IP-COM

Manual utilizare interfață web de gestionare

pentru punctele de acces Wi-Fi 6, modele **Pro-6-LR, Pro-6-Lite și Pro-6-Mini**,

destinate utilizării în spații interioare

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

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-6-LR**
- **Pro-6-Lite**
- **Pro-6-Mini**

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.

În acest ghid, dacă nu se specifică altfel, toate capturile de ecran sunt preluate de la un AP model **Pro-6-LR**

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	>	**Meniu principal** > **Funcție**
Parametru și valoare	Aldin, cu valoarea uneori cursiv	La **Nume utilizator** introduceți ***Albert***.
Variabilă	Cursiv	Format adresă MAC: *XX*:*XX*:*XX*:*XX*:*XX*:*XX*
Controlul interfeței utilizator	Aldin	Pe pagina **Politică**, faceți clic pe butonul **OK**.
Mesaj	Între ghilimele sau 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	2026.06.23	Prima publicare în limba română.

Cuprins

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 prin cablu Ethernet către un switch sau ruter — caz în care echipamentul funcționează în modul de lucru cunoscut ca **Access Point** sau prescurtat **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 **LAN0/PoE** de pe AP la un port Ethernet cu PoE de pe un switch PoE sau de pe un ruter cu porturi PoE.

   Sau dacă doriți să utilizați injectorul inclus, atunci conectați portul marcat **LAN0/PoE** de pe AP la portul marcat **AP** de pe injector. În injectorul PoE introduceți adaptorul de curent inclus în pachet și introduceți-l la o priză cu curent alternativ. Apoi la portul marcat **Switch** de pe injector conectați un cablu Ethernet care se va duce la rețeaua din amonte, adică îl conectați la un port Ethernet de pe un switch sau ruter sau AP din amonte.

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 și fixarea pe plafon.

   Ca bune practici se recomandă verificarea, actualizarea și configurarea AP-ului și abia apoi montarea acestuia pe tavan sau perete.

3. Conectați un dispozitiv client la Wi-Fi-ul emis de AP sau conectați prin cablu Ethernet la portul **LAN1** sau la switch-ul sau ruterul la care e conectat AP-ul.

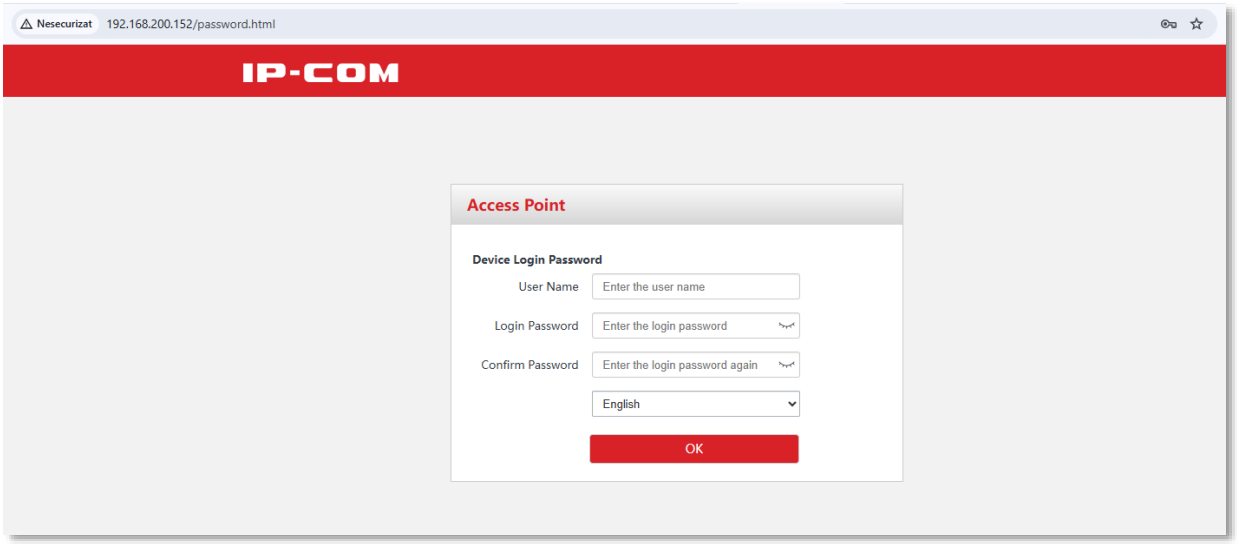
   Tip

   - 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. Accesați apoi pagina web de gestionare la adresa IP atribuită AP-ului de către un server DHCP din amonte (de regulă de ruterul din amonte), de exemplu http://192.168.200.152.

Dacă în rețeaua din amonte nu există un server DHCP, puteți folosi adresa implicită a AP-ului, http://**192.168.0.254**. În acest caz, computerul trebuie să se afle în aceeași subrețea cu AP-ul, așa că este necesar să setați manual o adresă IP și masca de subrețea pe adaptorul de rețea folosit pentru conectare. Alegeți o adresă din intervalul 192.168.0.x (de exemplu 192.168.0.10), diferită de cea a AP-ului, și masca 255.255.255.0.

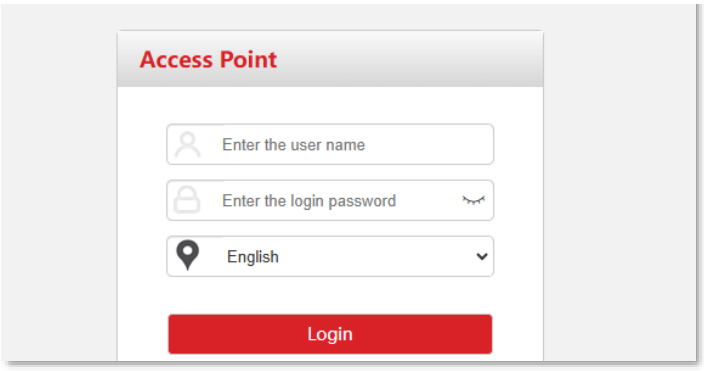
5. În pagină vă va cere să setați numele de utilizator și parola de autentificare la interfața locală de gestionare. Astfel la **User Name (Nume utilizator)** introduceți orice nume de utilizator doriți. Mai jos la **Login Password (Parolă autentificare)** și **Confirm Password (Confirmare parolă)** introduceți parola dorită care poate să conțină litere mari, litere mici, numere și liniuță jos. A se reține că parola nu permite caractere speciale precum !, @, #, $, %, ^, &, * etc.



La unele versiuni mai vechi de firmware vă puteți autentifica cu userul **admin** și parola implicită **admin** apoi vă cere să schimbați parola implicită, nu și userul.

6. La final apăsați **OK** și așteptați câteva momente aplicarea modificărilor.

7. Apoi introduceți userul și parola setate la pasul **5** și apăsați **Login (Autentificare)**, pentru a accesa interfața de gestionare, dacă se dorește acest lucru.



---Sfârșit

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. 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), atunci AP-ul poate primi automat o adresă IP. 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 AP-ul nu obține un IP din variate motive, atunci încercați folosind adresa IP 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). Însă în acest caz este necesar să setați manual o adresă IP și mască de subrețea pe adaptorul de rețea folosit pentru conectare. Mai jos regăsiți pașii pentru două sisteme de operare.

  - Setare IP fix pe Windows:

    1. Apăsați simultan tastele **Windows** și **R**. Se va deschide **Run (Executare)**.
    2. Tastați **ncpa.cpl** și apoi **OK** pentru a deschide lista conexiunilor de rețea.
    3. În noua fereastră faceți clic dreapta pe adaptorul prin care sunteți conectat la AP de obicei denumit *Ethernet* sau *Wi-Fi* și apăsați **Properties (Proprietăți)**.
    4. Selectați din listă **Internet Protocol Version 4 (TCP/IPv4)** și apăsați **Properties (Proprietăți)**.
    5. Bifați **Use the following IP address (Utilizați următoarea adresă IP**) și completați de exemplu *192.168.0.10* la **IP Address (Adresă IP)** și *255.255.255.0* la **Subnet Mask (Mască subrețea)**.
    6. Apăsați **OK** pentru a aplica setările.

  - Setare IP fix pe macOS:

    1. Deschideți **System Settings (Reglaje sistem)** apoi **Network (Rețea)**.
    2. Selectați adaptorul de rețea folosit, de regulă găsit sub denumirea *Ethernet* sau *USB-Ethernet* sau *Wi-Fi*.
    3. Intrați la **Details (Detalii)**, fila **TCP/IP** și schimbați **Configure IPv4 (Configurare IPv4)** din **Using DHCP (Folosind DHCP)** în **Manual**.
    4. Apoi introduceți de exemplu *192.168.0.10* la I**P Address (Adresă IP)** și *255.255.255.0* la **Subnet Mask (Mască subrețea)**.
    5. Apăsați **OK**, apoi **Apply (Aplică)** pentru a salva.
- 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.

2 Acces interfață web gestionare

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 client la Wi-Fi-ul emis de AP sau conectați prin cablu Ethernet la portul **LAN1** lăsat liber sau la switch-ul sau ruterul la care e conectat AP-ul. În esență conectați un client fie prin cablu, fie prin Wi-Fi, la aceeași rețea locală logică în care se află și AP-ul.

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.

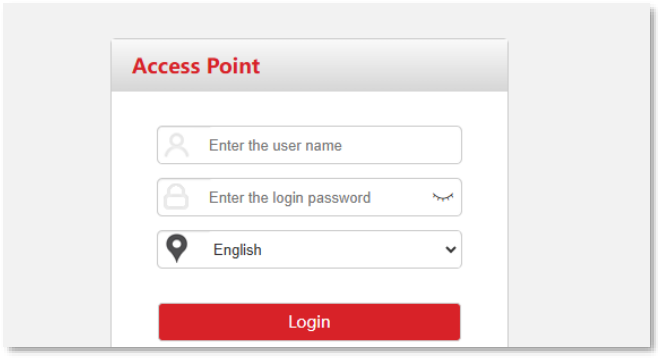
2. Porniți un browser și introduceți în bara de adrese adresa IP a punctului de acces — fie cea alocată de un server DHCP din amonte, fie cea setată manual din meniul **Internet Settings (Setări internet)** pentru a vă conecta la interfața web a punctului de acces. Puteți accesa interfața folosind și IP-ul implicit http://192.168.0.254/.

Tip

- Încercați să utilizați adresa IP din rețeaua locală (LAN) a punctului de acces pentru a vă conecta la interfața web a acestuia 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. IP-ul se poate modifica manual direct pe echipament din meniul **Internet Settings (Setări internet).**
- Dacă punctul de acces nu a primit nicio adresă IP de la un server DHCP — fie pentru că în rețeaua din amonte nu există niciun astfel de server — și doriți să accesați adresa implicită http://192.168.0.254/, rețineți că trebuie să configurați manual adresa IP și masca de subrețea ale adaptorului de rețea prin care vă conectați la AP. Acest lucru este necesar deoarece punctul de acces nu dispune de un server DHCP propriu și nu poate atribui adrese IP clienților conectați prin el. Mai jos regăsiți pașii pentru setarea unui IP fix pe adaptorul de rețea al unui client, pentru două sisteme de operare.
  - Setare IP fix pe Windows:
    1. Apăsați simultan tastele **Windows** și **R**. Se va deschide **Run (Executare)**.
    2. Tastați **ncpa.cpl** și apoi **OK** pentru a deschide lista conexiunilor de rețea.
    3. În noua fereastră faceți clic dreapta pe adaptorul prin care sunteți conectat la AP de obicei denumit *Ethernet* sau *Wi-Fi* și apăsați **Properties (Proprietăți)**.
    4. Selectați din listă **Internet Protocol Version 4 (TCP/IPv4)** și apăsați **Properties (Proprietăți)**.
    5. Bifați **Use the following IP address (Utilizați următoarea adresă IP**) și completați de exemplu *192.168.0.10* la **IP Address (Adresă IP)** și *255.255.255.0* la **Subnet Mask (Mască subrețea)**.
    6. Apăsați **OK** pentru a aplica setările.
  - Setare IP fix pe macOS:
    1. Deschideți **System Settings (Reglaje sistem)** apoi **Network (Rețea)**.
    2. Selectați adaptorul de rețea folosit, de regulă găsit sub denumirea *Ethernet* sau *USB-Ethernet* sau *Wi-Fi*.
    3. Intrați la **Details (Detalii)**, fila **TCP/IP** și schimbați **Configure IPv4 (Configurare IPv4)** din **Using DHCP (Folosind DHCP)** în **Manual**.
    4. Apoi introduceți de exemplu *192.168.0.10* la I**P Address (Adresă IP)** și *255.255.255.0* la **Subnet Mask (Mască subrețea)**.
    5. Apăsați **OK**, apoi **Apply (Aplică)** pentru a salva.
- Dacă în rețea există două sau mai multe AP-uri neconfigurate, toate vor avea inițial aceeași adresă IP implicită, ceea ce poate genera un conflict, în anumite situații. 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 din meniul **Internet Settings (Setări internet)**.
- 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.

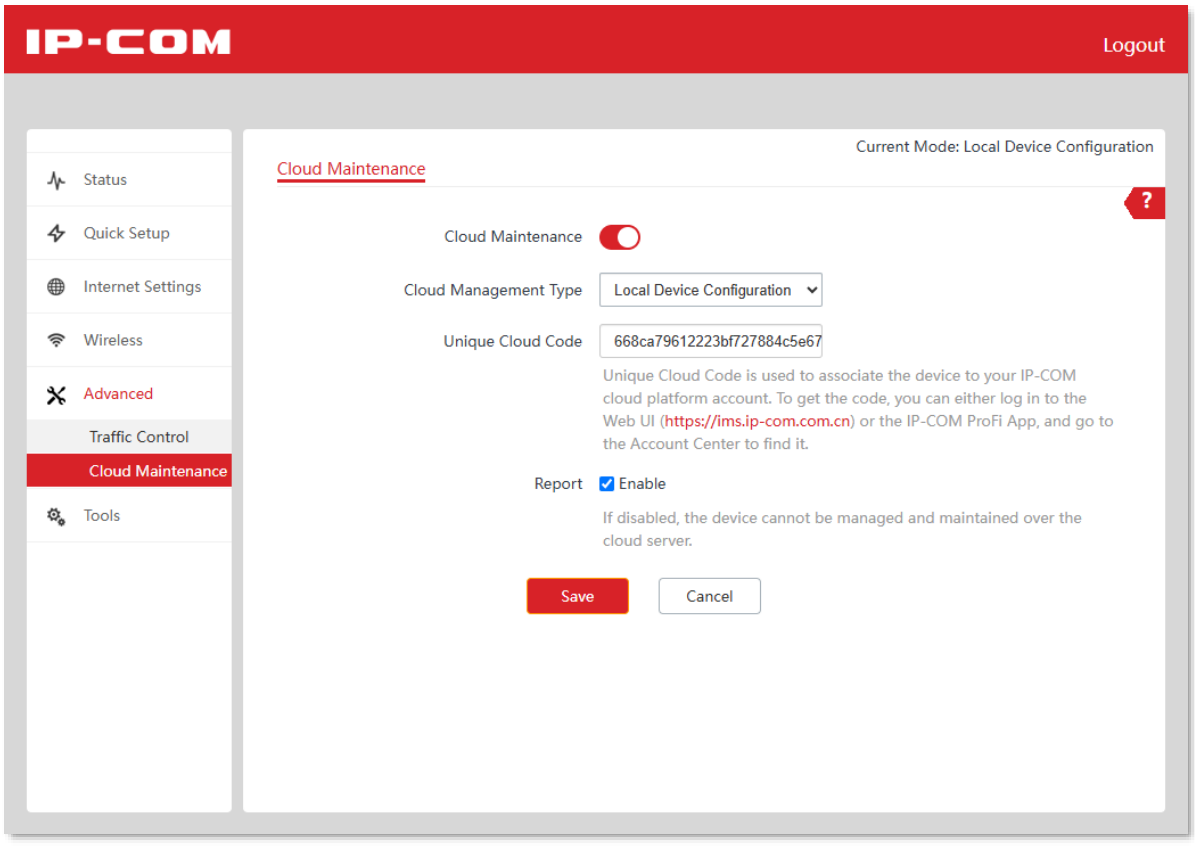
- Asigurați-vă că punctul de acces funcționează corect și că dispozitivul client este conectat la rețeaua Wi-Fi corectă.
- Când vă conectați folosind un telefon inteligent, asigurați-vă că datele mobile sunt dezactivate.

3. Apoi introduceți userul și parola setate la pasul 5 din subcapitolul 1.3 Configurarea inițială din interfața locală web și apăsați **Login (Autentificare)**, pentru a accesa interfața de gestionare. Numele de utilizator și parola pot fi modificate ulterior din meniul **Tools (Instrumente) > Account (Cont)**.



4. Se va deschide pagina **Quick Setup (Configurare rapidă)** dacă AP-ul nu e gestionat de niciun sistem centralizat precum de serviciul cloud **IP-COM ProFi Cloud**. Sau se va deschide pagina **Status (Stare) > System Status (Stare sistem)** dacă AP-ul este gestionat de un sistem centralizat precum de serviciul cloud **IP-COM ProFi Cloud.**

   Pentru a vedea cum anume e gestionat AP-ul, atunci verificați sau/și configurați setările de la meniul **Advanced (Avansat) > Cloud Maintenance (Mentenanță cloud)**, precum în imaginea de mai jos.



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

- Când este afișat **Cloud Configuration (Configurare 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 Device Configuration (Configurare locală)** toate setările avansate redevin disponibile, și acesta poate fi gestionat din interfața locală sau de un controler de AP-uri, precum un ruter multi-WAN seria **M** de la IP-COM. În imaginea următoare e activ acest mod.

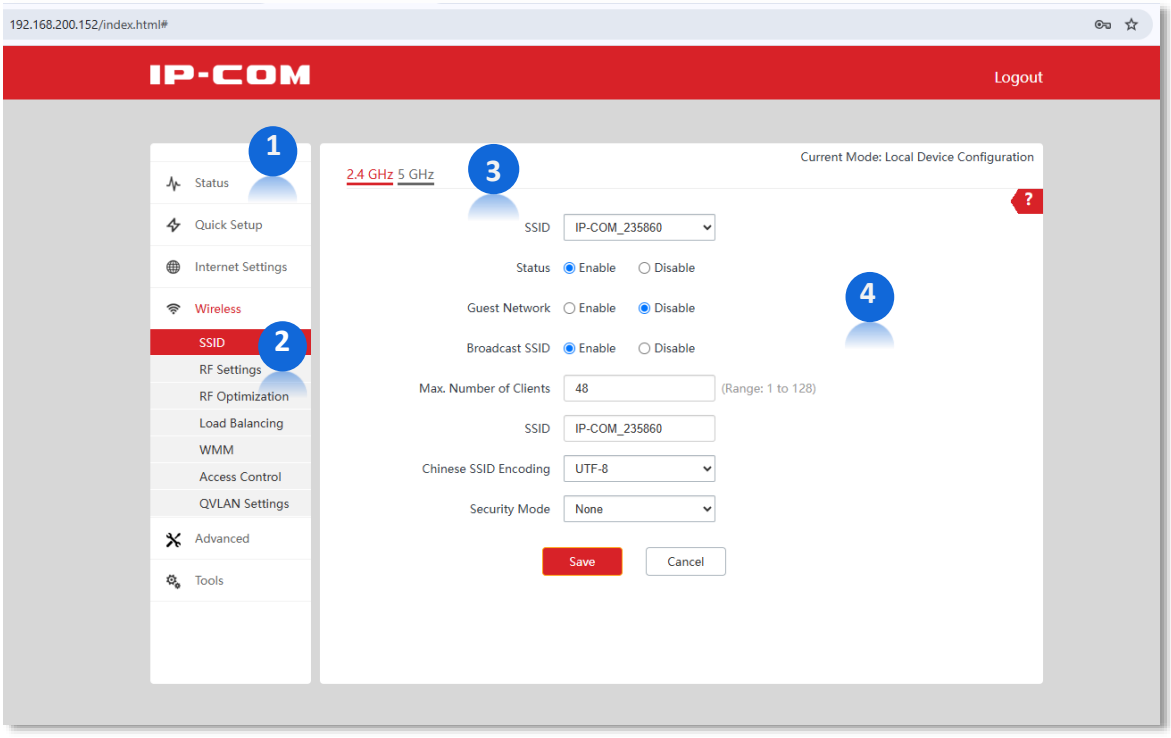
2.2 Deconectare din interfața web

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 1-60 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 userul și 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.

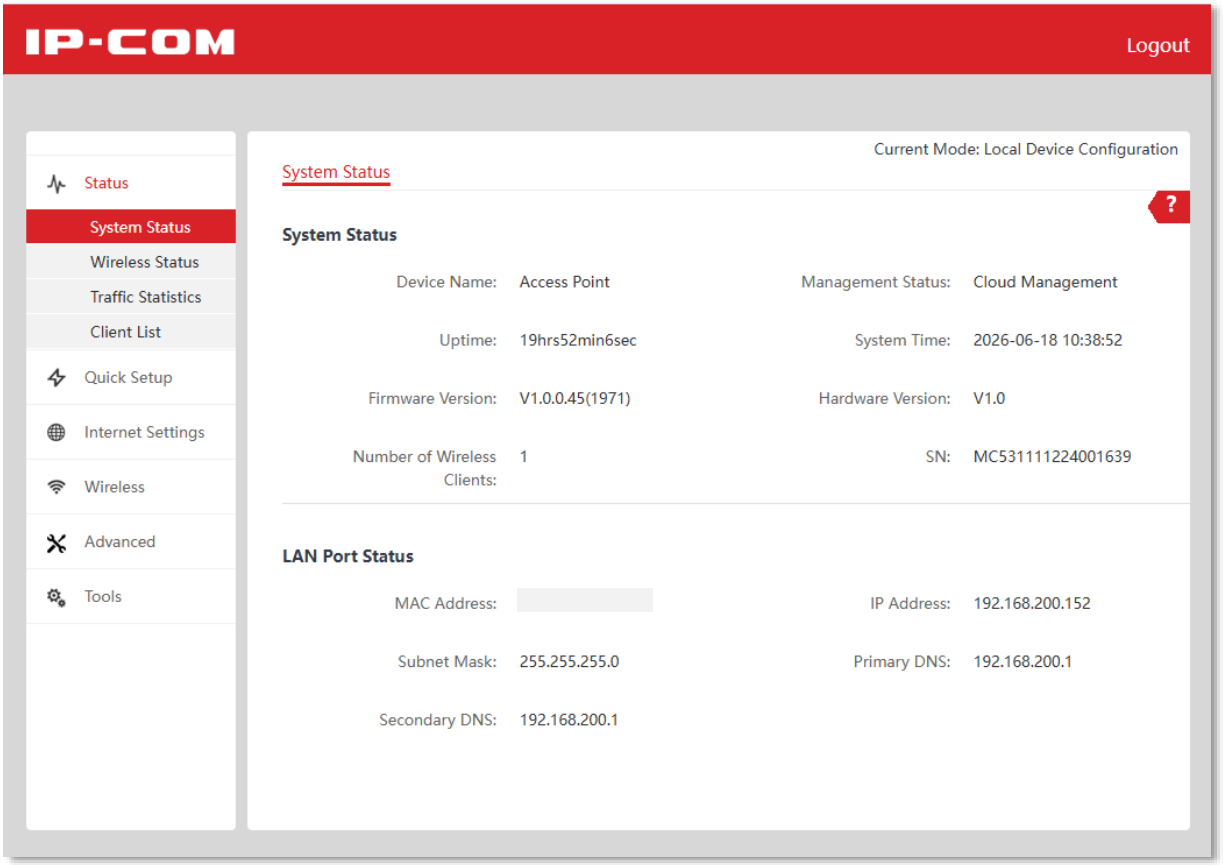
3 Meniul Status (Stare)

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)

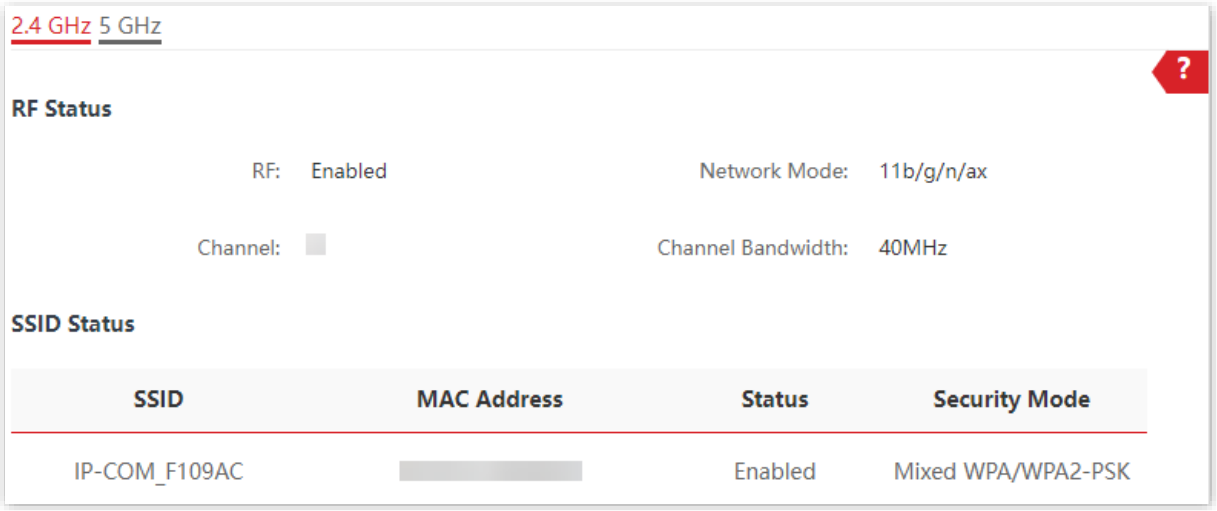
Parametru		Descriere
Secțiune **System Status (Stare sistem)**	**Device Name (Nume dispozitiv)**	Specifică numele punctului de acces. Puteți schimba numele echipamentului de la meniul **Internet Settings (Setări internet)** câmpul **Device Name (Nume dispozitiv).** Se recomandă să schimbați numele punctului de acces pentru a indica locația acestuia, astfel încât să puteți identifica cu ușurință pe teren echipamentul când gestionați mai multe puncte de acces. Această denumire e și cea afișată în rețeaua logică.
	Management Status (Stare gestionare)	Specifică starea conexiunii dintre punctul de acces și platforma de gestionare unificată din cloud **IP-COM ProFi Cloud**. Dacă e afișat **Cloud Management (Gestionare cloud)** atunci e conectat la serviciul **IP-COM ProFi Cloud**. Setările aferente pentru conectarea la serviciul **IP-COM ProFi Cloud** se fac din meniul **Advanced (Avansat) > Cloud Maintenance (Mentenanță cloud)**.
	Uptime (Timp funcționare)	Specifică timpul scurs de la pornirea echipamentului.
	System Time (Timp sistem)	Specifică data și ora setată pe echipament. Timpul sistemului se modifică din **Tools (Instrumente) > Date & Time (Dată și oră)**.
	Firmware Version (Versiune firmware)	Specifică versiunea de firmware a echipamentului. Actualizarea de firmware se poate face din meniul **Tools (Instrumente) > Maintenance (Mentenanță)**.
	Hardware Version (Versiune hardware)	Specifică versiunea hardware a echipamentului. 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 (Număr clienți wireless)	Specifică numărul de clienți conectați prin punctul de acces.
	SN	Specifică numărul de serie unic al echipamentului.
Secțiune **LAN Port Status (Stare port LAN)**	**MAC Address (Adresă MAC)**	Specifică identificatorul unic MAC de pe portul Ethernet principal.

Parametru		Descriere
	IP Address **(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. 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 de la meniul **Internet Settings (Setări internet)**. 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. Tip – 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. – 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 **(Mască subrețea)**	Indică masca de subrețea corespunzătoare adresei IP a portului LAN al punctului de acces. Puteți schimba de la meniul **Internet Settings (Setări internet)**.
	Primary DNS **(DNS principal)**	Indică adresa IP a serverului DNS principal al punctului de acces. Puteți schimba de la meniul **Internet Settings (Setări internet).**
	Secondary DNS **(DNS secundar)**	Indică adresa IP a serverului DNS secundar al punctului de acces. Puteți schimba de la meniul **Internet Settings (Setări internet).**

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 **2.4 GHz** și **5 GHz**		Apăsați fila **2.4 GHz** pentru informații despre starea conexiunilor wireless pe banda de 2,4 GHz. Apăsați fila **5 GHz** pentru informații despre starea conexiunilor wireless pe banda de 5 GHz. Opțiunile de mai jos pot fi diferite în funcție de fila apăsată.
Secțiune **RF Status (Stare radiofrecvență)**	**RF (Radiofrecvență)**	Indică dacă banda, fie că e 2,4 GHz, fie că e 5 GHz, e activă sau nu.
	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. 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). Se aplică pentru toate SSID-urile din listă.
	Channel (Canal)	Indică numărul canalului din bandă pe care se emit. Se aplică pentru toate SSID-urile din listă.

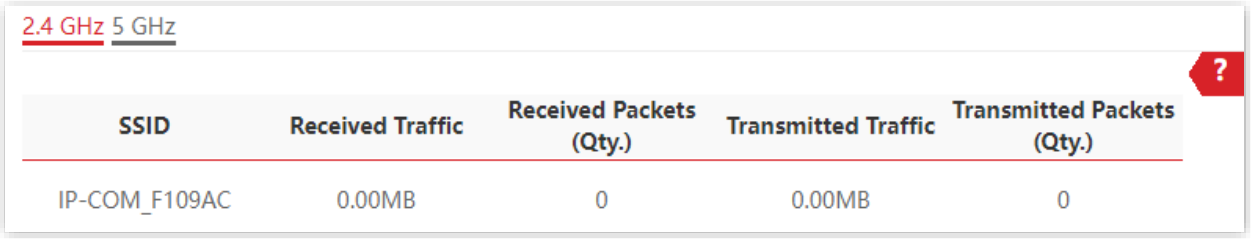
Parametru		Descriere
	Channel Bandwidth (Lățime canal)	Indică lățimea canalului radio, exprimată în **MHz**; aceasta nu trebuie confundată cu frecvența benzii pe care funcționează rețeaua Wi-Fi. Se aplică pentru toate SSID-urile din listă.
Tabelul **SSID Status (Stare SSID)**	**SSID**	Se indică numele rețelelor Wi-Fi emise de echipamentul IP-COM. Denumirile, activarea, dar și alte setări pentru aceste SSID-uri se fac 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.** 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)**. 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)

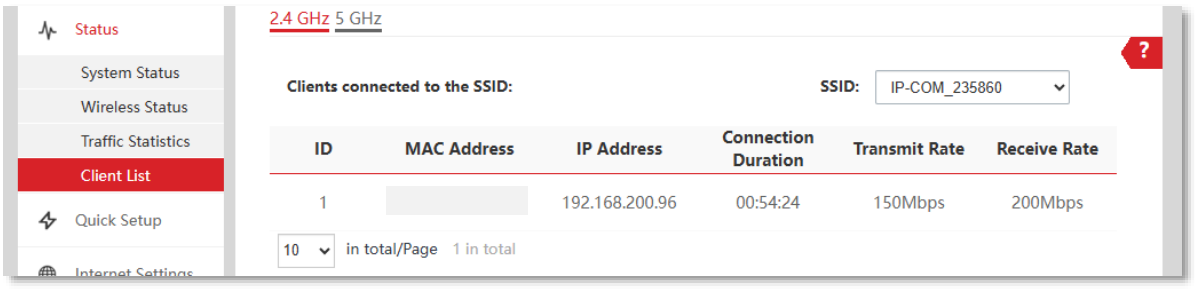
Parametru	Descriere
Filele **2.4 GHz** și **5 GHz**	Apăsați fila **2.4 GHz** pentru informații despre traficul wireless pe banda de 2,4 GHz. Apăsați fila **5 GHz** pentru informații despre traficul wireless pe banda de 5 GHz.
SSID	Se indică numele rețelelor Wi-Fi emise de echipamentul IP-COM. Denumirile, activarea, dar și alte setări pentru aceste SSID-uri se fac din meniul Wireless > **SSID**.
Received Traffic **(Trafic primit)**	Specifică numărul total de octeți primiți de o rețea Wi-Fi (SSID).
Received Packets (Qty.) **(Pachete primite (cantitate))**	Specifică numărul total de pachete primite de o rețea Wi-Fi.
Transmitted Traffic **(Trafic trimis)**	Specifică numărul total de octeți transmiși de o rețea Wi-Fi (SSID).
Transmitted Packets (Qty.) **(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**.



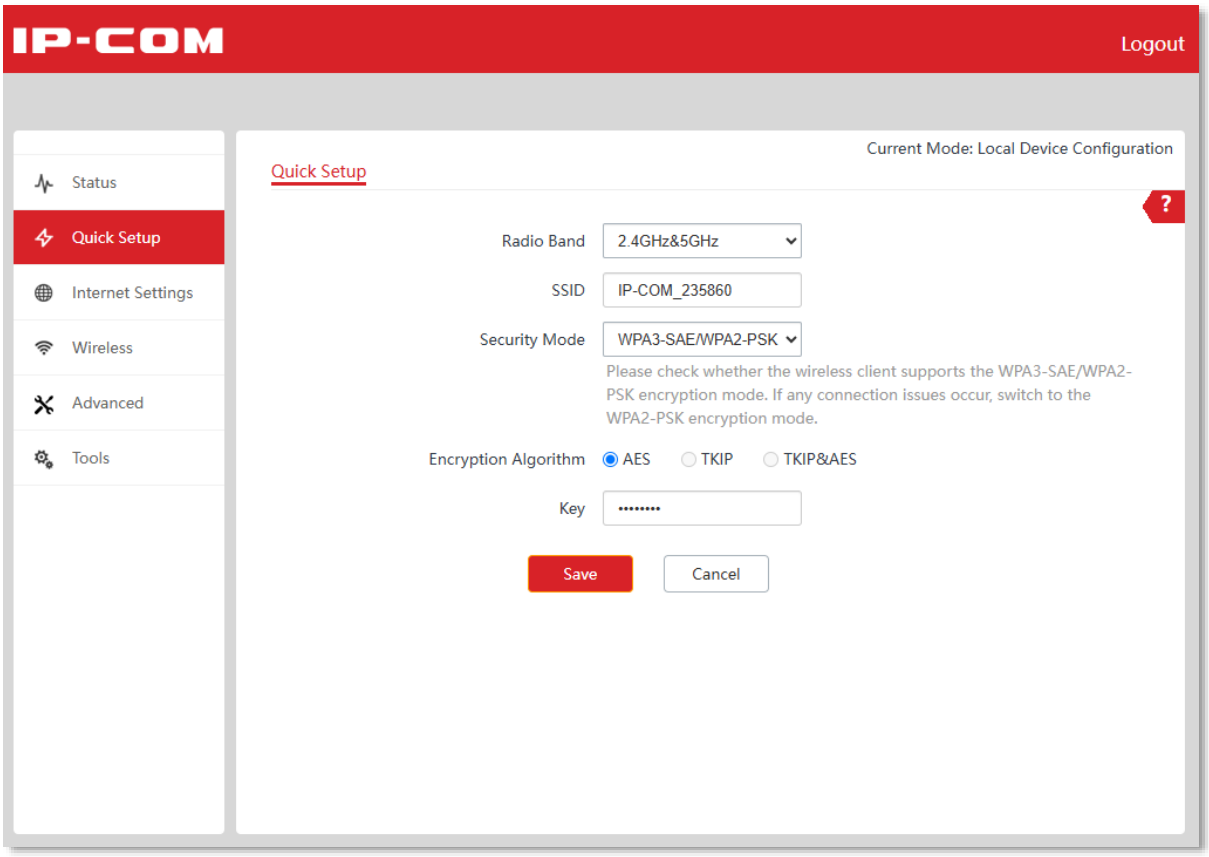
Descriere parametri Status (Stare) > Client List (Listă clienți)

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 în 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.
Connection Duration **(Durată conexiune)**	Specifică durata de conectare online, neîntreruptă, a clientului wireless.
Transmit Rate **(Rată transmitere)**	Specifică rata negociată automat de transmisie, maximă, dintre client și SSID-ul respectiv.
Receive Rate **(Rată primire)**	Specifică rata negociată automat de primire, maximă, dintre client și SSID-ul respectiv.

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.

Aparatul 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 acesta. Aparatul se conectează la rețeaua din amonte prin cablu Ethernet, mod de lucru cunoscut ca **Access Point** sau **AP**.



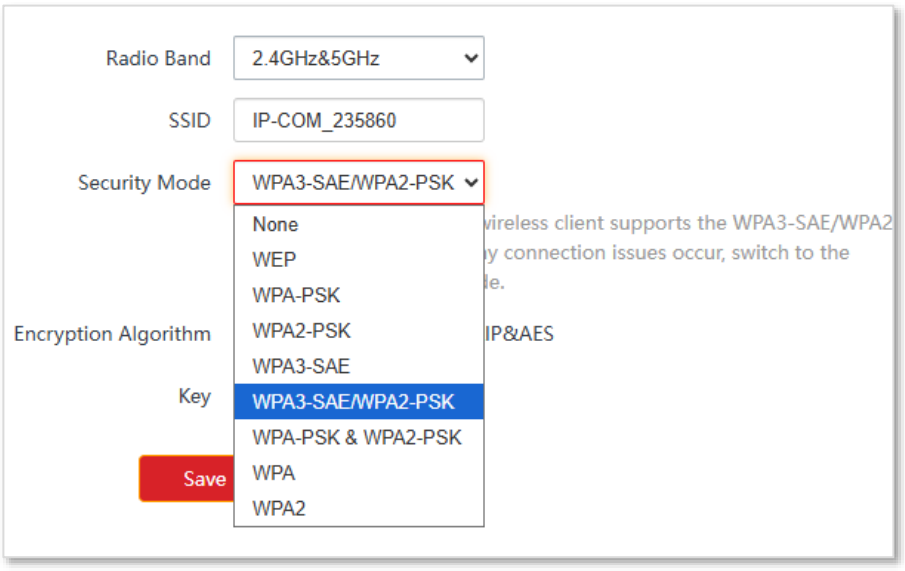
Din meniul **Quick Setup (Configurare rapidă)** se poate configura rețeaua Wi-Fi principală emisă de echipamentul IP-COM, mai exact primul SSID de pe fiecare bandă (2,4 GHz și 5 GHz). A se reține faptul că acest echipament poate emite mai multe SSID-uri, toate pot fi activate și modificate ulterior din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

Procedură modificare SSID principal

1. Conectați-vă la interfața web de gestionare.
2. Accesați meniul din stânga **Quick Setup (Configurare rapidă)**.
3. Selectați banda dorită din câmpul **Radio Band (Bandă radio)**. Puteți să selectați pe ce bandă să efectuați modificările, anume pe banda de **2.4 GHz** sau/și pe **5 GHz** sau pe ambele benzi selectând **2.4 GHz & 5 GHz**.
4. Introduceți denumirea rețelei Wi-Fi emise în câmpul **SSID**.
5. Alegeți tipul de criptare din **Security Mode (Mod securitate)** și introduceți și parola Wi-Fi, dacă e cazul, la câmpul **Key (Cheie)**.

   În funcție de tipul de criptare o 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**.

   Opțiunile de la **Security Mode (Mod securitate)** sunt **None (Niciuna)**, **WEP**, **WPA-PSK**, **WPA2-PSK**, **WPA3-SAE**, **WPA3-SAE/WPA2-PSK**, **WPA-PSK & WPA2-PSK**, **WPA** și **WPA2**.



Aceste opțiuni stabilesc modul de criptare și de autentificare a rețelei wireless. **None (Niciuna)** dezactivează criptarea și lasă rețeaua deschisă, fără parolă, fiind recomandată doar în scenarii speciale. **WEP** este un standard vechi, considerat nesigur, și ar trebui evitat. **WPA-PSK** și **WPA2-PSK** folosesc o parolă comună (cheie pre-partajată) pentru autentificarea clienților, **WPA2-PSK** oferind un nivel de securitate net superior și fiind cea mai răspândită alegere pentru rețelele casnice și de birou.

WPA3-SAE este cel mai nou și mai sigur standard, care îmbunătățește protecția parolei prin mecanismul SAE, însă necesită dispozitive client compatibile. Opțiunile mixte **WPA3-SAE/WPA2-PSK** și **WPA-PSK & WPA2-PSK** sunt moduri de tranziție, care permit conectarea simultană atât a dispozitivelor mai noi, cât și a celor mai vechi, asigurând compatibilitate maximă.

În final, **WPA** și **WPA2** (fără *PSK*) sunt modurile de tip *Enterprise*, în care autentificarea se realizează printr-un server **RADIUS**, fiind destinate rețelelor de companie ce necesită identificarea individuală a utilizatorilor.

6. 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** sau/și fila **5GHz**.

---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.

Configurările IP de la **Internet Settings (Setări internet)** 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

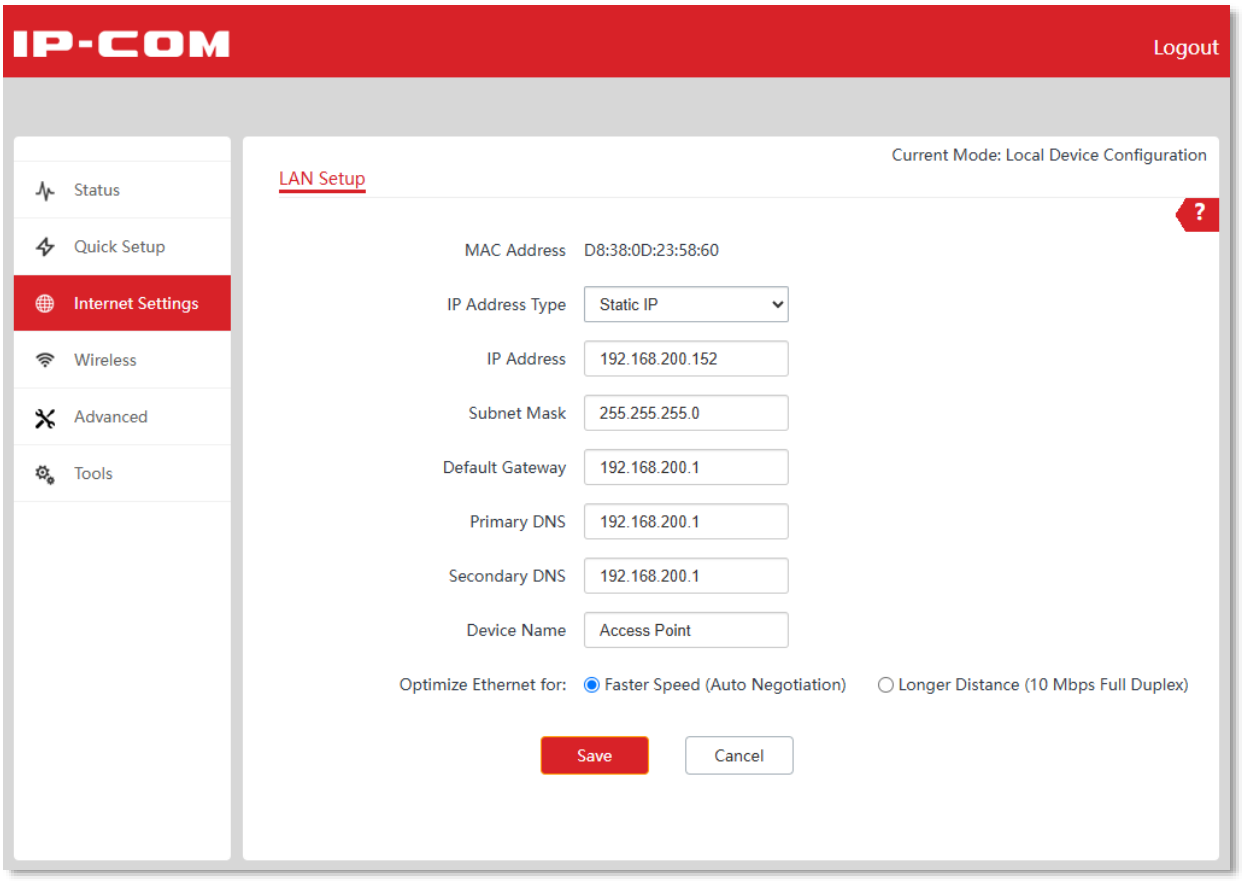
1. Conectați-vă la interfața web a punctului de acces.
2. Navigați la **Internet Settings (Setări internet)**.
3. La **IP Address Type (Tip adresă IP)** selectați modul în care punctul de acces obține informațiile IP. Fie selectați **Static IP (IP static)** și completați manual toate câmpurile de sub, 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.

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

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



---Sfârșit

Descriere parametri din meniul Internet Settings (Setări internet)

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

Parametru	Descriere
IP Address Type **(Tip adresă IP)**	Specifică modul de obținere a adresei IP a punctului de acces. – **Static IP (IP static):** Indică faptul că adresa IP, masca de subrețea, gateway-ul și serverul DNS sunt setate manual. – **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.  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 **(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.  – 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)**.
Subnet Mask **(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 **(Gateway implicit)**	Specifică IP-ul de comunicare cu un ruter (sau gateway) pentru a avea acces la internet (sau la o rețea externă). De obicei acest IP este cel al ruterului din amonte ce partajează internetul.

Parametru	Descriere
Primary DNS **(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. 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. 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 **(DNS secundar)**	Specifică adresa IP a serverului DNS secundar al punctului de acces. Acest parametru este opțional. Dacă există două adrese IP de server DNS, puteți introduce adresa IP secundară în acest câmp.
Device Name **(Nume dispozitiv)**	Specifică numele punctului de acces, acesta fiind utilizat pentru identificarea în rețea. 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.
Optimize Ethernet for (Optimizare port Ethernet pentru)	Specifică modul de comunicare și funcționare pentru portul Ethernet, cel cu PoE: – **Faster Speed (Auto Negotiation) (Viteză mai rapidă (Negociere automată)):** Acest mod oferă o rată de transmisie mare, dar o distanță scurtă de transmisie. În general, acest mod este recomandat. – **Longer Distance (10 Mbps Full Duplex) (Distanță mai lungă (10 Mbps Full Duplex)):** Acest mod prezintă o distanță de transmisie lungă, dar o rată de transmisie relativ scăzută, de obicei 10 Mbps. Opțiunea **Longer Distance (10 Mbps Full Duplex) (Distanță mai lungă (10 Mbps Full Duplex))** este recomandată numai dacă lungimea cablului Ethernet, care conectează portul PoE al punctului de acces la echipamentul de la celălalt capăt, depășește 100 de metri. În această situație, portul LAN al celuilalt echipament conectat trebuie să fie setat pe modul de auto-negociere. În caz contrar, este posibil ca portul de pe echipamentul IP-COM să nu poată transmite sau primi date corect**.**

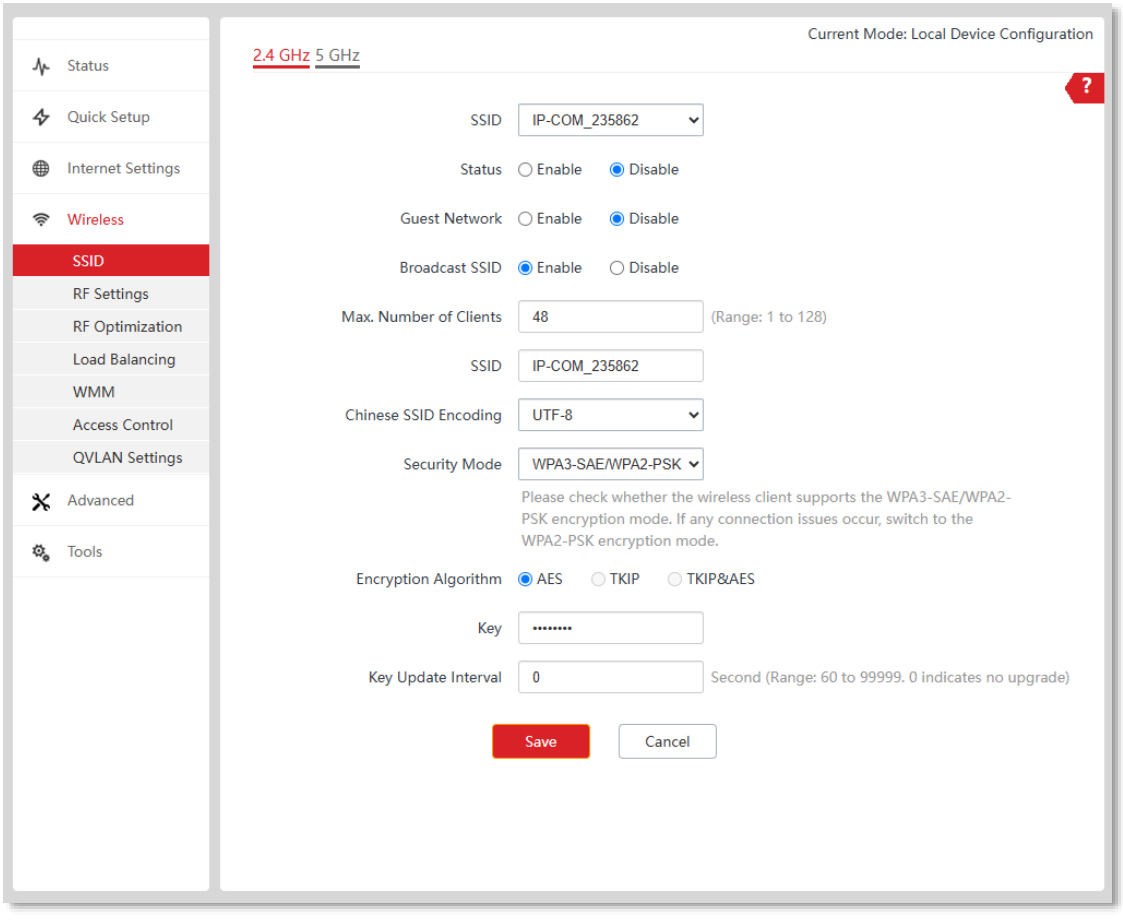
6 Meniul Wireless

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 7 sau 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** 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. Primul SSID afișat pe pagină, sub fila benzii radio, este SSID-ul principal al benzii radio. Se permite configurarea unui număr de 7 sau 8 SSID-uri pe fila **2.4 GHz** și 4 SSID-uri pe **5 GHz**.
Status **(Stare)**	Se activează sau dezactivează SSID-ul selectat. 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 **(Difuzare SSID)**	Ascunde sau afișează numele rețelei Wi-Fi — funcție cunoscută la alte echipamente comerciale și ca *ascundere rețea Wi-Fi*. 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. Dezactivarea difuzării contribuie la îmbunătățirea securității rețelei Wi-Fi.
Guest Network **(Rețea 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. 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. Note 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.
Max. Number of Clients **(Număr maxim de clienți)**	Stabilește câți clienți se pot conecta simultan la rețeaua Wi-Fi a unui SSID. Odată atinsă această limită, clienții noi nu se mai pot conecta la SSID până când alți clienți nu se deconectează. Numărul maxim e indicat în interfață. Se acceptă maxim 128 de clienți.

Parametru	Descriere
SSID	Folosit pentru a schimba numele SSID-ului selectat. Mai exact, e numele rețelei Wi-Fi.
Chinese SSID Encoding **(Codificare SSID chineză)**	Este o opțiune care stabilește schema de codificare a caracterelor folosită pentru numele rețelei (SSID) atunci când acesta conține caractere chinezești. Caracterele chinezești nu pot fi reprezentate prin codarea standard ASCII, ci necesită seturi de caractere dedicate. Pentru a se asigura că dispozitivele client afișează corect un SSID care include astfel de caractere, echipamentul trebuie să utilizeze aceeași schemă de codificare ca și clienții care se conectează. Cele două opțiuni disponibile sunt: – **UTF-8:** standardul universal de codificare Unicode, compatibil cu majoritatea dispozitivelor moderne și capabil să reprezinte practic orice caracter, indiferent de limbă. Aceasta este opțiunea implicită și cea recomandată în mod obișnuit. – **GB2312:** un standard de codificare mai vechi, dezvoltat specific pentru caracterele chinezești simplificate, utilizat în special de dispozitivele și sistemele mai vechi din regiunea respectivă. În practică, această setare are relevanță doar dacă SSID-ul conține caractere chinezești. Dacă numele rețelei folosește exclusiv caractere latine (litere, cifre, simboluri uzuale), opțiunea nu influențează afișarea, iar valoarea implicită **UTF-8** poate fi păstrată fără probleme.
Security Mode **(Mod securitate)**	Se aleg protocoalele de securitate Wi-Fi pentru SSID-ul selectat. Opțiunile includ: None (Niciuna), WPA-PSK, WPA2-PSK, Mixed WPA/WPA2-PSK (Mixt WPA/WPA2-PSK), WPA, WPA2, WPA3-SAE și WPA2-PSK&WPA3-SAE. Modurile de securitate cu toate sub-opțiunile afișate sunt prezentate începând cu secțiunea următoare. Note 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.

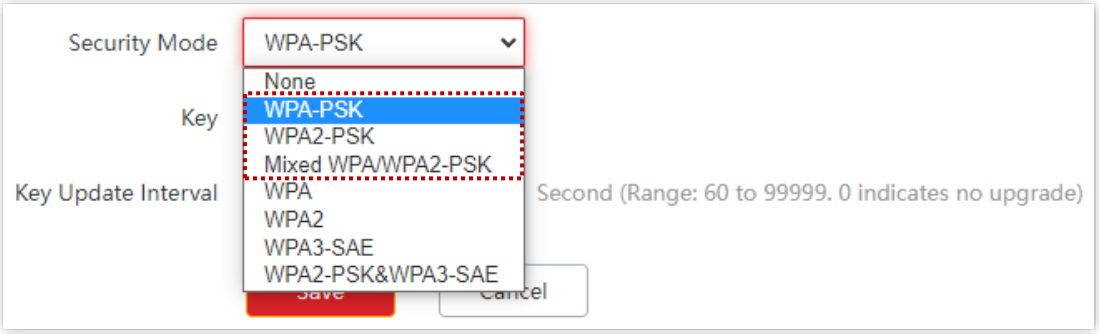
Echipamentul acceptă diverse moduri de securitate pentru criptarea rețelei, anume: **None (Niciuna)**, **WPA-PSK**, **WPA2-PSK**, **Mixed WPA/WPA2-PSK (Mixt WPA/WPA2-PSK)**, **WPA**, **WPA2**, **WPA3-SAE** și **WPA2-PSK&WPA3-SAE**. Modurile pot diferi în funcție de modelul de echipament și bandă selectată.

- **None (Niciuna)**

  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 (Mixt WPA/WPA2-PSK)**

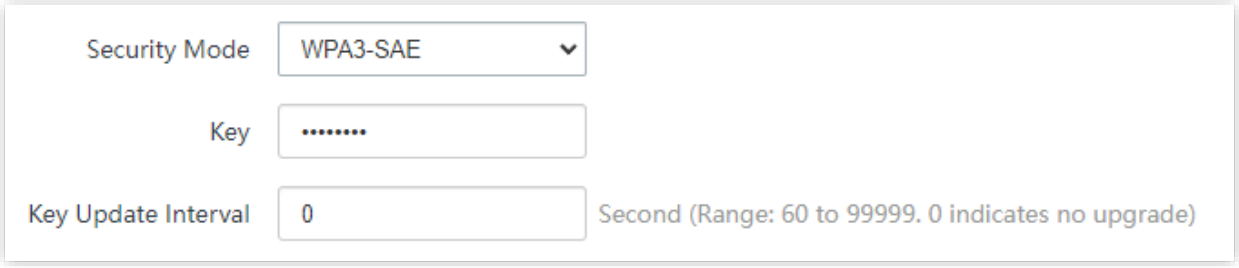
  Permite conectarea simultană a clienților care suportă **WPA-PSK** și a celor care suportă **WPA2-PSK**. Punctul de acces negociază automat cu fiecare client cel mai bun protocol suportat. Această opțiune este utilă în rețelele cu dispozitive eterogene, unde coexistă echipamente vechi alături de unele 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.

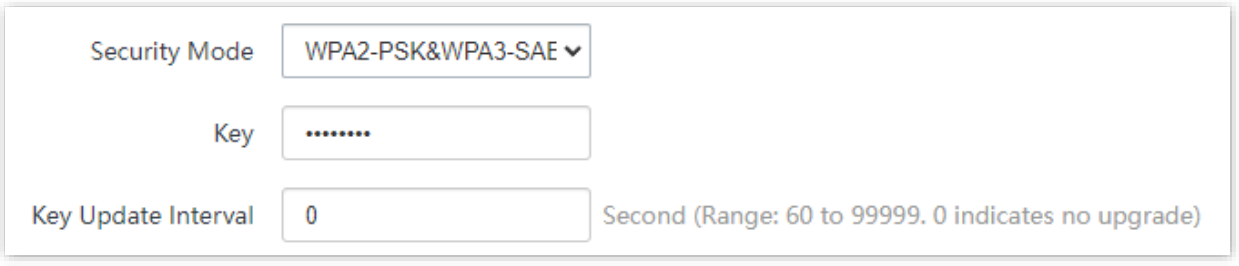
  Tip

  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

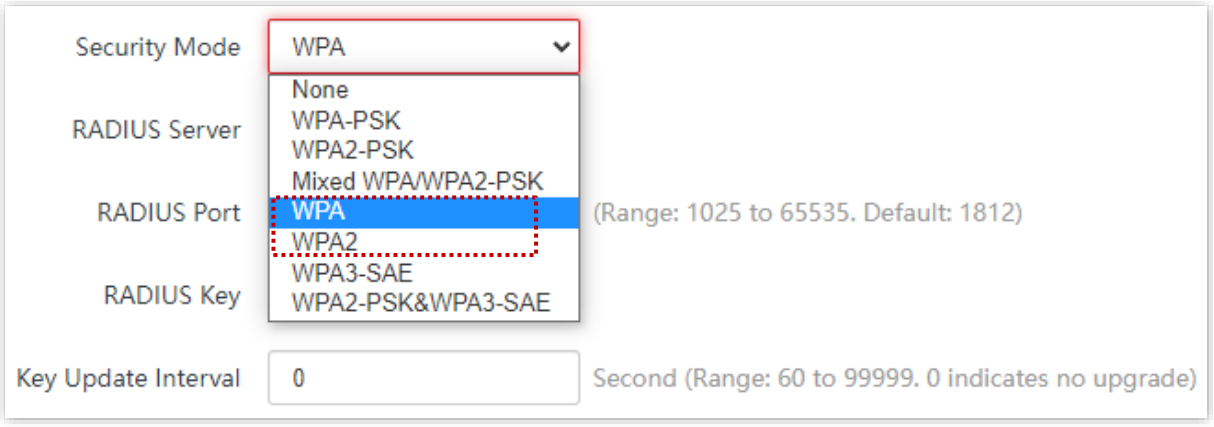
Parametru	Descriere
Security Mode **(Mod securitate)**	Specifică modul de securitate cu cheie personală sau pre-partajată, inclusiv **WPA-PSK, WPA2-PSK, Mixed WPA/WPA2-PSK (Mixt WPA/WPA2-PSK), WPA3-SAE** și **WPA2-PSK&WPA3-SAE.** – **WPA-PSK:** Indică faptul că rețeaua Wi-Fi corespunzătoare SSID-ului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

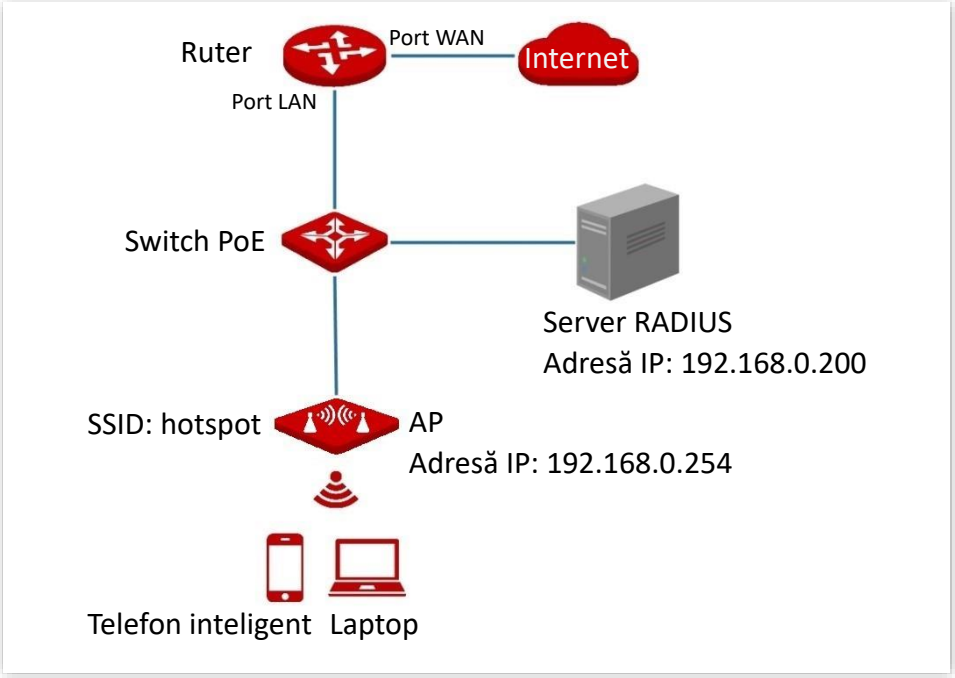
Parametru	Descriere
Security Mode **(Mod securitate)**	Opțiunile **WPA** și **WPA2** sunt disponibile pentru protecția rețelei cu un server RADIUS. – **WPA:** Indică faptul că rețeaua Wi-Fi corespunzătoare SSID-ului selectat este criptată cu WPA. – **WPA2:** Indică faptul că rețeaua Wi-Fi corespunzătoare SSID-ului selectat este criptată cu WPA2.
RADIUS Server **(Server RADIUS)**	Specifică adresa IP a serverului RADIUS pentru autentificarea clientului. 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 **(Port RADIUS)**	Specifică numărul de port logic UDP al serverului RADIUS pentru autentificarea clientului. Portul UDP folosit pentru autentificare poate fi în general **1812**.
RADIUS Key **(Cheie RADIUS)**	Cheia (parola) comună între AP și serverul RADIUS, folosită pentru autentificarea reciprocă a celor două dispozitive.

6.1.3 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.

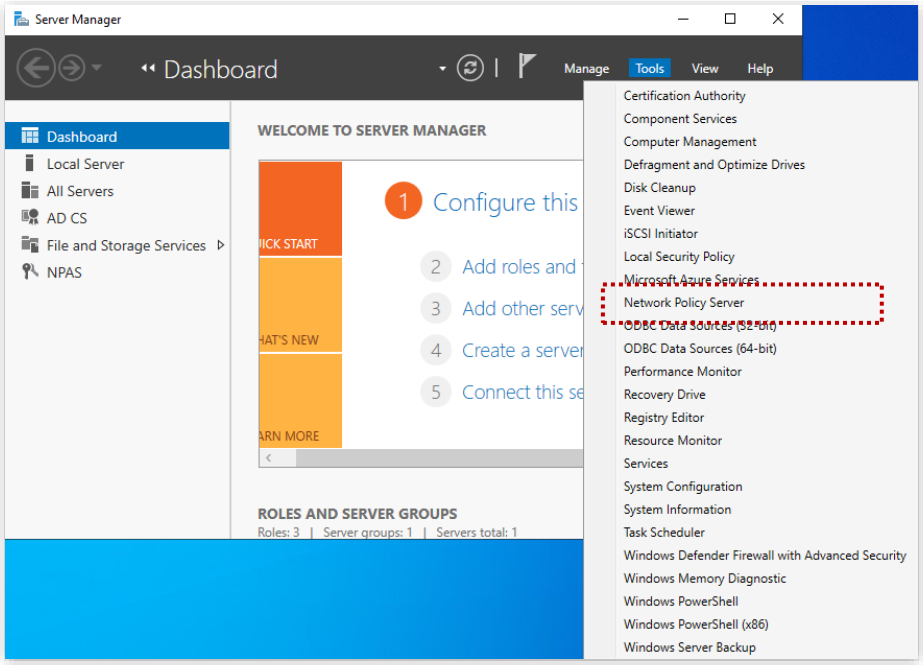
1. Conectați-vă la interfața web a punctului de acces.
2. Navigați la **Wireless** > **SSID.**
3. Asigurați-vă că sunteți pe fila **2.4 GHz**.
4. Selectați al doilea SSID din lista derulantă **SSID.**
5. Setați **Status (Starea)** pe **Enable (Activat).**

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).**

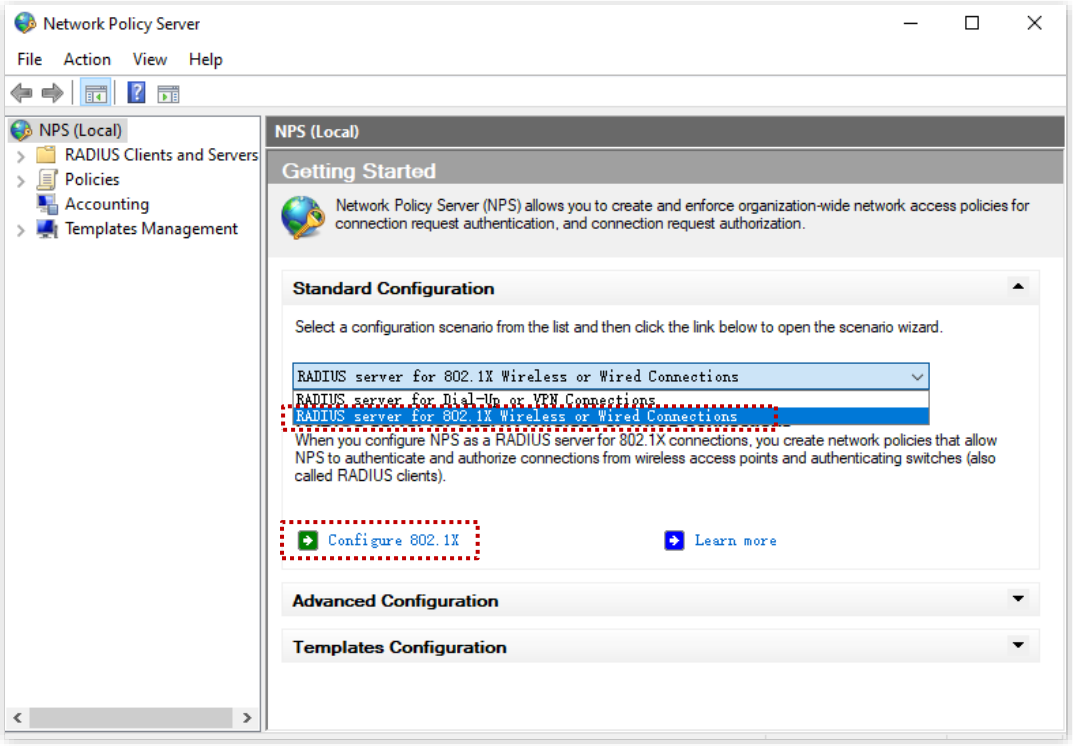
II. Acum trebuie să configurați serverul RADIUS plus alte politici pe un server Windows

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.

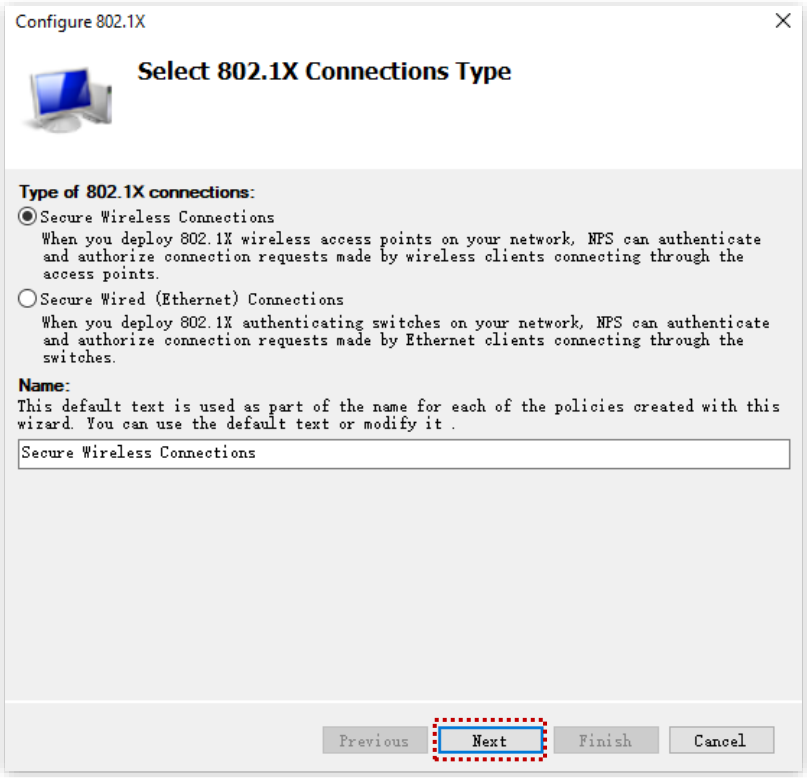
1. Trebuie să instalați serviciile **Active Directory Certificate Services** și **Network Policy and Access Services** și să implementați un certificat. Din meniul de **Start** din Windows Server căutați și deschideți **Server Manager**.
2. Din **Server Manager** accesați **Dashboard** > **Add roles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

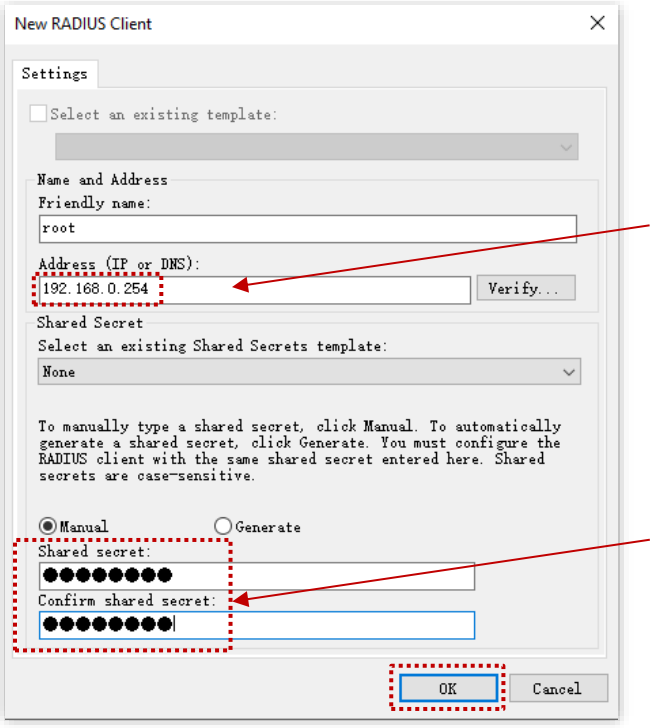


7. Selectați **Secure Wireless Connections** pentru **Type of 802.1X connections**. Modificați numele după cum este necesar, care în acest exemplu este *Secure Wireless Connections*, și faceți clic pe **Next**.



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

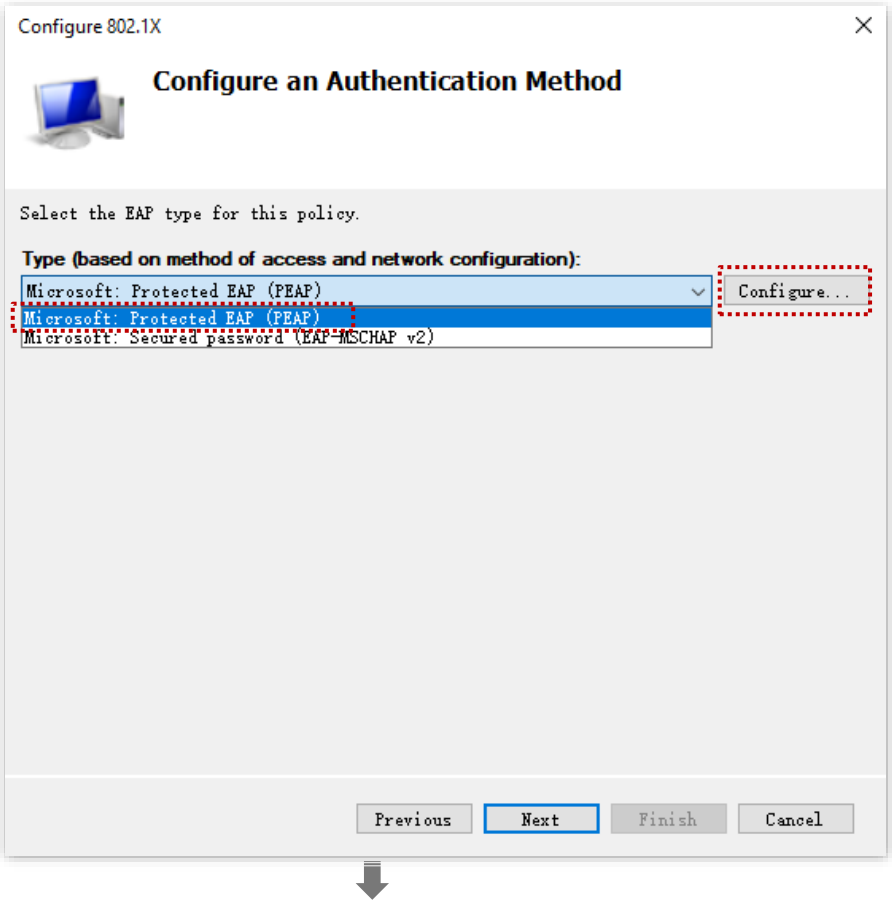
9. Introduceți un nume la **Friendly name** și adresa IP a punctului de acces IP-COM. Introduceți parola *UmXmL9UK* în casetele text **Shared secret** și **Confirm shared secret**. Apoi faceți clic pe **OK**.

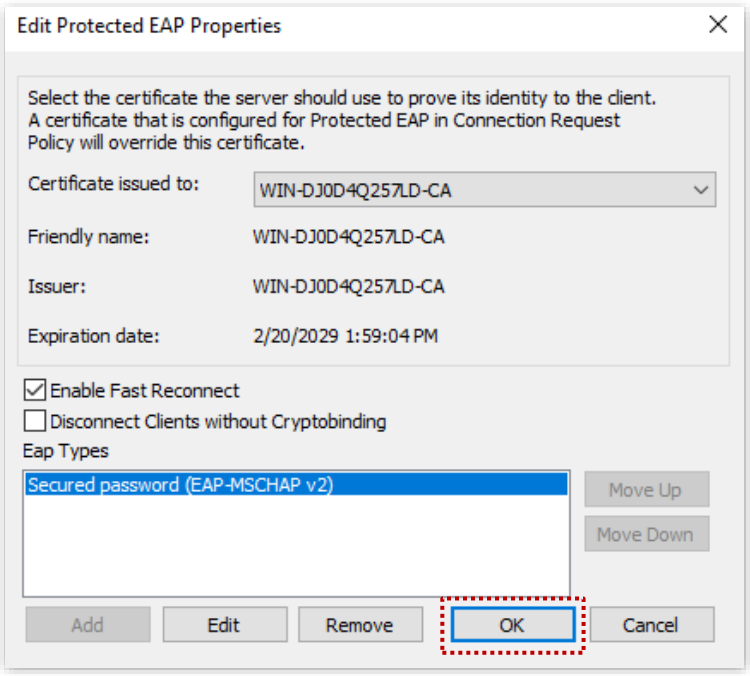


Adresa IP a punctului de acces.

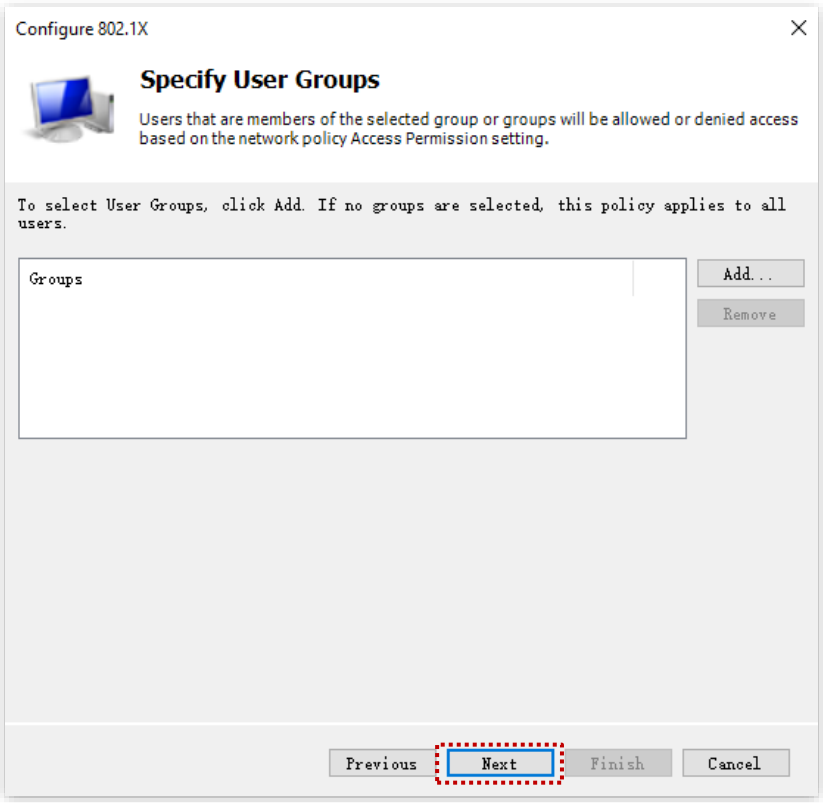
Același cu cel specificat la câmpul **RADIU Key (Cheie RADIUS)** din interfața punctului de acces IP-COM.

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.

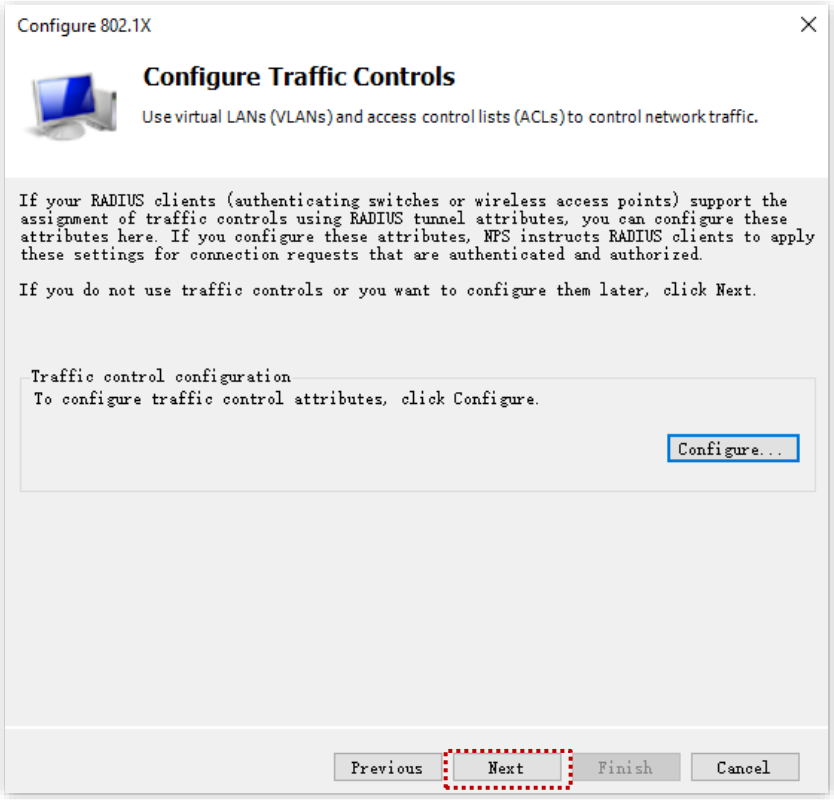


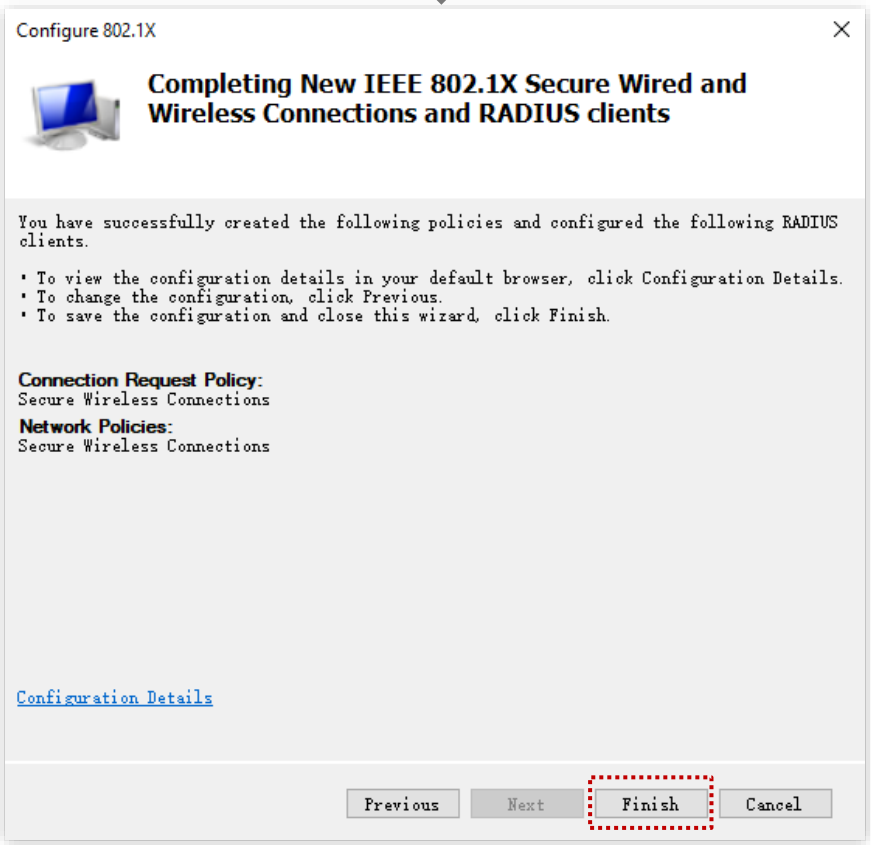


11. Faceți clic pe **Next** din fereastra **Specify User Groups.**



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**.

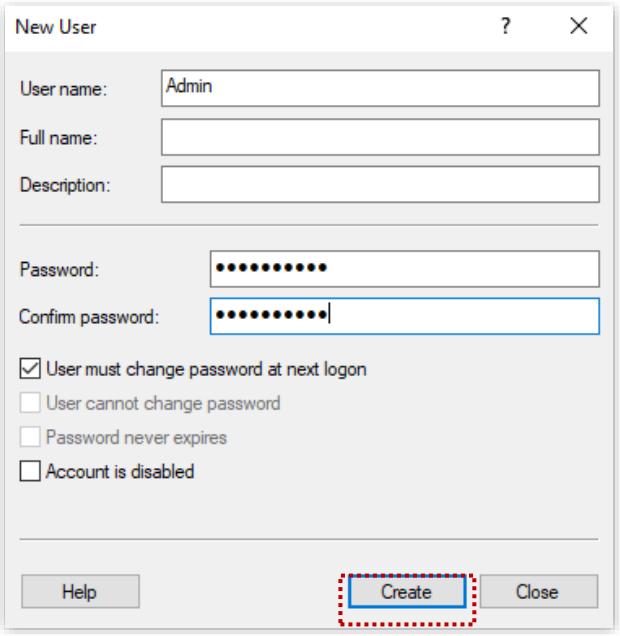




III. Creați conturile de autentificare și unele politici

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**.

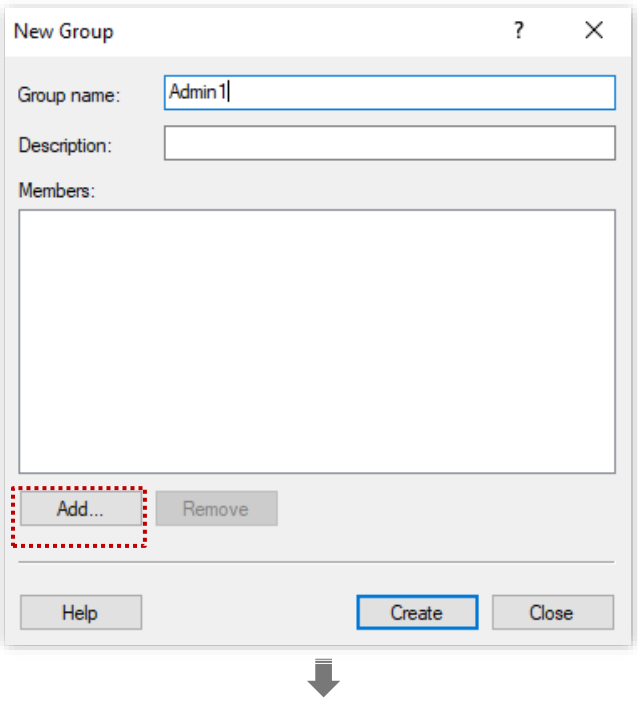
2. Faceți clic dreapta pe **Users** și clic pe **New User**. Introduceți numele de utilizator și parola, care în acest exemplu sunt ***Admin*** ca nume de utilizator și ***JohnDoe123*** pentru parolă. Apoi faceți clic pe **Create**.

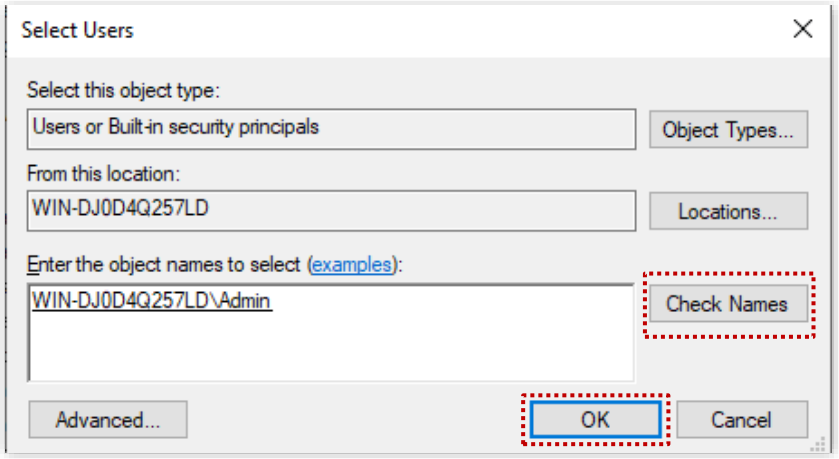


3. Acum creați un grup de utilizatori în care va fi adăugat acest cont nou creat. Pentru asta, faceți clic dreapta pe **Groups** și selectați **New Group**. La **Group name** introduceți ca exemplu ***Admin1*,** și faceți clic pe **Add.**

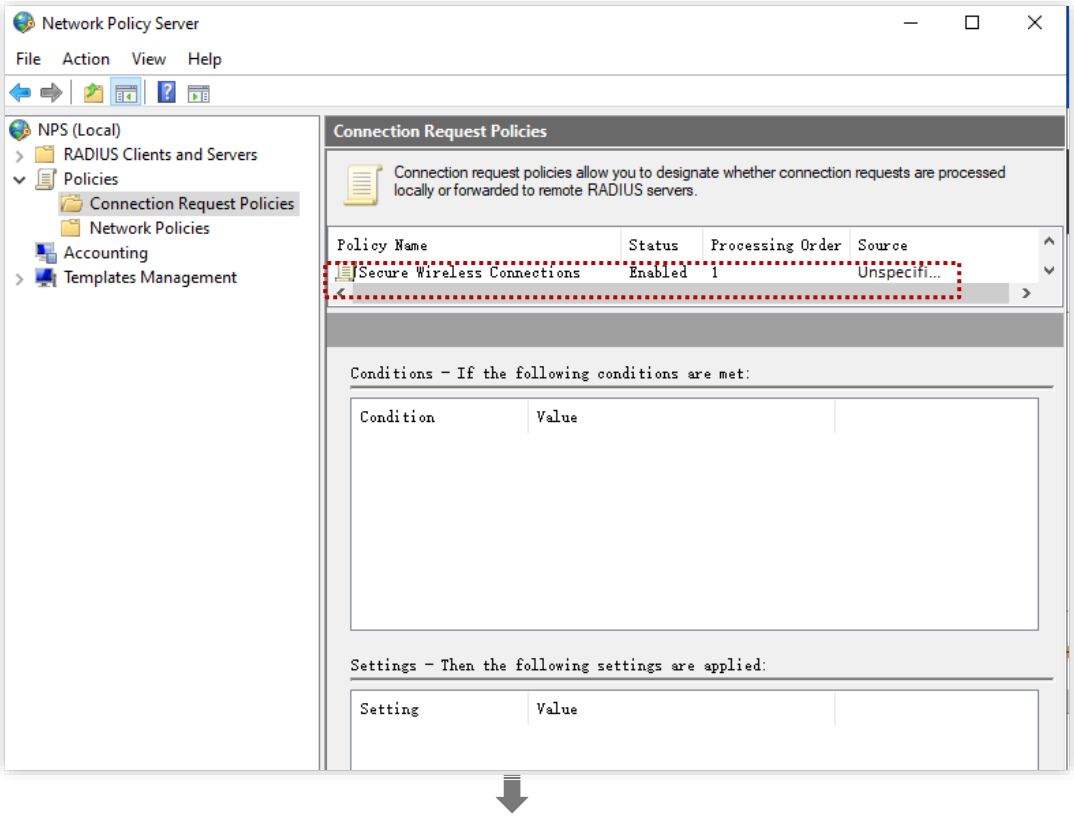
4. În noua fereastră în câmpul **Enter the object names to select**, tastați numele de utilizator creat și faceți clic pe butonul din dreapta **Check Names** și apoi pe **OK**.

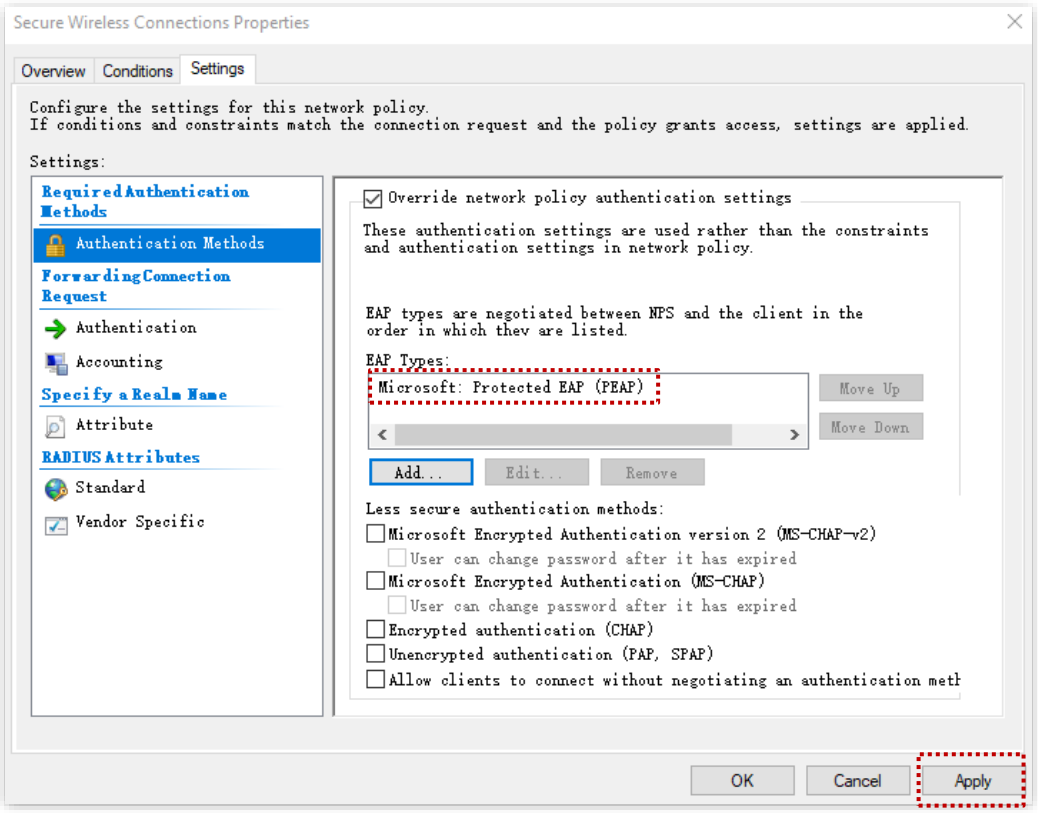
5. La final, în fereastra **New Group** faceți clic pe butonul **Create**.





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**.

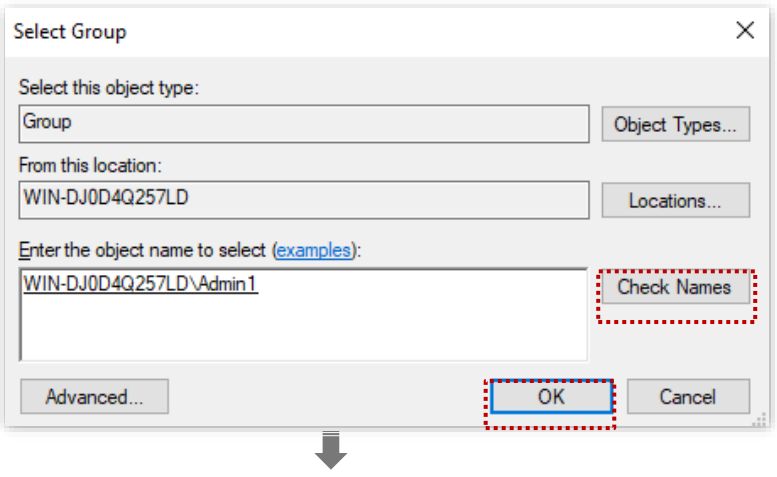


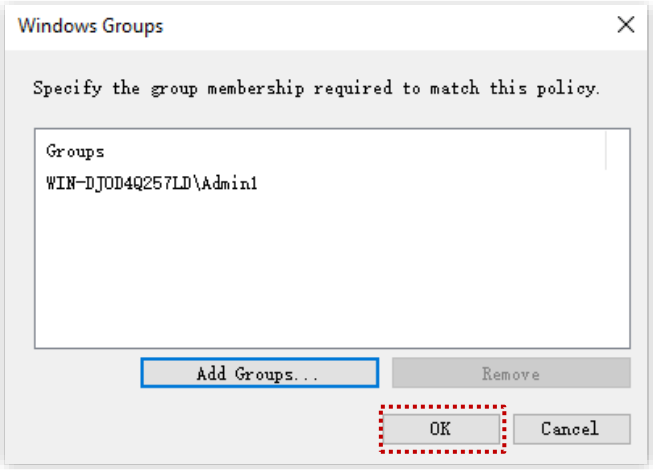


11. Apoi faceți clic pe **Network Policies**, de unde faceți dublu clic pe **Secure Wireless Connections**.

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 user 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

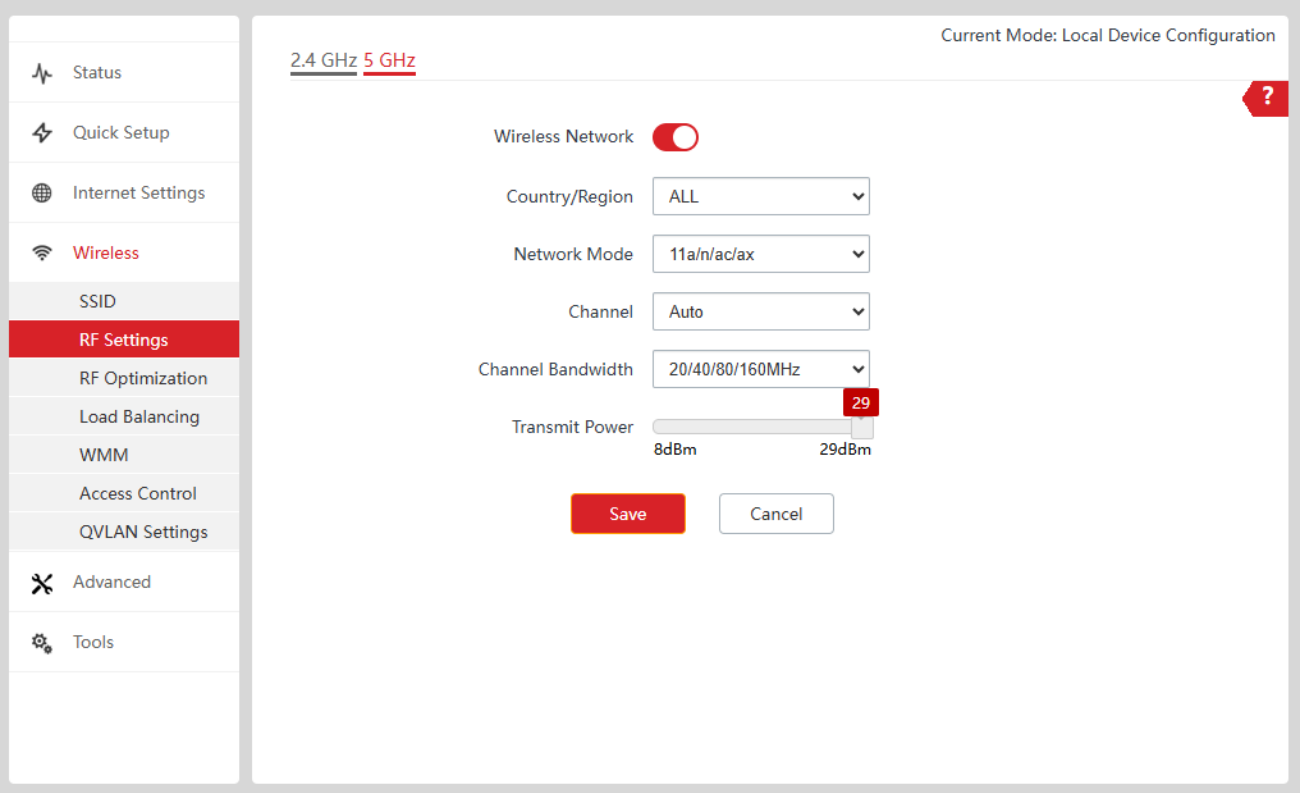
Dacă conexiunea eșuează, vă rugăm:

- 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**	Utilizat pentru a selecta banda radio pentru care urmează să fie modificate setările.
Fila **5 GHz**	
Wireless Network (Rețea wireless)	Specifică dacă se activează funcția de rețea Wi-Fi pe banda respectivă. Această setare se aplică pentru toate SSID-urile din bandă.

Parametru	Descriere
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. În listă găsiți majoritatea țărilor și regiunilor, inclusiv România.
Network Mode (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)**. Opțiunile disponibile pentru **2.4 GHz** sunt **11b, 11g, 11b/g, 11b/g/n** și **11b/g/n/ax,** iar opțiunile disponibile pentru **5 GHz** sunt **11a, 11ac, 11a/n** și **11a/n/ac/ax.** – **11b:** AP-ul emite pe banda respectivă rețea Wi-Fi conformă standardului IEEE 802.11b. – **11g:** AP-ul emite pe banda respectivă rețea Wi-Fi conformă standardului IEEE 802.11g. – **11b/g:** AP-ul emite pe banda respectivă rețea Wi-Fi conformă standardelor IEEE 802.11b și 802.11g. – **11b/g/n:** AP-ul emite pe banda respectivă rețea Wi-Fi conformă standardelor IEEE 802.11b, 802.11g și 802.11n. – **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. – **11a:** AP-ul emite pe banda respectivă rețea Wi-Fi conformă standardului IEEE 802.11a. – **11ac:** AP-ul emite pe banda respectivă rețea Wi-Fi conformă standardului 802.11ac. – **11a/n:** AP-ul emite pe banda respectivă rețea Wi-Fi conformă standardelor IEEE 802.11a și 802.11n. – **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. Tip Modurile de rețea Wi-Fi ale punctului de acces pot diferi în funcție de modelul de punct de acces. Prevalează produsul real.

Parametru	Descriere
Channel **(Canal)**	Specifică canalul de operare pe banda selectată și se aplică pentru toate SSID-urile de pe bandă. **Auto (Automat):** Indică faptul că punctul de acces își ajustează automat canalul de operare în funcție de rețelele din jur sau diverși algoritmi. 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-6-LR, pe banda de 5 GHz se regăsesc canalele identificate cu numerele standard **36**, **40**, **44**, **48**, **149**, **153**, **157**, **161.** Iar pe banda de 2,4 GHz se regăsesc canalele identificate cu numerele standard **1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12** și **13**. Mai multe detalii despre frecvențele de operare, despre corespondența dintre numerele de canal și frecvențele asociate, precum și despre frecvențele permise oficial în România și condițiile de utilizare (puterea maximă admisă, restricțiile DFS) se găsesc pe pagina web ANCOM (www.ancom.ro) și în standardele ETSI aplicabile, anume, EN 300 328 pentru banda de 2,4 GHz și EN 301 893 pentru banda de 5 GHz. Dacă întâmpinați frecvent deconectări, întârzieri sau rate reduse, atunci încercați să schimbați canalul.
Channel Bandwidth **(Lățime canal)**	Specifică lățimea canalului de la **Channel (Canal)** și se aplică pentru toate SSID-urile de pe bandă. 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. Lățimea unui canal poate fi: – **20 MHz:** Indică faptul că punctul de acces poate utiliza o lățime a canalului de 20 MHz. Opțiune găsită pe banda de 2,4 GHz și 5 GHz. – **40 MHz:** Indică faptul că punctul de acces poate utiliza o lățime a canalului de 40 MHz. Opțiune găsită pe banda de 2,4 GHz și 5 GHz. – **80 MHz:** Indică faptul că punctul de acces poate utiliza o lățime a canalului de 80 MHz. Opțiune găsită pe banda de 5 GHz. – **160 MHz:** Indică faptul că punctul de acces poate utiliza o lățime a canalului de 160 MHz. Opțiune găsită pe banda de 5 GHz. – Automat cu opțiunea selectabilă **20/40MHz** pe 2,4 GHz și **20/40/80/160MHz** pe 5 GHz. AP-ul ajustează automat lățimea canalului în funcție de interferențele din jur și în funcție de diverși algoritmi.

Parametru	Descriere
Transmit Power **(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)**. 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. 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.
Save **(Salvare)**	Apăsați acest buton pentru salvarea și aplicarea locală a acestor setări. E posibil ca conexiunea să fie întreruptă.
Cancel **(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)

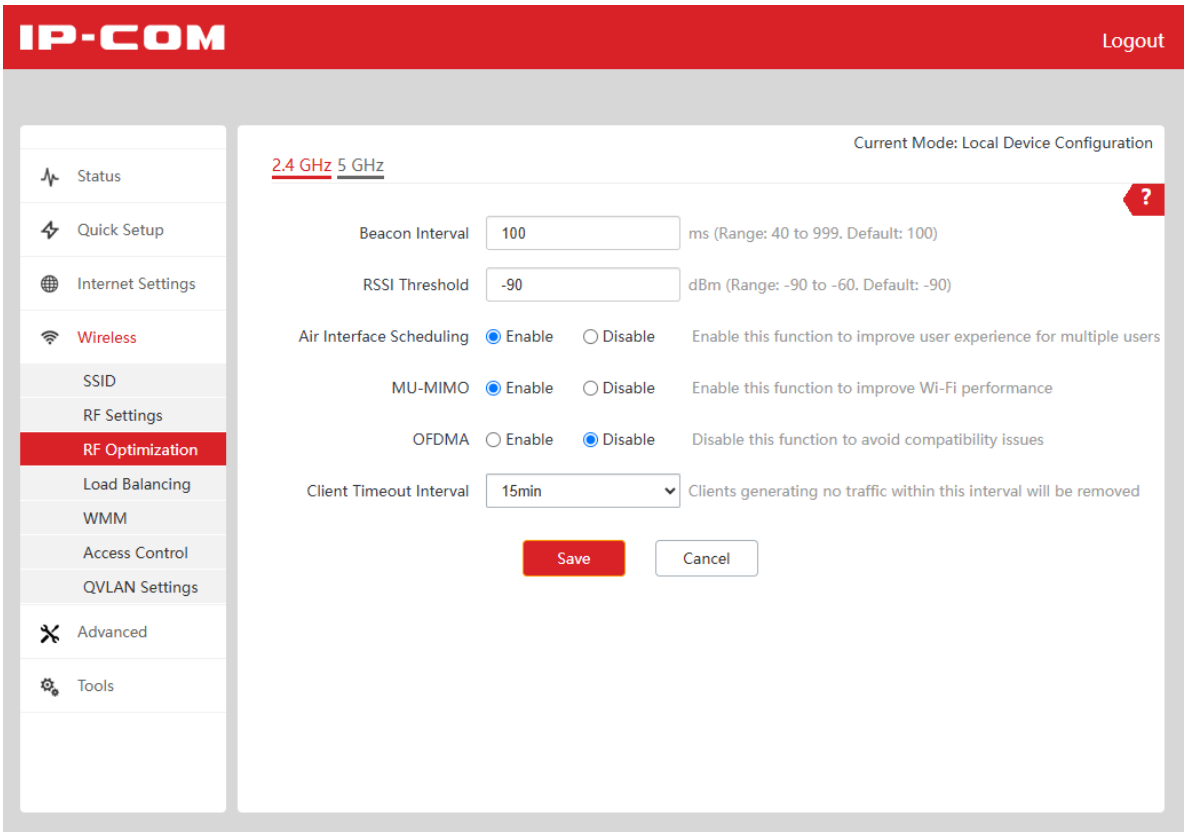
Pentru a accesa pagina de optimizare radio avansată, conectați-vă la interfața web de gestionare și navigați la **Wireless** > **RF Optimization (Optimizare radiofrecvențe)**. Puteți modifica parametrii pentru a optimiza performanța wireless.

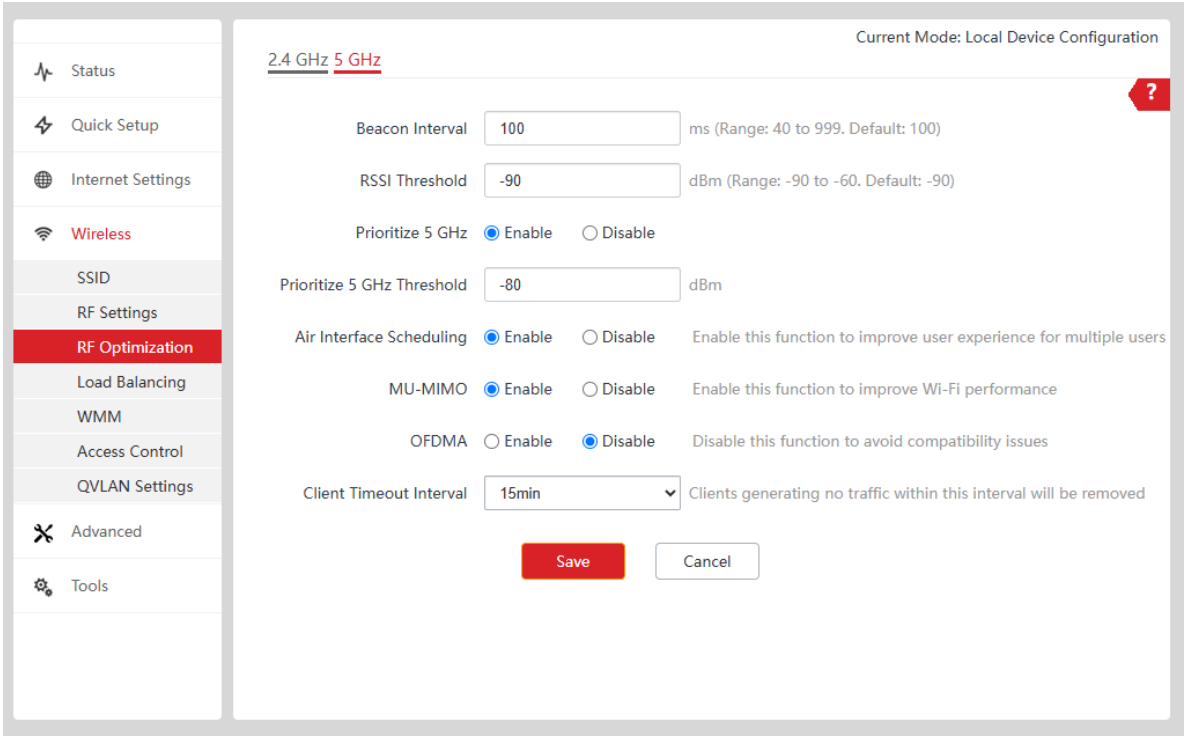
Toate setările de aici se aplică pentru toate SSID-urile pe fiecare bandă în parte, apăsând fila **2.4 GHz** pentru banda de 2,4 GHz și fila **5 GHz** pentru banda de 5 GHz.

Următoarele imagini prezintă setările aferente pentru banda de 2,4 GHz și apoi pentru 5 GHz.

Note

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





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**	

Parametru	Descriere
Beacon Interval **(Interval cadre Beacon)**	Specifică intervalul de timp la care punctul de acces transmite cadre *Beacon*, măsurat în milisecunde. 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. 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. 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. Valoarea implicită este de obicei **100** milisecunde, fiind un echilibru între durata de conectare și performanța rețelei. Se pot introduce valori între **40-999** milisecunde.
RSSI Threshold **(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. Setarea greșită poate duce la deconectări frecvente sau imposibilitatea conectării dispozitivelor aflate în camerele mai îndepărtate. Intervalul admis este de la **-90** până la **-60 dBm.** Implicit fiind -**90 dBm**.
Air Interface Scheduling (Programare interfață aeriană)	Este o funcție care gestionează modul în care punctul de acces alocă timpul de transmisie pe canalul radio între clienții conectați, cu scopul de a oferi fiecărui dispozitiv o felie egală de timp de comunicare Wi-Fi (*airtime fairness*), indiferent de viteza la care comunică acesta cu AP-ul. Într-o rețea Wi-Fi clasică, dispozitivele lente (de exemplu, un telefon vechi pe standard 802.11n sau aflat la distanță, cu semnal slab) ocupă canalul radio mult mai mult timp pentru a transmite aceeași cantitate de date decât un dispozitiv modern (Wi-Fi 6, aproape de AP). Astfel, un singur client lent poate „bloca" practic canalul, încetinind întreaga rețea.  Această funcție este disponibilă pe unele puncte de acces. Produsul real prevalează.

Parametru	Descriere
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. 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.
OFDMA	Acronim pentru *Orthogonal Frequency-Division Multiple Access (acces multiplu prin diviziune ortogonală a frecvenței)* — o tehnologie introdusă de standardul Wi-Fi 6, care împarte canalul radio în mai multe subcanale (numite unități de resurse) și le alocă simultan mai multor clienți. 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). Totuși, **OFDMA** este disponibil doar pe clienții compatibili cu Wi-Fi 6 (802.11ax) 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. O funcție utilă de alocare a resurselor. Puteți seta o perioadă de deconectare după **1 minut** sau **2**, **5**, **10**, **15**, **30** sau **60 minute**. Implicit e pe **15 minute**, depinzând de model.
Prioritize 5 GHz **(Prioritizare 5 GHz)**	Activare sau dezactivare prioritizării conectării clienților Wi-Fi pe banda de 5 GHz în detrimentul 2,4 GHz, în anumite condiții. 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. 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).

Parametru	Descriere
Prioritize 5 GHz Threshold (Prag prioritizare 5 GHz)	Câmp vizibil doar dacă e activată opțiunea **Prioritize 5 GHz (Prioritizare 5 GHz).** Dacă puterea semnalelor transmise de un dispozitiv compatibil Wi-Fi este mai mare sau egală cu acest prag setat aici, atunci 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: – 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). – 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). Implicit este **-80 dBm**.

6.4 Submeniul Load Balancing (Echilibrare încărcare)

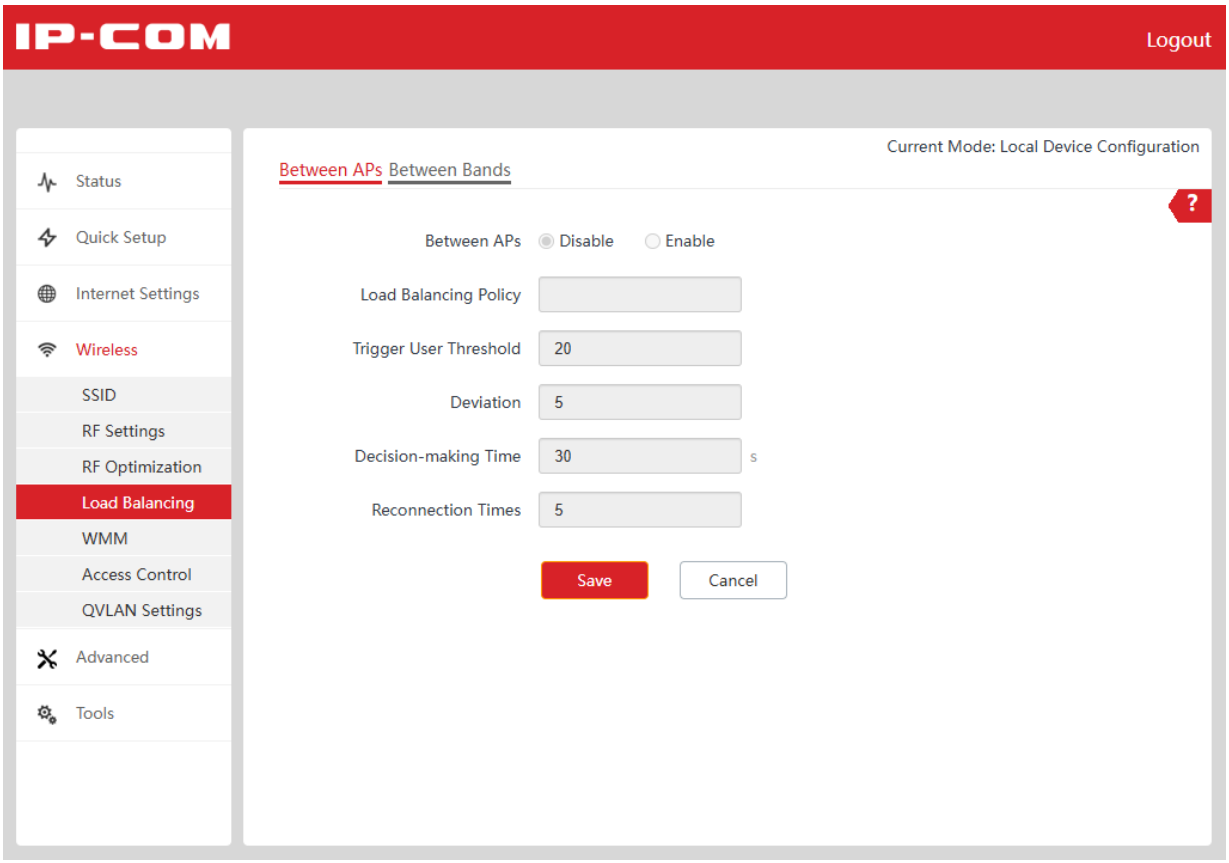
6.4.1 Echilibrare încărcare între AP-uri

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 aceeași politică de echilibrare a încărcării, anume informația trecută la câmpul **Load Balancing Policy (Politică echilibrare încărcare).** Dar au și SSID-uri și parole Wi-Fi identice, setate din **Wireless >** SSID, pe fiecare bandă de 2,4 GHz și 5 GHz.

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 AP-uri compatibile.
Load Balancing Policy **(Politică echilibrare încărcare)**	Acest parametru identifică politica de echilibrare a încărcării aplicată între punctele de acces care funcționează în cadrul aceleiași rețele gestionate. Politica nu se configurează manual la nivelul echipamentului, ci este transmisă de dispozitivul de management (controlerul de rețea). Funcția poate echilibra încărcarea numai între punctele de acces care aplică aceeași politică de echilibrare. Astfel, politica funcționează ca un identificator de grup: doar punctele de acces care partajează aceeași politică își redistribuie utilizatorii între ele, în vederea îmbunătățirii experienței utilizatorului. Câmpul devine activ numai atunci când funcția **Between APs (Între AP-uri)** este setată pe **Enable (Activare)**, iar echipamentul este administrat printr-un dispozitiv de management central care furnizează valoarea politicii.
Trigger User Threshold **(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. Implicit este setat pe **20 clienți**.

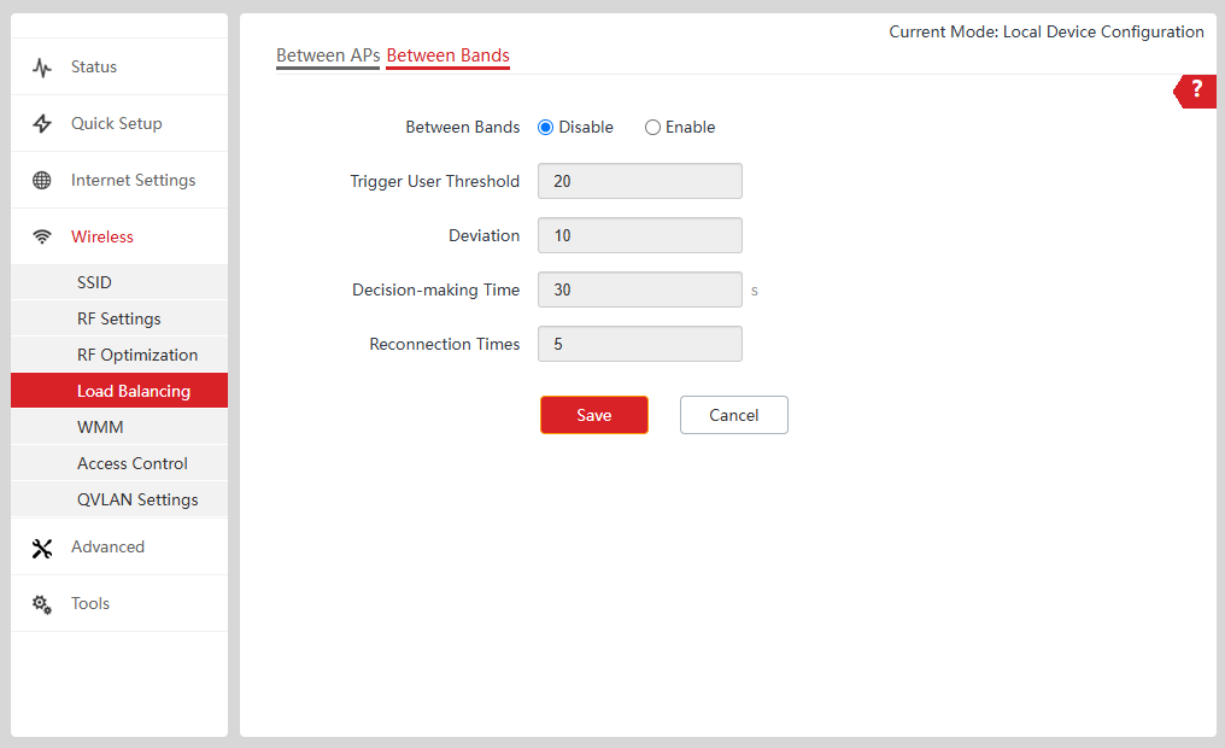
Parametru	Descriere
Deviation **(Deviere)**	Acest parametru stabilește diferența maximă admisă între numărul de utilizatori conectați la două puncte de acces care aplică aceeași politică de echilibrare a încărcării. Dacă abaterea dintre numărul de utilizatori ai celor două puncte de acces depășește această valoare, utilizatorii noi sunt direcționați cu prioritate către punctul de acces cu mai puțini utilizatori, în vederea reechilibrării încărcării între acestea. Implicit: **5 clienți**.
Decision-making Time **(Timp de decizie)**	Acest parametru stabilește intervalul de timp în care punctul de acces poate refuza cererile de conectare ale unui utilizator. În cadrul acestui interval, comportamentul punctului de acces este următorul: – Dacă numărul de refuzuri atinge valoarea stabilită în câmpul **Reconnection Times (Număr reconectări)**, punctul de acces permite accesul utilizatorului respectiv. – Dacă numărul de refuzuri nu atinge valoarea stabilită în câmpul **Reconnection Times (Număr reconectări)** în intervalul de timp specificat, contorul de refuzuri este resetat. Se recomandă păstrarea valorii implicite de **30 secunde**.
Reconnection Times **(Număr reconectări)**	Acest parametru stabilește numărul maxim de încercări de conectare ale unui utilizator. Dacă numărul de refuzuri ale punctului de acces atinge această valoare în cadrul intervalului stabilit în câmpul **Decision-making Time (Timp de decizie)**, atunci AP-ul permite accesul clientului respectiv. Se recomandă păstrarea valorii implicite de **5** 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 **(Între benzi)**	Această funcție permite echilibrarea încărcării între benzile de frecvență ale punctului de acces (2,4 GHz și 5 GHz), în vederea îmbunătățirii experienței utilizatorului. Echilibrarea se realizează pe baza numărului de utilizatori.
Trigger User Threshold **(Prag declanșare per user)**	Acest parametru stabilește pragul la care se declanșează echilibrarea încărcării între benzi. Atunci când numărul de utilizatori ai punctului de acces atinge acest prag, echilibrarea încărcării între benzi este activată. Valoarea implicită este de **20** de utilizatori.
Deviation **(Deviere)**	Acest parametru stabilește diferența admisă între numărul de utilizatori ai celor două benzi. Dacă abaterea depășește această valoare, utilizatorii noi sunt direcționați cu prioritate către banda cu mai puțini utilizatori. Valoarea implicită este de **10** utilizatori.
Decision-making Time **(Timp de decizie)**	Acest parametru stabilește intervalul de timp în care punctul de acces poate refuza cererile de conectare ale unui utilizator. În cadrul acestui interval, comportamentul punctului de acces este următorul: – Dacă numărul de refuzuri atinge valoarea stabilită în câmpul **Reconnection Times (Număr reconectări)**, punctul de acces permite accesul utilizatorului respectiv. – Dacă numărul de refuzuri nu atinge valoarea stabilită în câmpul **Reconnection Times (Număr reconectări)** în intervalul de timp specificat, contorul de refuzuri este resetat. Se recomandă păstrarea valorii implicite de **30** secunde.

Parametru	Descriere
Reconnection Times **(Număr reconectări)**	Acest parametru stabilește numărul maxim de încercări de conectare ale unui utilizator. Dacă numărul de refuzuri ale punctului de acces atinge această valoare în cadrul intervalului stabilit în câmpul **Decision-making Time (Timp de decizie)**, atunci se permite accesul clientului respectiv. Se recomandă păstrarea valorii implicite de 5 reconectări.

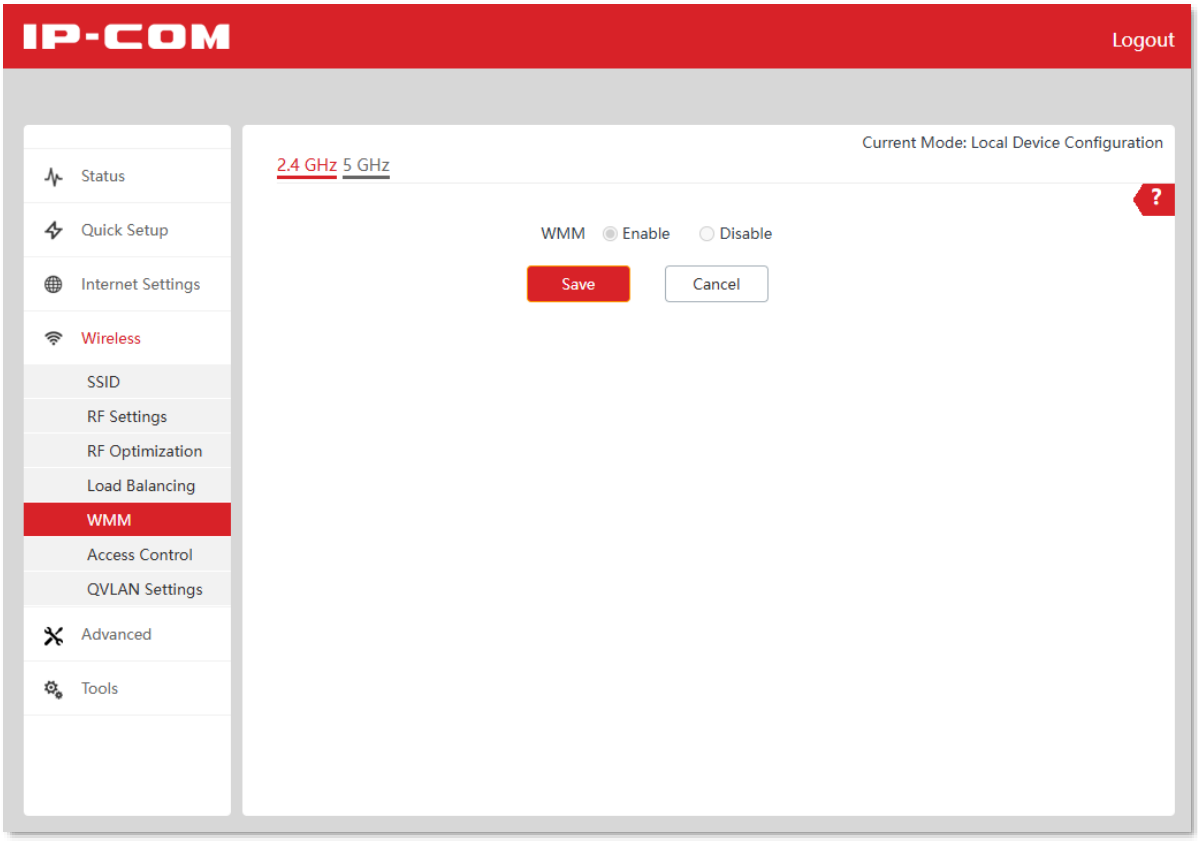
6.5 Submeniul WMM

Această pagină, accesibilă din **Wireless > WMM**, permite configurarea avansată a mecanismului WMM (Wi-Fi Multimedia) — un standard definit în specificația IEEE 802.11e, care asigură prioritizarea diferitelor tipuri de trafic wireless în funcție de sensibilitatea lor la întârzieri. Practic, **WMM** garantează că traficul critic, cum ar fi apelurile vocale, videoconferințele sau jocurile online, primește acces prioritar la canalul radio, în detrimentul traficului mai puțin urgent, precum transferurile de fișiere, e-mail-urile sau descărcările care rulează în fundal.

Mecanismul WMM stă la baza calității serviciilor *QoS (Quality of Service*) în rețelele wireless moderne și este indispensabil în medii dense, unde mai mulți utilizatori partajează simultan aceeași bandă radio. Fără WMM, toate tipurile de trafic ar concura egal pentru accesul la canal, ceea ce ar duce la sacadări în apelurile VoIP, întârzieri în jocurile online și calitate degradată a streaming-ului video, mai ales atunci când rețeaua este aglomerată.

Configurarea WMM se realizează separat pentru fiecare bandă radio (2,4 GHz și 5 GHz), prin intermediul filelor disponibile în partea superioară a paginii, întrucât caracteristicile de propagare și nivelul de interferențe diferă semnificativ între cele două frecvențe.

Următoarea imagine prezintă meniul **Wireless > WMM** cu fila **2.4 GHz** selectată. Există opțiunea de activare sau dezactivare a funcției **WMM** pe fiecare bandă în parte apăsând fila **2.4 GHz sau 5 GHz**.



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 setate de la **Mode (Mod)**:

- **Forbid only (Doar interzicere):** Dispozitivele cu adresele MAC adăugate în lista de mai jos nu au voie să se conecteze la rețea prin SSID-ul selectat. Toate celelalte dispozitive se pot conecta normal. E același lucru cu *Blacklist (Listă neagră)*.

- **Permit only (Doar permitere):** Doar dispozitivele cu adresele MAC adăugate în listă au voie să se conecteze. Toate celelalte sunt blocate. E același lucru cu *Whitelist (Listă albă)*.

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.

6.6.1 Blocarea unei adrese MAC pentru accesul printr-o rețea Wi-Fi (SSID)

Pentru a împiedica un anumit dispozitiv pe baza adresei MAC a adaptorului de rețea prin care acesta se conectează să se conecteze la rețeaua locală — și, implicit, la internet — printr-o rețea Wi-Fi emisă de punctul de acces, urmați pașii de mai jos:

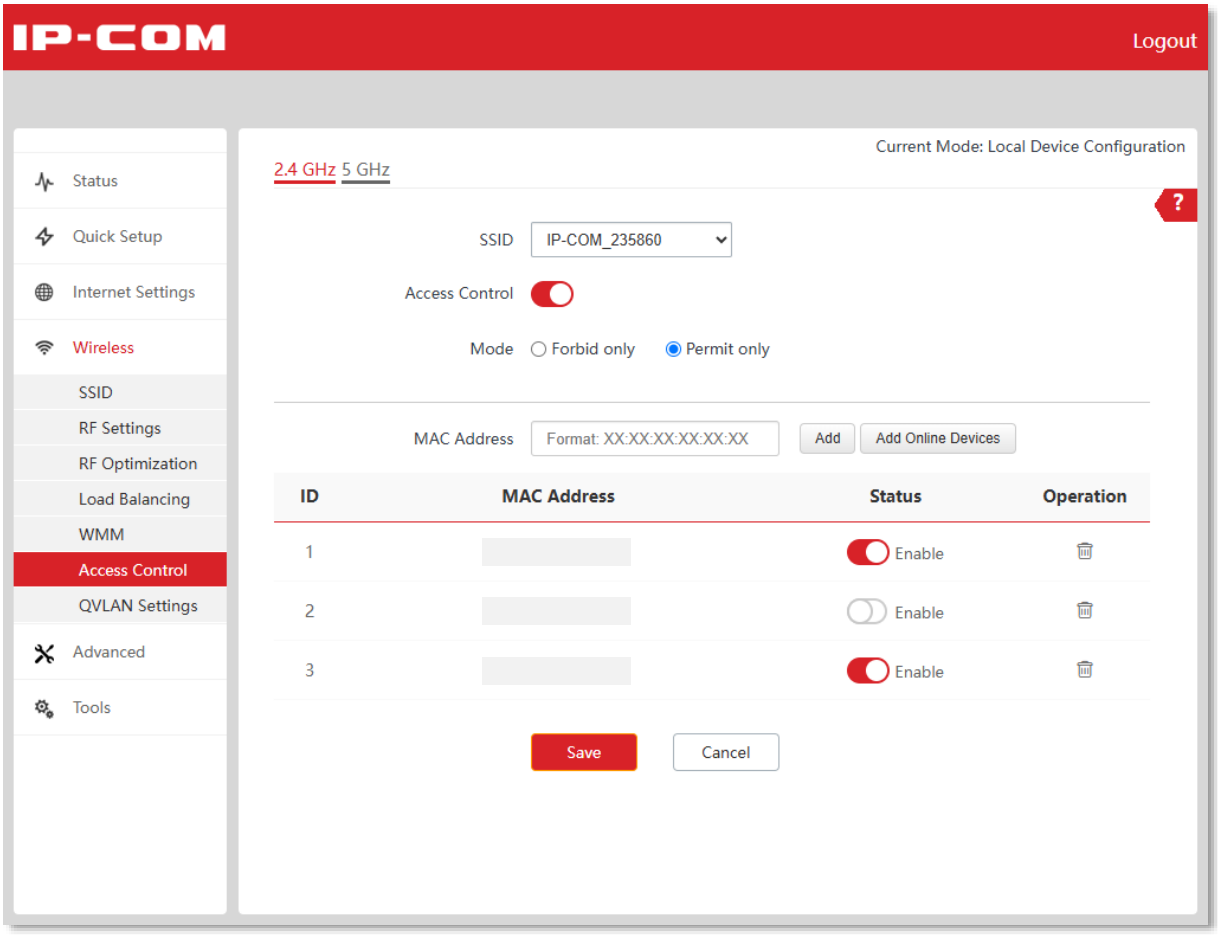
1. Conectați-vă la interfața web de gestionare a punctului de acces.
2. Navigați către **Wireless** > **Access Control (Control acces)**.
3. Selectați o bandă radio Wi-Fi unde trebuie implementată politica. În acest exemplu va fi banda de 2,4 GHz așadar se va apăsa fila **2.4 GHz**.
4. De la lista derulantă **SSID** selectați denumirea rețelei Wi-Fi pe care se va face filtrarea. Selectați ca exemplu ***IP-COM_235860***.
5. Activați funcția **Access Control (Control acces)**.
6. De la **Mode (Mod)** selectați **Forbid only (Doar interzicere)**.
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***.

   În listă asigurați-vă că adresa MAC respectivă are butonul **Enable (Activare)** activ.

   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 pasul **7** și **8**.



---Sfârșit

6.6.2 Permiterea doar anumitor adrese MAC să acceseze rețeaua printr-un SSID

În modul **Permit only (Doar permitere)**, numai dispozitivele ale căror adrese MAC au fost adăugate în listă se pot conecta la rețeaua Wi-Fi (SSID) selectată a punctului de acces, putând astfel accesa rețeaua locală și, implicit, internetul partajat de ruter. Toate celelalte dispozitive sunt blocate.

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

Prin contrast, filtrarea în modul **Forbid only (Doar interzicere)** presupune blocarea manuală a fiecărui dispozitiv nedorit în parte, ceea ce devine rapid impracticabil: 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.
1. Navigați către **Wireless** > **Access Control (Control acces).**

2. 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**.

3. Apoi de la meniul derulant **SSID** selectați rețeaua Wi-Fi corespunzătoare. De exemplu se va selecta SSID-ul ***IP-COM_235860***.

4. Activați funcția **Access Control (Control acces)**.

5. De la **Mode (Mod)** selectați **Permit only (Doar permitere)**.

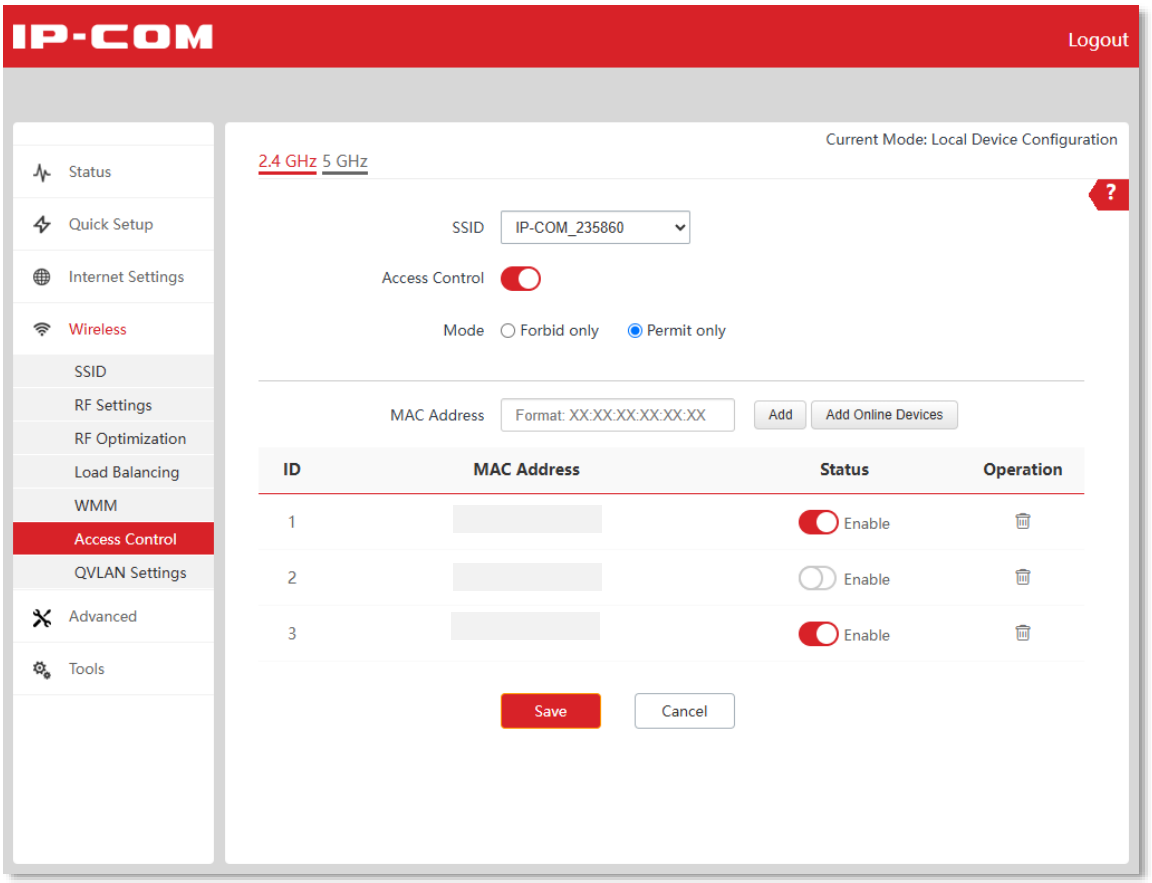
6. La câmpul **MAC Address (Adresă MAC)** introduceți identificatorul MAC al adaptorului de rețea al unui dispozitiv client. Apoi faceți clic pe butonul **Add (Adăugare)**. Doar dispozitivul cu adresa MAC adăugată în lista de mai jos va avea acces la rețea prin conectarea la SSID-ul ***IP-COM_235860.***

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.

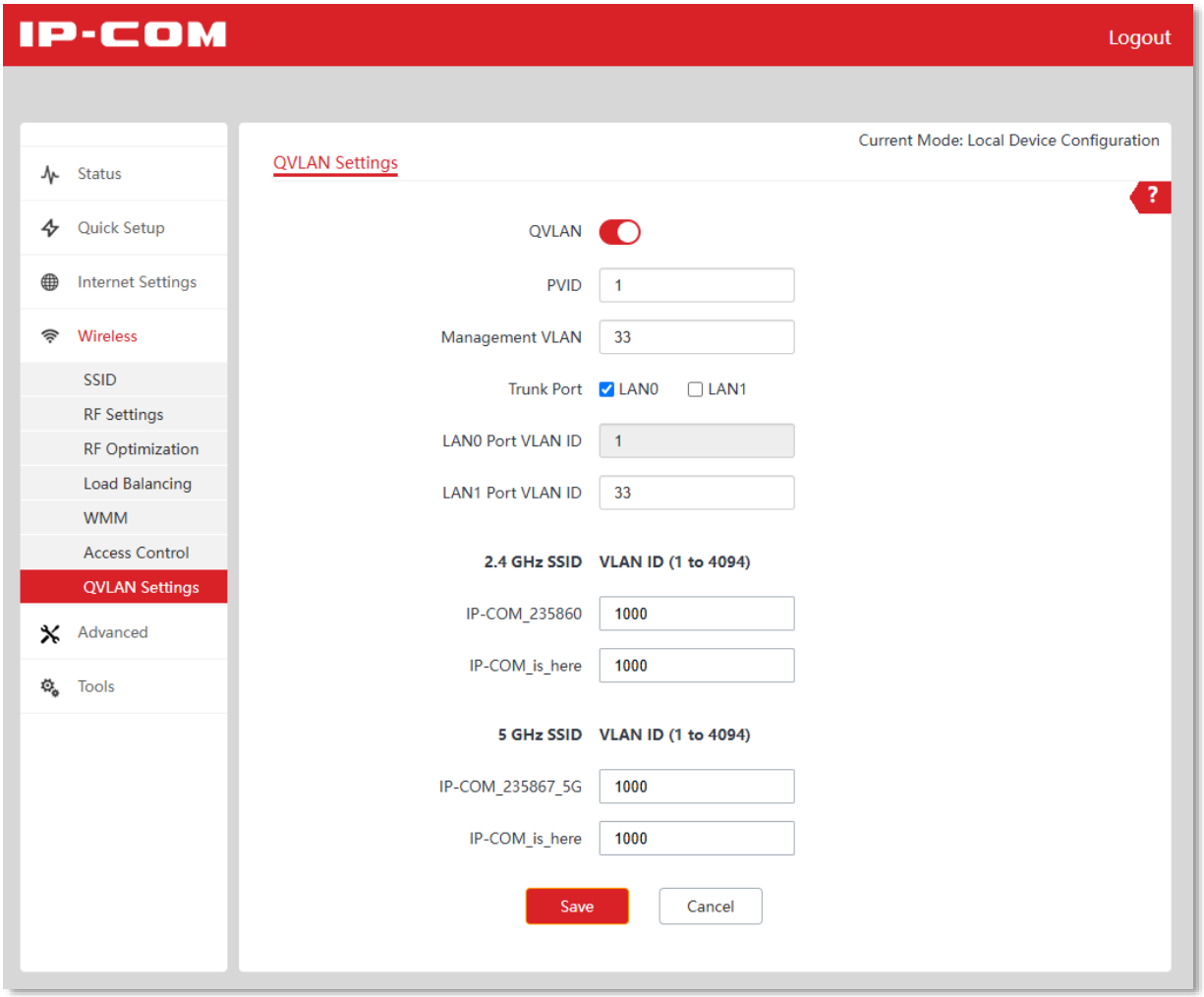
7. Faceți clic pe **Save (Salvare).**



---Sfârșit

6.7 Submeniul QVLAN Settings (Setări QVLAN)

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 și încă două pe 5 GHz.



Descriere parametri Wireless > QVLAN Settings (Setări QVLAN)

Parametru	Descriere
QVLAN	Utilizată pentru activarea sau dezactivarea funcției VLAN a echipamentului. Această funcție permite echipamentului să colaboreze cu switch-uri care acceptă VLAN-uri, în vederea creării mai multor rețele virtuale (VLAN-uri). Clienții conectați la VLAN-uri cu identificatori (VLAN ID) diferiți nu pot comunica între ei.
PVID	Specifică ID-ul VLAN-ului nativ implicit al portului trunk al punctului de acces. E identificatorul VLAN implicit asociat traficului fără etichetă (untagged). 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.

Parametru	Descriere
Management VLAN (VLAN de gestionare)	Identificatorul VLAN-ului de management al echipamentului. Valoarea implicită este **1**. După modificarea VLAN-ului de management, veți putea administra echipamentul doar după conectarea calculatorului dumneavoastră la noul VLAN de management.
Trunk Port **(Port trunk)**	Cele două porturi Ethernet (marcate **LAN0**, **LAN1**) configurate, prin bifare, să transporte traficul mai multor rețele VLAN. Portul trunk implicit este **LAN0.** Unele modele au un singur port Ethernet marcat **LAN0** sau **LAN**.
LAN0 Port VLAN ID **(ID VLAN port LAN0)** și **LAN1 Port VLAN ID** **(ID VLAN port LAN1)**	Identificatorul VLAN-ului căruia îi aparține portul **LAN0**, dar și celuilalt port Ethernet **LAN1**. Valoarea implicită este **1**. Se poate seta VLAN ID cu valori de la **1** la **4094**. Unele modele au un singur port Ethernet marcat **LAN0** sau **LAN**.
2.4 GHz SSID și **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 activ. Așadar, aici puteți eticheta fiecare rețea Wi-Fi cu un VLAN. Tip 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. ID-urile VLAN pot fi între **1-4094**. ID-ul implicit e **1000**.

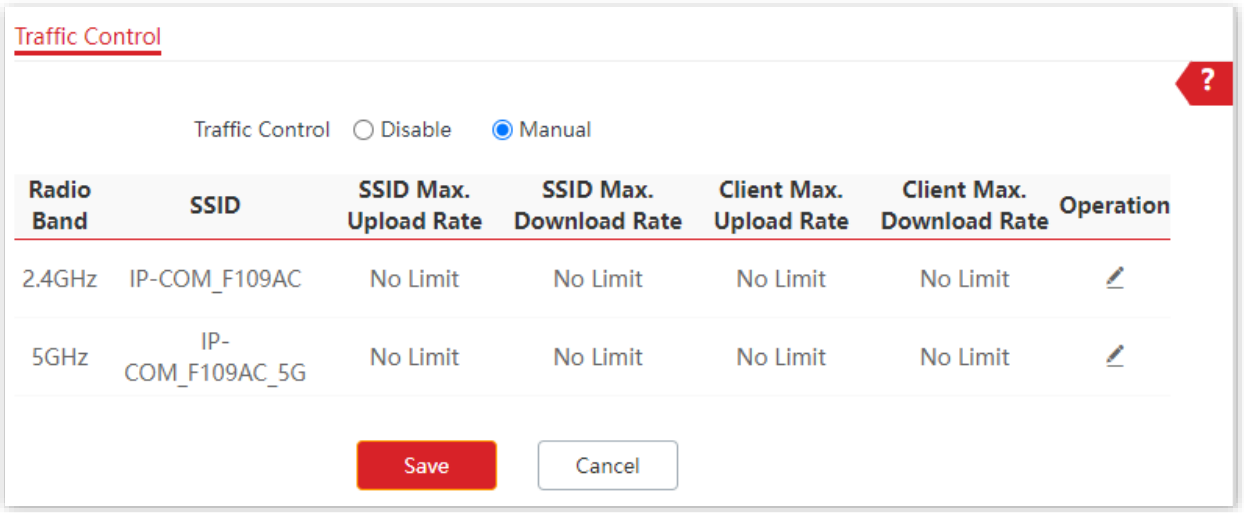
7 Meniul Advanced (Avansat)

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.

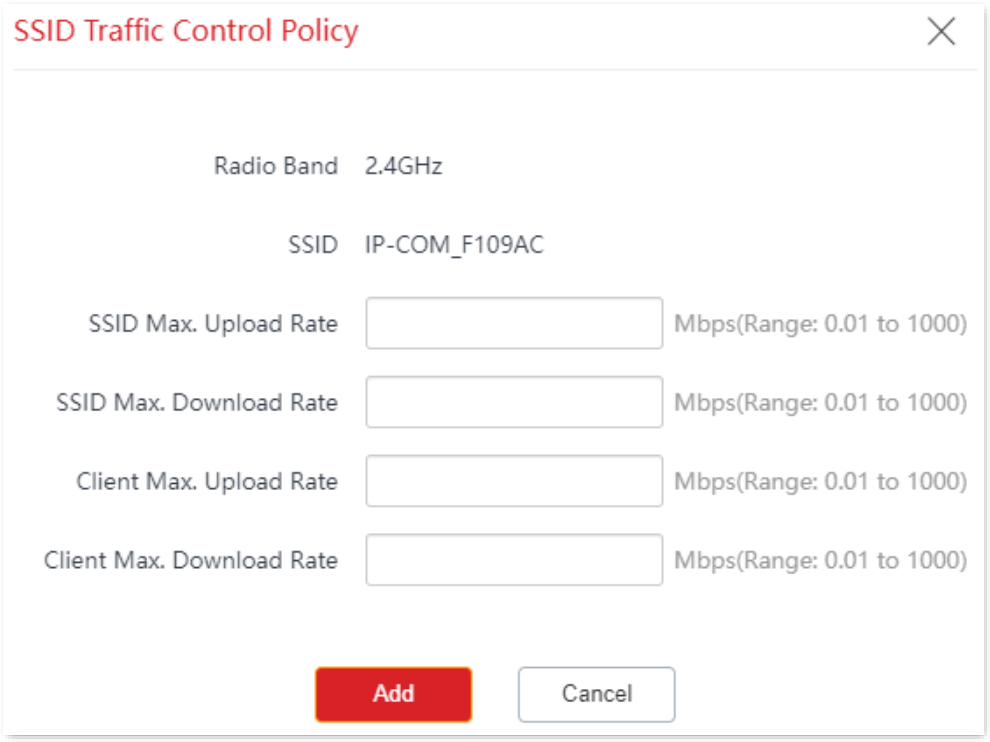
7.1 Submeniul Traffic Control (Control trafic)

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 **(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 **(Bandă radio)**	Coloana care indică banda Wi-Fi pentru SSID-ul din tabel.
SSID	Afișează numele rețelei Wi-Fi activate din meniul **Wireless > SSID**. 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**.
SSID Max. Upload Rate **(Rată maximă încărcare per SSID)** și **SSID Max. Download Rate** **(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. Dacă aceste câmpuri sunt lăsate necompletate, traficul de încărcare și descărcare al rețelei wireless nu va fi limitat în niciun fel. 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.

Parametru	Descriere
Client Max. Upload Rate **(Rată maximă încărcare per client)** și **Client Max. Download Rate** **(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. 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. Dacă aceste câmpuri sunt lăsate necompletate, viteza de încărcare și descărcare a fiecărui dispozitiv conectat la SSID-ul respectiv nu va fi limitată. Parametrii sunt disponibili pentru configurare numai atunci când funcția **Traffic Control (Control trafic)** este setată în mod **Manual**.
Operation **(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. Se va deschide o nouă fereastră denumită **SSID Traffic Control Policy (Politică control trafic SSID)**. 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)**. Toate cele patru câmpuri acceptă valori exprimate în **Mbps**, în intervalul **0,01 – 1000 Mbps**. Pentru salvarea limitărilor apăsați butonul **Add (Adăugare)**. Parametrii sunt disponibili pentru configurare numai atunci când funcția **Traffic Control (Control trafic)** este setată în mod **Manual**.
Save **(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 **(Anulare)**	Anulați modificările dacă nu ați apăsat încă **Save (Salvare)**.

7.2 Submeniul Cloud Maintenance (Mentenanță cloud)

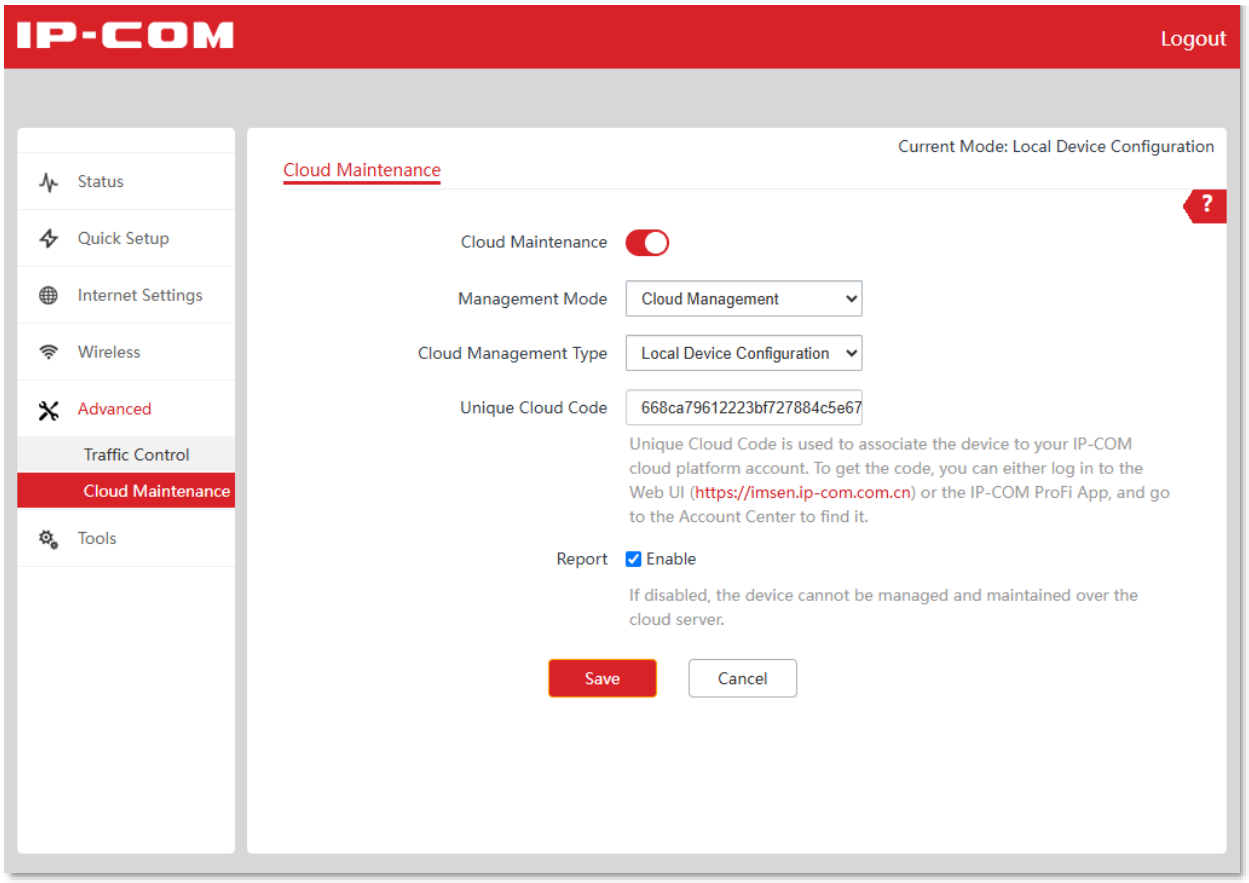
7.2.1 Prezentare generală

Meniul **Advanced (Avansat) > Cloud Maintenance (Mentenanță cloud)** vă permite să configurați modul în care echipamentul este administrat și întreținut de la distanță, prin intermediul unui

sistem de management centralizat. Activând funcția de întreținere în cloud, puteți integra punctul de acces într-o infrastructură gestionată unitar, fără a fi necesară configurarea manuală, individuală, a fiecărui echipament.

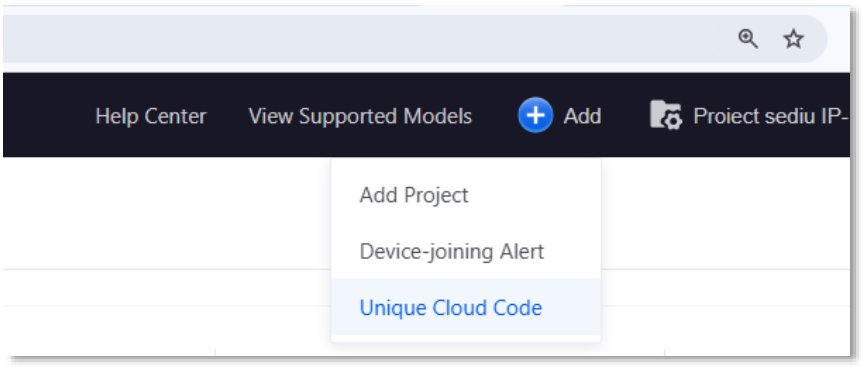
Pagina oferă trei abordări principale de management centralizat al echipamentului: fie prin intermediul unui ruter multi-WAN seria **M** cu control de AP-uri de la IP-COM, fie cu un controler software instalat într-o rețea externă sau locală precum **IP-COM ProFi Software Controller**, fie din cloud prin intermediul serviciului gratuit **IP-COM ProFi Cloud**.

Indiferent de modul ales, administrarea centralizată simplifică semnificativ gestionarea rețelelor cu mai multe puncte de acces, permițând configurarea, monitorizarea și actualizarea AP-ului împreună cu alte AP-uri dintr-un singur punct de control.



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

Parametru	Descriere
Cloud Maintenance (Mentenanță cloud)	Se specifică dacă se activează funcția de mentenanță din cloud prin **IP-COM ProFi Cloud** sau prin controler software precum **IP-COM ProFi Software Controller,** dar și alte moduri.

Parametru	Descriere
Management Mode **(Mod gestionare)**	Specifică modurile în care este gestionat punctul de acces, astfel: – **Cloud Management (Gestionare cloud):** Aplicabil scenariilor care necesită configurare și întreținere unificate prin serviciul cloud **IP-COM ProFi Cloud**. – **Soft AC across Internet (Soft AC prin internet):** Acest mod este utilizat pentru administrarea centralizată a AP-ului prin intermediul controlerului software **IP-COM ProFi Software Controller** (precurtat în interfață **Soft AC**), prin internet. În acest mod, toate configurările echipamentului sunt transmise de la controler.
Cloud Management Type **(Tip gestionare cloud)**	Acest câmp e afișat dacă e selectat **Cloud Management (Gestionare cloud)** de la meniul de mai sus **Management Mode (Mod gestionare)**. Permite specificarea modului în care este gestionat punctul de acces, astfel: – **Cloud Management (Gestionare cloud):** 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. Asigurați-vă că setările IP, pentru o comunicare corectă pe internet a AP-ului, sunt corect setate la meniul **Internet Settings (Setări internet)**. – **Local Device Configuration (Gestionare locală):** În acest mod, toate configurațiile dispozitivului sunt făcute din propria interfață web, iar informațiile sunt doar raportate către platforma cloud **IP-COM ProFi**. Această opțiune este selectată și dacă AP-ul este gestionat unificat printr-un ruter multi-WAN seria **M** de la IP-COM.
Unique Cloud Code **(Cod cloud unic)**	Acest câmp e afișat dacă e selectat **Cloud Management (Gestionare cloud)** de la meniul de mai sus **Management Mode (Mod gestionare)**. 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)**. 

Parametru	Descriere
Report (Raportare)	Acest câmp e afișat dacă e selectat **Cloud Management (Gestionare cloud)** de la meniul de mai sus **Management Mode (Mod gestionare)**. Activează sau dezactivează funcția de raportare a punctului de acces către platforma cloud de gestionare unificată **IP-COM ProFi Cloud**. 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. Asigurați-vă că setările IP, pentru o comunicare corectă pe internet a AP-ului, sunt corect setate la meniul **Internet Settings (Setări internet)**.
Connection Type (Tip conexiune) și **Soft AC Address (Adresă Soft AC)**	Acest câmp e afișat dacă e selectat **Soft AC across Internet (Soft AC prin internet)** de la meniul de mai sus **Management Mode (Mod gestionare).** Sunt două opțiuni: – **By Domain Name (Nume domeniu):** Dacă se selectează această opțiune atunci se va completa la câmpul de mai jos **Soft AC Address (Adresă Soft AC)** numele de domeniu unde se află controlerul software **IP-COM ProFi Software Controller**. – **By IP Address (Adresă IP):** Dacă se selectează această opțiune atunci se va completa la câmpul de mai jos **Soft AC Address (Adresă Soft AC)** adresa IP externă unde se află controlerul software **IP-COM ProFi Software Controller**. Indiferent de opțiunea selectată asigurați-vă că setările IP, pentru o comunicare corectă pe internet a AP-ului, sunt corect setate la meniul **Internet Settings (Setări internet)**.
Save (Salvare)	Apăsați acest buton pentru salvarea modificărilor și așteptați aplicarea setărilor.
Cancel (Anulare)	Anulați modificările făcute, însă, înainte de apăsarea butonului **Save (Salvare)**.

7.2.2 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)**.

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.

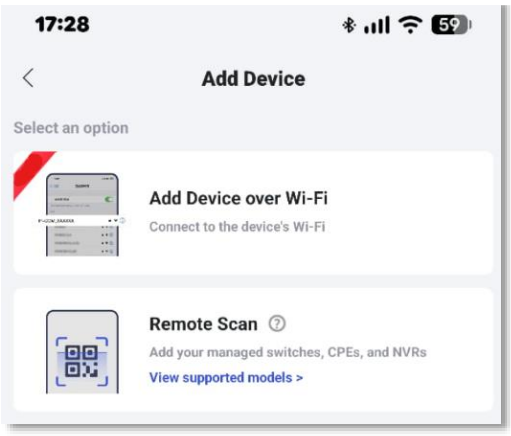
IP-COM ProFi

2. Conectați-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.

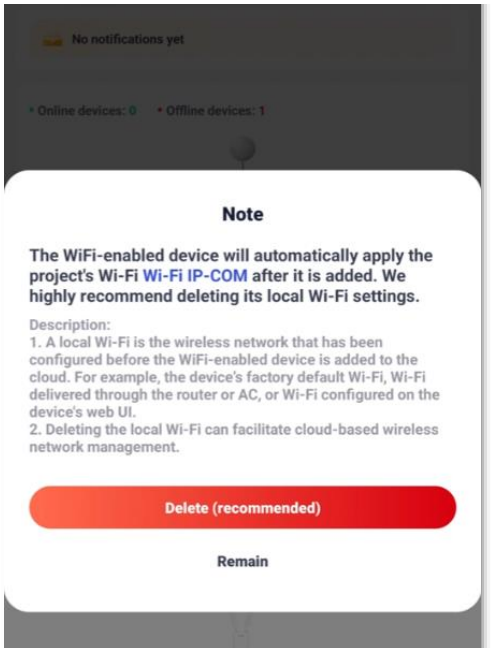
4. Deschideți aplicația **IP-COM ProFi**.
5. Alegeți un proiect existent sau creați unul nou apăsând butonul de jos-dreapta.
6. Apoi, atingeți fereastra pop-up care arată că AP-ul este detectat.
7. Bifați **Agree to enable Cloud Management, and activate report function of the device (De acord cu activarea funcției Gestionare cloud și a funcției de raportare a echipamentului)**.
8. Apoi apăsați butonul **Add to Project (Adăugare la proiect)**. Dacă fereastra pop-up nu apare, atingeți butonul din sus-dreapta și urmați instrucțiunile din fereastra **Add Device (Adăugare dispozitiv)**.
9. 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.



10. 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.



11. Confirmați adoptarea în cloud.

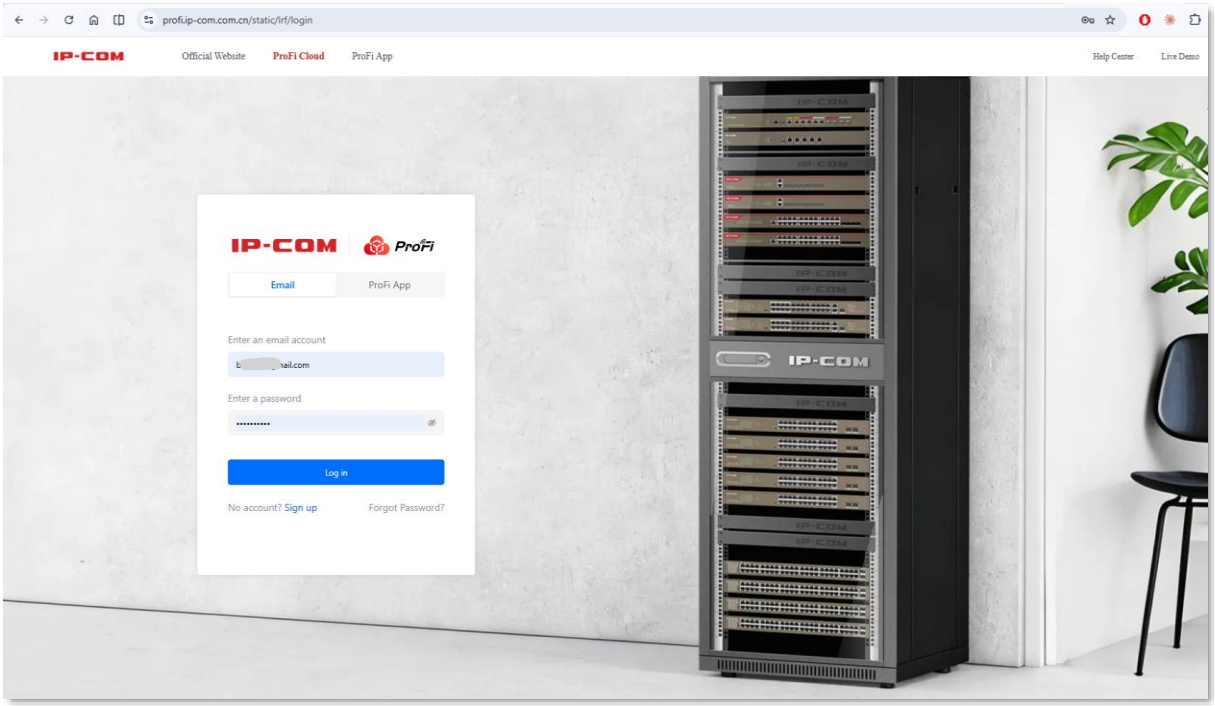
12. Apoi, după câteva momente, o să vedeți echipamentul în proiectul adăugat, fie din **aplicația IP-COM ProFi**, de Android și iOS, fie din pagina web https://imsen.ip-com.com.cn.

    ---Sfârșit

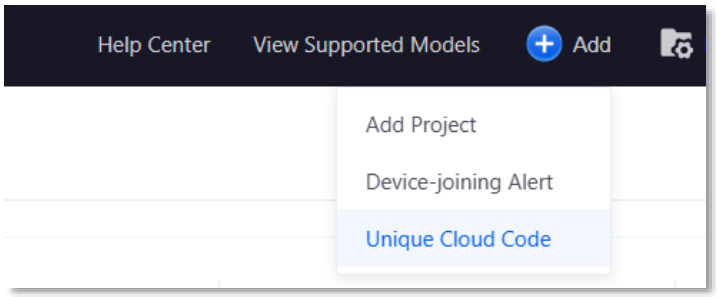
Metoda 2: Adăugare în cloud, din interfața locală web a AP-ului, copiind codul unic de cloud

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.

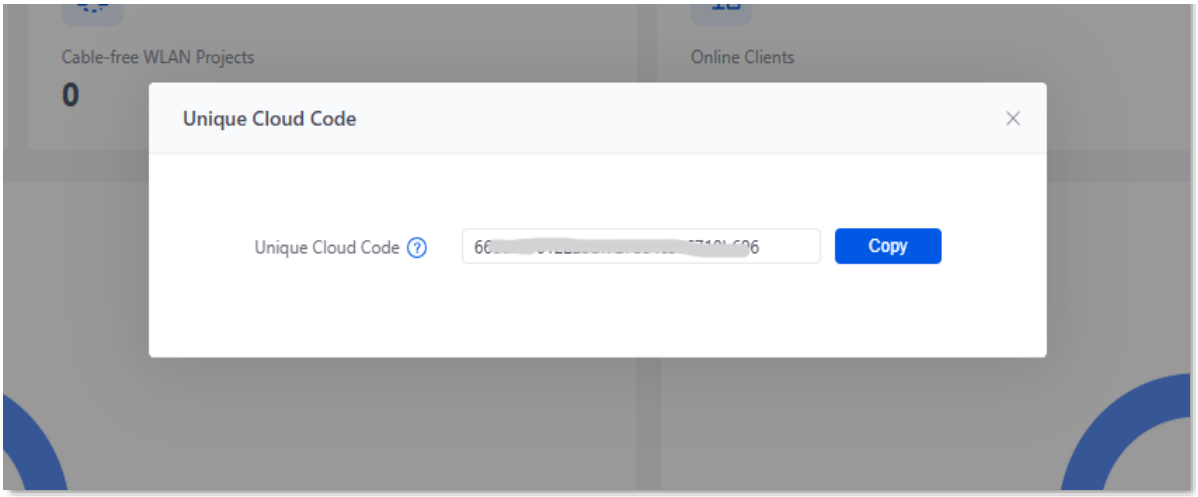
2. Autentificați-vă cu contul dumneavoastră de **IP-COM ProFi Cloud**, folosind adresa de email și parola, apoi apăsați **Login (Autentificare)**. Se consideră că deja v-ați creat un cont apăsând **Sign up (Înregistrare)**.



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

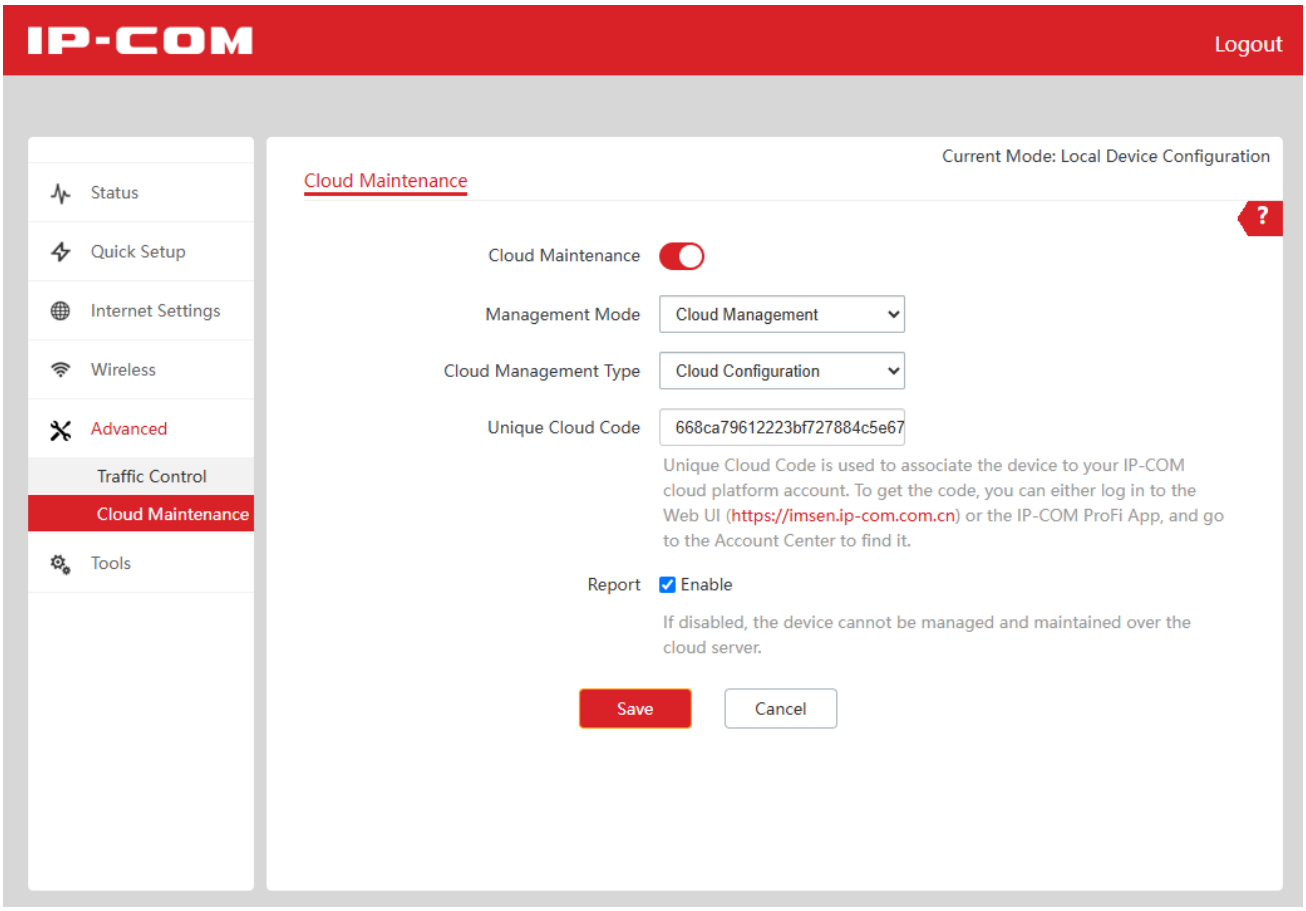


4. Copiați codul apăsând **Copy (Copiere)** în noua fereastră. Salvați codul pentru utilizarea ulterioară.



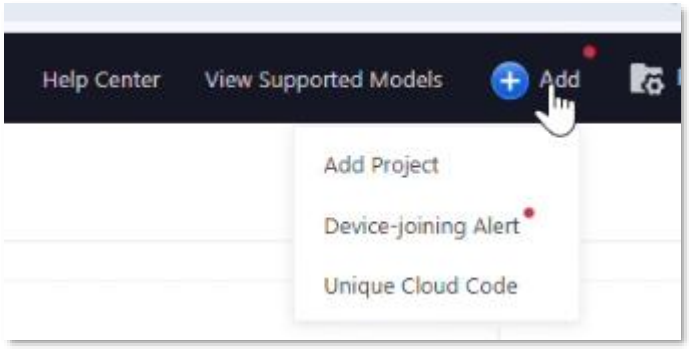
5. Acum accesați interfața web de gestionare a AP-ului. Așadar, conectați-vă la interfața web a punctului de acces. Se presupune că ați efectuat deja configurarea inițială pas cu pas a echipamentului.

6. Din interfața web de gestionare vă asigurați că echipamentul are acces la internet, verificând setările IP de la **Internet Settings (Setări internet)**.
7. Apoi, navigați la meniul **Advanced (Avansat)** > **Cloud Maintenance (Mentenanță cloud).**
8. De aici activați funcția **Cloud Maintenance (Mentenanță cloud).**
9. La **Management Mode (Mod gestionare)**, activați gestionarea din cloud selectând opțiunea **Cloud Management (Gestionare cloud)**.
10. Mai jos, la **Cloud Management Type (Tip gestionare cloud)** selectați **Cloud Configuration (Configurare cloud)**.
11. Lipiți codul copiat de la pasul **4**, la câmpul **Unique Cloud Code (Cod cloud unic)**.
12. Bifați funcția **Report (Raportare).**
13. Faceți clic pe **Save (Salvare)** și așteptați câteva momente.



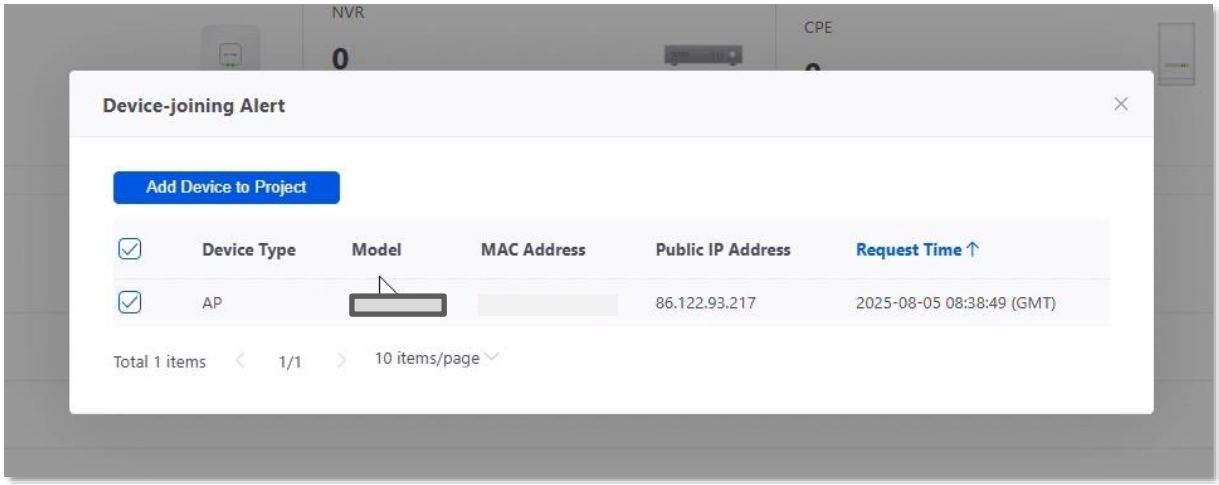
14. După 1-5 minute, reaccesați platforma web **IP-COM ProFi Cloud**, tastând în bara de adrese a unui browser: https://imsen.ip-com.com.cn.

15. 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. Dacă nu observați acest punct faceți o reîmprospătare (reîncărcare) a paginii web sau reautentificați-vă.

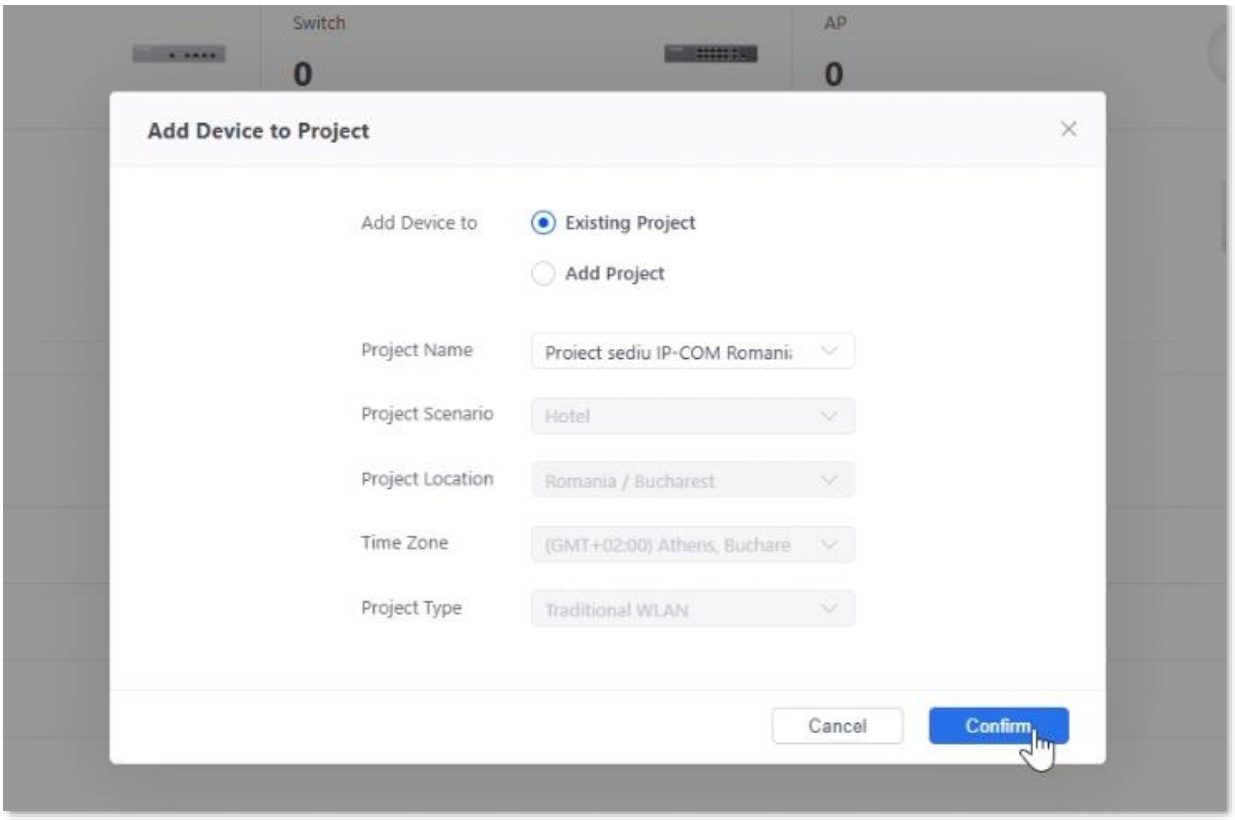
16. Apoi în noua fereastră **Device-joining Alert (Alertă asociere echipament)**, bifați AP-ul din listă și clic pe butonul **Add Device to Project (Adăugare dispozitiv la proiect)**.



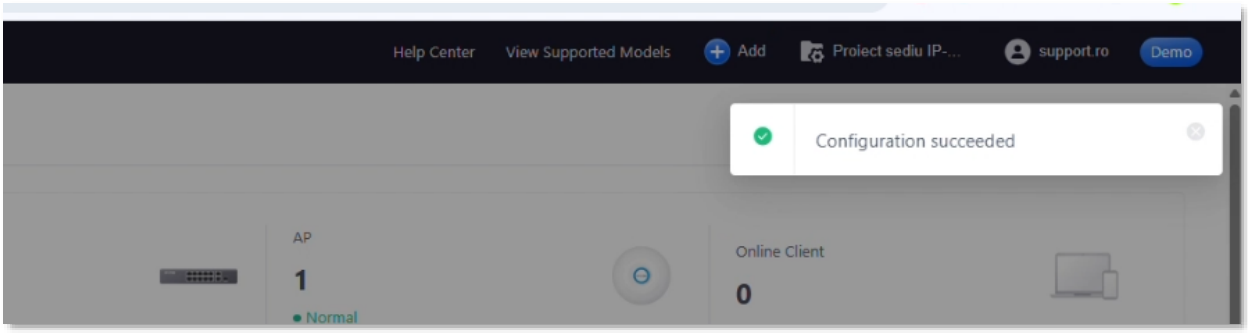
17. Acum trebuie să stabiliți la ce proiect adăugați AP-ul. Un proiect este pur și simplu un container logic în care grupați toate echipamentele de rețea dintr-o locație sau de la un beneficiar. E ca un „dosar” virtual în care puneți laolaltă switch-urile, AP-urile, ruterele și alte echipamente IP-COM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

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.

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



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



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

21. 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.

---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.

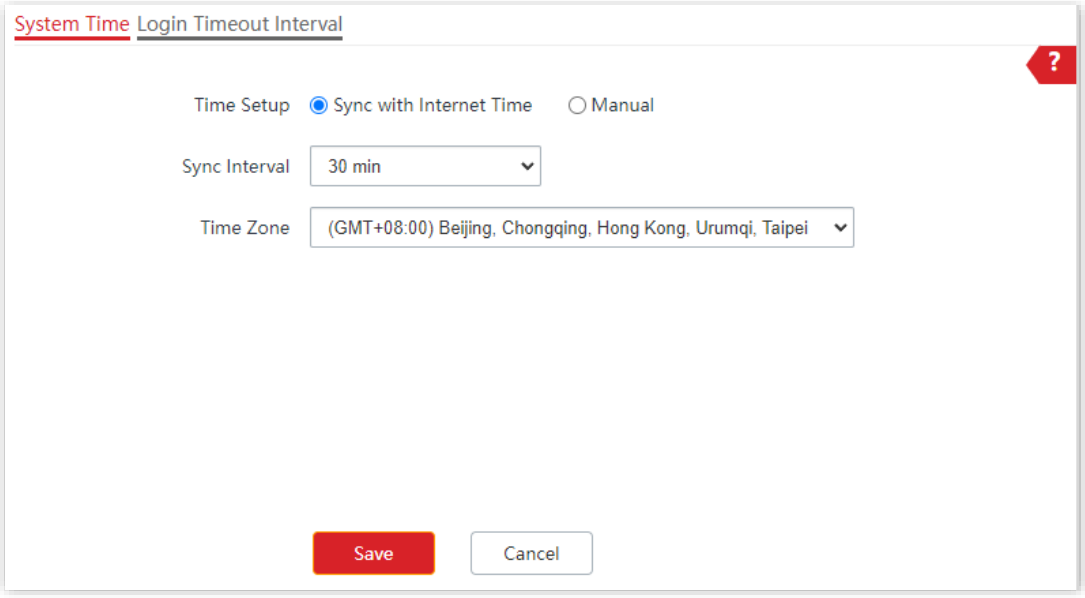
Tot din meniul **Tools (Instrumente) > Date & Time (Dată și oră)** se poate configura și intervalul după care utilizatorul este deconectat automat din interfața de gestionare, în urma unei perioade de inactivitate.

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.

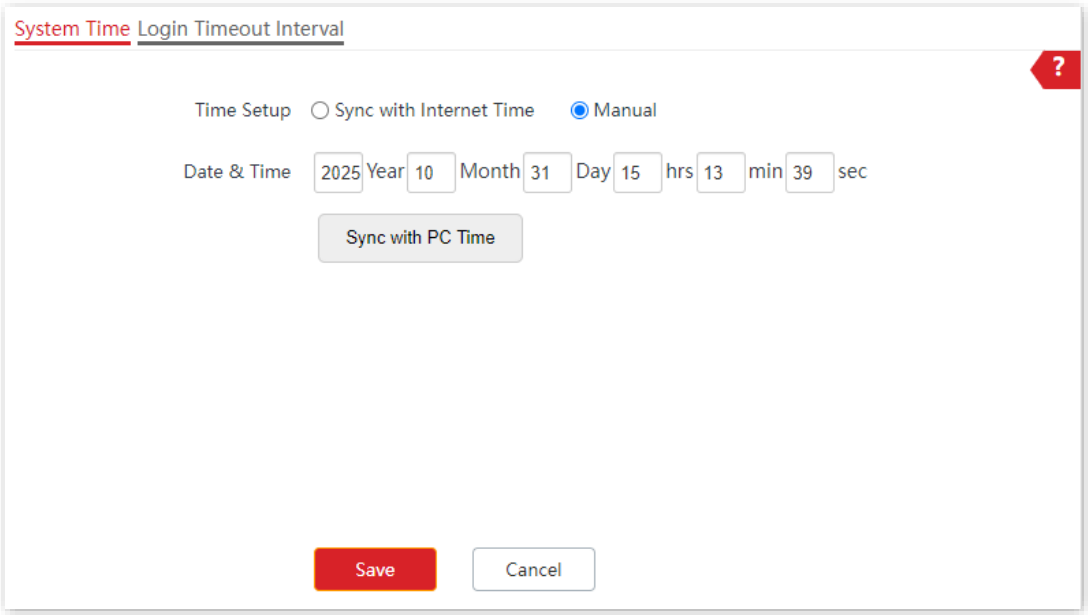
---Sfârșit

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

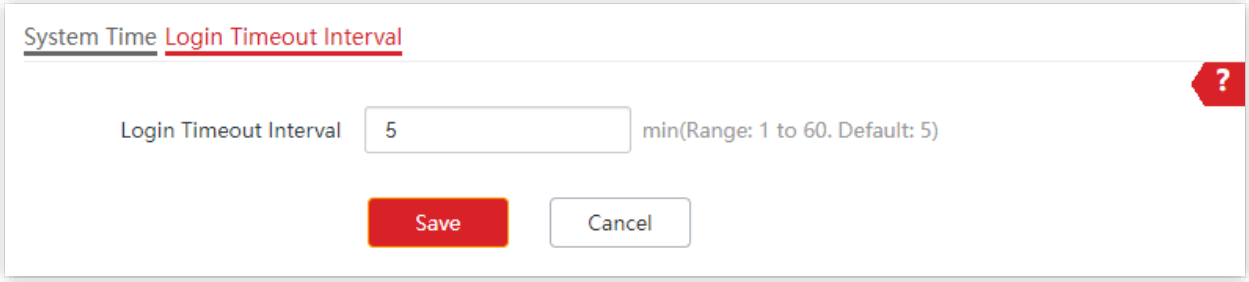
8.1.3 Deconectare automată de la interfața de gestionare după o perioadă de inactivitate

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)**.

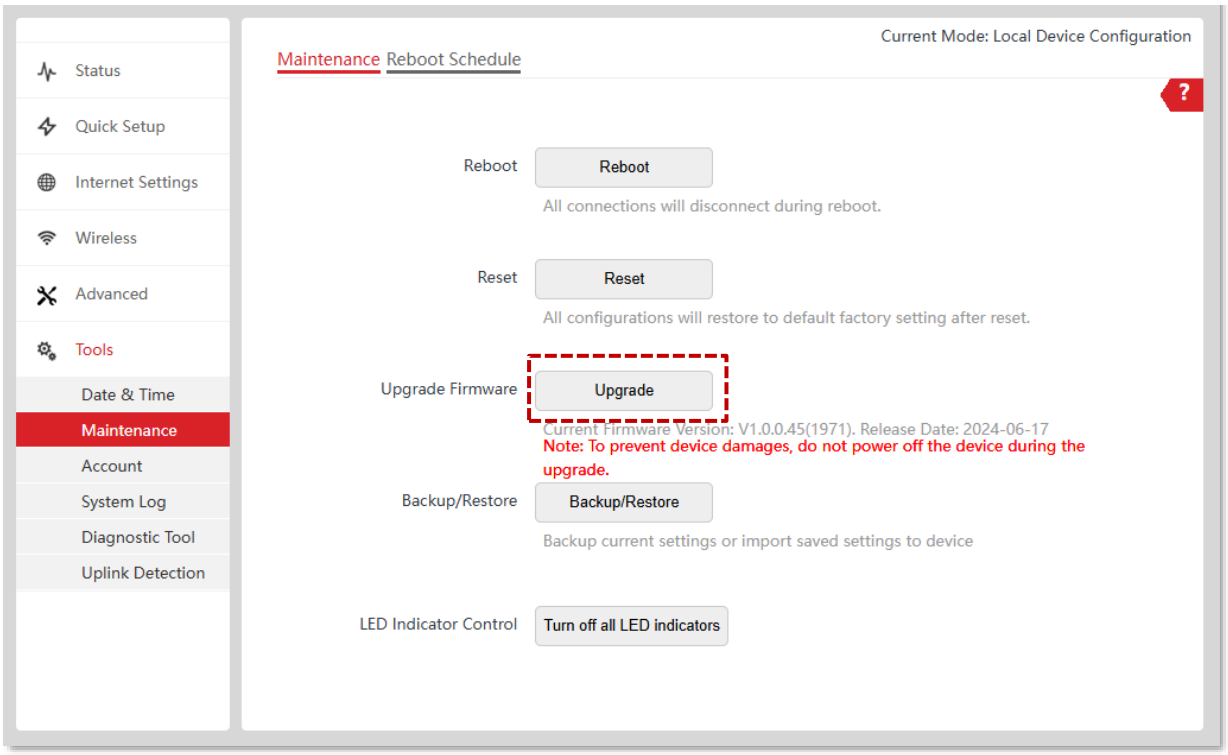


---Sfârșit

8.2 Submeniul Maintenance (Mentenanță)

8.2.1 Actualizare de firmware

Pentru actualizarea manuală de firmware a echipamentului accesați **Tools (Instrumente) > Maintenance (Mentenanță)** > fila **Maintenance (Mentenanță)**. Aici căutați butonul **Upgrade (Actualizare)** de la secțiunea **Upgrade Firmware (Actualizare firmware)**.



Procedură actualizare manuală de firmware

1. Conectați-vă la interfața web a punctului de acces.
2. Aflați versiunea hardware și de firmware a echipamentului, dar și modelul. Versiunea hardware și cea de firmware se află în meniul **Status (Stare) > System Status (Stare sistem)**, în câmpurile **Hardware Version (Versiune hardware)**, respectiv **Firmware Version (Versiune firmware)**. Modelul echipamentului este înscris pe etichetă, în dreptul câmpului **Model**.
3. Accesați pagina oficială IP-COM România https://www.ip-com.com.cn/ro și căutați ultima versiune de firmware ținând cont de model și versiunea hardware a echipamentului.
4. Descărcați fișierul și dezarhivați-l. Salvați fișierul de firmware cu terminația ***.bin*** pe computer.
5. Reconectați-vă la interfața web a punctului de acces.
6. Navigați la **Tools (Instrumente)** > **Maintenance (Mentenanță)** > fila **Maintenance (Mentenanță)**.
7. Apăsați butonul **Upgrade (Actualizare)**.

8. Apoi navigați pe computer după fișierul de firmware, cu terminația ***.bin***. Selectați-l și apăsați **Open (Deschidere)**.

9. Confirmați și așteptați instalarea noului firmware. Echipamentul va reporni. În unele cazuri e recomandată și o resetare a echipamentului la setările din fabrică și reconfigurarea acestuia pas cu pas. Resetarea se face apăsând butonul **Reset** tot din acest meniu, **Tools (Instrumente)** > **Maintenance (Mentenanță)** > fila **Maintenance (Mentenanță)**.

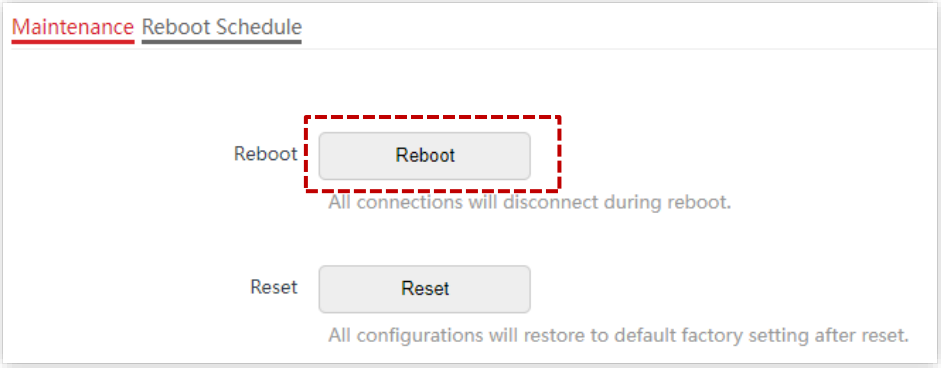
---Sfârșit

8.2.2 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.
2. Navigați la **Tools (Instrumente)** > **Maintenance (Mentenanță)** > fila **Maintenance (Mentenanță)**.
3. Faceți clic pe **Reboot (Repornire)**.



4. Un dialog va fi afișat, confirmați informațiile din solicitare și faceți clic pe **OK.**

---Sfârșit

8.2.3 Repornire periodică automată

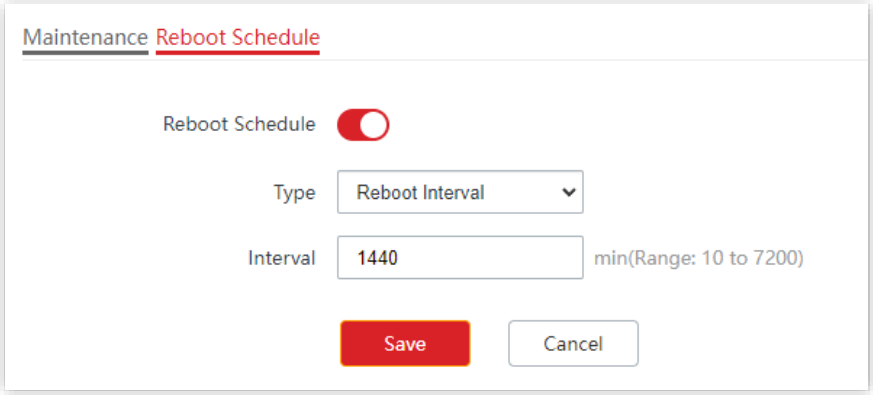
Această funcționalitate permite punctului de acces să repornească automat conform unui orar setat sau la un anumit interval de timp. Puteți utiliza această funcție pentru a preveni anumite tipuri de blocaje care pot apărea după o perioadă lungă de funcționare a punctului de acces în medii extreme de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

8.2.3.1 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 – 7200 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

8.2.3.2 Repornire periodică pe baza unui orar

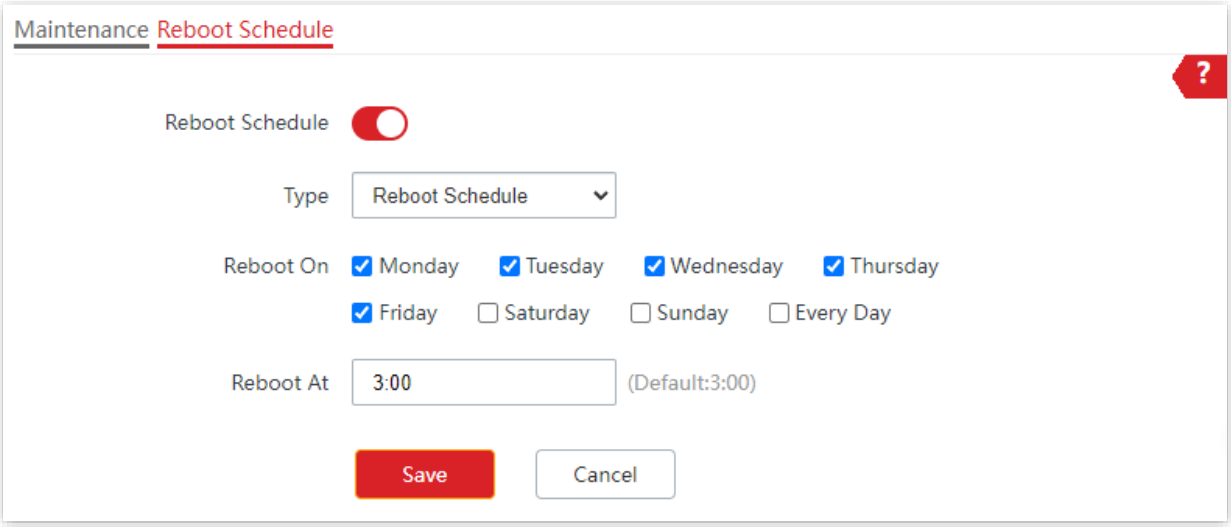
Tip

Repornirea la ora specificată se bazează pe ora AP-ului. Pentru a evita erorile de repornire, asigurați-vă că data și ora e setată 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

8.2.4 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.

8.2.4.1 Resetare folosind butonul fizic de pe echipament

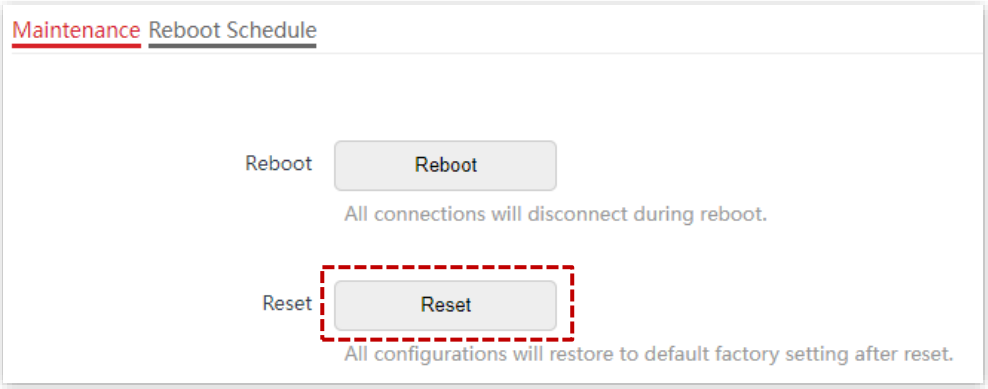
Când punctul de acces este alimentat, țineți apăsat butonul fizic marcat **RESET** timp de aproximativ 8-25 secunde.

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

8.2.4.2 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

8.2.5 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.

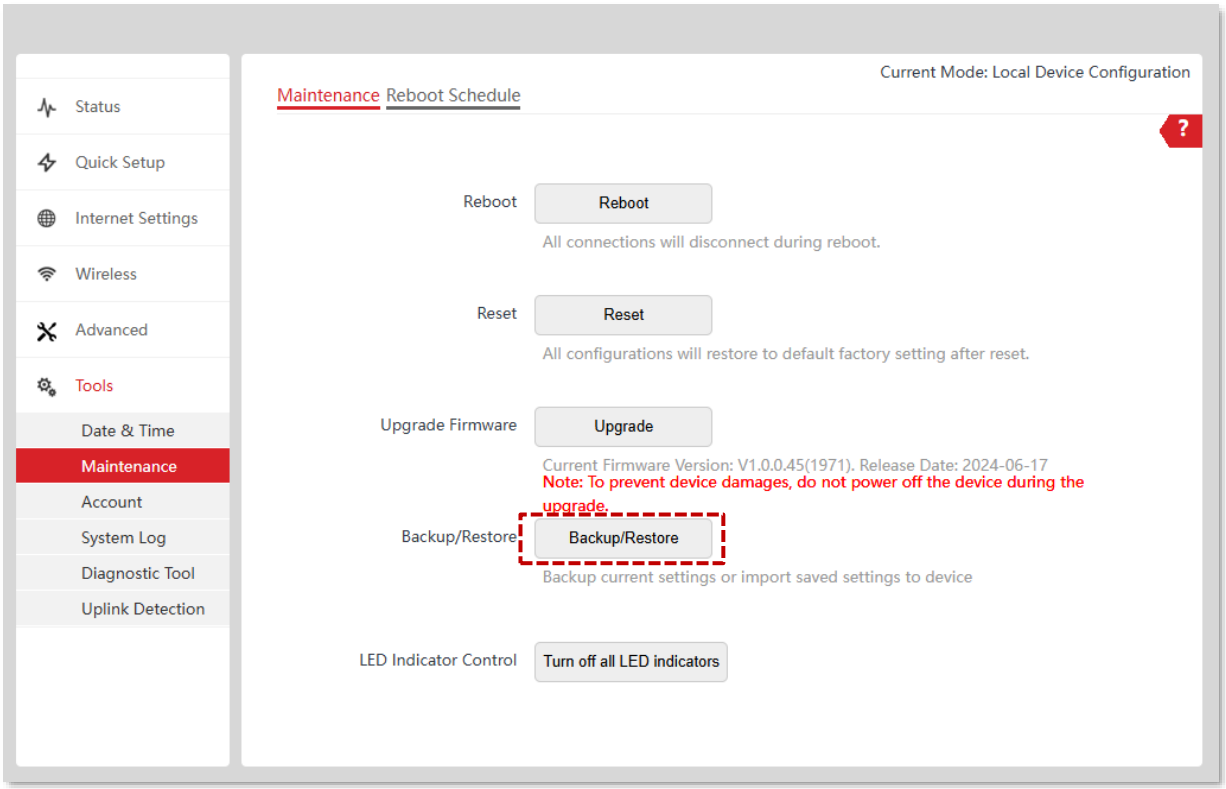
În cazul în care, după modificări semnificative ale configurației, punctul de acces ajunge la o stare de funcționare optimă, vă recomandăm să realizați o copie de rezervă a noii configurații. Astfel, o veți putea restaura cu ușurință după o actualizare sau o resetare a AP-ului.

Tip

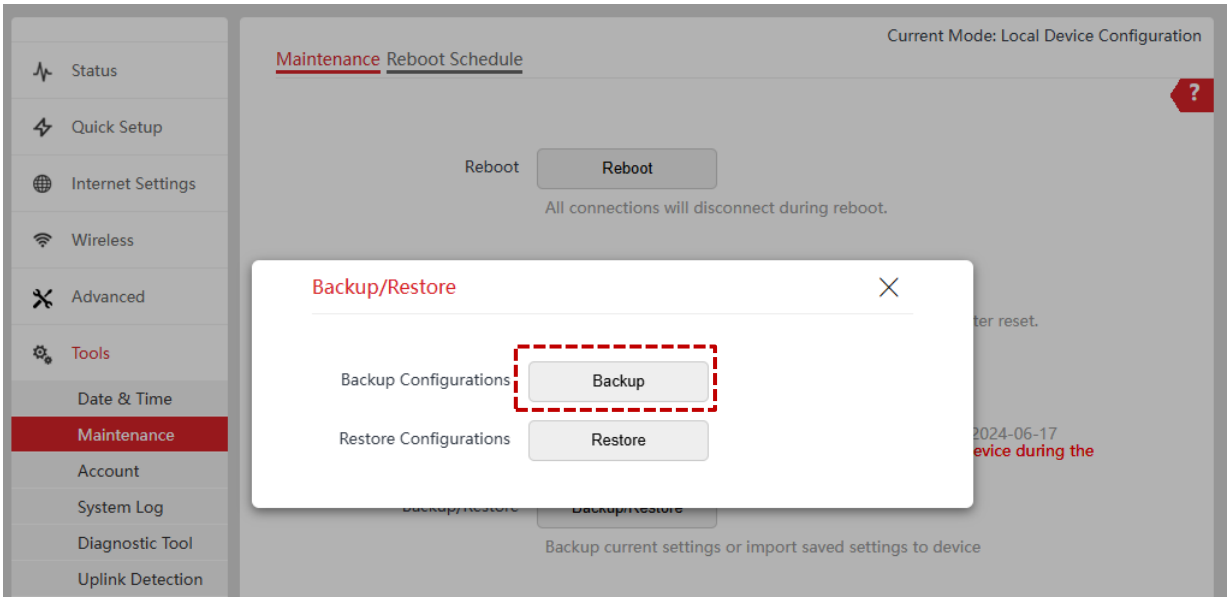
Dacă trebuie să aplicați configurații identice sau similare pe mai multe puncte de acces, este suficient să configurați un singur AP, să creați o copie de rezervă a configurației acestuia și să o utilizați pentru a replica setările pe celelalte echipamente. În acest fel, timpul necesar implementării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

8.2.5.1 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 criptat conține setările echipamentului salvate până la momentul apăsării butonului **Backup (Copie de rezervă)**.

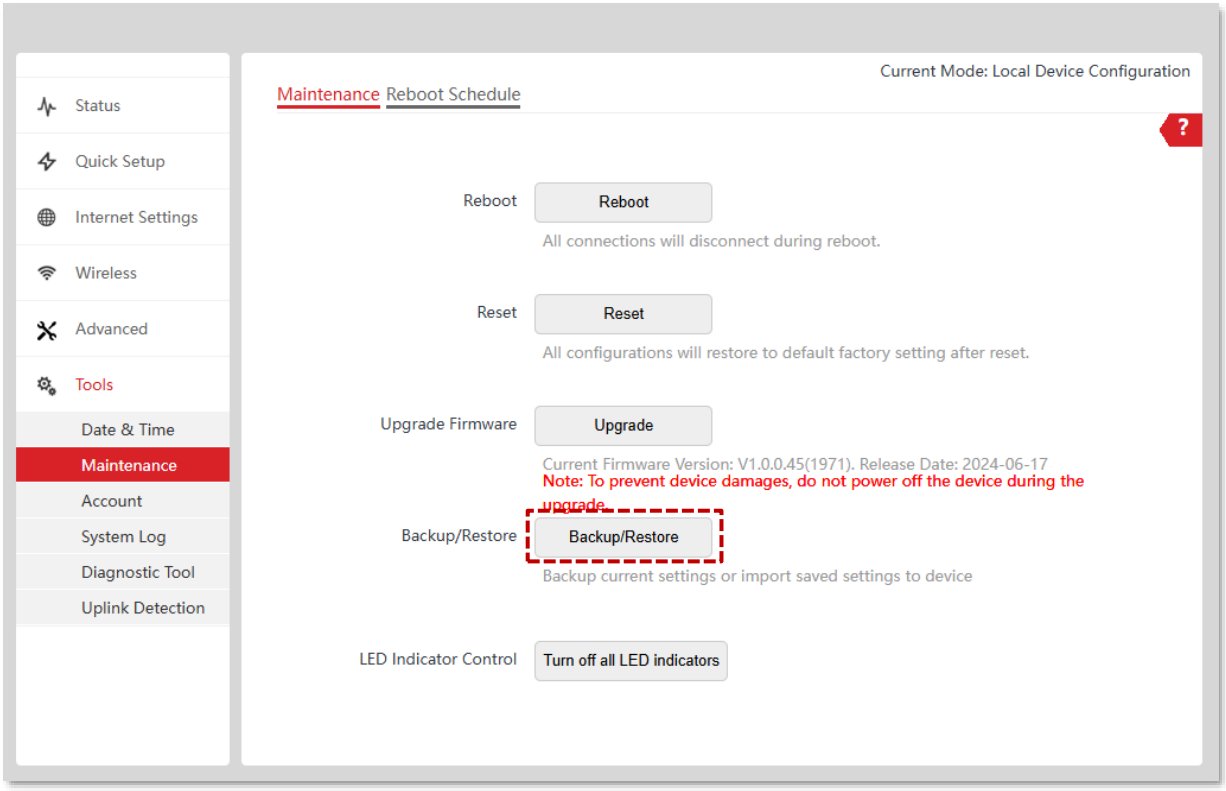
---Sfârșit

Tip

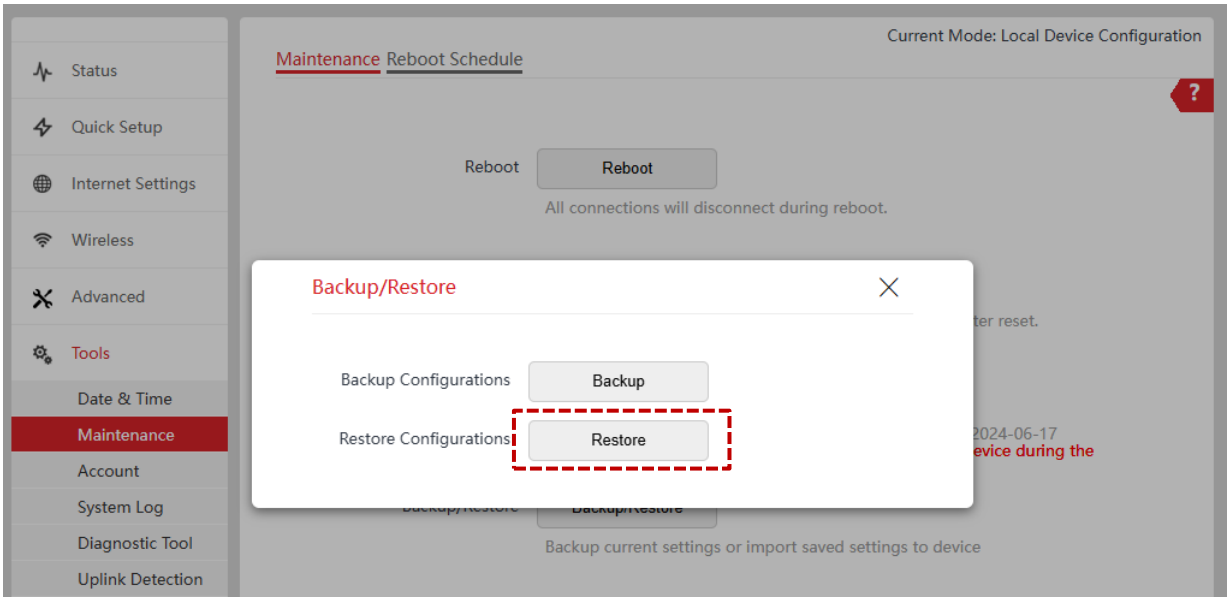
Dacă în browser apare mesajul de avertizare ***Acest tip de fișier poate dăuna computerului. Doriți să păstrați APCfm.cfg oricum?***, faceți clic pe ***Păstrare***.

8.2.5.2 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).**

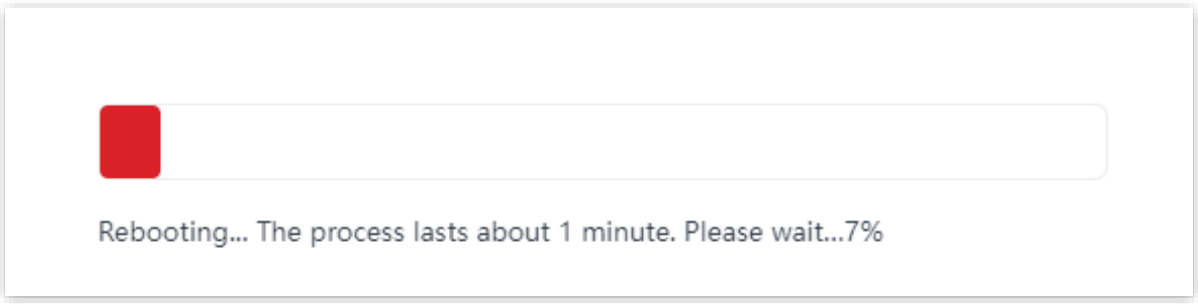


4. Faceți clic pe **Restore (Restaurare).**



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.

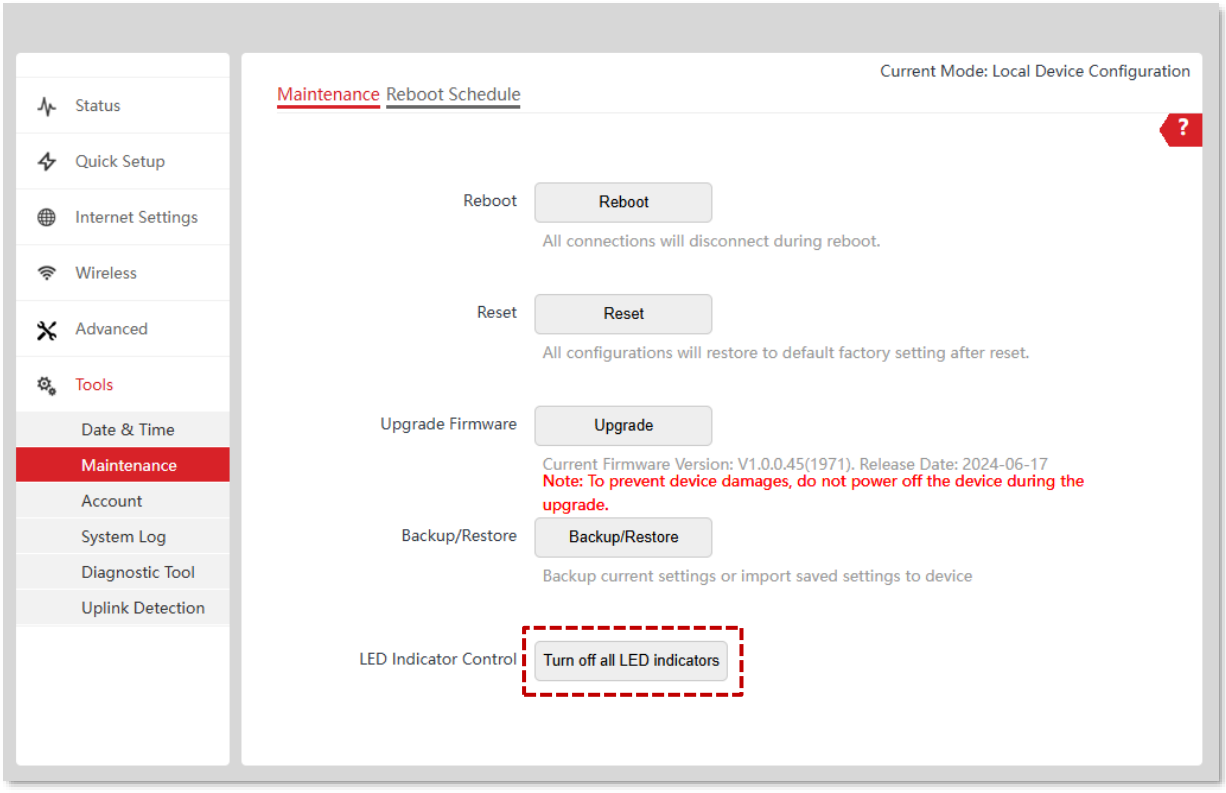


8.2.6 Control indicator led de pe echipament

8.2.6.1 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 (Dezactivați 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

8.2.6.2 Activare led

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 on all LED indicators (Activați toate ledurile indicatoare).**

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

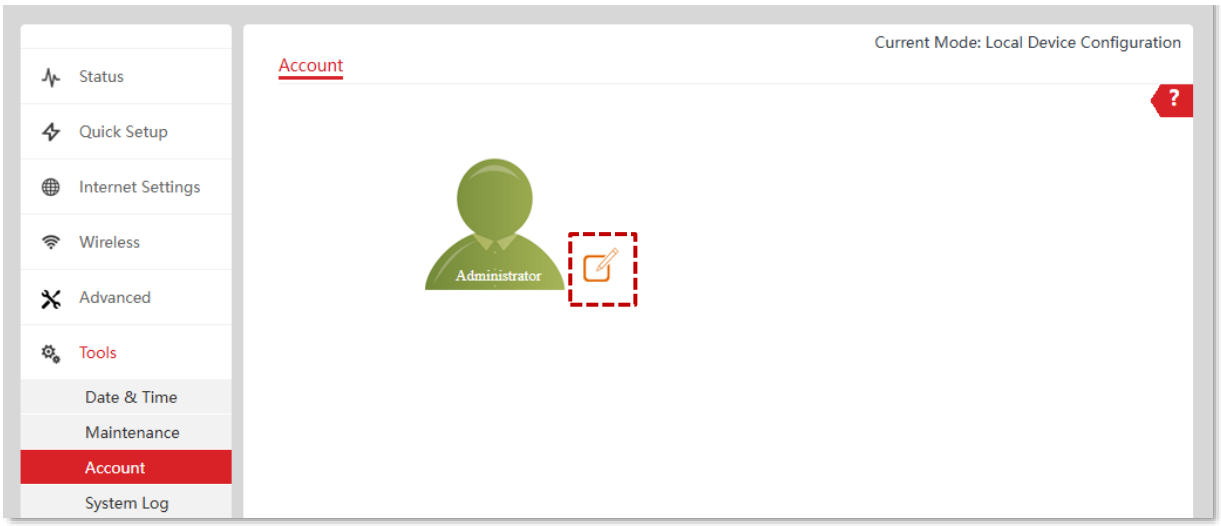
---Sfârșit

8.3 Submeniul Account (Cont)

Când vă conectați pentru prima dată la interfața web a punctului de acces, sistemul vă cere să setați un nume de utilizator și o parolă de autentificare la interfața de gestionare. Pașii sunt explicați în subcapitolul 1.3 Configurarea inițială din interfața locală web. Însă, ca bună practică, schimbați periodic parola interfeței web pe durata utilizării punctului de acces, pentru a menține un nivel de securitate constant din meniul **Tools (Instrumente)** > **Account (Cont)**.

Procedură pentru schimbarea utilizatorului și parolei de autentificare la sistem

1. Conectați-vă la interfața web a punctului de acces.
2. Navigați la **Tools (Instrumente)** > **Account (Cont).**



3. O să vedeți un singur cont de administrator, aici apăsați butonul de editare din dreapta jos. O nouă fereastră se va deschide.

4. Acum, în noua fereastră, în câmpul **Old User Name (Nume utilizator vechi)** este afișat numele de utilizator curent, în exemplul de față, ***admin2***.

5. Introduceți parola actuală cu care deja v-ați autentificat la interfață în câmpul **Old Password (Parolă veche)**.

6. Completați câmpul **New User Name (Nume utilizator nou)** cu noul nume de utilizator dorit în locul vechiului utilizator ***admin2***.

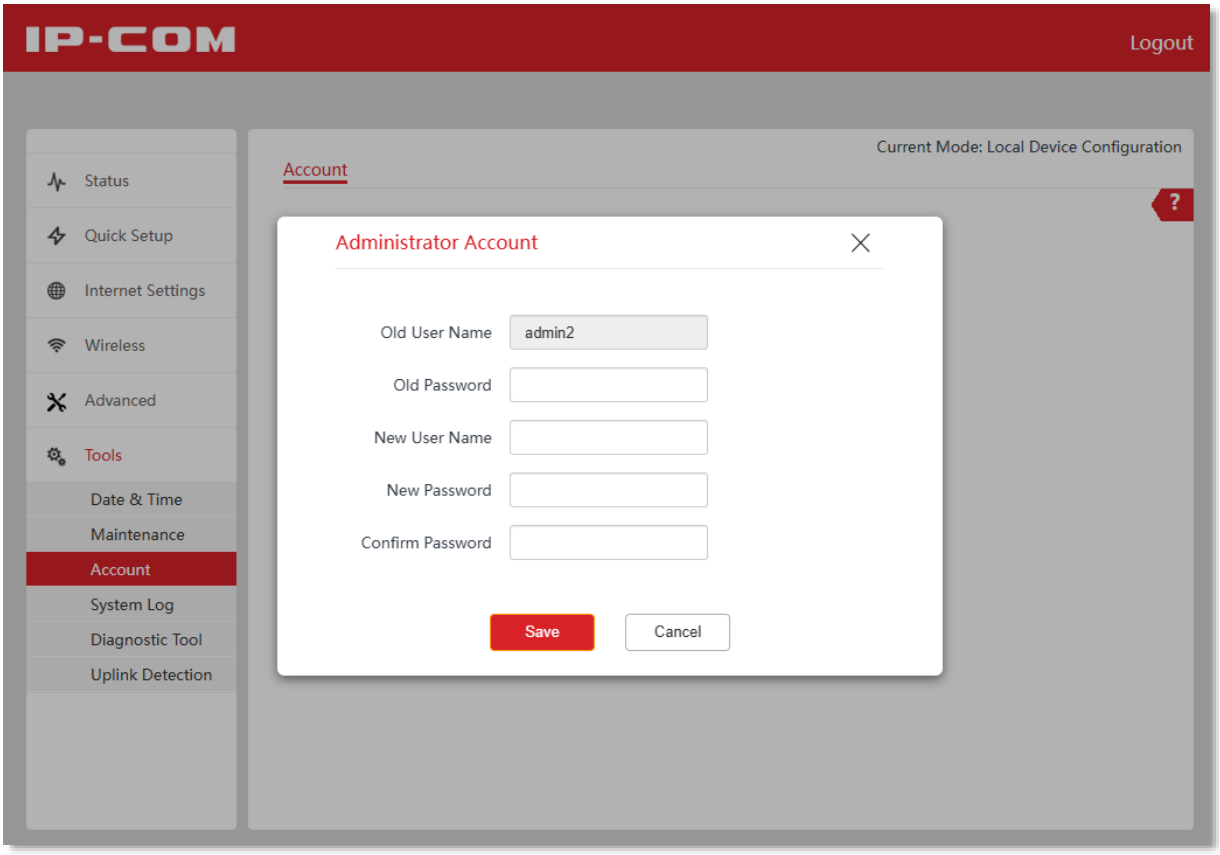
7. Introduceți noua parolă în **New Password (Parolă nouă).**

Note

La configurarea inițială sau după o resetare, definiți un nume de utilizator și o parolă noi de conectare, pentru a asigura confidențialitatea și securitatea accesului. Cu cât parola este mai lungă, cu atât nivelul de securitate este mai ridicat. Numărul maxim de caractere și regulile de compunere a parolei sunt afișate direct în interfața web. Parola poate conține litere mari, litere mici, cifre și liniuță de subliniere (_). Nu sunt permise alte caractere speciale.

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

9. Faceți clic pe **Save (Salvare).**



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

---Sfârșit

8.4 Submeniul System Log (Jurnal sistem)

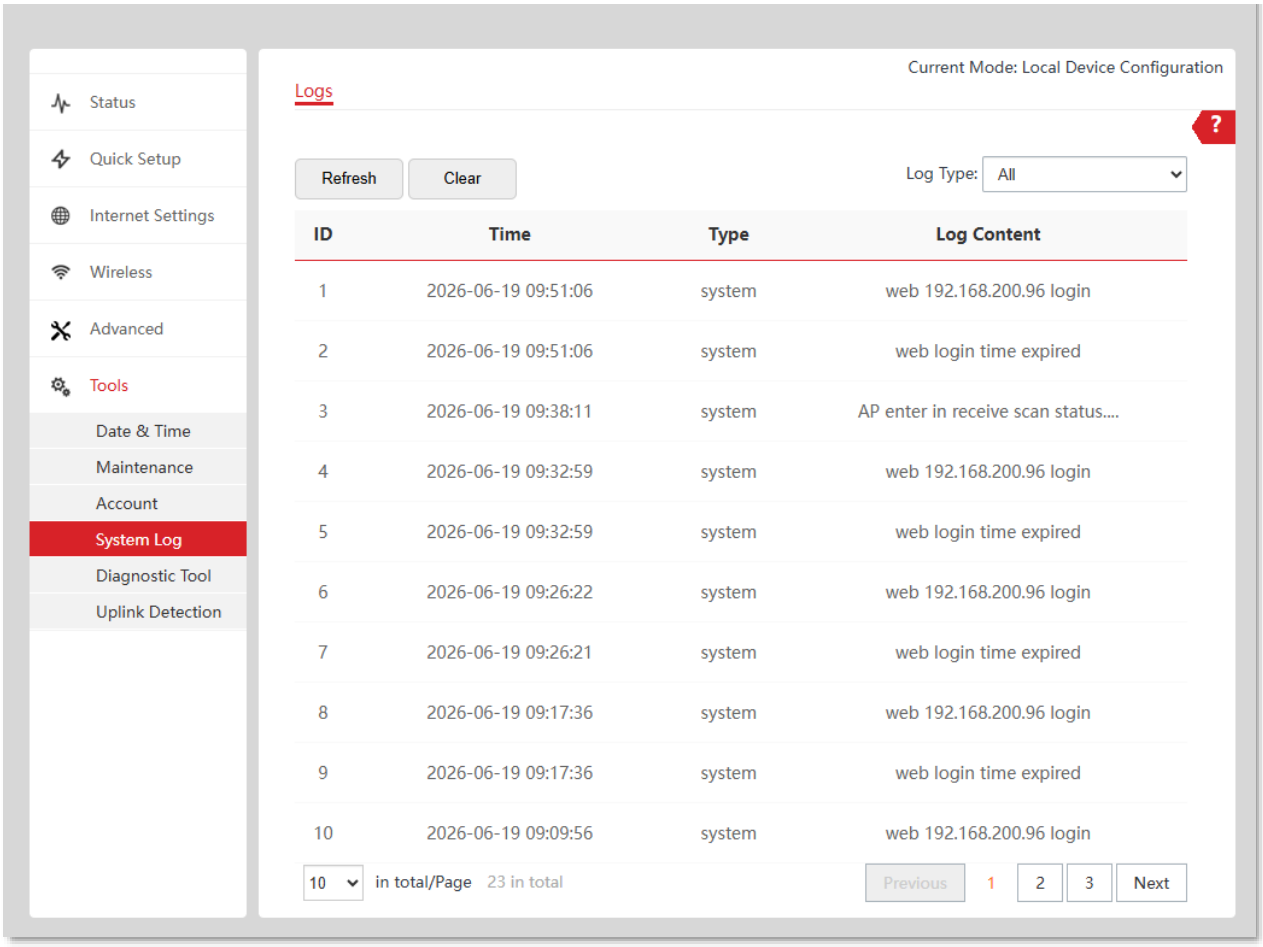
Jurnalul sistemului înregistrează în mod sistematic evenimentele care au loc la nivelul echipamentului, precum și operațiunile efectuate de utilizatori autentificați la interfața de gestionare, după pornirea acestuia. Aceste informații detaliate oferă o vizibilitate completă asupra activității dispozitivului, 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.

Procedură pentru vizualizarea jurnalului cu evenimente de sistem

1. Conectați-vă la interfața web 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.



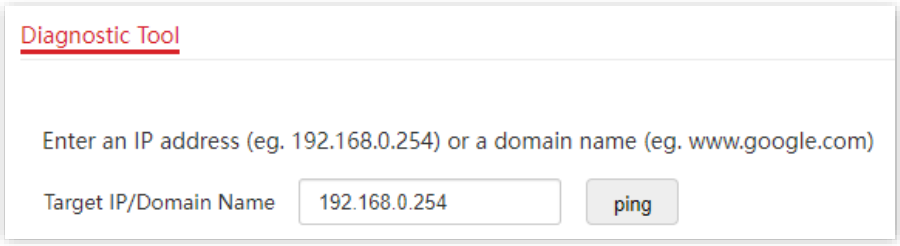
---Sfârșit

8.5 Submeniul Diagnostic Tool (Instrument diagnosticare)

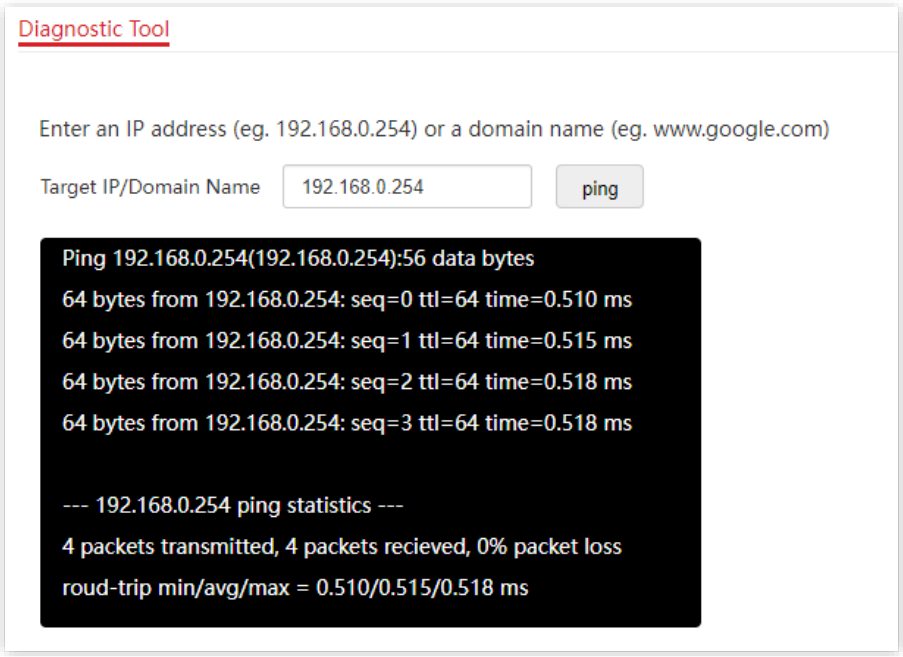
La **Tools (Instrumente)** > **Diagnostic Tool (Instrument diagnosticare)** se găsește unealta ce permite testarea prin ping a conexiunii între echipament și un IP.

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.



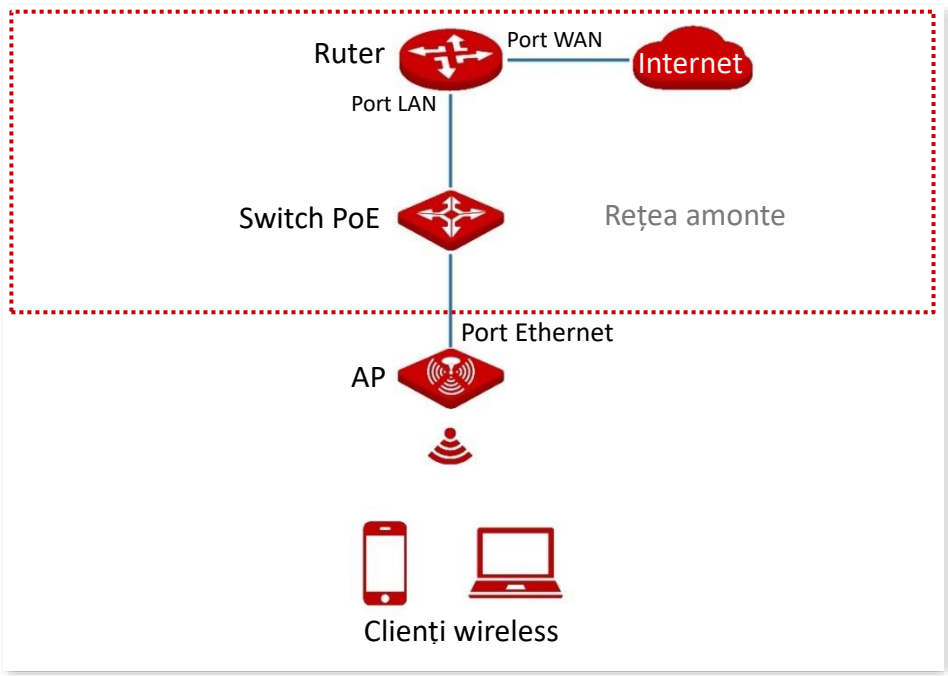
---Sfârșit

8.6 Submeniul Uplink Detection (Detectare legătură amonte)

În mod implicit 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 sau se repornește echipamentul, 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 și acțiunii aferente

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 **Operation (Operație)** selectați ce acțiune să fie executată când nu se mai răspunde la ping. Puteți selecta **Disable RF (Dezactivare RF)** ceea ce duce la oprirea rețelelor Wi-Fi emise de AP sau **Reboot (Repornire)** ceea ce duce la repornirea AP-ului. În acest exemplu se va selecta **Disable RF (Dezactivare RF)**.

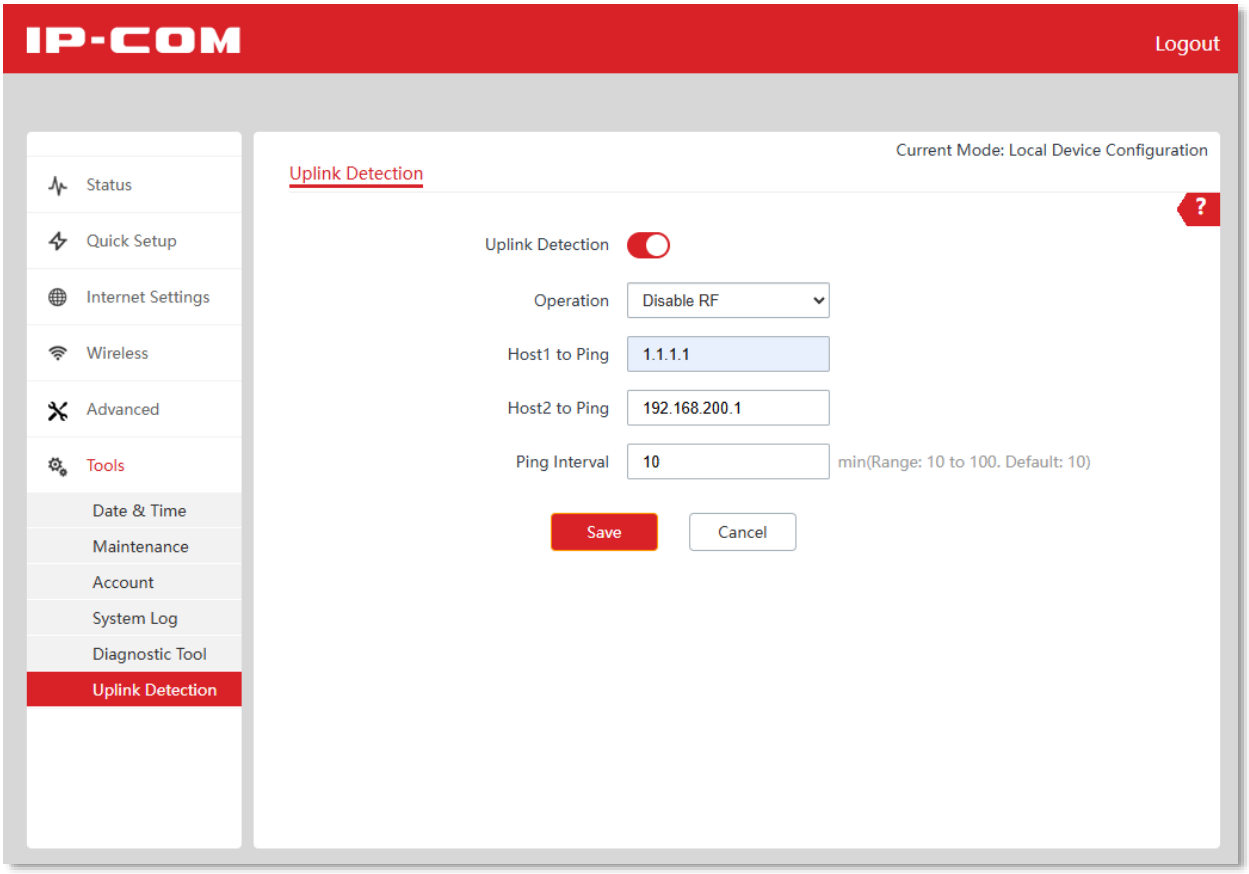
5. La câmpurile **Host1 to Ping (Ping către gazda 1)** sau/și **Host2 to Ping (Ping către gazda 2)** introduceți câte o adresă IP validă ce va fi verificată prin pachete ping, prin portul Ethernet al punctului de acces. De exemplu puteți introduce adresa IP a ruterului conectat direct la punctul de acces precum ***192.168.200.1*** și un IP extern precum ***1.1.1.1*** un DNS public.

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).**

6. La **Ping Interval (Interval ping)** se introduce în minute o perioadă din cât în cât timp se efectuează pingul către adresele IP gazdă. Se va lăsa intervalul implicit de **10 minute**, deși se poate introduce între **10-100 minute**.

7. Faceți clic pe **Save (Salvare).**



---Sfârșit

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

Parametru	Descriere
Uplink Detection **(Detectare legătură amonte)**	Specifică dacă se activează funcția de detectare a legăturii cu rețeaua din amonte. 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.
Operation **(Operație)**	Selectați ce acțiune să fie executată când nu se mai răspunde la ping. Puteți selecta **Disable RF (Dezactivare RF)** ceea ce duce la oprirea rețelelor Wi-Fi emise de AP sau **Reboot (Repornire)** ceea ce duce la repornirea AP-ului.
Host1 to Ping **(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 din amonte este activată.
Host2 to Ping **(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 **(Interval ping)**	Intervalul de timp (în minute) între două verificări succesive. 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 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
AIFSN	Arbitration Inter Frame Spacing Number
AP	Access Point
APSD	Automatic Power Save Delivery
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CTS	Clear To Send
DHCP	Dynamic Host Configuration Protocol
DTIM	Delivery Traffic Indication Map
DNS	Domain Name System
EDCA	Enhanced Distributed Channel Access
FIFO	First-in First-out
GI	Guard Interval
ID	Identifier
IP	Internet Protocol
LAN	Local Area Network
MAC	Media Access Control
MIB	Management Information Base
MU-MIMO	Multi-User Multiple-Input Multiple-Output

Acronim sau abreviere	Denumire originală completă, în engleză
NMS	Network Management System
OID	Object Identifier
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
SAE	Simultaneous Authentication of Equals
Short GI	Short Guard Interval
SNMP	Simple Network Management Protocol
SSID	Service Set Identifier
TCP/IP	Transmission Control Protocol/Internet Protocol
TXOP	Transmission Opportunity
VLAN	Virtual Local Area Network
WAN	Wide Area Network
WLAN	Wireless Local Area Network
WMF	Wireless Multicast Forwarding
WMM	Wi-Fi Multimedia
WPA	Wi-Fi Protected Access