentru salvarea și aplicarea locală a acestor setări. E posibil ca conexiunea să fie întreruptă. |
| **Cancel**<br><br>**(Anulare)** | Apăsați pentru a anula modificările de setări din pagină, care încă nu au fost salvate după apăsarea butonului **Save (Salvare).** |

## 6.3 Submeniul RF Optimization (Optimizare radiofrecvențe)

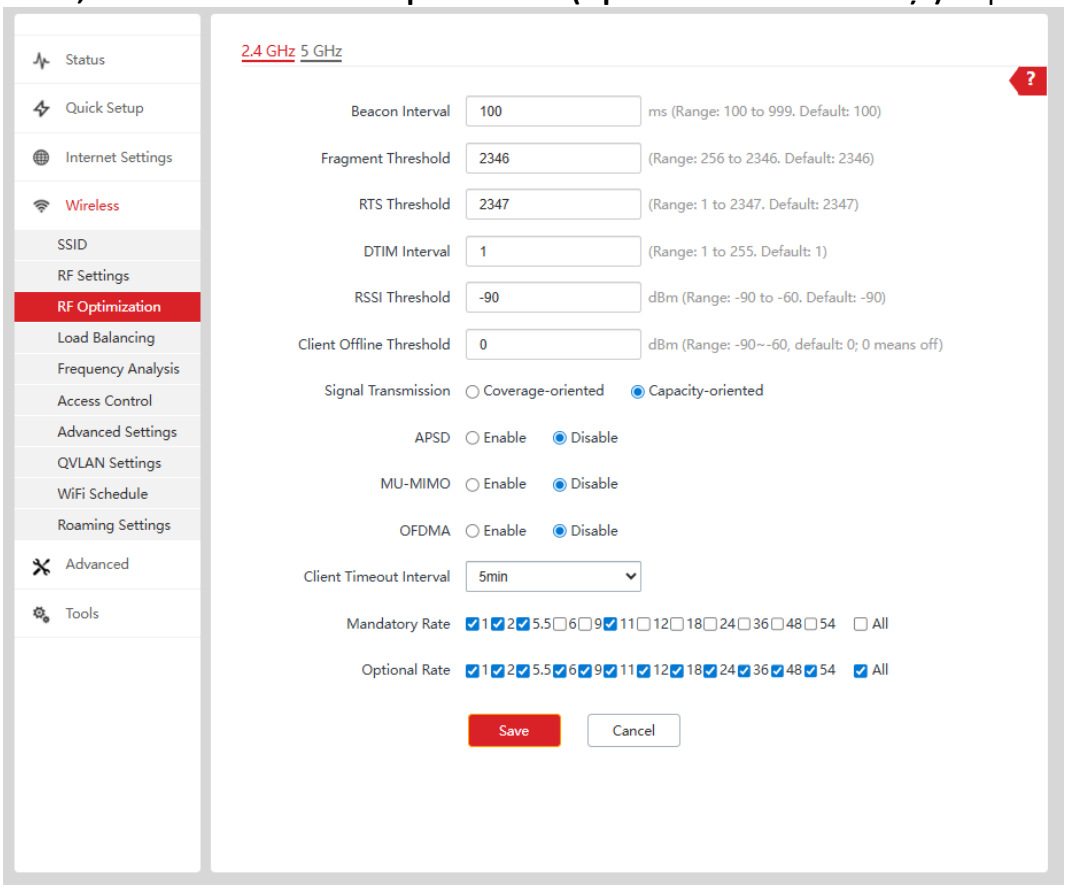
Pentru a accesa pagina de optimizare radio avansată, conectați-vă la interfața web de gestionare și navigați la **Wireless** > **RF Optimization (Optimizare radiofrecvențe)**. Puteți modifica parametrii pentru a optimiza performanța wireless.

Toate setările de aici se aplică pentru toate SSID-urile pe fiecare bandă în parte, apăsând fila **2,4 GHz** pentru banda de 2,4 GHz și fila **5 GHz** pentru banda de 5 GHz.

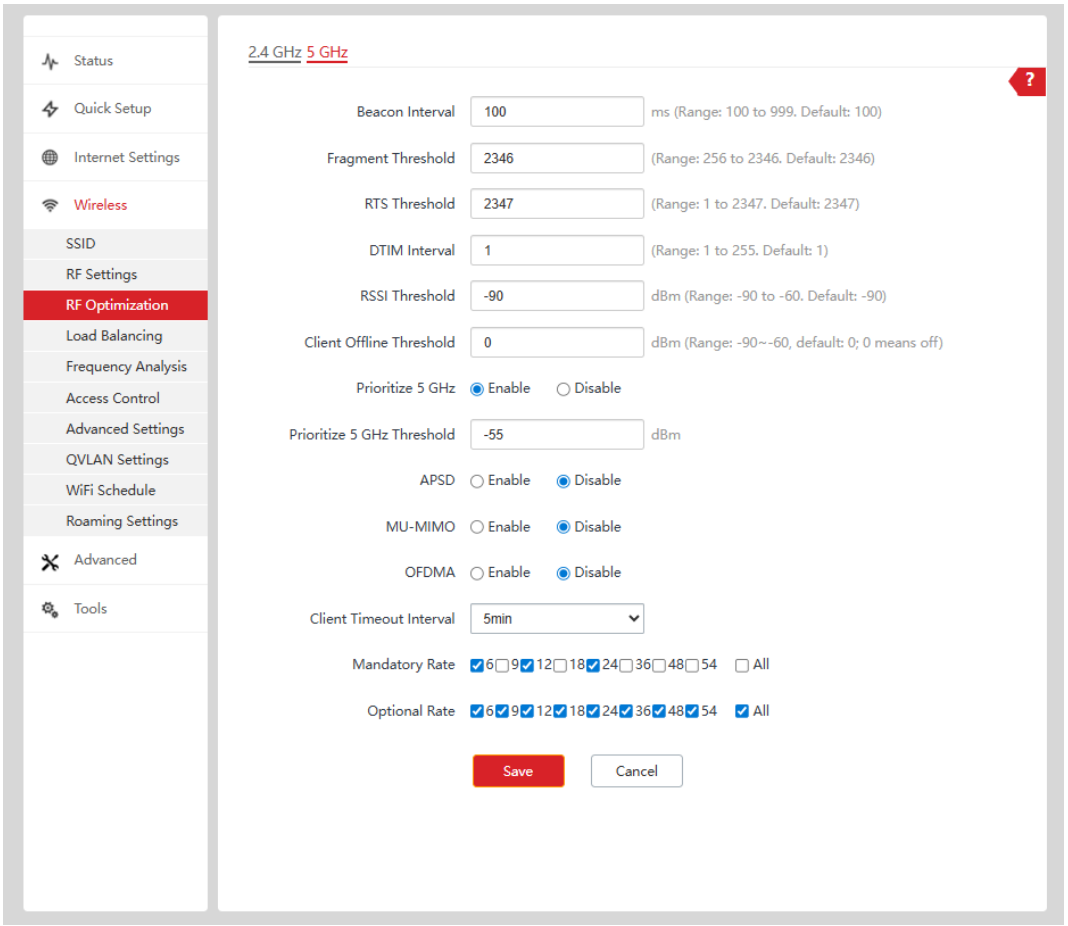
Note

Se recomandă păstrarea setărilor implicite, fără îndrumare profesională, pentru a evita reducerea performanței echipamentului.

Fila **2,4 GHz** din meniul **RF Optimization (Optimizare radiofrecvențe)** e prezentată mai jos.




Fila **5 GHz** din meniul **RF Optimization (Optimizare radiofrecvențe)** e prezentată mai jos.



### Descriere parametri Wireless > RF Optimization (Optimizare radiofrecvențe)

| Parametru | Descriere |
|---|---|
| Fila **2,4 GHz** | Utilizat pentru a selecta banda care urmează să fie configurată. |
| Fila **5 GHz** | |
| **Beacon Interval**<br>**(Interval cadre Beacon)** | Specifică intervalul de timp la care punctul de acces transmite cadre *Beacon*, măsurat în milisecunde.<br>Cadrele *Beacon* sunt pachete mici transmise periodic de către punctul de acces pentru a anunța existența rețelei Wi-Fi, conținând informații esențiale precum numele rețelei (SSID), parametrii de securitate și capacitățile suportate.<br>Un interval mai mic înseamnă că aceste cadre sunt trimise mai frecvent — dispozitivele din apropiere detectează și se conectează la rețea mai rapid, însă acest lucru consumă mai multe resurse wireless și reduce ușor lățimea de bandă disponibilă pentru transmiterea datelor.<br>Un interval mai mare reduce frecvența acestor cadre, eliberând astfel mai multe resurse pentru transmiterea efectivă a datelor și îmbunătățind debitul rețelei, însă timpul de detectare și conectare a noilor clienți wireless crește.<br>Valoarea implicită este de obicei **100** milisecunde, fiind un echilibru între durata de conectare și performanța rețelei. Se pot introduce valori între 40 și 999 de milisecunde. |
| **Fragment Threshold**<br>**(Prag de fragmentare)** | Specifică dimensiunea maximă (în octeți) a unui cadru wireless înainte ca acesta să fie divizat în fragmente mai mici. Fragmentarea este procesul prin care un cadru de dimensiuni mari este împărțit în mai multe fragmente mai mici, fiecare transmis și confirmat separat de către receptor. Dacă dimensiunea unui cadru depășește pragul setat, acesta este automat fragmentat înainte de transmitere.<br>Această setare influențează performanța rețelei în funcție de mediul în care operează punctul de acces.<br>Într-un mediu cu interferențe ridicate sau semnal slab, reducerea pragului face ca fragmentele să fie mai mici, iar în cazul unei erori de transmisie, dispozitivul retransmite doar fragmentul afectat și nu întregul cadru, reducând astfel risipa de resurse și crescând debitul efectiv al rețelei;<br>Într-un mediu cu interferențe reduse și semnal puternic, creșterea pragului reduce numărul de fragmentări și implicit numărul de confirmări necesare, ceea ce scade overhead-ul și crește debitul general al rețelei.<br>Valoarea implicită este de obicei **2346** octeți (dimensiunea maximă a unui cadru), ceea ce înseamnă că fragmentarea este practic dezactivată în condiții normale. Se poate introduce o valoare între 256 și 2346 de octeți. |

| Parametru | Descriere |
|---|---|
| **RTS Threshold**<br><br>**(Prag RTS)** | Specifică pragul, exprimat în octeți (bytes), peste care se declanșează mecanismul *RTS/CTS (Request to Send / Clear to Send)*: orice cadru mai mare decât această valoare activează mecanismul pentru a reduce conflictele.<br><br>Ajustați pragul RTS în funcție de condițiile reale ale rețelei: o valoare prea mică sporește frecvența cadrelor RTS și, implicit, lățimea de bandă consumată, însă permite rețelei Wi-Fi să se recupereze mai rapid după conflicte. În rețelele cu densitate mare de utilizatori, reducerea pragului ajută la diminuarea conflictelor.<br><br>Valoarea implicită este de obicei **2347** (practic dezactivat), iar reducerea ei (de exemplu, la **500**–**1000**) este utilă în rețele aglomerate sau cu interferențe, deoarece scade riscul coliziunilor, însă introduce overhead suplimentar de trafic de control, motiv pentru care nu se recomandă modificarea decât atunci când apar probleme reale de performanță.<br><br>Deoarece mecanismul RTS consumă lățime de bandă, acesta se activează doar pentru cadrele care depășesc pragul stabilit.<br><br>Se poate seta între 1 și 2347 de octeți. Implicit e **2347** octeți. |
| **DTIM Interval**<br><br>**(Interval DTIM)** | *DTIM Interval (Delivery Traffic Indication Message)* reprezintă numărătoarea inversă înainte ca acest echipament să transmită prin Wi-Fi cadrele broadcast și multicast aflate în memoria sa cache. Unitatea de măsură este intervalul *Beacon*. De exemplu, dacă Intervalul *DTIM* este setat la **1**, acest dispozitiv transmite toate cadrele din cache la fiecare interval *Beacon*.<br><br>Implicit **DTIM Interval (Interval DTIM)** este setat la **1**, dar poate fi setat în intervalul **1-255**. |
| **RSSI Threshold**<br><br>**(Prag RSSI)** | Pragul *RSSI (Received Signal Strength Indicator)* este un parametru care stabilește intensitatea minimă a semnalului pe care un client wireless trebuie să o aibă pentru a fi acceptat de către punctul de acces (AP). Valoarea se exprimă în **dBm** (decibeli raportați la 1 miliwatt), iar scala este negativă — cu cât valoarea este mai apropiată de zero, cu atât semnalul este mai puternic (de exemplu, **-60 dBm** înseamnă semnal bun, **-70 dBm** acceptabil, iar **-85 dBm** foarte slab). Dacă semnalul transmis de un dispozitiv (telefon, laptop) către AP este mai slab decât pragul configurat, AP-ul refuză conexiunea, forțând clientul să se conecteze la un alt punct de acces mai apropiat sau să rămână deconectat, ceea ce este util în special în rețele cu mai multe AP-uri (mesh sau roaming), unde se dorește ca dispozitivele să nu se „agațe" de un AP îndepărtat cu semnal slab, ci să comute automat către cel mai apropiat, păstrând astfel o performanță stabilă a întregii rețele.<br><br>Setarea greșită poate duce la deconectări frecvente sau imposibilitatea conectării dispozitivelor aflate în camerele mai îndepărtate.<br><br>Intervalul admis este de la **-90** până la **-60 dBm. Valoarea implicită este -90 dBm.** |

| Parametru | Descriere |
| --- | --- |
| **Client Offline Threshold (Prag deconectare client)** | Folosit pentru a seta puterea minimă a semnalului necesară unui client pentru a menține conexiunea la punctul de acces. Dacă puterea semnalului de acces al unui client scade sub pragul configurat, punctul de acces îl va deconecta.<br><br>În completare, acest prag de deconectare a clientului este un parametru care stabilește intensitatea minimă a semnalului sub care punctul de acces (AP) deconectează forțat un client deja conectat, exprimat în **dBm**, cu un interval admis între **-90 dBm** (semnal foarte slab) și **-60 dBm** (semnal bun), valoarea implicită fiind **0 dBm**, ceea ce înseamnă că funcția este dezactivată și clienții rămân conectați indiferent cât de slab devine semnalul.<br><br>Spre deosebire de **RSSI Threshold (Prag RSSI)**, care decide dacă un client se poate conecta inițial, **Client Offline Threshold (Prag deconectare client)** monitorizează permanent semnalul clienților deja conectați și îi deconectează atunci când semnalul scade sub valoarea setată — de obicei pentru că utilizatorul s-a deplasat prea departe de AP sau au apărut obstacole (pereți, mobilier, interferențe). |
| **Signal Transmission (Transmisie semnal)** | Selectați opțiunea în funcție de situația pe teren, pentru banda de 2,4 GHz.<br><br>– **Coverage-oriented (Orientat spre acoperire):** Acest mod lărgește acoperirea wireless a punctelor de acces și este de obicei utilizat în scenarii implementate cu mai puține puncte de acces.<br><br>– **Capacity-oriented (Orientat spre capacitate):** Acest mod reduce eficient interferențele reciproce dintre punctele de acces și este de obicei utilizat în scenarii implementate cu un număr mare de puncte de acces.<br><br>Tip<br><br>Această funcție este disponibilă pe unele puncte de acces. Produsul real prevalează.<br><br>Pentru a identifica setarea optimă, experimentați diferite opțiuni și monitorizați performanța rețelei Wi-Fi. |
| **APSD** | *APSD (Automatic Power Save Delivery)* este un mecanism de economisire a energiei definit în standardul Wi-Fi 802.11e, care permite dispozitivelor wireless (în special telefoane, tablete, ceasuri smart și alte aparate alimentate de la baterie) să „adoarmă" temporar interfața radio atunci când nu transmit date, și să fie „trezite" doar atunci când există trafic relevant pentru ele. |
| **MU-MIMO** | Acronim pentru *Multi-User, Multiple-Input, Multiple-Output (multi-utilizator, intrări multiple, ieșiri multiple)* — o tehnologie Wi-Fi care folosește mai multe antene pentru a transmite și recepționa date către mai mulți utilizatori în paralel.<br><br>Când funcția este activată, punctul de acces poate deservi simultan mai mulți clienți, în loc să-i servească pe rând. Astfel se reduce timpul de așteptare, se diminuează congestia rețelei Wi-Fi și crește debitul total, mai ales în mediile cu mulți utilizatori conectați simultan. |

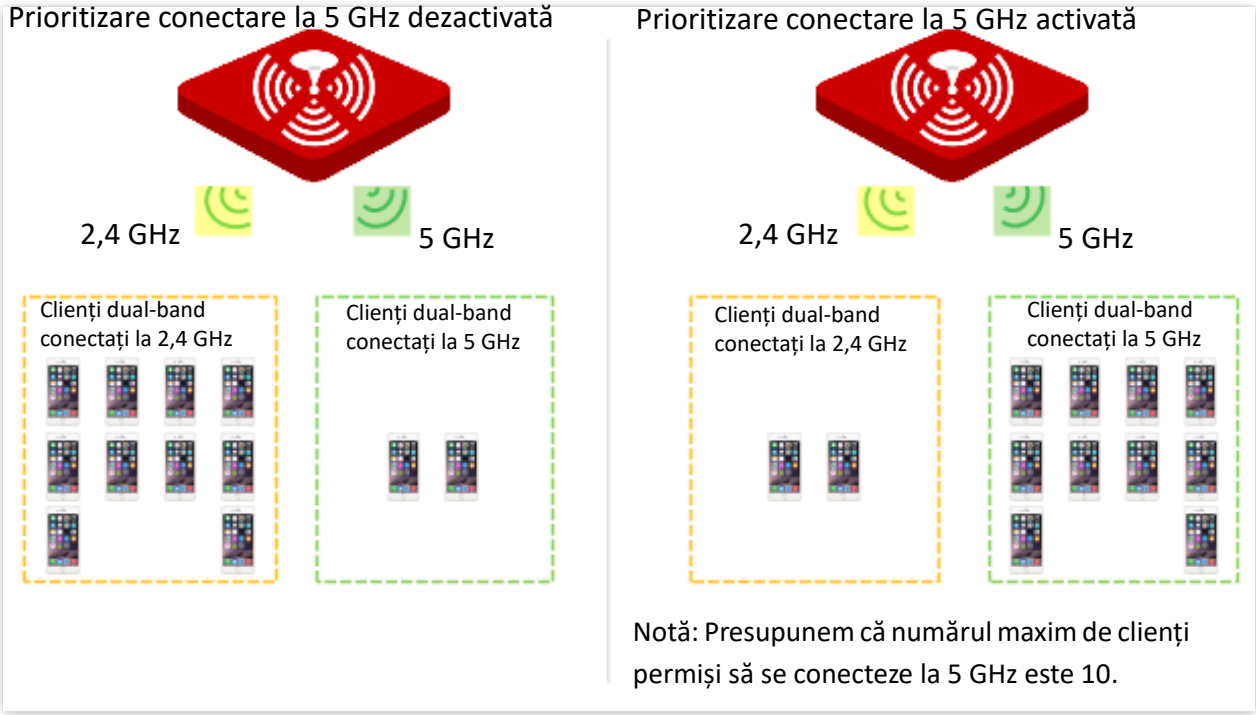
| Parametru | Descriere |
|---|---|
| **OFDMA** | Acronim pentru *Orthogonal Frequency-Division Multiple Access (acces multiplu prin diviziune ortogonală a frecvenței)* — o tehnologie care împarte canalul radio în mai multe subcanale (numite unități de resurse) și le alocă simultan mai multor clienți.<br><br>Când funcția este activată, mai mulți clienți pot transmite și recepționa date simultan, în cadrul aceluiași canal radio. Astfel, eficiența transmisiei crește, latența scade, iar experiența utilizatorului se îmbunătățește, în special în rețelele aglomerate cu trafic redus per client (mesagerie, IoT, navigare web).<br><br>Totuși, **OFDMA** este disponibil doar pe clienții compatibili cu Wi-Fi 6 și Wi-Fi 7 și, în unele cazuri, poate cauza probleme de conectivitate sau performanță cu dispozitivele mai vechi (Wi-Fi 5 sau anterior). Dacă observați astfel de probleme în rețea, se recomandă dezactivarea funcției. |
| **Client Timeout Interval (Interval expirare client)** | Punctul de acces se deconectează de la un client wireless dacă nu se transmite sau nu se primește trafic de către clientul wireless în intervalul respectiv.<br><br>O funcție utilă de alocare a resurselor.<br><br>Puteți seta o perioada de deconectare după **1 minut** sau **2**, **5**, **10**, **15**, **30** sau **60 minute**. Implicit e pe **5 minute**, depinzând de model. |
| **Mandatory Rate**<br><br>**(Rată obligatorie)** | Vitezele (ratele) pe care un client wireless trebuie obligatoriu să le suporte pentru a se putea conecta la AP. Dacă dispozitivul clientului nu suportă toate ratele bifate ca obligatorii, nu i se permite asocierea cu rețeaua. Aceste rate sunt folosite și pentru transmiterea cadrelor de management (beacon, broadcast, multicast).<br><br>Se pot selecta ratele de **1**, **2**, **5.5**, **6**, **9**, **11**, **12**, **18**, **24**, **36**, **48**, **54 Mbps** pe banda de 2,4 GHz și se pot selecta **6, 9, 12, 18, 24, 36, 48, 54** pe banda de 5 GHz. |
| **Optional Rate**<br><br>**(Rată opțională)** | Specifică ratele suplimentare acceptate de punctul de acces, care sunt opționale pentru clienții wireless.<br><br>Clienții care îndeplinesc rata obligatorie se pot conecta la punctul de acces cu o rată mai mare.<br><br>Se pot selecta ratele de **1**, **2**, **5.5**, **6**, **9**, **11**, **12**, **18**, **24**, **36**, **48**, **54 Mbps pe banda de 2,4 GHz** și se pot selecta **6, 9, 12, 18, 24, 36, 48, 54** pe banda de 5 GHz. |

| Parametru | Descriere |
| --- | --- |
| **Prioritize 5 GHz**<br><br>**(Prioritizare 5 GHz)** | Activare sau dezactivare prioritizării conectării clienților Wi-Fi pe banda de 5 GHz în detrimentul 2,4 GHz, în anumite condiții.<br><br>În mod normal, multe dispozitive aleg automat banda de 2,4 GHz pentru că aceasta are o rază de acoperire mai mare, chiar și atunci când banda de 5 GHz ar oferi viteze mult mai mari și mai puține interferențe. Cu această funcție activată, punctul de acces „împinge" activ dispozitivele conectate pe ambele benzi către banda de 5 GHz atunci când semnalul lor pe această bandă este suficient de bun — adică mai mare sau egal cu valoarea setată în **Prioritize 5 GHz Threshold (Prag prioritizare 5 GHz)**, de obicei exprimată în dBm, ex. -70 dBm.<br><br>Funcția intră în vigoare numai cu condiția ca ambele benzi de 2,4 GHz și 5 GHz să fie activate și să aibă același SSID (nume Wi-Fi), mod de securitate și parolă (cheie). |
| **Prioritize 5 GHz Threshold (Prag prioritizare 5 GHz)** | Cu această funcție activată, dacă puterea semnalelor transmise de un dispozitiv compatibil Wi-Fi este mai mare sau egală cu acest prag, dispozitivul compatibil Wi-Fi se conectează la rețeaua Wi-Fi de 5 GHz. În caz contrar, se conectează la rețeaua Wi-Fi de 2,4 GHz. Logica deciziei:<br><br>– Dacă semnalul clientului pe 5 GHz este peste prag, atunci AP-ul îl direcționează către banda de 5 GHz (viteze mai mari, mai puține interferențe).<br><br>– Dacă semnalul pe 5 GHz este sub prag (clientul este prea departe sau există obstacole), atunci AP-ul îi permite conectarea pe 2,4 GHz (rază mai mare, semnal mai stabil).<br><br>Pragul implicit este de **-55 dBm**. |

- **Funcția Prioritize 5 GHz (Prioritizare 5 GHz)**

Deși banda de 2,4 GHz este utilizată mai pe scară largă decât cea de 5 GHz în rețelele Wi-Fi reale, ea suferă de congestie și interferențe mult mai serioase, întrucât pune la dispoziție doar 3 canale nesuprapuse. În schimb, banda de 5 GHz oferă un număr considerabil mai mare de canale nesuprapuse — peste 20 în unele țări și regiuni — ceea ce permite o distribuție mult mai eficientă a traficului.

Odată cu evoluția tehnologiilor wireless, clienții care suportă ambele benzi (2,4 și 5 GHz) au devenit tot mai răspândiți. Problema este că, în mod implicit, aceste dispozitive dual-band aleg conectarea pe 2,4 GHz, ceea ce duce la o aglomerare suplimentară a acestei benzi și, în paralel, la subutilizarea benzii de 5 GHz.




Funcția rezolvă tocmai acest dezechilibru: direcționează clienții dual-band către banda de 5 GHz în momentul conectării, cu condiția ca intensitatea semnalului recepționat de punctul de acces pe această bandă să atingă sau să depășească pragul configurat. În felul acesta, banda de 5 GHz este valorificată mai eficient, banda de 2,4 GHz este descongestionată, iar experiența utilizatorului se îmbunătățește vizibil — cu viteze mai mari, latențe mai mici și mai puține interferențe

Note

Funcția de prioritizare a conectării la banda de 5 GHz intră în vigoare numai cu condiția ca ambele benzi de 2,4 GHz și 5 GHz să fie activate și ca cele două benzi să aibă același SSID (nume Wi-Fi), mod de securitate și parolă (cheie).

# 6.4 Submeniul Load Balancing (Echilibrare încărcare)

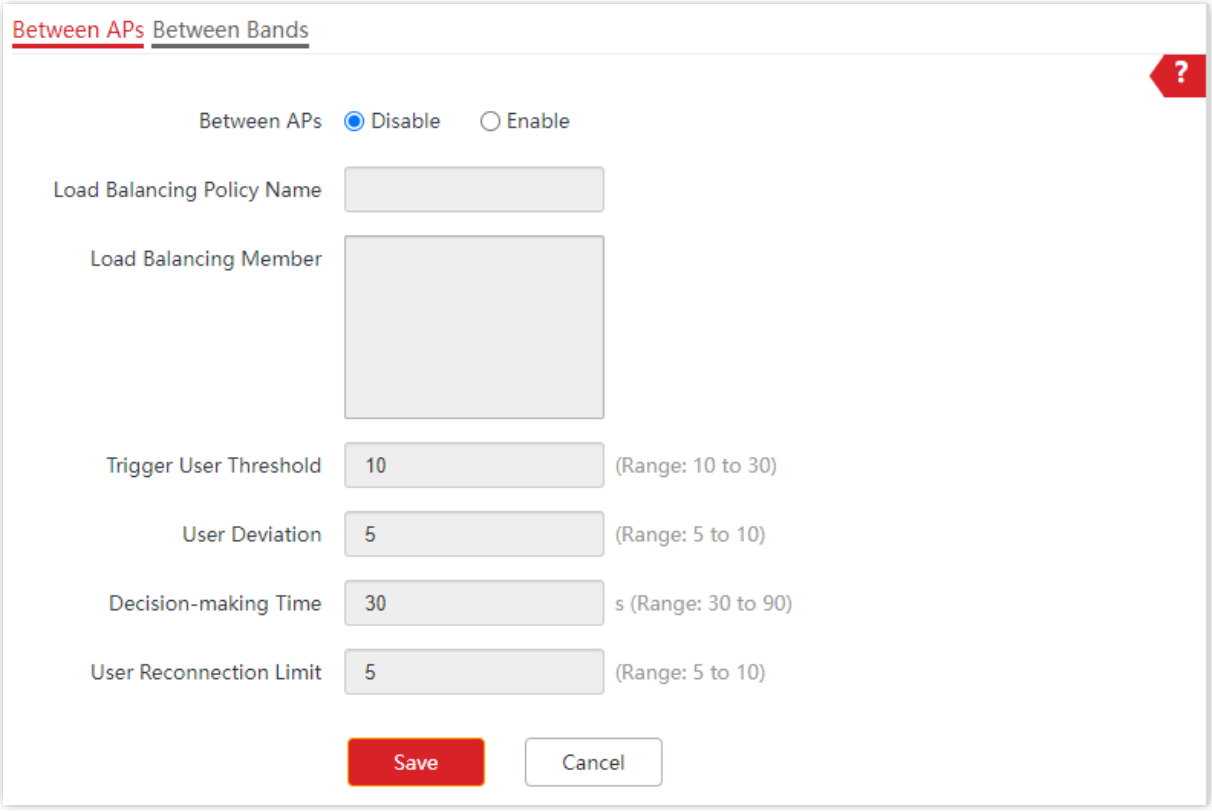
## 6.4.1 Echilibrare încărcare între AP-uri

În rețelele Wi-Fi reale, mai ales în scenariile cu densitate mare de utilizatori, se întâmplă frecvent ca prea mulți clienți să se conecteze la același punct de acces — de obicei la cel cu semnalul cel mai puternic. Drept urmare, unele AP-uri devin supraîncărcate, în timp ce altele rămân subutilizate. Funcția de echilibrare a încărcării între punctele de acces distribuie clienții în mod uniform între AP-urile disponibile. Astfel, resursele rețelei sunt folosite la capacitate maximă, iar performanța globală a sistemului crește.

Tip

- Politica de echilibrare a încărcării intră în vigoare numai atunci când punctele de acces utilizează același nume de politică de echilibrare a încărcării, anume denumirea trecută la câmpul **Load Balancing Policy Name (Nume politică echilibrare încărcare).** Dar au și SSID-uri și parole Wi-Fi identice setate din **Wireless > SSID**.

Pentru a vizualiza sau configura parametrii de echilibrare a încărcării între puncte de acces, conectați-vă la interfața web de gestionare și navigați la **Wireless** > **Load Balancing (Echilibrare încărcare)** > fila **Between APs (Între AP-uri)**. Următoarea figură este doar pentru exemplificare.




**Descriere parametri Wireless > Load Balancing (Echilibrare încărcare) > Between APs (Între AP-uri)**

| Parametru | Descriere |
|---|---|
| **Between APs (Între AP-uri)** | Specifică dacă se activează funcția de echilibrare a încărcării între mai multe echipamente compatibile. |

| Parametru | Descriere |
| --- | --- |
| **Load Balancing Policy Name**<br><br>**(Nume politică echilibrare încărcare)** | Se introduce denumirea politicii de echilibrare a încărcării între puncte de acces.<br><br>Această politică poate fi aplicată punctului de acces în mai multe moduri: fie transmisă centralizat printr-un controler dedicat de AP-uri, fie distribuită de la un ruter multi-WAN cu funcții integrate de control și echilibrare a încărcării, fie configurată direct din interfața web a punctului de acces.<br><br><br><br>Dacă nu există niciun controler în rețeaua locală unde se află punctele de acces, acestea cu același nume de politică de echilibrare a încărcării vor forma automat un grup de echilibrare a încărcării.<br><br>Acceptă echilibrarea încărcării pe baza numărului de utilizatori. |
| **Load Balancing Member**<br><br>**(Membrii grup echilibrare încărcare)** | Doar indică punctele de acces incluse în politica de echilibrare a încărcării. Adresele MAC ale tuturor punctelor de acces din rețea care au activată aceeași politică de echilibrare (cu același nume) sunt adăugate automat în această listă, fără a fi necesară introducerea manuală.<br><br>La unele modele acest câmp informativ nu este afișat. |
| **Trigger User Threshold**<br><br>**(Prag declanșare per user)** | Se setează numărul minim de utilizatori conectați la un AP de la care mecanismul de echilibrare devine activ. Sub această valoare, sistemul nu intervine, considerând că AP-ul nu este suficient de încărcat pentru a justifica redirecționarea clienților<br><br>Intervalul permis este între **10–30 clienți**. |
| **User Deviation**<br><br>**(Deviere utilizator)** | Se setează diferența maximă acceptată între numărul de clienți conectați la două AP-uri din același grup. Când abaterea depășește această valoare, noii clienți sunt direcționați automat către AP-ul cu mai puțini utilizatori.<br><br>De exemplu, dacă e setat **User Deviation (Deviere utilizator)** = 5 utilizatori, iar dacă *AP1* are 18 utilizatori conectați curent și *AP2* are 12, diferența de 6 depășește pragul, iar următorul client va fi îndrumat spre *AP2*.<br><br>Interval permis: **5–10 clienți**.<br><br>La unele modele această opțiune poate fi denumită simplu **Deviation (Deviere)**. |
| **Decision-making Time**<br><br>**(Timp de decizie)** | Se setează perioada în care punctul de acces refuză solicitarea de conectare a utilizatorului. Se recomandă păstrarea setărilor implicite.<br><br>Dacă în această perioadă numărul de refuzuri ale punctului de acces a atins valoarea setată la **User Reconnection Limit (Limită reconectare utilizator)**, atunci punctul de acces permite accesul acestui utilizator.<br><br>Dacă în această perioadă, numărul de refuzuri ale punctului de acces nu atinge **User Reconnection Limit (Limită reconectare utilizator),** atunci numărul de refuzuri este șters.<br><br>Intervalul permis este de **30–90 secunde**. |

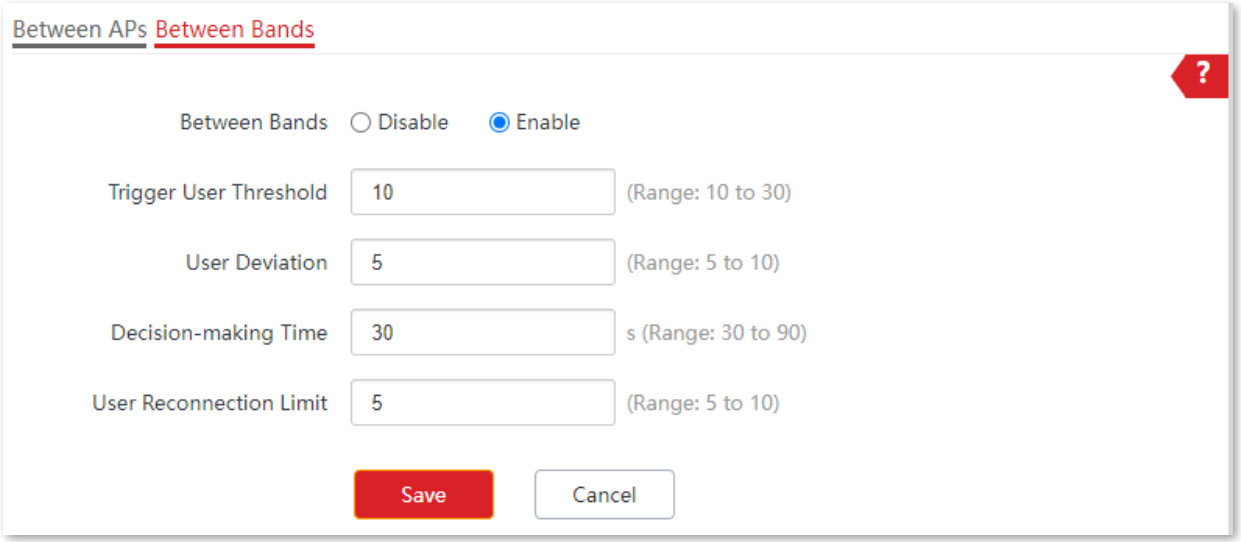
| Parametru | Descriere |
| --- | --- |
| **User Reconnection Limit**<br><br>**(Limită reconectare utilizator)** | Se setează cel mai mare număr de încercări de conectare ale utilizatorilor. Dacă numărul de refuzuri ale punctului de acces a atins această valoare în **Decision-making Time (Timp de decizie),** punctul de acces permite accesul acestui utilizator. Se recomandă păstrarea setărilor implicite.<br><br>Ca exemplu, dacă, într-un interval de 30 de secunde setat la **Decision-making Time (Timp de decizie)**, clientul insistă să se conecteze la AP și atinge numărul de 5 încercări stabilit la **User Reconnection Limit (Limită reconectare utilizator)**, AP-ul renunță să-l mai refuze și îl acceptă, considerând că dispozitivul nu poate ajunge la alt AP din grup. Dacă, dimpotrivă, clientul nu atinge limita de încercări în intervalul stabilit (probabil pentru că s-a conectat între timp la alt AP), contorul se resetează. Acest mecanism previne situațiile în care un client rămâne blocat fără conexiune pentru că toate AP-urile din apropiere sunt aglomerate sau pentru că dispozitivul nu poate ajunge fizic la un alt AP din grup.<br><br>Intervalul permis este de **5–10 reconectări**. |

## 6.4.2 Echilibrare încărcare între benzi

Punctul de acces operează simultan pe două benzi de frecvență: 2,4 GHz și 5 GHz. Unele dispozitive din rețea suportă doar banda de 2,4 GHz, în timp ce altele (mai moderne) sunt dual-band, putând funcționa pe ambele. Problema este că, în mod implicit, clienții dual-band aleg de cele mai multe ori să se conecteze pe 2,4 GHz, ceea ce duce la un dezechilibru evident: banda de 2,4 GHz devine suprasolicitată și aglomerată, în timp ce banda de 5 GHz, mai rapidă și cu mai puține interferențe, rămâne subutilizată.

Pentru a corecta acest dezechilibru, se recomandă activarea funcției de echilibrare a încărcării între benzi, care distribuie inteligent clienții între cele două benzi. Rezultatul este o utilizare mai eficientă a resurselor radio, o reducere semnificativă a congestiei și o experiență de navigare vizibil mai bună pentru toți utilizatorii.

Pentru a vizualiza sau configura parametrii de echilibrare a încărcării între benzi, conectați-vă la interfața web de gestionare și navigați la **Wireless** > **Load Balancing (Echilibrare încărcare)** > fila **Between Bands (Între benzi)**. Următoarea figură este doar pentru exemplificare.




## Descriere parametri Wireless > Load Balancing (Echilibrare încărcare) > Between Bands (Între benzi)

| Parametru | Descriere |
|---|---|
| **Between Bands**<br>**(Între benzi)** | Specifică dacă se activează funcția de echilibrare a încărcării între benzi. |
| **Trigger User Threshold**<br>**(Prag declanșare per user)** | Se setează pragul pentru declanșarea echilibrării încărcării între benzi. Când utilizatorii conectați la punctul de acces ating pragul, se declanșează echilibrarea încărcării între benzi.<br>Intervalul permis este între 10 și 30. |
| **User Deviation**<br>**(Deviere utilizator)** | Se setează abaterea dintre numărul de utilizatori conectați la două benzi. Dacă abaterea depășește această valoare, noii utilizatori sunt direcționați mai întâi către banda cu mai puțini utilizatori.<br>Intervalul permis este între 5 și 10.<br>La unele modele această opțiune poate fi denumită simplu **Deviation (Deviere)**. |
| **Decision-making Time**<br>**(Timp de decizie)** | Se setează perioada în care punctul de acces refuză solicitarea de conectare a utilizatorului. Se recomandă păstrarea setărilor implicite.<br>Dacă în această perioadă numărul de refuzuri ale punctului de acces a atins valoarea setată la **User Reconnection Limit (Limită reconectare utilizator)**, atunci punctul de acces permite accesul acestui utilizator.<br>Dacă în această perioadă, numărul de refuzuri ale punctului de acces nu atinge **User Reconnection Limit (Limită reconectare utilizator),** atunci numărul de refuzuri este șters.<br>Intervalul permis este de **30–90 secunde**. |
| **User Reconnection Limit (Limită reconectare utilizator)** | Se setează cel mai mare număr de încercări de conectare ale utilizatorilor. Dacă numărul de refuzuri ale punctului de acces a atins această valoare în **Decision-making Time (Timp de decizie),** punctul de acces permite accesul acestui utilizator. Se recomandă păstrarea setărilor implicite.<br>Intervalul permis este de **5–10 reconectări**. |

# 6.5 Submeniul Frequency Analysis (Analiză frecvențe)

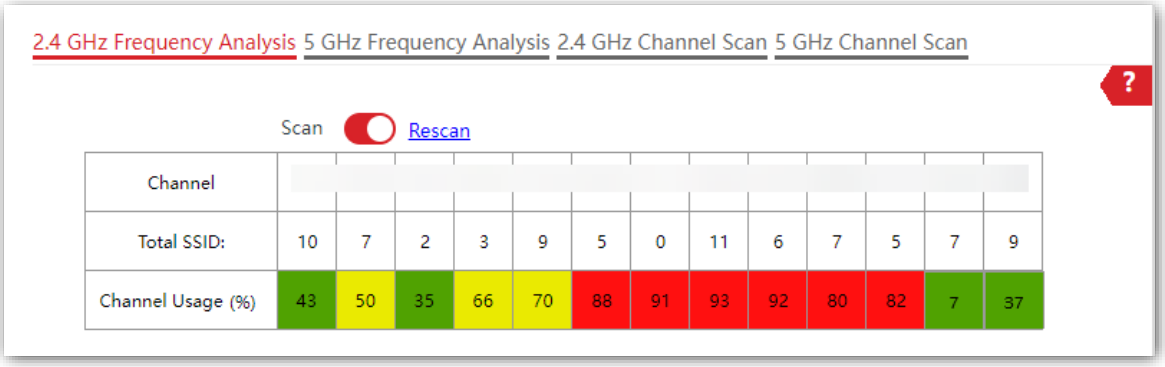
Această secțiune oferă o imagine completă a mediului radio din jurul punctului de acces, scanând eterul și raportând atât utilizarea canalelor, cât și rețelele Wi-Fi vecine detectate. Pe baza acestor informații, administratorul poate alege canalele optime pentru propriile rețele, evitând zonele aglomerate și reducând interferențele.

## 6.5.1 Afișare utilizare spectru

Puteți consulta situația fiecărei benzi de frecvență accesând tabul corespunzător: **2,4 GHz Frequency Analysis (Analiză frecvență 2,4 GHz)** pentru banda de 2,4 GHz, respectiv **5 GHz Frequency Analysis (Analiză frecvență 5 GHz)** pentru cea de 5 GHz. Pentru fiecare canal în parte sunt afișate numărul de rețele Wi-Fi (SSID-uri) detectate și gradul de utilizare exprimat procentual, informații pe baza cărora puteți alege un canal cu utilizare redusă ca frecvență de lucru a punctului de acces, îmbunătățind astfel eficiența transmisiei wireless și reducând interferențele cu rețelele învecinate.

**Procedură**

1. Conectați-vă la interfața web de gestionare.
2. Navigați către **Wireless** > **Frequency Analysis (Analiză frecvențe).**
3. Faceți clic pe fila **2,4 GHz Frequency Analysis (Analiză frecvență 2,4 GHz)** sau **5 GHz Frequency Analysis (Analiză frecvență 5 GHz)** pentru a selecta banda radio pentru care doriți analizarea rețelelor vecine și implicit a eventualelor interferențe. În acest exemplu se apasă fila **2,4 GHz Frequency Analysis (Analiză frecvență 2,4 GHz).**
4. Activați **Scan (Scanare).**
5. După aproximativ 30 de secunde este afișat un tabel cu numărul de SSID-uri și încărcarea pe fiecare canal.




| Channel | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Total SSID: | 10 | 7 | 2 | 3 | 9 | 5 | 0 | 11 | 6 | 7 | 5 | 7 | 9 |
| Channel Usage (%) | 43 | 50 | 35 | 66 | 70 | 88 | 91 | 93 | 92 | 80 | 82 | 7 | 37 |

După scanare, puteți selecta un canal cu utilizare mai redusă ca și canal de lucru AP.

- : Utilizare intensă a canalului. Canalul nu este recomandat.
- : Utilizare moderată a canalului.

- : Utilizare redusă a canalului. Canalul este recomandat.

6. Apoi în funcție de rezultate puteți selecta manual un număr de canal pentru toate SSID-urile de pe banda de 2,4 GHz de la opțiunea **Channel (Canal)**, din meniul **Wireless** > **RF Settings (Setări radiofrecvențe) >** fila **2,4 GHz**.

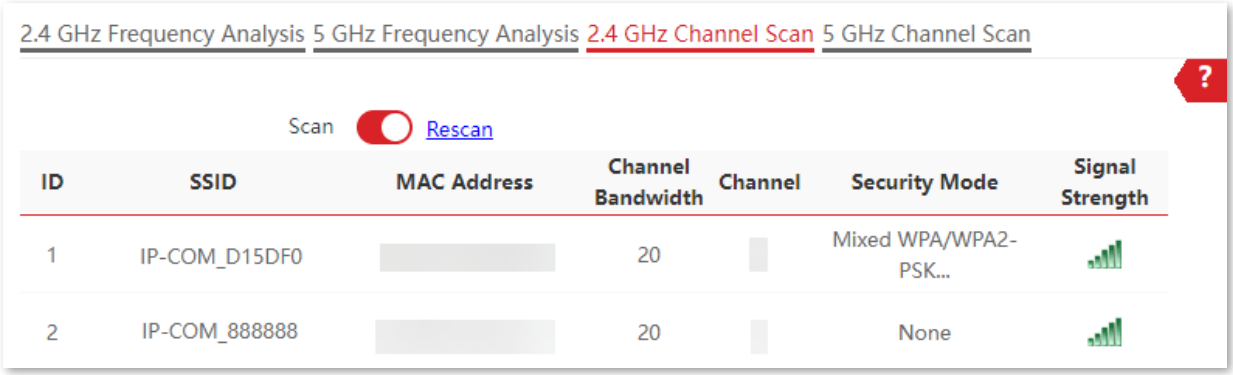
**---Sfârșit**

## 6.5.2 Detalii rețele Wi-Fi din zonă

Apăsând fila **2,4 GHz Channel Scan (Scanare canale 2,4 GHz)** sau fila **5 GHz Channel Scan (Scanare canale 5 GHz)** se afișează lista detaliată a tuturor rețelelor Wi-Fi vecine detectate pe banda de 2,4 GHz sau 5 GHz, cu informații despre fiecare. Lista cu rezultatele scanării vă prezintă informații despre rețele Wi-Fi din apropiere, incluzând denumirea Wi-Fi (SSID-ul), adresa MAC, canalul (identificatorul standard), lățimea canalului, modul de securitate dar și puterea semnalului Wi-Fi transmis.

**Procedură**

1. Conectați-vă la interfața web de gestionare.
2. Navigați către **Wireless** > **Frequency Analysis (Analiză frecvențe).**
3. Faceți clic pe fila **2,4 GHz Channel Scan (Scanare canale 2,4 GHz)** sau **5 GHz Channel Scan (Scanare canale 5 GHz)** pentru a selecta banda radio pe care doriți analiza. În acest exemplu va fi apăsat tabul **2,4 GHz Channel Scan (Scanare canale 2,4 GHz)**.
4. Activați **Scan (Scanare)**.
5. Așteptați aproximativ 30 de secunde. Rezultatele scanării sunt așa cum se arată în figura de mai jos. Țineți cont de aceste informații pentru a seta corespunzător rețelele emise de echipament, de la meniul **Wireless**.




**---Sfârșit**

## 6.6 Submeniul Access Control (Control acces)

Din **Wireless > Access Control (Control acces)** se permite restricționarea accesului la rețeaua Wi-Fi pe baza adreselor MAC ale dispozitivelor, oferind un nivel suplimentar de securitate. Pentru fiecare rețea wireless (SSID) și fiecare bandă radio (2,4 GHz și 5 GHz), administratorul poate activa controlul accesului și alege unul dintre cele două moduri de filtrare:

- **Blacklist (Listă neagră):** Dispozitivele cu adresele MAC adăugate în listă nu au voie să se conecteze la rețea prin SSID-ul selectat. Toate celelalte dispozitive se pot conecta normal.
- **Whitelist (Listă albă):** Doar dispozitivele cu adresele MAC adăugate în listă au voie să se conecteze. Toate celelalte sunt blocate.

Adresa MAC (Media Access Control) este un identificator unic, format din 48 de biți (reprezentat de obicei sub forma a șase grupuri hexazecimale, ex. 94:9B:2C:F3:1B:70), atribuit din fabrică fiecărui adaptor de rețea — fie el Ethernet, Wi-Fi — și înscris permanent în memoria internă a acestuia. Prima jumătate a adresei (OUI) identifică producătorul echipamentului, iar a doua jumătate reprezintă numărul unic al adaptorului. Spre deosebire de adresa IP, care indică unde se află un dispozitiv în rețea și poate fi modificată oricând, adresa MAC indică cine este dispozitivul fizic și rămâne, în principiu, neschimbată pe toată durata de viață a echipamentului. Este folosită pentru identificarea dispozitivelor în rețeaua locală, pentru filtrarea accesului prin **Blacklist (Listă neagră)** și **Whitelist (Listă albă)**, pentru rezervarea de adrese IP în serverul DHCP și, în general, în toate operațiunile care necesită recunoașterea unică a unui adaptor de rețea la nivelul stratului de legătură de date (Layer 2).

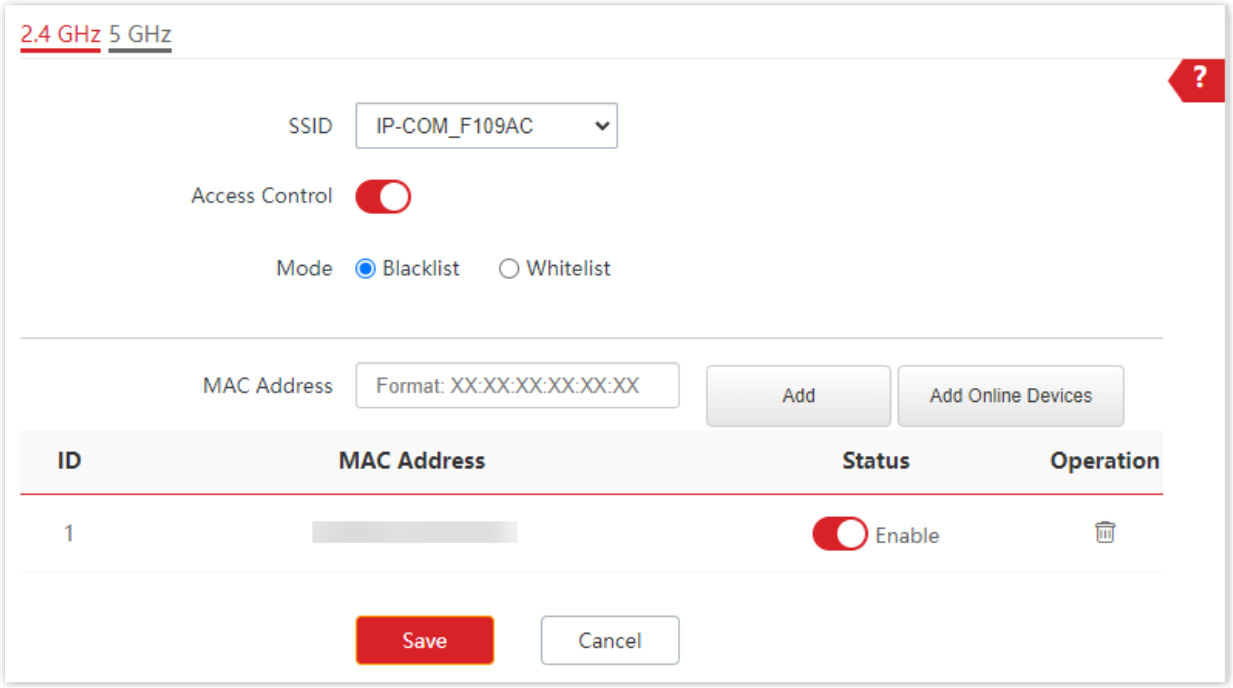
### 6.6.1 Adăugarea unei adrese MAC la Blacklist (Listă neagră), din meniul Access Control (Control acces)

1. Conectați-vă la interfața web de gestionare a punctului de acces.
2. Navigați către **Wireless** > **Access Control (Control acces)**.
3. Selectați o bandă radio Wi-Fi unde trebuie implementată politica. În acest exemplu va fi banda de 2,4 GHz, așadar se va apăsa fila **2,4 GHz**.
4. De la lista derulantă **SSID** selectați denumirea rețelei Wi-Fi pe care se va face filtrarea. Selectați ca exemplu ***IP-COM_F109AC***.
5. Activați funcția **Access Control (Control acces)**.
6. De la **Mode (Mod)** selectați **Blacklist (Listă neagră)**.
7. La câmpul **MAC Address (Adresă MAC)** introduceți identificatorul MAC al adaptorului de rețea al unui dispozitiv client. Apoi faceți clic pe butonul **Add (Adăugare)**. Adresa MAC adăugată în lista de mai jos nu va avea acces la rețea prin conectarea la SSID-ul ***IP-COM_F109AC***.

Tip

Dacă dispozitivul cu Wi-Fi care urmează să fie controlat s-a conectat deja prin punctul de acces, atunci faceți clic pe butonul **Add Online Devices (Adăugare dispozitive online)** pentru a adăuga rapid adresa MAC aferentă dispozitivului în lista de MAC-uri blocate.

8. Faceți clic pe **Save (Salvare).**
9. Dacă dispozitivul client are mai multe adaptoare de rețea (de exemplu are două adaptoare de rețea Wi-Fi) atunci blocați adresa MAC și a celuilalt adaptor de rețea, reluând pașii 7 și 8.




**---Sfârșit**

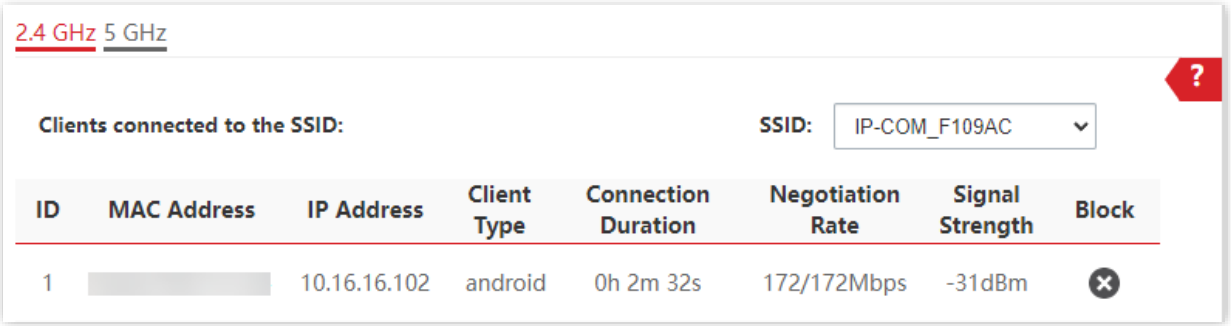
## 6.6.2 Adăugarea unei adrese MAC la Blacklist (Listă neagră), din meniul Client List (Listă clienți)

Puteți bloca o adresă MAC și din meniul **Status (Stare)** > **Client List (Listă clienți)**, nu neapărat doar din meniul **Wireless > Access Control (Control acces)**. Urmați pașii următori.

1. Conectați-vă la interfața web de gestionare a punctului de acces.
2. Navigați la **Status (Stare)** > **Client List (Listă clienți)**.
3. Selectați o bandă radio Wi-Fi apăsând fila **2,4 GHz** sau **5 GHz**. În acest exemplu se va selecta banda de 2,4 GHz, așadar se va apăsa fila **2,4 GHz**.
4. Apoi de la meniu derulant **SSID** selectați rețeaua Wi-Fi corespunzătoare.
5. După câteva secunde, o să vedeți o listă cu clienții conectați prin această rețea Wi-Fi.

6. Găsiți adresa MAC a dispozitivului pe care doriți să îl adăugați la lista de blocare și faceți clic pe butonul ⊗, de sub coloana **Block (Blocare)**, pentru a deconecta și bloca dispozitivul corespunzător.

7. După finalizarea configurării, dispozitivul este adăugat la lista de MAC-uri blocate, **Blacklist (Listă neagră)**, din meniul **Wireless > Access Control (Control acces)**, corespunzător SSID-ului selectat.




**---Sfârșit**

## 6.6.3 Adăugare unei adrese MAC la Whitelist (Listă albă)

MAC-urile dispozitivelor aflate pe **Whitelist (Listă albă)** se pot conecta la rețeaua Wi-Fi (SSID) selectată a punctului de acces pentru a accesa rețeaua locală și implicit internetul partajat de un ruter, în timp ce celelalte dispozitive nu se pot conecta.

Aceasta este cea mai simplă și sigură metodă de a filtra accesul la rețea: administratorul adaugă explicit doar dispozitivele autorizate, iar orice alt dispozitiv este blocat automat, indiferent dacă este cunoscut sau nu.

Prin contrast, filtrarea prin **Blacklist (Listă neagră)** presupune blocarea manuală a fiecărui dispozitiv nedorit în parte — ceea ce devine rapid impractică, deoarece un dispozitiv nou sau necunoscut poate accesa rețeaua până în momentul în care administratorul îl identifică și îl adaugă explicit pe listă.

**Procedură**

1. Conectați-vă la interfața web de gestionare a punctului de acces.
2. Navigați către **Wireless** > **Access Control (Control acces).**
3. Selectați o bandă radio Wi-Fi apăsând fila **2,4 GHz** sau **5 GHz**. În acest exemplu se va selecta banda de 2,4 GHz, așadar se va apăsa fila **2,4 GHz**.
4. Apoi de la meniu derulant **SSID** selectați rețeaua Wi-Fi corespunzătoare. De exemplu se va selecta SSID-ul ***IP-COM_F109AC***.
5. Activați funcția **Access Control (Control acces)**.
6. De la **Mode (Mod)** selectați **Whitelist (Listă albă)**.
7. La câmpul **MAC Address (Adresă MAC)** introduceți identificatorul MAC al adaptorului de rețea al unui dispozitiv client. Apoi faceți clic pe butonul **Add (Adăugare)**. Doar dispozitivul cu adresa

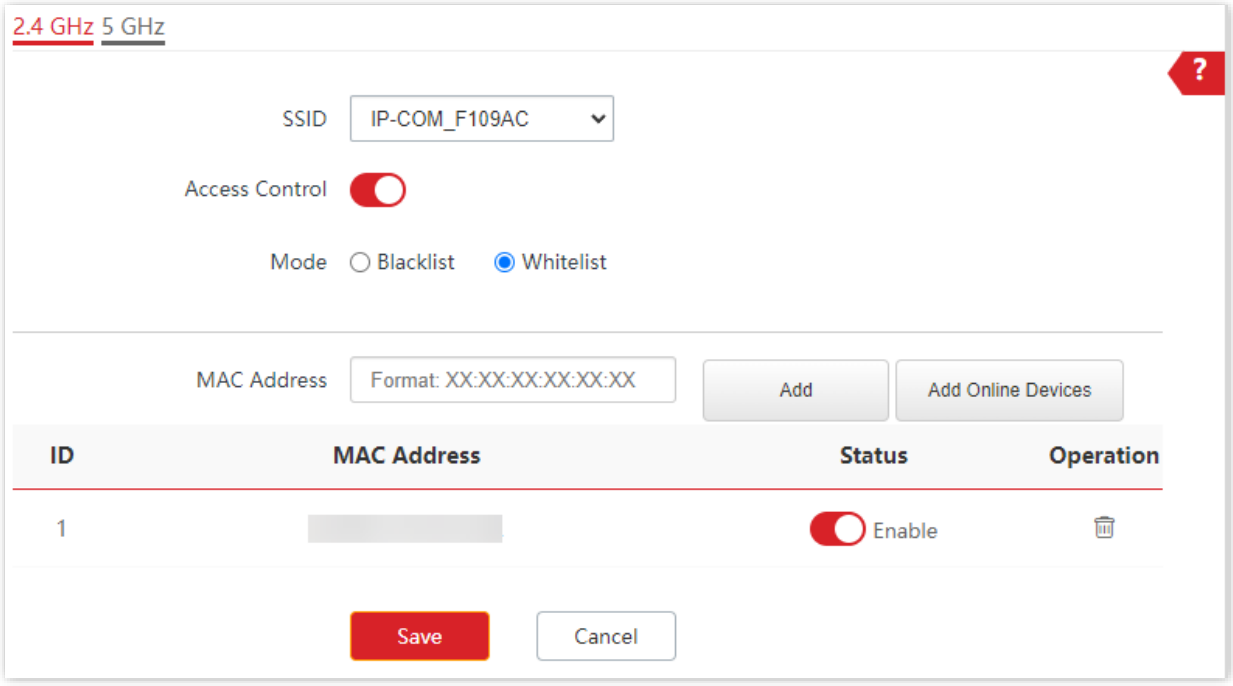
MAC adăugată în lista de mai jos va avea acces la rețea prin conectarea la SSID-ul ***IP-COM_F109AC*.**

Tip

Dacă dispozitivul cu Wi-Fi care urmează să fie controlat s-a conectat deja prin punctul de acces, atunci faceți clic pe butonul **Add Online Devices (Adăugare dispozitive online)** pentru a adăuga rapid adresa MAC aferentă dispozitivului în lista de MAC-uri acceptate.

Aceasta este cea mai simplă și sigură metodă de a filtra accesul la rețea prin Wi-Fi: administratorul adaugă explicit doar dispozitivele autorizate, iar orice alt dispozitiv este blocat automat, indiferent dacă este cunoscut sau nu.

8. Faceți clic pe **Save (Salvare).**




**---Sfârșit**

## 6.6.4 Eliminarea unei adrese MAC din Blacklist (Listă neagră) sau din Whitelist (Listă albă)

Pașii pentru eliminarea unei adrese MAC din **Blacklist (Listă neagră)** și din Whitelist (Listă albă) sunt similari. Mai jos este prezentat un exemplu de eliminare din lista de blocare **Blacklist (Listă neagră)**.

**Procedură**

1. Conectați-vă la interfața web de gestionare a punctului de acces.
2. Navigați către **Wireless** > **Access Control (Control acces)**.
3. Selectați o bandă radio Wi-Fi apăsând fila **2,4 GHz** sau **5 GHz**. În acest exemplu se va selecta banda de 2,4 GHz, așadar se va apăsa fila **2,4 GHz**.

4. Apoi de la meniu derulant **SSID** selectați rețeaua Wi-Fi corespunzătoare.
5. În lista de control de mai jos, găsiți adresa MAC a dispozitivul care va fi deblocat, apoi dezactivați comutatorul **Enable (Activare)** sau faceți clic pe **Delete (Ștergere)**.
6. Faceți clic pe **Save (Salvare)**.

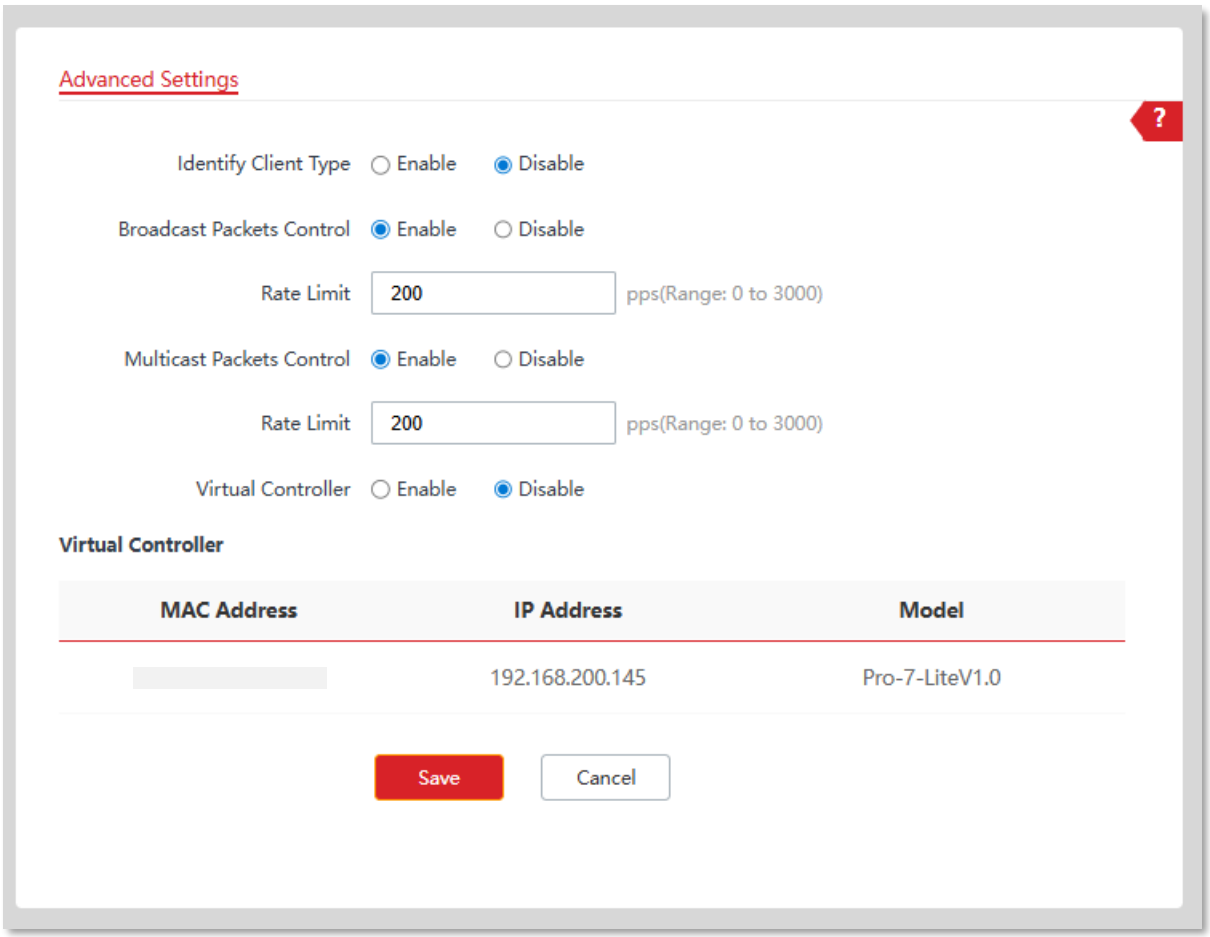
**---Sfârșit**

# 6.7 Submeniul Advanced Settings (Setări avansate)

## 6.7.1 Prezentare generală

După activarea acestei funcții, punctul de acces poate identifica tipurile de sisteme de operare ale dispozitivelor compatibile Wi-Fi conectate la rețeaua sa Wi-Fi, ceea ce face ca gestionarea rețelei Wi-Fi să fie mai eficientă. Tipurile de clienți pe care punctul de acces îi poate identifica includ: Android, iOS, WPhone, Windows, MacOS și așa mai departe.

Pentru accesarea meniului accesați **Wireless > Advanced Settings (Setări avansate)**.



### Descriere parametri Wireless > Advanced Settings (Setări avansate)

| Parametru | Descriere |
|---|---|
| **Identify Client Type (Identificare tip client)** | După activarea acestei funcții, punctul de acces poate identifica tipurile de sisteme de operare ale dispozitivelor compatibile Wi-Fi conectate la rețeaua sa Wi-Fi, ceea ce face ca gestionarea rețelei Wi-Fi să fie mai eficientă. Tipurile de clienți pe care punctul de acces îi poate identifica includ: Android, iOS, Windows, MacOS și așa mai departe.<br><br>La conectarea unui client nou, AP-ul examinează pachetele de inițiere a sesiunii și extrage informații specifice fiecărui sistem de operare, dacă clientul se conectează la punctul de acces și a accesat pagini web HTTP.<br><br>Rezultatul este afișat în meniul **Status (Stare) >** Client List (Listă clienți), în dreptul fiecărui dispozitiv conectat. |
| **Broadcast Packets Control (Control pachete broadcast)** | La activare, punctul de acces limitează numărul de pachete broadcast redirecționate pe secundă, eliminând pachetele care depășesc rata configurată. Astfel, banda radio rămâne disponibilă pentru traficul util.<br><br>Pachetele broadcast sunt cadre de rețea transmise simultan către toți clienții conectați și include cereri *ARP*, anunțuri *NetBIOS*, cereri *DHCP*. În rețelele Wi-Fi, aceste pachete consumă timp de aer comun (*airtime*) pentru toți clienții, indiferent dacă au nevoie sau nu de informația respectivă.<br><br>Mai jos la câmpul **Rate Limit (Limitare rată**) se introduce numărul maxim de pachete broadcast pe secundă **pps** (pachete per secundă) permise să treacă prin punctul de acces. Pachetele care depășesc această limită sunt eliminate. Intervalul permis este de **0–3000 pps** (pachete per secundă), iar valori orientative sunt prezentate mai jos:<br><br>– **0:** Blochează complet pachetele broadcast. Nu este recomandat, poate afecta DHCP și descoperirea dispozitivelor.<br>– **100:** Pentru rețele aglomerate sau cu trafic broadcast excesiv.<br>– **200:** Valoare echilibrată, potrivită pentru majoritatea scenariilor (valoare implicită).<br>– **500–1000:** Pentru rețele cu multe imprimante de rețea, servere de fișiere sau aplicații care depind de broadcast.<br>– **3000:** Maximum permis. |

| Parametru | Descriere |
|---|---|
| **Multicast Packets Control (Control pachete multicast)** | Identic cu **Broadcast Packets Control (Control pachete broadcast)**, dar aplicat traficului multicast. La activare, AP-ul limitează rata de redirecționare a pachetelor multicast pentru a păstra banda radio disponibilă traficului util.<br><br>Pachetele multicast reprezintă o formă intermediară de transmisie în rețea: spre deosebire de traficul broadcast, care ajunge la toți clienții din rețea, și de cel unicast, care se transmite către un singur destinatar, traficul multicast livrează informația simultan doar către un grup specific de dispozitive interesate. Această abordare este folosită de protocoale precum *mDNS*, *AirPlay*, *Chromecast*, descoperirea imprimantelor, *IPTV*, transmisiile video în direct și aplicațiile de colaborare, fiind mult mai eficientă decât trimiterea unor copii individuale către fiecare destinatar.<br><br>Mai jos la câmpul **Rate Limit (Limitare rată**) se introduce numărul maxim de pachete multicast pe secundă (**pps)** permise să treacă prin punctul de acces. Valori orientative:<br>– **0:** Blochează complet traficul multicastat și va afecta *AirPlay*, *Chromecast*, *IPTV*, descoperirea imprimantelor etc.<br>– **200:** Valoare implicită, potrivită pentru trafic obișnuit de internet și e-mail.<br>– **500–1000:** Recomandat dacă în rețea există *AirPlay*, *Chromecast*, *IPTV* sau imprimante de rețea descoperite prin *mDNS.*<br>– **2000–3000:** Pentru rețele dedicate transmisiunilor video multicastate. |
| **Virtual Controller (Controler virtual)** | Funcție de control centralizat care permite ca unul dintre punctele de acces din rețea să preia rolul de controler de AP-uri, eliminând necesitatea unui controler hardware dedicat sau a unei soluții cloud.<br><br>AP-ul desemnat ca controler virtual descoperă automat celelalte puncte de acces compatibile din aceeași rețea, le preia în administrare și le distribuie configurația comună (SSID, parametri RF etc.). Asigură stabilitatea roamingului între AP-uri prin sincronizarea parametrilor.<br><br>**Î**ntr-o rețea poate fi activ un singur controler virtual. Activarea funcției pe mai multe AP-uri simultan duce la conflict de configurație.<br><br>Opțiuni disponibile:<br>– **Enable (Activare)**: Acest AP devine controler virtual în rețea pentru alte AP-uri compatibile.<br>– **Disabled (Dezactivare)**: AP-ul funcționează *standalone* sau ca dispozitiv administrat de alt controler.<br><br>După o scurtă perioadă de funcționare, în care punctul de acces scanează rețeaua locală, sub secțiune apare un tabel cu informații suplimentare. |

## 6.7.2 Activare identificare tip client conectat

După activarea acestei funcții, punctul de acces poate identifica tipurile de sisteme de operare ale dispozitivelor compatibile Wi-Fi conectate la rețeaua sa Wi-Fi, ceea ce face ca gestionarea rețelei Wi-Fi să fie mai eficientă. Tipurile de clienți pe care punctul de acces îi poate identifica includ: Android, iOS, Windows, MacOS și așa mai departe.

**Procedură**

1. Conectați-vă la interfața web de gestionare a punctului de acces.
2. Navigați la **Wireless** > **Advanced Settings (Setări avansate).**
3. Activați funcția **Identify Client Type (Identificare tip client).**
4. Faceți clic pe **Save (Salvare).**
5. După finalizarea configurării, dacă clientul se conectează la punctul de acces și a accesat pagini web HTTP, puteți vizualiza tipul de sistem de operare al clientului pe pagina **Status (Stare)** > **Client List (Listă clienți)**.

**---Sfârșit**

## 6.7.3 Limitare rată trafic broadcast și multicast prin Wi-Fi

Limitarea ratei de transmisie a pachetelor de tip broadcast sau multicast poate împiedica ocuparea canalului de către un astfel de trafic invalid, reducând risipa de resurse a interfeței aeriene Wi-Fi, diminuând interferențele, îmbunătățind eficiența transmisiei și îmbunătățind experiența utilizatorului.

**Procedură**

1. Conectați-vă la interfața web de gestionare a punctului de acces.
2. Navigați la **Wireless** > **Advanced Settings (Setări avansate).**
3. Activați funcția de **Broadcast Packets Control (Control pachete broadcast).**
4. Setați **Rate Limit (Limitare rată)** pentru pachetele de difuzare (broadcast). În mod implicit, este de **200 pps**.
5. Activați funcția de **Multicast Packets Control (Control pachete multicast).** Se recomandă activarea simultană a funcției **WMF** din meniul **Wireless > SSID**.
6. Setați **Rate Limit (Limitare rată)** pentru pachetele multicast. În mod implicit, aceasta este de **200 pps**.
7. Faceți clic pe **Save (Salvare).**

**---Sfârșit**

## 6.7.4 Utilizare AP ca un controler virtual de AP-uri

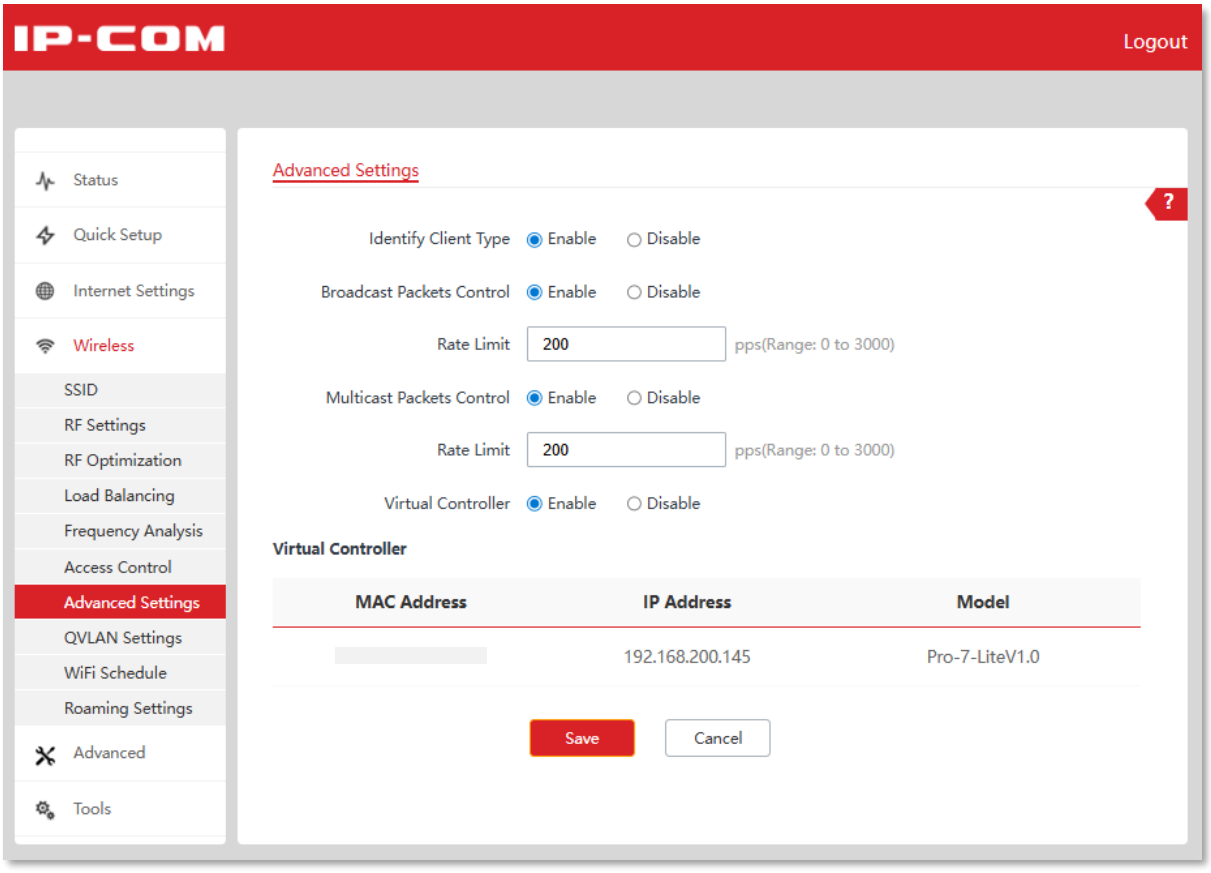
Când nu există un controler dedicat de AP-uri sau un ruter multi-WAN cu control de AP-uri precum cele din seria M care să accepte gestionarea punctelor de acces în rețea, puteți configura un punct de acces ca controler wireless virtual pentru a descoperi și gestiona automat alte puncte de acces cu același SSID, asigurând o stabilitate perfectă a roamingului. În cadrul aceleiași rețele locale poate fi atribuit un singur controler virtual.

Tip

Această funcție poate fi utilizată doar într-un mediu de rețea cu cel puțin două puncte de acces. Informațiile despre punctul de acces principal sunt afișate în lista din acest meniu curent.

**Procedură**

1. Conectați-vă la interfața web de gestionare a punctului de acces.
2. Navigați la **Wireless** > **Advanced Settings (Setări avansate).**
3. Activați funcția **Virtual Controller (Controler virtual).**




4. Faceți clic pe **Save (Salvare).**

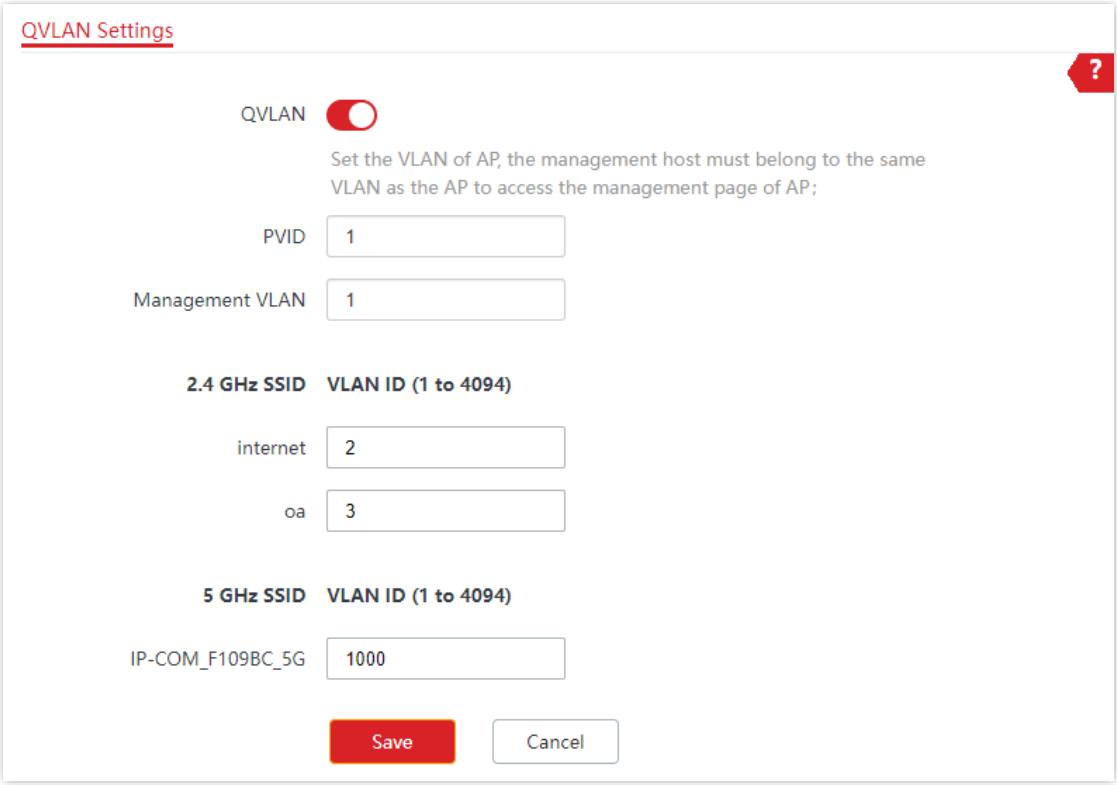
**---Sfârșit**

# 6.8 Submeniul QVLAN Settings (Setări QVLAN)

## 6.8.1 Prezentare generală

Echipamentul acceptă etichetarea VLAN conform standardului IEEE 802.1q și poate fi integrat în orice rețea în care sunt deja definite VLAN-uri compatibile cu acest standard. Implicit, funcția QVLAN este dezactivată.

Pentru accesarea meniului navigați la **Wireless > QVLAN Settings (Setări QVLAN)**. Următoarea figură este doar pentru exemplificare, cu două SSID-uri pe 2,4 GHz, denumite ***internet, și un SSID*** pe 5 GHz denumit ***IP-COM_F109BC_5G***.




**Descriere parametri Wireless > QVLAN Settings (Setări QVLAN)**

| Parametru | Descriere |
|---|---|
| **QVLAN** | Specifică dacă se activează VLAN-urile pe echipament, conform IEEE 802.1q. În mod implicit, funcționalitatea este dezactivată.<br>– Activ: Funcția **QVLAN** este activată, iar portul PoE al AP-ului devine port *Trunk*, capabil să transporte trafic etichetat (*tagged*) de la mai multe VLAN-uri simultan.<br>– Inactiv: Funcția este dezactivată, AP-ul tratează tot traficul ca aparținând unei singure rețele.<br>După activarea **QVLAN**, switch-ul la care este conectat AP-ul trebuie configurat corespunzător, cu portul respectiv setat ca Trunk și cu VLAN-urile permise. În caz contrar, riscați să pierdeți complet accesul la AP. |

| Parametru | Descriere |
| --- | --- |
| **PVID** | Specifică ID-ul VLAN-ului nativ implicit al portului trunk al punctului de acces.<br>Recomandarea este să păstrați valoarea **1**, dacă nu aveți o cerință specifică din partea administratorului de rețea. Modificarea PVID-ului trebuie corelată cu configurația switch-ului. |
| **Management VLAN (VLAN de gestionare)** | Specifică ID-ul VLAN-ului de gestionare, sau cunoscut ca *VLAN-ul de management*, pentru accesarea interfeței de gestionare a punctul de acces. |
| **2,4 GHz SSID**<br>**5 GHz SSID** | Specificați SSID-urile activate în prezent pe banda de 2,4 GHz sau 5 GHz și ID-urile VLAN corespunzătoare fiecărui SSID. Aici puteți eticheta fiecare rețea Wi-Fi cu un VLAN.<br>Tip<br>După activarea funcției QVLAN, SSID-urile funcționează ca *porturi de acces* (*Access*). PVID-ul și ID-ul VLAN al unui port de acces sunt aceleași. |
| **VLAN ID**<br>**(ID VLAN)** | ID-urile pot fi între 1 și 4094. ID-ul implicit e **1000**. |

## 6.8.2 Exemplu de configurare a setărilor QVLAN

**Cerințe**

Un complex industrial are următoarele cerințe de acoperire a rețelei Wi-Fi:

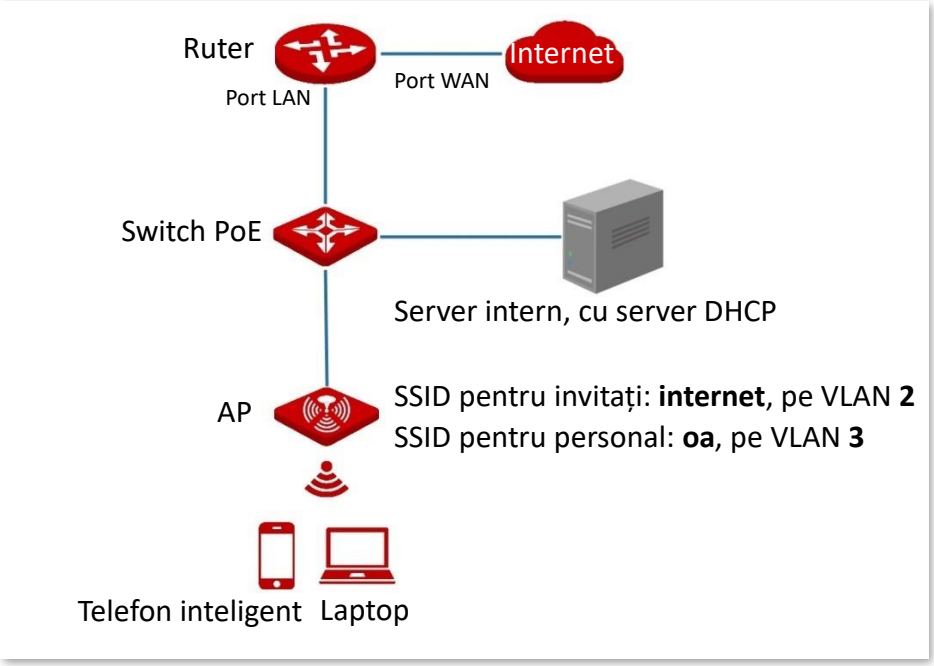
- Invitații să fie conectați la rețeaua virtuală VLAN **2** și să poată accesa doar internetul.
- Personalul să fie conectat la rețeaua virtuală VLAN **3** și să poată accesa doar servere din rețeaua locală, fără internet.

**Soluție**

- Setați SSID-ul denumit ***internet*** pentru invitați, pe banda de 2,4 GHz.
- Setați SSID-ul denumit ***oa*** pentru personalul din companie, pe banda de 2,4 GHz.
- Configurați VLAN-urile pentru SSID-urile de mai sus pe punctul de acces.
- Apoi configurați politicile de redirecționare VLAN pe switch.

Tip

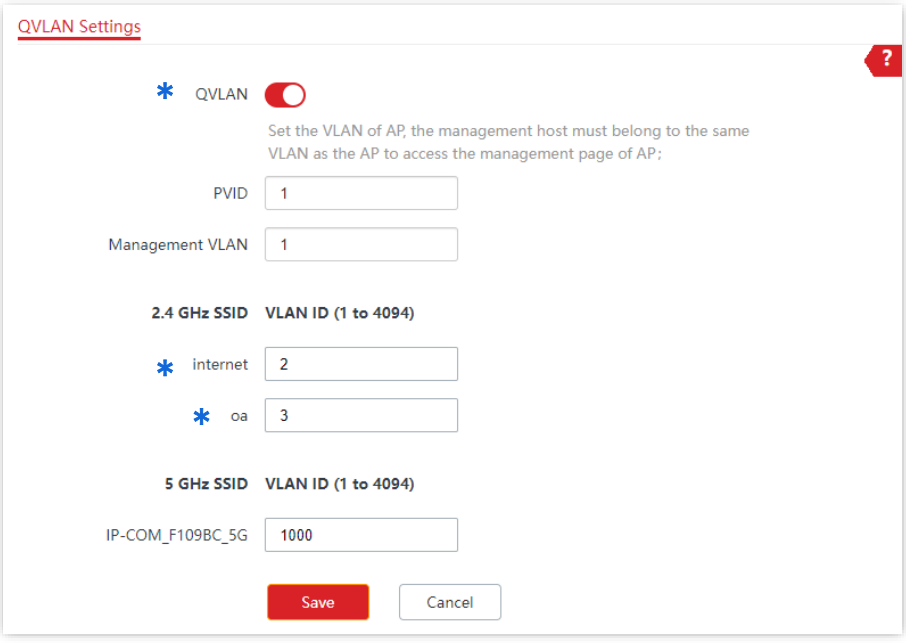
În infrastructura companiei trebuie implementat un serviciu DHCP responsabil cu atribuirea adreselor IP către dispozitivele conectate. Serviciul DHCP trebuie configurat să deservească fiecare VLAN definit în rețea, prin scope-uri (intervale de adrese) separate.




**Procedură**

## I. Configurați punctul de acces

1. Conectați-vă la interfața web de gestionare a punctului de acces.
2. Se consideră că deja ați configurat corespunzător rețele Wi-Fi ***oa*** și ***internet*** din meniul **Wireless > SSID**.
3. Pentru setările VLAN navigați la **Wireless** > **QVLAN Settings (Setări QVLAN)**.
4. Activați funcția **QVLAN.**
5. Modificați ID-urile VLAN ale SSID-urilor la banda de 2,4 GHz. Astfel, de la secțiunea **2,4 GHz SSID**, introduceți ID-ul VLAN numărul ***2*** la SSID-ul ***internet***. Introduceți ***3*** la SSID-ul denumit ***oa***.
6. Faceți clic pe **Save (Salvare).** Următoarea figură este doar pentru referință.



### II. Configurați switch-ul la care e conectat AP-ul

1. Creați ID-urile VLAN pe switch-ul din amonte, apoi aplicați-le pe porturile sale Ethernet conform tabelului de mai jos. Se presupune că switch-ul este un model gestionabil (cu interfață de management), care vă permite atât definirea VLAN-urilor, cât și asocierea acestora cu porturile Ethernet configurate ca *Trunk* și *Access*.

| Port Ethernet conectat la | ID VLAN | Tip de port | PVID |
|---|---|---|---|
| AP | 1, 2, 3 | Trunk | 1 |
| Server intern | 3 | Access | 3 |
| Ruter | 2 | Access | 2 |

2. Păstrați setările implicite ale celorlalte porturi. Pentru detalii, consultați ghidul utilizatorului pentru switch.

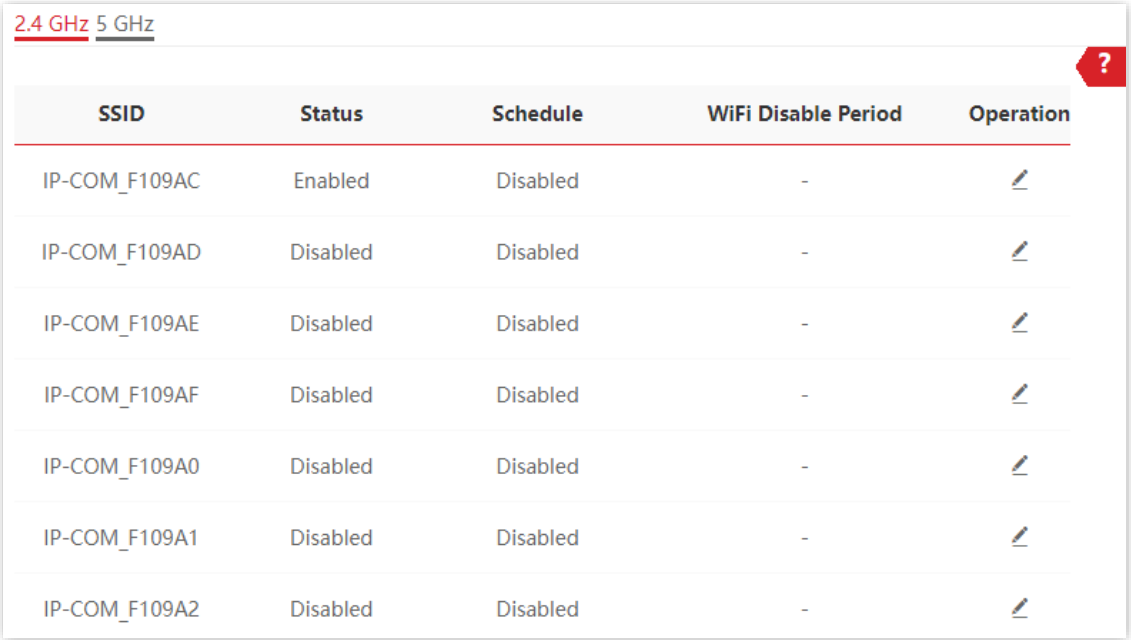
3. Verificați. Astfel, clienții wireless conectați la rețeaua Wi-Fi ***internet*** pot accesa doar internetul, iar clienții wireless conectați la ***oa*** pot accesa doar servere din rețeaua locală a companiei.

**---Sfârșit**

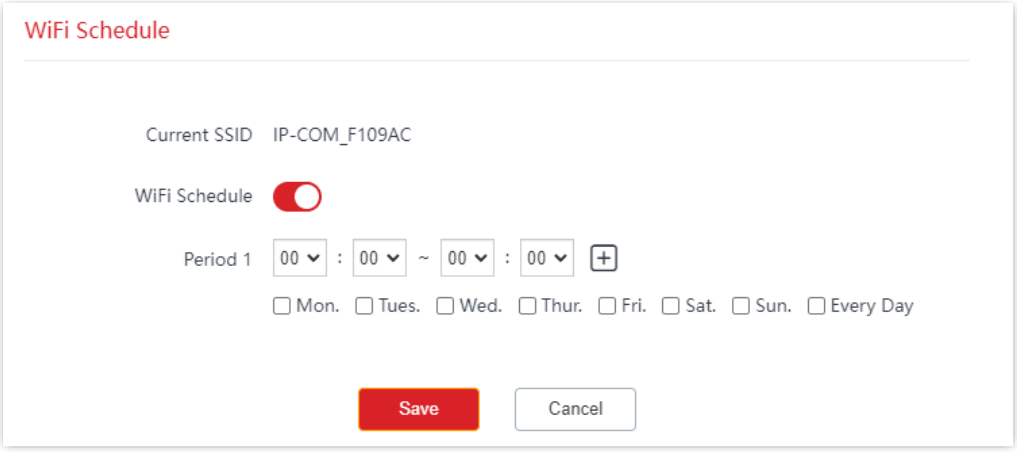
# 6.9 Submeniul WiFi Schedule (Orar Wi-Fi)

Opțiunile din acest meniu pot fi diferite în funcție de model.

Pentru fiecare SSID pe ambele benzi (2,4 GHz și 5 GHz) puteți defini orare de funcționare a rețelei Wi-Fi. În intervalele de timp configurate, rețeaua Wi-Fi este dezactivată automat, iar dispozitivele compatibile — telefoane, laptopuri, tablete — nu o mai detectează în lista rețelelor disponibile. Configurarea se face individual, pe rândul corespunzător fiecărei rețele Wi-Fi pe care doriți să o controlați. Accesați meniul **Wireless > WiFi Schedule (Orar Wi-Fi)**.



Configurarea se poate face inclusiv pentru SSID-urile dezactivate, iar meniul arată ca în imaginea următoare, după apăsarea butonului **Edit (Editare)** de sub coloana **Operation (Operație)**.




### Descriere parametri Wireless > WiFi Schedule (Orar Wi-Fi)

| Parametru | Descriere |
|---|---|
| Fila **2,4 GHz**<br>Fila **5 GHz** | Utilizat pentru a selecta banda Wi-Fi pe care urmează să fie configurate orarele.<br>După apăsarea unei file aferente benzii vor fi afișate toate SSID-urile active și dezactivate. |
| **SSID** | Cap de tabel ce specifică numele rețelei Wi-Fi. Numele pentru fiecare se modifică din **Wireless > SSID**. |
| **Status**<br>**(Stare)** | Cap de tabel ce specifică starea rețelei Wi-Fi dacă e activată sau dezactivată. Activarea acestora se face din meniul **Wireless > SSID**. |
| **Schedule**<br>**(Orar)** | Cap de tabel ce specifică dacă e activ un orar Wi-Fi. |
| **WiFi Disable Period**<br>**(Perioadă dezactivare Wi-Fi)** | Specifică orarul configurat de dezactivare automată a rețelei respective. |
| **Operation**<br>**(Operație)** | Faceți clic pe butonul **Edit (Editare)** pentru a activa/dezactiva sau edita efectiv orarul de dezactivare a rețelei Wi-Fi.<br>Apoi va fi afișată o nouă pagină ce permite setarea mai multor perioade, pe fiecare zi din săptămână.<br>Se pot seta mai multe intervale orare, diferite, dacă se apasă butonul **+**.<br>Pentru salvarea modificărilor trebuie apăsat **Save (Salvare)** și citite eventualele suprapuneri de perioade orare. |
| **Save**<br>**(Salvare)** | Apăsați acest buton pentru a salva toate modificările din întreaga listă. |
| **Cancel**<br>**(Anulare)** | Anulați modificările, înainte de a apăsa **Save (Salvare), iar pagina** se va reîmprospăta. |

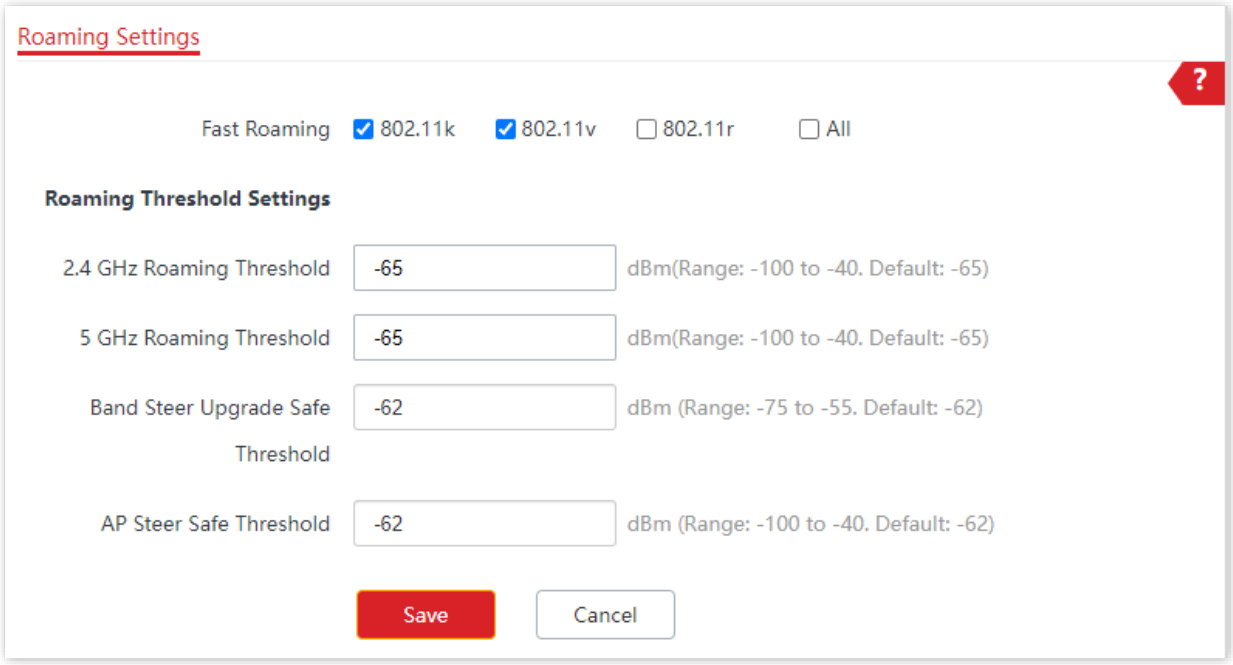
# 6.10 Submeniul Roaming Settings (Setări roaming)

Roamingul wireless permite unui client să comute automat la punctul de acces cu cel mai bun semnal atunci când se deplasează într-o zonă acoperită simultan de mai multe puncte de acces, deconectându-se în același timp de la AP-ul original. Funcția presupune ca toate punctele de acces implicate să difuzeze același SSID, să folosească același mod de securitate și aceeași cheie de criptare.

Funcția de roaming rapid conform standardelor *IEEE 802.11k/v/r* poate rezolva eficient următoarele probleme.

- Pierderi semnificative de pachete în timpul tranziției între puncte de acces.
- Momentul nepotrivit al declanșării roamingului iar clientul rămâne agățat de AP-ul vechi chiar și atunci când semnalul devine slab.
- Alegerea unui AP nepotrivit, iar clientul migrează către un AP care nu este, de fapt, cel mai bun candidat din zonă.

Pentru a accesa pagina, conectați-vă la interfața de gestionare și navigați la **Wireless** > **Roaming Settings (Setări roaming).**



### Descriere parametri Wireless > Roaming Settings (Setări roaming)

| Parametru | Descriere |
|---|---|
| Secțiunea **Fast Roaming** **(Roaming rapid)** | Specifică dacă se activează anumite protocoale de roaming, standardizate de IEEE:<br>– **802.11k:** La activare, punctul de acces furnizează clienților o listă cu AP-urile vecine, împreună cu canalele pe care funcționează și nivelul de semnal disponibil. Clientul nu mai trebuie să scaneze întregul spectru radio pentru a găsi un AP mai bun, ci primește direct lista candidaților optimi. Rezultatul: tranziția devine semnificativ mai rapidă, iar consumul bateriei dispozitivelor mobile scade.<br>– **802.11v:** Permite punctului de acces să sugereze clientului momentul potrivit pentru a iniția roamingul și să recomande AP-ul țintă cel mai potrivit. În roamingul tradițional, clientul decide singur când și unde să migreze, adesea prea târziu sau către un AP nepotrivit. Cu 802.11v, AP-ul preia inițiativa și ghidează clientul către cea mai bună opțiune disponibilă.<br>– **802.11r:** Accelerează procesul de re-autentificare la noul AP, eliminând întârzierile cauzate de schimbul complet de chei de criptare WPA2/WPA3. În loc de o re-autentificare completă (care poate dura sute de milisecunde), 802.11r efectuează o pre-autentificare paralelă, reducând timpul de tranziție la câteva milisecunde.<br>– **All (Toate):** Toate cele trei protocoale sunt activate.<br>Note<br>Unele dispozitive Android mai vechi sau imprimante/scanere industriale pot avea probleme cu **802.11r** activat. Dacă apar deconectări neașteptate după activare, se recomandă testarea individuală a protocoalelor. |
| **2.4 GHz Roaming Threshold** **(Prag roaming pe 2,4 GHz)** și **5 GHz Roaming Threshold** **(Prag roaming pe 5 GHz)** | Folosit pentru a seta pragul de roaming de 2,4 GHz sau 5 GHz, ceea ce înseamnă setarea sensibilității clientului la roaming.<br>Când puterea semnalului recepționat de client de la punctul de acces scade sub pragul de roaming, roamingul este declanșat și clientul e conectat la un AP cu o calitate mai bună a legăturii.<br>Valoarea implicită: −65 dBm.<br>Interval permis: **−100 dBm** până la **−40 dBm**.<br>Tip<br>Cu cât pragul de roaming este setat la o valoare mai mare (mai apropiată de 0 dBm, de exemplu −65 dBm față de −80 dBm), cu atât sensibilitatea la roaming este mai ridicată — clientul va iniția mai rapid trecerea la un alt AP. Invers, cu cât pragul este mai mic (mai apropiat de −90 dBm), cu atât sensibilitatea este mai redusă, iar clientul va rămâne asociat cu AP-ul curent chiar și la un semnal slab. |

| Parametru | Descriere |
| --- | --- |
| **Band Steer Upgrade Safe Threshold**<br>**(Prag siguranță îmbunătățire redirecționare între benzi)** | Folosit pentru a seta pragul de siguranță pentru îmbunătățirea redirecționării către o altă bandă.<br>Când un client este conectat fie la banda de 2,4 GHz, fie la cea de 5 GHz a unui punct de acces, acesta se va conecta automat la o altă bandă de frecvență dacă intensitatea semnalului recepționat din banda curentă scade sub pragul configurat.<br>Valoare implicită: **–62 dBm**.<br>Interval permis: **–75 dBm** până la **–55 dBm**. |
| **AP Steer Safe Threshold**<br>**(Prag siguranță îmbunătățire redirecționare între AP-uri)** | Folosit pentru a seta pragul de siguranță pentru îmbunătățirea redirecționării către un alt AP din sistem.<br>Pe măsură ce clientul se deplasează, dacă puterea semnalului recepționat scade sub pragul configurat, acesta comută automat la punctul de acces cu semnal mai bun.<br>Valoare implicită: **–62 dBm**.<br>Interval permis: **–100 dBm** până la **–40 dBm**. |

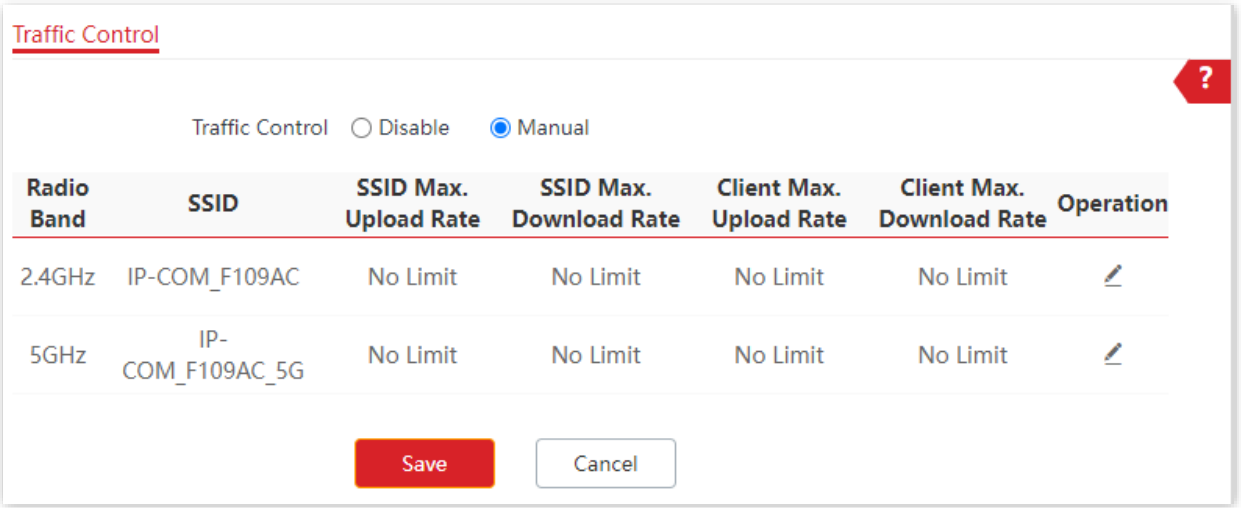
# 7 Meniul Advanced (Avansat)

Funcțiile pot varia în funcție de model și de versiunea software instalată. Imaginile, pașii și descrierile prezentate în acest manual au caracter orientativ și pot diferi de interfața sau funcționarea reală. În acest manual, denumirile meniurilor și ale opțiunilor sunt prezentate în limba engleză, iar echivalentul în limba română este indicat între paranteze. Manualul este adaptat utilizatorilor cunoscători de limba română.

## 7.1 Submeniul Traffic Control (Control trafic)

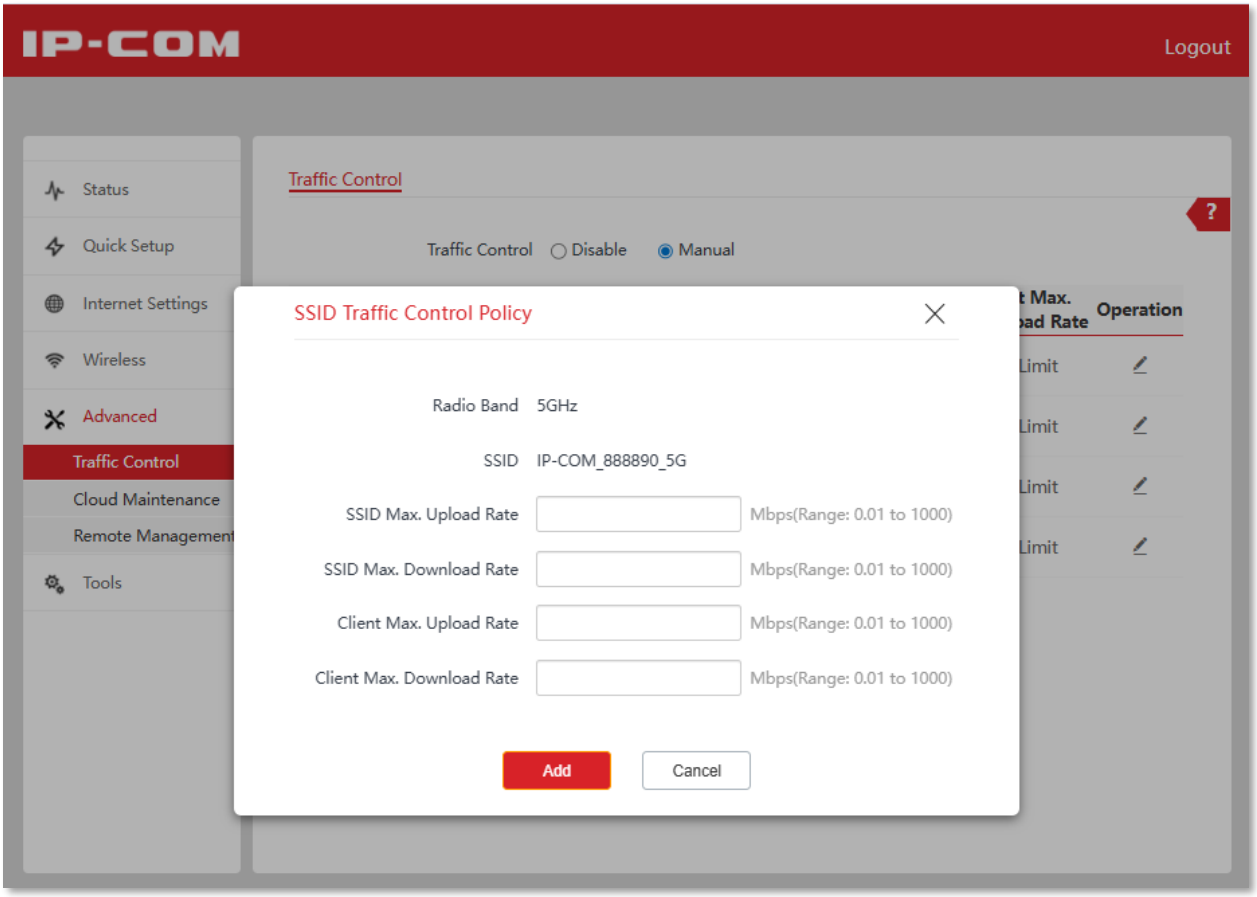
Din meniul **Advanced (Avansat) > Traffic Control (Control trafic)**, funcția de control al traficului permite stabilirea unor limite de lățime de bandă atât la nivel global, pe fiecare SSID în parte, cât și individual, pe fiecare client conectat la un SSID. Astfel, pot fi configurate independent rata maximă de încărcare (upload) și de descărcare (download) pentru întregul SSID, precum și valorile maxime alocate fiecărui utilizator în parte. Această funcționalitate este utilă în special atunci când pe același AP sunt active mai multe rețele wireless cu priorități diferite — de exemplu, o rețea principală pentru angajați și o rețea separată pentru invitați.

În mod implicit, funcția de control al traficului este dezactivată de la **Traffic Control (Control trafic)**, iar dacă se activează **Manual**, pentru configurarea limitelor, atunci pagina va fi astfel afișată:




Dacă se apasă butonul **Edit (Editare)** de la coloana **Operation (Operație)** puteți seta limitele de rată.

Se va deschide o nouă fereastră denumită **SSID Traffic Control Policy (Politică control trafic SSID)**, ca în imaginea următoare.




### Descriere parametri Advanced (Avansat) > Traffic Control (Control trafic)

| Parametru | Descriere |
|---|---|
| **Traffic Control**<br>**(Control trafic)** | Specifică dacă se activează funcția de control al traficului. Pentru activare se selectează **Manual** iar pentru dezactivare se selectează **Disable (Dezactivare)**. |
| **Radio Band**<br>**(Bandă radio)** | Coloana care indică banda Wi-Fi pentru SSID-ul din tabel. |
| **SSID** | Afișează numele rețelei Wi-Fi activate din meniul **Wireless > SSID**.<br>Pentru fiecare SSID listat se poate defini o regulă nouă de control al traficului sau se poate modifica o regulă deja existentă, apăsând **Edit (Editare)** din coloana **Operation**. |

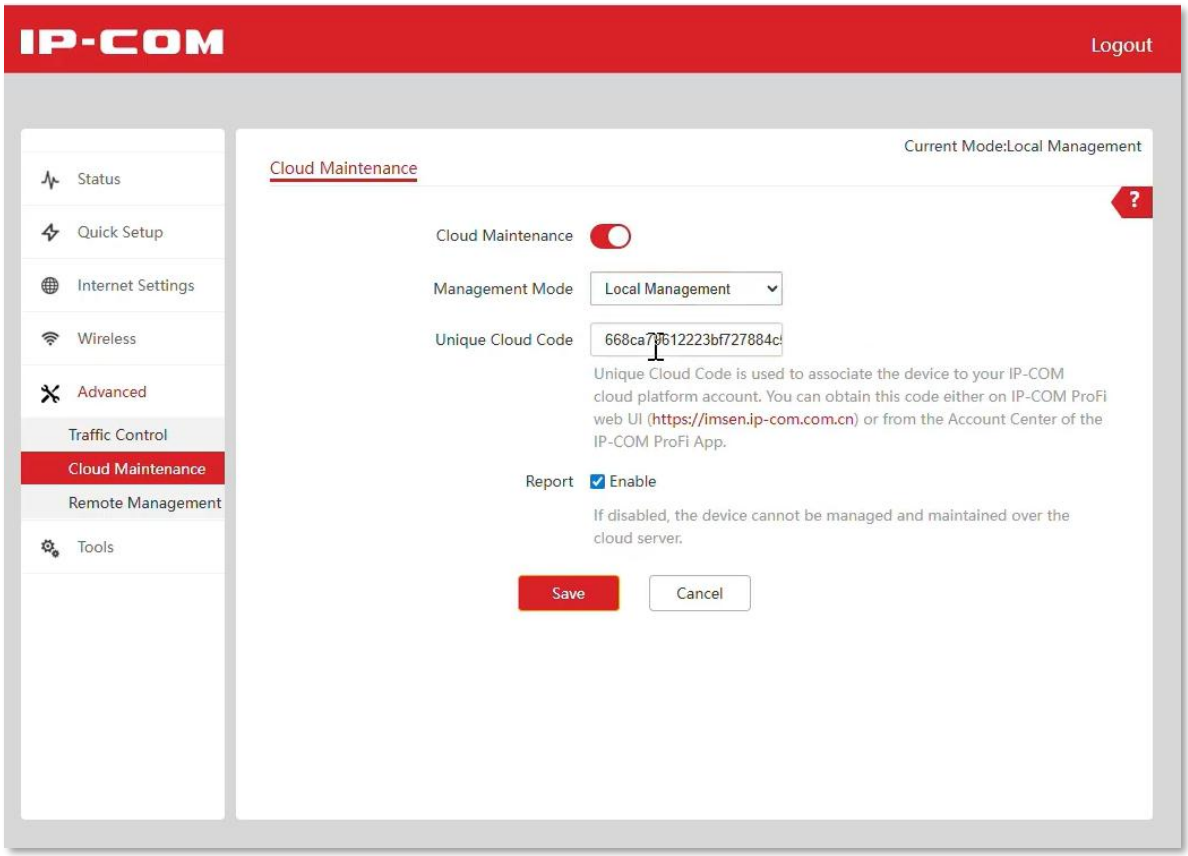
| Parametru | Descriere |
|---|---|
| **SSID Max. Upload Rate**<br>**(Rată maximă încărcare per SSID)**<br>și<br>**SSID Max. Download Rate**<br>**(Rată maximă descărcare per SSID)** | Permit stabilirea limitei totale de lățime de bandă, pentru încărcare, respectiv descărcare, alocată întregii rețele Wi-Fi, acelui SSID. Valoarea introdusă reprezintă plafonul maxim distribuit între toți clienții conectați la acel SSID.<br>Dacă aceste câmpuri sunt lăsate necompletate, traficul de încărcare și descărcare al rețelei wireless nu va fi limitat în niciun fel.<br>Parametrii sunt disponibili pentru configurare numai atunci când funcția **Traffic Control (Control trafic)** este setată în mod **Manual**, opțiunea activată în partea superioară a paginii. |
| **Client Max. Upload Rate**<br>**(Rată maximă încărcare per client)**<br>și<br>**Client Max. Download Rate**<br>**(Rată maximă descărcare per client)** | Permit stabilirea limitei individuale de lățime de bandă, pentru încărcare, respectiv descărcare, alocată fiecărui dispozitiv conectat la rețeaua Wi-Fi vizată, SSID-ul vizat.<br>Spre deosebire de limitele aplicate la nivel de SSID, aceste valori se aplică separat fiecărui client în parte, asigurând o distribuție echitabilă a resurselor între utilizatori.<br>Dacă aceste câmpuri sunt lăsate necompletate, viteza de încărcare și descărcare a fiecărui dispozitiv conectat la SSID-ul respectiv nu va fi limitată.<br>Parametrii sunt disponibili pentru configurare numai atunci când funcția **Traffic Control (Control trafic)** este setată în mod **Manual**. |
| **Operation**<br>**(Operație)** | Faceți clic pe butonul **Edit (Editare)** pentru a seta rata maximă de încărcare sau descărcare permisă pentru rețeaua Wi-Fi (SSID) dorită și rata maximă de încărcare sau descărcare permisă pentru fiecare dispozitiv conectat la rețeaua Wi-Fi (SSID) dorită.<br>Se va deschide o nouă fereastră denumită **SSID Traffic Control Policy (Politică control trafic SSID)**.<br>Aveți cele patru câmpuri pentru stabilirea limitărilor, anume, **SSID Max. Upload Rate (Rată maximă încărcare per SSID), SSID Max. Download Rate (Rată maximă descărcare per SSID), Client Max. Upload Rate (Rată maximă încărcare per client)** și **Client Max. Download Rate (Rată maximă descărcare per client)**.<br>Toate cele patru câmpuri acceptă valori exprimate în **Mbps**, în intervalul **0,01 – 1000 Mbps**.<br>Pentru salvarea limitărilor apăsați butonul **Add (Adăugare)**.<br>Parametrii sunt disponibili pentru configurare numai atunci când funcția **Traffic Control (Control trafic)** este setată în mod **Manual**. |
| **Save**<br>**(Salvare)** | Apăsați acest buton pentru salvarea tuturor modificărilor, bineînțeles, după ce activați controlul traficului selectând **Manual** și apoi introduceți limitările de rată după ce apăsați **Edit (Editare)** și apoi **Add (Adăugare)**. |
| **Cancel**<br>**(Anulare)** | Anulați modificările dacă nu ați apăsat încă **Save (Salvare)**. |

# 7.2 Submeniul Cloud Maintenance (Mentenanță cloud)

## 7.2.1 Prezentare generală

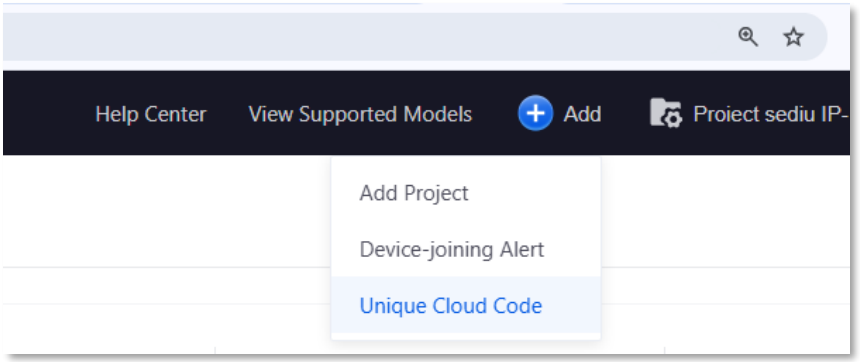
Meniul **Advanced (Avansat) > Cloud Maintenance (Mentenanță cloud)** permite adoptarea punctului de acces în platforma de gestionare unificată **IP-COM ProFi Cloud**, soluția cloud dezvoltată de IP-COM pentru administrarea centralizată a echipamentelor compatibile. Odată adoptat, AP-ul (împreună și cu alte AP-uri) poate fi configurat și monitorizat de oriunde, fie din aplicația mobilă **IP-COM ProFi**, de Android și iOS, fie din interfața web a platformei, accesibilă la adresa https://imsen.ip-com.com.cn. Astfel, toți parametrii echipamentului — de la setările radio și SSID-uri, până la regulile de securitate și optimizările de performanță — devin accesibili centralizat, fără a mai fi necesară conectarea directă la interfața locală a fiecărui AP.

Din acest meniu, **Advanced (Avansat) > Cloud Maintenance (Mentenanță cloud)**, se permite comutarea modului de gestionare a AP-ului, din cloud sau locală.



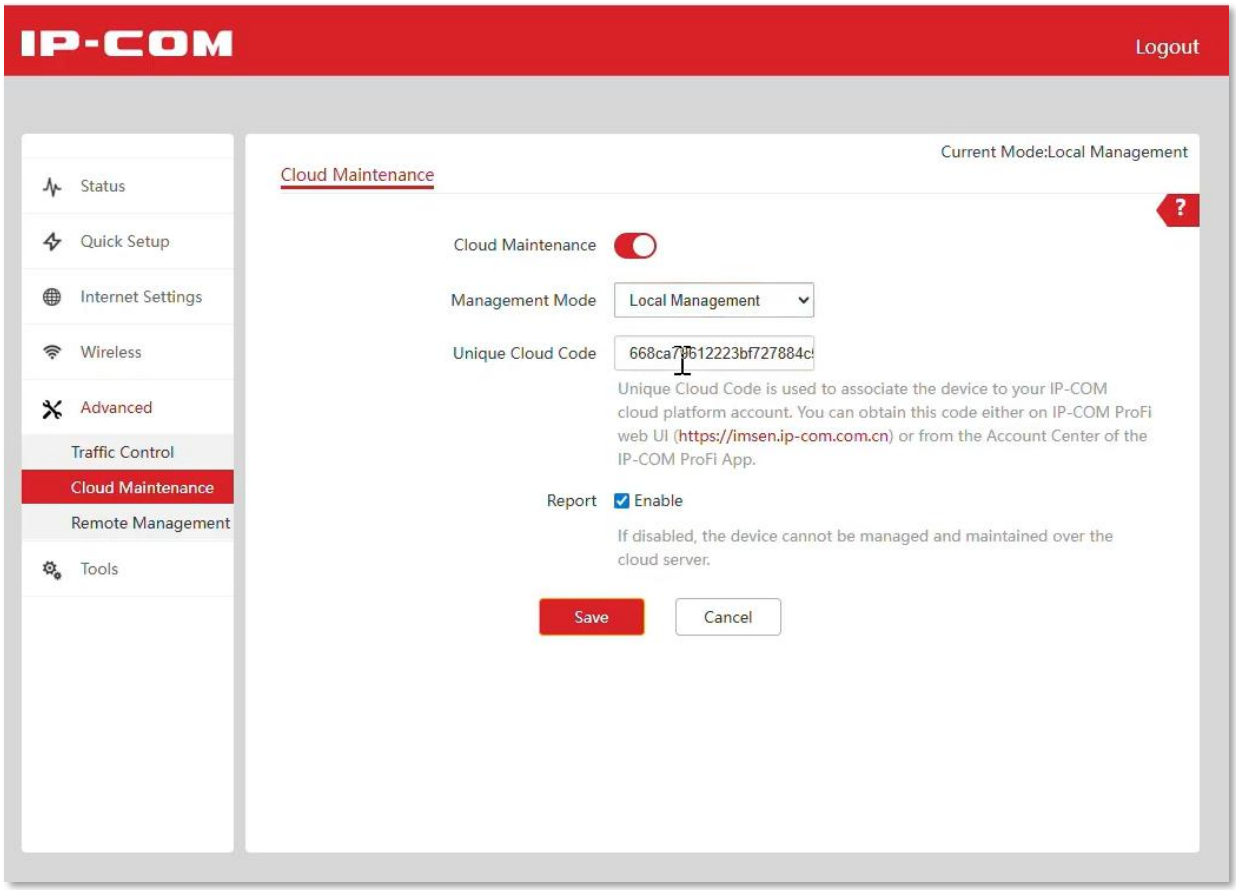

**Descriere parametri Advanced (Avansat) > Cloud Maintenance (Mentenanță cloud)**

| Parametru | Descriere |
|---|---|
| **Cloud Maintenance (Mentenanță cloud)** | Specifică dacă se activează funcția de mentenanță din cloud prin **IP-COM ProFi Cloud** și a tuturor opțiunilor de configurare din pagină, inclusiv comutarea modului de gestionare a punctului de acces. |

| Parametru | Descriere |
| --- | --- |
| Management Mode<br>(Mod gestionare) | Specifică modurile în care este gestionat punctul de acces.<br>– **Cloud Management (Managementul cloud-ului):** Aplicabil scenariilor care necesită configurare și întreținere unificate prin serviciul cloud **IP-COM ProFi Cloud**. În acest mod, toată configurația dispozitivului este furnizată din cloud către AP. Aproape toate meniurile și opțiunile din interfața locală nu mai sunt vizibile și nu pot fi configurate din interfața locală.<br>– **Local Management (Gestionare locală):** În acest mod, toate configurațiile dispozitivului sunt finalizate pe propria interfață web, iar informațiile sunt doar raportate către platforma cloud **IP-COM ProFi**. În acest mod toate meniurile și opțiunile din interfața locală sunt vizibile și configurabile. |
| **Unique Cloud Code**<br>**(Cod cloud unic)** | În acest câmp se copiază codul unic aferent contului cu care v-ați înregistrat în **IP-COM ProFi Cloud**. Îl puteți obține din aplicația de Android sau iOS sau din platforma web https://imsen.ip-com.com.cn, accesând apoi meniul **+Add (+Adăugare) > Unique Cloud Code (Cod cloud unic)**.<br> |
| **Report**<br>**(Raportare)** | Activează sau dezactivează funcția de raportare a punctului de acces către platforma cloud.<br>Această opțiune este dezactivată în mod implicit. Odată activată, AP-ul transmite periodic către platforma **IP-COM ProFi Cloud** informații despre parametrii săi de funcționare, permițând astfel administratorului să gestioneze și să întrețină echipamentul direct din cloud, fără a fi necesară conectarea locală la AP. |
| **Save**<br>**(Salvare)** | Apăsați acest buton pentru salvarea modificărilor și așteptați aplicarea setărilor. |
| **Cancel**<br>**(Anulare)** | Anulați modificările făcute, însă, înainte de apăsarea butonului **Save (Salvare)**. |

## 7.2.2 Selectarea modului de gestionare

Tot din meniul **Advanced (Avansat) > Cloud Maintenance (Mentenanță cloud)**, secțiunea **Management Mode (Mod gestionare)** permite alegerea modului în care este administrat AP-ul.




Sunt disponibile două opțiuni:

- **Local Management (Gestionare locală)**: AP-ul este gestionat exclusiv prin interfața sa web locală sau prin controlerul ruterului multi-WAN din seria M etc., dacă a fost adoptat acolo.
- **Cloud Management (Gestionare cloud)**: AP-ul este gestionat din platforma IP-COM ProFi Cloud.

Atunci când este activată opțiunea **Cloud Management (Gestionare cloud)**, interfața locală a AP-ului devine simplificată: majoritatea opțiunilor granulare și avansate precum setările fine de roaming, optimizările radio sau politicile de control al traficului sunt ascunse, întrucât administrarea se presupune a fi făcută din cloud din **IP-COM ProFi Cloud**. În schimb, dacă se selectează **Local Management (Gestionare locală)**, chiar și atunci când AP-ul este deja adoptat în cloud, atunci toate setările avansate redevin vizibile și editabile din interfața web locală.

Pentru a configura opțiuni specifice modelului respectiv, precum, parametri care nu sunt expuși în interfața **IP-COM ProFi Cloud** sau care necesită ajustare fină, procedați astfel:

1. Comutați temporar pe **Local Management (Gestionare locală)** și salvați apăsând **Save (Salvare)**.
2. Efectuați configurările dorite din interfața web locală.

3. Reactivați **Cloud Management (Gestionare cloud)** și salvați pentru a reveni la administrarea unificată din **IP-COM ProFi Cloud**.

   Este important de precizat că, indiferent de modul selectat — **Local Management (Gestionare locală)** sau **Cloud Management (Gestionare cloud)** — AP-ul adoptat nu va dispărea din platforma **IP-COM ProFi Cloud**. Comutarea între cele două moduri afectează exclusiv locul din care se efectuează configurările, nu și statutul de adopție al echipamentului în cloud.

## 7.2.3 Moduri de adăugare echipament în IP-COM ProFi Cloud

Pentru gestionarea echipamentului din **IP-COM ProFi Cloud** trebuie ca acesta să fie adoptat. Există mai multe metode de adoptare la acest serviciu.

Tip

Înainte de a configura funcția de gestionare din IP-COM ProFi Cloud a punctului de acces, asigurați-vă că echipamentul este conectat la internet. Pentru asta verificați setările IP de la meniul **Internet Settings (Setări internet)** > **LAN Setup (Configurare LAN)** > fila **LAN Setup (Configurare LAN)**.

### Metoda 1: Adăugare în cloud folosind aplicația de mobil IP-COM ProFi

1. Obțineți aplicația **IP-COM ProFi** din **Google Play** sau **App Store** sau scanând codul QR.




**IP-COM ProFi**

2. Autentificați-vă la aplicație cu contul anterior creat.
3. Conectați mobilul la Wi-Fi-ul emis de AP.

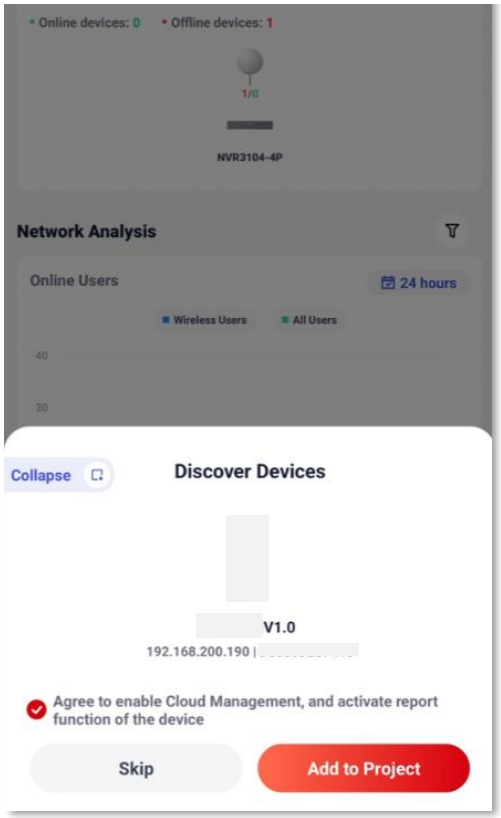
Tip

- Dacă ați configurat rețeaua Wi-Fi emisă de punctul de acces prin intermediul interfeței web a acestuia, numele și parola Wi-Fi ale punctului de acces sunt cele pe care le-ați setat la **Wireless > SSID**.
- Dacă punctul de acces este gestionat de un controler de AP-uri sau ruter multi-WAN IP-COM seria M, atunci conectați-vă la pagina de gestionare a controlerului sau a ruterului pentru a vizualiza numele și parola Wi-Fi împinse către acest punct de acces.
- Dacă punctul de acces nu este gestionat de niciun dispozitiv de rețea (ruter cu funcție de controler sau platformă cloud) și nu a fost configurat detaliat, acesta va emite rețelele Wi-Fi implicite din fabrică, cu denumirile **IP-COM_XXXXXX** (banda de 2,4 GHz) și **IP-COM_XXXXXX_5G** (banda de 5 GHz), unde *XXXXXX* reprezintă ultimele șase caractere ale adresei MAC inscripționate pe eticheta echipamentului.

4. Deschideți aplicația **IP-COM ProFi**

5. Alegeți un proiect existent sau creați unul nou apăsând butonul din colțul din dreapta-jos.

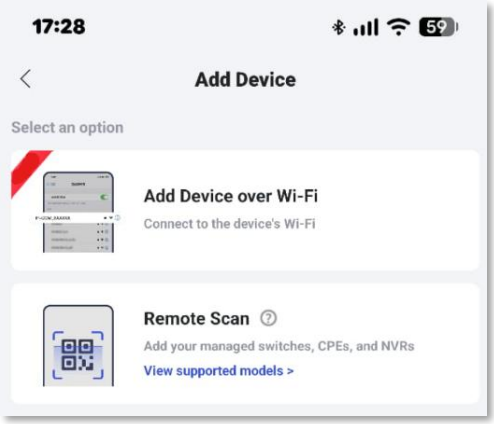
6. Apoi, atingeți fereastra pop-up care arată că AP-ul este detectat. Bifați **Agree to enable Cloud Management, and activate report function of the device (De acord cu activarea funcției Gestionare cloud și a funcției de raportare a echipamentului)**. Apoi apăsați butonul **Add to Project (Adăugare la proiect)**.




7. Dacă fereastra pop-up nu apare, atingeți butonul din sus-dreapta și urmați instrucțiunile din fereastra **Add Device (Adăugare dispozitiv)**.

   – Aveți de selectat **Add Device over Wi-Fi (Adăugare dispozitiv via Wi-Fi)** iar echipamentul va fi detectat după o scanare a rețelei locale, de aproximativ 30 de secunde.

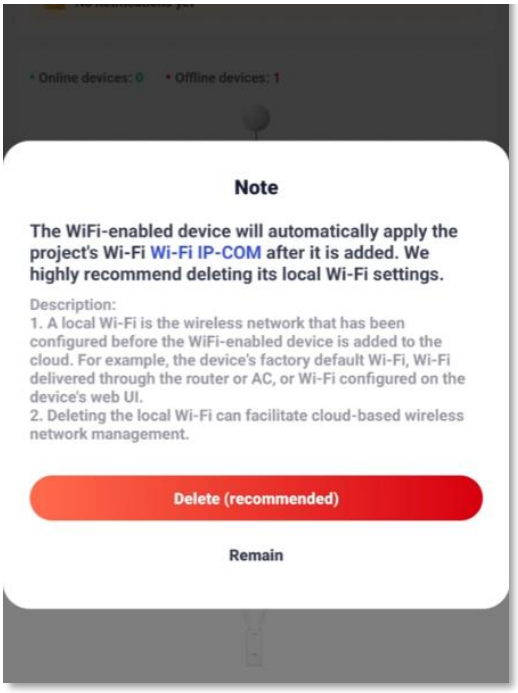
– Sau puteți selecta **Remote Scan (Scanare remote)** care vă permite să scanați codul QR de pe echipament.




8. Apoi după selectarea echipamentului adăugați-l.

   La adoptarea AP-ului în platforma cloud, aplicația **IP-COM ProFi** afișează o notificare care anunță că echipamentul va prelua automat configurația Wi-Fi definită la nivelul proiectului (în exemplu, rețeaua ***Wi-Fi IP-COM***) și recomandă ștergerea setărilor Wi-Fi locale existente pe AP — fie cele implicite din fabrică, fie cele configurate anterior prin ruter multi-WAN seria M, controler dedicat sau interfața web a echipamentului.

   Utilizatorul are două opțiuni: **Delete (recommended) (Ștergere (recomandat))**, care elimină configurația locală și permite gestionarea unitară a rețelei wireless din cloud, sau **Remain (Păstrare)**, care menține setările Wi-Fi existente pe AP.



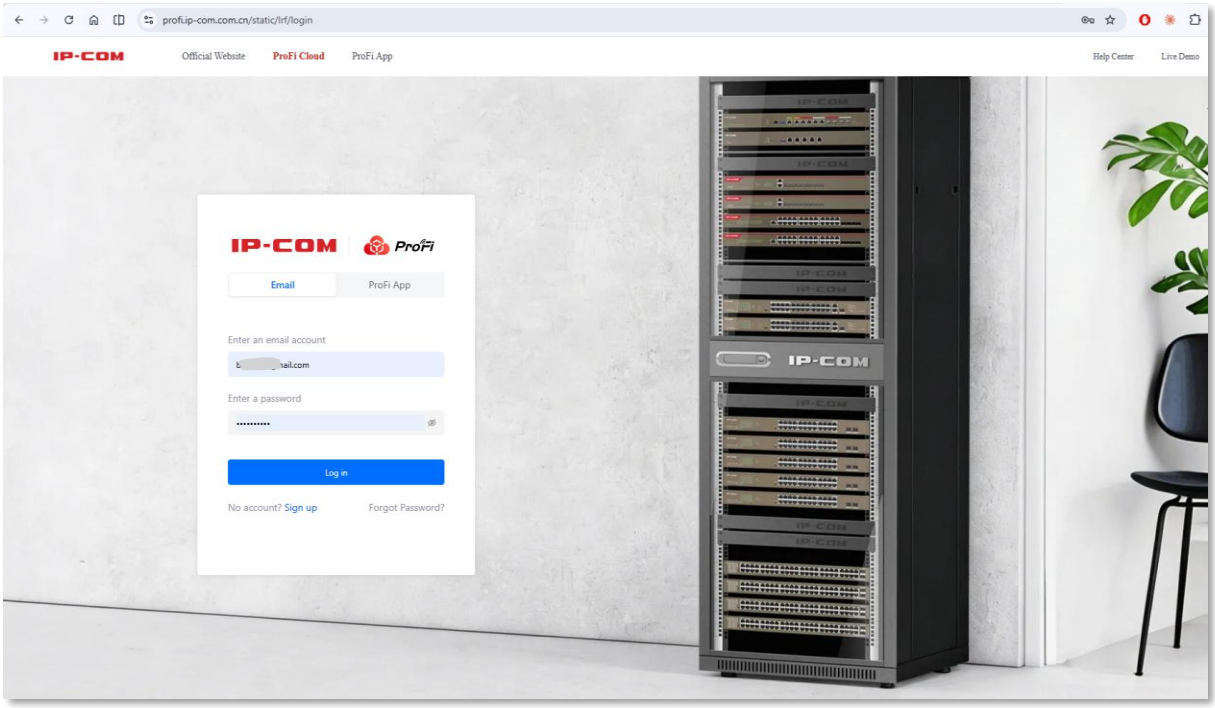

9. Confirmați adoptarea în cloud.

10. Apoi, după câteva momente, o să vedeți echipamentul în proiectul adăugat, fie din **aplicația IP-COM ProFi**, de Android și iOS, fie din pagina web https://imsen.ip-com.com.cn.

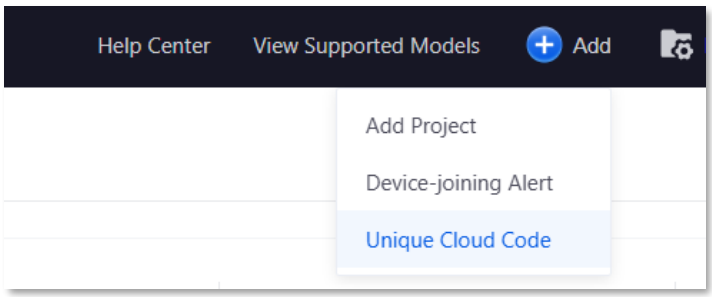
**---Sfârșit**

## Metoda 2: Adăugare în cloud, din interfața locală web a AP-ului, copiind codul unic de cloud

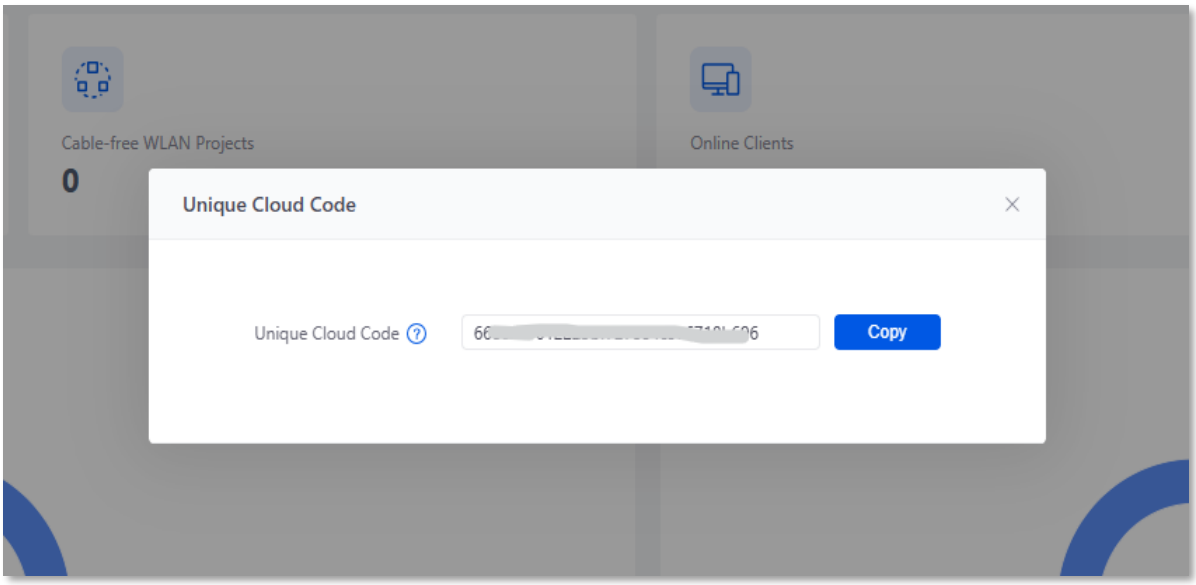
1. Prima dată trebuie să faceți rost de codul unic aferent contului cu care v-ați înregistrat în **IP-COM ProFi Cloud**. Așadar accesați platforma web https://imsen.ip-com.com.cn folosind un browser.
2. Autentificați-vă cu contul dumneavoastră de **IP-COM ProFi Cloud**, folosind adresa de email și parola, apoi apăsați **Login (Autentificare)**. Se consideră că deja v-ați creat un cont apăsând **Sign up (Înregistrare)**.



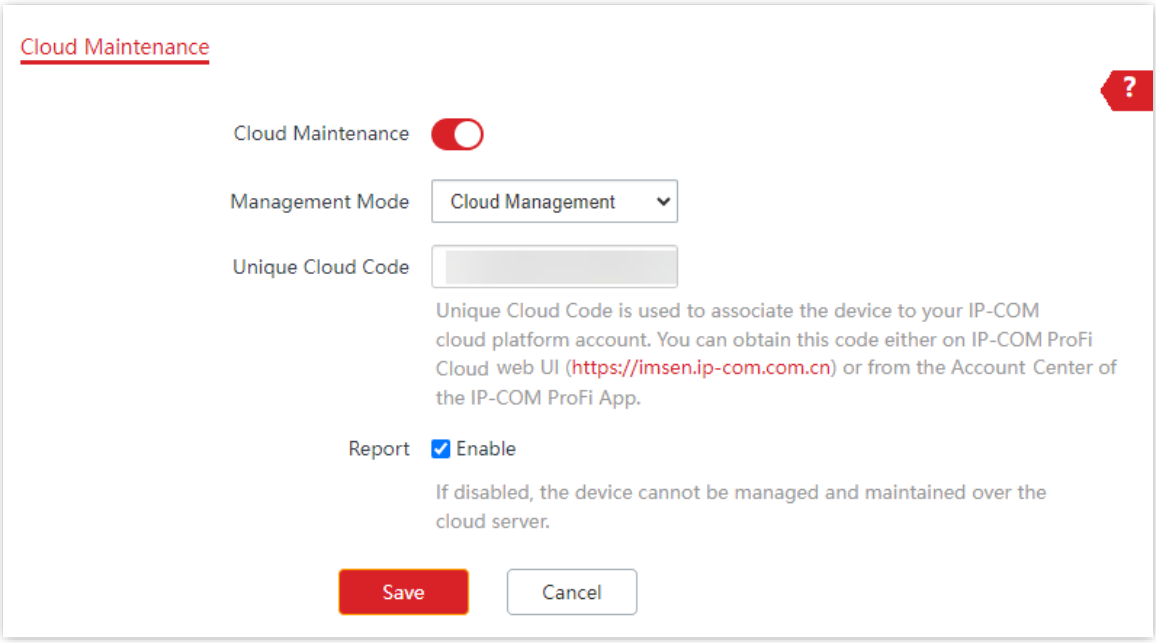

3. Apoi accesați meniul de sus **+Add (+Adăugare) > Unique Cloud Code (Cod cloud unic)**.



4. Copiați codul apăsând **Copy (Copiere)** în noua fereastră. Salvați codul pentru utilizarea ulterioară.

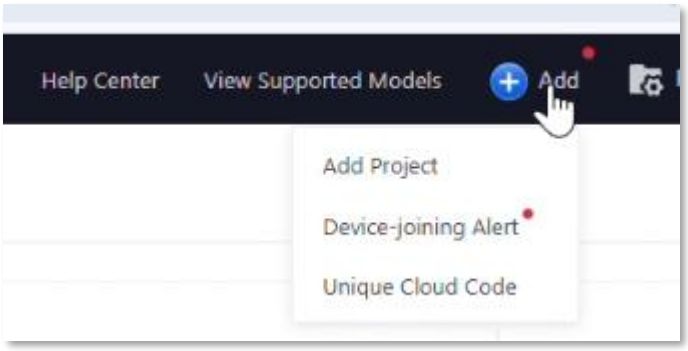



5. Acum accesați interfața web de gestionare a AP-ului. Așadar, conectați-vă la interfața web a punctului de acces. Se presupune că ați efectuat deja configurarea inițială pas cu pas a echipamentului.
6. Din interfața web de gestionare vă asigurați că echipamentul are acces la internet, verificând setările IP de la **Internet Settings (Setări internet) > LAN Setup (Configurare LAN) >** fila **LAN Setup (Configurare LAN)**.
7. Apoi, navigați la meniul **Advanced (Avansat)** > **Cloud Maintenance (Mentenanță cloud).**
8. De aici activați funcția **Cloud Maintenance (Mentenanță cloud).**
9. Mai jos la **Management Mode (Mod gestionare)**, pentru moment, activați gestionarea din cloud selectând opțiunea **Cloud Management (Gestionare cloud)**.
10. Lipiți codul copiat de la pasul 4, la câmpul **Unique Cloud Code (Cod cloud unic)**.
11. Bifați funcția **Report (Raportare).**
12. Faceți clic pe **Save (Salvare)** și așteptați câteva momente.

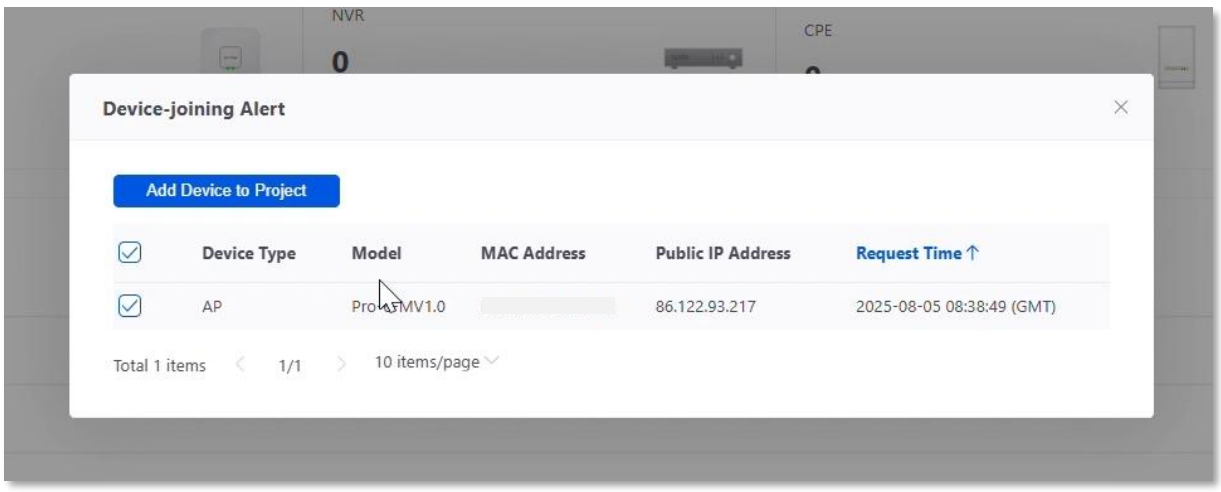



13. După 1-5 minute, reaccesați platforma web **IP-COM ProFi Cloud**, tastând în bara de adrese a unui browser: https://imsen.ip-com.com.cn.

14. Accesați meniul de sus **+Add (+Adăugare) > Device-joining Alert (Alertă asociere echipament)**. O să observați un punct roșu ceea ce indică că un nou echipament este în așteptare spre a fi adăugat la un proiect.



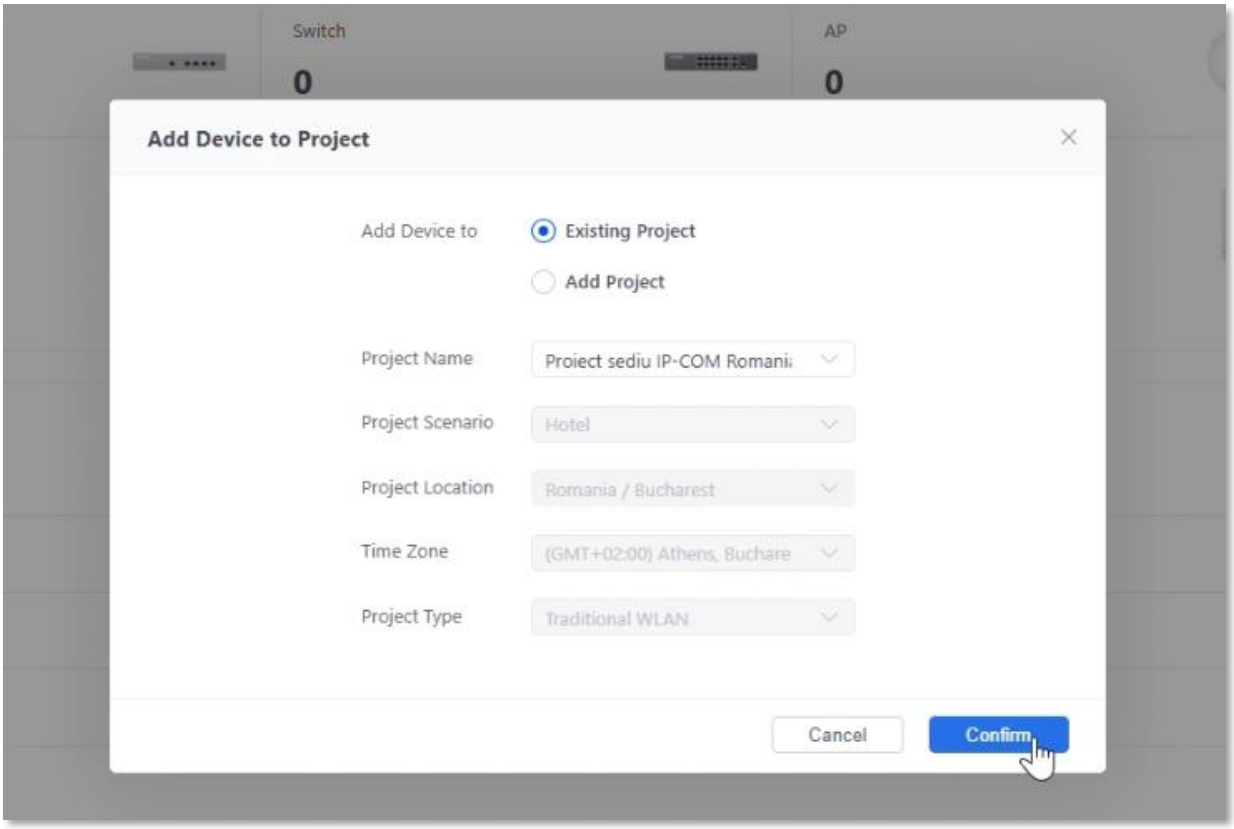

15. Apoi în noua fereastră **Device-joining Alert (Alertă asociere echipament)**, bifați AP-ul din listă și clic pe butonul **Add Device to Project (Adăugare dispozitiv la proiect)**.



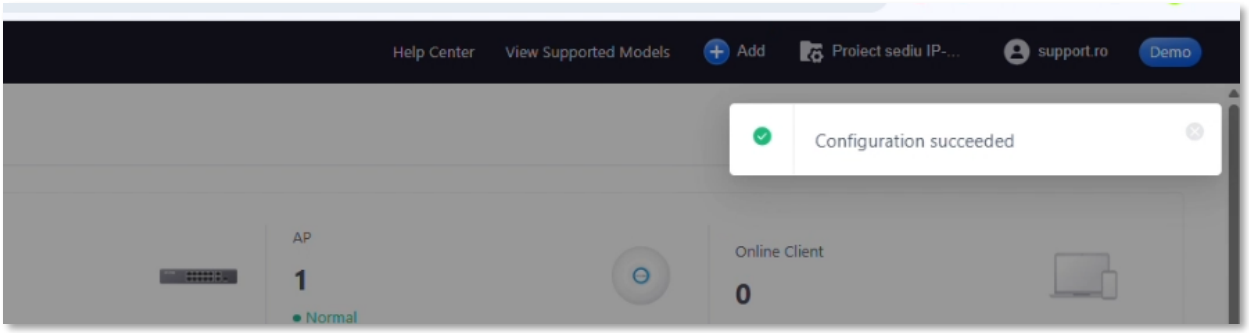
16. Acum trebuie să stabiliți la ce proiect adăugați AP-ul. Un proiect este pur și simplu un container logic în care grupați toate echipamentele de rețea dintr-o locație sau de la un beneficiar. E ca un „dosar” virtual în care puneți laolaltă switch-urile, AP-urile, ruterele și alte echipamente IP-COM care deservesc aceeași rețea fizică.

    Astfel, creați un proiect apăsând **Add Project (Adăugare proiect)** sau selectați un proiect deja creat apăsând **Existing Project (Proiect existent)**. În imaginea de mai jos AP-ul e adăugat la un proiect existent.

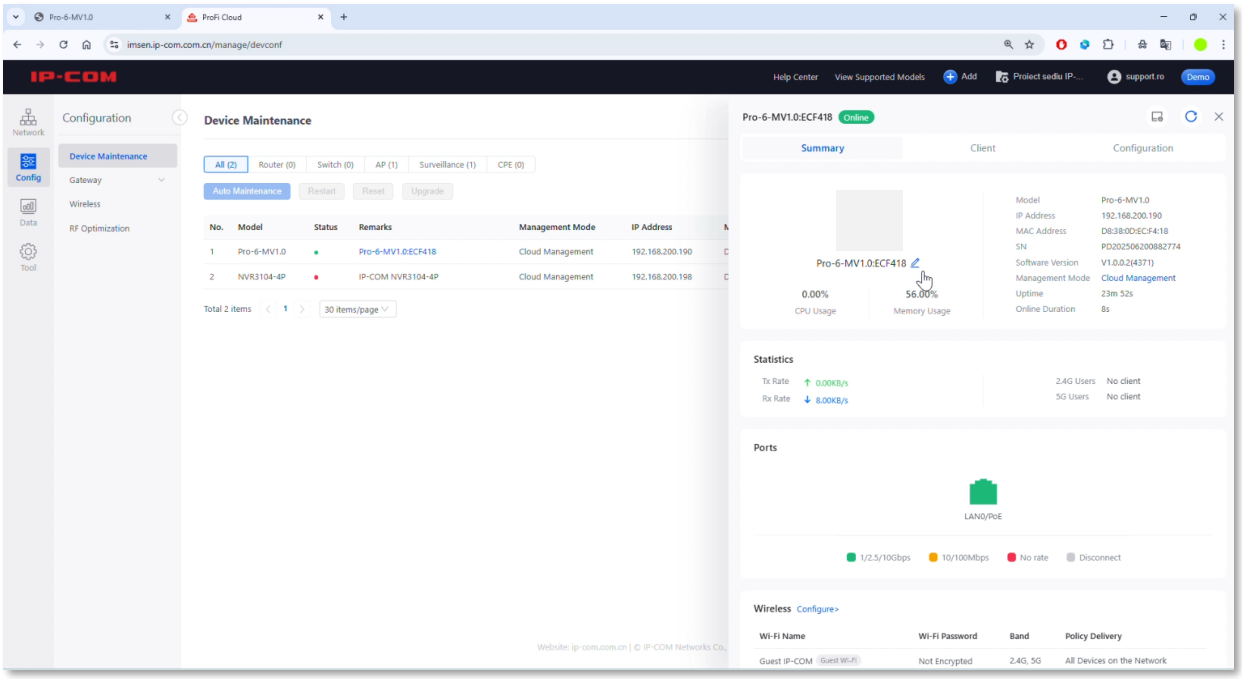
17. Apoi apăsați **Confirm (Confirmare)**.




18. Așteptați câteva momente. Apoi o să vedeți un mesaj de confirmare a adoptării reușite în colțul dreapta-sus al paginii **IP-COM ProFi Cloud**.




19. O să vedeți AP-ul adăugat la proiect. Dați clic pe acesta pentru a deschide panoul de setări aferent AP-ului.

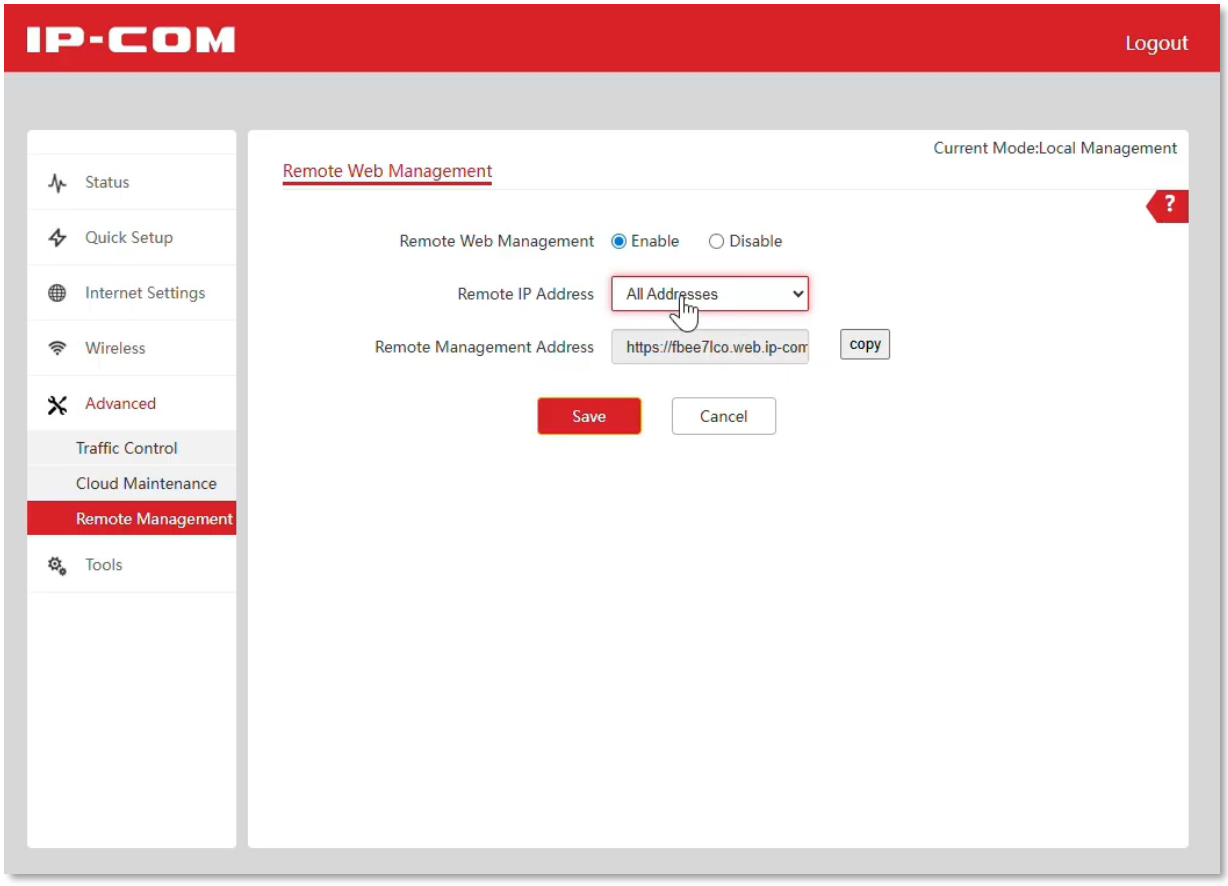



**20.** După finalizarea configurării, punctul de acces poate fi gestionat prin intermediul interfeței web a platformei **IP-COM ProFi Cloud** (https://imsen.ip-com.com.cn) sau prin intermediul aplicației **IP-COM ProFi**. Bineînțeles, trebuie să vă autentificați cu același cont.

# 7.3 Submeniul Remote Management (Gestionare de la distanță)

## 7.3.1 Prezentare generală

Submeniul **Remote Management (Gestionare de la distanță)**, din meniul **Advanced (Avansat)**, vă permite să accesați interfața web de gestionare a punctului de acces de oriunde din internet, nu doar din rețeaua locală. Funcția permite accesul de la distanță la interfața web prin intermediul unui nume de domeniu predefinit oferit de IP-COM, astfel nu mai e nevoie să cunoașteți adresa IP externă. Funcția de gestionare web la distanță este dezactivată în mod implicit.




**Descriere parametri Advanced (Avansat) > Remote Management (Gestionare de la distanță)**

| Parametru | Descriere |
|---|---|
| **Remote Web Management** | Activarea sau dezactivarea funcției de accesarea interfeței web de gestionare a echipamentului din afara rețelei locale, de pe internet. |
| **(Gestionare web de la distanță)** | Cât timp e pe **Disable (Dezactivare)**, restul opțiunilor sunt inactive și nimeni nu poate ajunge la interfața web de gestionare din afara rețelei locale (LAN-ului). |

| Parametru | Parametru |
|---|---|
| **Remote IP Address**<br>**(Adresă IP de la distanță)** | Specifică ce adrese externe pot accesa interfața web de gestionare de pe internet. Există două opțiuni:<br>– **All Addresses (Toate adresele):** Orice IP de pe internet poate încerca să se conecteze la URL-ul de management. Este cea mai permisivă și cea mai riscantă variantă.<br>– **Specified Address (Adresă specificată):** Apare un câmp suplimentar unde introduceți un IP public anume, de exemplu IP-ul fix al unui alt sediu de unde să accesați interfața web de gestionare. Doar acel IP poate accesa interfața. E varianta recomandată într-o implementare sigură. |
| **Remote Management Address**<br>**(Adresă gestionare de la distanță)** | Acesta este URL-ul generat automat de serviciul IP-COM, în forma, de exemplu, ***https://xxxxxxxxxxx.web.ip-com.com.cn:8082***. Unde șirul de caractere ***xxxxxxxxxxx*** este un șir aleator.<br>Salvați această adresă copiind adresa folosind butonul din dreapta.<br>Deschideți apoi această adresă într-un browser. Certificatul SSL emis de IP-COM pentru subdomeniul ***xxxxxxxxxxx.web.ip-com.com.cn*** nu este semnat de o autoritate publică recunoscută de sistemul de operare — este un certificat intern al ecosistemului IP-COM. Conexiunea este criptată, însă browserul nu poate verifica identitatea serverului printr-o autoritate de certificare. De exemplu, în *Google Chrome* apăsați **Advanced (Avansat)** apoi clic pe **Proceed to *xxxxxxxxxxx.web.ip-com.com.cn* (Continuați la *xxxxxxxxxxx.web.ip-com.com.cn)*** și veți putea accesa interfața de gestionare a AP-ului. Desigur, va trebui apoi să introduceți parola de autentificare pentru interfața web, parolă setată din meniul **Tools (Instrumente)** > System Account (Cont sistem). Țineți cont de faptul că navigarea de la un meniu la altul și de la o pagină la alta nu se va efectua instant ca în cazul accesului din rețeaua locală (LAN). |

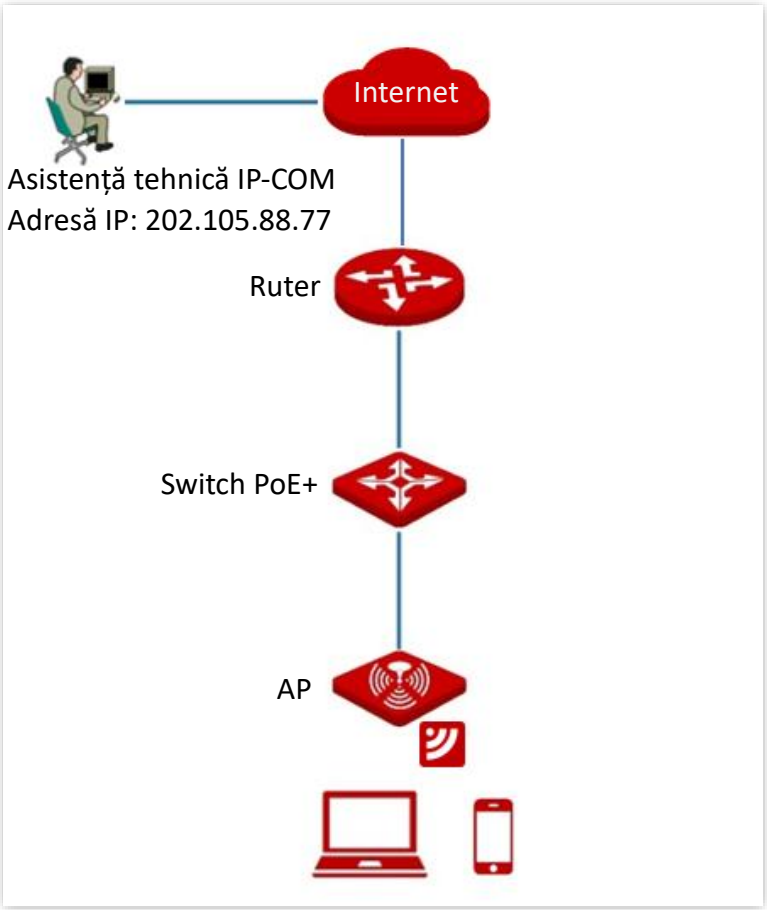
## 7.3.2 Exemplu de configurare a accesului la interfața web de gestionare din afara rețelei locale

**Cerințe**

O întreprindere utilizează un punct de acces IP-COM pentru a configura o rețea Wi-Fi prin care se oferă conexiune la internet. Administratorul de rețea a întâmpinat o problemă în timpul configurării și are nevoie de asistență tehnică din partea IP-COM pentru ca aceștia să se conecteze de la distanță la interfața web a punctului de acces în vederea efectuării unei analize și a operațiunilor de depanare.

**Soluție**

Puteți utiliza funcția **Remote Management (Gestionare de la distanță)** pentru a îndeplini cerințele.

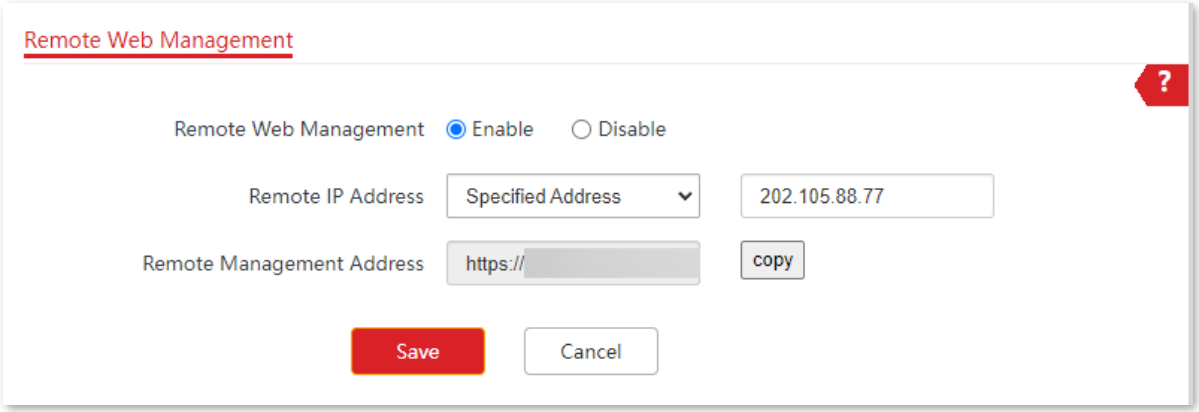



**Procedură**

1. De pe un laptop din rețeaua locală (LAN) în care se află și AP-ul, conectați-vă la interfața web de gestionare a AP-ului.
2. Navigați la **Advanced (Avansat)** > **Remote Management (Gestionare de la distanță).**
3. Activați funcția de **Remote Web Management (Gestionare web de la distanță)**.
4. De la opțiunea **Remote IP Address (Adresă IP de la distanță)** alegeți **Specified Address (Adresă specificată).** Apoi în câmpul din dreapta nou apărut introduceți adresa IP externă dată de tehnicianul IP-COM, care în acest exemplu este ***202.105.88.77***.

   De asemenea, de la Remote IP Address **(Adresă IP de la distanță)** puteți selecta oricare opțiune:

   - **All Addresses (Toate adresele):** Dispozitivele cu orice adresă IP de pe internet pot accesa interfața web a punctului de acces. Din motive de securitate a rețelei, această opțiune nu este recomandată, însă în acest caz puteți selecta această opțiune și nu mai aveți nevoie de IP-ul extern ***202.105.88.77***, primit de la tehnicianul IP-COM.
   - **Specified Address (Adresă specificată):** Doar dispozitivele care comunică de la adresa IP specificată vor putea accesa interfața web a punctului de acces. Dacă dispozitivul aflat la distanță, de pe internet, se află într-o rețea locală, trebuie completată adresa IP publică a gateway-ului acelei rețele. Prin urmare, tehnicianul vă va comunica adresa IP externă a rețelei în care se află, în acest caz ***202.105.88.77***.
5. Faceți clic **pe Save (Salvare)**. Figura următoare este doar pentru exemplificare.




6. Trimiteți tehnicianului IP-COM adresa de la câmpul **Remote Management Address (Adresă gestionare de la distanță)**. Copiați adresa folosind butonul din dreapta.

7. Trimiteți tehnicianului și parola de autentificare la interfața de gestionare, cea de la **Tools (Instrumente)** > **System Account (Cont sistem)**.

8. Asistența tehnică IP-COM se poate conecta la interfața web a punctului de acces accesând URL-ul generat de la **Remote Management Address (Adresă gestionare de la distanță)** și introducând apoi parola de autentificare la interfață. Ulterior puteți accesa jurnalul de sistem pentru a verifica modificări sau conectări efectuate, din meniul **Tools (Instrumente)** > **System Log (Jurnal sistem)**.

**---Sfârșit**

# 8 Meniul Tools (Instrumente)

Funcțiile pot varia în funcție de model și de versiunea software instalată. Imaginile, pașii și descrierile prezentate în acest manual au caracter orientativ și pot diferi de interfața sau funcționarea reală. În acest manual, denumirile meniurilor și ale opțiunilor sunt prezentate în limba engleză, iar echivalentul în limba română este indicat între paranteze. Manualul este adaptat utilizatorilor cunoscători de limba română.

## 8.1 Submeniul Date & Time (Dată și oră)

Din meniul **Tools (Instrumente) > Date & Time (Dată și oră)**, asigurați-vă că data și ora punctului de acces sunt corecte, pentru ca funcțiile bazate pe timp să opereze corespunzător. Acestea pot fi setate fie prin sincronizarea cu un server de timp de pe internet prestabilit, fie manual.

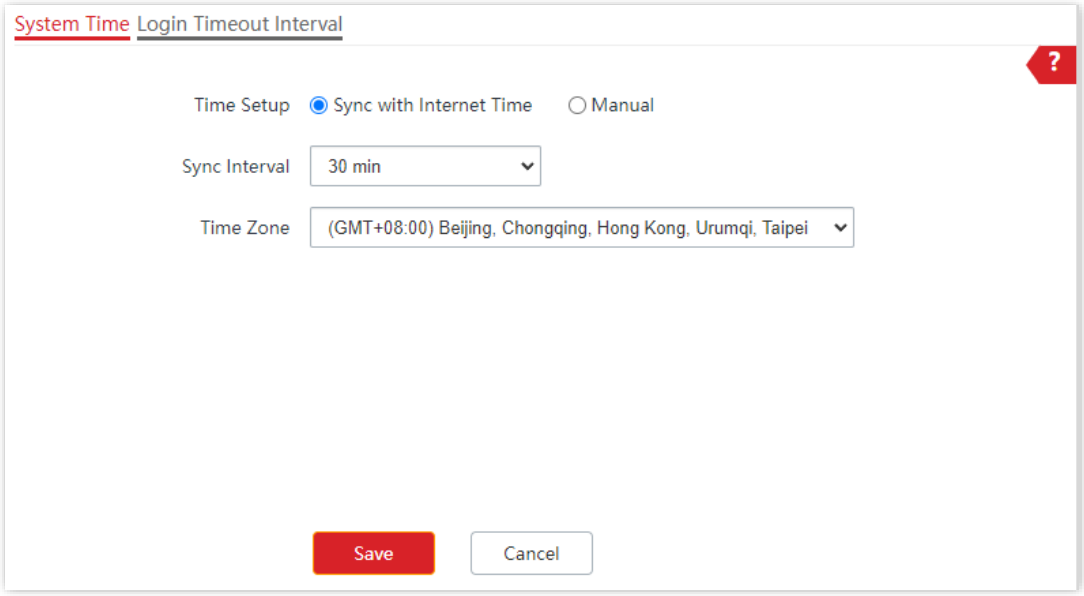
Tot din meniul **Tools (Instrumente) > Date & Time (Dată și oră)** se poate configura și intervalul după care utilizatorul este deconectat automat din interfața de gestionare, în urma unei perioade de inactivitate.

### 8.1.1 Sincronizare dată și oră automată

Punctul de acces își sincronizează automat data și ora sistemului cu un server de timp de pe internet. Acest lucru permite punctului de acces să își corecteze automat ora sistemului după conectarea la internet.

**Procedură pentru sincronizarea automată a timpului**

1. Conectați-vă la interfața web a punctului de acces.
2. Navigați la **Tools (Instrumente)** > **Date & Time (Dată și oră)** > fila **System Time (Timp sistem).**
3. Setați **Time Setup (Configurare timp)** pe **Sync with Internet Time (Sincronizare cu timp internet)**.
4. Setați intervalul la care punctul de acces se va sincroniza automat cu un server de timp al internetului, de exemplu din 30 în 30 de minute selectând **30 min (30 minute)** de la **Sync Interval (Interval sincronizare)**. Puteți selecta **30 min (30 minute)**, **1 hr (1 oră)**, **12 hrs (12 ore)**, **1 day (1 zi)**, **2 days (2 zile)**, **7 days (7 zile)** sau **2 weeks (2 săptămâni)**.
5. Setați fusul orar standard al regiunii în care se află punctul de acces de la **Time Zone (Fus orar)**.
6. Faceți clic pe **Save (Salvare).**




7. După finalizarea configurării, punctul de acces își sincronizează automat data și ora cu un server de timp prestabilit.

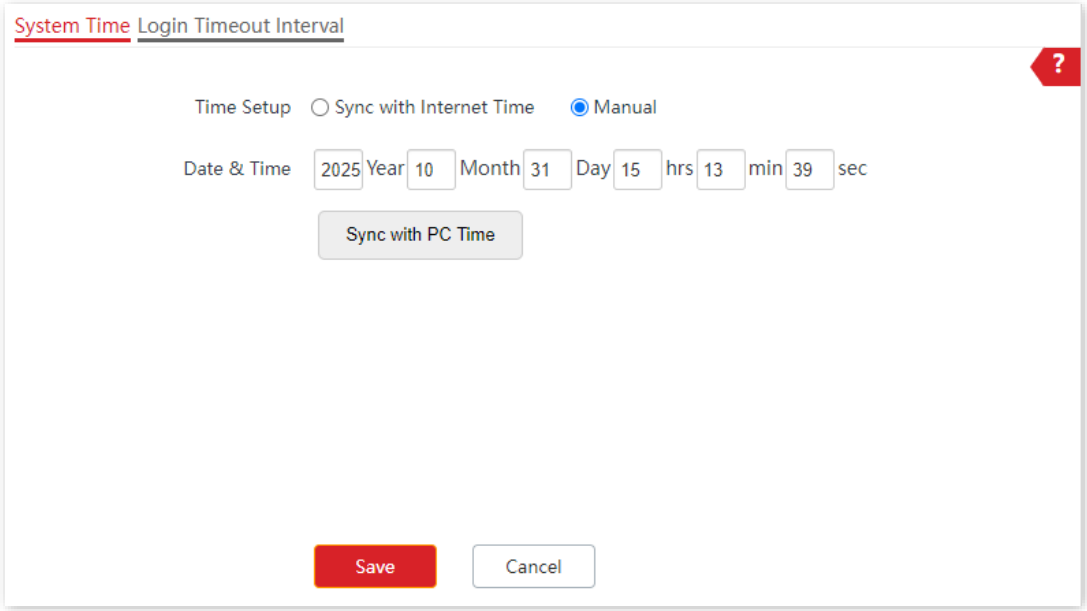
**---Sfârșit**

## 8.1.2 Setare manuală dată și oră

Puteți seta manual data și ora sistemului. Dacă alegeți această opțiune, trebuie să setați ora sistemului de fiecare dată după repornirea AP-ului.

**Procedură pentru setarea manuală a timpului**

1. Conectați-vă la interfața web a punctului de acces.
2. Navigați la **Tools (Instrumente)** > **Date & Time (Dată și oră)** > fila **System Time (Timp sistem)**.



3. Setați **Time Setup (Configurare timp)** pe **Manual.**

4. Apoi, fie introduceți manual anul, luna, ziua, ora, minutul și secunda la câmpurile din secțiunea **Date & Time (Dată și oră)**, fie faceți clic pe butonul **Sync with PC Time (Sincronizare cu timp PC)** pentru a sincroniza data și ora punctului de acces, cu data și ora computerului cu care accesați la acest moment interfața web de gestionare.

5. Faceți clic pe **Save (Salvare).**

**---Sfârșit**

## 8.1.3 Deconectare automată de la interfața de gestionare după o perioadă de inactivitate

De la fila **Login Timeout Interval (Interval expirare autentificare)**, din meniul **Tools (Instrumente)** > **Date & Time (Dată și oră)**, puteți seta intervalul de deconectare de la interfața web de gestionare a AP-ului dacă nu se execută nicio operațiune, precum navigarea între meniuri, selectarea unei funcții sau o configurare.

Intervalul implicit de expirare pentru conectare este de **5** minute. Puteți seta valori între **1** și **60** de minute.

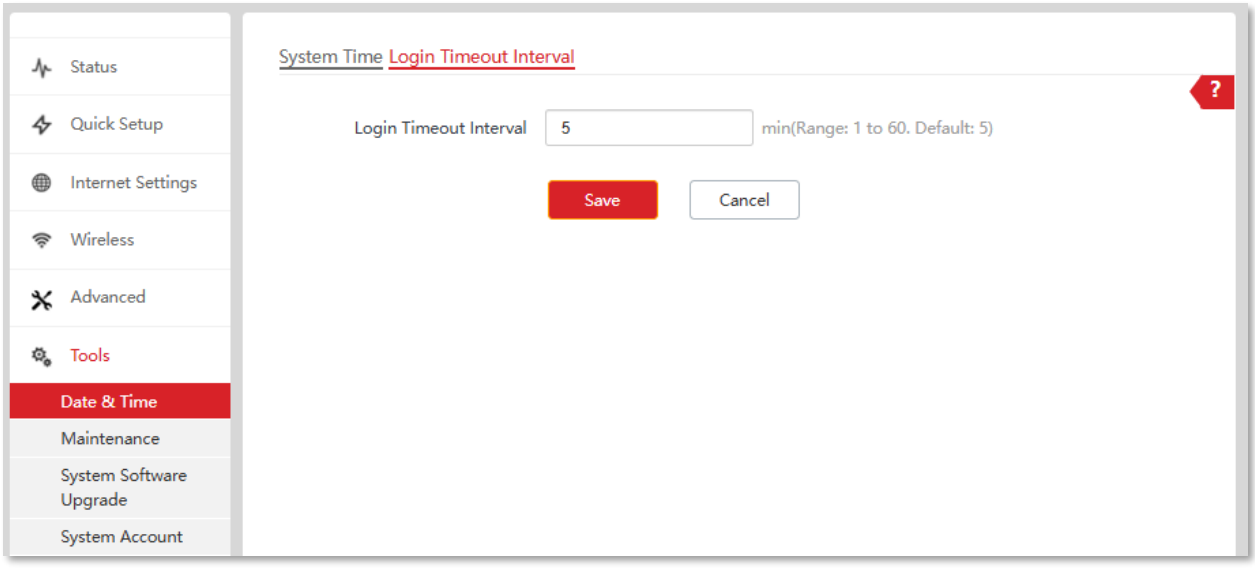
**Procedură pentru configurarea intervalului de deconectare de la interfața web de gestionare**

1. Conectați-vă la interfața web a punctului de acces.

2. Navigați la **Tools (Instrumente)** > **Date & Time (Dată și oră)** > fila **Login Timeout Interval (Interval expirare autentificare)**.

3. Introduceți o valoare validă între **1** și **60** la **Login Timeout Interval (Interval expirare autentificare)** după cum este necesar. În mod implicit, sunteți deconectat după 5 minute. Se pot seta valori între **1** și **60** de minute.

4. Faceți clic pe **Save (Salvare)**.

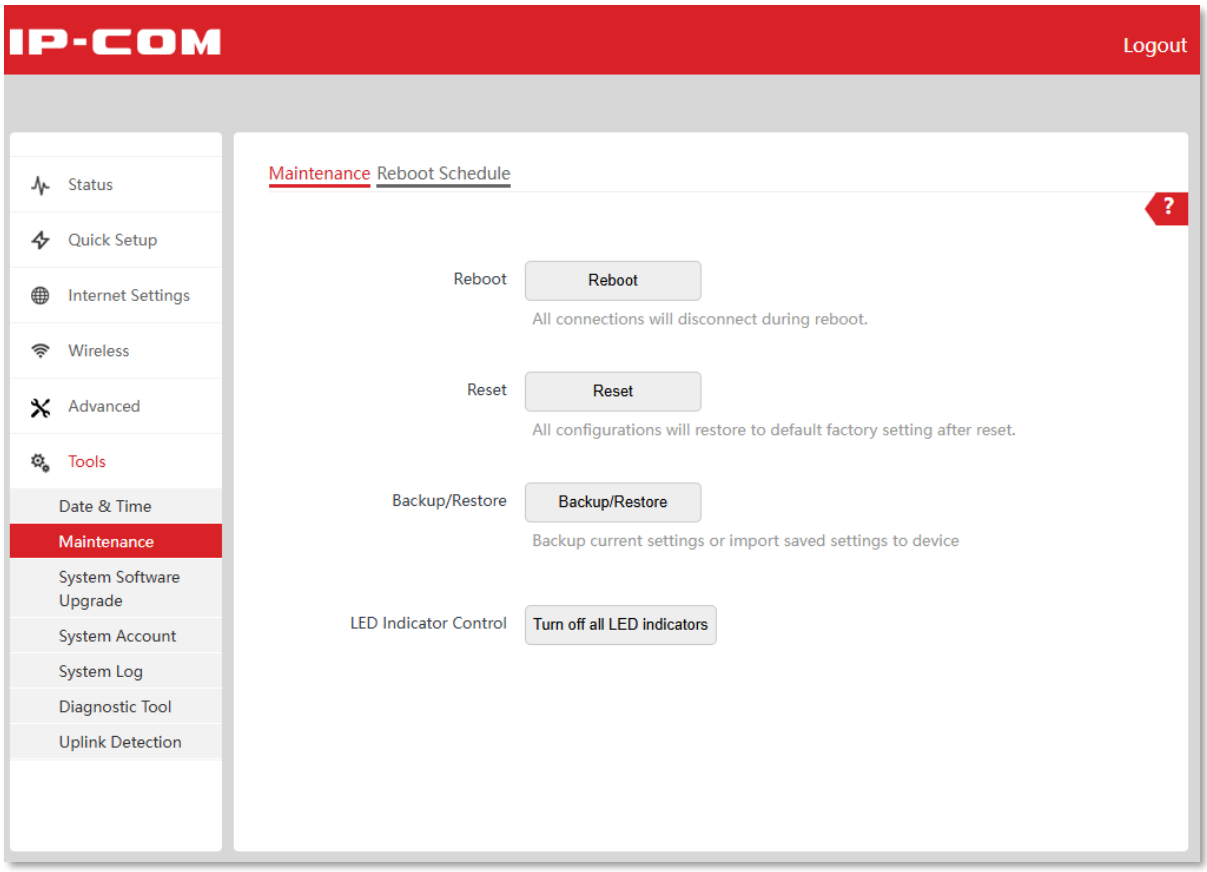



**---Sfârșit**

# 8.2 Submeniul Maintenance (Mentenanță)

Submeniul **Maintenance (Mentenanță)** poate să difere ușor între modele IP-COM.

Astfel, dacă accesați **Tools (Instrumente) > Maintenance (Mentenanță)** > fila **Maintenance (Mentenanță)** arată ca în imaginea de mai jos pe modelele mai noi. Submeniul are două file, anume, **Maintenance (Mentenanță)** unde se regăsesc mai multe funcții de bază precum repornirea, resetarea, salvarea și restaurarea setărilor, dar și oprirea indicatorului led de pe echipament și fila **Reboot Schedule (Programare repornire)** de unde se poate programa repornirea ciclică și pe baza unui orar.

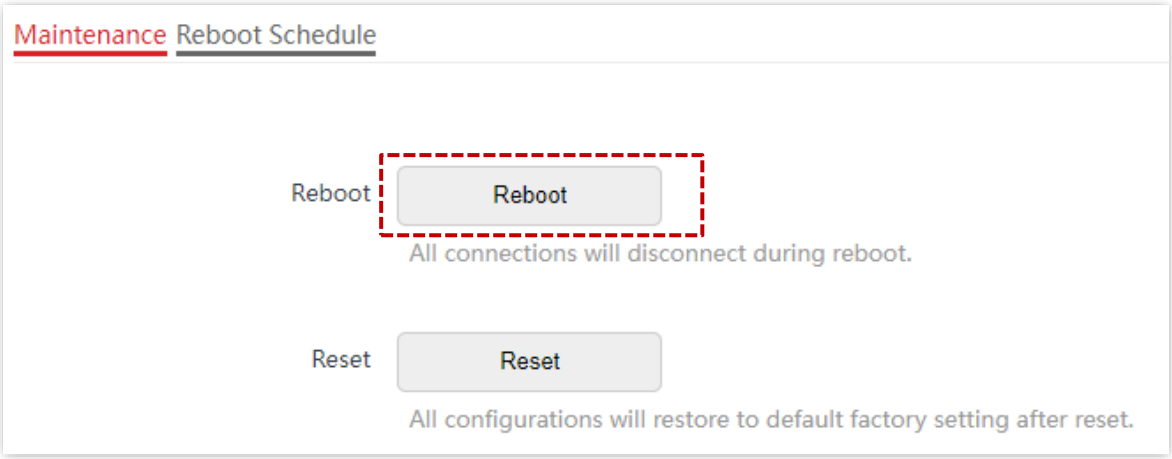



## 8.2.1 Repornire manuală

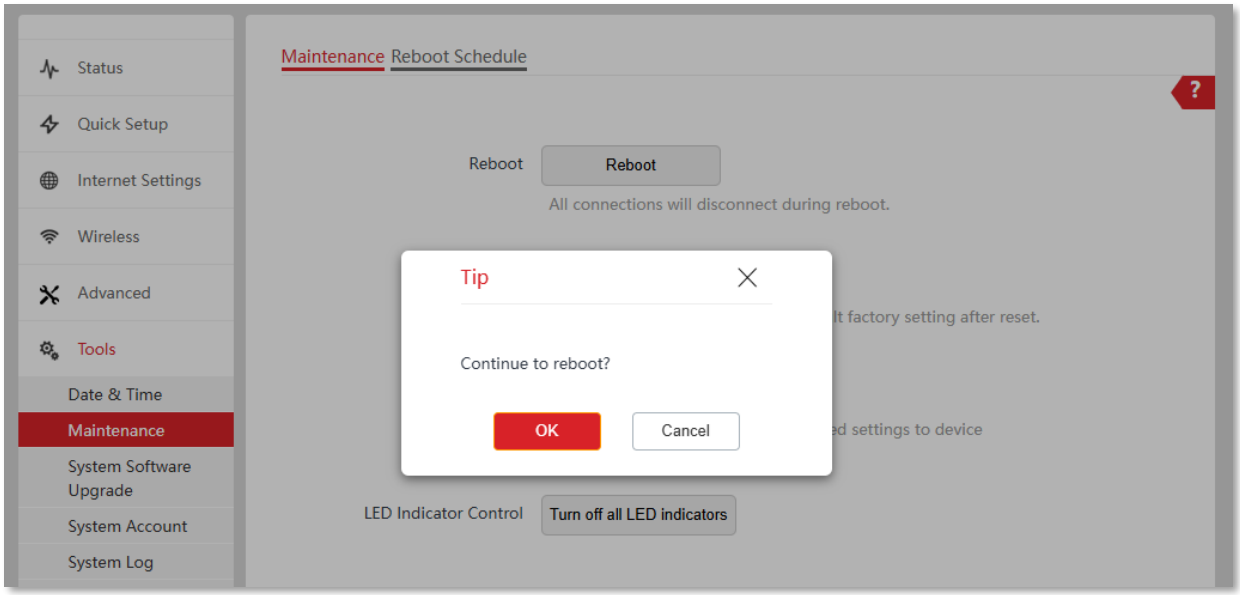
Dacă o setare nu are efect sau punctul de acces funcționează necorespunzător, puteți încerca să reporniți manual punctul de acces pentru a rezolva problema.

**Procedură pentru repornirea AP-ului**

1. Conectați-vă la interfața web a punctului de acces.
1. Navigați la **Tools (Instrumente)** > **Maintenance (Mentenanță)** > fila **Maintenance (Mentenanță)**.
2. Faceți clic pe **Reboot (Repornire)**.




3. Un dialog va fi afișat, confirmați făcând clic pe **OK.**




**---Sfârșit**

## 8.2.2 Repornire periodică automată

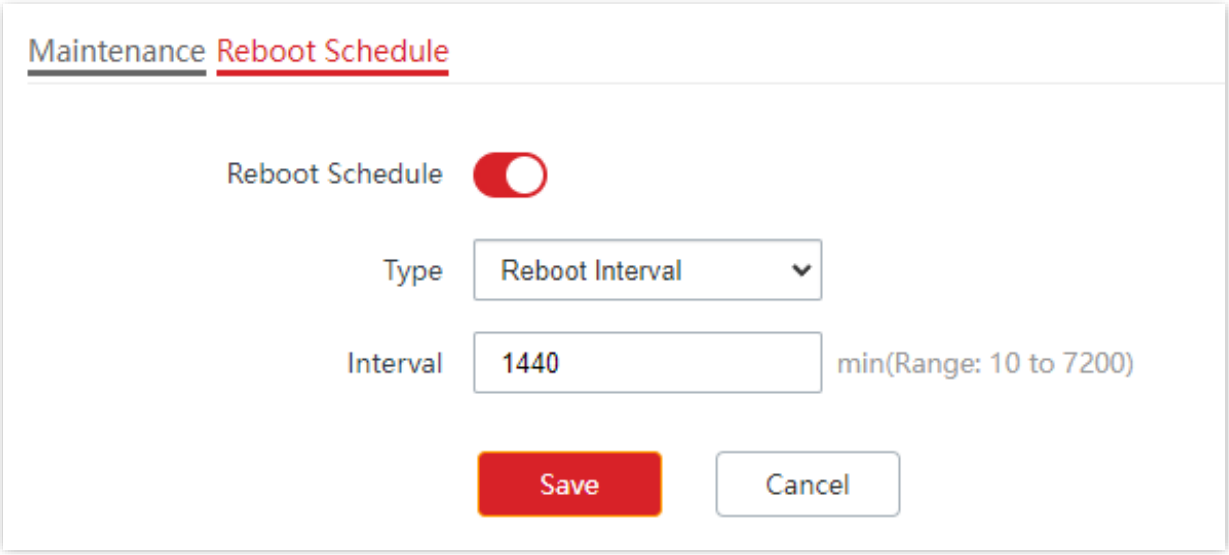
Această funcționalitate permite punctului de acces să repornească automat conform unui orar setat sau la un anumit interval de timp. Puteți utiliza această funcție pentru a preveni anumite tipuri de blocaje care pot apărea după o perioadă lungă de funcționare a punctului de acces în medii extreme de utilizare.

Punctul de acces se poate reporni pe baza unui:

- Interval de repornire: AP-ul se repornește la intervalul specificat.
- Orar de repornire: AP-ul se repornește automat la o anumită oră din zilele din săptămână.

### 8.2.2.1 Repornire periodică la un anumit interval

1. Conectați-vă la interfața web de gestionare a punctului de acces.
2. Navigați la **Tools (Instrumente)** > **Maintenance (Mentenanță)** > fila **Reboot Schedule (Programare repornire)**.
3. Activați funcția **Reboot Schedule (Programare repornire).**
4. De la meniul **Type (Tip)** selectați **Reboot Interval (Interval de repornire)**.
5. La câmpul **Interval** introduceți o valoare în minute, care în acest exemplu este **1440** echivalentul a 24 de ore. Intervalul permis e între 10 și 7200 de minute.
6. Faceți clic pe **Save (Salvare)**.
7. După finalizarea configurării, punctul de acces se va reporni automat la fiecare 24 de ore (1440 minute).




**---Sfârșit**

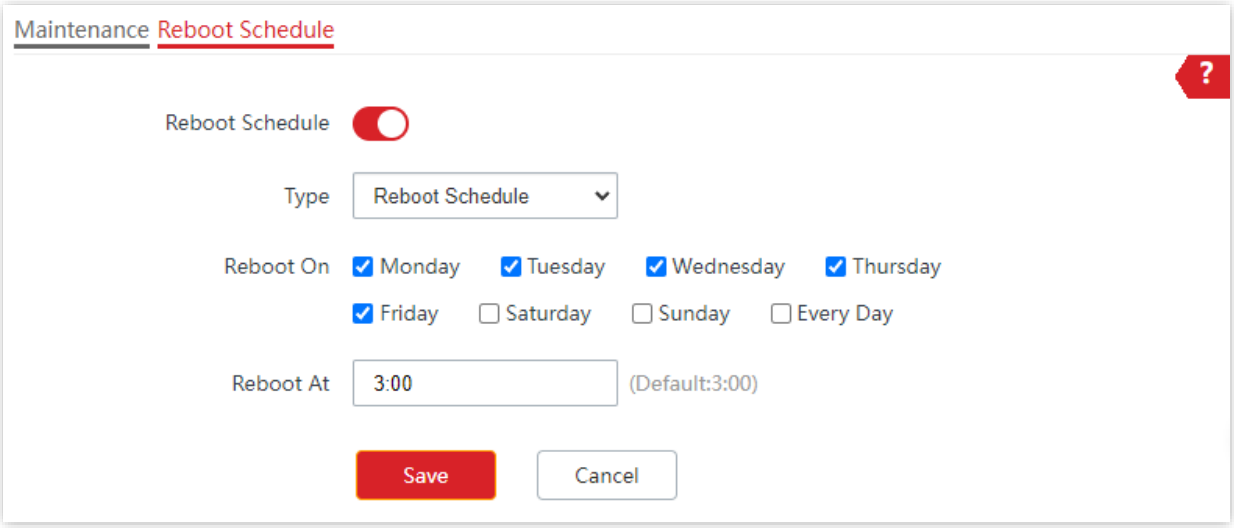
### 8.2.2.2 Repornire periodică pe baza unui orar

Tip

Repornirea la ora specificată se bazează pe ora AP-ului. Pentru a evita erorile de repornire, asigurați-vă că data și ora sunt setate corect de la **Tools (Instrumente) >** **Date & Time (Dată și oră)**.

1. Conectați-vă la interfața web de gestionare a punctului de acces.
2. Navigați la **Tools (Instrumente)** > **Maintenance (Mentenanță)** > fila **Reboot Schedule (Programare repornire)**.
3. Activați funcția **Reboot Schedule (Programare repornire)**.

4. Setați **Type (Tip)** pe **Reboot Schedule (Orar repornire)**.
5. De la **Reboot On (Repornire pe)** bifați zilele din săptămână la care punctul de acces se repornește. În acest exemplu se bifează următoarele zile din săptămână: **Monday (Luni)**, **Tuesday (Marți), Wednesday (Miercuri), Thursday (Joi)** și **Friday (Vineri).**
6. Apoi setați ora pentru repornire aplicabilă pentru orice zi bifată mai sus. Astfel, de la **Reboot At (Repornire la)** se setează ***3:00*.**
7. Faceți clic pe **Save (Salvare).** După finalizarea configurării, punctul de acces se va reporni automat la ora 3 dimineața, în fiecare zi de luni până vineri.




**---Sfârșit**

## 8.2.3 Resetare

Dacă nu puteți depana o defecțiune a punctului de acces sau ați uitat parola de acces la interfața web de gestionare a punctului de acces, puteți reseta echipamentul pentru a restabili setările din fabrică și apoi să îl reconfigurați pas cu pas.

Note

- Când setările din fabrică sunt restaurate, setările făcute anterior vor fi șterse/anulate. Prin urmare, trebuie să reconfigurați punctul de acces pentru a se reconecta la rețeaua din amonte, și implicit la internet. Restaurați setările din fabrică ale punctului de acces numai atunci când este necesar.
- Se recomandă să faceți o copie de rezervă a configurației înainte de a restaura setările din fabrică.
- Pentru a preveni deteriorarea punctului de acces, asigurați-vă că alimentarea cu energie a acestuia funcționează normal atunci când acesta este resetat.

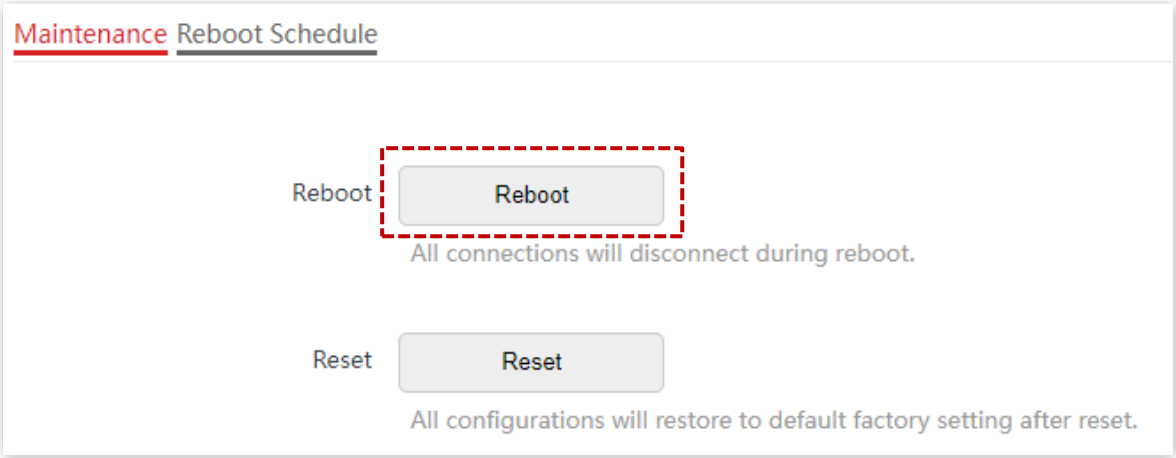
### 8.2.3.1 Resetare folosind butonul fizic de pe echipament

Când punctul de acces este alimentat, țineți apăsat butonul fizic marcat **Reset** timp de aproximativ 8 secunde.

Așteptați aproximativ 1 minut până când punctul de acces este resetat cu succes.

### 8.2.3.2 Resetare din interfața web

1. Conectați-vă la interfața web a punctului de acces.
2. Navigați la **Tools (Instrumente) > Maintenance (Mentenanță) >** fila **Maintenance (Mentenanță)**.
3. Faceți clic pe butonul **Reset (Resetare).**




4. Citiți mesajul afișat și faceți clic pe **OK**. Nu deconectați sursa de curent. Așteptați finalizarea.

**---Sfârșit**

## 8.2.4 Salvare și restaurare setări echipament

Funcția de salvare a configurării sau copie de rezervă, denumită **Backup (Copie de rezervă)**, vă permite să salvați pe computerul local configurația curentă a punctului de acces, iar funcția de restaurare a setărilor, denumită **Restore (Restaurare)**, vă permite să readuceți punctul de acces la o configurație salvată anterior.

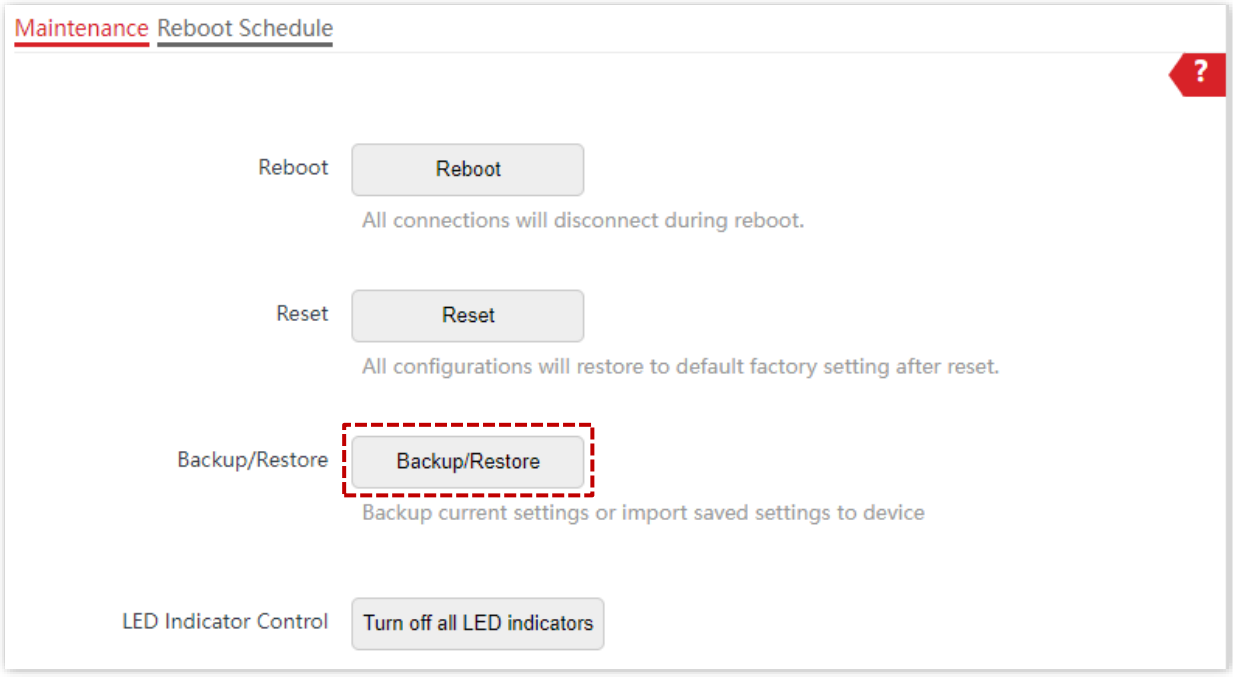
În cazul în care, după modificări semnificative ale configurației, punctul de acces ajunge la o stare de funcționare optimă, vă recomandăm să realizați o copie de rezervă a noii configurații. Astfel, o veți putea restaura cu ușurință după o actualizare sau o resetare a AP-ului.

Tip

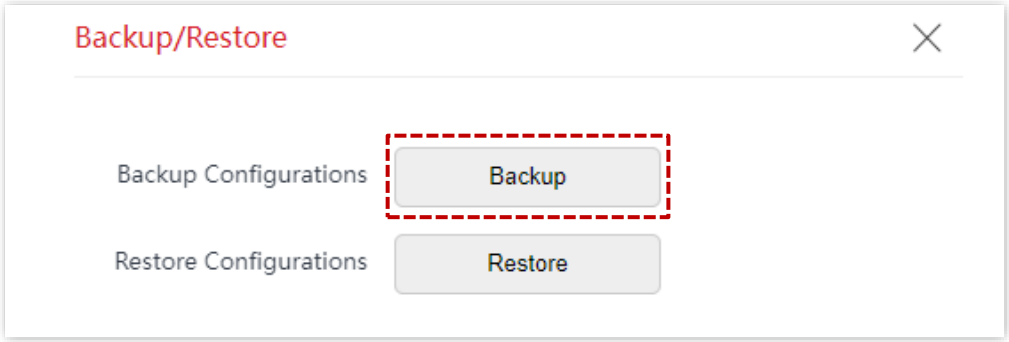
Dacă trebuie să aplicați configurații identice sau similare pe mai multe puncte de acces, este suficient să configurați un singur AP, să creați o copie de rezervă a configurației acestuia și să o utilizați pentru a replica setările pe celelalte echipamente. În acest fel, timpul necesar implementării este redus considerabil, iar consistența configurației în întreaga rețea este garantată.

### 8.2.4.1 Realizare copie de rezervă a setărilor curente

1. Conectați-vă la interfața web a punctului de acces.
2. Navigați la **Tools (Instrumente) > Maintenance (Mentenanță) >** fila **Maintenance (Mentenanță).**
3. Faceți clic pe butonul **Backup/Restore (Copie de rezervă/Restaurare).**




4. În noul dialog faceți clic pe **Backup (Copie de rezervă).**




5. Un fișier de configurare numit ***APCfm.cfg*** este descărcat pe computer. Acest fișier conține setările echipamentului salvate până la momentul apăsării butonului **Backup (Copie de rezervă)**.

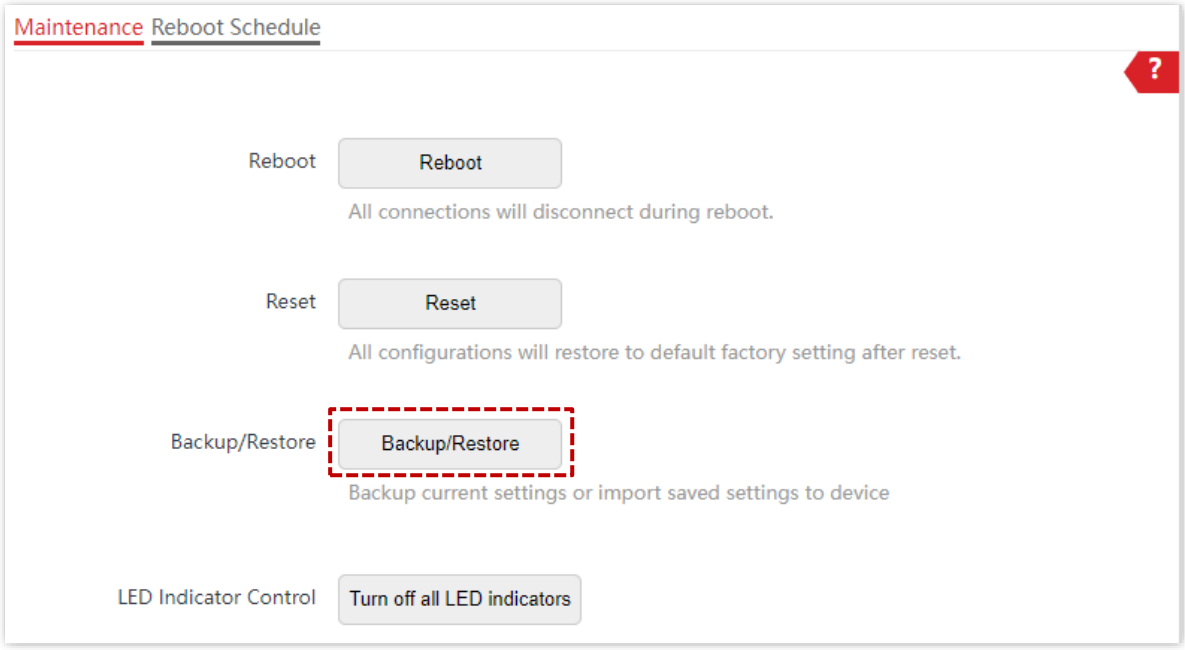
**---Sfârșit**

Tip

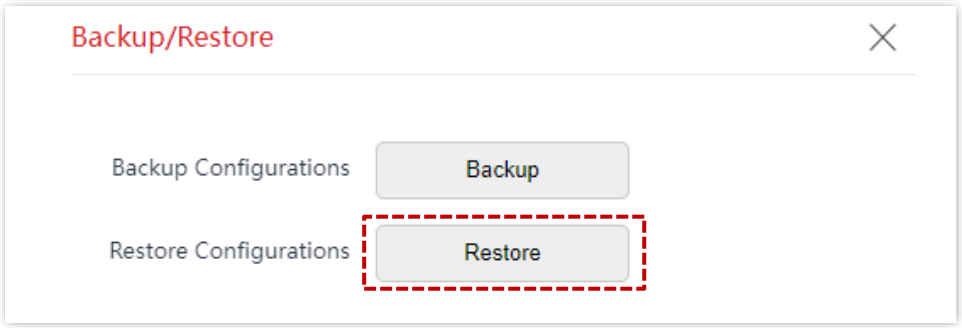
Dacă în browser apare mesajul de avertizare ***Acest tip de fișier poate dăuna computerului. Doriți să păstrați APCfm.cfg oricum?***, faceți clic pe ***Păstrare***.

## 8.2.4.2 Restaurare setări dintr-o copie de rezervă

1. Conectați-vă la interfața web a punctului de acces.
2. Navigați la **Tools (Instrumente) > Maintenance (Mentenanță) >** fila **Maintenance (Mentenanță).**
3. Faceți clic pe **Backup/Restore (Copie de rezervă/Restaurare).**

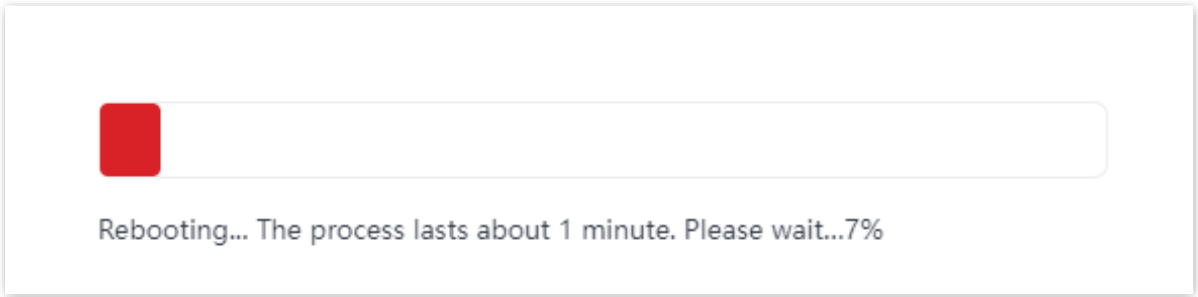



4. Faceți clic pe **Restore (Restaurare).**




5. Apoi pe computer navigați și găsiți un fișier cu setări salvate anterior. Selectați și încărcați fișierul cu sufixul ***.cfg***.

6. Confirmați și așteptați finalizarea procesului de restabilire a setărilor. AP-ul restaurează configurațiile cu succes când bara de progres este finalizată. Echipamentul va reporni pentru a aplica anumite setări restaurate.

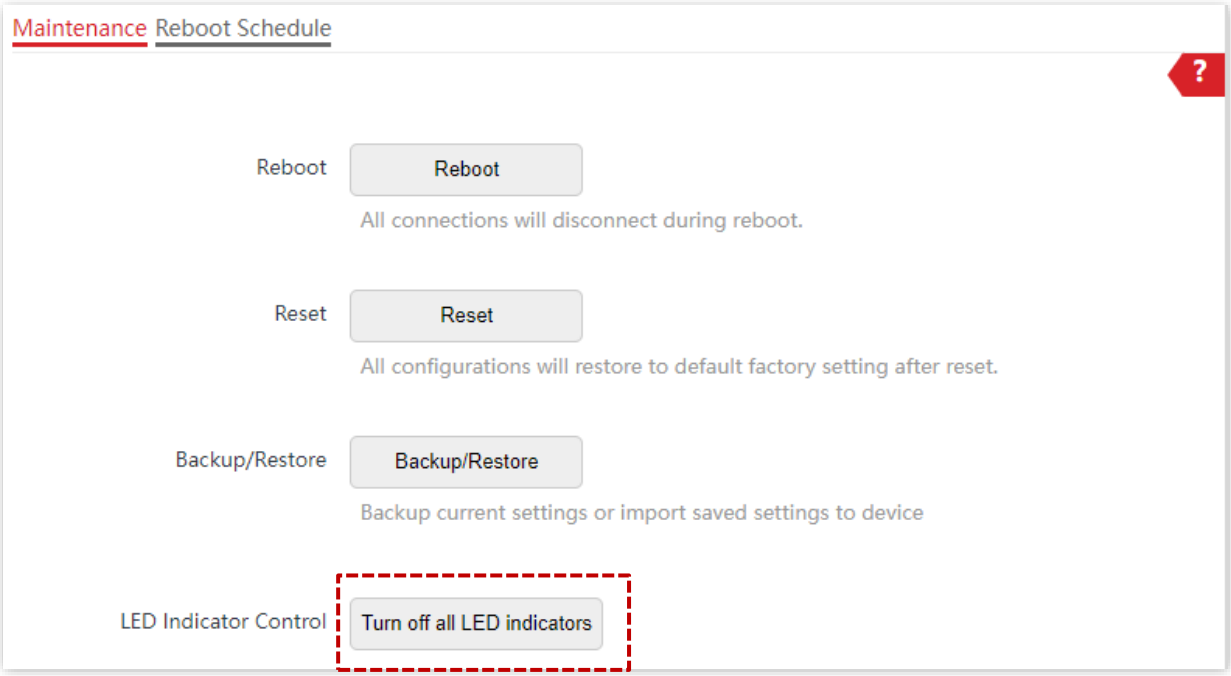


## 8.2.5 Control indicator led de pe echipament

### 8.2.5.1 Dezactivare led

Interfața web oferă posibilitatea de a dezactiva ledul indicator de pe punctul de acces în timpul funcționării normale. Această opțiune este utilă în situațiile în care se dorește evitarea poluării vizuale — de exemplu, în spații de cazare, săli de conferință sau zone de relaxare. Prin punerea la dispoziție a acestui control direct din interfața de administrare, configurarea se realizează rapid, fără intervenție fizică asupra dispozitivului.

1. Conectați-vă la interfața web a punctului de acces.
2. Navigați la **Tools (Instrumente)** > **Maintenance (Mentenanță)** > fila **Maintenance (Mentenanță)**.
3. Faceți clic pe **Turn off all LED indicators (Dezactivare toate ledurile indicatoare).**

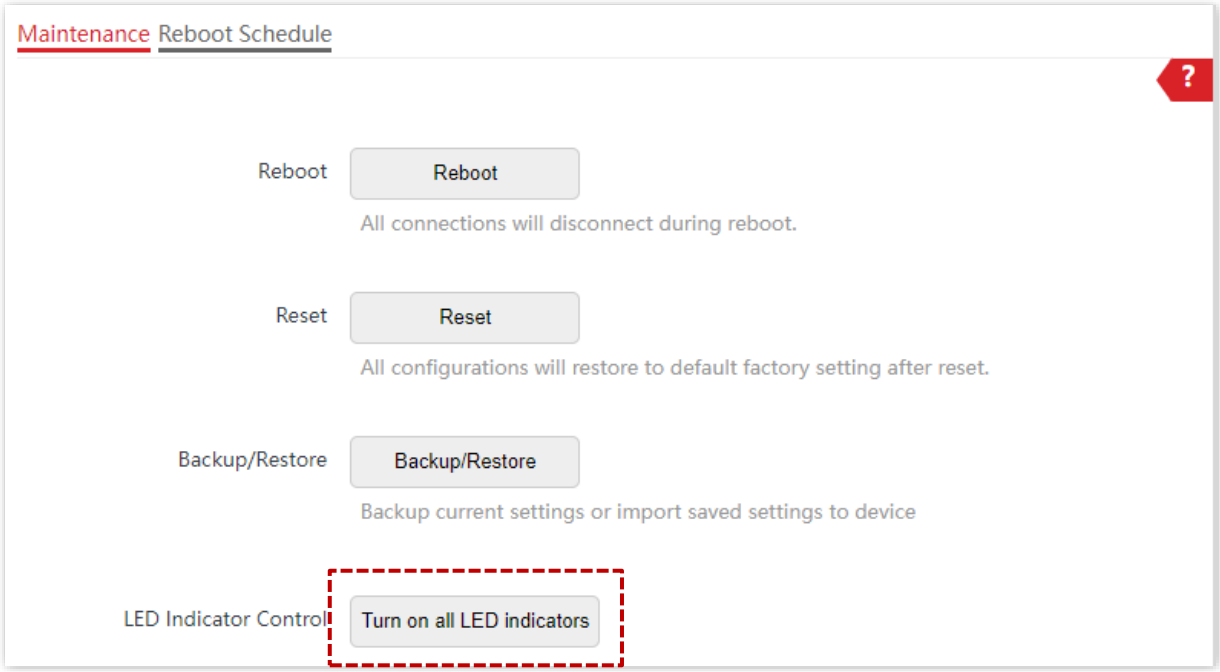



4. După finalizarea configurării, indicatorul se stinge și nu mai afișează starea de funcționare a punctului de acces. Însă, la repornire sau resetare acesta va indica starea.

**---Sfârșit**

### 8.2.5.2 Activare led

1. Conectați-vă la interfața web a punctului de acces.
2. Navigați la **Tools (Instrumente)** > **Maintenance (Mentenanță)** > **Maintenance (Mentenanță).**
3. Faceți clic pe **Turn on all LED indicators (Activare toate ledurile indicatoare).**




4. După finalizarea configurării, indicatorul LED se aprinde din nou și puteți evalua starea de funcționare a punctului de acces.

**---Sfârșit**

## 8.3 Submeniul System Software Upgrade (Actualizare software sistem)

Acest submeniu **System Software Upgrade (Actualizare software sistem)** pune la dispoziție un sistem complet de actualizare a firmware-ului pentru punctele de acces, cu două metode flexibile la alegere: actualizare manuală, prin încărcarea unui fișier local de firmware, sau actualizare online, prin care echipamentul verifică automat disponibilitatea unei versiuni noi pe serverele IP-COM și o descarcă fără intervenția administratorului. Astfel, punctele de acces beneficiază permanent de cele mai recente îmbunătățiri de performanță, securitate și funcționalitate, indiferent de dimensiunea rețelei sau de preferințele de administrare.

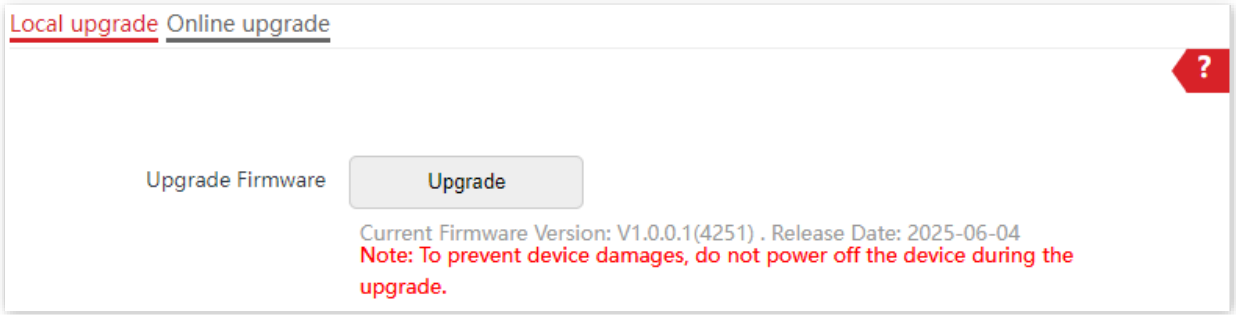
Note

Pentru a asigura o actualizare corectă și a evita deteriorarea echipamentului:

- Asigurați-vă că noul firmware este aplicabil punctului de acces. În general, formatul fișierului dezarhivat are terminația **.bin.**
- În timpul actualizării mențineți alimentarea cu curent a echipamentului.

## 8.3.1 Actualizare locală de firmware

1. Conectați-vă la interfața web a punctului de acces.
2. Prima dată navigați la **Status (Stare)** > **System Status (Stare sistem)** și verificați versiunea hardware a echipamentului de la câmpul **Hardware Version (Versiune hardware)** și, bineînțeles, versiunea de firmware a echipamentului, de la **Firmware Version (Versiune firmware)**.
3. Apoi accesați pagina web www.ip-com.com.cn/ro. Căutați pagina de produs a modelului.
4. Căutați ultima versiune de firmware ținând cont și de versiunea hardware a modelului. Citiți cu atenție toate notele aferente versiunii de firmware. Descărcați pachetul pe computer și dezarhivați pachetul. În general, fișierul de firmware are terminația .**bin**.
5. Apoi reconectați-vă la interfața web de gestionare a punctului de acces.
6. Navigați la **Tools (Instrumente)** > **System Software Upgrade (Actualizare software sistem)** > fila **Local upgrade (Actualizare locală)**.
7. Faceți clic pe **Upgrade (Actualizare).** Următoarea figură este doar pentru referință.




8. Căutați și selectați de pe computer fișierul de firmware cu terminația **.bin**. Încărcați fișierul de actualizare. Confirmați.
9. Așteptați până când bara de progres este completă. Echipamentul va reporni.
10. Conectați-vă din nou la interfața web a punctului de acces, navigați la **Status (Stare)** > **System Status (Stare sistem)** și verificați dacă actualizarea a reușit în funcție de informația de la câmpul **Firmware Version (Versiune firmware)**.

**---Sfârșit**

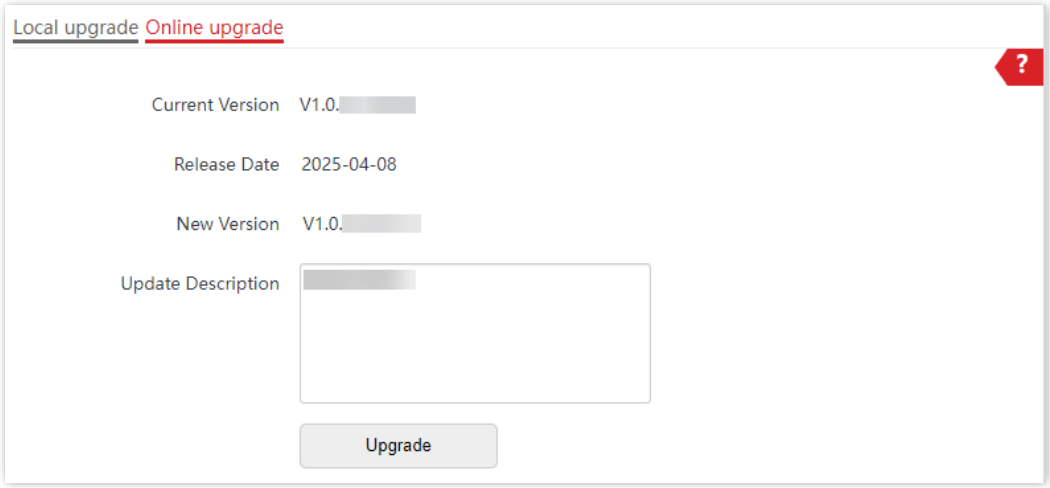
## 8.3.2 Actualizare online de firmware

După ce punctul de acces este conectat la internet, verificând informațiile IP de la **Internet Settings (Setări internet)** > **LAN Setup (Configurare LAN)** > fila **LAN Setup (Configurare LAN)**, atunci sistemul detectează automat dacă există o nouă actualizare de firmware și afișează informațiile relevante despre actualizarea detectată. Când o nouă actualizare de firmware este afișată pe pagină, atunci puteți actualiza AP-ul după cum este necesar.

**Procedură pentru efectuarea actualizării online**

1. Conectați-vă la interfața web a punctului de acces.

2. Navigați la **Tools (Instrumente)** > **System Software Upgrade (Actualizare software sistem)** > fila **Online upgrade (Actualizare online)**.
3. Așteptați până când este detectată o nouă versiune de firmware.




4. Dacă există o nouă versiune, atunci faceți clic pe **Upgrade (Actualizare).**
5. Așteptați până când bara de progres este completă.
6. Conectați-vă din nou la interfața web a punctului de acces, navigați la **Status (Stare)** > System Status (Stare sistem) și verificați dacă actualizarea a reușit în funcție de versiunea de la câmpul **Firmware Version (Versiune firmware)**.

**---Sfârșit**

# 8.4 Submeniul System Account (Cont sistem)

Când vă conectați pentru prima dată la interfața web a punctului de acces, setați o parolă de conectare, după cum este necesar, pentru a asigura securitatea. În plus, în timpul utilizării AP, schimbați periodic parola interfeței web pentru a menține securitatea continuă.

**Procedură pentru schimbarea parolei de autentificare la sistem, și implicit la interfața web de gestionare**

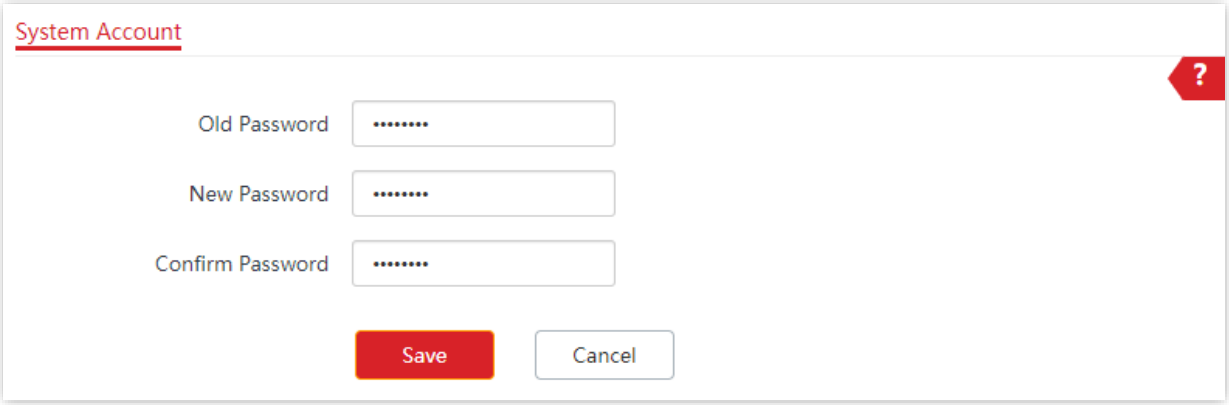
1. Conectați-vă la interfața web a punctului de acces.
2. Navigați la **Tools (Instrumente)** > **System Account (Cont sistem).**
3. Introduceți parola curentă în **Old Password (Parolă veche).**
4. Introduceți noua parolă în **New Password (Parolă nouă).**

Note

Pentru configurarea inițială sau după o resetare, setați noua parolă de conectare pentru a asigura confidențialitatea și securitatea. Cu cât parola este mai lungă, cu atât este mai mare securitatea. Limita de caractere și regulile de compunere pentru parole sunt afișate în interfața web.

5. Introduceți din nou noua parolă în **Confirm Password (Confirmare parolă).**

6. Faceți clic pe **Save (Salvare).**




7. Apoi veți fi redirecționat către interfața web de gestionare. Introduceți noua parolă și faceți clic pe **Login (Autentificare)**.

**---Sfârșit**

# 8.5 Submeniul System Log (Jurnal sistem)

Jurnalul sistemului înregistrează în mod sistematic evenimentele care au loc la nivelul echipamentului, precum și operațiunile efectuate de utilizatori autentificați la interfața de gestionare, după pornirea acestuia. Aceste informații detaliate oferă o vizibilitate completă asupra activității dispozitivului, fiind un instrument valoros pentru diagnosticarea rapidă a eventualelor erori de sistem și pentru menținerea unei rețele stabile.

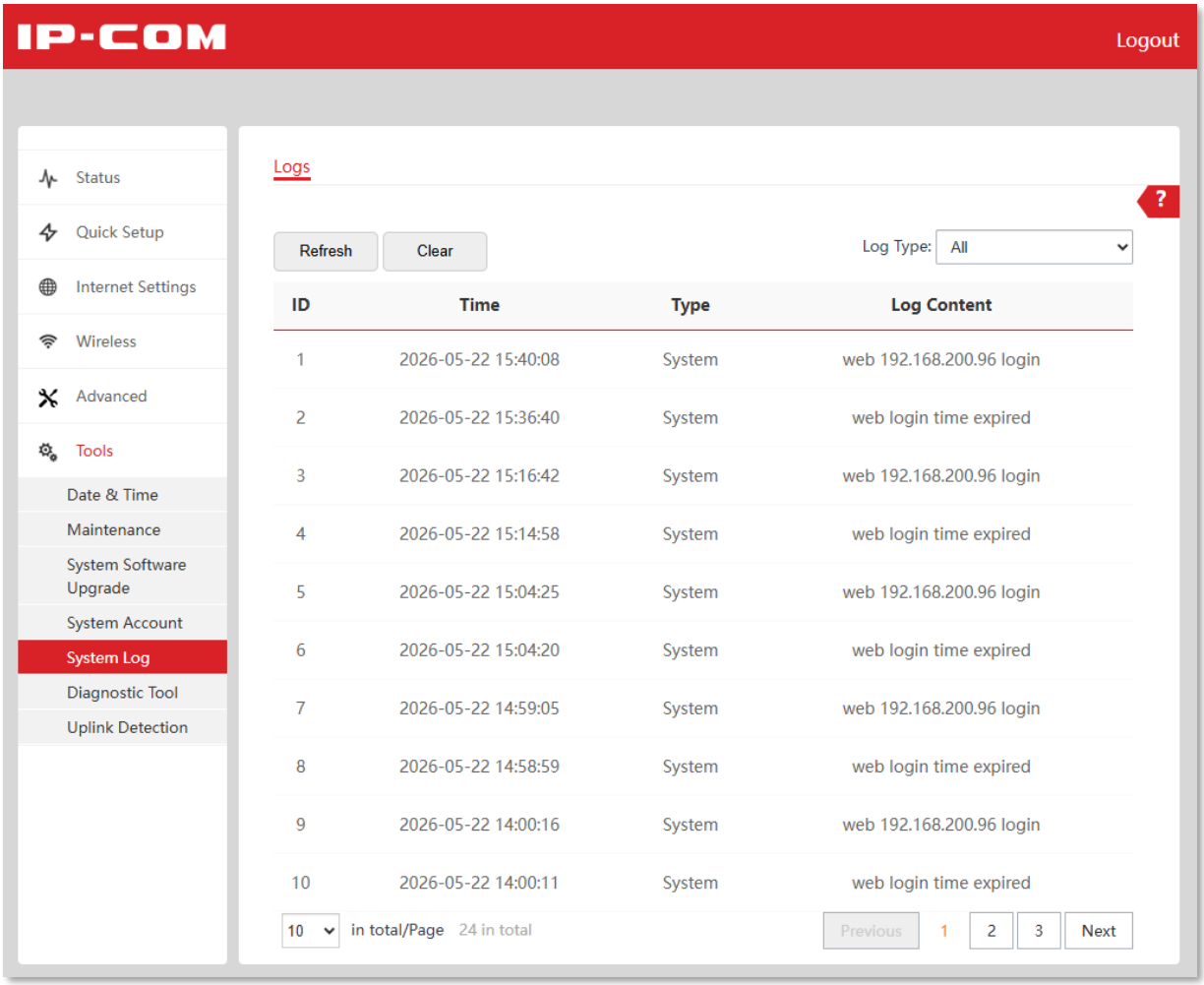
În cazul unei erori de sistem, puteți consulta meniul **Tools (Instrumente)** > **System Log (Jurnal sistem)**.

Note

- Pentru a vă asigura că evenimentele din jurnal sunt înregistrate corect, verificați data și ora echipamentului. Puteți corecta data și ora navigând la **Tools (Instrumente)** > **Date & Time (Dată și oră).**
- Când punctul de acces repornește, evenimentele din jurnal vor fi șterse. AP-ul repornește după o pană de curent, atunci când funcția QVLAN este configurată, firmware-ul este actualizat, un fișier de setări este restaurat sau echipamentul este resetat la setările din fabrică.

**Procedură pentru vizualizarea jurnalului cu evenimente de sistem**

1. Conectați-vă la interfața web de gestionare a punctului de acces.
2. Navigați la **Tools (Instrumente)** > **System Log (Jurnal sistem)**.
3. Opțional, faceți clic pe **Refresh (Actualizare)** pentru a vizualiza cele mai recente evenimente sau faceți clic pe **Clear (Ștergere)** pentru a șterge evenimentele existente.



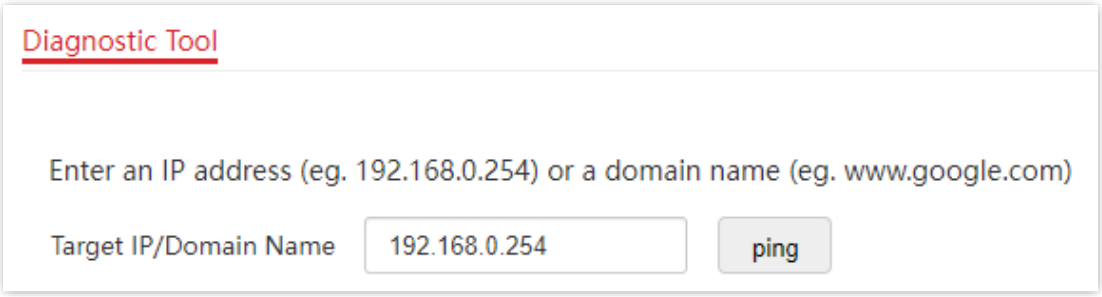

**---Sfârșit**

# 8.6 Submeniul Diagnostic Tool (Instrument diagnosticare)

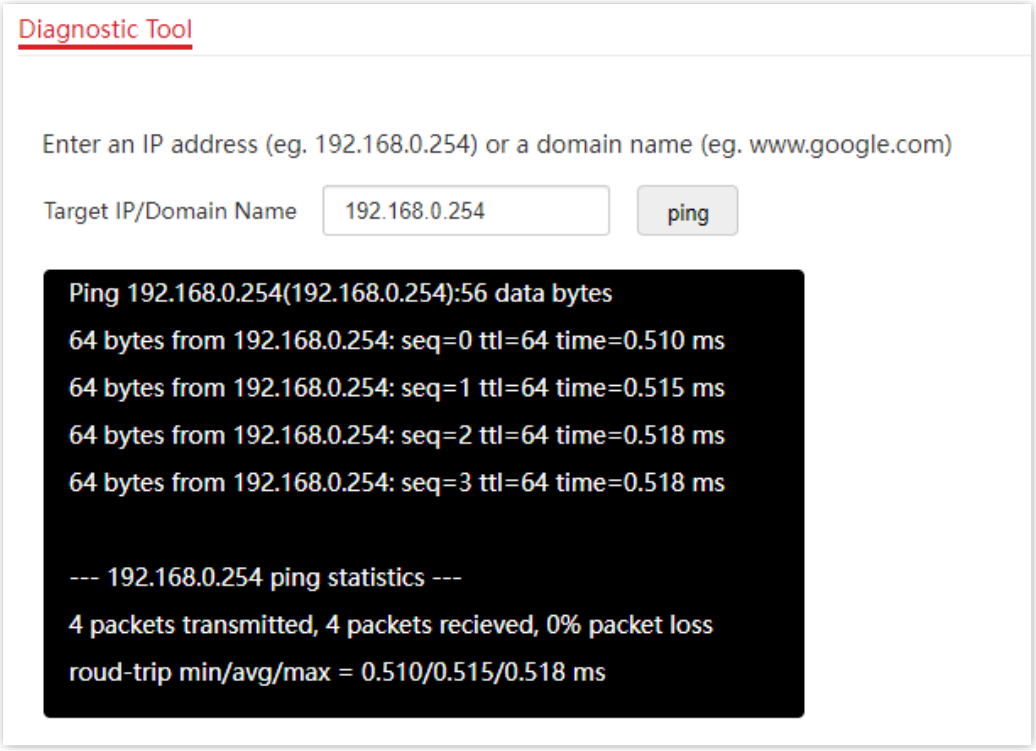
La **Tools (Instrumente)** > **Diagnostic Tool (Instrument diagnosticare)** se găsește unealta ce permite testarea prin ping a conexiunii între echipament și un IP.

**Procedură testare ping**

1. Conectați-vă la interfața web a punctului de acces.
2. Navigați la **Tools (Instrumente)** > **Diagnostic Tool (Instrument diagnosticare)**.
3. În caseta **Target IP/Domain Name (IP/domeniu țintă)** introduceți adresa IP sau numele domeniului pentru efectuarea unui test ping. În acest exemplu, ***192.168.0.254*.**
4. Faceți clic pe butonul **ping**.




5. Rezultatul diagnosticului va fi afișat în câteva secunde în caseta de text neagră de sub caseta de text **Target IP/Domain Name (IP/domeniu țintă).** Consultați figura următoare. Se observă că celălalt IP a răspuns.




**---Sfârșit**

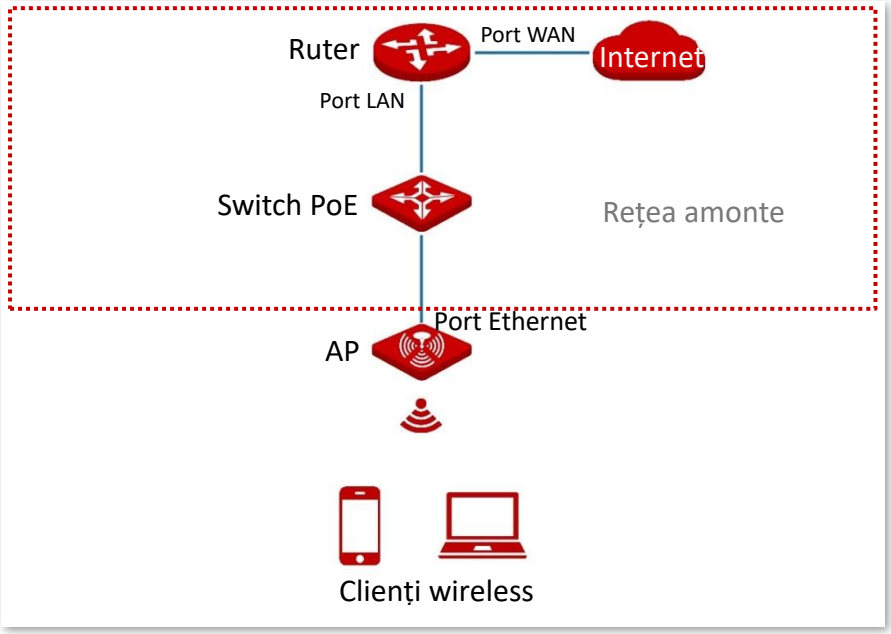
# 8.7 Submeniul Uplink Detection (Detectare legătură amonte)

În **modul de lucru AP**, punctul de acces se conectează prin cablu Ethernet la rețeaua din amonte, utilizând, bineînțeles, portul Ethernet LAN. Dacă un nod critic între portul Ethernet și rețeaua din amonte se defectează, atât punctul de acces, cât și clienții wireless conectați la acesta nu pot accesa rețeaua din amonte.

Dacă este activată funcția **Uplink Detection (Detectare legătură amonte)**, punctul de acces trimite în mod regulat pachete *ping* către anumite gazde setate la **Host1 to Ping (Ping către gazda 1)** și **Host2 to Ping (Ping către gazda 2)**, prin portul Ethernet bineînțeles. Dacă nu toate gazdele

sunt accesibile, punctul de acces își oprește serviciul wireless, iar clienții wireless nu pot găsi SSID-urile punctului de acces. Clientul se poate reconecta la punctul de acces numai după ce conexiunea dintre punctul de acces și rețelele din amonte este restabilită.

Dacă conexiunea acestui AP cu rețeaua din amonte e defectuoasă, clienții wireless se pot conecta la rețeaua din amonte printr-un alt AP din apropiere care funcționează corespunzător. Consultați următoarea topologie.




**Procedură pentru configurarea detectării legăturii din amonte**

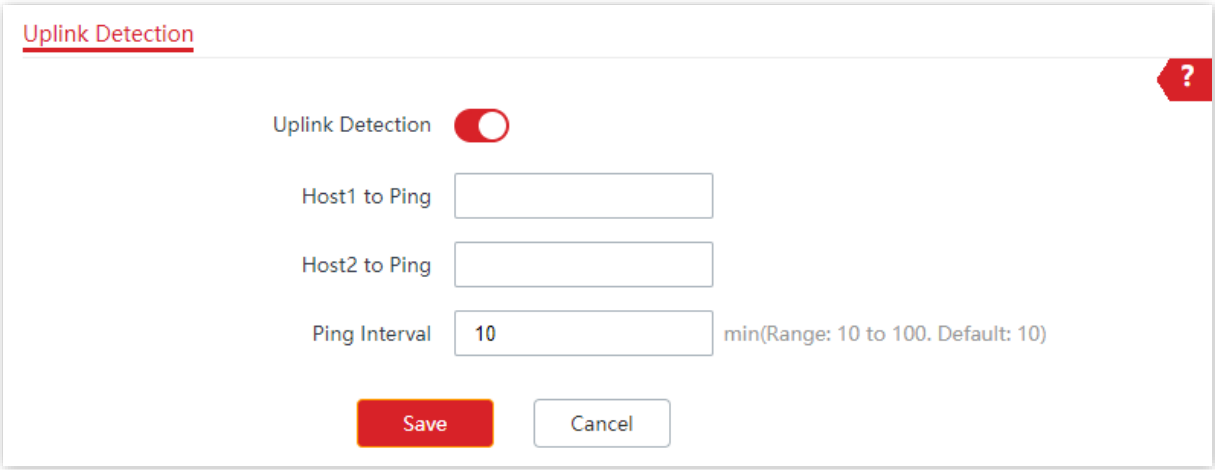
1. Conectați-vă la interfața web de gestionare a punctului de acces.
2. Navigați la **Tools (Instrumente)** > **Uplink Detection (Detectare legătură amonte)**.
3. Activați funcția de **Uplink Detection (Detectare legătură amonte)**.
4. La câmpurile **Host1 to Ping (Ping către gazda 1)** sau/și **Host2 to Ping (Ping către gazda 2)** introduceți câte o adresă IP validă ce va fi verificată prin pachete ping, prin portul Ethernet al punctului de acces. De exemplu puteți introduce adresa IP a ruterului conectat direct la punctul de acces sau/și un IP extern precum 8.8.8.8 DNS-ul public Google.

Tip

Dacă doriți să se verifice o singură adresă de gazdă destinație, atunci introduceți acea adresă atât pentru **Host1 to Ping (Ping către gazda 1)**, cât și pentru **Host2 to Ping (Ping către gazda 2).**

5. La **Ping Interval (Interval ping)** se introduce în minute intervalul de timp la care se efectuează pingul către adresele IP gazdă. Se va lăsa intervalul implicit de **10 minute**, deși se poate introduce între 10 și 100 de minute.
6. Faceți clic pe **Save (Salvare).**

**--Sfârșit**




## Descriere parametri Tools (Instrumente) > Uplink Detection (Detectare legătură amonte)

| Parametru | Descriere |
|---|---|
| **Uplink Detection**<br>**(Detectare legătură amonte)** | Specifică dacă se activează funcția de detectare a legăturii cu rețeaua din amonte.<br>Punctul de acces trimite periodic pachete *ping (ICMP Echo Request)* către una sau două adrese IP din rețea, definite de dumneavoastră. Dacă nu primește răspuns, înseamnă că legătura amonte este pierdută, iar AP-ul poate reacționa în consecință — de regulă prin dezactivarea SSID-urilor wireless, astfel încât clienții wireless să se reasocieze cu un alt AP care încă are conectivitate. Acest comportament este util mai ales în implementări cu mai multe puncte de acces, unde nu doriți ca un client să rămână conectat la un AP „orfan" care nu mai oferă acces la rețea. |
| **Host1 to Ping**<br>**(Ping către gazda 1)** | Specificați adresa IP a gazdei care va fi verificată prin ping prin portul Ethernet al punctului de acces. Este disponibilă numai atunci când funcția de detectare a legăturii amonte este activată. |
| **Host2 to Ping**<br>**(Ping către gazda 2)** | Dacă doriți să se verifice o singură adresă de gazdă destinație, atunci introduceți acea adresă atât pentru **Host1 to Ping (Ping către gazda 1)**, cât și pentru **Host2 to Ping (Ping către gazda 2).** |
| **Ping Interval**<br>**(Interval ping)** | Intervalul de timp (în minute) între două verificări succesive.<br>Intervalul acceptat este **10–100 minute**, iar valoarea implicită este **10**. O valoare mai mică înseamnă detecție mai rapidă a căderii uplink-ului, dar și trafic ping ușor mai ridicat; o valoare mai mare reduce traficul, dar întârzie reacția AP-ului la o eventuală cădere**.** |

# 9 Anexe

## 9.1 Setări implicite

Următorul tabel prezintă valorile implicite ale principalilor parametri ai punctului de acces.

| Parametru | | | Valoare implicită |
|---|---|---|---|
| Autentificare | Adresă IP din rețeaua locală (LAN) | | **192.168.0.254**<br><br>Tip<br><br>Cu serverul DHCP în LAN, punctul de acces poate obține o adresă IP de la un server DHCP și puteți verifica noua adresă IP din lista de clienți a serverului DHCP. Aceasta este disponibilă numai când punctul de acces este la setările din fabrică. |
| | Adresă IP de gestionare, secundară | | **10.16.16.169** |
| Configurare rapidă | Mod de lucru | | Mod **AP** |
| Setări SSID | SSID | 2,4 GHz | SSID-ul afișat este de forma **IP-COM_XXXXXX**, unde **XXXXXX** are legătură cu adresa MAC. Această informație e pe etichetă.<br><br>În mod implicit, primul SSID este activat, iar celelalte SSID-uri sunt dezactivate. |
| | | 5 GHz | SSID-ul afișat este **IP-COM_*XXXXXX*_5G, unde XXXXXX** are legătură cu adresa MAC. Această informație e pe etichetă.<br><br>În mod implicit, primul SSID este activat, iar celelalte SSID-uri sunt dezactivate. |

## 9.2 Acronime și abrevieri

| Acronim sau abreviere | Denumire originală completă, în engleză |
|---|---|
| AC | Access Point Controller sau Access Controller |
| ACK | Acknowledge Character |
| AES | Advanced Encryption Standard |
| AP | Access Point |
| APSD | Automatic Power Save Delivery |
| CTS | Clear To Send |
| DHCP | Dynamic Host Configuration Protocol |
| DTIM | Delivery Traffic Indication Map |
| DNS | Domain Name System |
| FIFO | First-in First-out |
| GI | Guard Interval |
| ID | Identity Document |
| IP | Internet Protocol |
| LAN | Local Area Network |
| MAC | Media Access Control |
| MU-MIMO | Multi-User Multiple-Input Multiple-Output |
| OFDMA | Orthogonal Frequency Division Multiple Access |
| PoE | Power over Ethernet |
| PSK | Pre-shared Key |
| PVID | Port-based VLAN ID |
| RF | Radio Frequency |
| RSSI | Received Signal Strength Indication |
| RTS | Request To Send |

| Acronim sau abreviere | Denumire originală completă, în engleză |
|---|---|
| SAE | Simultaneous Authentication of Equals |
| SSID | Service Set Identifier |
| VLAN | Virtual Local Area Network |
| WAN | Wide Area Network |
| WLAN | Wireless Local Area Network |
| WMF | Wireless Multicast Forwarding |
| WPA | Wi-Fi Protected Access |