Manualul utilizatorului

Router VPN Gigabit Omada cu porturi PoE+ și
Abilitatea de controler

Despre acest Ghid

Acest Ghid al utilizatorului oferă informații pentru gestionarea centrală a routerului VPN Gigabit Omada cu porturi PoE+ și capacitatea de controler. Vă rugăm să citiți cu atenție acest ghid înainte de utilizare.

Cititorii vizați

Acest Ghid de utilizare este destinat managerilor de rețea familiarizați cu conceptele IT și terminologiile de rețea.

Convenții

Când utilizați acest ghid, observați că:

■ Controlerul, gateway-ul, routerul, routerul integrat sau ER7212PC menționate în acest Ghid de utilizare reprezintă ER7212PC Omada Gigabit VPN Router cu porturi PoE+ și capacitate de controler fără nicio explicație.

■ Caracteristicile disponibile în Omada SDN Controller pot varia în funcție de regiune, versiunea controlerului și modelul dispozitivului. Toate imaginile, pașii și descrierile din acest ghid sunt doar exemple și este posibil să nu reflecte experiența dvs. reală.

■ Informațiile din acest document pot fi modificate fără notificare. S-au depus toate eforturile în pregătirea acestui document pentru a asigura acuratețea conținutului, dar toate declarațiile, informațiile și recomandările din acest document nu constituie garanție de niciun fel, expresă sau implicită. Utilizatorii trebuie să-și asume întreaga responsabilitate pentru aplicarea oricăror produse.

■ Acest ghid folosește formatele specifice pentru a evidenția mesajele speciale. Următorul tabel listează pictogramele de notificare care sunt utilizate în acest ghid.

Notă	Nota conține informații utile pentru o mai bună utilizare a controlerului.
Ghid de configurare	Oferiți sfaturi pentru a afla despre caracteristică și configurațiile acesteia.

Mai multe informatii

■ Pentru asistenţă tehnică, cea mai recentă versiune a Ghidului utilizatorului şi alte informaţii, vă rugăm să vizitaţi https://www.tp-link.com/support .

■ Pentru a pune întrebări, a găsi răspunsuri și a comunica cu utilizatorii sau inginerii TP-Link, vă rugăm să vizitați https://community.tp-link.com pentru a vă alătura comunității TP-Link.

CUPRINS

Configurați controlerul Omada SDN

Configurați și monitorizați dispozitivele gestionate Omada

Monitorizați și gestionați clienții

Monitorizați rețeaua

Gestionați conturile de administrator ale Omada SDN Controller

Accesarea Controllerului

1. 1 Acces interfață web

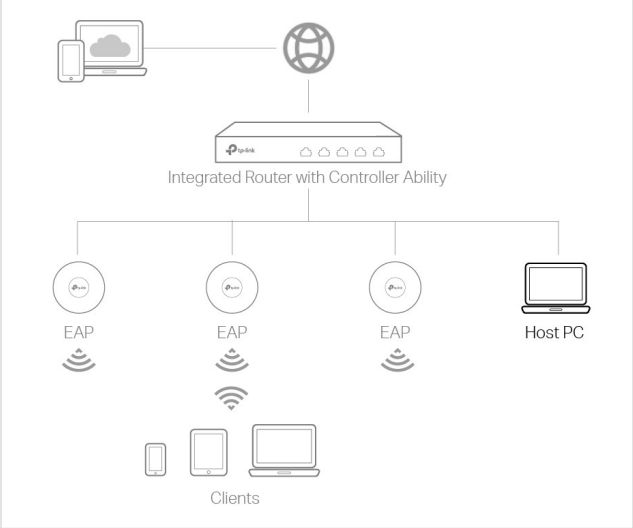
Soluția Omada SDN Controller este concepută pentru rețele scalabile. Implementările și configurațiile variază în funcție de situațiile reale. Înțelegerea cerințelor de rețea este primul pas atunci când planificați furnizarea oricărui proiect. După ce ați identificat aceste cerințe, urmați pașii de mai jos pentru a configura inițial routerul dvs. integrat (denumit în continuare „controller”):

1)Determinați topologia rețelei.

2)Porniți și conectați-vă la controlerul dvs.

1. 1. 1 Determinați topologia rețelei

Topologia de rețea pe care o creați pentru controler variază în funcție de cerințele dvs. de afaceri. Figura următoare arată o topologie tipică pentru un caz de utilizare cu disponibilitate ridicată.



Notă:

Când utilizați Omada SDN Controller, vă recomandăm să implementați topologia completă Omada cu dispozitive TP-Link acceptate. Dacă utilizați dispozitive terțe, Omada SDN Controller nu le poate descoperi și gestiona.

1. 1. 2 Porniți și conectați-vă la controlerul dvs

Conectați-vă la interfața de management

Urmați pașii de mai jos pentru a intra în interfața de gestionare a controlerului dvs.

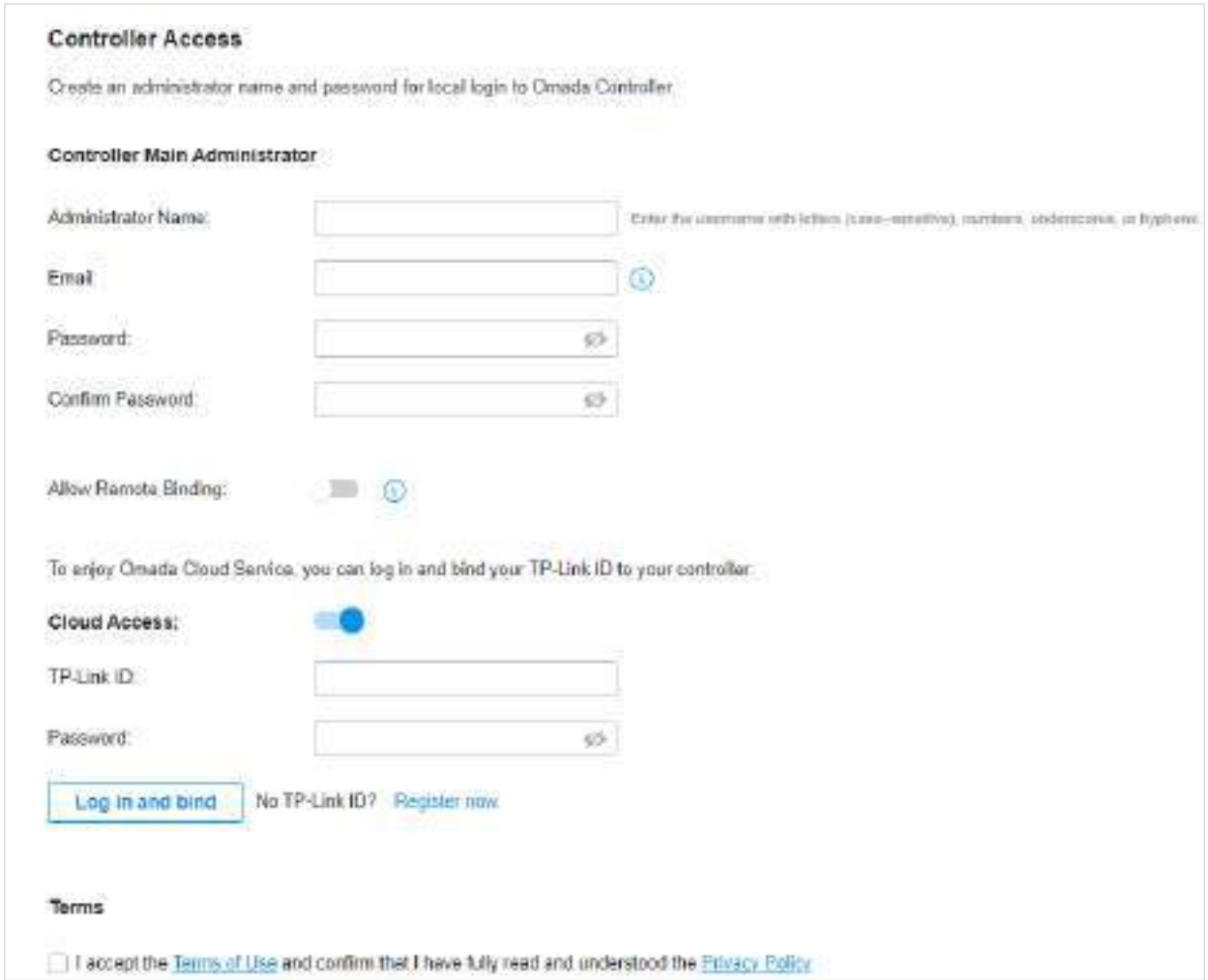
1. Conectați corect un computer la un port LAN al controlerului cu un port RJ45. Dacă computerul dvs. este configurat cu o adresă IP fixă, schimbați-o înObțineți automat o adresă IP.
2. Deschideți un browser web și introduceți adresa de gestionare implicită192.168.0.1în câmpul de adresă al browserului și apăsați tastaintroducecheie.
3. Începeți cuExpertul de configurare Omadapentru a configura rețeaua.

Configurații de bază complete

În browserul web, puteți vedea pagina de configurare. Urmați expertul de configurare pentru a finaliza setările de bază.

1. Faceți clicSă începem.

2. Configurați setările de acces la controler.



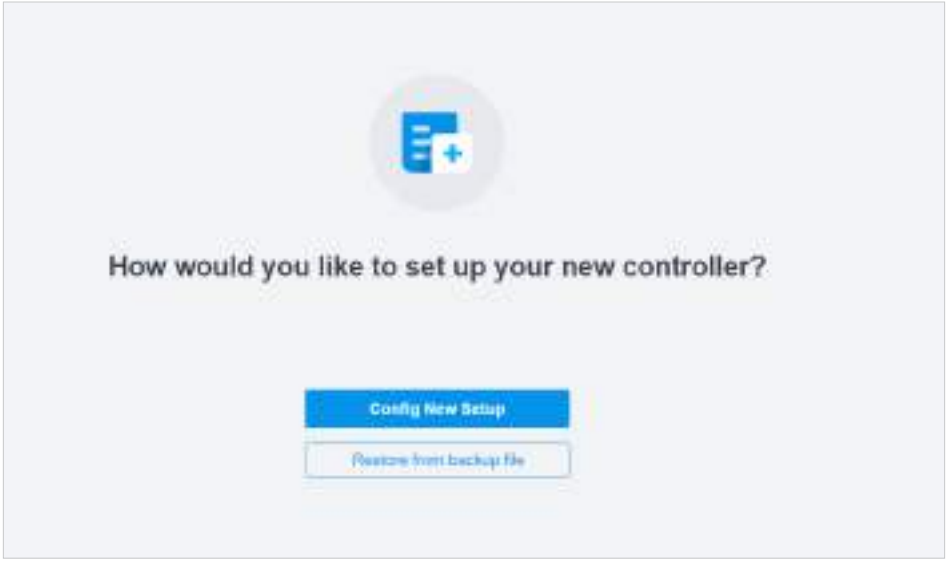
A. Creați un nume de utilizator și o parolă de administrator pentru a vă conecta la controlerul Omada. Specificați adresa de e-mail pentru resetarea parolei în cazul în care uitați parola. După ce vă conectați la controlerul Omada, setați un server de e-mail astfel încât să puteți primi e-mailuri și să vă resetați parola. Pentru cum să setați un server de e-mail, consultați7. 6. 3 Notificări .

b. Dacă doriți să accesați controlerul pentru a gestiona rețelele de la distanță, activațiAcces la cloudși legați-vă ID-ul TP-Link la controlerul Omada. Pentru mai multe detalii despre Omada Cloud, vă rugăm să consultați4. 2 Gestionați-vă controlerul de la distanță prin acces la cloud .

c. Citiți și sunteți de acord cu Termenii de utilizare ai TP-Link.

d. ClicUrmătorul.

3. Alegeți cum doriți să configurați noul controler. Puteți configura o nouă configurare sau restaurați din fișierul de rezervă.



4. Urmați expertul de configurare pentru a configura controlerul.

Conectați-vă la interfața de management

Odată ce configurațiile de bază sunt finalizate, browserul va fi redirecționat către următoarea pagină. Conectați-vă la interfața de management folosind numele de utilizator și parola pe care le-ați setat în configurațiile de bază.

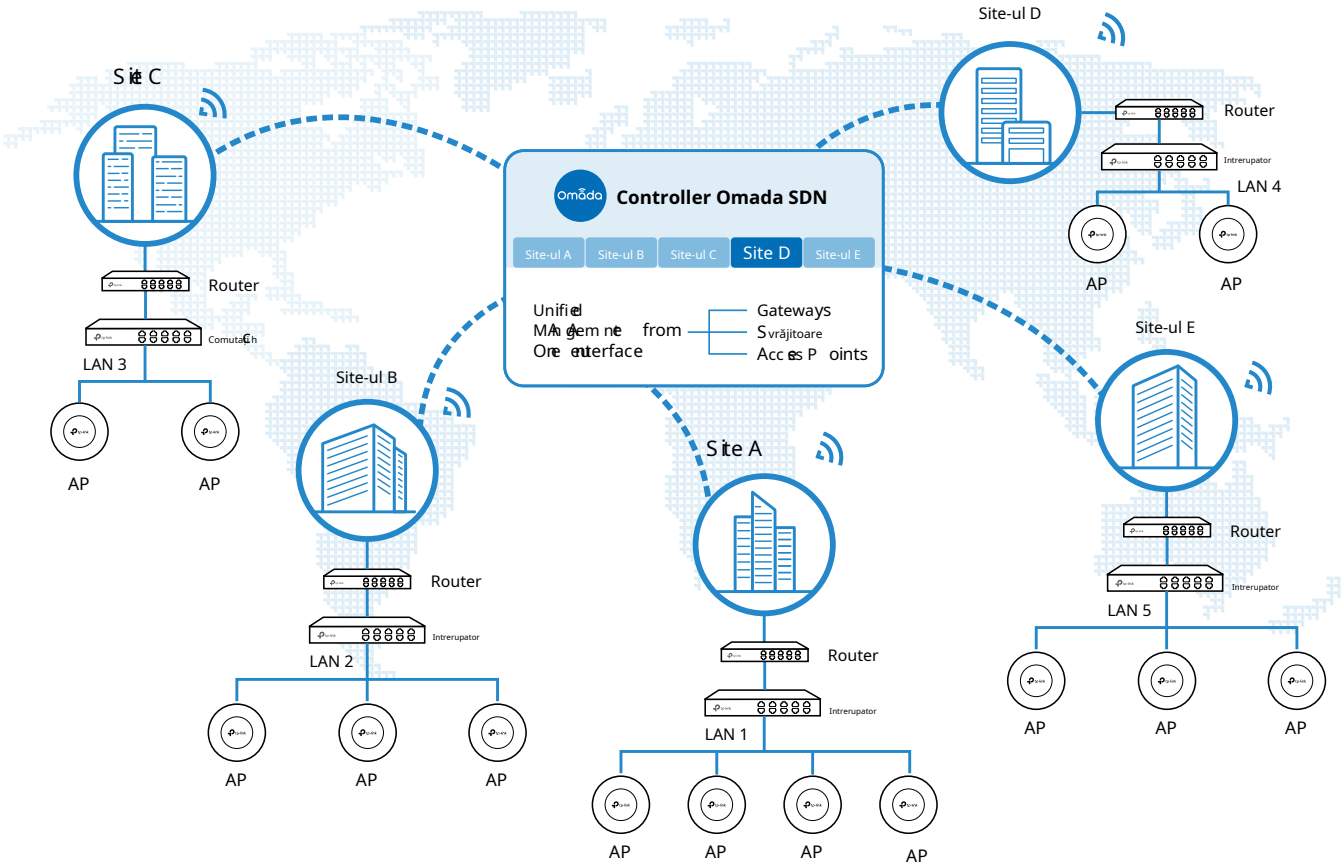
Gestionați dispozitivele și site-urile gestionate de Omada

Începeți să vă gestionați rețeaua creând site-uri și adoptând dispozitive, astfel încât să vă puteți configura și monitoriza dispozitivele central, menținând în același timp lucrurile organizate. Capitolul include următoarele secțiuni:

2. 1 Creați site-uri

Prezentare generală

Site-urile diferite sunt locații de rețea separate logic, cum ar fi diferite companii subsidiare sau departamente. Este cea mai bună practică să creați un site pentru fiecare LAN (Local Area Network) și să adăugați toate dispozitivele din rețea la site, inclusiv routerul, switch-urile și AP-urile.



Dispozitivele de la un site necesită configurații unificate, în timp ce cele de la diferite site-uri nu sunt relative. Pentru a profita la maximum de un site, configurați funcțiile simultan pentru mai multe dispozitive de pe site, cum ar fi VLAN și PoE Schedule pentru switch-uri și SSID și WLAN Schedule pentru AP-uri, în loc să le configurați unul câte unul.

Configurare

Pentru a crea și gestiona un site, urmați acești pași:

1)Creați un site.

2)Vizualizați și editați site-ul.

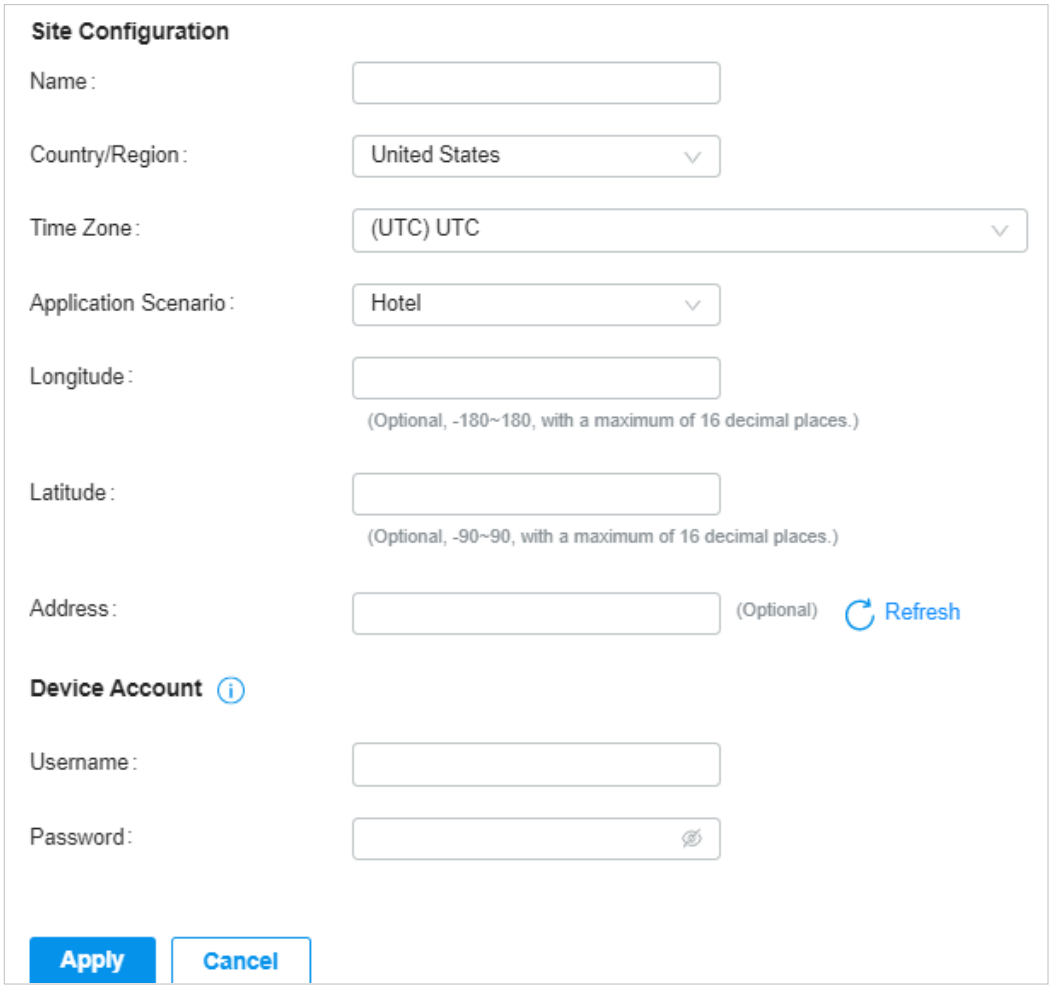
3)Intră pe site.

Creați un site | Vizualizați și editați site-ul | Accesați site-ul

Pentru a crea un site, alegeți una dintre următoarele metode în funcție de nevoile dvs.

■ Creați un site de la zero

1. În vizualizarea globală, accesațiDashboardși localizațiLista site-urilorsecțiune. ClicAdăugați site nou.
2. Introduceți aNumele site-uluipentru a identifica site-ul și a configura alți parametri în funcție de locul în care se află site-ul. Creați un nume de utilizator și o parolă pentru autentificare la dispozitivele nou adoptate. Apoi apasa aplica. Noul site va fi adăugat laLista site-urilorși lista derulantă aOrganizare.



■ Copiați un site existent

Puteți crea rapid un site bazat pe unul existent, prin copierea configurației site-ului, a configurației cu fir și a configurației fără fir, printre altele. După aceea, puteți modifica în mod flexibil configurația noului site pentru a o face diferită de cea veche.

1. ÎnLista site-urilor, faceți clic Site Manager în coloana ACȚIUNE a site-ului pe care doriți să îl copiați.

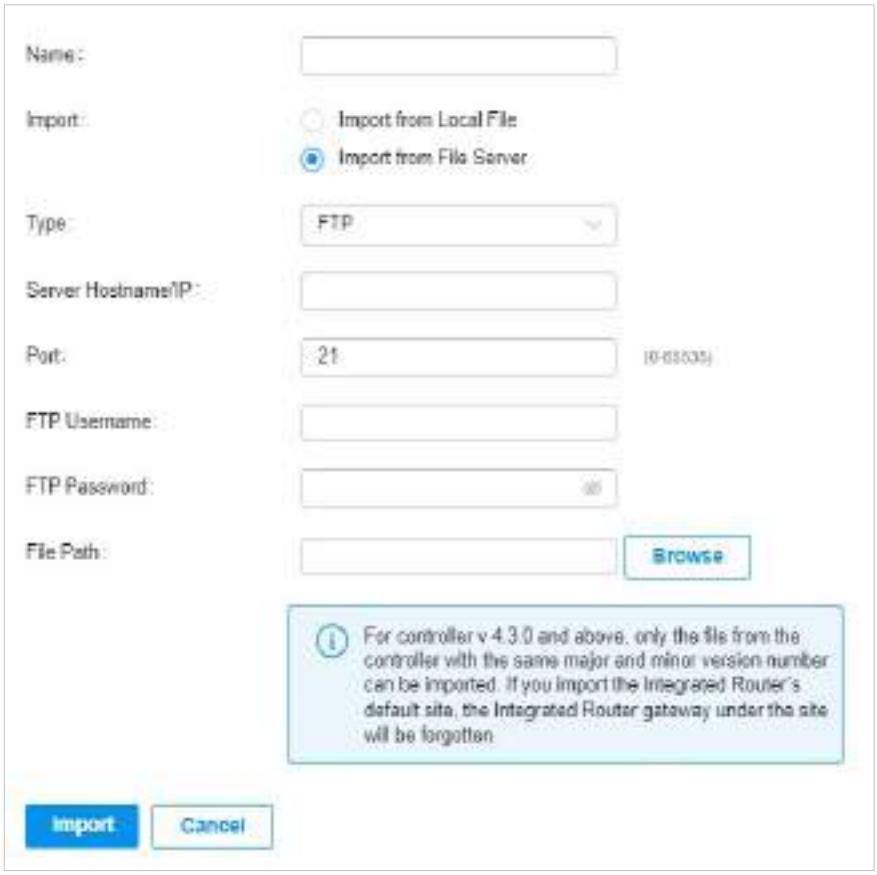
2. Introduceți aNumele site-uluipentru a identifica noul site. Clicaplica. Noul site va fi adăugat laLista site-urilor și lista derulantă aOrganizare.

■ Importați un site de la alt controler

Dacă doriți să migrați fără probleme de la un controler vechi la unul nou, importați fișierul de configurare a site-ului controlerului vechi în cel nou. Înainte de aceasta, trebuie să exportați fișierul de configurare a site-ului de pe vechiul controler, care este acoperit în4. 4. 1 Migrarea site-ului .

1. Faceți clic Import Site înLista site-urilorsecțiune.

2. Introduceți aNumele site-uluipentru a identifica site-ul și a configura alți parametri în funcție de nevoile reale ale site-ului. Răsfoiți exploratorul de fișiere și alegeți un fișier de configurare a site-ului. ClicImport. Noul site va fi adăugat laLista site-urilorși lista derulantă aOrganizare.



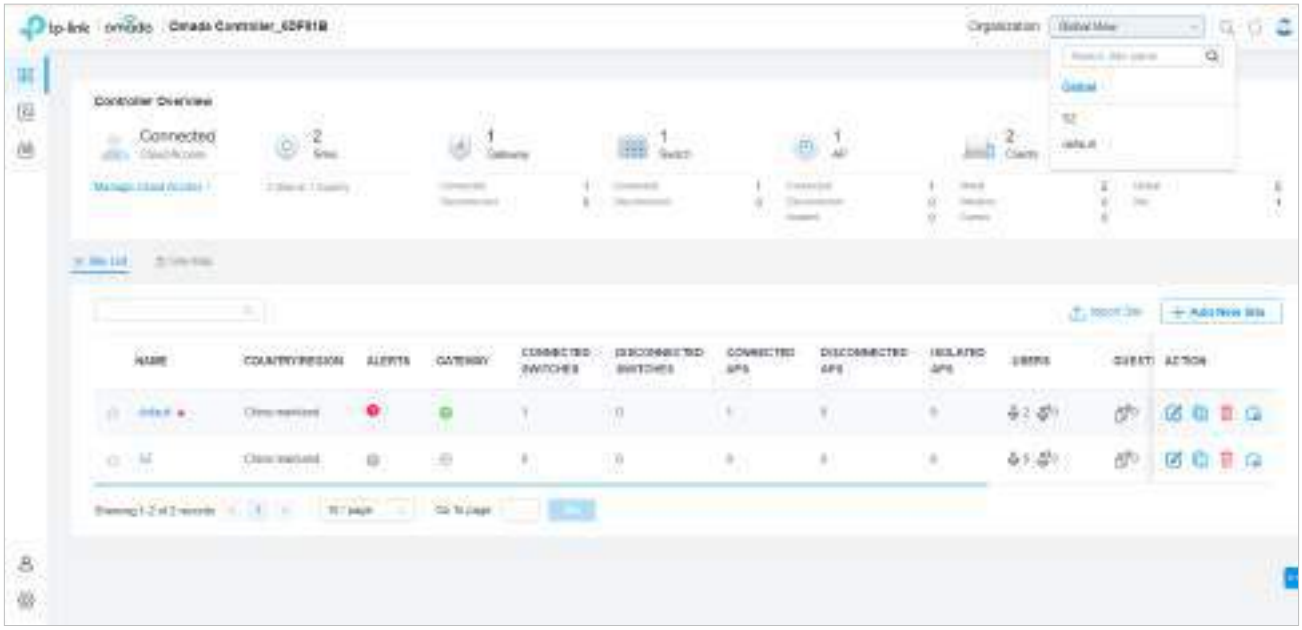
Creați un site | Vizualizați și editați site-ul | Accesați site-ul

După ce creați site-ul, puteți vedea starea site-ului înLista site-urilor. Puteți face clic pe pictogramele din coloana ACȚIUNE pentru a edita, copia, șterge și lansa site-ul.

Creați un site | Vizualizați și editați site-ul | Accesați site-ul

Pentru a monitoriza și configura un site, trebuie mai întâi să accesați site-ul.

Faceți clic pe pictograma site-ului din Lista site-urilor pentru a accesa site-ul. Alternativ, selectați site-ul din lista verticală aOrganizare.

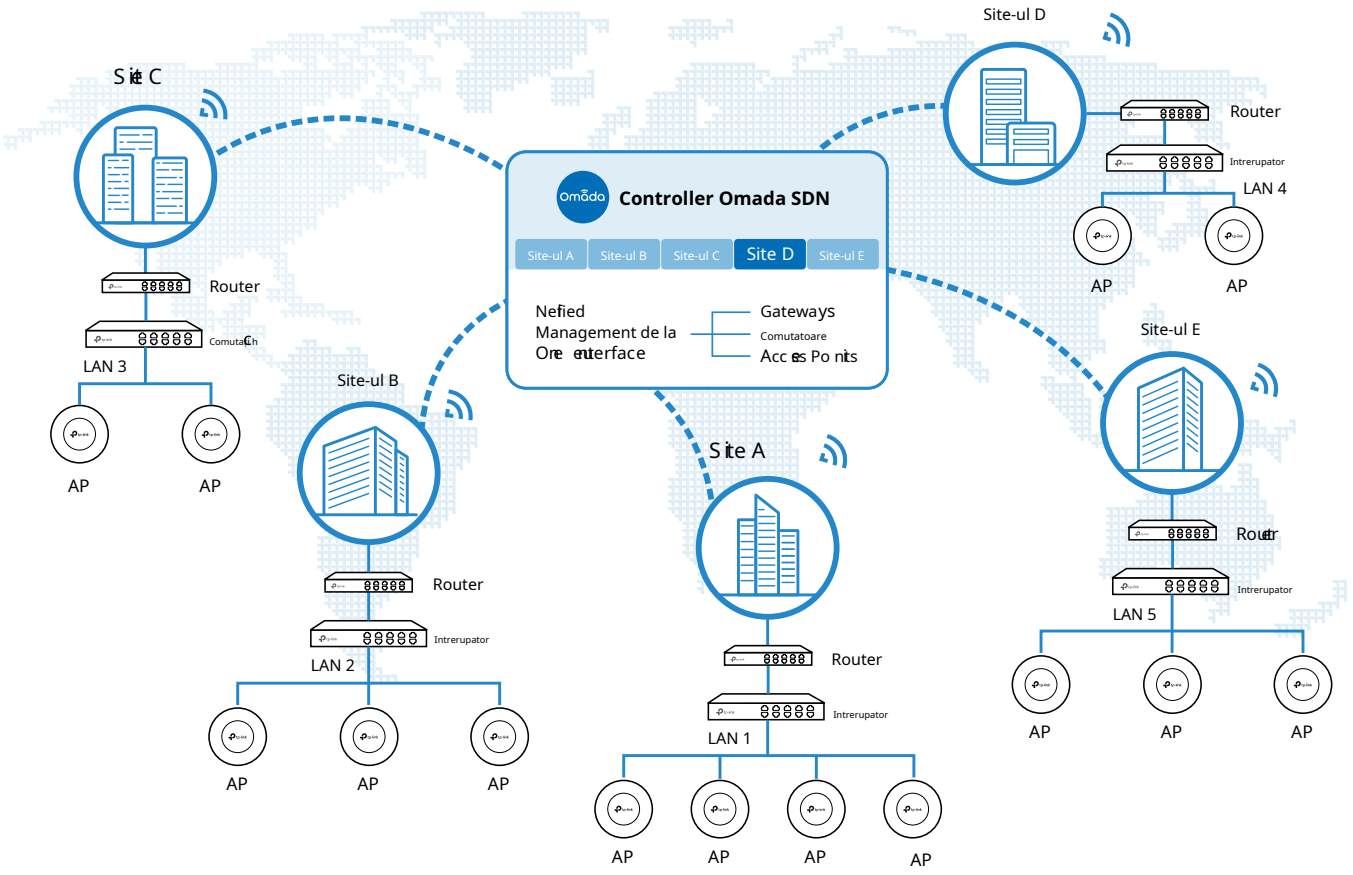


3. CelOrganizarecâmpul indică site-ul în care vă aflați în prezent. Unele elemente de configurare din meniu sunt aplicate site-ului în care vă aflați în prezent, în timp ce altele sunt aplicate întregului controler.

2. 2 Adopta dispozitive

Prezentare generală

După ce creați un site, adăugați dispozitivele dvs. pe site, făcând controlorul să le adopte. Asigurați-vă că dispozitivele dvs. din fiecare LAN sunt adăugate la site-ul corespunzător, astfel încât să poată fi gestionate central.



Configurare

Pentru a adopta dispozitivele pe controler, urmați acești pași:

1)Pregătiți-vă pentru comunicarea între controler și dispozitive.

2)Pregătiți-vă pentru descoperirea dispozitivului.

3)Adoptă dispozitivele.

Pregătiți-vă pentru comunicare → Pregătiți-vă pentru Descoperirea dispozitivului → Adoptă Dispozitivele

Notă:

Dacă controlerul și dispozitivele sunt în aceeași rețea LAN, subrețea și VLAN, săriți peste acest pas.

Asigurați-vă că controlerul poate comunica cu dispozitivele. În caz contrar, controlorul nu poate descoperi sau adopta dispozitivele prin niciun mijloc. Dacă controlerul și dispozitivele sunt în rețele LAN, subrețele sau VLAN-uri diferite, utilizați următoarele tehnici pentru a construi conexiunea în funcție de scenariul dvs.

1. Configurați rețeaua

■ Scenariul 1: peste VLAN-uri sau subrețele

Dacă controlerul și dispozitivele sunt în VLAN-uri sau subrețele diferite. Trebuie să configurați o interfață de nivel 3 pentru fiecare VLAN sau subrețea și să vă asigurați că interfețele pot comunica între ele.

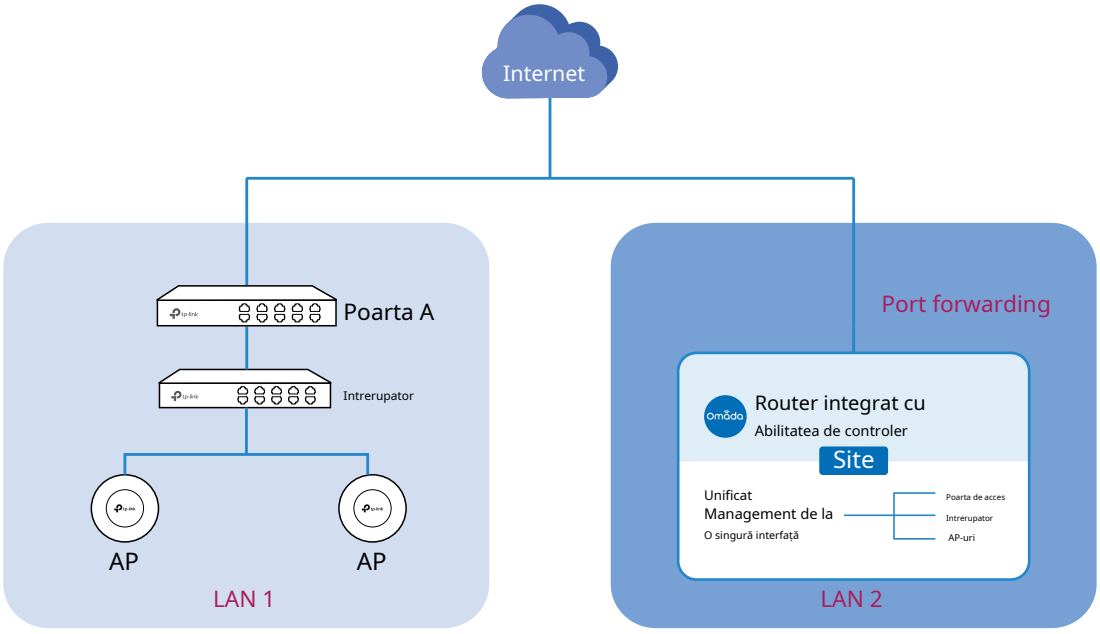
■ Scenariul 2: peste rețele LAN

După cum se arată în figura următoare, controlerul și dispozitivele sunt în rețele LAN diferite. Trebuie să stabiliți comunicarea prin internet și gateway-uri.

În mod implicit, dispozitivele din LAN 1 nu pot comunica cu controlerul din LAN 2, deoarece Gateway-ul A le blochează accesul la controler. Pentru a face controlerul accesibil dispozitivelor, puteți utiliza Port Forwarding sau VPN.

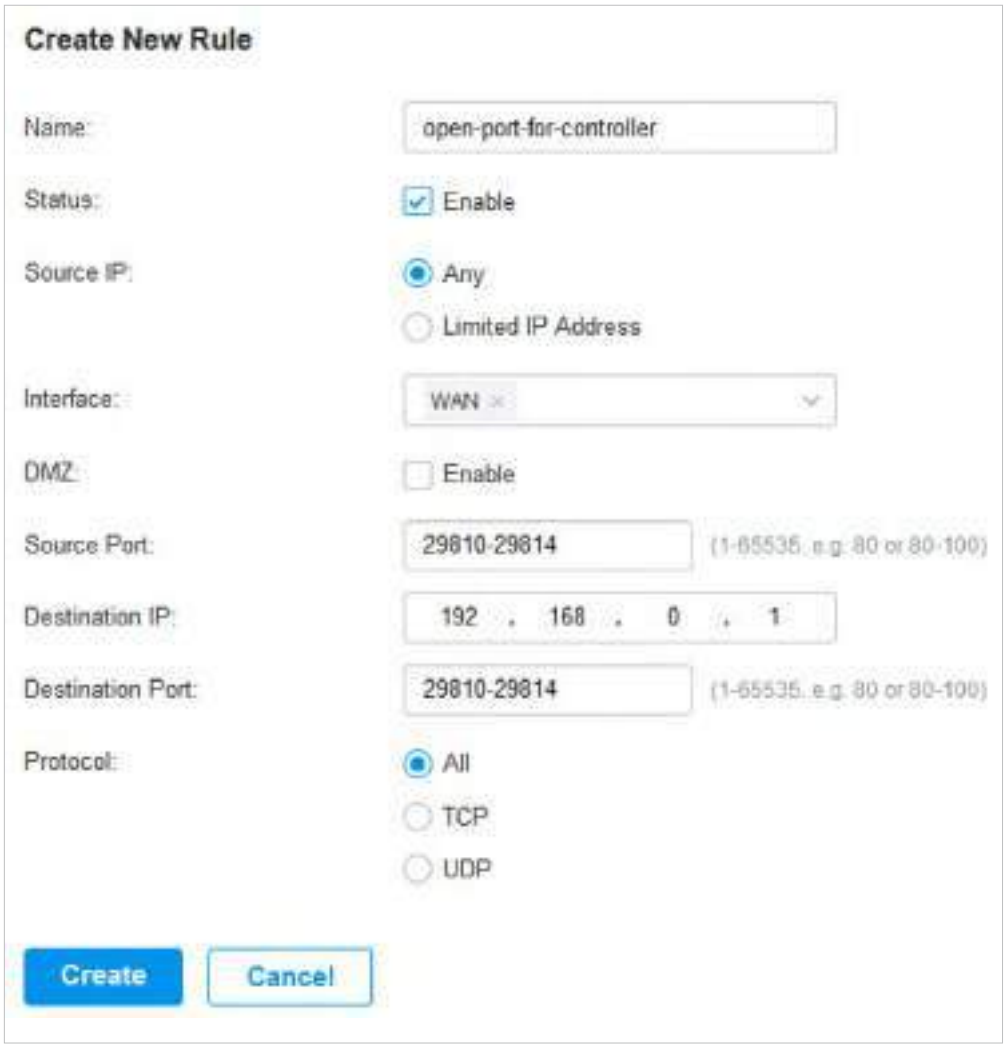
• Utilizați Port Forwarding

Configurați Port Forwarding pe Gateway B și deschideți portul 29810-29814 pentru controler, care sunt esențiale pentru descoperirea și adoptarea dispozitivelor. Dacă utilizați firewall-uri în rețele, asigurați-vă că firewall-urile nu blochează acele porturi.



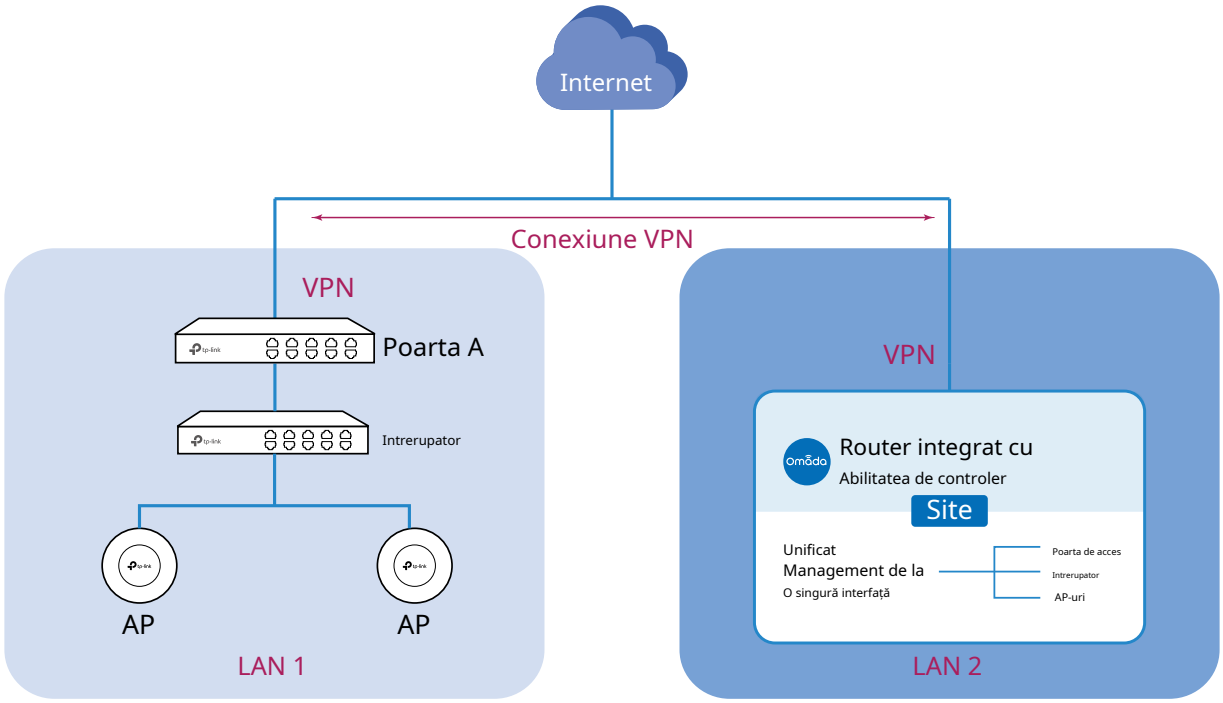
Pentru a configura redirecționarea portului pe controler, accesațiSetări>Transmitere>NAT>Port forwarding. Clic+ Creați o nouă regulăpentru a încărca următoarea pagină. Specificați un nume pentru a identifica regula de redirecționare a portului, bifați Activare pentru Stare, selectați Oricare ca IP sursă, selectați portul WAN dorit

ca Interfață, dezactivați DMZ, specificați 29810-29814 ca Port sursă și Port de destinație, specificați adresa IP a controlerului ca IP de destinație și selectați Toate ca Protocol. Apoi apasaCrea.



• Utilizați VPN

Configurați o conexiune VPN între Gateway A și controler. Pentru detalii despre configurarea VPN, consultați Ghidul utilizatorului al gateway-urilor și3. 7 Configurați VPN a acestui ghid.



2. (Opțional) Testați rețeaua

Dacă nu sunteți sigur dacă controlerul și dispozitivele pot stabili o comunicare, se recomandă să faceți testul ping de la dispozitive la controler.

Să luăm de exemplu un comutator. Conectați-vă la pagina web a comutatorului în modul Standalone. Apoi Mergi laÎNTREȚINERE>Diagnosticarea rețelei>Pingpentru a încărca următoarea pagină și a specifica Destination IP ca adresă IP a controlerului (dacă ați configurat Port Forwarding pe partea controlerului, utilizați în schimb adresa IP WAN publică a gateway-ului). Apoi apasaPing.

Notă:

Pentru a trimite ping la un router, dezactivați Block WAN Ping pe**Setări**>**Securitatea retelei**>Pagina Apărare împotriva atacului.

Dacă rezultatul ping-ului arată că pachetele sunt primite, înseamnă că controlerul poate comunica cu dispozitivele. În caz contrar, controlerul nu poate comunica cu dispozitivele, atunci trebuie să vă verificați rețeaua.

Pregătiți-vă pentru comunicare | Pregătiți-vă pentru Descoperirea dispozitivului | Adoptă Dispozitivele

Notă:

Dacă controlerul și dispozitivele sunt în aceeași rețea LAN, subrețea și VLAN, săriți peste acest pas. În acest scenariu, controlerul poate descoperi dispozitivele direct și nu sunt necesare setări suplimentare.

Asigurați-vă că controlerul poate descoperi dispozitivele.

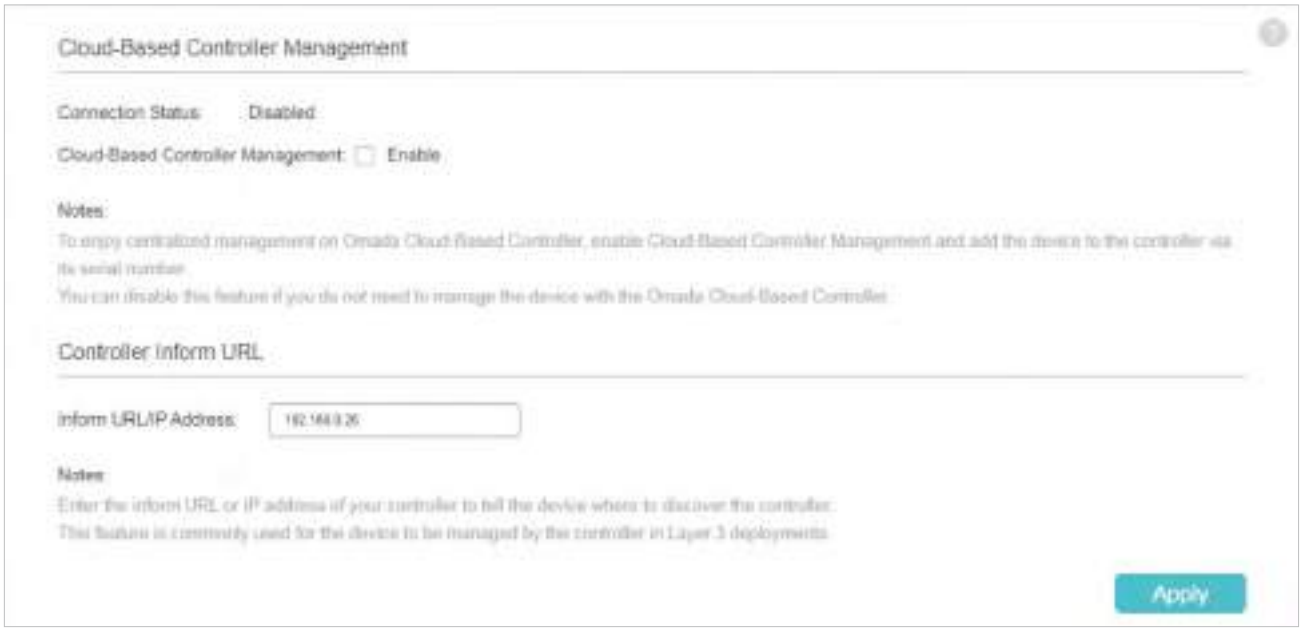
Când controlerul și dispozitivele sunt în rețele LAN, subrețele sau VLAN-uri diferite, controlerul nu poate descoperi dispozitivele direct. Trebuie să alegiAdresa URL de informare a controlorului,Utilitar Discovery, sauOpțiunea DHCP 138 ca metodă de a ajuta controlerul să descopere dispozitivele.

■ Adresa URL de informare a controlorului

Controller Inform URL informează dispozitivele despre adresa URL sau IP a controlerului. Apoi dispozitivele intră în contact cu controlerul, astfel încât controlerul să poată descoperi dispozitivele.

Puteți configura URL-ul Controller Inform pentru dispozitivele în modul Standalone. Să luăm de exemplu un comutator. Conectați-vă la pagina de gestionare a comutatorului în modul Standalone și accesațiSISTEM

> Setări controlerpentru a încărca următoarea pagină. ÎnAdresa URL de informare a controlorului, specificați Inform URL/IP Address ca URL sau adresă IP a controlerului (dacă ați configurat Port Forwarding pe partea controlerului, utilizați în schimb adresa IP WAN publică a gateway-ului). Apoi apasaaplica.

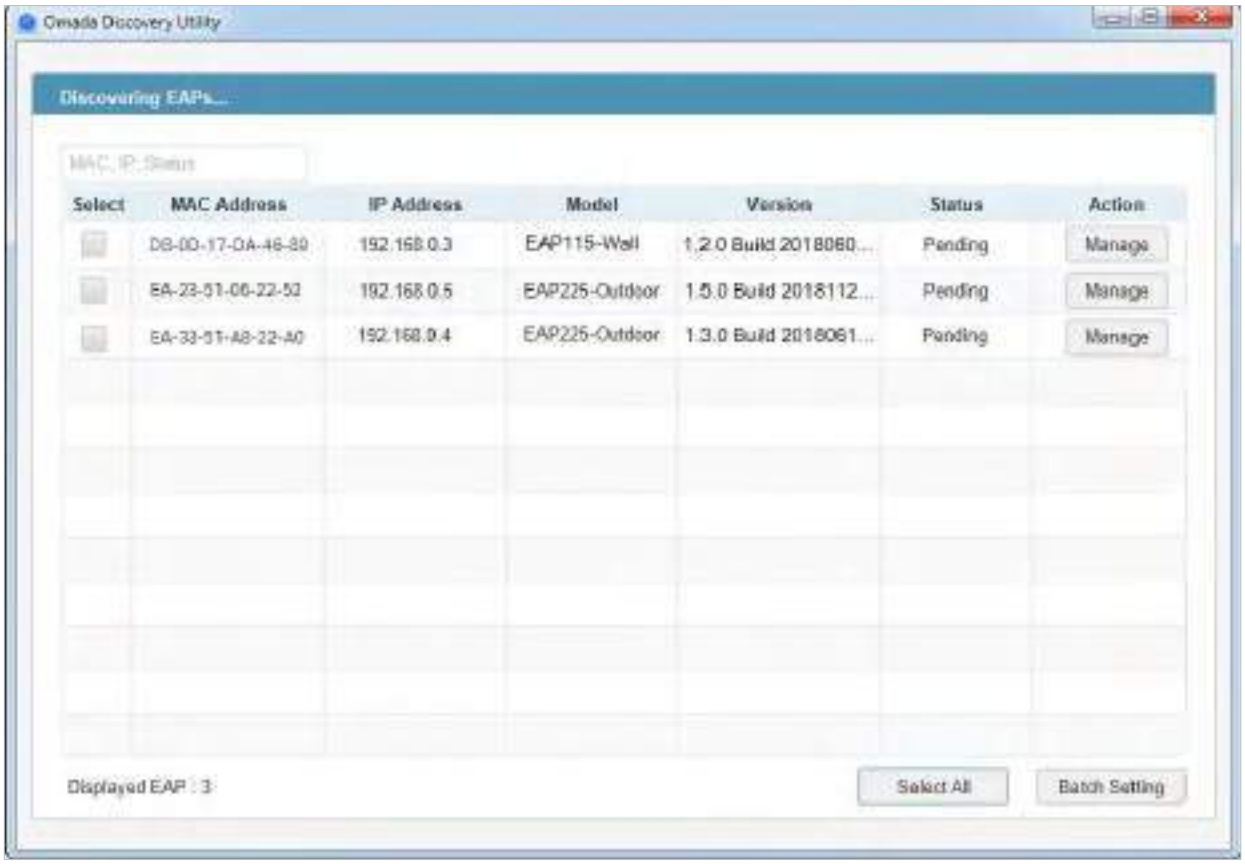


■ Utilitar Discovery

Discovery Utility poate descoperi dispozitivele din aceeași rețea LAN, subrețea și VLAN și poate informa dispozitivele despre adresa IP a controlerului. Apoi dispozitivele intră în contact cu controlerul, astfel încât controlerul să poată descoperi dispozitivele.

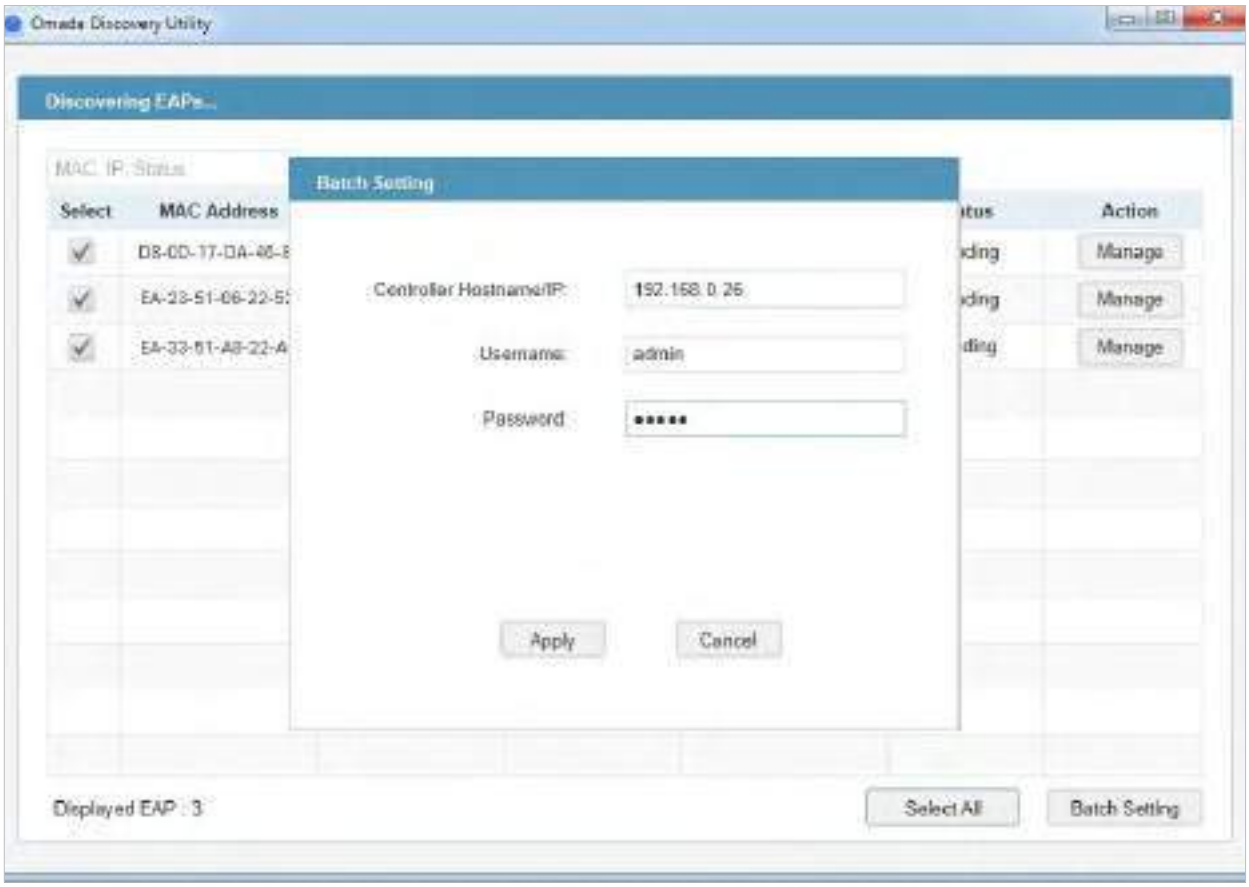
1. Descărcați utilitarul Discovery dinsite-ul web și apoi instalați-l pe computerul dvs., care ar trebui să fie situat în aceeași rețea LAN, subrețea și VLAN ca și dispozitivele dvs.

2. Deschideți Discovery Utility și puteți vedea o listă de dispozitive. Selectați dispozitivele de adoptat și faceți clicSetarea lotului.



3. Specificați Controller Hostname/IP ca adresa IP a controlerului (dacă ați configurat Port Forwarding pe partea controlerului, utilizați în schimb adresa IP WAN publică a gateway-ului) și

introduceți numele de utilizator și parola dispozitivelor. În mod implicit, numele de utilizator și parola sunt ambele admin. Apoi apasaaplica. Așteptați până când setarea reușește.



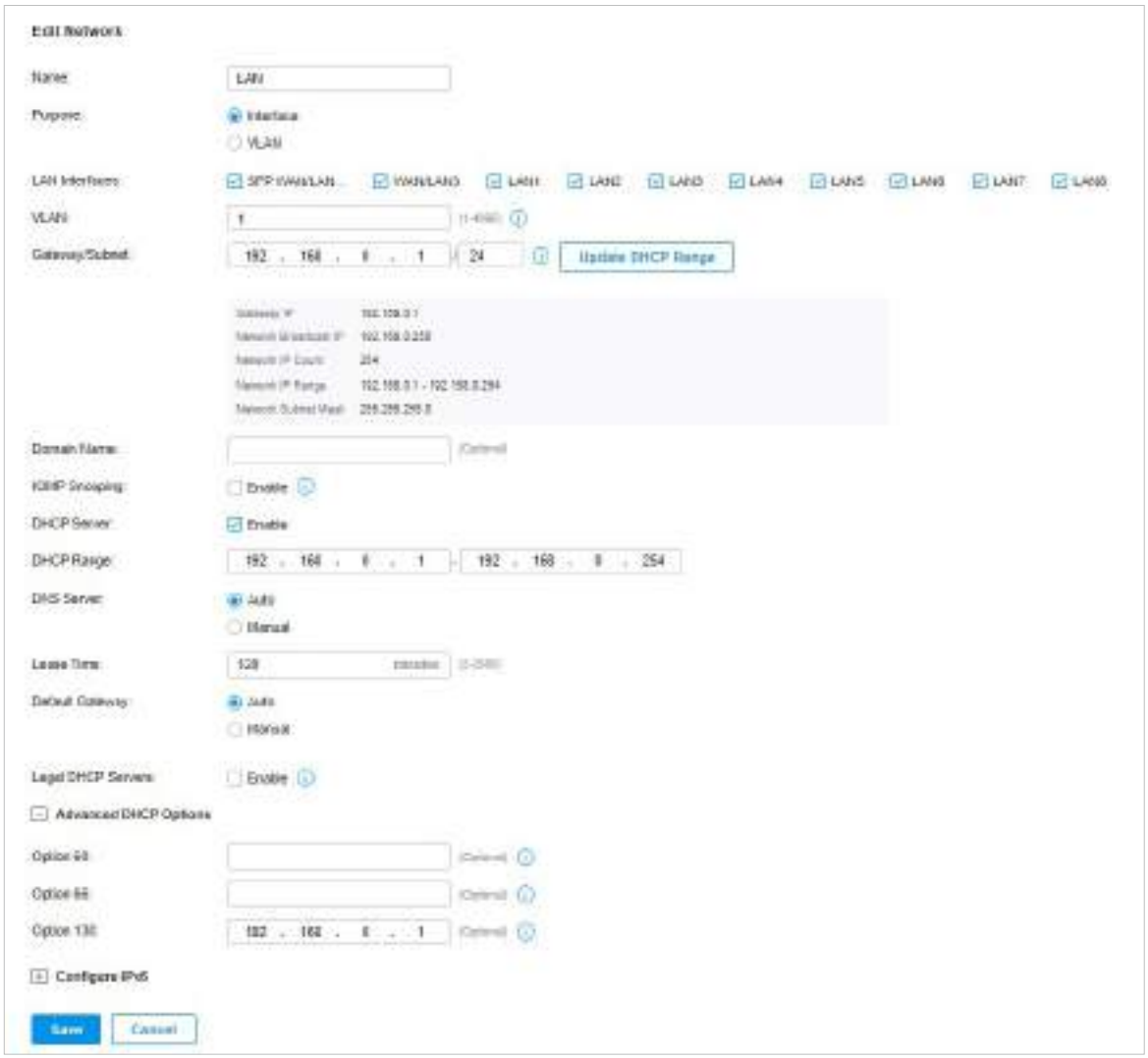
■ Opțiunea DHCP 138

Opțiunea DHCP 138 informează un client DHCP, cum ar fi un comutator sau un EAP, despre adresa IP a controlerului atunci când clientul DHCP trimite solicitări DHCP către serverul DHCP, care este de obicei un gateway.

1. Pentru a utiliza opțiunea DHCP 138, trebuie să adoptați mai întâi gateway-ul pe controler, care poate necesita alte tehnici precumAdresa URL de informare a controlorului sauUtilitar Discovery daca este necesar.

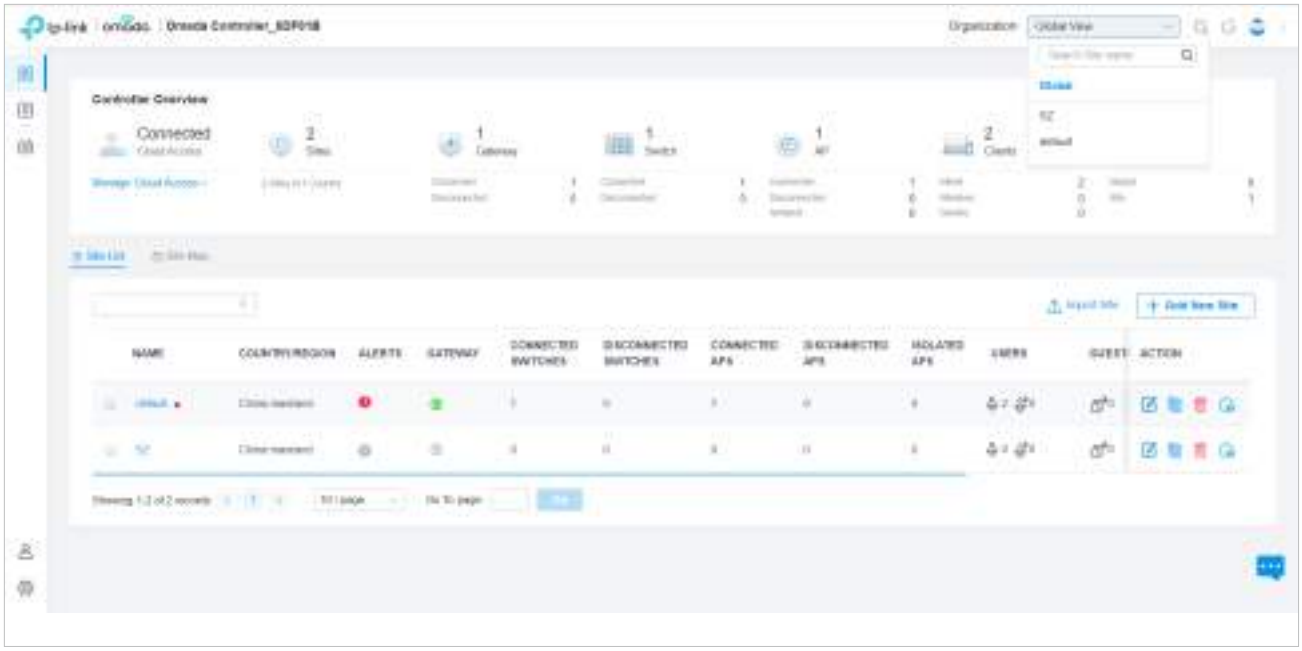
2. După ce gateway-ul este adoptat, accesațiSetări>Rețele cu fir>LAN>Rețele, și faceți clic în coloana ACTION a rețelei LAN în care se află clienții DHCP. Activați serverul DHCP și configurați parametrii DHCP comuni. Apoi apasaOpțiuni avansate DHCPși specificați Opțiune

138 ca adresa IP a controlerului (dacă ați configurat Port Forwarding pe partea controlerului, utilizați în schimb adresa IP WAN publică a gateway-ului). ClicSalvați.

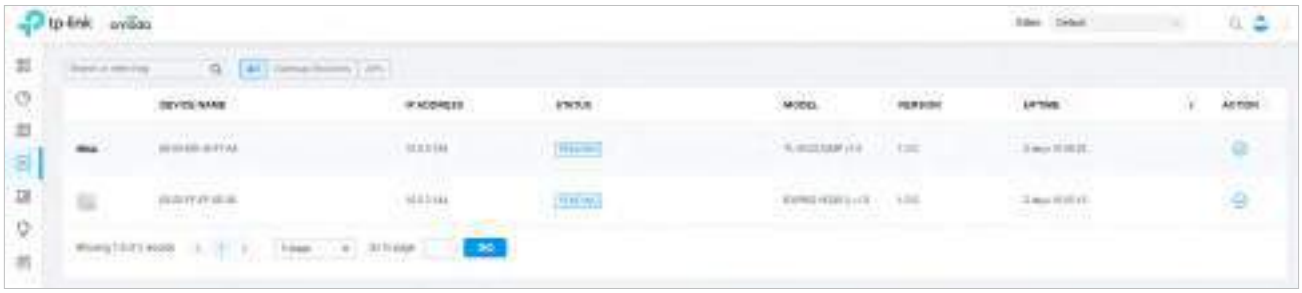


3. Pentru ca opțiunea DHCP 138 să intre în vigoare, trebuie să reînnoiți parametrii DHCP pentru clienții DHCP. O modalitate posibilă este să deconectați clienții DHCP și apoi să îi reconectați.

1. Decideți pe ce site doriți să adăugați dispozitivele. Pe pagina de configurare a controlerului, selectați site-ul din lista derulantă aOrganizare.



2. AccesațiDispozitive, iar dispozitivele care au fost descoperite de controler sunt afișate. Faceți clic în coloana ACȚIUNE a dispozitivelor pe care doriți să le adăugați pe site.



3. Așteptați până cândSTAREse transformă înConectat. Apoi dispozitivele sunt adoptate de controlor și adăugate la site-ul curent. Odată adoptate dispozitivele, acestea sunt supuse managementului central în site.

Configurați rețeaua cu Omada SDN Controller

Acest capitol vă ghidează despre cum să configurați rețeaua cu Omada SDN Controller. Fiind centru de comandă și platformă de management din centrul rețelei Omada, Omada SDN Controller oferă o abordare unificată pentru configurarea rețelelor de întreprindere compuse din routere, switch-uri și puncte de acces wireless. Capitolul include următoarele secțiuni:

3. 1 Navigați în interfața de utilizare

Pe măsură ce începeți să utilizați interfața de gestionare a controlerului (Controller UI) pentru a vă configura și monitoriza rețeaua, este util să vă familiarizați cu Controller UI.

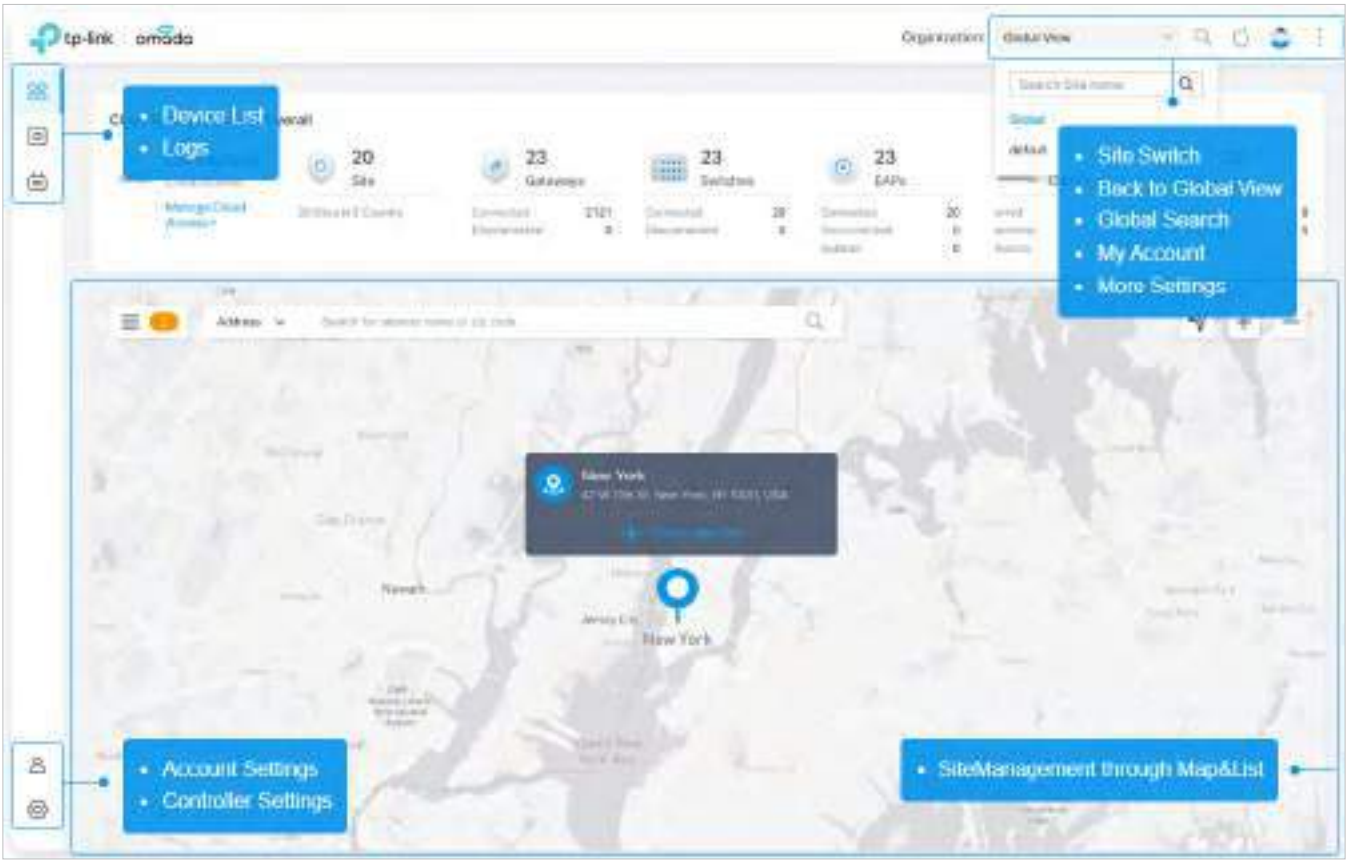
■ Prezentare globală

Cunoașteți starea site-urilor dvs. dintr-o privire și gestionați site-urile în platforma Omada.

• Monitorizarea site-ului—Vă ține informat cu privire la starea exactă, în timp real, a fiecărui site.

• Site Management—Gestionați toate site-urile pentru a implementa întreaga rețea.

• Setări cont—Gestionați toate conturile administrative.



■ Prezentare generală a site-ului

Cunoașteți starea rețelei dvs. dintr-o privire, obțineți informații și gestionați dispozitivele de rețea, totul în platforma Omada.

• Statistici și monitorizare—Vă ține la curent cu privire la starea precisă, în timp real, a fiecărei rețele

dispozitiv și client.

• Setări—Configurați central toate dispozitivele de rețea.

Prezentare generală a site-ului

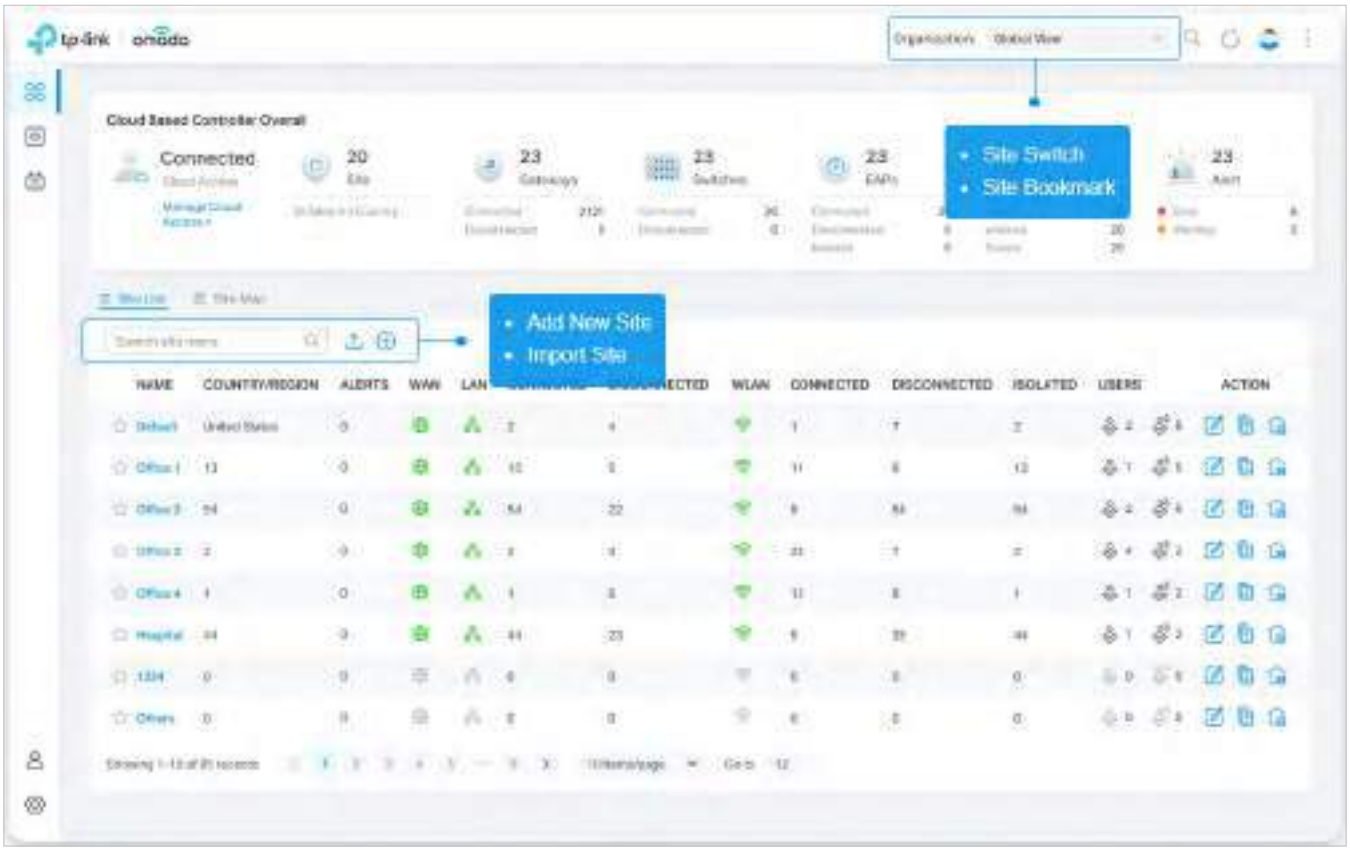
Site, care înseamnă locație separată logic, este cea mai mare unitate de gestionare a rețelelor cu Omada SDN Controller. Puteți configura simultan funcții pentru mai multe dispozitive de pe un site.

• Adăugare site nou — Faceți clic pe Adăugare site nou pentru a adăuga un site nou, care este rețeaua separată logic

Locație. Site-ul este cea mai mare unitate de gestionare a rețelei.

• Import Site — Faceți clic pe Import Site pentru a importa site-ul de la alt controler.

• Marcaj site – Faceți clic pe Marcaj pentru a plasa site-urile utilizate frecvent în partea de sus a listei.



■ Monitorizarea rețelei

Datele vizuale țin administratorul de rețea informat despre starea exactă a fiecărui dispozitiv de rețea și client din rețeaua cu fir și fără fir.

Interfața de utilizare a controlerului este grupată în meniuri orientate către sarcini. Aceste meniuri sunt situate în colțul din dreapta sus și bara de navigare din stânga a paginii. Rețineți că setările și caracteristicile care apar în interfața de utilizare depind de permisiunile contului dvs. de utilizator. Următoarea imagine ilustrează elementele principale ale interfeței de utilizare a controlerului.

Elementele din colțul din dreapta sus al ecranului oferă acces rapid la:

Managementul organizației

Vedere globală —Cunoașteți starea site-ului dvs. dintr-o privire și gestionați site-urile în platforma Omada.

Vizualizare site —Cunoașteți starea rețelei dvs. dintr-o privire, obțineți informații și gestionați dispozitivele de rețea, totul în platforma Omada.

Manager hotspot —Monitorizează și gestionează central clienții autorizați prin autentificarea portalului.

Funcția de căutare globală

Clic și introduceți cuvintele cheie pentru a căuta rapid funcțiile sau dispozitivele pe care doriți să le configurați. Si tu poti căutați dispozitivele după adresele MAC și numele dispozitivelor.

Contul meu

Faceți clic pe parola pictogramei pentru a afișa informații despre cont, Setări cont și Deconectare. Îți poți schimba contului din Setările contului.

Mai multe setari

Clic pentru a afișa Preferințe, Despre, Tutorial și Feedback.

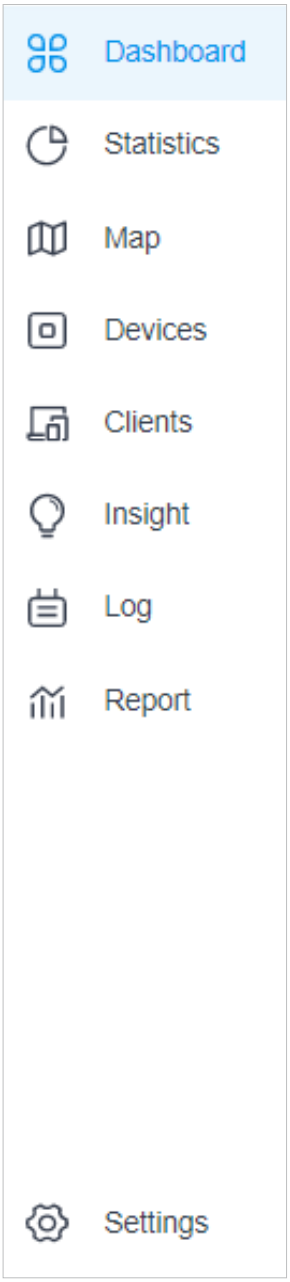
Preferințe:Faceți clic pentru a trece la Întreținere și a personaliza interfața de utilizare a controlerului în funcție de nevoile dvs. Pentru detalii, consultați4. 3 Întreținere

Despre:Faceți clic pentru a afișa versiunea controlerului.

Tutorial:Faceți clic pentru a vizualiza ghidul rapid Noțiuni introductive care demonstrează navigarea și instrumentele disponibile pentru controler.

Părere:Faceți clic pentru a ne trimite feedback-ul dvs.

Bara de navigare din stânga oferă acces la:



Bordafișează o vedere rezumată a stării rețelei prin diferite vizualizări. Tabloul de bord personalizabil și bazat pe widget-uri este un instrument puternic care vă oferă date în timp real pentru monitorizarea rețelei. Cu funcția de glisare și plasare, puteți modifica tabloul de bord și îl puteți rearanja pentru a vă permite să urmăriți toate valorile importante.

Statisticioferă o reprezentare vizuală a clienților și a rețelei gestionate de controler. Diagramele de rulare arată modificări ale performanțelor dispozitivului de-a lungul timpului, inclusiv starea comutatoarelor și rezultatele testelor de viteză.

Hartăgenerează automat topologia sistemului și puteți verifica starea de furnizare a dispozitivelor. Făcând clic pe fiecare nod, puteți vizualiza informații detaliate despre fiecare dispozitiv. De asemenea, puteți încărca imagini cu locația dvs. pentru o reprezentare vizuală a rețelei dvs.

Dispozitiveafișează toate dispozitivele TP-Link descoperite pe site și informațiile generale ale acestora. Această vizualizare de listă se poate modifica în funcție de nevoile dvs. de monitorizare prin personalizarea coloanelor. Puteți face clic pe orice dispozitiv din listă pentru a afișa fereastra Proprietăți pentru informații mai detaliate despre fiecare dispozitiv și pentru a furniza configurații individuale pentru dispozitiv.

Cliențiiafișează o listă de clienți cu fir și fără fir care sunt conectați la rețea. Această vizualizare de listă se poate modifica în funcție de nevoia dvs. de monitorizare prin personalizarea coloanelor. Puteți face clic pe orice client din listă pentru a dezvălui fereastra Proprietăți pentru informații mai detaliate despre fiecare client și furnizarea de configurații individuale pentru client.

Perspectivăafișează o listă de statistici ale dispozitivului dvs. de rețea, clienților și serviciilor într-o anumită perioadă. Puteți modifica intervalul de date în trepte de o zi.

Buturugaafișează linii de jurnal despre activități variate ale utilizatorilor, dispozitivelor și evenimentelor de sistem, cum ar fi acțiuni administrative și comportamente anormale ale dispozitivului. Jurnalele cuprinzătoare fac informațiile istorice mai precise, mai ușor accesibile și mai utilizabile, ceea ce permite depanarea proactivă. Și puteți determina evenimente la nivel de alertă și puteți activa notificările push.

Raportoferă diagrame intuitive și statistici detaliate privind situația rețelei, dispozitivele gestionate și clienții conectați.

Setărivă permite să furnizați și să configurați toate dispozitivele de rețea de pe același site în câteva minute și să mențineți sistemul de controler pentru performanță optimă.

3. 2 Modificați configurația curentă a site-ului

Puteți vizualiza și modifica configurațiile site-ului curent înSite, inclusiv informațiile de bază ale site-ului, funcțiile dispozitivului gestionate central și contul dispozitivului. Funcțiile și contul de dispozitiv configurat aici sunt aplicate tuturor dispozitivelor de pe site, astfel încât să puteți gestiona cu ușurință dispozitivele central.

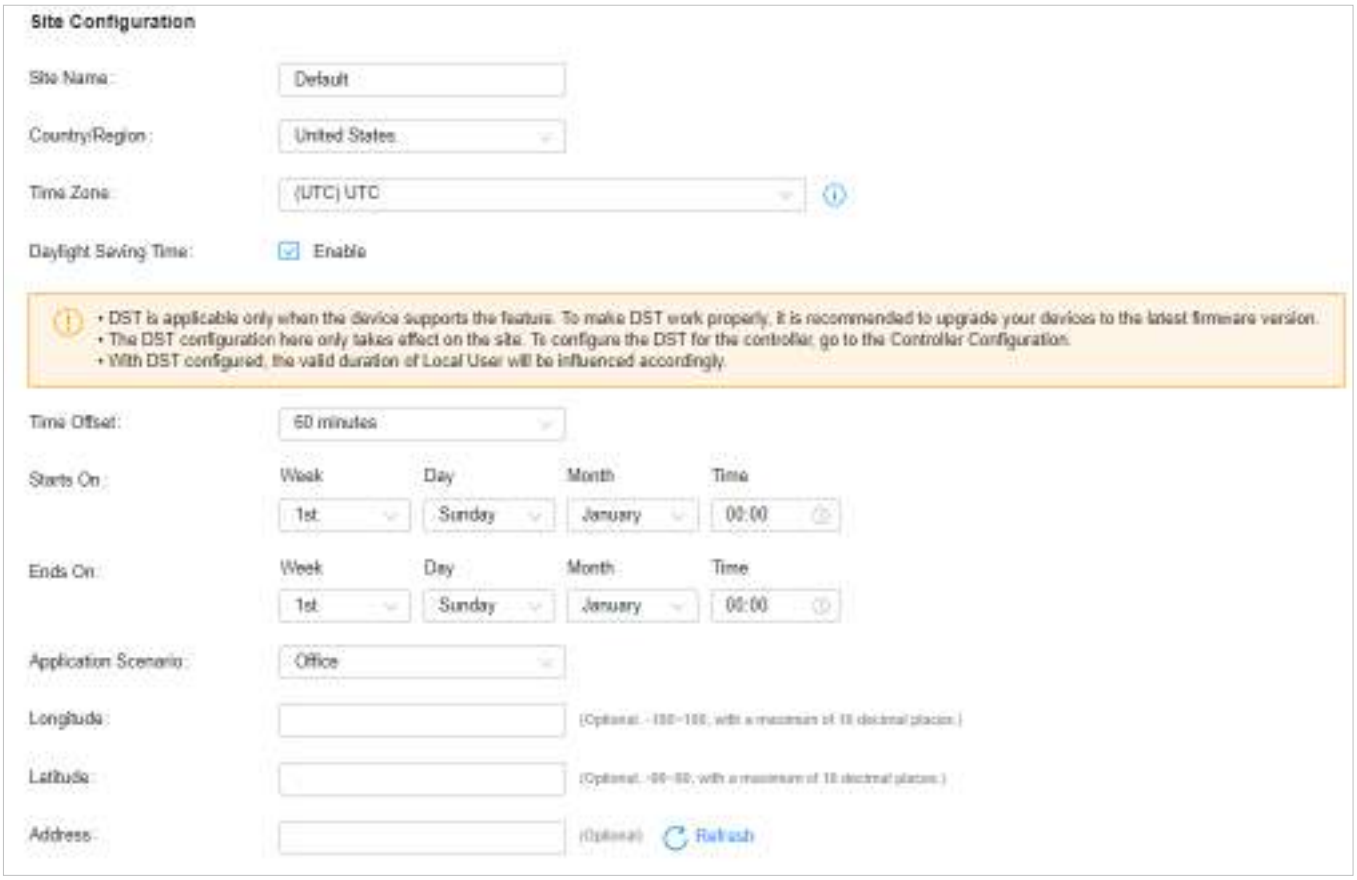
3. 2. 1 Configurare site

Prezentare generală

În Configurarea site-ului, puteți vizualiza și modifica numele site-ului, locația, fusul orar și scenariul de aplicație al site-ului curent.

Configurare

Selectați un site din lista derulantă aOrganizareîn colțul din dreapta sus, accesațiSetări>Site, și configurați următoarele informații ale site-ului înConfigurarea site-ului. ClicSalvați.



Numele site-ului	Specificați numele site-ului curent. Nu trebuie să depășească 64 de caractere.
Țara/Regiune	Selectați locația site-ului.

Fus orar	Selectați fusul orar al site-ului.
Ora de vară	Activați funcția dacă țara/regiunea dvs. implementează DST. Când este activat, pictograma DST va apărea în dreapta sus, arătând setările și starea DST.
Time Offset	Selectați ora adăugată în minute când începe ora de vară.
Pornește pe	Specificați ora la care începe DST. Ceasul va fi setat înainte cu decalajul de timp pe care îl specificați.
Se termină pe	Specificați ora la care se termină ora de vară. Ceasul va fi reglat înapoi cu decalajul de timp pe care îl specificați.
Scenariul aplicației	Specificați scenariul de aplicare al site-ului. Pentru a vă personaliza scenariul, faceți clicCreați un scenariu nouîn lista derulantă.
Longitudine / Latitudine / Adresă	Configurați parametrii în funcție de locul în care se află site-ul. Aceste câmpuri sunt opționale.

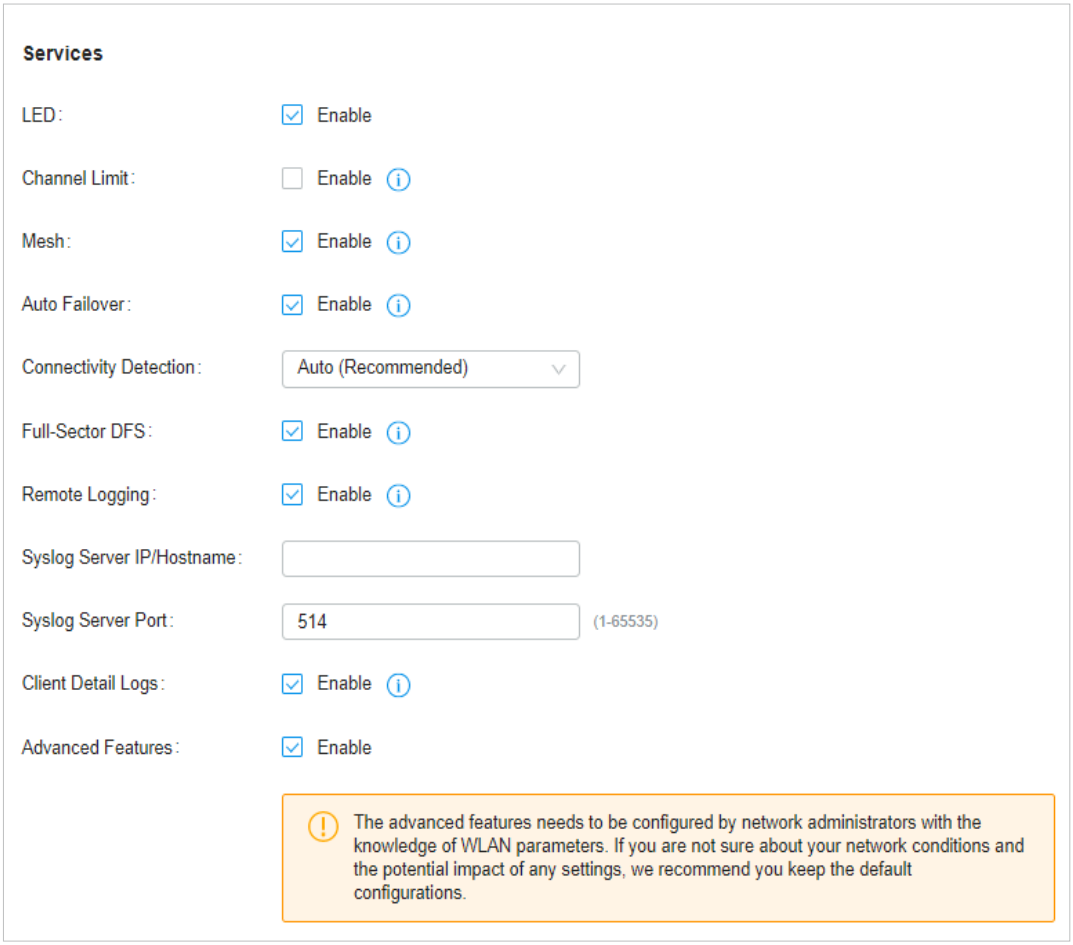
3. 2. 2 Servicii

Prezentare generală

În Servicii, puteți vizualiza și modifica caracteristicile aplicate dispozitivelor de pe site-ul curent. Cele mai multe funcții sunt aplicate tuturor dispozitivelor, cum ar fi LED-urile, în timp ce unele sunt aplicate numai EAP-urilor, cum ar fi Channel Limit și Mesh.

Configurare

Selectați un site din lista verticală aOrganizareîn colțul din dreapta sus, accesațiSetări>Sitesi configurați următoarele caracteristici pentru site-ul curent înServicii. ClicSalvați.



LED	Activați sau dezactivați LED-urile tuturor dispozitivelor din site. În mod implicit, dispozitivul urmează setarea LED-ului site-ului căruia îi aparține. Pentru a modifica setarea LED-ului pentru anumite dispozitive, consultațiCapitolul 5 Configurarea și monitorizarea dispozitivelor gestionate Omada .
Limită de canal	(Pentru AP-urile în aer liber) Când sunt activate, EAP-urile în aer liber nu utilizează canalul cu frecvența cuprinsă între 5150 MHz și 5350 MHz pentru a respecta limita de legile și reglementările locale din țările UE.
Plasă	Când este activat, EAP-urile care acceptă Mesh pot stabili rețeaua mesh la site.
Failover automat	(Pentru AP-urile din rețeaua mesh) Auto Failover este utilizată pentru a menține automat rețeaua mesh. Când este activat, controlerul va selecta automat o nouă legătură în sus fără fir pentru AP dacă legătura inițială a eșuat. Pentru a activa această funcție, activați mai întâi Mesh.

Detectare conectivitate	(Pentru punctele de acces din rețeaua mesh) Specificați metoda de detectare a conexiunii când este activată mesh. Într-o rețea mesh, AP-urile pot trimite pachete de solicitare ARP la o adresă IP fixă pentru a testa conectivitatea. Dacă legătura eșuează, starea acestor AP-uri se va schimba în Izolat. Auto (recomandat): Selectați această metodă și AP-urile mesh vor trimite pachete de solicitare ARP către gateway-ul implicit pentru detectare. Adresă IP personalizată: Selectați această metodă și specificați adresa IP dorită. AP-urile mesh vor trimite pachete de solicitare ARP la adresa IP personalizată pentru a testa conectivitatea. Dacă adresa IP a AP-ului se află în segmente de rețea diferite față de adresa IP personalizată, AP-ul va folosi adresa IP implicită a gateway-ului pentru detectare.
DFS cu sector complet	(Pentru AP-urile din rețeaua mesh) Cu această caracteristică activată, atunci când semnalele radar sunt detectate pe canalul curent de către un EAP, celelalte EAP-uri din rețeaua mesh vor fi de asemenea informate. Apoi, toate EAP-urile din rețeaua mesh vor trece la un canal alternativ. Pentru a activa această funcție, activați mai întâi Mesh.
Înregistrare de la distanță	Cu această caracteristică configurată, controlerul va trimite jurnalele de site generate către serverul de jurnal. Când este activat, sunt necesare următoarele elemente: IP server Syslog/Nume gazdă: Introduceți adresa IP sau numele de gazdă al serverului de jurnal. Port server Syslog: Introduceți portul serverului. Jurnalele de detalii ale clientului: Cu această caracteristică activată, jurnalele clienților vor fi trimise la serverul syslog.
Caracteristici avansate	(Pentru AP-uri) Când este activat, puteți configura mai multe funcții pentru AP-uri înCaracteristici avansate. Când sunt dezactivate, aceste caracteristici păstrează setările implicite. Pentru configurarea detaliată, consultați3. 2. 3 Caracteristici avansate.

3. 2. 3 Caracteristici avansate

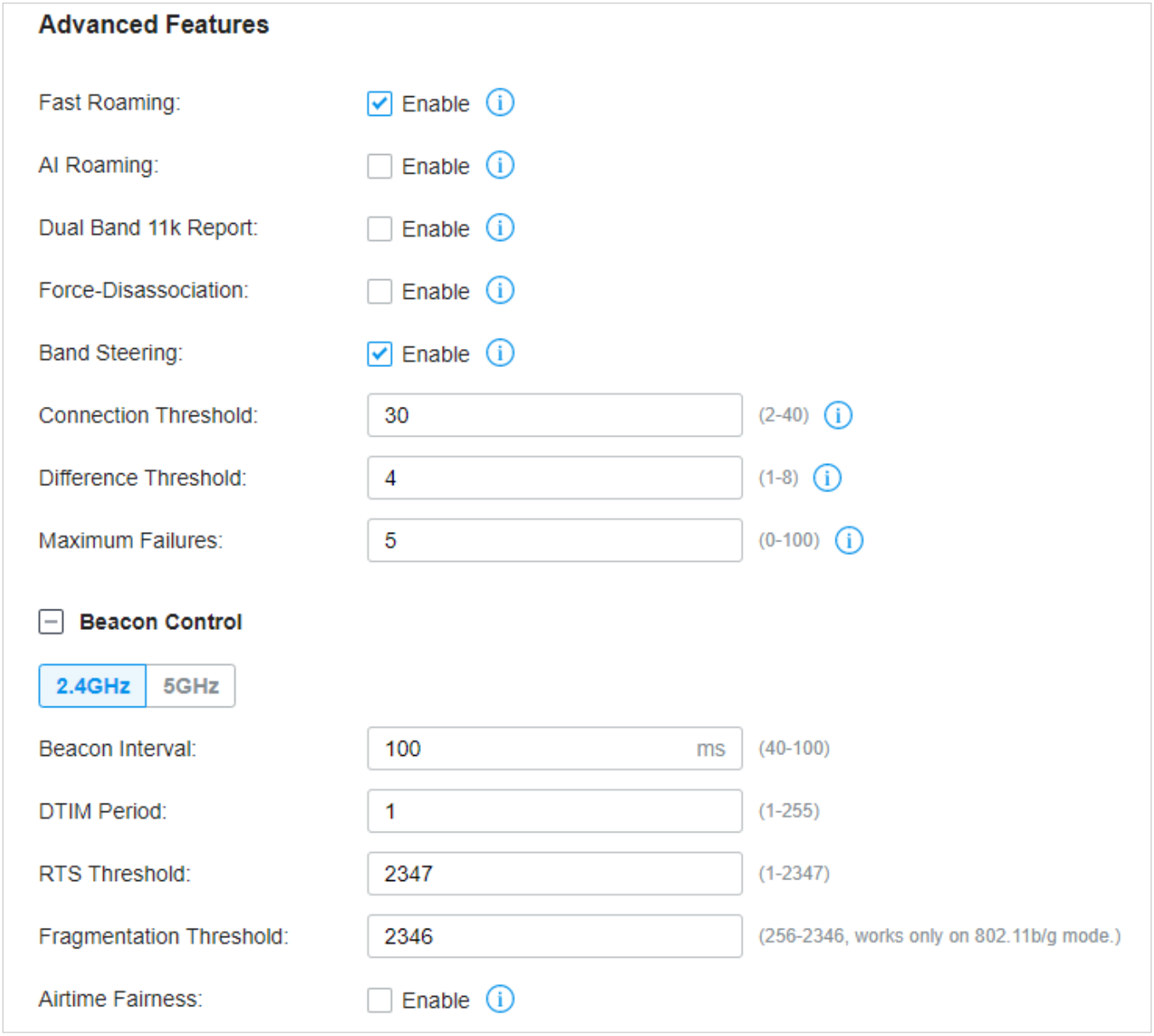
Prezentare generală

Funcțiile avansate includ roaming rapid, direcționare bandă și control al farului, care sunt aplicabile numai AP-urilor. Cu aceste caracteristici avansate configurate corect, puteți îmbunătăți stabilitatea, fiabilitatea și eficiența comunicării rețelei.

Se recomandă configurarea funcțiilor avansate de către administratorii de rețea cu cunoștințe WLAN. Dacă nu sunteți sigur de condițiile rețelei dvs. și de impactul potențial al tuturor setărilor, păstrațiCaracteristici avansatedezactivat înServiciipentru a utiliza configurațiile lor implicite.

Configurare

Selectați un site din lista verticală aOrganizareîn colțul din dreapta sus, accesațiSetări>Site, și activați Caracteristici avansateînServiciiprimul. Apoi configurați următoarele caracteristici înCaracteristici avansate. ClicSalvați.



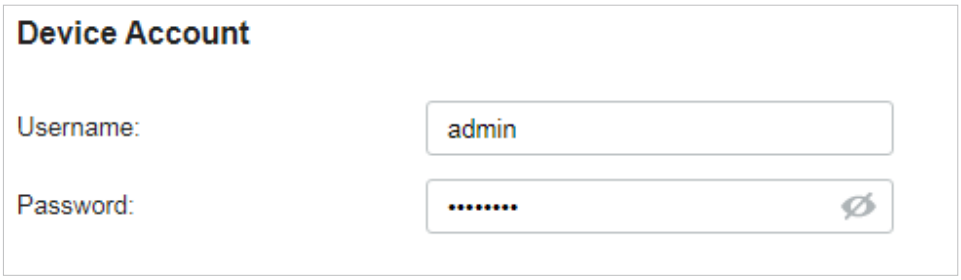
Roaming rapid	Cu această caracteristică activată, clienții wireless care acceptă 802.11k/v pot îmbunătăți experiența de roaming rapid atunci când se deplasează între diferite AP-uri. În mod implicit, este dezactivat. Această caracteristică este disponibilă pentru anumite dispozitive.
Roaming AI	Cu funcția Fast Roaming activată, puteți activa AI Roaming pentru a facilita Roamingul rapid, ceea ce îmbunătățește experiența de roaming a clienților fără fir care acceptă 802.11k/v. Această caracteristică este disponibilă pentru anumite dispozitive.
Raport dual band 11k	Când este dezactivat, controlerul oferă o listă de vecini care conține numai AP-uri vecine din aceeași bandă cu care este asociat clientul. Când este activat, controlerul oferă o listă de vecini care conține puncte de acces vecine în ambele benzi de 2,4 GHz și 5 GHz. Această caracteristică este disponibilă numai când este activată Roaming rapid. În mod implicit, este dezactivat.
Forța-Disociere	Cu această funcție dezactivată, AP-ul emite o sugestie de roaming 802.11v numai atunci când calitatea conexiunii unui client scade sub pragul predefinit și există o opțiune mai bună de AP, dar dacă să roaming sau nu este determinat de client. Cu această caracteristică activată, AP-ul va forța să disocieze clientul dacă nu se reasociază cu un alt AP. Această caracteristică este disponibilă numai când este activată Roaming rapid. În mod implicit, este dezactivat.
Direcție bandă	Band Steering poate ajusta numărul de clienți pe benzile de 2,4 GHz și 5 GHz pentru a oferi o experiență wireless mai bună. Când este activat, clienții dual-band vor fi direcționați către banda de 5 GHz în funcție de parametrii configurați. Cu setări adecvate, Band Steering poate îmbunătăți performanța rețelei, deoarece banda de 5 GHz acceptă un număr mai mare de canale care nu se suprapun și este mai puțin zgomotoasă. În mod implicit, este dezactivat.

Controlul farului	Balizele sunt transmise periodic de către EAP pentru a anunța prezența unui wireless rețea pentru clienți. Faceți clic pe , selectați banda și configurați următorii parametri ai Beacon Control. Interval de semnalizare: Specificați cât de des AP-urile trimit o baliză către clienți. În mod implicit, este 100. Perioada DTIM: specificați cât de des verifică clienții pentru datele stocate în tampon care se află încă pe EAP în așteptare. În mod implicit, clienții le verifică la fiecare baliză. DTIM (Delivery Traffic Indication Message) este conținut în unele cadre Beacon care indică dacă EAP-ul are date tampon pentru dispozitivele client. Un interval DTIM excesiv poate reduce performanța aplicațiilor multicast, așa că vă recomandăm să păstrați intervalul implicit, 1. Pragul RTS: RTS (Request to Send) poate asigura o transmisie eficientă a datelor prin evitarea conflictului de pachete. Dacă un client dorește să trimită un pachet mai mare decât pragul, mecanismul RTS va fi activat pentru a întârzia pachetele altor clienți din aceeași rețea fără fir. Vă recomandăm să păstrați pragul implicit, care este 2347. Dacă specificați o valoare de prag scăzută, mecanismul RTS poate fi activat mai des pentru a recupera rețeaua de la posibile interferențe sau coliziuni. Cu toate acestea, consumă și mai multă lățime de bandă și reduce debitul pachetului. Pragul de fragmentare: Fragmentarea poate limita dimensiunea pachetelor transmise prin rețea. Dacă un pachet care urmează să fie trimis depășește pragul de Fragmentare, funcția Fragmentare va fi activată, iar pachetul va fi fragmentat în mai multe pachete. În mod implicit, pragul este 2346. Fragmentarea ajută la îmbunătățirea performanței rețelei dacă este configurată corect. Cu toate acestea, un prag de fragmentare prea scăzut poate duce la performanțe wireless slabe din cauza traficului de mesaje crescut și a muncii suplimentare de împărțire și reasamblare a cadrelor. Corectitudinea timpului de difuzare: Cu această opțiune activată, fiecare client care se conectează la EAP poate obține aceeași perioadă de timp pentru a transmite date, astfel încât clienții cu rată scăzută de date să nu ocupe prea multă lățime de bandă a rețelei și performanța rețelei să se îmbunătățească în ansamblu. Vă recomandăm să activați această funcție în rețelele fără fir cu rate multiple.

3. 2. 4 Cont dispozitiv

Puteți specifica un cont de dispozitiv pentru toate dispozitivele adoptate de pe site în loturi. Odată ce dispozitivele sunt adoptate de controler, numele de utilizator și parola lor devin aceleași cu setările din Contul dispozitivului pentru a proteja comunicarea dintre controler și dispozitive. În mod implicit, numele de utilizator este admin și parola este generată aleatoriu.

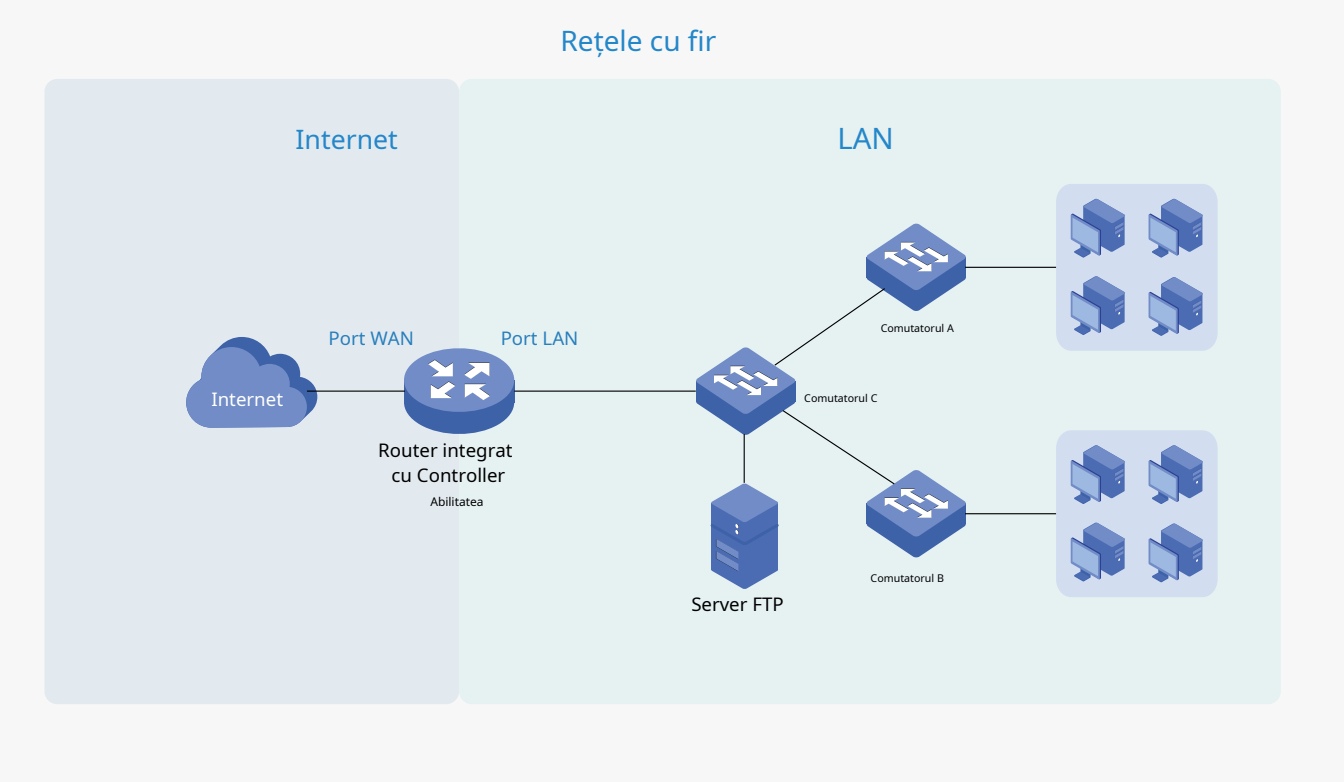
Selectați un site din lista derulantă aOrganizare. Mergi laSetări>Sitesi modificați numele de utilizator și parola înCont de dispozitiv. ClicSalvațiiar noul nume de utilizator și parola sunt aplicate tuturor dispozitivelor de pe site.



3. 3 Configurați rețelele cu fir

Rețelele cu fir permit dispozitivelor și clienților dvs. cu fir, inclusiv gateway-ul, comutatoarele, EAP-urile și PC-urile să se conecteze între ele și la internet.

După cum se arată în figura următoare, rețelele cu fir constă din două părți: Internet și LAN.



Pentru Internet, determinați numărul de porturi WAN de pe gateway și modul în care acestea se conectează la internet. Puteți configura o conexiune IPv4 și o conexiune IPv6 la furnizorul dvs. de servicii de internet (ISP) în funcție de nevoile dvs. Parametrii conexiunii la internet pentru gateway depind de tipurile de conexiune pe care le utilizați. Pentru o conexiune IPv4, sunt disponibile următoarele tipuri de conexiune la internet: IP dinamic, IP static, PPPoE, L2TP și PPTP. Pentru o conexiune IPv6, sunt disponibile următoarele tipuri de conexiune la internet: IP dinamic (SLAAC/ DHCPv6), IP static, PPPoE, 6to4 Tunnel și Pass-Through (Bridge). Și, când sunt configurate mai multe porturi WAN, puteți configura Load Balancing pentru a optimiza utilizarea resurselor, dacă este necesar.

Pentru LAN, configurați rețeaua internă cu fir și modul în care dispozitivele dvs. se separă logic sau se conectează între ele prin intermediul VLAN-urilor și interfețelor. Caracteristicile LAN avansate includ IGMP Snooping, Server DHCP și Opțiuni DHCP, PoE, Rețea de voce, Control 802.1X, Izolarea portului, Spanning Tree, LLDP-MED și Controlul lățimii de bandă.

3. 3. 1 Configurați o conexiune la internet

Configurare

Pentru a configura o conexiune la internet, urmați acești pași:

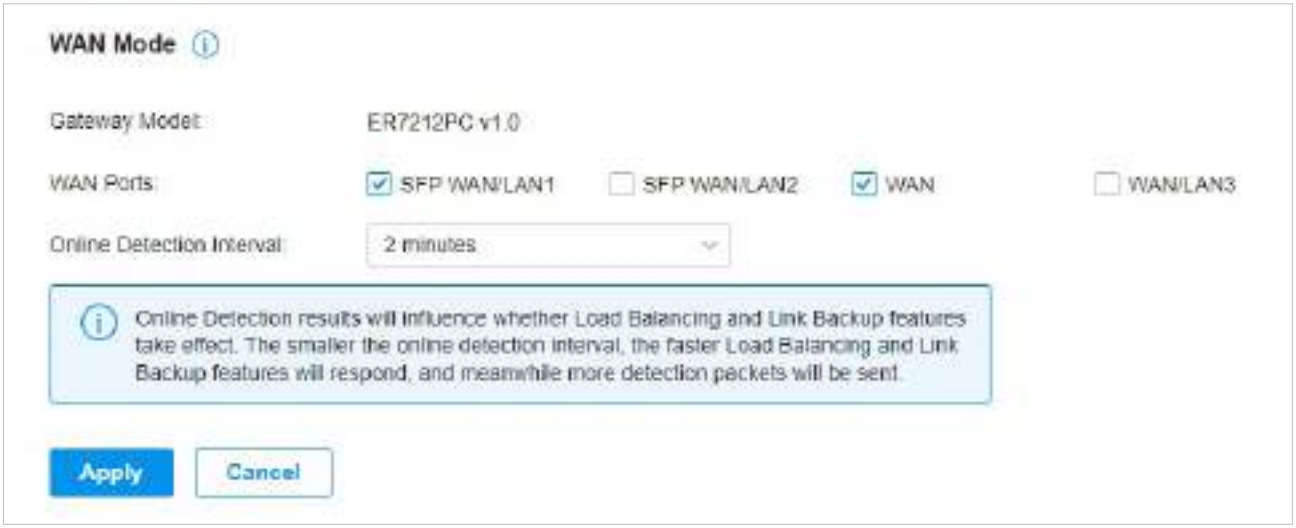
1)Configurați numărul de porturi WAN de pe gateway în funcție de nevoi.

2)Configurați conexiunile WAN. Puteți configura conexiunea IPv4, conexiunea IPv6 sau ambele.

3) (Opțional) Configurați Load Balancing dacă este configurat mai mult de un port WAN.

Selectați modul WAN > Configurați conexiunile WAN > (Opțional) Configurați încărcarea Balansare

Selectați un site din lista derulantă aOrganizare. Mergi laSetări>Rețele cu fir>Internetpentru a încărca următoarea pagină. ÎnModul WAN, configurați numărul de porturi WAN implementate de gateway și alți parametri. Apoi apasaaplica.



Model Gateway	Afișați modelul și versiunea gateway-ului.
Porturi WAN	Faceți clic pe caseta de validare pentru a activa portul ca port WAN. Pentru a configura mai multe porturi WAN, activați porturile unul câte unul. Rețineți că modificarea porturilor WAN va șterge automat configurațiile curente asociate cu porturile, iar gateway-ul va reporni.
Interval de detectare online	Selectați cât de des porturile WAN detectează starea conexiunii WAN. Dacă nu doriți să activați detectarea online, selectați Dezactivare. Rețineți că Load Balancing și Link Backup vor avea efecte pe baza rezultatelor detectării online. Configurați un interval adecvat de detectare online pentru a vă asigura că Load Balancing și Link Backup funcționează.

Selectați modul WAN > Configurați conexiunile WAN > (Opțional) Configurați încărcarea Balansare

Notă:

Numărul de porturi WAN configurabile este decis de modul WAN.

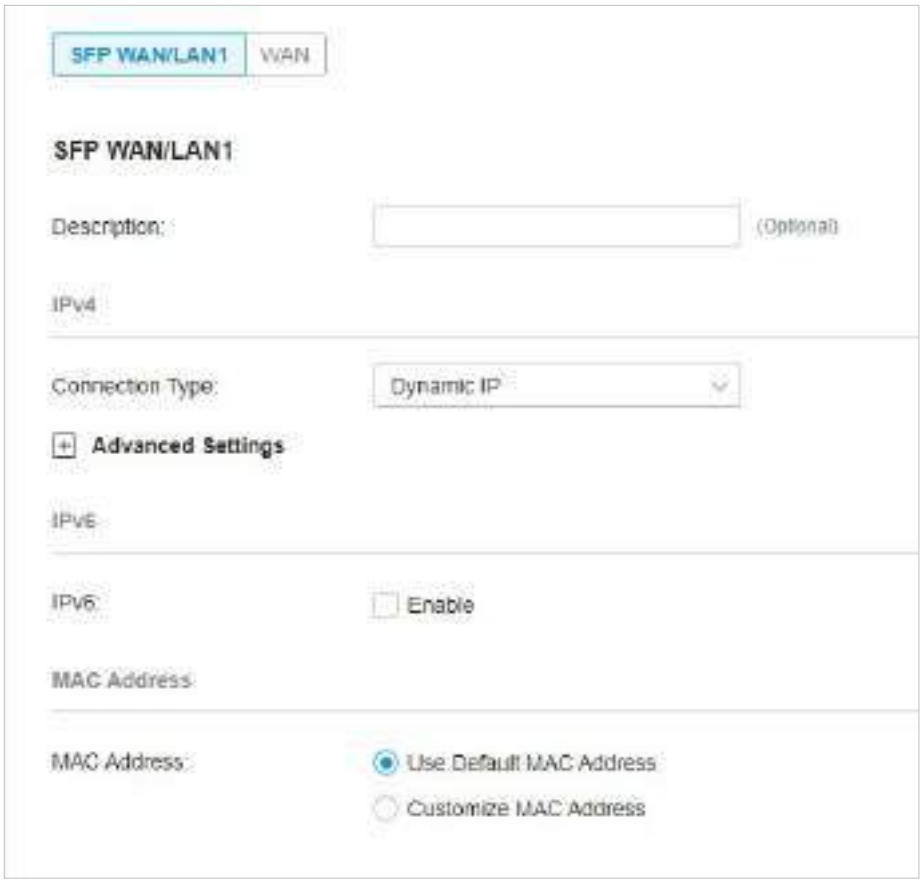
- Configurați conexiunea IPv4

Selectați un site din lista derulantă aOrganizare. Mergi laSetări>Rețele cu fir>Internet. Pentru conexiunile WAN, alegeți un tip de conexiune în funcție de serviciul oferit de ISP.

Tipul conexiunii	IP dinamic: Dacă ISP-ul dvs. atribuie automat adresa IP și parametrii corespunzători, alegeți IP dinamic. Adresa IP statică: Dacă ISP-ul dvs. vă oferă o adresă IP fixă și parametrii corespunzători, alegeți IP Static. PPPoE: Dacă ISP-ul dvs. vă oferă un cont PPPoE, alegeți PPPoE. L2TP: Dacă ISP-ul dvs. vă oferă un cont L2TP, alegeți L2TP. PPTP: Dacă ISP-ul dvs. vă oferă un cont PPTP, alegeți PPTP.

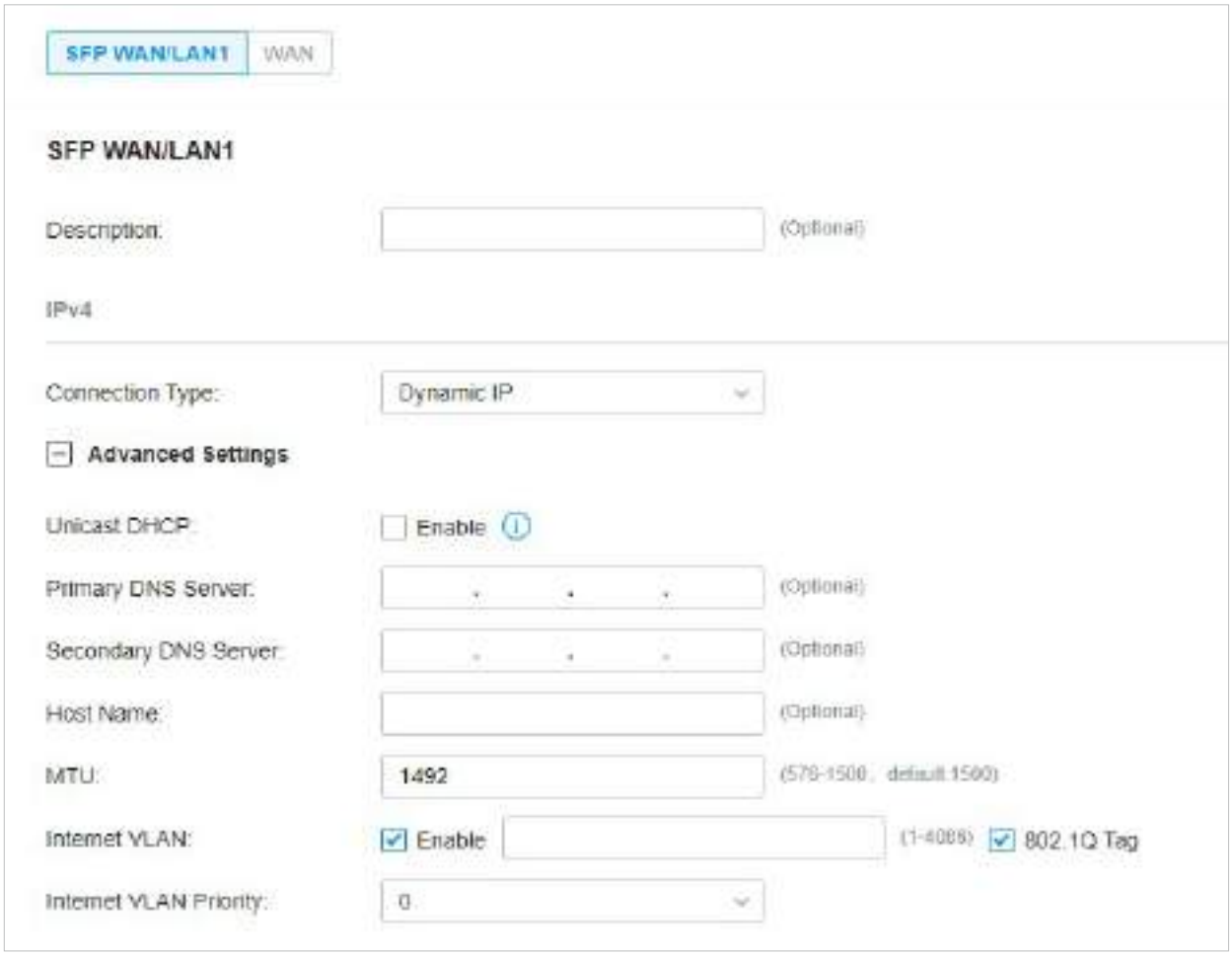
■ IP dinamic

1. Alegeți Tipul de conexiune ca IP dinamic și configurați următorii parametri.



Adresa mac	Utilizați adresa MAC implicită: portul WAN utilizează adresa MAC implicită pentru a configura conexiunea la internet. Este recomandat să utilizați adresa MAC implicită, dacă nu este necesar altfel. Personalizați adresa MAC: Portul WAN utilizează o adresă MAC personalizată pentru a configura conexiunea la internet și trebuie să specificați adresa MAC. De obicei, acest lucru este necesar atunci când ISP-ul dvs. a legat adresa MAC cu contul sau adresa IP. Dacă nu sunteți sigur, contactați ISP-ul.

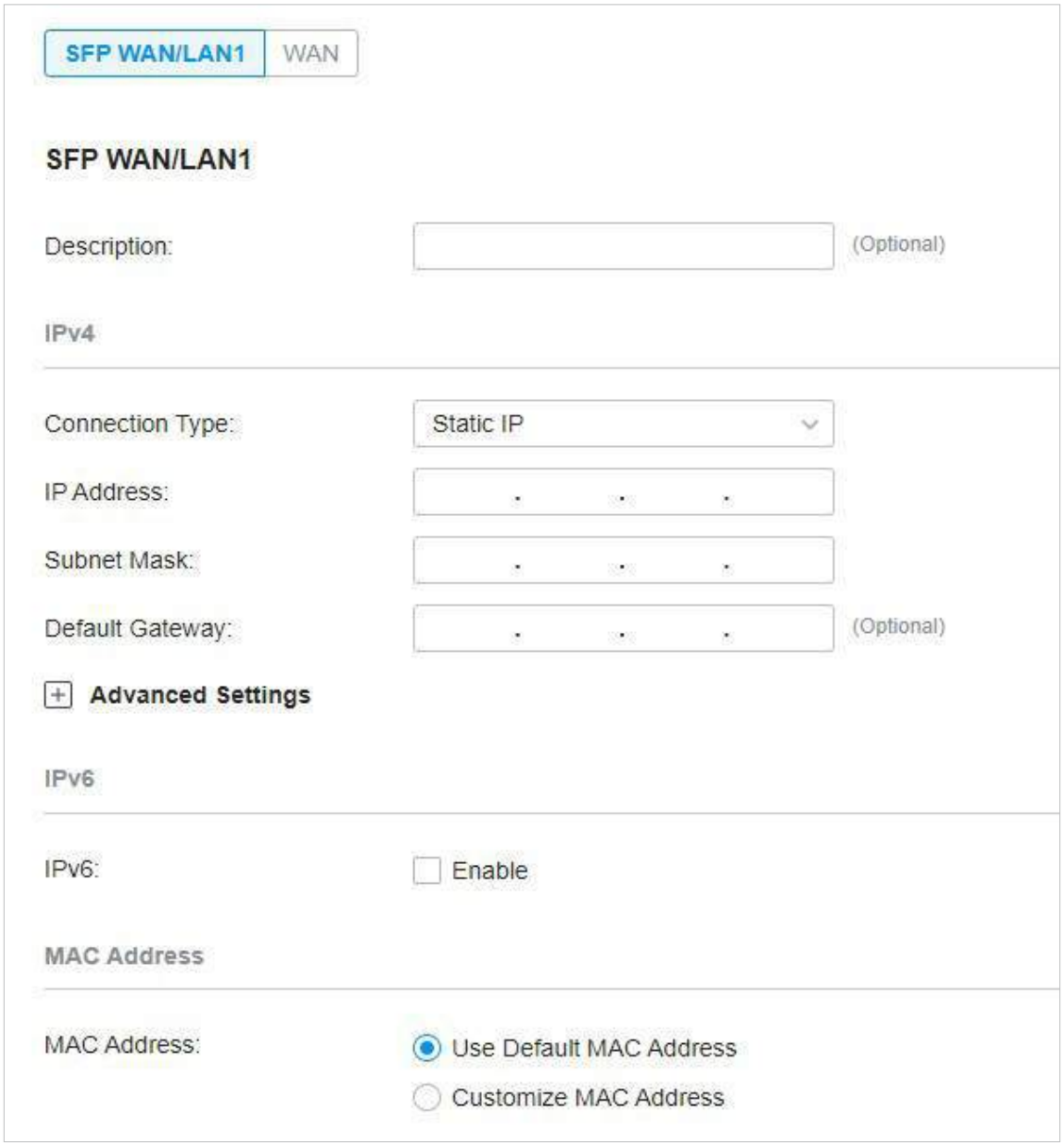
2. Faceți clic+ Setări avansatesi configurați următorii parametri. Apoi apasaaplica.



DHCP unicast	Cu această opțiune activată, gateway-ul va solicita serverului DHCP să atribuie adresa IP prin trimiterea de pachete DHCP unicast. De obicei, nu trebuie să activați opțiunea.
Server DNS primar / Server DNS secundar	Introduceți adresa IP a serverului DNS furnizată de ISP-ul dvs., dacă există.
Nume gazdă	Introduceți un nume pentru gateway.
MTU	Specificați MTU (Unitatea de transmisie maximă) a portului WAN. MTU este unitatea maximă de date transmisă în rețeaua fizică. Când tipul de conexiune este IP dinamic, MTU poate fi setat în intervalul 576-1500 de octeți. Valoarea implicită este 1500.
Internet VLAN	Adăugați portul WAN la un VLAN și trebuie să specificați VLAN-ul. În general, nu trebuie să-l configurați manual decât dacă este necesar de către furnizorul de servicii de internet.
Internet VLAN Prioritate	Prioritatea este disponibilă numai când VLAN-ul Internet este activat. Funcția Internet VLAN Priority ajută la prioritizarea traficului de internet în funcție de nevoile dvs. Puteți determina nivelul de prioritate pentru trafic specificând eticheta. Eticheta variază de la 0 la 7. Niciuna înseamnă că pachetul va fi transmis fără nicio operațiune.

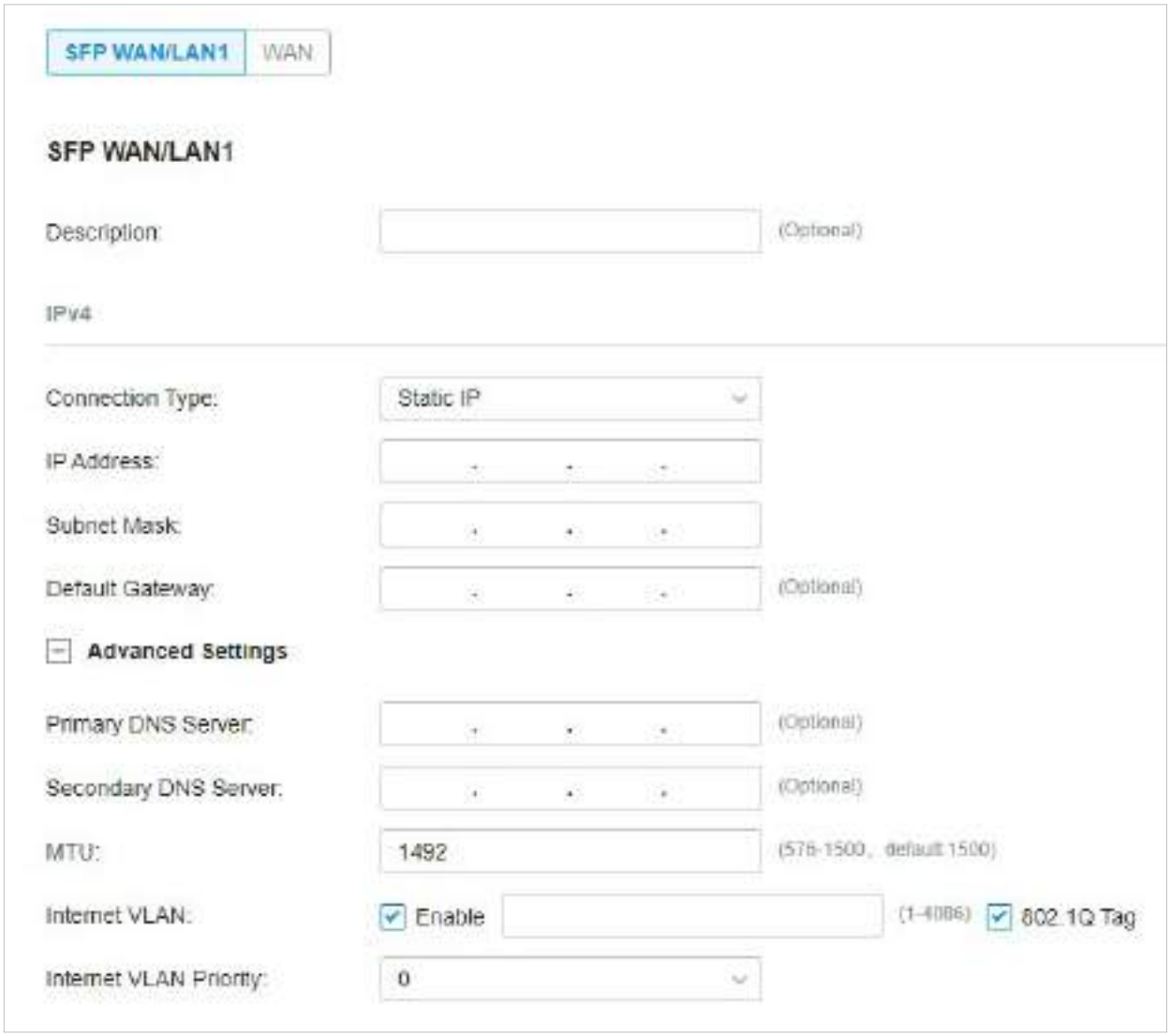
■ Adresa IP statică

1. Alegeți Tip de conexiune ca IP static și configurați următorii parametri.



Adresa IP	Introduceți adresa IP furnizată de ISP.
Mască de rețea	Introduceți masca de subrețea furnizată de ISP-ul dumneavoastră.
Gateway implicit	Introduceți gateway-ul implicit furnizat de ISP-ul dumneavoastră.
Adresa mac	Utilizați adresa MAC implicită: portul WAN utilizează adresa MAC implicită pentru a configura conexiunea la internet. Este recomandat să utilizați adresa MAC implicită, dacă nu este necesar altfel. Personalizați adresa MAC: Portul WAN utilizează o adresă MAC personalizată pentru a configura conexiunea la internet și trebuie să specificați adresa MAC. De obicei, acest lucru este necesar atunci când ISP-ul dvs. a legat adresa MAC cu contul sau adresa IP. Dacă nu sunteți sigur, contactați ISP-ul.

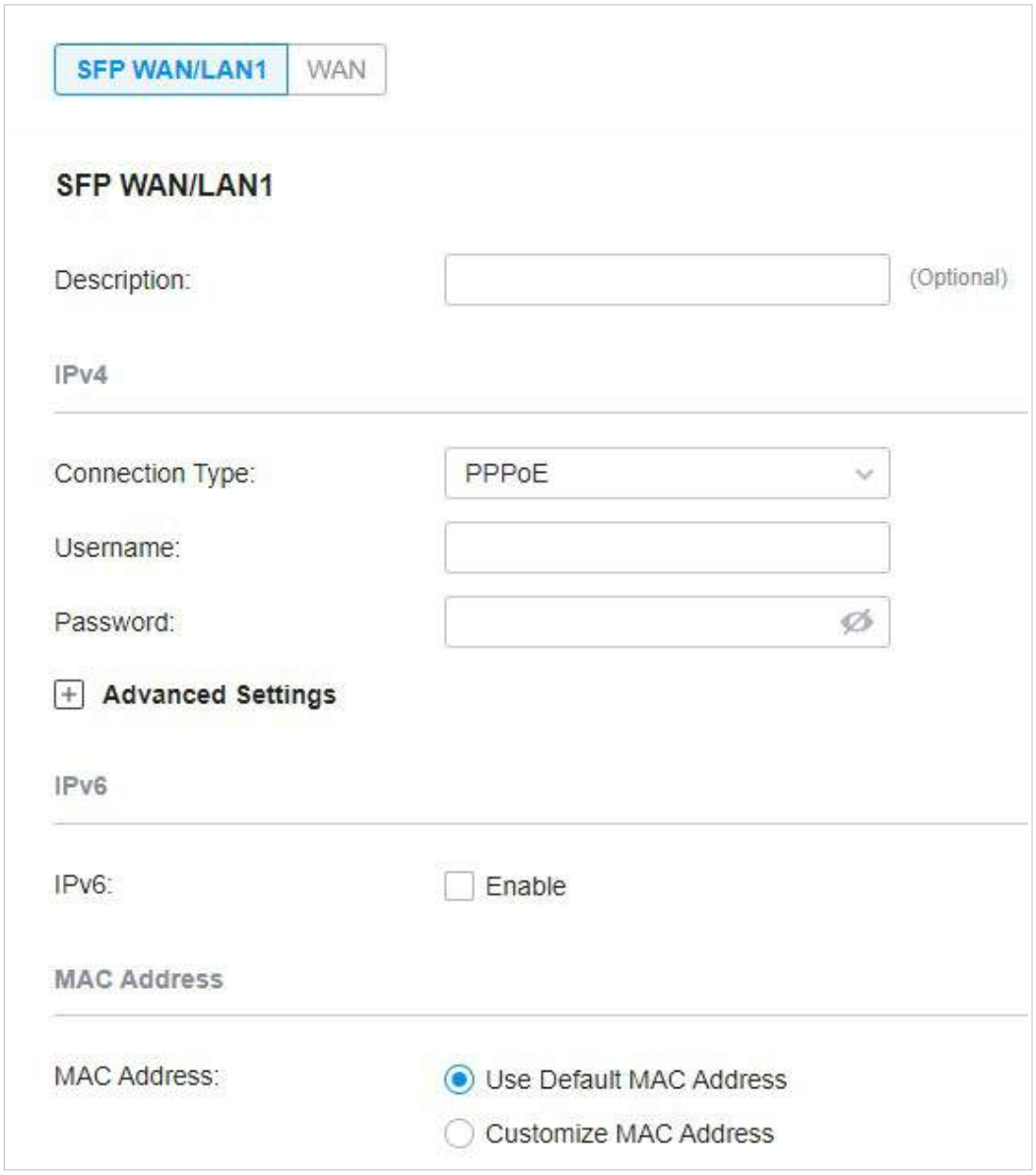
2. Faceți clic+ Setări avansatesi configurați următorii parametri. Apoi apasaaplica.



Server DNS primar / Server DNS secundar	Introduceți adresa IP a serverului DNS furnizată de ISP-ul dvs., dacă există.
MTU	Specificați MTU (Unitatea de transmisie maximă) a portului WAN. MTU este unitatea maximă de date transmisă în rețeaua fizică. Când tipul de conexiune este IP static, MTU poate fi setat în intervalul 576-1500 de octeți. Valoarea implicită este 1500.
Internet VLAN	Adăugați portul WAN la un VLAN și trebuie să specificați VLAN-ul. În general, nu trebuie să-l configurați manual decât dacă este necesar de către furnizorul de servicii de internet.
Internet VLAN Prioritate	Prioritatea este disponibilă numai când VLAN-ul Internet este activat. Funcția Internet VLAN Priority ajută la prioritizarea traficului de internet în funcție de nevoile dvs. Puteți determina nivelul de prioritate pentru trafic specificând eticheta. Eticheta variază de la 0 la 7. Niciuna înseamnă că pachetul va fi transmis fără nicio operațiune.

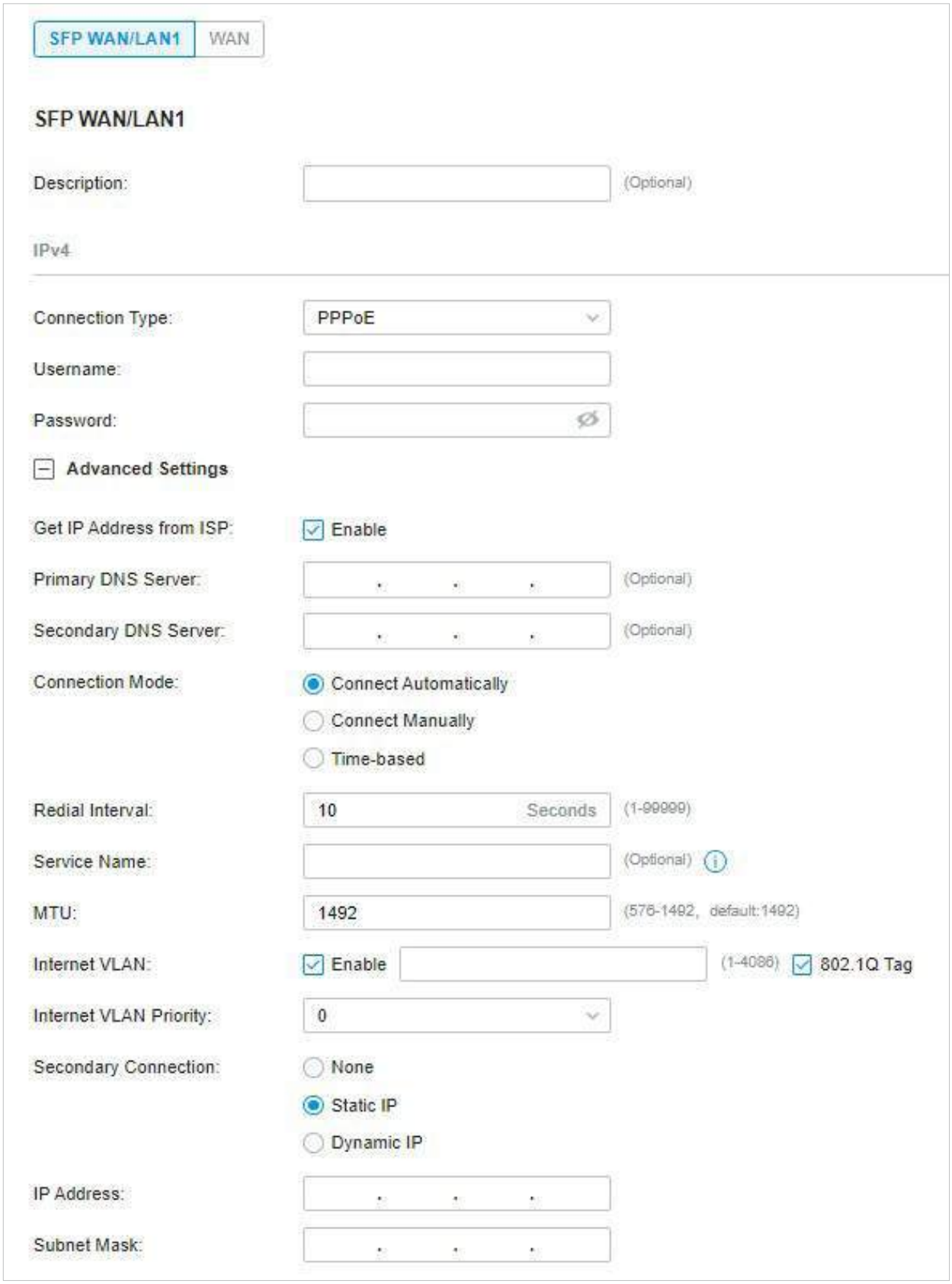
■ PPPoE

1. Alegeți Tipul de conexiune ca PPPoE și configurați următorii parametri.



Nume de utilizator	Introduceți numele de utilizator PPPoE furnizat de ISP-ul dumneavoastră.
Parola	Introduceți parola PPPoE furnizată de ISP-ul dumneavoastră.
Adresa mac	Utilizați adresa MAC implicită: portul WAN utilizează adresa MAC implicită pentru a configura conexiunea la internet. Este recomandat să utilizați adresa MAC implicită, dacă nu este necesar altfel. Personalizați adresa MAC: Portul WAN utilizează o adresă MAC personalizată pentru a configura conexiunea la internet și trebuie să specificați adresa MAC. De obicei, acest lucru este necesar atunci când ISP-ul dvs. a legat adresa MAC cu contul sau adresa IP. Dacă nu sunteți sigur, contactați ISP-ul.

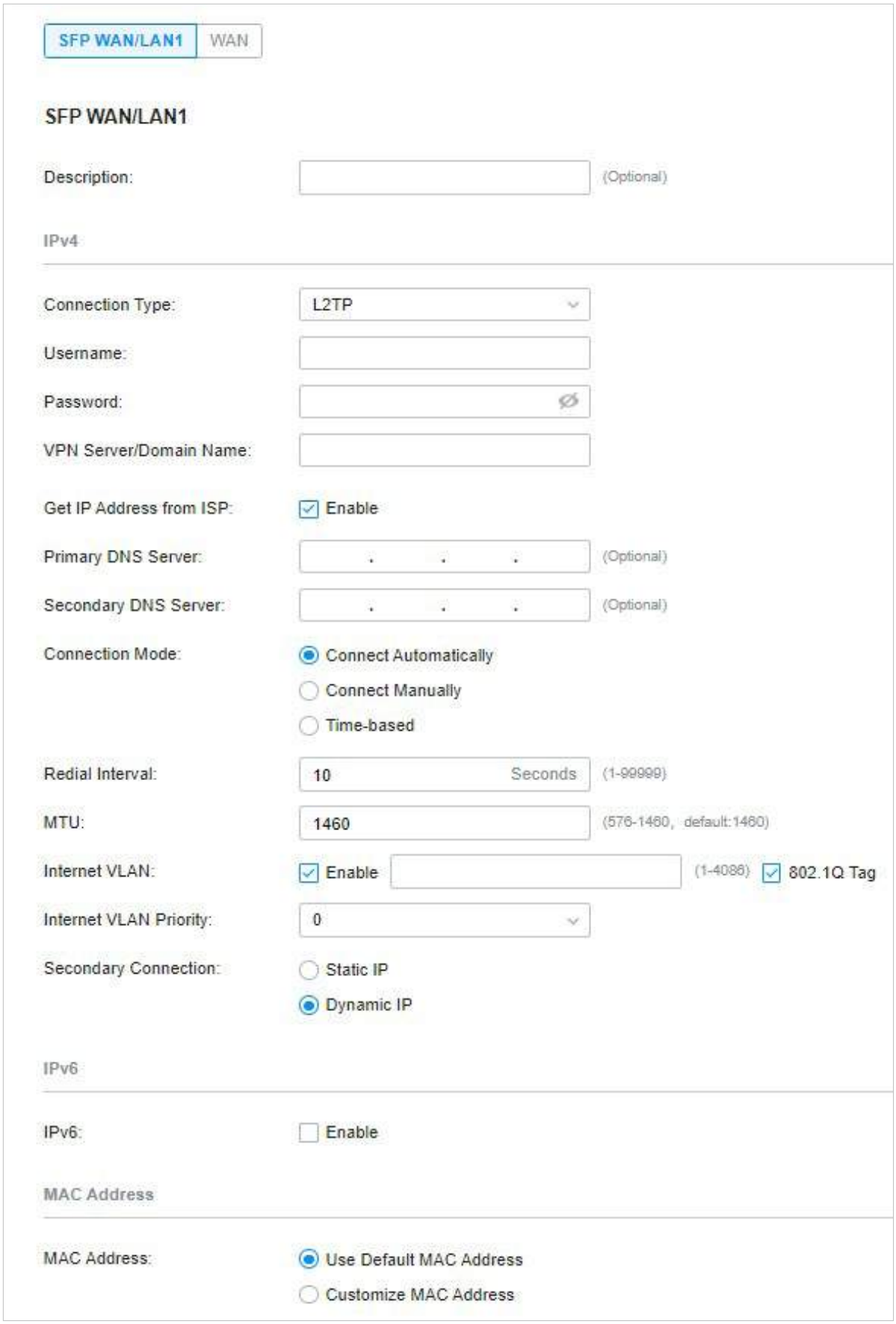
2. Faceți clic+ Setări avansatesi configurați următorii parametri. Apoi apasaaplica.



Obțineți adresa IP de la ISP	Cu această opțiune activată, gateway-ul primește adresa IP de la ISP la configurarea conexiunii WAN. Cu această opțiune dezactivată, trebuie să specificațiAdresa IPfurnizate de ISP-ul dumneavoastră.
Server DNS primar / Server DNS secundar	Introduceți adresa IP a serverului DNS furnizată de ISP-ul dvs., dacă există.
Modul de conectare	Conectare automata: Gateway-ul activează automat conexiunea atunci când conexiunea este întreruptă. Trebuie să specificațiInterval de reapelare, care decide cât de des încearcă gateway-ul să reapeleze după ce conexiunea este întreruptă. Conectați manual: Puteți activa sau opri manual conexiunea. Bazat pe timp: În perioada specificată, gateway-ul va activa automat conexiunea. Trebuie să specificațiInterval de timpcând conexiunea este întreruptă.
numele serviciului	Păstrați-l necompletat, cu excepția cazului în care ISP-ul dvs. vă solicită să îl configurați.
MTU	Specificați MTU (Unitatea de transmisie maximă) a portului WAN. MTU este unitatea maximă de date transmisă în rețeaua fizică. Când tipul de conexiune este PPPoE, MTU poate fi setat în intervalul 576-1492 de octeți. Valoarea implicită este 1492.
Internet VLAN	Adăugați portul WAN la un VLAN și trebuie să specificați VLAN-ul. În general, nu trebuie să-l configurați manual decât dacă este necesar de către furnizorul de servicii de internet.
Internet VLAN Prioritate	Prioritatea este disponibilă numai când VLAN-ul Internet este activat. Funcția Internet VLAN Priority ajută la prioritizarea traficului de internet în funcție de nevoile dvs. Puteți determina nivelul de prioritate pentru trafic specificând eticheta. Eticheta variază de la 0 la 7. Niciuna înseamnă că pachetul va fi transmis fără nicio operațiune.
Conexiune secundară	Conexiunea secundară este necesară de către unii ISP. Selectați tipul de conexiune cerut de ISP-ul dvs. Nici unul: Selectați această opțiune dacă conexiunea secundară nu este cerută de ISP-ul dumneavoastră. Adresa IP statică: Selectați această opțiune dacă ISP-ul dvs. vă oferă o adresă IP fixă și o mască de subrețea pentru conexiunea secundară. Trebuie să specificațiAdresa IPși Mască de rețea furnizate de ISP-ul dumneavoastră. IP dinamic: Selectați această opțiune dacă ISP-ul dvs. atribuie automat adresa IP și masca de subrețea pentru conexiunea secundară.

■ L2TP

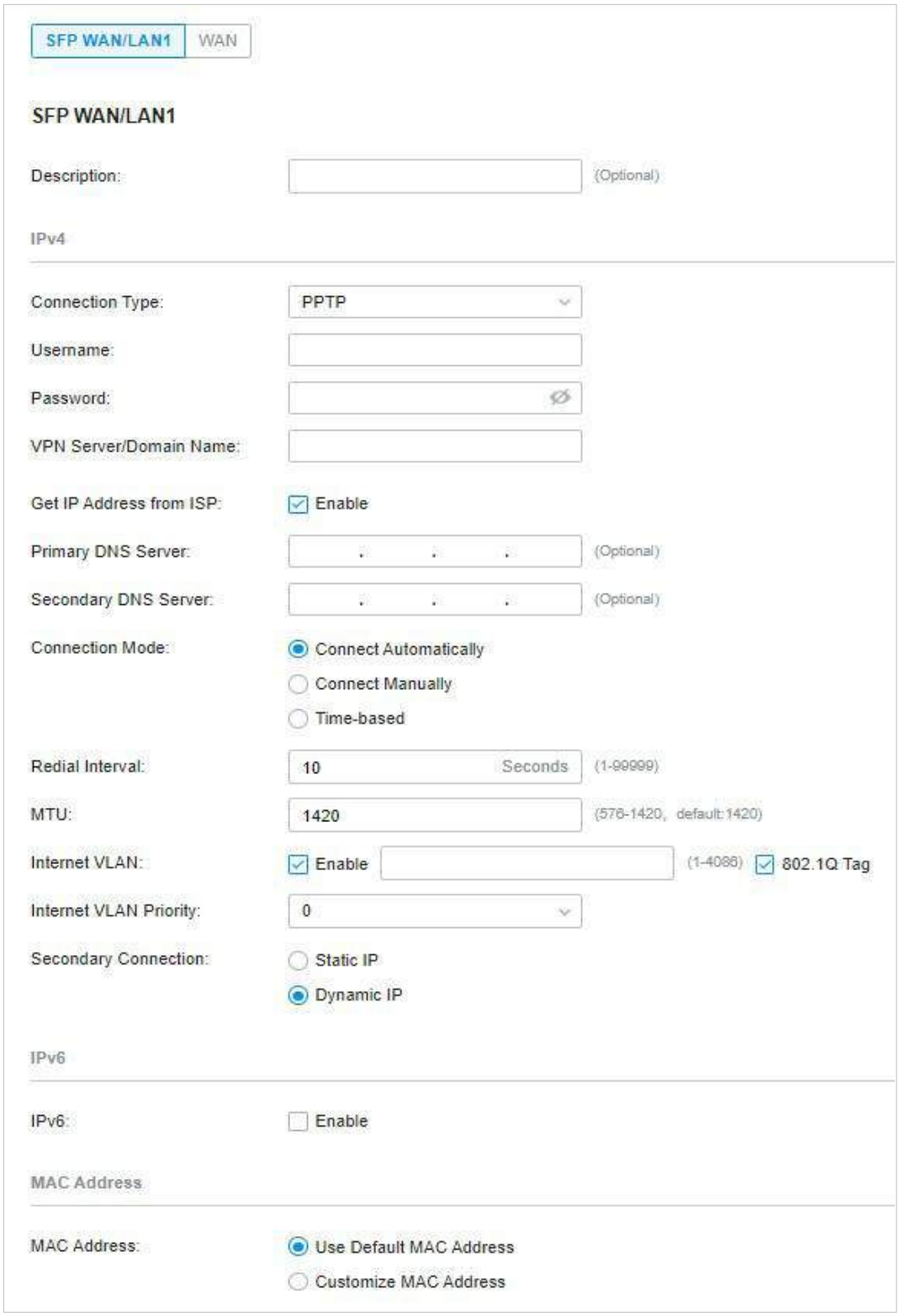
Alegeți Tipul de conexiune ca L2TP și configurați următorii parametri. Apoi apasaaplica.



Nume de utilizator	Introduceți numele de utilizator L2TP furnizat de ISP-ul dumneavoastră.
Parola	Introduceți parola L2TP furnizată de ISP.
Server VPN / Nume de domeniu	Introduceți serverul VPN/Numele de domeniu furnizat de ISP-ul dumneavoastră.
Obțineți adresa IP de la ISP	Cu această opțiune activată, gateway-ul primește adresa IP de la ISP la configurarea conexiunii WAN. Cu această opțiune dezactivată, trebuie să specificațiadresa IPfurnizate de ISP-ul dumneavoastră.
Server DNS primar / Server DNS secundar	Introduceți adresa IP a serverului DNS furnizată de ISP-ul dvs., dacă există.
Modul de conectare	Conectare automata: Gateway-ul activează automat conexiunea atunci când conexiunea este întreruptă. Trebuie să specificațiInterval de reapelare, care decide cât de des încearcă gateway-ul să reapeleze după ce conexiunea este întreruptă. Conectați manual: Puteți activa sau opri manual conexiunea. Bazat pe timp: În perioada specificată, gateway-ul va activa automat conexiunea. Trebuie să specificațiInterval de timpcând conexiunea este întreruptă.
MTU	Specificați MTU (Unitatea de transmisie maximă) a portului WAN. MTU este unitatea maximă de date transmisă în rețeaua fizică. Când tipul de conexiune este L2TP, MTU poate fi setat în intervalul 576-1460 de octeți. Valoarea implicită este 1460.
Internet VLAN	Adăugați portul WAN la un VLAN și trebuie să specificați VLAN-ul. În general, nu trebuie să-l configurați manual decât dacă este necesar de către furnizorul de servicii de internet.
Internet VLAN Prioritate	Prioritatea este disponibilă numai când VLAN-ul Internet este activat. Funcția Internet VLAN Priority ajută la prioritizarea traficului de internet în funcție de nevoile dvs. Puteți determina nivelul de prioritate pentru trafic specificând eticheta. Eticheta variază de la 0 la 7. Niciuna înseamnă că pachetul va fi transmis fără nicio operațiune.
Conexiune secundară	Selectați tipul de conexiune cerut de ISP-ul dvs. Adresa IP statică: Selectați această opțiune dacă ISP-ul dvs. vă oferă o adresă IP fixă și o mască de subrețea pentru conexiunea secundară. Trebuie să specificațiAdresa IP,Mască de rețea,Gateway implicit (Opțional),Server DNS primar (Opțional), șiServer DNS secundar (Opțional)furnizate de ISP-ul dumneavoastră. IP dinamic: Selectați această opțiune dacă ISP-ul dvs. atribuie automat adresa IP și masca de subrețea pentru conexiunea secundară.
Adresa mac	Utilizați adresa MAC implicită: portul WAN utilizează adresa MAC implicită pentru a configura conexiunea la internet. Este recomandat să utilizați adresa MAC implicită, dacă nu este necesar altfel. Personalizați adresa MAC: Portul WAN utilizează o adresă MAC personalizată pentru a configura conexiunea la internet și trebuie să specificați adresa MAC. De obicei, acest lucru este necesar atunci când ISP-ul dvs. a legat adresa MAC cu contul sau adresa IP. Dacă nu sunteți sigur, contactați ISP-ul.

■ PPTP

Alegeți Tipul de conexiune ca PPTP și configurați următorii parametri. Apoi apasaaplica.



Nume de utilizator	Introduceți numele de utilizator PPTP furnizat de ISP-ul dumneavoastră.
Parola	Introduceți parola PPTP furnizată de ISP-ul dumneavoastră.

Server VPN / Nume de domeniu	Introduceți serverul VPN/Numele de domeniu furnizat de ISP-ul dumneavoastră.
Obțineți adresa IP de la ISP	Cu această opțiune activată, gateway-ul primește adresa IP de la ISP la configurarea conexiunii WAN. Cu această opțiune dezactivată, trebuie să specificațiadresa IPfurnizate de ISP-ul dumneavoastră.
Server DNS primar / Server DNS secundar	Introduceți adresa IP a serverului DNS furnizată de ISP-ul dvs., dacă există.
Modul de conectare	Conectare automata: Gateway-ul activează automat conexiunea atunci când conexiunea este întreruptă. Trebuie să specificațiInterval de reapelare, care decide cât de des încearcă gateway-ul să reapeleze după ce conexiunea este întreruptă. Conectați manual: Puteți activa sau opri manual conexiunea. Bazat pe timp: În perioada specificată, gateway-ul va activa automat conexiunea. Trebuie să specificațiInterval de timpcând conexiunea este întreruptă.
MTU	Specificați MTU (Unitatea de transmisie maximă) a portului WAN. MTU este unitatea maximă de date transmisă în rețeaua fizică. Când tipul de conexiune este PPTP, MTU poate fi setat în intervalul 576-1420 octeți. Valoarea implicită este 1420.
Internet VLAN	Adăugați portul WAN la un VLAN și trebuie să specificați VLAN-ul. În general, nu trebuie să-l configurați manual decât dacă este necesar de către furnizorul de servicii de internet.
Internet VLAN Prioritate	Prioritatea este disponibilă numai când VLAN-ul Internet este activat. Funcția Internet VLAN Priority ajută la prioritizarea traficului de internet în funcție de nevoile dvs. Puteți determina nivelul de prioritate pentru trafic specificând eticheta. Eticheta variază de la 0 la 7. Niciuna înseamnă că pachetul va fi transmis fără nicio operațiune.
Conexiune secundară	Selectați tipul de conexiune cerut de ISP-ul dvs. Adresa IP statică: Selectați această opțiune dacă ISP-ul dvs. vă oferă o adresă IP fixă și o mască de subrețea pentru conexiunea secundară. Trebuie să specificațiAdresa IP,Mască de rețea,Gateway implicit (Opțional),Server DNS primar (Opțional), șiServer DNS secundar (Opțional)furnizate de ISP-ul dumneavoastră. IP dinamic: Selectați această opțiune dacă ISP-ul dvs. atribuie automat adresa IP și masca de subrețea pentru conexiunea secundară.
Adresa mac	Utilizați adresa MAC implicită: portul WAN utilizează adresa MAC implicită pentru a configura conexiunea la internet. Este recomandat să utilizați adresa MAC implicită, dacă nu este necesar altfel. Personalizați adresa MAC: Portul WAN utilizează o adresă MAC personalizată pentru a configura conexiunea la internet și trebuie să specificați adresa MAC. De obicei, acest lucru este necesar atunci când ISP-ul dvs. a legat adresa MAC cu contul sau adresa IP. Dacă nu sunteți sigur, contactați ISP-ul.

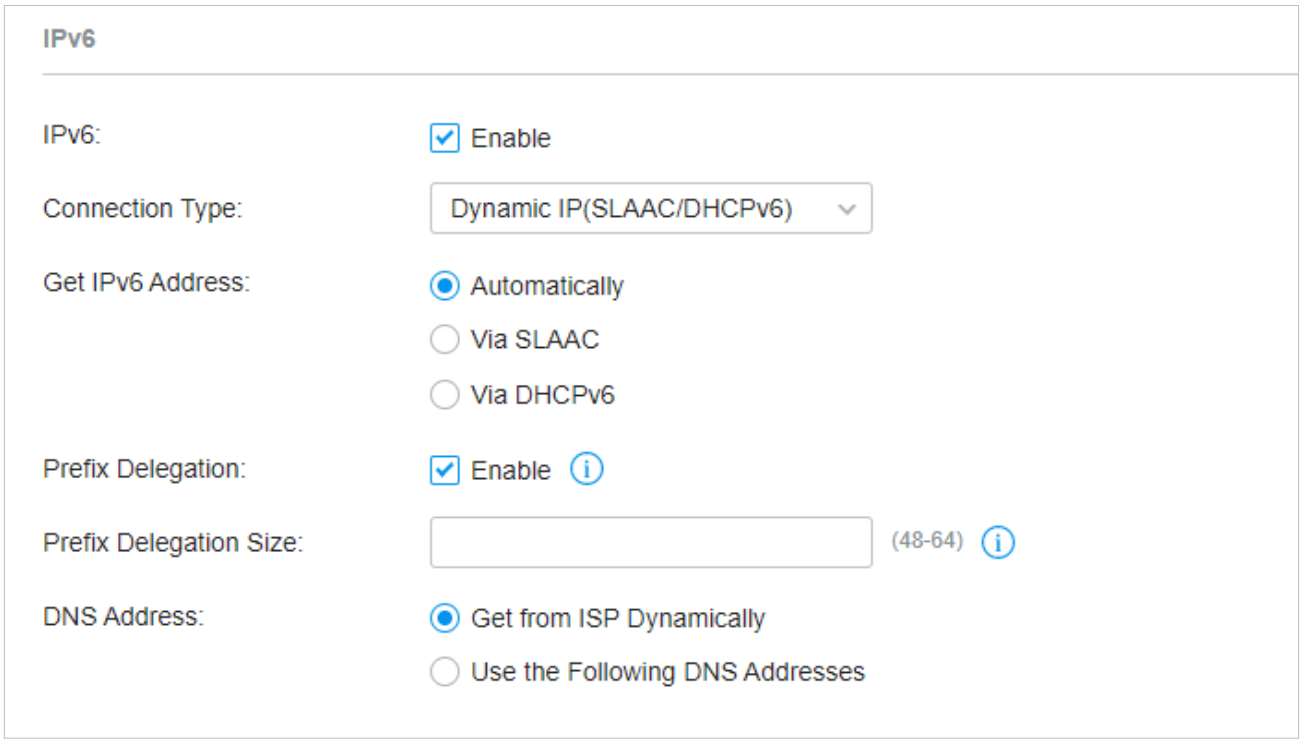
- Configurați conexiunea IPv6

Pentru conexiunile IPv6, bifați caseta pentru a activa conexiunea IPv6, selectați tipul de conexiune la internet conform cerințelor ISP-ului dumneavoastră.

Tipul conexiunii	IP dinamic (SLAAC/DHCPv6): Dacă ISP-ul dvs. utilizează atribuirea adresei IPv6 dinamice, fie DHCPv6, fie SLAAC+Stateless DHCP, selectați IP dinamic (SLAAC/DHCPv6). Adresa IP statică: Dacă ISP-ul dvs. vă oferă o adresă IPv6 fixă, selectați IP static. PPPoE: Dacă ISP-ul dvs. utilizează PPPoEv6 și oferă un nume de utilizator și o parolă, selectați PPPoE. Tunelul 6to4: Dacă ISP-ul dvs. utilizează implementarea 6to4 pentru alocarea adresei IPv6, selectați 6to4 Tunnel. 6to4 este un mecanism de tranziție pe internet pentru migrarea de la IPv4 la IPv6, un sistem care permite ca pachetele IPv6 să fie transmise printr-o rețea IPv4. Pachetul IPv6 va fi încapsulat în pachetul IPv4 și transmis către destinația IPv6 prin intermediul rețelei IPv4. Pass-through (Pont): În modul Pass-Through (Bridge), gateway-ul funcționează ca o punte transparentă. Pachetele IPv6 primite de la portul WAN vor fi transmise transparent către portul LAN și invers. Nu este necesar niciun parametru suplimentar.

■ IP dinamic (SLAAC/DHCPv6)

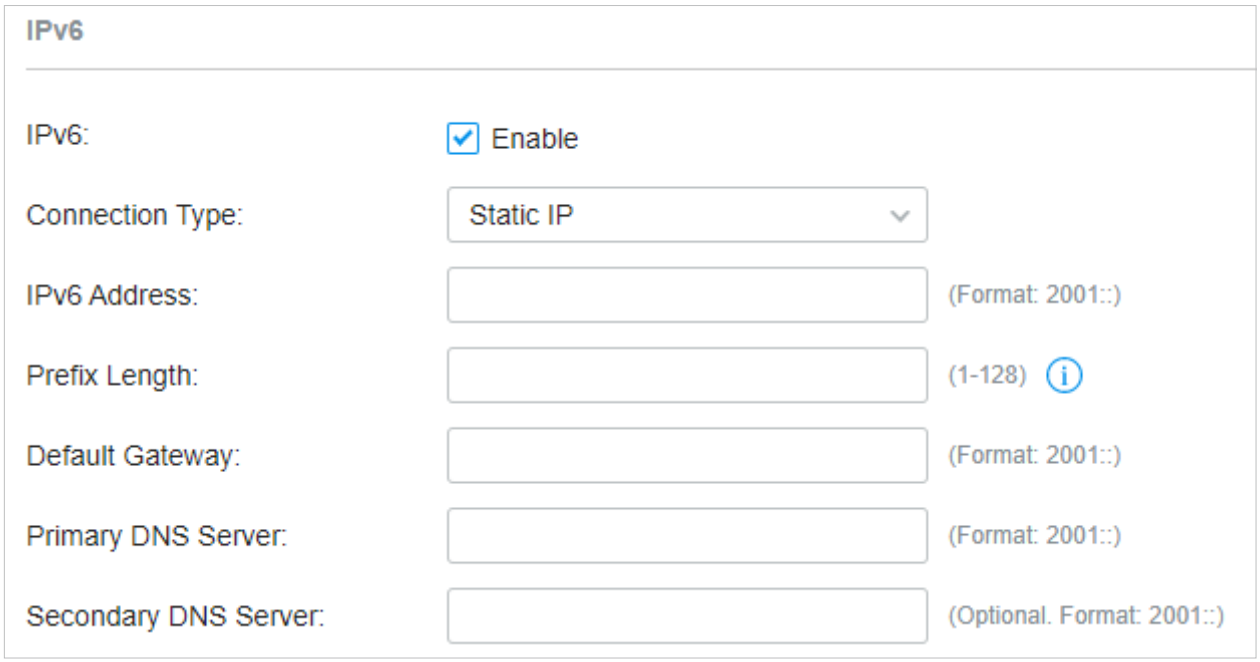
Alegeți Tipul de conexiune ca IP dinamic (SLAAC/DHCPv6) și configurați următorii parametri. Apoi apasaaplica.



Obțineți adresa IPv6	Selectați metoda potrivită prin care ISP-ul dvs. atribuie adresa IPv6 gateway-ului dvs. Automat: Cu această opțiune selectată, gateway-ul va selecta automat SLAAC sau DHCPv6 pentru a obține adrese IPv6. Prin SLAAC: Cu SLAAC (Configurare automată a adresei fără stat) selectată, ISP-ul dumneavoastră atribuie prefixul adresei IPv6 gateway-ului, iar gateway-ul generează automat propria sa adresă IPv6. De asemenea, ISP-ul dvs. atribuie gateway-ului alți parametri, inclusiv adresa serverului DNS. Prin DHCPv6: Cu DHCPv6 selectat, ISP-ul dvs. atribuie o adresă IPv6 și alți parametri, inclusiv adresa serverului DNS, gateway-ului folosind DHCPv6.
Delegarea prefixului	Selectați Activare pentru a obține un prefix de adresă de către serverul DHCPv6 de la ISP-ul dvs. sau Dezactivare pentru a desemna manual un prefix de adresă pentru portul dvs. LAN. Clienții din LAN vor primi o adresă IPv6 cu acest prefix.
Dimensiunea delegației prefixului	Cu Delegarea prefixului activată, introduceți Mărimea delegației prefixului pentru a determina lungimea prefixului de adresă. Dacă nu sunteți sigur de valoare, puteți întreba ISP-ul dvs.
Adresa DNS	Selectați dacă doriți să obțineți adresa DNS în mod dinamic de la ISP-ul dvs. sau să desemnați manual adresa DNS. Obțineți dinamic de la ISP: Adresa DNS va fi atribuită automat de către ISP. Utilizați următoarele adrese DNS: Introduceți adresa DNS furnizată de ISP.

■ Adresa IP statică

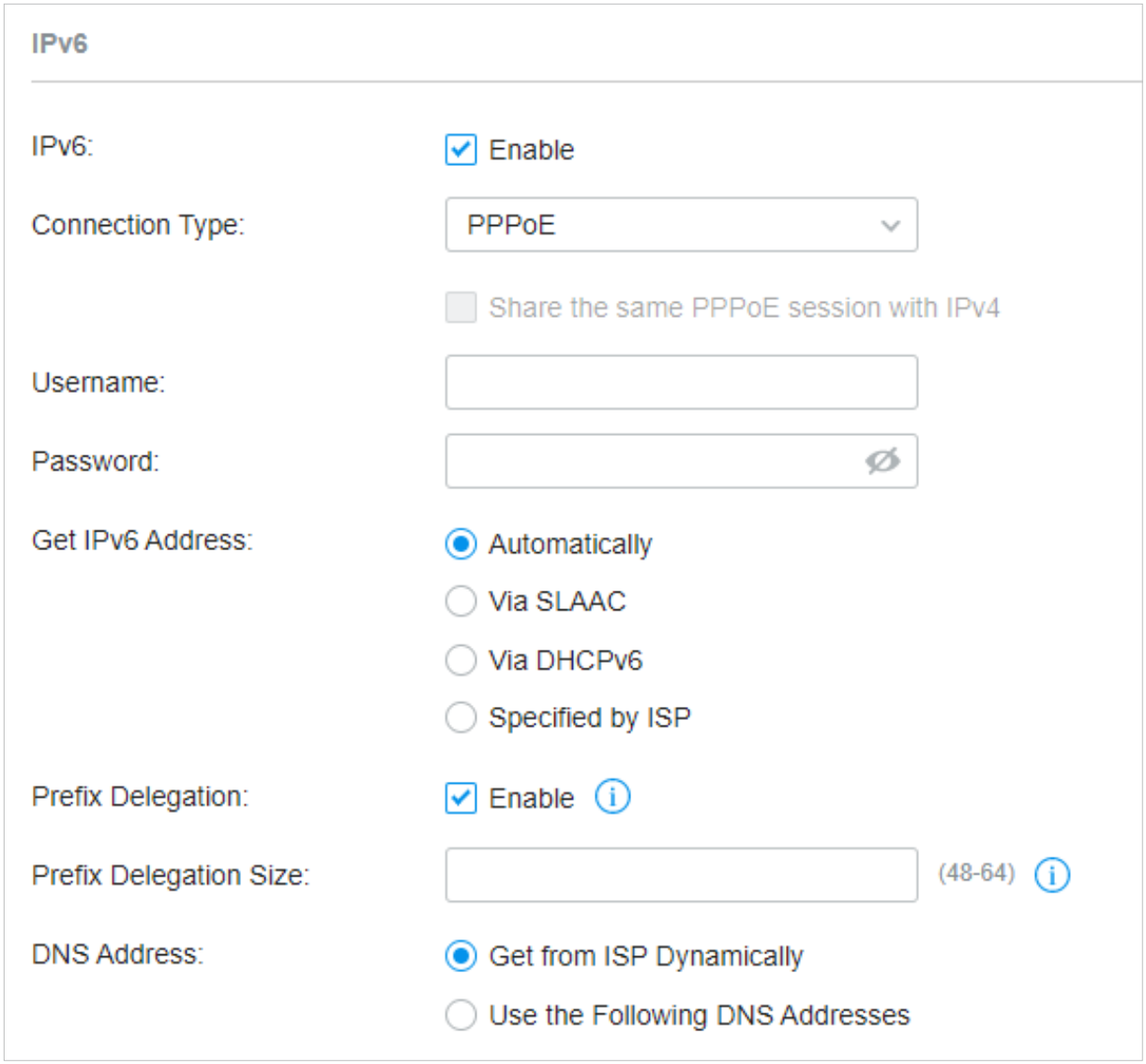
Alegeți Tipul de conexiune ca IP static și configurați următorii parametri. Apoi apasaaplica.



Adresa IPv6	Introduceți informațiile privind adresa IPv6 statică primite de la ISP.
Lungimea prefixului	Introduceți lungimea prefixului adresei IPv6 primite de la ISP.
Gateway implicit	Introduceți gateway-ul implicit furnizat de ISP-ul dumneavoastră.
Server DNS primar	Introduceți adresa IP a serverului DNS principal furnizat de ISP-ul dumneavoastră.
Server DNS secundar	(Opțional) Introduceți adresa IP a serverului DNS secundar, care oferă redundanță în cazul în care serverul DNS primar se defectează.

- PPPoE

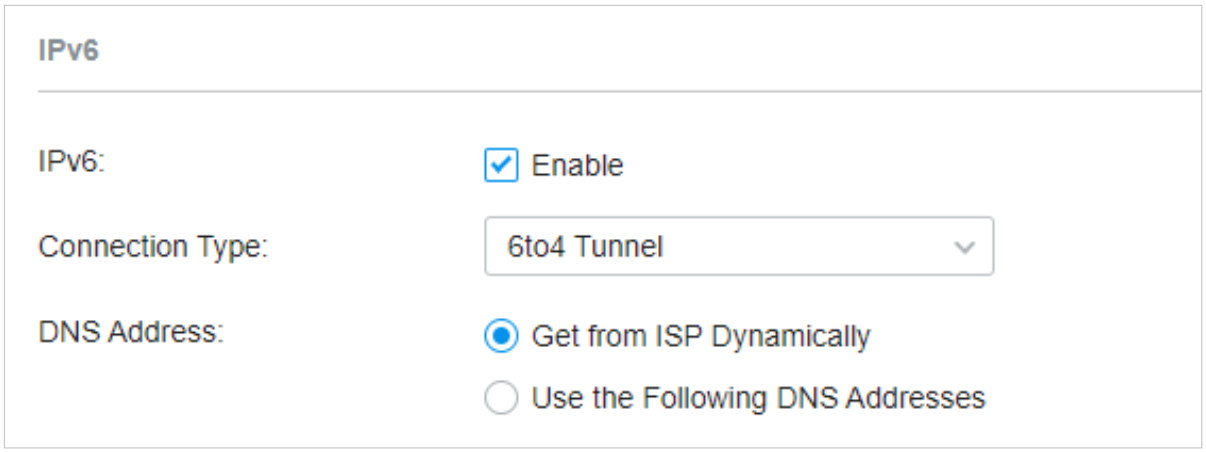
Alegeți Tipul de conexiune ca PPPoE și configurați următorii parametri. Apoi apasaaplica.



Partajați aceeași sesiune PPPoE cu IPv4	Dacă ISP-ul dvs. oferă un singur cont PPPoE atât pentru conexiunile IPv4, cât și pentru IPv6 și ați stabilit deja o conexiune IPv4 pe acest port WAN, puteți bifa caseta, atunci portul WAN va folosi sesiunea PPP a conexiunii IPv4 PPPoE pentru a obține adresa IPv6. În acest caz, nu este nevoie să introduceți numele de utilizator și parola contului PPPoE. Dacă ISP-ul dvs. furnizează două conturi PPPoE separate pentru conexiunile IPv4 și IPv6 sau dacă conexiunea IPv4 a acestui port WAN nu se bazează pe PPPoE, nu bifați caseta și introduceți manual numele de utilizator și parola pentru conexiunea IPv6.
Nume de utilizator	Introduceți numele de utilizator al contului dvs. PPPoE furnizat de ISP.
Parola	Introduceți parola contului dvs. PPPoE furnizată de ISP.
Obțineți adresa IPv6	Selectați metoda potrivită prin care ISP-ul dvs. atribuie adresa IPv6 gateway-ului dvs. Automat: Cu această opțiune selectată, gateway-ul va selecta automat metoda de a obține adrese IPv6 între SLAAC și DHCPv6. Prin SLAAC: Cu SLAAC (Configurare automată a adresei fără stat) selectată, ISP-ul dumneavoastră atribuie prefixul adresei IPv6 gateway-ului, iar gateway-ul generează automat propria sa adresă IPv6. De asemenea, ISP-ul dvs. atribuie gateway-ului alți parametri, inclusiv adresa serverului DNS. Prin DHCPv6: Cu DHCPv6 selectat, ISP-ul dvs. atribuie o adresă IPv6 și alți parametri, inclusiv adresa serverului DNS, gateway-ului folosind DHCPv6. Specificat de ISP: Cu această opțiune selectată, introduceți adresa IPv6 pe care o obțineți de la ISP.
Delegarea prefixului	Selectați Activare pentru a obține un prefix de adresă de către serverul DHCPv6 de la ISP-ul dvs. sau Dezactivare pentru a desemna manual un prefix de adresă pentru portul dvs. LAN. Clienții din LAN vor primi o adresă IPv6 cu acest prefix.
Dimensiunea delegației prefixului	Cu Delegarea prefixului activată, introduceți Mărimea delegației prefixului pentru a determina lungimea prefixului de adresă. Dacă nu sunteți sigur de valoare, puteți întreba ISP-ul dvs.
Adresa DNS	Selectați dacă doriți să obțineți adresa DNS în mod dinamic de la ISP-ul dvs. sau să desemnați manual adresa DNS. Obțineți dinamic de la ISP: Adresa DNS va fi atribuită automat de către ISP. Utilizați următoarele adrese DNS: Introduceți adresa DNS furnizată de ISP.

■ Tunelul 6to4

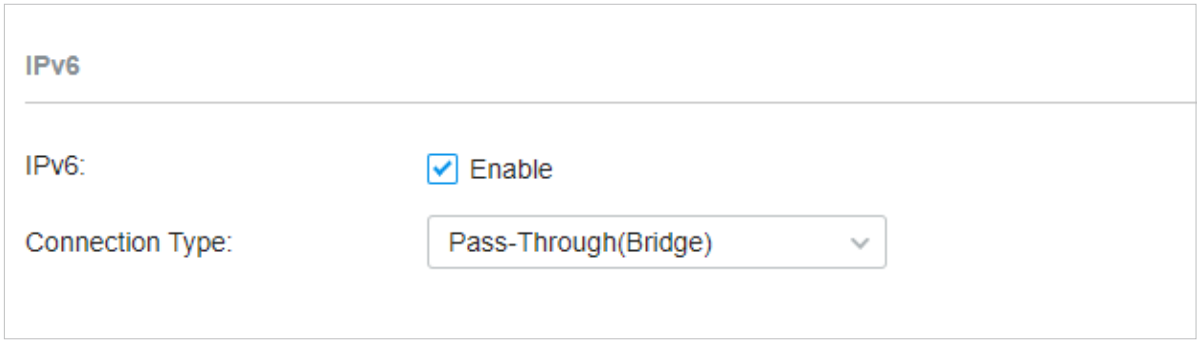
Alegeți tipul de conexiune ca tunel 6to4 și configurați următorii parametri. Apoi apasaaplica.



Adresa DNS	Selectați dacă doriți să obțineți adresa DNS în mod dinamic de la ISP-ul dvs. sau să desemnați manual adresa DNS. Obțineți dinamic de la ISP: Adresa DNS va fi atribuită automat de către ISP. Utilizați următoarele adrese DNS: Introduceți adresa DNS furnizată de ISP.

■ Pass-through (Pont)

Alegeți Tipul de conexiune ca Pass-Through (Pont) și nu este necesară nicio configurație pentru acest tip de conexiune Apoi faceți clicaplica.

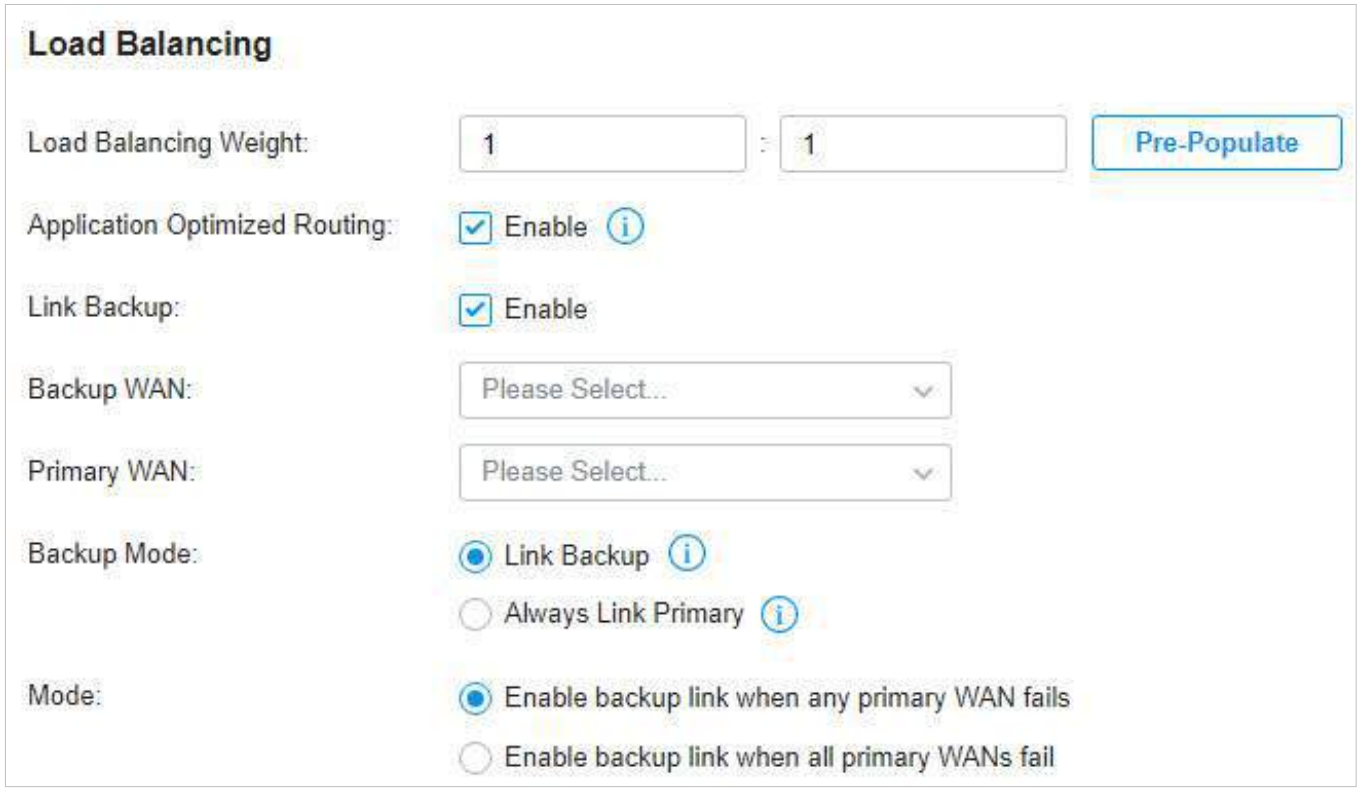


Selectați modul WAN > Configurați conexiunile WAN > (Opțional) Configurați încărcarea Balansare

Notă:

Loading Balancing este disponibil numai atunci când configurați mai mult de un port WAN.

Selectați un site din lista derulantă aOrganizare. Mergi laSetări>Rețele cu fir>Internetpentru a încărca următoarea pagină. ÎnEchilibrarea sarcinii, configurați următorii parametri și faceți clicaplica.



Greutate de echilibrare a sarcinii	Specificați raportul de trafic de rețea pe care îl transportă fiecare port WAN. Alternativ, puteți face clicPrepopulatepentru a testa viteza porturilor WAN și a completa automat raportul corespunzător în funcție de rezultatul testului.
Aplicație optimizată Dirijare	Cu Rutarea optimizată pentru aplicație activată, routerul va lua în considerare adresa IP sursă și adresa IP de destinație (sau portul de destinație) a pachetelor ca întreg și va înregistra portul WAN prin care trec. Apoi pachetele cu aceeași adresă IP sursă și adresa IP destinație (sau portul destinație) vor fi redirecționate către portul WAN înregistrat. Această caracteristică asigură că aplicațiile multiconectate funcționează corect.
Link Backup	Cu Link Backup activat, routerul va comuta automat toate sesiunile noi de la liniile abandonate la alta pentru a menține o rețea mereu online.
WAN de rezervă / WAN primar	Portul WAN de rezervă realizează o copie de rezervă a traficului pentru porturile WAN primare în condiția specificată.

Modul de rezervă	Backup link:Sistemul va comuta automat toate noile sesiuni de la linia abandonată la alta pentru a menține o rețea mereu conectată. Conectați întotdeauna principalul:Traficul este întotdeauna redirecționat prin portul WAN principal, cu excepția cazului în care eșuează. Sistemul va încerca să redirecționeze traficul prin portul WAN de rezervă atunci când eșuează și va comuta înapoi când își revine.
Modul	Selectați dacă activați legătura de rezervă atunci când orice WAN primar eșuează sau toate WAN-urile primare eșuează.

3. 3. 2 Configurați rețele LAN

Prezentare generală

TheLANfuncția vă permite să configurați rețeaua internă cu fir. Bazat pe 802.1Q VLAN, Omada Controller oferă o modalitate convenabilă și flexibilă de a separa și implementa rețeaua. Rețeaua poate fi segmentată în mod logic pe departamente, aplicații sau tipuri de utilizatori, fără a ține cont de locațiile geografice.

Configurare

Urmați instrucțiunile pentru a crea o rețea LAN:

1)Creați o rețea cu un scop specific. Pentru izolarea stratului 2, creați o rețea caVLAN.Pentru a realiza rutarea inter-VLAN, creați o rețea cainterfata,care este configurat cu o interfață VLAN.

2)Creați un profil de port pentru rețea. Profilul definește modul în care sunt gestionate pachetele atât în direcția de intrare, cât și în direcția de ieșire.

3)Atribuiți profilul portului la porturile dorite ale comutatorului pentru a activa LAN.

Notă:

O rețea implicită (VLAN implicit) numită LAN este preconfigurată ca interfață și este asociată cu toate porturile LAN ale Omada Gateway și toate porturile de comutare. ID-ul VLAN al rețelei implicite este 1. Rețeaua implicită poate fi editată, dar nu ștearsă.

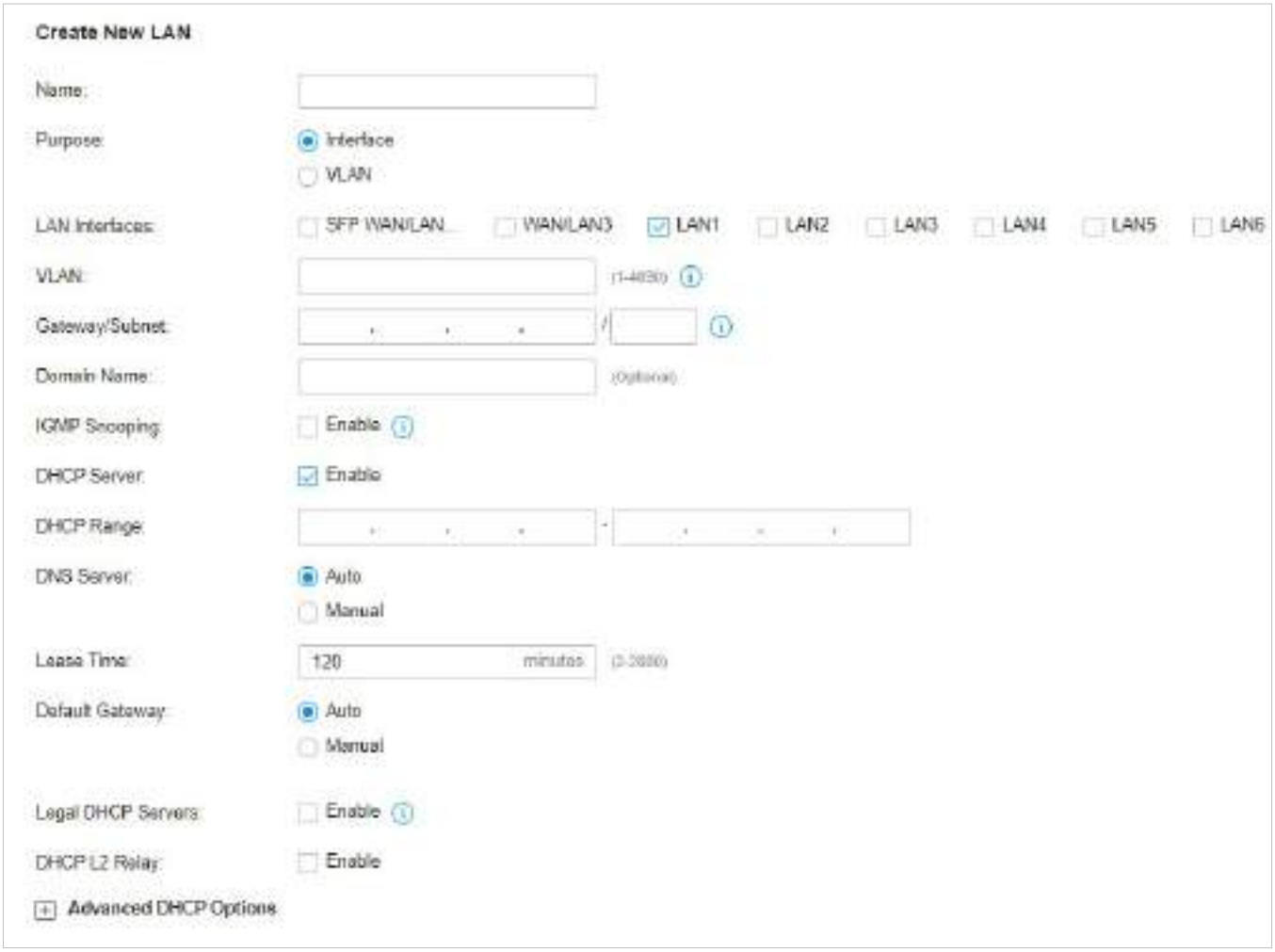
1. Selectați un site din lista derulantă aOrganizare. Mergi laSetări>Rețele cu fir>LAN> Rețelepentru a încărca următoarea pagină.

2. Faceți clic+ Creați un nou LANpentru a încărca următoarea pagină, introduceți un nume pentru a identifica rețeaua și selectați scopul rețelei.

Scop	Interfata:Creați rețeaua cu o interfață de nivel 3, care este necesară pentru rutarea inter-VLAN. VLAN:Creați rețeaua ca un VLAN de nivel 2.

3. Configurați parametrii în funcție de scopul rețelei.

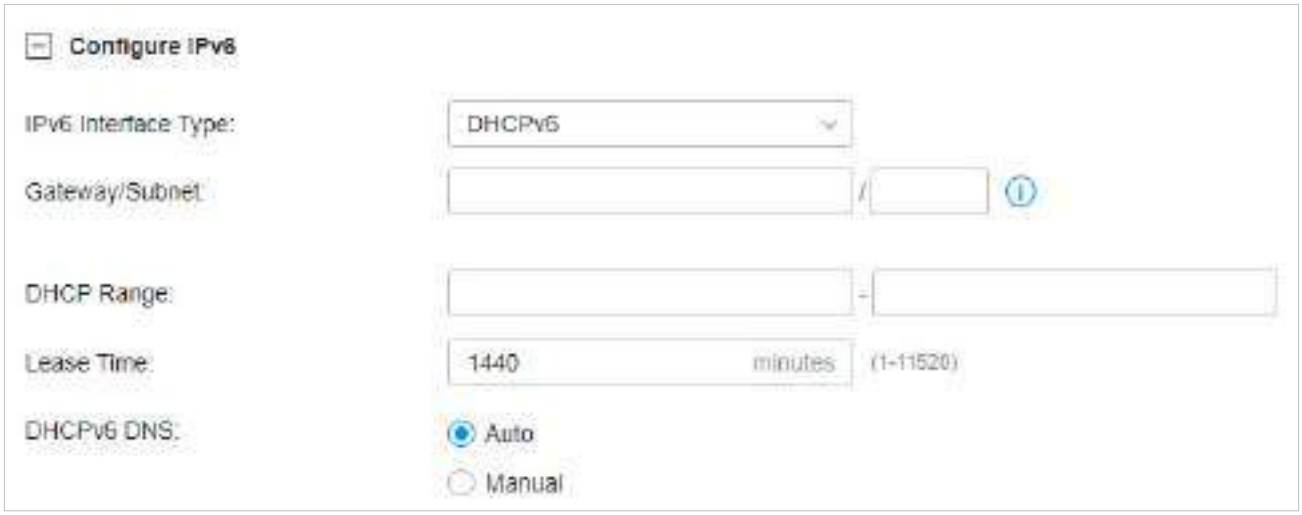
■ Interfață



Interfață LAN	Selectați interfețele fizice ale Omada Gateway cu care va fi asociată această rețea.
VLAN	Introduceți un ID VLAN cu valori între 1 și 4090. Fiecare VLAN poate fi identificat în mod unic prin ID-ul VLAN, care este transmis și primit ca etichetă IEEE 802.1Q într-un cadru Ethernet.
Gateway/Subnet	Introduceți adresa IP și masca de subrețea în format CIDR. Notația CIDR aici include adresa IP și masca de subrețea a gateway-ului implicit. Rezumatul informațiilor pe care le-ați introdus va apărea mai jos în timp real.
Numele domeniului	Introduceți numele domeniului.
Snooping IGMP	Faceți clic pe caseta de selectare pentru a monitoriza traficul IGMP (Internet Group Management Protocol) și, astfel, a gestiona traficul multicast.
Server DHCP	Faceți clic pe caseta de selectare pentru a permite Omada Gateway să servească drept server DHCP pentru această rețea. Un server DHCP atribuie adrese IP, server DNS, gateway implicit și alți parametri tuturor dispozitivelor din rețea. Debifați caseta dacă există deja un server DHCP în rețea.
Interval DHCP	Introduceți adresele IP de început și de sfârșit ale grupului de adrese DHCP în câmpurile furnizate. Pentru o operare rapidă, faceți clic peActualizați intervalul DHCPlângăGateway/ Subrețeaintrare pentru a obține intervalul de adrese IP populat automat și pentru a edita intervalul în funcție de nevoile dvs.
Server DNS	Selectați o metodă pentru a configura serverul DNS pentru rețea. Auto:Serverul DHCP atribuie automat serverul DNS pentru dispozitivele din rețea. Utilizează adresa IP specificată înGateway/Subnetintrare ca adresa serverului DNS. Manual:Specificați manual serverele DNS. Introduceți adresa IP a unui server în fiecare câmp de server DNS.
Timp de închiriere	Specificați cât timp un client poate folosi adresa IP atribuită din acest grup de adrese.
Gateway implicit	Introduceți adresa IP a gateway-ului implicit. Auto:Serverul DHCP atribuie automat gateway-ul implicit pentru dispozitivele din rețea. Utilizează adresa IP specificată în intrarea Gateway/Subnet ca adresă implicită de gateway. Manual:Specificați manual gateway-ul implicit. Introduceți în câmp adresa IP a gateway-ului implicit.
Servere DHCP legale	Faceți clic pe caseta de selectare pentru a specifica serverele DHCP legale pentru rețea. Cu serverele DHCP legale configurate, Omada Gateways și Switch-urile asigură că clienții primesc adrese IP numai de la serverele DHCP ale căror adrese IP sunt specificate aici.
Releu DHCP L2	Faceți clic pe caseta de selectare pentru a activa DHCP L2 Relay pentru rețea.
Opțiunea 60	Introduceți valoarea pentru Opțiunea DHCP 60. Clienții DHCP folosesc acest câmp pentru a identifica opțional tipul de furnizor și configurația unui client DHCP. În cea mai mare parte, este utilizat în scenariul în care AP-urile aplică pentru diferite adrese IP de la diferite servere, în funcție de nevoi.

Opțiunea 66	Introduceți valoarea pentru Opțiunea DHCP 66. Specifică informațiile serverului TFTP și acceptă o singură adresă IP a serverului TFTP.
Opțiunea 138	Introduceți valoarea pentru Opțiunea DHCP 138. Este utilizată în descoperirea dispozitivelor de către controlerul Omada.

Puteți configura conexiunile IPv6 pentru clienții LAN în funcție de nevoile dvs. Mai întâi, determinați metoda prin care gateway-ul atribuie adrese IPv6 clienților din rețeaua locală. Unii clienți pot accepta doar câteva dintre aceste tipuri de conexiune, așa că ar trebui să o alegeți în funcție de compatibilitatea clienților din rețeaua locală.



Tip de interfață IPv6	Configurați tipul de atribuire a adresei IPv6 clienților din rețeaua locală. Nici unul: Conexiunea IPv6 nu este activată pentru clienții din rețeaua locală. DHCPv6: gateway-ul atribuie o adresă IPv6 și alți parametri, inclusiv adresa serverului DNS, fiecărui client care utilizează DHCPv6. SLAAC + DHCP fără stat: Gateway-ul atribuie prefixul adresei IPv6 fiecărui client, iar clientul generează automat propria sa adresă IPv6. De asemenea, gateway-ul atribuie alți parametri, inclusiv adresa serverului DNS fiecărui client folosind DHCPv6. SLAAC+RDNSS: Gateway-ul atribuie prefixul adresei IPv6 fiecărui client, iar clientul generează automat propria sa adresă IPv6. De asemenea, gateway-ul atribuie alți parametri, inclusiv adresa serverului DNS fiecărui client utilizând opțiunea RDNSS din RA (Router Advertisement). A trece prin: Selectați acest tip dacă porturile WAN ale gateway-ului folosesc Pass-Through pentru conexiunile IPv6.
Cu DHCPv6 selectat, configurați următorii parametri.	
Gateway/Subnet	Introduceți adresa IP și masca de subrețea în format CIDR. Notația CIDR aici include adresa IP și masca de subrețea a gateway-ului implicit. Rezumatul informațiilor pe care le-ați introdus va apărea mai jos în timp real.

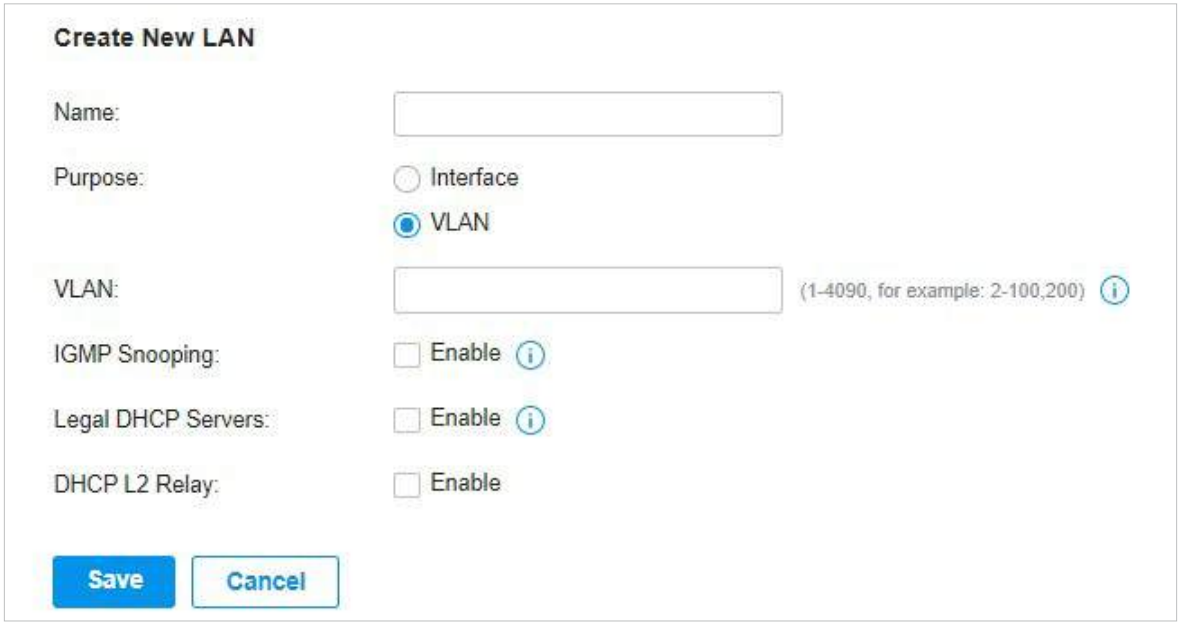
Interval DHCP	Introduceți adresele IP de început și de sfârșit ale grupului de adrese DHCP în câmpuri furnizate. Pentru o operare rapidă, faceți clic pe Update DHCP Range lângă Gateway/Subnet intrare pentru a obține intervalul de adrese IP populat automat și pentru a edita intervalul în funcție de nevoile dvs.
Timp de închiriere	Această intrare determină cât timp rămâne valabilă adresa IPv6 atribuită. Fie păstrați valoarea implicită de 1440 de minute, fie modificați-o dacă este solicitat de ISP-ul dumneavoastră.
DNS DHCPv6	Selectați o metodă pentru a configura serverul DNS pentru rețea. Cu Auto selectat, serverul DHCP atribuie automat serverul DNS pentru dispozitivele din rețea. Cu Manual selectat, introduceți adresa IP a unui server în fiecare câmp de server DNS.
Cu SLAAC+Stateless DHCP selectat, configurați următorii parametri.	
Prefix	Configurați prefixul adresei IPv6 pentru fiecare client din rețeaua locală. Prefix manual: Cu Prefix manual selectat, introduceți prefixul în câmpul Prefix de adresă. Obțineți de la Prefix Delegation: Cu Obținere de la Delegarea Prefixului selectat, selectați portul WAN cu Delegarea Prefixului configurat, iar clienții vor primi prefixul de adresă de la Delegarea Prefixului.
Delegarea prefixului IPv6 Interfață	Selectați portul WAN utilizând SLAAC+Stateless DHCP pentru conexiunea IPv6.
ID prefix IPv6	Cu Prefixul Prefix selectat, introduceți ID-ul prefixului, care va fi adăugat la prefix pentru a obține o subrețea /64. Intervalul ID-ului de prefix IPv6 este determinat de valoarea mai mare a Dimensiunii de delegare a prefixului și a Lungimei de delegare a prefixului (obținută de la ISP). Rețineți că, dacă lungimea delegării prefixului este mai mare de 64, ID-ul prefixului IPv6 nu poate fi obținut de la delegarea prefixului, vă rugăm să selectați o altă metodă. Mergi laSetări>Rețea cu fir>Internetpentru a configura Prefix Delegation Size.
Server DNS	Selectați o metodă pentru a configura serverul DNS pentru rețea. Auto: Cu Auto selectat, serverul DHCP atribuie automat serverul DNS pentru dispozitivele din rețea. Manual: Cu Manual selectat, introduceți adresa IP a unui server în fiecare câmp de server DNS.
Cu SLAAC+RDNSS selectat, configurați următorii parametri.	
Prefix	Configurați prefixul adresei IPv6 pentru fiecare client din rețeaua locală. Prefix manual: Cu Prefix manual selectat, introduceți prefixul în câmpul Prefix de adresă. Obțineți de la Prefix Delegation: Cu Obținere de la Delegarea Prefixului selectat, selectați portul WAN cu Delegarea Prefixului configurat, iar clienții vor primi prefixul de adresă de la Delegarea Prefixului.
Delegarea prefixului IPv6 Interfață	Selectați portul WAN folosind SLAAC+RDNSS pentru conexiunea IPv6.
ID prefix IPv6	Cu Prefixul Prefix selectat, introduceți ID-ul prefixului, care va fi adăugat la prefix pentru a obține o subrețea /64.

Server DNS	Selectați o metodă pentru a configura serverul DNS pentru rețea. Auto: Cu Auto selectat, serverul DHCP atribuie automat serverul DNS pentru dispozitivele din rețea. Manual: Cu Manual selectat, introduceți adresa IP a unui server în fiecare câmp de server DNS.

Cu Pass-Through selectat, configurați următorii parametri.

IPv6 Passthrough WAN	Selectați portul WAN utilizând Pass-Through (Bridge) pentru conexiunea IPv6.

■ VLAN



VLAN	Introduceți un ID VLAN cu valori între 1 și 4090. Fiecare VLAN poate fi identificat în mod unic prin ID-ul VLAN, care este transmis și primit ca etichetă IEEE 802.1Q într-un cadru Ethernet.
Snooping IGMP	Faceți clic pe caseta de selectare pentru a monitoriza traficul IGMP (Internet Group Management Protocol) și, astfel, a gestiona traficul multicast.
Servere DHCP legale	Faceți clic pe caseta de selectare pentru a specifica serverele DHCP legale pentru rețea. Cu serverele DHCP legale configurate, Omada Gateway-urile și Switch-urile asigură că clienții primesc adrese IP numai de la serverele DHCP specificate aici.

4. Faceți clicSalvați. Noul LAN este adăugat la lista LAN. Puteți face clic pe în coloana ACȚIUNE pentru a edita LAN. Puteți face clic în coloana ACȚIUNE pentru a șterge LAN.

Creați o rețea | Creați un profil de port | Atribuiți profilul portului porturilor

Notă:

- Trei profiluri de porturi implicite sunt preconfigurate pe controler. Ele pot fi vizualizate, dar nu editate sau șterse.

  Toate:În profilul Toate, toate rețelele, cu excepția rețelei implicite (LAN) sunt configurate ca Rețea etichetată, iar rețeaua nativă este rețeaua implicită (LAN). Acest profil este atribuit în mod implicit tuturor porturilor de comutare.

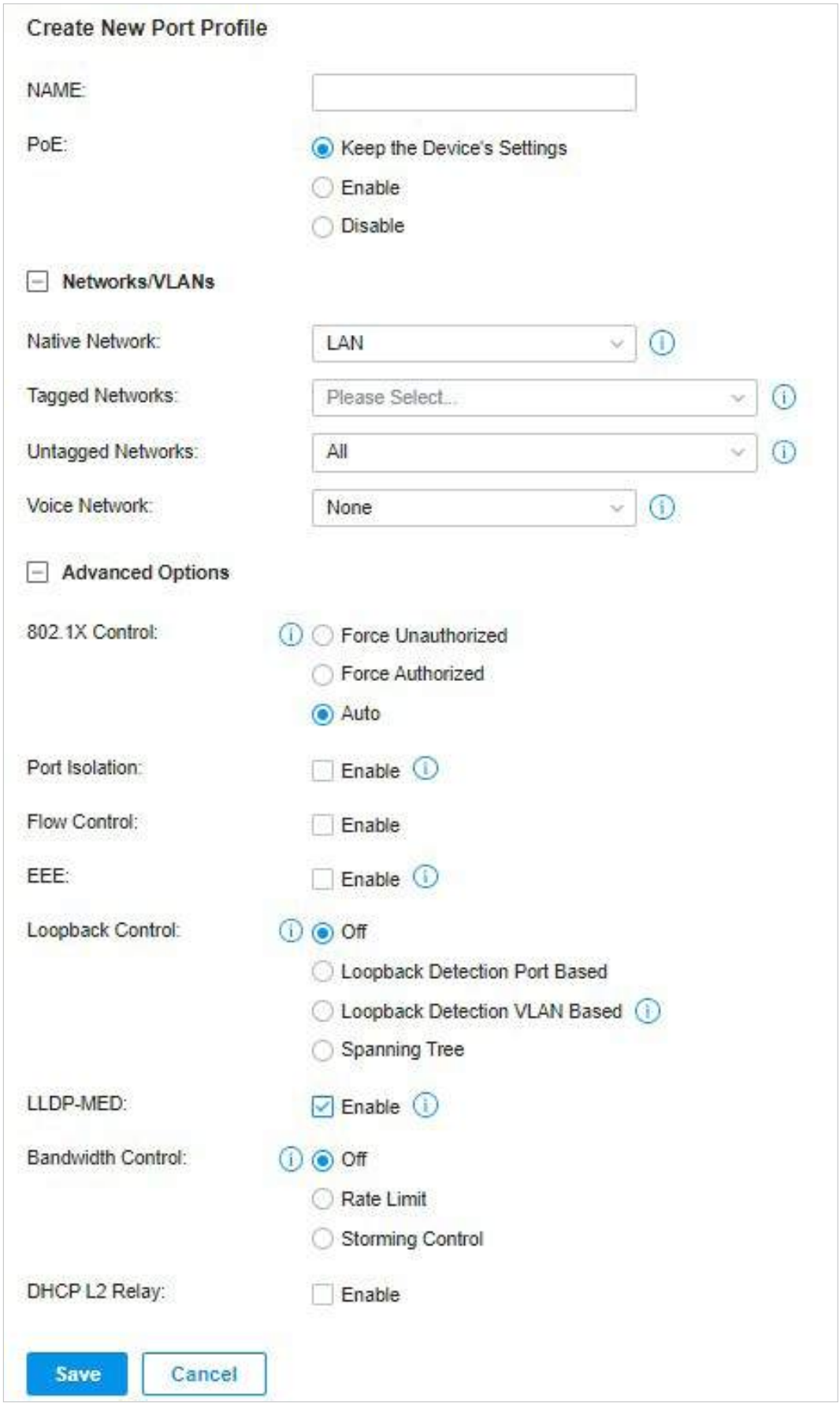
  Dezactivați:În profilul Dezactivare, nu sunt configurate rețele ca rețele native, Rețele etichetate și Rețele neetichetate. Cu acest profil atribuit unui port, portul nu aparține niciunui VLAN.

  LAN:În profilul LAN, rețeaua nativă este rețeaua implicită (LAN) și nicio rețea nu este configurată ca Rețele etichetate și Rețele neetichetate.

- Când se creează o rețea, sistemul va crea automat un profil cu același nume și va configura rețeaua ca rețea nativă pentru profil. În acest profil, rețeaua în sine este configurată ca rețele neetichetate, în timp ce nicio rețea nu este configurată ca rețele etichetate. Profilul poate fi vizualizat și șters, dar nu editat.

1. AccesațiRețele cu fir>LAN>Profiluripentru a încărca următoarea pagină.

2. Faceți clic+ Creați un profil de port noupentru a încărca următoarea pagină și a configura următorii parametri.



Nume	Introduceți un nume pentru a identifica profilul portului.
PoE	Selectați modul PoE pentru porturi. Păstrați setările dispozitivului:PoE rămâne activat sau dezactivat în funcție de setările comutatoarelor. În mod implicit, comutatoarele activează PoE pe toate porturile PoE. Permite:Activați PoE pe porturile PoE. Dezactivați:Dezactivați PoE pe porturile PoE.
Rețea nativă	Selectați rețeaua nativă din toate rețelele. Rețeaua nativă determină Port VLAN Identifier (PVID) pentru porturile de comutare. Când un port primește un cadru neetichetat, comutatorul inserează o etichetă VLAN în cadru pe baza PVID și redirecționează cadrul în rețeaua nativă. Fiecare port de comutare fizic poate avea mai multe rețele atașate, dar numai una dintre ele poate fi nativă.
Rețele etichetate	Selectați rețelele etichetate. Cadrele trimise dintr-o rețea etichetată sunt păstrate cu etichete VLAN. De obicei, rețelele care conectează comutatorul la dispozitive de rețea, cum ar fi routere și alte dispozitive swithe, sau dispozitive VoIP, cum ar fi telefoanele IP, ar trebui configurate ca rețele etichetate.
Rețele neetichetate	Selectați rețelele neetichetate. Cadrele care sunt trimise dintr-o rețea neetichetată sunt lipsite de etichetele VLAN. De obicei, rețelele care conectează comutatorul la dispozitive terminale, cum ar fi computerele, ar trebui configurate ca rețele neetichetate. Rețineți că rețeaua nativă nu este etichetată.
Rețeaua de voce	Selectați rețeaua care conectează dispozitivele VoIP, cum ar fi telefoanele IP, ca Rețea vocală. Omada Switches va acorda prioritate traficului vocal prin schimbarea priorității 802.1p. Pentru a configura o rețea ca rețea vocală, configurați-o mai întâi ca rețea etichetată, apoi activați LLDP-MED. Numai rețelele etichetate pot fi configurate ca Rețea de voce, iar Rețeaua de voce va avea efect cu LLDP-MED activat.
Control 802.1X	Selectați modul de control 802.1X pentru porturi. Pentru a configura autentificarea 802.1X la nivel global, accesațiSetări > Autentificare > 802.1X. Auto:Portul este neautorizat până când clientul este autentificat cu succes de către serverul de autentificare. Forțat autorizat:Portul rămâne în starea autorizată, trimite și primește trafic normal fără autentificarea 802.1X a clientului. Forțat neautorizat:Portul rămâne în starea neautorizată, ignorând toate încercările clientului de a se autentifica. Switch-ul nu poate furniza servicii de autentificare clientului prin port.
Izolarea portului	Faceți clic pe caseta de selectare pentru a activa Izolarea portului. Un port izolat nu poate comunica direct cu niciun alt port izolat, în timp ce portul izolat poate trimite și primi trafic către porturi neizolate.
Controlul debitului	Cu această opțiune activată, atunci când un dispozitiv este supraîncărcat, va trimite un cadru PAUSE pentru a anunța dispozitivul egal să nu mai trimită date pentru o perioadă de timp specificată, evitând astfel pierderea de pachete cauzată de congestie.
EEE	Faceți clic pe caseta de selectare pentru a activa EEE (Energy Efficient Ethernet) pentru a permite reducerea puterii.

Control Loopback	CLoopback se referă la rutarea fluxurilor de date înapoi la sursa lor în rețea. Puteți dezactiva controlul loopback-ului pentru rețea sau puteți alege o metodă pentru a preveni producerea buclei înapoi în rețea. Oprit: Dezactivează controlul loopback pe port. Loopback Detection Port Bazat:Loopback Detection Port Based ajută la detectarea buclelor care apar pe un anumit port. Când este detectată o buclă pe un port, portul va fi blocat. Loopback Detection bazat pe VLAN:Loopback Detection VLAN Based ajută la detectarea buclelor care apar pe un anumit VLAN. Când este detectată o buclă pe un VLAN, VLAN-ul va fi blocat. Spanning Tree: Selectați STP (Spanning Tree Protocal) pentru a preveni buclele în rețea. STP ajută la blocarea anumitor porturi ale comutatoarelor pentru a construi o topologie fără buclă și pentru a detecta modificările topologiei și pentru a genera automat o nouă topologie fără buclă. Dacă doriți să activați Spanning Tree pentru comutator, trebuie să selectați și protocolul Spanning Tree în pagina Device Config. Pentru detalii, consultați5. 3 Configurați și monitorizați comutatoarele.
LLDP-MED	Faceți clic pe caseta de selectare pentru a activa LLDP-MED (Link Layer Discovery Protocol-Media Endpoint Discovery) pentru descoperirea dispozitivelor și configurarea automată a dispozitivelor VoIP.
Controlul lățimii de bandă	Selectați tipul de funcții de control al lățimii de bandă pentru a controla rata de trafic și pragul de trafic pe fiecare port pentru a asigura performanța rețelei. Off:Dezactivați Controlul lățimii de bandă pentru port. Limita ratei:Selectați Rate limit pentru a limita rata de trafic de intrare/ieșire pe fiecare port. Cu această funcție, lățimea de bandă a rețelei poate fi distribuită și utilizată în mod rezonabil. Controlul furtunii:Selectați Storm Control pentru a permite comutatorului să monitorizeze cadrele de difuzare, cadrele multicast și cadrele UL (cadre unicast necunoscute) în rețea. Dacă viteza de transmisie a cadrelor depășește rata setată, cadrele vor fi eliminate automat pentru a evita furtuna de transmisie în rețea.
Limita ratei de intrare	CândLimită de ratăselectat, faceți clic pe caseta de selectare și specificați limita superioară a ratei pentru primirea pachetelor pe port.
Limita ratei de ieșire	CândLimită de ratăselectat, faceți clic pe caseta de selectare și specificați limita superioară a ratei pentru trimiterea de pachete pe port.
Pragul de difuzare	CândControlul furtuniiselectat, faceți clic pe caseta de selectare și specificați limita superioară a ratei de recepție a cadrelor de difuzare. Traficul de difuzare care depășește limita va fi procesat conform configurațiilor Acțiunii.
Prag multicast	CândControlul furtuniiselectat, faceți clic pe caseta de selectare și specificați limita superioară a ratei pentru primirea cadrelor multicast. Traficul multicast care depășește limita va fi procesat conform configurațiilor Action.
Unicast necunoscut Prag	CândControlul furtuniiselectat, faceți clic pe caseta de selectare și specificați limita superioară a ratei pentru primirea cadrelor unicast necunoscute. Traficul care depășește limita va fi procesat conform configurațiilor Acțiunii.

Acțiune	CândControlul furtuniiselectat, selectați acțiunea pe care o va întreprinde comutatorul atunci când traficul depășește limita corespunzătoare. Cu Drop selectat, portul va renunța la cadrele ulterioare când traficul depășește limita. Cu Oprire selectată, portul va fi oprit atunci când traficul depășește limita.
Releu DHCP L2	Faceți clic pe caseta de selectare pentru a activa DHCP L2 Relay pentru rețea.
Format	Selectați formatul câmpului pentru valoarea subopțiunii 82. Normal:Formatul câmpului de valoare a sub-opțiunii este TLV (tip-lungime-valoare). Privat:Formatul câmpului de valoare a sub-opțiunii este doar valoare.

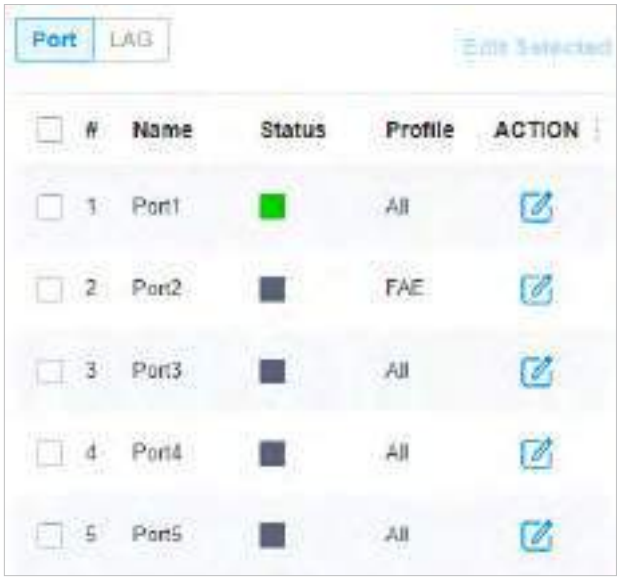
3. Faceți clicSalvați. Noul profil de port este adăugat la lista de profiluri. Puteți face clic în coloana ACȚIUNE pentru a edita profilul portului. Puteți face clic în coloana ACȚIUNE pentru a șterge profilul portului.

Creați o rețea > Creați un profil de port > **Atribuiți profilul de port la Porturi**

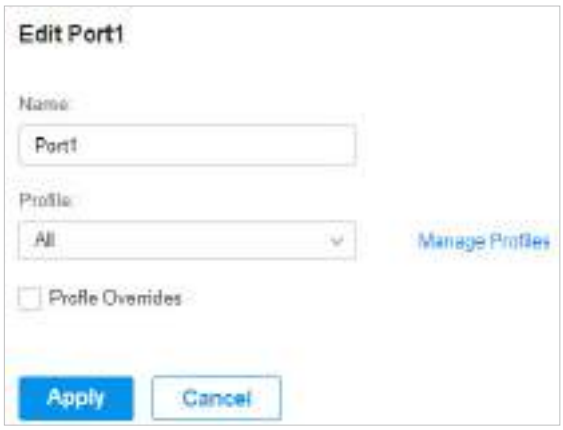
Notă:

În mod implicit, există un profil de port numit All, care este atribuit implicit tuturor porturilor de comutare. În profilul Toate, toate rețelele, cu excepția rețelei implicite (LAN) sunt configurate ca Rețea etichetată, iar rețeaua nativă este rețeaua implicită (LAN).

1. AccesațiDispozitivesi faceți clic pe comutatorul din lista de dispozitive pentru a afișa fereastra Proprietăți. Du-te la porturi, puteți fie să faceți clic în coloana Acțiune pentru a atribui profilul de port unui singur port, fie să selectați porturile dorite și să faceți clicEditați selectatîn partea de sus pentru a atribui profilul portului mai multor porturi în lot.



2. Selectați profilul din lista derulantă pentru a atribui profilul de port porturilor dorite ale comutatorului. Puteți activa suprascrierile de profil pentru a personaliza setările pentru porturi, iar toată configurația de aici înlocuiește profilul portului. Pentru detalii, consultațiCapitolul 5 Configurarea și monitorizarea dispozitivelor gestionate Omada .



3. 4 Configurați rețele wireless

Rețelele wireless le permit clienților dumneavoastră wireless să acceseze internetul. Odată ce ați configurat o rețea fără fir, EAP-urile dvs. difuzează de obicei numele rețelei (SSID) în aer, prin care clienții dvs. fără fir se conectează la rețeaua fără fir și accesează internetul.

Un grup WLAN este o combinație de rețele wireless. Configurați fiecare grup astfel încât să puteți aplica în mod flexibil aceste grupuri de rețele fără fir la diferite EAP-uri în funcție de nevoile dvs.

După configurarea rețelelor wireless de bază, puteți configura în continuare Programul WLAN, Controlul ratei 802.11 și Filtrul MAC, printre alte setări avansate.

3. 4. 1 Configurați rețele wireless de bază

Configurare

Pentru a crea, configura și aplica rețele wireless, urmați acești pași:

1)Creați un grup WLAN.

2)Creați rețele wireless

3)Aplicați grupul WLAN la EAP-urile dvs

Notă:

Controlerul oferă un grup WLAN implicit. Dacă doriți pur și simplu să configurați rețelele fără fir pentru grupul WLAN implicit și să îl aplicați tuturor EAP-urilor, săriți peste acest pas.

1. Selectați un site din lista derulantă aOrganizare. Mergi laSetări>Rețele fără firpentru a încărca următoarea pagină.

2. Selectați+ Creați un grup noudin lista derulantă aGrupul WLANpentru a încărca următoarea pagină. Introduceți un nume pentru a identifica grupul WLAN.

3. (Opțional) Dacă doriți să creați un nou grup WLAN bazat pe unul existent, bifațiCopiați toate SSID-urile din grupul WLANși selectați grupul WLAN dorit. Apoi, puteți configura în continuare rețelele wireless pe baza setărilor curente.

4. Faceți clicSalvați. Noul grup WLAN este adăugat la lista WLAN Group. Puteți selecta un grup WLAN din listă pentru a crea și configura în continuare rețelele sale fără fir. Puteți face clic pentru a edita numele grupului WLAN. Puteți face clic pentru a șterge grupul WLAN.

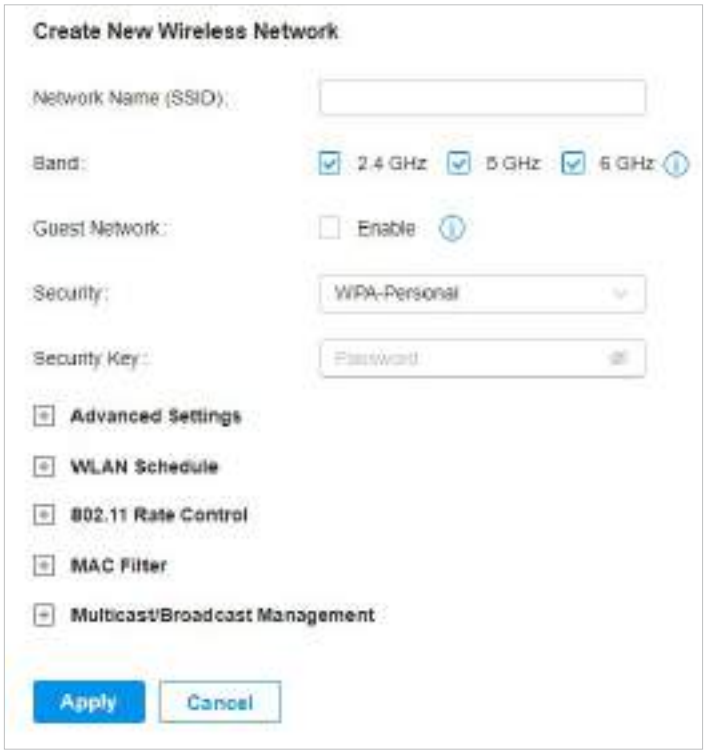
Creați un grup WLAN | Creați rețele wireless | Aplicați grupul WLAN

1. Selectați grupul WLAN pentru care doriți să configurați rețelele fără fir din lista derulantă a grupului WLAN.

2. Faceți clic+ Creați o nouă rețea fără firpentru a încărca următoarea pagină. Configurați parametrii de bază pentru rețea.

Notă:

Banda de 6 GHz este disponibilă numai pentru anumite dispozitive.



Numele rețelei (SSID)	Introduceți numele rețelei (SSID) pentru a identifica rețeaua fără fir. Utilizatorii clienților fără fir aleg să se conecteze la rețeaua fără fir conform SSID-ului, care apare pe pagina de setări WLAN a clienților fără fir.
Grup	Activați benzile radio pentru rețeaua fără fir. Banda de 6 GHz este disponibilă numai pentru anumite dispozitive.
Rețeaua de oaspeți	Cu Rețeaua de oaspeți activată, toți clienții care se conectează la SSID nu pot ajunge la orice subrețea IP privată.

3. Selectați strategia de securitate pentru rețeaua wireless.

■ Nici unul

Dacă este selectat Niciunul, gazdele pot accesa rețeaua wireless fără autentificare, care se aplică cerințelor de securitate mai scăzute.

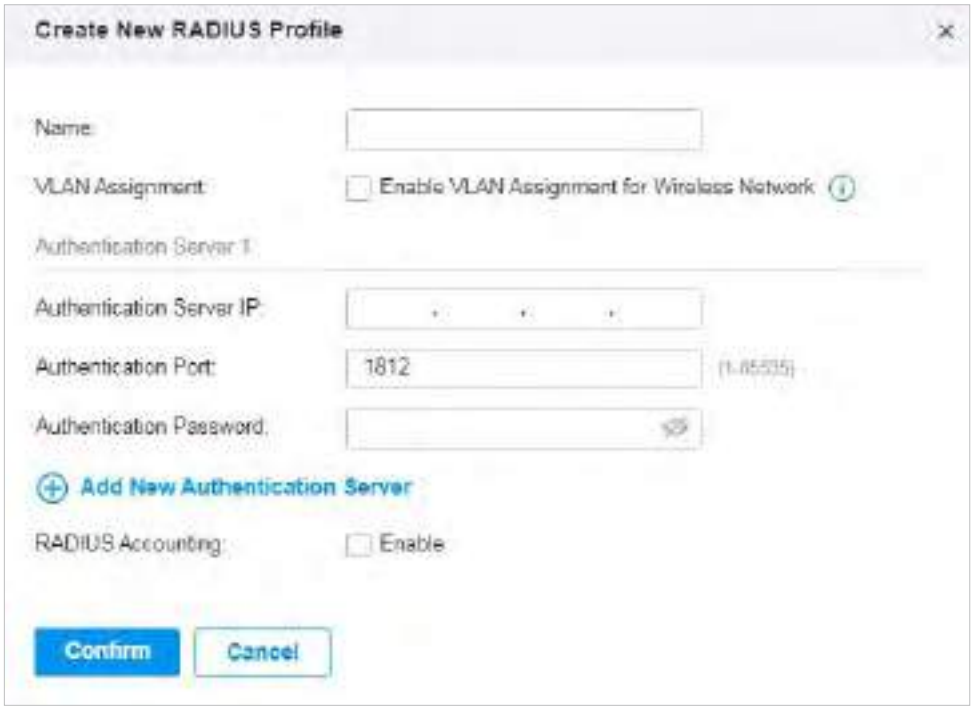
■ WPA-Personal

Traficul este criptat cu o cheie de securitate, pe care trebuie să o specificați. WPA-Personal este mai sigur decât WEP.

■ WPA-Enterprise

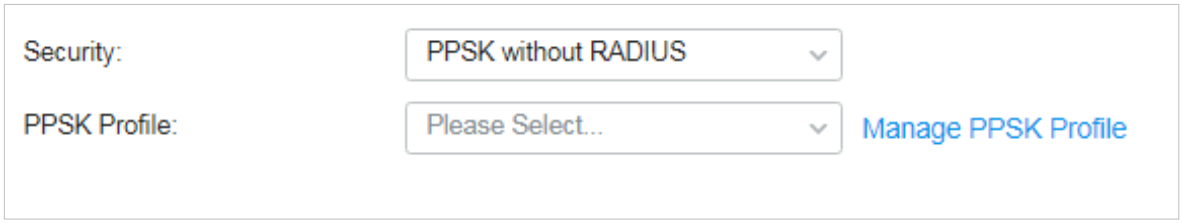
WPA-Enterprise necesită un server de autentificare pentru a autentifica clienții wireless și probabil un server de contabilitate pentru a înregistra statisticile de trafic.

Selectați un profil RADIUS, care înregistrează setările serverului de autentificare și ale serverului de contabilitate. Puteți crea un profil RADIUS făcând clic+ Creați un nou profil de razădin lista derulantă a Profilului RADIUS. Pentru detalii, consultați3. 9 Autentificare .



■ PPSK fără RAZĂ

PPSK (cheie privată pre-partajată) poate oferi un PSK unic pentru fiecare utilizator wireless. În comparație cu soluția tradițională SSID cu o singură parolă pentru toți utilizatorii, este mai sigură.

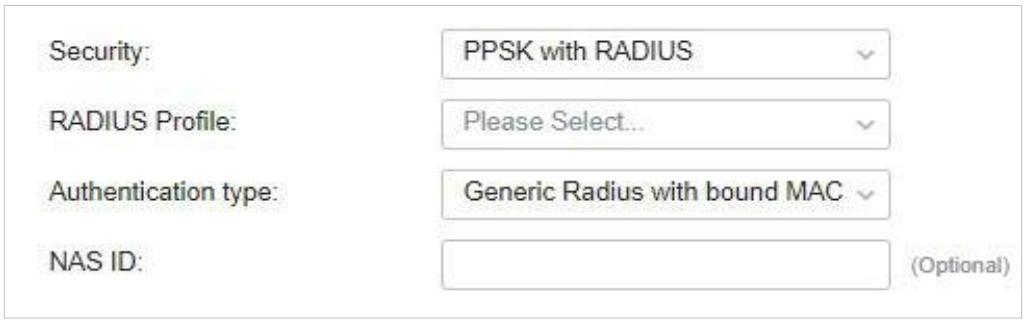


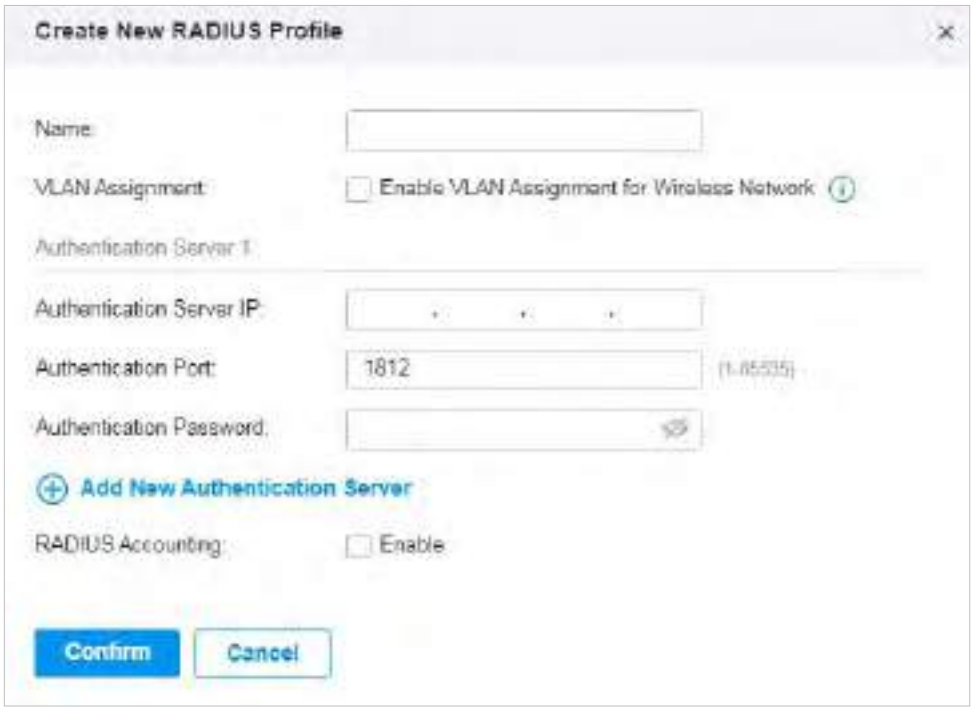
Selectați un profil PPSK, care înregistrează setările PPSK. Puteți crea un profil PPSK făcând clic+ Creați un nou profil PPSKdin lista derulantă a Profilului PPSK. Pentru detalii, consultați3. 8. 4 PPSK .

■ PPSK cu RAZĂ

PPSK (cheie privată pre-partajată) poate oferi un PSK unic pentru fiecare utilizare fără fir. PPSK cu RADIUS necesită un server de autentificare pentru a autentifica clienții wireless și probabil un server de contabilitate pentru a înregistra statisticile de trafic.

Selectați un profil RADIUS, care înregistrează setările serverului de autentificare și ale serverului de contabilitate. Puteți crea un profil RADIUS făcând clic+ Creați un nou profil de razădin lista derulantă a Profilului RADIUS. Selectați autentificarea Pentru detalii, consultați3. 9 Autentificare .





4. (Opțional) De asemenea, puteți configura3. 4. 2 Setări avansate ,3. 4. 3 Programare WLAN ,3. 4. 4 802.11 Controlul ratei , și3. 4. 5 Filtru MAC conform nevoilor tale. Subiectele înrudite sunt tratate mai târziu în acest capitol.

5. Faceți clicaplica. Noua rețea fără fir este adăugată la lista de rețele fără fir din grupul WLAN. Puteți face clic în coloana ACȚIUNE pentru a edita rețeaua wireless. Puteți face clic în coloana ACȚIUNE pentru a șterge rețeaua wireless.

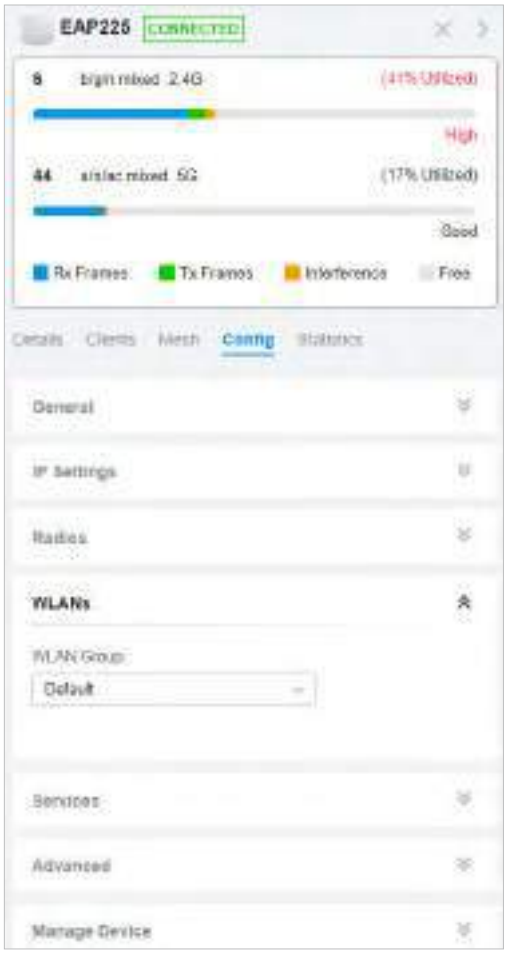
Creați un grup WLAN > Creați rețele wireless > **Aplicați grupul WLAN**

Notă:

Controlerul oferă un grup WLAN implicit. Dacă doriți pur și simplu să configurați rețelele fără fir pentru grupul WLAN implicit și să îl aplicați tuturor EAP-urilor, săriți peste acest pas.

■ Aplicați la un singur EAP

Accesați Dispozitive, selectați EAP. În fereastra Proprietăți, accesațiConfig>rețele WLAN, selectați grupul WLAN de aplicat.



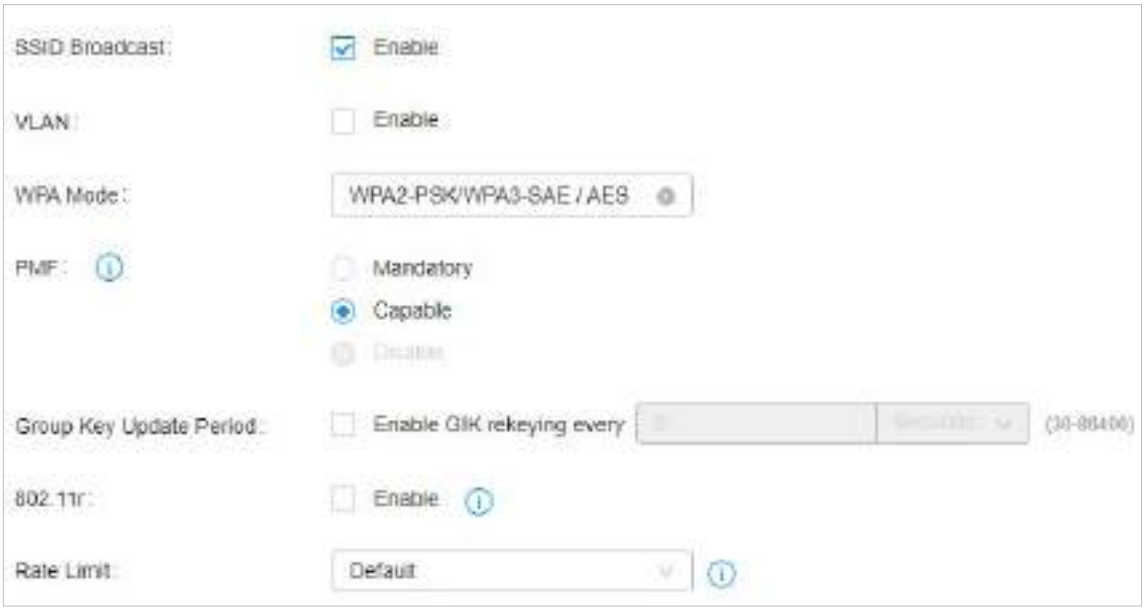
■ Aplicați la EAP-uri în lot

1. Accesați Dispozitive, selectațiAP-urifilă, faceți clicAcțiune în lot, apoi selectațiConfigurare lot, bifați casetele EAP la care doriți să aplicați grupul WLAN și faceți clicTerminat.

2. În fereastra Proprietăți, accesațiConfig>rețele WLAN, selectați grupul WLAN pe care doriți să îl aplicați la EAP.

3. 4. 2 Setări avansate

Selectați un site din lista derulantă aOrganizare. Mergi laSetări>Rețele fără fir,faceți clic în coloana ACȚIUNE a rețelei wireless pe care doriți să o configurați și faceți clic+ Setări avansatepentru a încărca următoarea pagină. Configurați parametrii și faceți clicaplica.



SSID Broadcast	Cu SSID Broadcast activat, EAP-urile difuzează SSID (numele rețelei) în aer, astfel încât clienții fără fir să se poată conecta la rețeaua fără fir, care este identificată prin SSID. Cu SSID Broadcast dezactivat, utilizatorii clienților wireless trebuie să introducă manual SSID-ul pentru a se conecta la rețeaua wireless.
VLAN	Pentru a seta un VLAN fără fir pentru rețeaua fără fir, activați această opțiune și setați un ID VLAN de la 1 la 4094. Cu această opțiune activată, traficul în diferite rețele wireless este marcat cu etichete VLAN diferite în funcție de ID-urile VLAN configurate. Apoi, EAP-urile lucrează împreună cu comutatoarele care acceptă și 802.1Q VLAN, pentru a distribui traficul către diferite VLAN-uri în funcție de etichetele VLAN. Ca rezultat, clienții fără fir din diferite VLAN-uri nu pot comunica direct între ei.
Modul WPA	Dacă selectați WPA-Personal sau WPA-Enterprise ca strategie de securitate, puteți selecta modul WPA, inclusiv versiunea WPA și tipul de criptare. Selectați versiunea WPA în funcție de nevoile dvs. Selectați tipul de criptare. Unele tipuri de criptare sunt disponibile numai în anumite circumstanțe. AES: AES înseamnă Advanced Encryption Standard. Auto:EAP-urile decid automat tipul de criptare în procesul de autentificare.

PMF	Cadrele de management protejate (PMF) oferă protecție pentru cadrele de acțiune de gestionare unicast și multicast. Când este selectat Obligatoriu, clienții care nu sunt capabili de PMF pot să nu reușească să se conecteze la rețea. Dezactivați:Dezactivează PMF pentru o rețea. Nu este recomandat să utilizați această setare, numai în cazul în care clienții care nu sunt capabili de PMF întâmpină probleme de conectare cu opțiunea „Capable”. Capabil:Ambele tipuri de clienți, capabili sau nu de PMF, se pot conecta la rețea. Clienții capabili de PMF îl vor negocia cu AP. Obligatoriu:Numai clienții capabili de PMF se pot conecta la rețea.
Perioada de actualizare a cheii de grup	Dacă selectați WPA-Personal sau WPA-Enterprise ca strategie de securitate, puteți specifica dacă și cât de des se schimbă cheia de securitate. Dacă doriți ca cheia de securitate să se schimbe periodic, activați reintroducerea GIK și specificați perioada de timp.
802.11r	Activați această funcție pentru a permite roaming mai rapid atunci când atât AP-ul, cât și clientul au capabilități 802.11r. În prezent, 802.11r nu acceptă criptarea WPA3.
Limită de rată	Puteți limita rata de descărcare și încărcare a fiecărui client pentru a echilibra utilizarea lățimii de bandă. Limită de descărcare: Setați rata de descărcare pentru fiecare client pentru a primi traficul. Limită de încărcare: Setați rata de încărcare pentru fiecare client pentru a transmite traficul.

3. 4. 3 Programare WLAN

Prezentare generală

Programul WLAN vă poate porni sau opri rețeaua fără fir într-o anumită perioadă de timp, după cum doriți.

Configurare

Selectați un site din lista derulantă aOrganizare. Mergi laSetări>Rețele fără fir,faceți clic în coloana ACȚIUNE a rețelei wireless pe care doriți să o configurați și faceți clic+ Program WLANpentru a încărca următoarea pagină. Activați programul WLAN și configurați parametrii. Apoi faceți clicaplica.

Acțiune	Radio Pornit: porniți rețeaua fără fir în intervalul de timp pe care îl setați și opriți-o dincolo de intervalul de timp. Radio oprit: Opriți rețeaua fără fir în intervalul de timp setat și porniți-o dincolo de intervalul de timp.

Interval de timp	Selectați intervalul de timp pentru ca acțiunea să aibă efect. Puteți crea o intrare de interval de timp făcând clic+ Creați o nouă intrare în intervalul de timpdin lista derulantă a Interval de timp. Pentru detalii, consultați3. 8 Creați profiluri.

3. 4. 4 802.11 Controlul ratei

Prezentare generală

Notă:

Controlul ratei 802.11 este disponibil numai pentru anumite dispozitive.

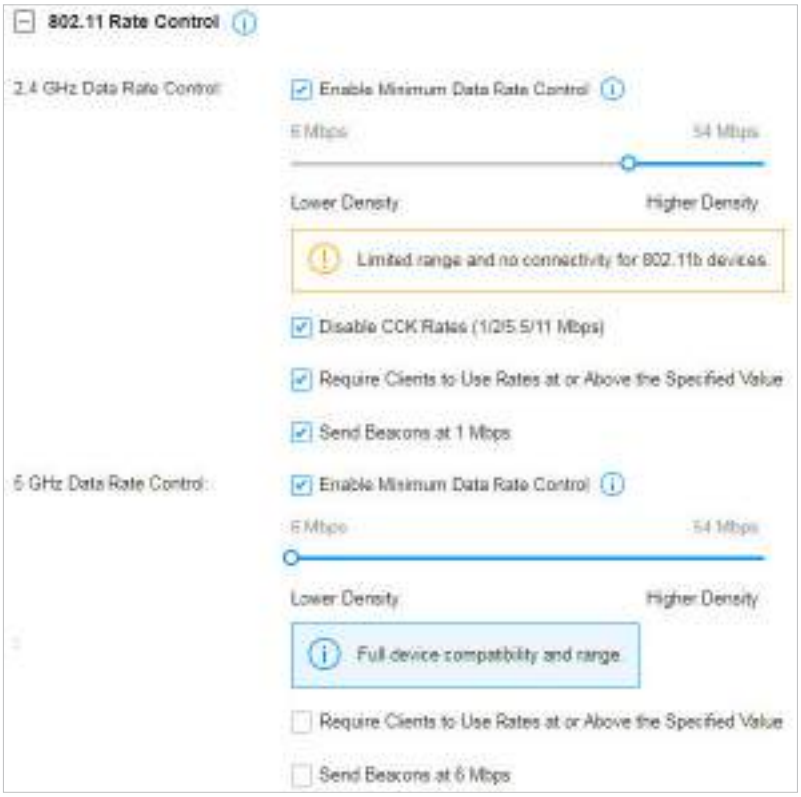
Controlul ratei 802.11 poate îmbunătăți performanța pentru rețelele cu densitate mai mare prin dezactivarea ratelor de biți mai mici și permițând doar cele mai mari. Cu toate acestea, 802.11 Rate Control poate face unele dispozitive vechi să fie incompatibile cu rețelele dvs. și să limiteze raza de acțiune a rețelelor dvs. fără fir.

Configurare

Selectați un site din lista derulantă aOrganizare. Mergi laSetări>Rețele fără fir,faceți clic în coloana ACȚIUNE a rețelei wireless pe care doriți să o configurați și faceți clic+ 802.11 Controlul ratei pentru a încărca următoarea pagină. Selectați una sau mai multe benzi pentru a activa controlul minim al ratei de date în funcție de nevoile dvs., mutați glisorul pentru a determina ce rate de biți permite rețeaua dvs. wireless și configurați parametrii. Apoi apasaaplica.

Notă:

Banda de 6 GHz este disponibilă numai pentru anumite dispozitive.



Dezactivați ratele CCK (1/2/5,5/11 Mbps)	Selectați dacă doriți să dezactivați CCK (Complementary Code Keying), schema de modulație care funcționează cu dispozitivele 802.11b. Dezactivarea ratelor CCK (1/2/5,5/11 Mbps) este disponibilă numai pentru banda de 2,4 GHz.
Solicitați clienților să utilizeze tarife la sau peste valoarea specificată	Selectați dacă doriți sau nu să solicitați clienților să folosească tarife la sau peste valoarea pe care o indică cursorul.
Trimiteți semnalizatoare la 1 Mbps/6 Mbps	Selectați dacă trimiteți sau nu semnalizatoarele la o rată minimă de 1 Mbps pentru banda de 2,4 GHz sau 6 Mbps pentru banda de 5 GHz și banda de 6 GHz.

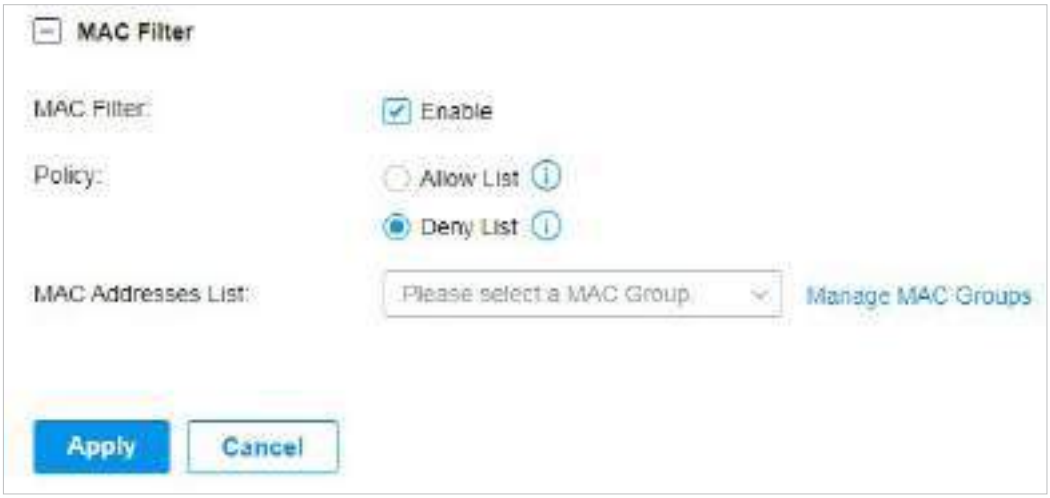
3. 4. 5 Filtru MAC

Prezentare generală

Filtrul MAC permite sau blochează conexiunile de la clienți wireless cu anumite adrese MAC.

Configurare

Selectați un site din lista derulantă aOrganizare. Mergi laSetări>Rețele fără fir,faceți clic în coloana ACȚIUNE a rețelei wireless pe care doriți să o configurați și faceți clic+ Filtru MACpentru a încărca următoarea pagină. Activați filtrul MAC și configurați parametrii. Apoi faceți clicaplica.



Politică	Lista de permisiuni: Permite conectarea clienților ale căror adrese MAC se află în Lista de adrese MAC specificată, blocând în același timp altele. Lista de respingere: Blocați conexiunea clienților a căror adresă MAC se află în lista de adrese MAC specificată, permițând în același timp altora.
Lista de adrese MAC	Selectați grupul MAC pe care doriți să îl permiteți sau să îl blocați conform politicii. Puteți crea un nou grup MAC făcând clic+ Creați un nou grup MACdin lista derulantă a Listei de adrese MAC. Pentru detalii, consultați3. 8 Creați profiluri.

3. 4. 6 Optimizare AI WLAN

Prezentare generală

Optimizarea AI WLAN ajută la îmbunătățirea performanței rețelei wireless. Cu funcția de optimizare AI WLAN, controlerul va detecta interferențele WiFi și va monitoriza mediul wireless. Pe baza factorilor de mediu, inclusiv traficul, topologia rețelei, dimensiunea implementării și factorii de client, controlerul poate determina canalele optime de operare și puterea pentru punctele de acces (AP) și astfel se asigură că clienții fără fir ai fiecărui AP se pot bucura de o experiență WiFi mai bună. .

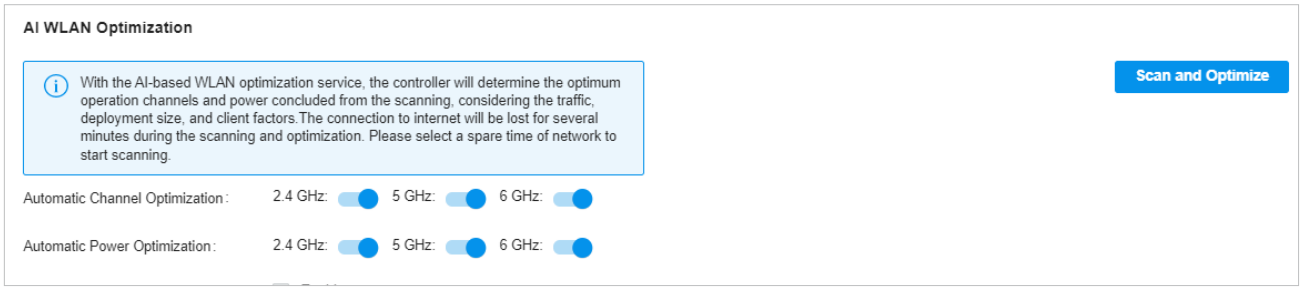
Configurare

Notă:

1. Experiența WiFi poate fi influențată în timpul optimizării, vă rugăm să selectați timpul liber pentru scanare și optimizare pentru a reduce impactul acestuia asupra experienței utilizatorului.
2. Deoarece AP-urile ar trebui să rămână conectate în timpul optimizării, vă rugăm să setați o oră diferită pentru Optimizarea AI WLAN și Programul de repornire. Se recomandă să eșalonați cel puțin 10 minute pentru a evita rezultate nesatisfăcătoare.

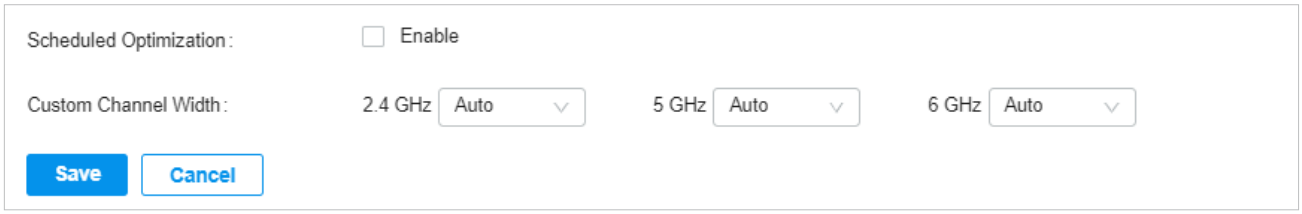
1. Selectați un site din lista derulantă aOrganizare. Mergi laSetări>Rețele fără fir>Optimizare AI WLAN.

2. ActivațiOptimizare automată a canaluluișiOptimizare automată a puteriipe benzile de frecvență dorite și faceți clicScanați și optimizați. Controlerul va scana mediul wireless pentru a încheia canalele optime de operare pentru AP-uri.



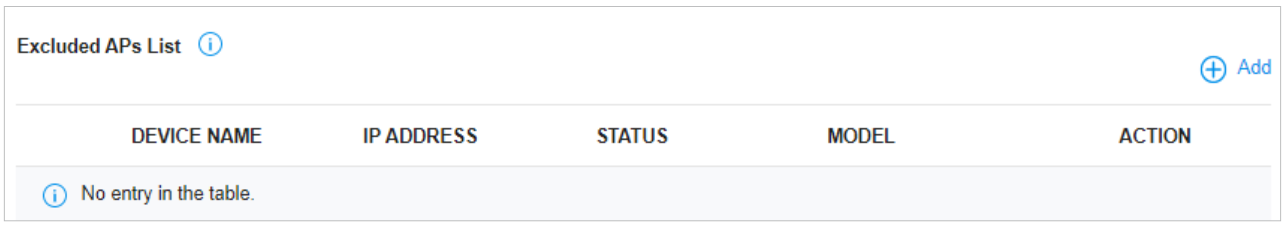
Puteți vizualiza rezultatele optimizării în Jurnalul de optimizare.

3. (Opțional) Setați programe pentru optimizarea canalului și faceți clicSalvați.



Programat Optimizare	Activați optimizarea programată, iar controlerul va ajusta automat canalele pentru AP-uri în mod regulat.
Apariția	Setați programul pentru optimizarea WLAN obișnuită.
Canal personalizat Lățime	Selectați lățimea canalului pentru fiecare bandă, iar optimizarea va menține lățimea canalului selectat.

4. (Opțional) ÎnLista AP-uri excluse, faceți clicAdăugapentru a adăuga AP-urile care vor fi excluse de la optimizarea AI WLAN. Următoarele AP-uri vor fi adăugate automat în listă: AP-uri din rețeaua mesh și AP-uri cu firmware neacceptat.



3. 5 Securitatea rețelei

Network Security este un portofoliu de caracteristici concepute pentru a îmbunătăți gradul de utilizare și pentru a asigura siguranța rețelei și a datelor dvs. Serviciile de securitate a rețelei includ3. 5. 1 ACL ,3. 5. 2 Filtrare URL , și3. 5. 3 Apărare împotriva atacului ,3. 5. 4 Firewall , care implementează politici și controale pe mai multe straturi de apărare în rețea.

3. 5. 1 ACL

Prezentare generală

ACL (Access Control List) permite unui administrator de rețea să creeze reguli pentru a restricționa accesul la resursele rețelei. Regulile ACL filtrează traficul pe baza unor criterii specificate, cum ar fi adresele IP sursă, adresele IP de destinație și numerele de port și determină dacă să redirecționeze pachetele potrivite. Aceste reguli pot fi aplicate anumitor clienți sau grupuri al căror trafic trece prin gateway, switch-uri și EAP-uri.

Sistemul filtrează traficul în funcție de regulile din listă secvenţial. Prima potrivire determină dacă pachetul este acceptat sau abandonat, iar alte reguli nu sunt verificate după prima potrivire. Prin urmare, ordinea regulilor este critică. În mod implicit, regulile sunt prioritizate în funcție de timpul creat. Regula creată mai devreme este verificată pentru o potrivire cu prioritate mai mare. Pentru a reordona regulile, selectați o regulă și trageți-o într-o nouă poziție. Dacă nicio regulă nu se potrivește, dispozitivul redirecționează pachetul din cauza unei clauze implicite Permit All.

Sistemul oferă trei tipuri de ACL:

- Gateway ACL

  După ce ACL-urile Gateway sunt configurate pe controler, acestea pot fi aplicate la gateway pentru a controla traficul care provine din porturile LAN și redirecționat către porturile WAN.

  Puteți seta rețeaua, adresa IP, numărul de port al unui pachet ca criterii de filtrare a pachetelor în regulă.

- Comutați ACL

  După ce ACL-urile Switch sunt configurate pe controler, acestea pot fi aplicate comutatorului pentru a controla traficul de intrare și de ieșire prin porturile de comutare.

  Puteți seta rețeaua, adresa IP, numărul portului și adresa MAC a unui pachet ca criterii de filtrare a pachetelor în regulă.

- EAP ACL

  După ce ACL-urile EAP sunt configurate pe controler, acestea pot fi aplicate EAP-urilor pentru a controla traficul în rețelele fără fir.

  Puteți seta rețeaua, adresa IP, numărul portului și SSID-ul unui pachet ca criterii de filtrare a pachetelor în regulă.

Configurare

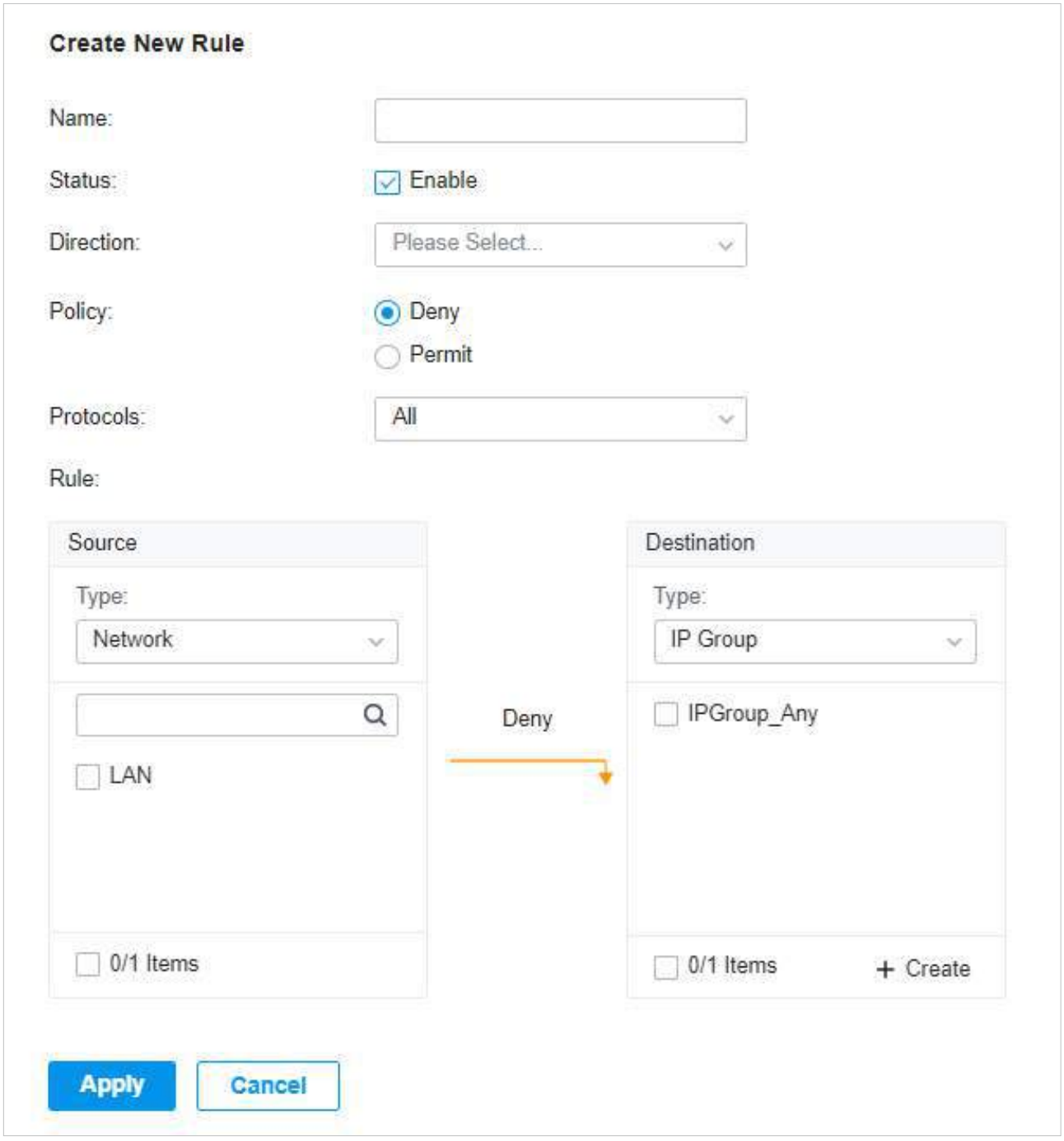
Pentru a finaliza configurarea ACL, urmați acești pași:

1)Creați un ACL cu tipul specificat.

2)Definiți criteriile de filtrare a pachetelor ale regulii, inclusiv protocoalele, sursa și destinația și determinați dacă să redirecționați pachetele potrivite.

■ Configurarea Gateway ACL

1. Selectați un site din lista derulantă aOrganizare. Mergi laSetări>Securitatea retelei>ACL. Pe fila Gateway ACL, faceți clic + Create New Rule pentru a încărca următoarea pagină.



2. Definiți criteriile de filtrare a pachetelor ale regulii, inclusiv protocoalele, sursa și destinația și determinați dacă să redirecționați pachetele potrivite. Consultați următorul tabel pentru a configura parametrii necesari și faceți clicaplica.

Nume	Introduceți un nume pentru a identifica ACL.
stare	Faceți clic pe caseta de selectare pentru a activa ACL.
Direcţie	Selectați portul WAN sau o intrare VPN. (Fiecare intrare VPN va avea un VLAN corespunzător)
Politică	Selectați acțiunea care trebuie întreprinsă atunci când un pachet se potrivește cu regula. Permite: Redirecționați pachetul potrivit. Negați: Aruncați pachetul potrivit.
Protocoale	Selectați unul sau mai multe tipuri de protocol cărora li se aplică regula din lista derulantă. Valoarea implicită este All, indicând că pachetele tuturor protocoalelor vor fi potrivite. Când selectați unul dintre TCP și UDP sau ambele, puteți seta adresa IP și numărul de port al unui pachet ca criterii de filtrare a pachetelor în regulă.

Din lista derulantă Sursă, alegeți una dintre aceste opțiuni pentru a specifica sursa pachetelor la care se aplică acest ACL:

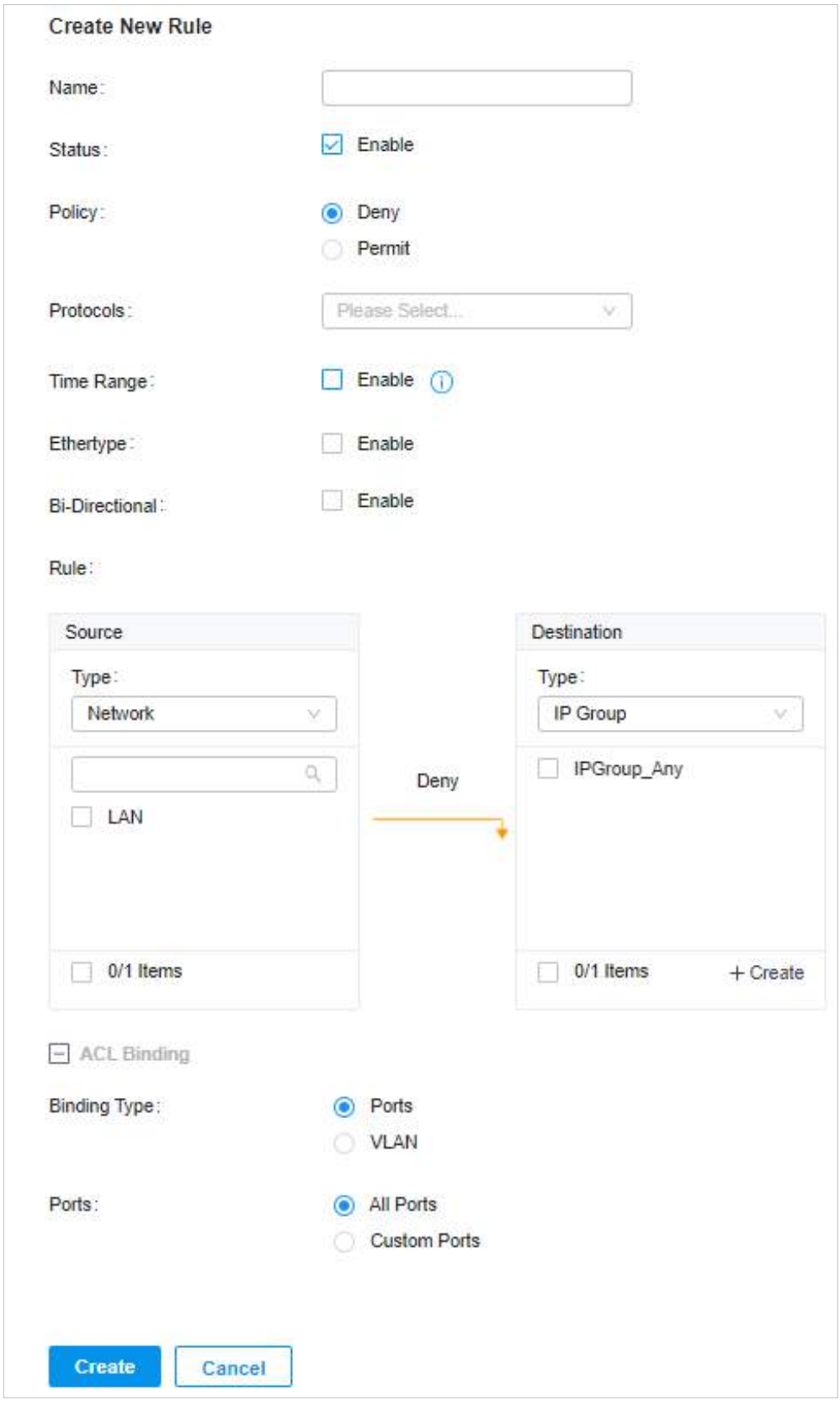
Reţea	Selectați rețeaua pe care ați creat-o. Dacă nu au fost create rețele, puteți selecta rețeaua implicită (LAN) sau puteți accesaSetări > Rețele cu fir > LANpentru a crea unul. Gateway-ul va examina dacă pachetele provin din rețeaua selectată.
IP Group	Selectați grupul IP pe care l-ați creat. Dacă nu a fost creat niciun grup de IP, faceți clic+Creează pe această pagină sau accesațiSetări > Profiluri > Grupuripentru a crea unul. Gateway-ul va examina dacă adresa IP sursă a pachetului se află în grupul IP.
Grupul de porturi IP	Selectați grupul de porturi IP pe care l-ați creat. Dacă nu a fost creat niciun grup de porturi IP, faceți clic+Creeazăpe această pagină sau accesațiSetări > Profiluri > Grupuripentru a crea unul. Gateway-ul va examina dacă adresa IP sursă și numărul portului pachetului se află în grupul de porturi IP.

Din lista derulantă Destinație, alegeți una dintre aceste opțiuni pentru a specifica destinația pachetelor cărora li se aplică acest ACL:

IP Group	Selectați grupul IP pe care l-ați creat. Dacă nu a fost creat niciun grup de IP, faceți clic+Creează pe această pagină sau accesațiSetări > Profiluri > Grupuripentru a crea unul. Gateway-ul va examina dacă adresa IP de destinație a pachetului se află în grupul IP.
Grupul de porturi IP	Selectați grupul de porturi IP pe care l-ați creat. Dacă nu a fost creat niciun grup de porturi IP, faceți clic+Creeazăpe această pagină sau accesațiSetări > Profiluri > Grupuripentru a crea unul. Gateway-ul va examina dacă adresa IP de destinație și numărul de port al pachetului se află în grupul de porturi IP.

■ Configurarea Switch ACL

1. Selectați un site din lista derulantă aOrganizare. Mergi laSetări>Securitatea retelei>ACL. Sub fila Comutare ACL, faceți clic + Create New Rule pentru a încărca următoarea pagină.



2. Definiți criteriile de filtrare a pachetelor ale regulii, inclusiv protocoalele, sursa și destinația și determinați dacă să redirecționați pachetele potrivite. Consultați următorul tabel pentru a configura parametrii necesari.

Nume	Introduceți un nume pentru a identifica ACL.
stare	Faceți clic pe caseta de selectare pentru a activa ACL.
Politică	Selectați acțiunea care trebuie întreprinsă atunci când un pachet se potrivește cu regula. Permite: Redirecționați pachetul potrivit. Negați: Aruncați pachetul potrivit.
Protocoale	Selectați unul sau mai multe tipuri de protocol cărora li se aplică regula din lista derulantă. Valoarea implicită este All, indicând că pachetele tuturor protocoalelor vor fi potrivite. Când selectați unul dintre TCP și UDP sau ambele, puteți seta adresa IP și numărul de port al unui pachet ca criterii de filtrare a pachetelor în regulă.
Interval de timp	Bifați caseta de selectare pentru a activa ACL bazat pe timp. Puteți crea un interval de timp sau puteți selecta un interval de timp existent pentru ca regula ACL să intre în vigoare.
Etertip	Faceți clic pe caseta de selectare dacă doriți ca comutatorul să verifice tipul eter al pachetelor și să configureze tipul Ether în funcție de nevoi.
Bidirecțional	Faceți clic pe caseta de selectare pentru a activa comutatorul pentru a crea un alt ACL simetric cu numele „xxx_reverse”, unde „xxx” este numele ACL-ului curent. Cele două ACL-uri vizează pachete cu direcția opusă unul celuilalt.

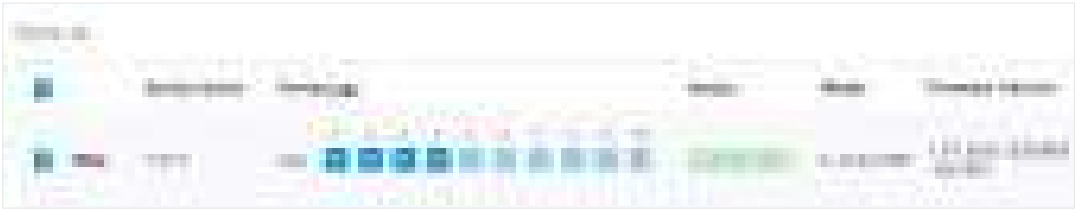
Din lista derulantă Sursă, alegeți una dintre aceste opțiuni pentru a specifica sursa pachetelor la care se aplică acest ACL:

Rețea	Selectați rețeaua pe care ați creat-o. Dacă nu au fost create rețele, puteți selecta rețeaua implicită (LAN) sau puteți accesaSetări > Rețele cu fir > LANpentru a crea unul. Comutatorul va examina dacă pachetele provin din rețeaua selectată.
IP Group	Selectați grupul IP pe care l-ați creat. Dacă nu a fost creat niciun grup de IP, faceți clic+Creează pe această pagină sau accesațiSetări > Profiluri > Grupuripentru a crea unul. Comutatorul va examina dacă adresa IP sursă a pachetului se află în grupul IP.
Grupul de porturi IP	Selectați grupul de porturi IP pe care l-ați creat. Dacă nu a fost creat niciun grup de porturi IP, faceți clic+Creeazăpe această pagină sau accesațiSetări > Profiluri > Grupuripentru a crea unul. Comutatorul va examina dacă adresa IP sursă și numărul portului pachetului se află în grupul de porturi IP.
Grupul MAC	Selectați grupul MAC pe care l-ați creat. Dacă nu a fost creat niciun grup MAC, faceți clic + Creațipe această pagină sau accesațiSetări > Profiluri > Grupuripentru a crea unul. Comutatorul va examina dacă adresa MAC sursă a pachetului se află în grupul MAC.

Din lista derulantă Destinație, alegeți una dintre aceste opțiuni pentru a specifica destinația pachetelor cărora li se aplică acest ACL:

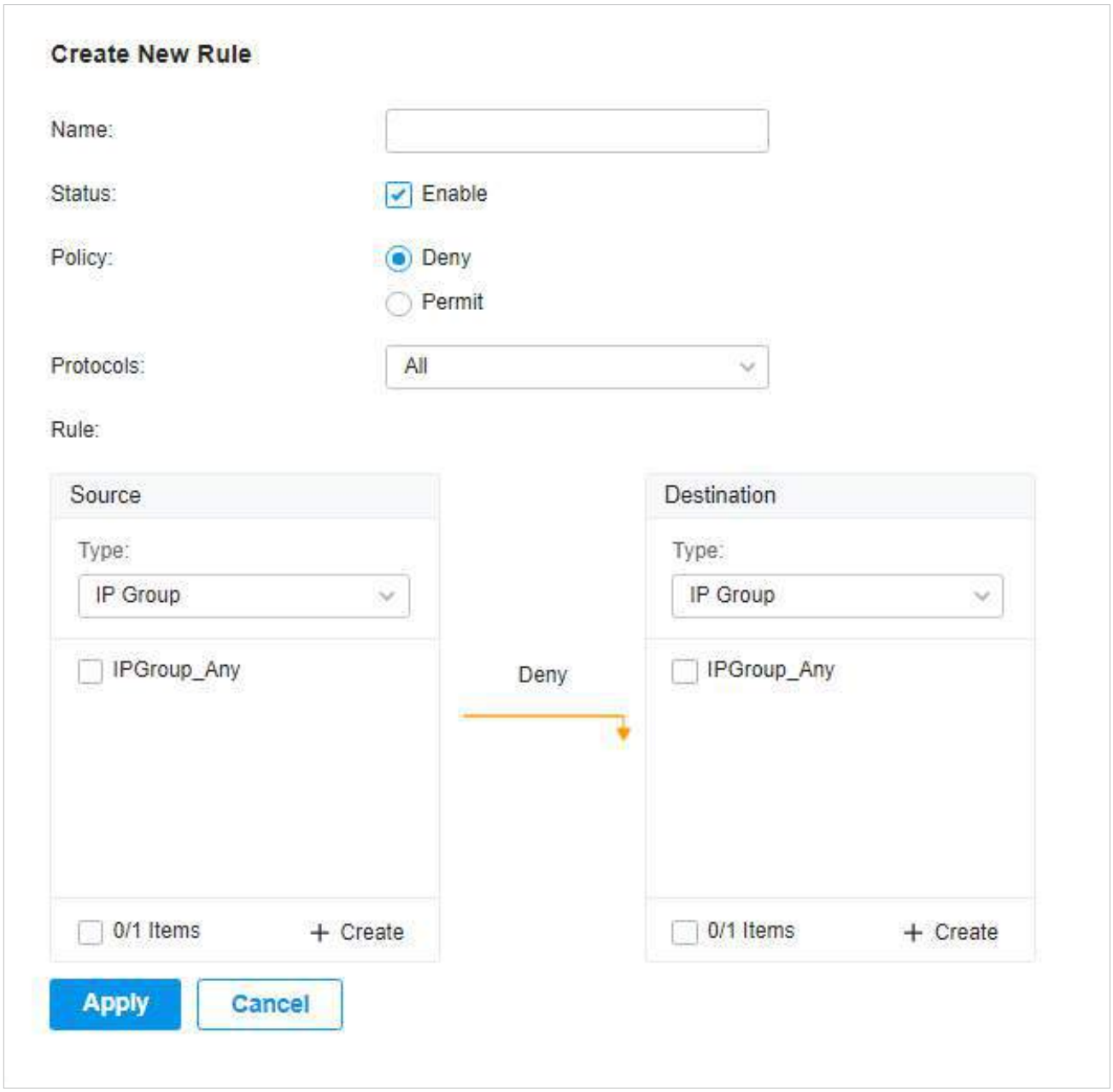
Rețea	Selectați rețeaua pe care ați creat-o. Dacă nu au fost create rețele, puteți selecta rețeaua implicită (LAN) sau puteți accesaSetări > Rețele cu fir > LANpentru a crea unul. Comutatorul va examina dacă pachetele sunt redirecționate către rețeaua selectată.
IP Group	Selectați grupul IP pe care l-ați creat. Dacă nu a fost creat niciun grup de IP, faceți clic+Creează pe această pagină sau accesațiSetări > Profiluri > Grupuripentru a crea unul. Comutatorul va examina dacă adresa IP de destinație a pachetului se află în grupul IP.
Grupul de porturi IP	Selectați grupul de porturi IP pe care l-ați creat. Dacă nu a fost creat niciun grup de porturi IP, faceți clic+Creeazăpe această pagină sau accesațiSetări > Profiluri > Grupuripentru a crea unul. Comutatorul va examina dacă adresa IP de destinație și numărul portului pachetului se află în grupul de porturi IP.
Grupul MAC	Selectați grupul MAC pe care l-ați creat. Dacă nu a fost creat niciun grup MAC, faceți clic + Creațipe această pagină sau accesațiSetări > Profiluri > Grupuripentru a crea unul. Comutatorul va examina dacă adresa MAC de destinație a pachetului se află în grupul MAC.

3. Legați ACL-ul comutatorului la un port de comutare sau un VLAN și faceți clicaplica. Rețineți că un switch ACL are efect numai după ce este legat la un port sau VLAN.

Tip de legare	Specificați dacă să legați ACL-ul la porturi sau la un VLAN. Porturi: SelectațiToate porturilesauPorturi personalizateca interfețe care urmează să fie legate cu ACL. Cu toate porturile selectate, regula se aplică tuturor porturilor switch-ului. Cu porturile personalizate selectate, regula se aplică la porturile selectate ale comutatorului. Faceți clic pe porturile din Lista de dispozitive pentru a selecta porturile de legare.  VLAN: Selectați un VLAN din lista derulantă ca interfață de legat cu ACL. Dacă nu au fost create VLAN-uri, puteți selecta VLAN-ul implicit 1 (LAN) sau puteți accesaSetări > Rețele cu fir > LAN pentru a crea unul.

■ Configurarea EAP ACL

1. Selectați un site din lista derulantă aOrganizare. Mergi laSetări>Securitatea retelei>ACL. Sub fila EAP ACL, faceți clic + Create New Rule pentru a încărca următoarea pagină.



2. Definiți criteriile de filtrare a pachetelor ale regulii, inclusiv protocoalele, sursa și destinația și determinați dacă să redirecționați pachetele potrivite. Consultați următorul tabel pentru a configura parametrii necesari și faceți clicaplica.

Nume	Introduceți un nume pentru a identifica ACL.
stare	Faceți clic pe caseta de selectare pentru a activa ACL.

Politică	Selectați acțiunea care trebuie întreprinsă atunci când un pachet se potrivește cu regula. Permite: Redirecționați pachetul potrivit. Negați: Aruncați pachetul potrivit.
Protocoale	Selectați unul sau mai multe tipuri de protocol cărora li se aplică regula din lista derulantă. Valoarea implicită este All, indicând că pachetele tuturor protocoalelor vor fi potrivite. Când selectați unul dintre TCP și UDP sau ambele, puteți seta adresa IP și numărul de port al unui pachet ca criterii de filtrare a pachetelor în regulă.

Din lista derulantă Sursă, alegeți una dintre aceste opțiuni pentru a specifica sursa pachetelor la care se aplică acest ACL:

Rețea	Selectați rețeaua pe care ați creat-o. Dacă nu au fost create rețele, puteți selecta rețeaua implicită (LAN) sau puteți accesaSetări > Rețele cu fir > LANpentru a crea unul. EAP va examina dacă pachetele provin din rețeaua selectată.
IP Group	Selectați grupul IP pe care l-ați creat. Dacă nu a fost creat niciun grup de IP, faceți clic+Creează pe această pagină sau accesațiSetări > Profiluri > Grupuripentru a crea unul. EAP va examina dacă adresa IP sursă a pachetului se află în grupul IP.
Grupul de porturi IP	Selectați grupul de porturi IP pe care l-ați creat. Dacă nu a fost creat niciun grup de porturi IP, faceți clic+Creeazăpe această pagină sau accesațiSetări > Profiluri > Grupuripentru a crea unul. EAP va examina dacă adresa IP sursă și numărul portului pachetului se află în grupul de porturi IP.
SSID	Selectați SSID-ul pe care l-ați creat. Dacă nu a fost creat niciun SSID, accesațiSetări > Rețele fără firpentru a crea unul. EAP va examina dacă SSID-ul pachetului este SSID-ul selectat aici.

Din lista derulantă Destinație, alegeți una dintre aceste opțiuni pentru a specifica destinația pachetelor cărora li se aplică acest ACL:

Rețea	Selectați rețeaua pe care ați creat-o. Dacă nu au fost create rețele, puteți selecta rețeaua implicită (LAN) sau puteți accesaSetări > Rețele cu fir > LANpentru a crea unul. EAP va examina dacă pachetele sunt redirecționate către rețeaua selectată.
IP Group	Selectați grupul IP pe care l-ați creat. Dacă nu a fost creat niciun grup de IP, faceți clic+Creează pe această pagină sau accesațiSetări > Profiluri > Grupuripentru a crea unul. EAP va examina dacă adresa IP de destinație a pachetului se află în grupul IP.
Grupul de porturi IP	Selectați grupul de porturi IP pe care l-ați creat. Dacă nu a fost creat niciun grup de porturi IP, faceți clic+Creeazăpe această pagină sau accesațiSetări > Profiluri > Grupuripentru a crea unul. EAP va examina dacă adresa IP de destinație și numărul de port al pachetului se află în grupul de porturi IP.

3. 5. 2 Filtrare URL

Prezentare generală

Filtrarea URL permite unui administrator de rețea să creeze reguli pentru a bloca sau a permite anumite site-uri web, ceea ce le protejează de amenințările bazate pe web și să interzică accesul la site-uri web rău intenționate.

În filtrarea URL, sistemul compară adresele URL din solicitările HTTP, HTTPS și DNS cu listele de adrese URL care sunt definite în regulile de filtrare URL și interceptează solicitările care sunt direcționate către adrese URL blocate. Aceste reguli pot fi aplicate anumitor clienți sau grupuri al căror trafic trece prin gateway și EAP-uri.

Sistemul filtrează traficul în funcție de regulile din listă secvenţial. Prima potrivire determină dacă pachetul este acceptat sau abandonat, iar alte reguli nu sunt verificate după prima potrivire. Prin urmare, ordinea regulilor este critică. În mod implicit, regulile sunt prioritizate în funcție de secvența în care sunt create. Regula creată mai devreme este verificată pentru o potrivire cu o prioritate mai mare. Pentru a reordona regulile, selectați o regulă și trageți-o într-o nouă poziție. Dacă nicio regulă nu se potrivește, dispozitivul redirecționează pachetul din cauza unei clauze implicite Permit All.

Rețineți că regulile de filtrare URL au efecte cu o prioritate mai mare față de regulile ACL. Adică, sistemul va procesa mai întâi regula de filtrare URL atunci când regula de filtrare URL și regulile ACL sunt configurate în același timp.

Configurare

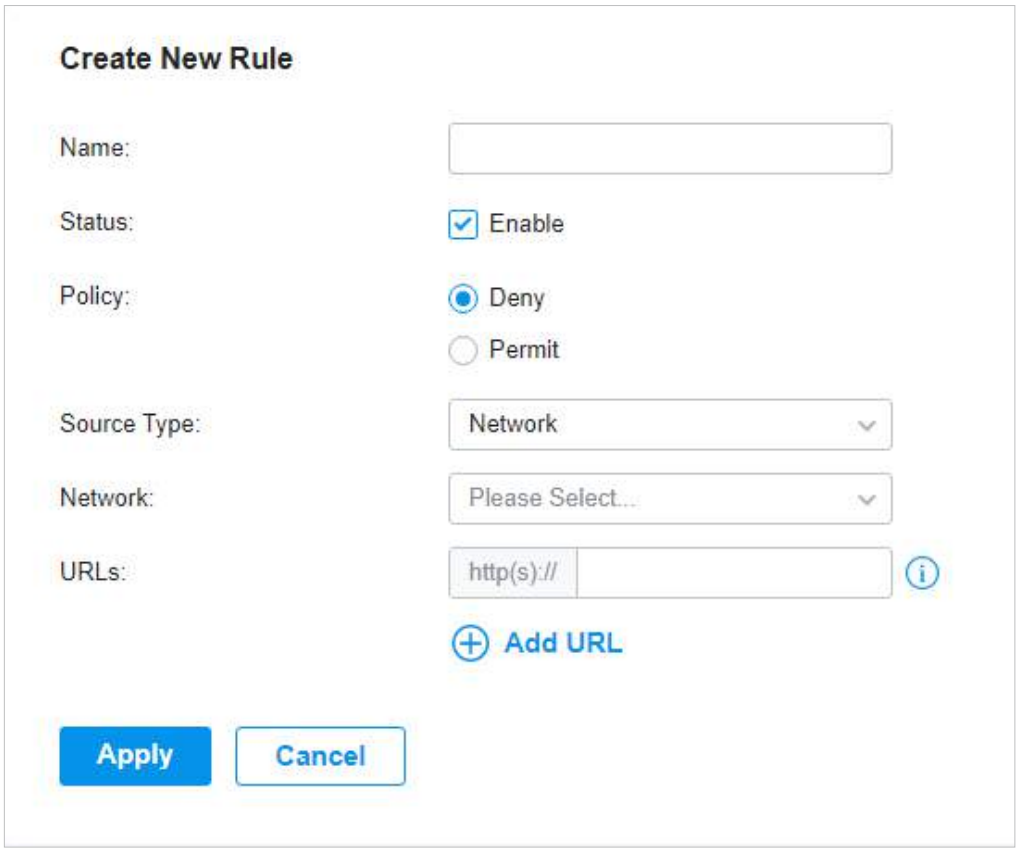
Pentru a finaliza configurația de filtrare URL, urmați acești pași:

1)Creați o nouă regulă de filtrare URL cu tipul specificat.

2)Definiți criteriile de filtrare ale regulii, inclusiv sursa și adresele URL și determinați dacă să redirecționați pachetele potrivite.

■ Configurarea regulilor Gateway

1. Selectați un site din lista derulantă aOrganizare. Mergi laSetări>Securitatea retelei>Filtrare URL. Sub fila Reguli Gateway, faceți clic + Create New Rule pentru a încărca următoarea pagină.



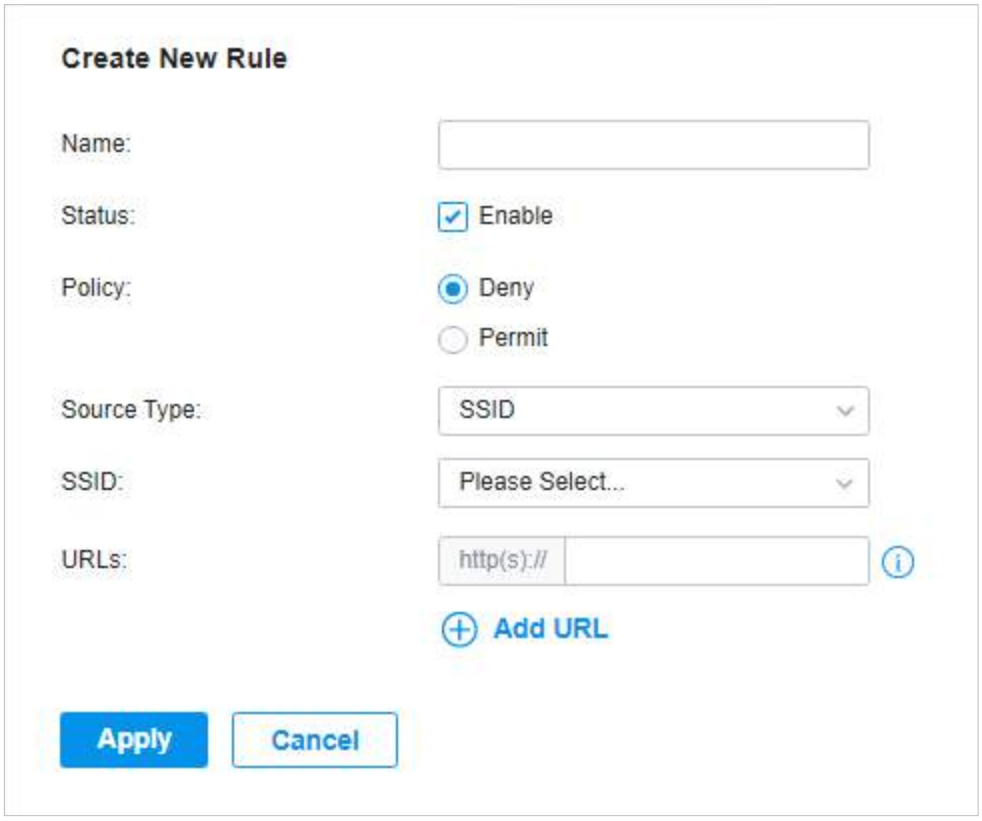
2. Definiți criteriile de filtrare ale regulii, inclusiv sursa și adresele URL și determinați dacă să redirecționați pachetele potrivite. Consultați următorul tabel pentru a configura parametrii necesari și faceți clic aplica.

Nume	Introduceți un nume pentru a identifica regula de filtrare a adreselor URL.
stare	Faceți clic pe caseta de selectare pentru a activa regula de filtrare a adreselor URL.
Politică	Selectați acțiunea care trebuie întreprinsă atunci când un pachet se potrivește cu regula. Negați: Aruncați pachetul potrivit și clienții nu pot accesa adresele URL. Permite: Redirecționați pachetul potrivit și clienții pot accesa adresele URL.
Tip sursă	Selectați sursa pachetelor pentru care se aplică această regulă. Rețea: Cu Rețea selectată, selectați rețeaua pe care ați creat-o din lista verticală Rețea. Dacă nu au fost create rețele, puteți selecta rețeaua implicită (LAN) sau puteți accesa Setări > Rețele cu fir > LANpentru a crea unul. Gateway-ul va filtra pachetele provenite din rețeaua selectată. IP Group: Cu IP Group selectat, selectați IP Group pe care l-ați creat din lista derulantă IP Group. Dacă nu a fost creat niciun grup de IP, faceți clic+CreeazăGrup IP nou pe această pagină sau accesațiSetări > Profiluri > Grupuripentru a crea unul. Gateway-ul va examina dacă adresa IP sursă a pachetului se află în grupul IP.

URL-uri	Introduceți adresa URL folosind până la 128 de caractere. Adresa URL trebuie furnizată într-un format valid. Adresa URL care conține un wildcard (*) este acceptată. O adresă URL cu un wildcard (*) poate corespunde mai multor subdomenii. De exemplu, cu *.tp-link.com specificat, community.tp-link.com va fi potrivit.

■ Configurarea regulilor EAP

1. Selectați un site din lista derulantă aOrganizare. Mergi laSetări>Securitatea retelei>Filtrare URL. În fila Reguli EAP, faceți clic + Create New Rule pentru a încărca următoarea pagină.



2. Definiți criteriile de filtrare ale regulii, inclusiv sursa și adresele URL și determinați dacă să redirecționați pachetele potrivite. Consultați următorul tabel pentru a configura parametrii necesari și faceți clic aplica.

Nume	Introduceți un nume pentru a identifica regula de filtrare a adreselor URL.
stare	Faceți clic pe caseta de selectare pentru a activa regula de filtrare a adreselor URL.
Politică	Selectați acțiunea care trebuie întreprinsă atunci când un pachet se potrivește cu regula. Negați: Aruncați pachetul potrivit și clienții nu pot accesa adresele URL. Permite: Redirecționați pachetul potrivit și clienții pot accesa adresele URL.
Tip sursă	Selectați SSID-ul pachetelor cărora li se aplică această regulă.

URL-uri	Introduceți adresa URL folosind până la 128 de caractere. Adresa URL trebuie furnizată într-un format valid. Adresa URL care conține un wildcard (*) este acceptată. O adresă URL cu un wildcard (*) poate corespunde mai multor subdomenii. De exemplu, cu *.tp-link.com specificat, community.tp-link.com va fi potrivit.

3. 5. 3 Apărare împotriva atacului

Prezentare generală

Atacurile inițiate prin utilizarea erorilor inerente ale protocoalelor de comunicare sau implementarea necorespunzătoare a rețelei au un impact negativ asupra rețelelor. În special, atacurile asupra unui dispozitiv de rețea pot cauza dispozitivul sau paralizia rețelei.

Cu caracteristica Attack Defense, gateway-ul poate identifica și elimina diferite pachete de atac din rețea și poate limita rata de primire a pachetelor. În acest fel, gateway-ul se poate proteja pe sine și rețeaua conectată împotriva atacurilor rău intenționate.

Gateway-ul oferă două tipuri de apărare împotriva atacurilor:

- Apărare împotriva inundațiilor

Dacă un atacator trimite un număr mare de pachete false către un dispozitiv țintă, dispozitivul țintă este ocupat cu aceste pachete false și nu poate procesa serviciile normale. Flood Defense detectează pachetele de inundații în timp real și limitează rata de primire a pachetelor pentru a proteja dispozitivul.

Atacurile de inundații includ atacuri de inundații TCP SYN, atacuri de inundații UDP și atacuri de inundații ICMP.

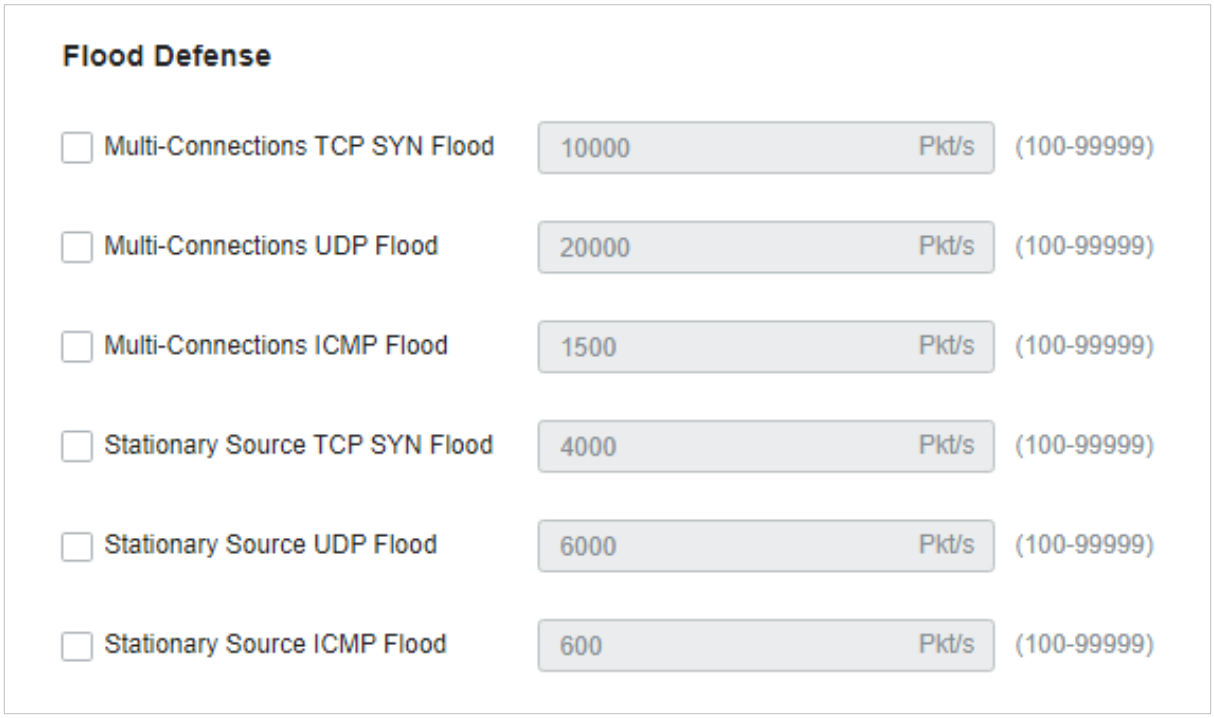
- Apărare împotriva anomaliilor de pachet

Pachetele anormale sunt pachete care nu se conformează standardelor sau conțin erori care le fac improprii procesării. Packet Anomaly Defense renunță direct la pachetele ilegale.

Configurare

Configurarea apărării împotriva inundațiilor

Selectați un site din lista derulantă aOrganizare. Mergi laSetări>Securitatea retelei>Apărare împotriva atacului. În Flood Defense, faceți clic pe caseta de selectare și setați limita corespunzătoare a ratei la care sunt primite anumite pachete.

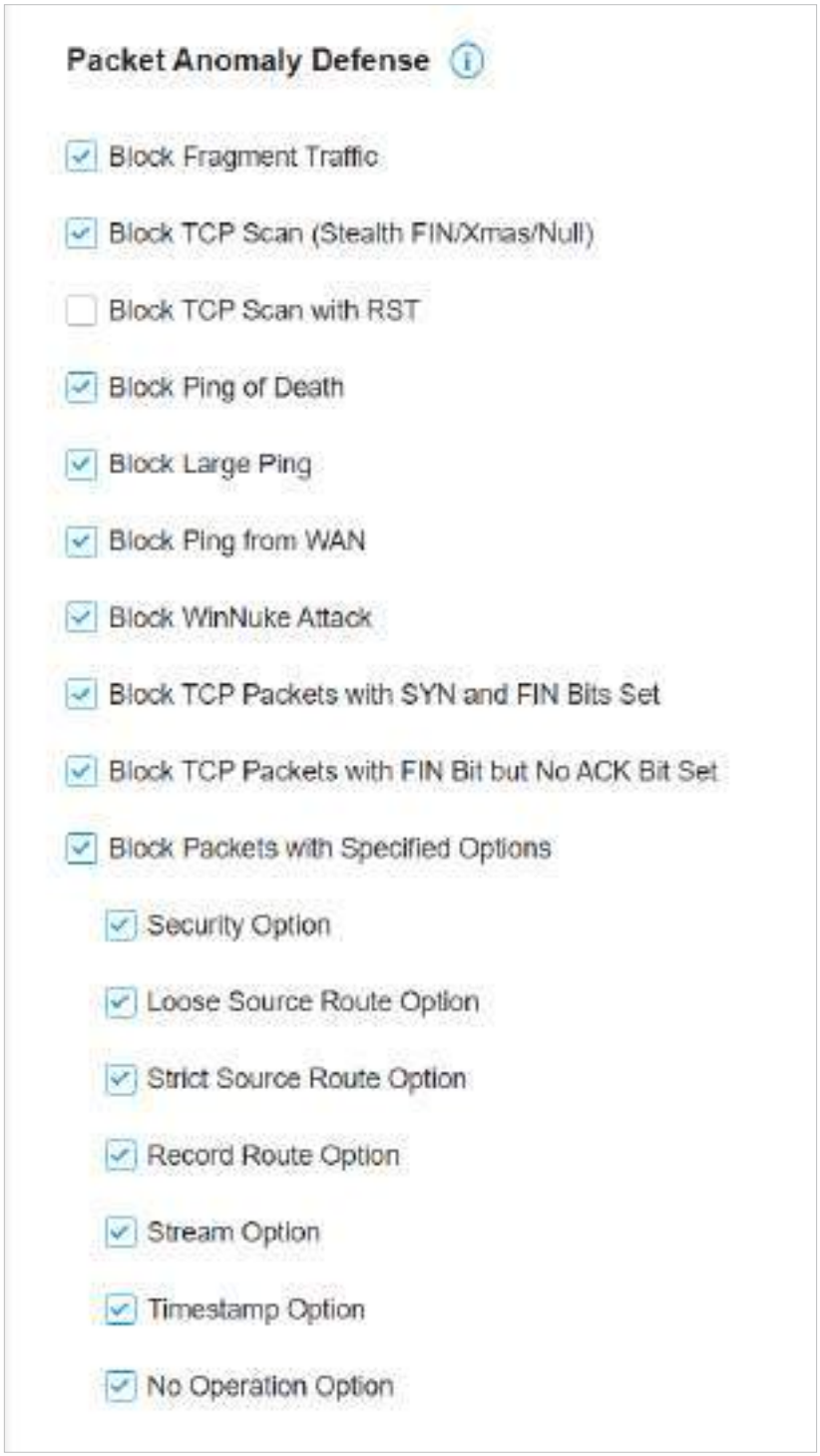


Multi-Conexiuni TCP SYN Flood	Un atac de inundație TCP SYN are loc atunci când atacatorul trimite sistemul țintă cu o succesiune de solicitări SYN (sincronizare). Când sistemul răspunde, atacatorul nu finalizează conexiunile, lăsând astfel conexiunea pe jumătate deschisă și inundând sistemul cu mesaje SYN. Atunci nu se pot face conexiuni legitime. Cu această caracteristică activată, gateway-ul limitează rata de primire a pachetelor TCP SYN de la toți clienții la rata specificată.
Multi-Conexiuni UDP Potop	Un atac UDP flood are loc atunci când atacatorul trimite un număr mare de pachete UDP către o gazdă țintă într-un timp scurt, gazda țintă este ocupată cu aceste pachete UDP și nu poate procesa serviciile normale. Cu această caracteristică activată, gateway-ul limitează rata de primire a pachetelor UDP de la toți clienții la rata specificată.
Multi-Conexiuni ICMP Potop	Dacă un atacator trimite multe mesaje ICMP Echo către dispozitivul țintă, dispozitivul țintă este ocupat cu aceste mesaje Echo și nu poate procesa alte pachete de date. Prin urmare, serviciile normale sunt afectate. Cu această caracteristică activată, sistemul limitează rata de primire a pachetelor ICMP de la toți clienții la rata specificată.

Sursă staționară TCP SYN Flood	Un atac de inundație TCP SYN are loc atunci când atacatorul trimite sistemul țintă cu o succesiune de solicitări SYN (sincronizare). Când sistemul răspunde, atacatorul nu finalizează conexiunile, lăsând astfel conexiunea pe jumătate deschisă și inundând sistemul cu mesaje SYN. Atunci nu se pot face conexiuni legitime. Cu această caracteristică activată, gateway-ul limitează rata de primire a pachetelor TCP SYN de la un singur client la rata specificată.
Sursă staționară UDP Potop	Un atac UDP flood are loc atunci când atacatorul trimite un număr mare de pachete UDP către o gazdă țintă într-un timp scurt, gazda țintă este ocupată cu aceste pachete UDP și nu poate procesa serviciile normale. Cu această caracteristică activată, gateway-ul limitează rata de primire a pachetelor UDP de la un singur client la rata specificată.
Sursă staționară ICMP Potop	Dacă un atacator trimite multe mesaje ICMP Echo către dispozitivul țintă, dispozitivul țintă este ocupat cu aceste mesaje Echo și nu poate procesa alte pachete de date. Prin urmare, serviciile normale sunt afectate. Cu această caracteristică activată, sistemul limitează rata de primire a pachetelor ICMP de la un singur client la rata specificată.

Configurarea apărării împotriva anomaliilor de pachete

Selectați un site din lista derulantă aOrganizare. Mergi laSetări>Securitatea retelei>Apărare împotriva atacului. În Packet Anomaly Defense, faceți clic pe caseta de selectare și setați limita corespunzătoare a ratei la care sunt primite anumite pachete.



Blocați traficul fragmentelor	Cu această opțiune activată, pachetele fragmentate fără prima parte a pachetului vor fi aruncate.

Blocare scanare TCP (Stealth FIN/Xmas/Null)	Cu această opțiune activată, gateway-ul va bloca pachetele anormale în următoarele scenarii de atac: Scanare FIN Stealth: Atacatorul trimite pachetul cu câmpul SYN și câmpul FIN setat la 1. Câmpul SYN este folosit pentru a solicita conexiunea inițială, în timp ce câmpul FIN este folosit pentru a solicita deconectarea. Prin urmare, pachetul de acest tip este ilegal. Scanare de Xmas: atacatorul trimite pachetul ilegal cu indexul TCP, câmpul FIN, URG și PSH setat la 1. Scanare nulă: Atacatorul trimite pachetul ilegal cu indexul său TCP și toate câmpurile de control setate la 0. În timpul conexiunii TCP și transmisiei de date, pachetele cu toate câmpurile de control setate la 0 sunt considerate ilegale.
Blocați scanarea TCP cu RST	Cu această opțiune activată, gateway-ul va răspunde la mesajele RST. Este dezactivat implicit.
Block Ping of Death	Cu această opțiune activată, gateway-ul va bloca atacul Ping of Death. Atacul Ping of Death înseamnă că atacatorul trimite pachete ping anormale care sunt mai mici de 64 de octeți sau mai mari de 65535 de octeți pentru a provoca blocarea sistemului pe computerul țintă.
Block Ping mare	Cu această opțiune activată, routerul va bloca pachetele ping care sunt mai mari de 1024 de pachete pentru a proteja sistemul de atacul Large Ping.
Blocați ping de la WAN	Cu această opțiune activată, routerul va bloca cererea ICMP de la WAN.
Blocați atacul WinNuke	Cu această opțiune activată, routerul va bloca atacurile WinNuke. Atacul WinNuke se referă la un atac la distanță DoS (denial-of-service) care afectează unele sisteme de operare Windows, cum ar fi Windows 95. Atacatorul trimite un șir de date OOB (Out of Band) către computerul țintă pe portul TCP 137, 138 sau 139, provocând blocarea sistemului sau Ecranul albastru al morții.
Blocați pachetele TCP cu setați de biți SYN și FIN	Cu această opțiune activată, routerul va filtra pachetele TCP cu atât SYN Bit, cât și FIN Bit setate.
Blocați pachetele TCP cu bit FIN dar fără set de biți ACK	Cu această opțiune activată, routerul va filtra pachetele TCP cu bitul FIN setat, dar fără bitul ACK setat.
Blocați pachetele cu Opțiuni specificate	Cu această opțiune activată, routerul va filtra pachetele cu opțiuni IP specificate, inclusiv Opțiunea de securitate, Opțiunea rută sursă liberă, Opțiunea rută sursă strictă, Opțiunea rută înregistrare, Opțiunea Stream, Opțiunea ștampilă de timp și Opțiunea fără operare. Puteți alege opțiunile în funcție de nevoile dvs.

3. 5. 4 Firewall

Prezentare generală

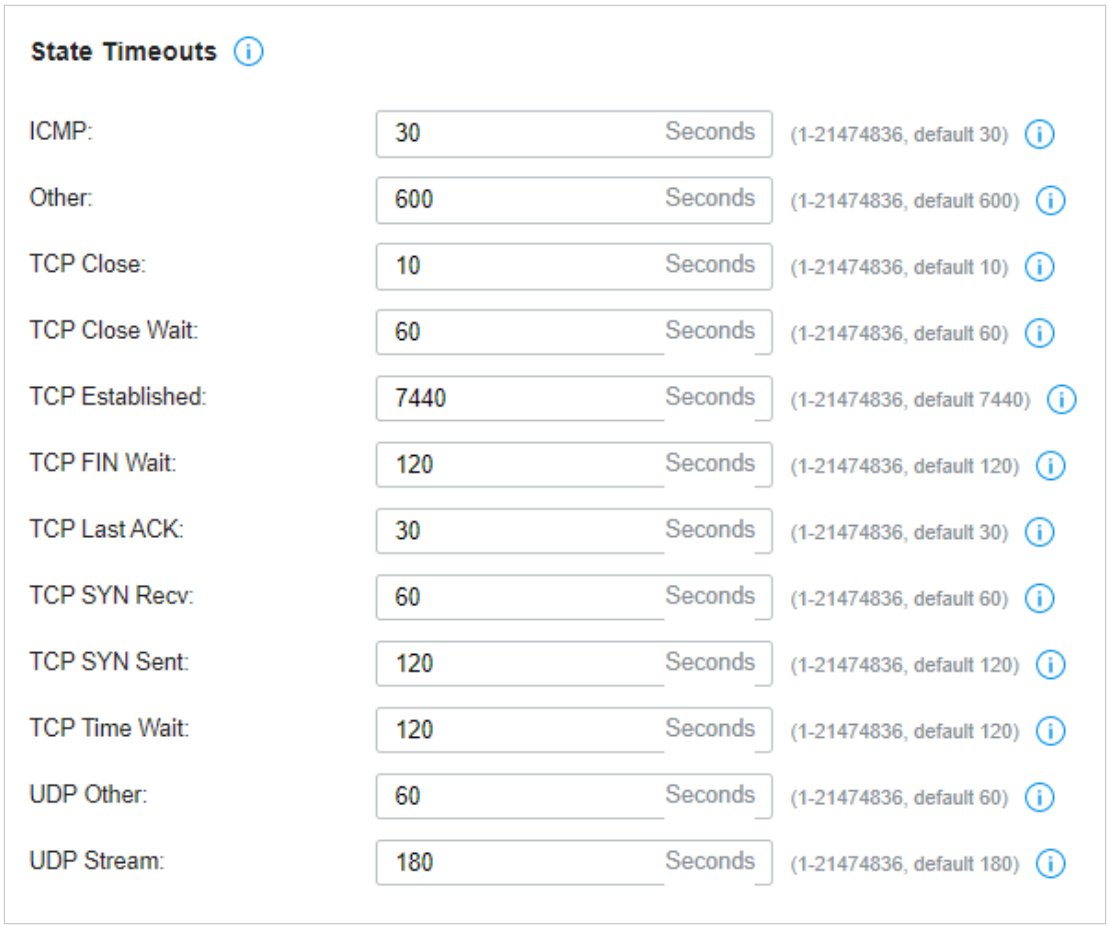
Firewall este folosit pentru a spori securitatea rețelei. În State Timeouts, puteți specifica un număr de timeouts pentru sesiuni, inclusiv conexiunea TCP, UDP și ICMP. Pachetele vor fi redirecționate în intervalul de timp specificat. Când nu există niciun răspuns după timpul specificat, sesiunea sau starea vor fi închise. Timeout de stare va ajuta la închiderea sesiunilor inactive și, astfel, va evita funcționarea defectuoasă a rețelei. În Firewall

Opțiuni, puteți configura în continuare gateway-ul pentru a preveni atacuri precum atacurile SYN flood și ping-ul de difuzare.

Configurare

■ Configurarea timeout-urilor de stat

Selectați un site din lista derulantă aOrganizare. Mergi laSetări>Securitatea retelei>Firewall. În Sate Timeouts, setați limita de timp pentru diferitele sesiuni.

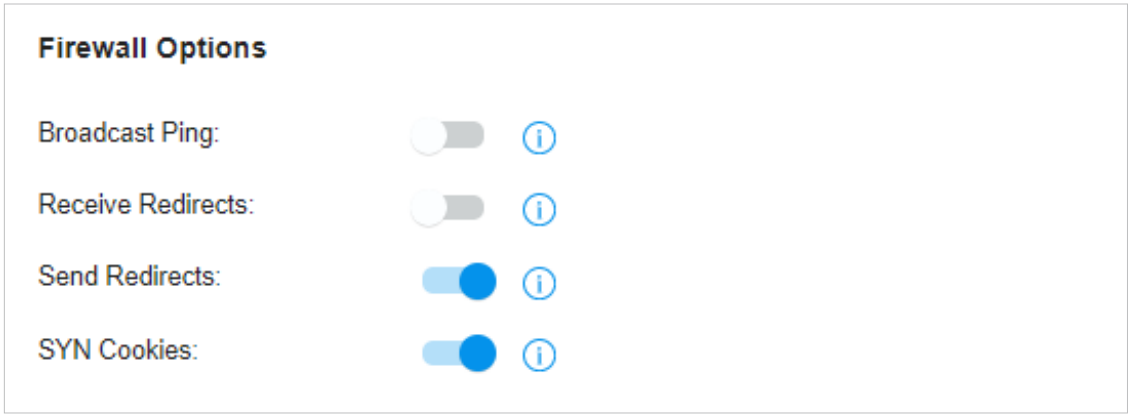


ICMP	Sesiunea ICMP va fi închisă dacă nu există niciun răspuns după timpul stabilit.
Alte	Sesiunile pentru protocoale care exclud TCP, UDP și ICMP vor fi închise dacă nu există niciun răspuns după timpul stabilit.
TCP Close	Starea TCP Close va fi închisă dacă nu există niciun răspuns după timpul stabilit.
TCP Închide Așteptați	Starea TCP Close Wait va fi închisă dacă nu există niciun răspuns după timpul stabilit.
TCP stabilit	Starea TCP Stabilit va fi închisă dacă nu există niciun răspuns după timpul stabilit.
TCP FIN Așteaptă	Starea TCP FIN Wait va fi închisă dacă nu există niciun răspuns după timpul stabilit.
Ultimul ACK TCP	Starea TCP Last ACK va fi închisă dacă nu există niciun răspuns după timpul stabilit.

TCP SYN Recv	Starea TCP SYN (Sincronizare) Recv va fi închisă dacă nu există niciun răspuns după timpul setat.
TCP SYN trimis	Starea TCP SYN (Synchronize) Sent va fi închisă dacă nu există niciun răspuns după timpul stabilit.
TCP Time Wait	Starea TCP Time Wait va fi închisă dacă nu există niciun răspuns după timpul stabilit.
UDP Altele	Conexiunile UDP cu trafic într-o singură direcție vor fi oprite dacă nu există niciun răspuns după ora stabilită.
Fluxul UDP	Conexiunile UDP cu trafic bidirecțional vor fi oprite dacă nu există niciun răspuns după timpul stabilit.

■ Configurarea opțiunilor pentru firewall

Selectați un site din lista derulantă aOrganizare. Mergi laSetări>Securitatea retelei>Firewall. În Sate Timeouts, setați limita de timp pentru diferitele sesiuni.



Transmite Ping	Cu aceasta activată, gateway-ul va răspunde la ping-urile difuzate.
Primiți redirecționări	Cu acesta activat, gateway-ul va accepta redirecționări ICMP.
Trimiteți redirecționări	Cu acesta activat, gateway-ul va trimite redirecționări ICMP.
Cookie-uri SYN	Cu acesta activat, cookie-urile SYN vor fi folosite pentru a rezista atacurilor SYN flood care doresc să deschidă porturi pe gateway.

3. 6 Transmisie

Transmisia vă ajută să controlați traficul în rețea în mai multe moduri. Puteți adăuga politici și reguli pentru a controla rutele de transmisie și pentru a limita sesiunea și lățimea de bandă.

3. 6. 1 Traseul

Prezentare generală

- Traseu Static

  Traficul de rețea este orientat către o destinație specifică, iar Ruta Statică desemnează următorul hop sau interfața către care să redirecționeze traficul.

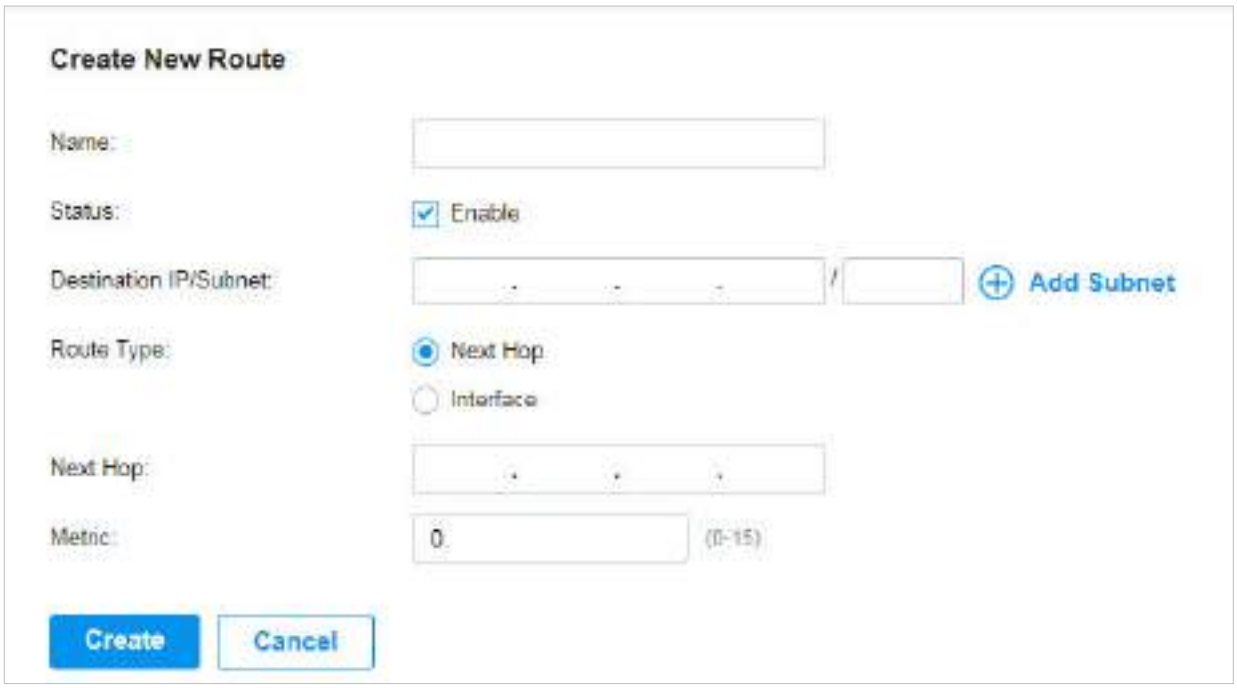
- Rutarea politicii

  Policy Routing desemnează portul WAN pe care routerul îl folosește pentru a redirecționa traficul în funcție de sursă, destinație și protocolul traficului.

Configurare

- Traseu Static

1. AccesațiSetări>Transmitere>Dirijare>Traseu Static. Clic+ Creați o rută nouăpentru a încărca următoarea pagină și a configura parametrii.



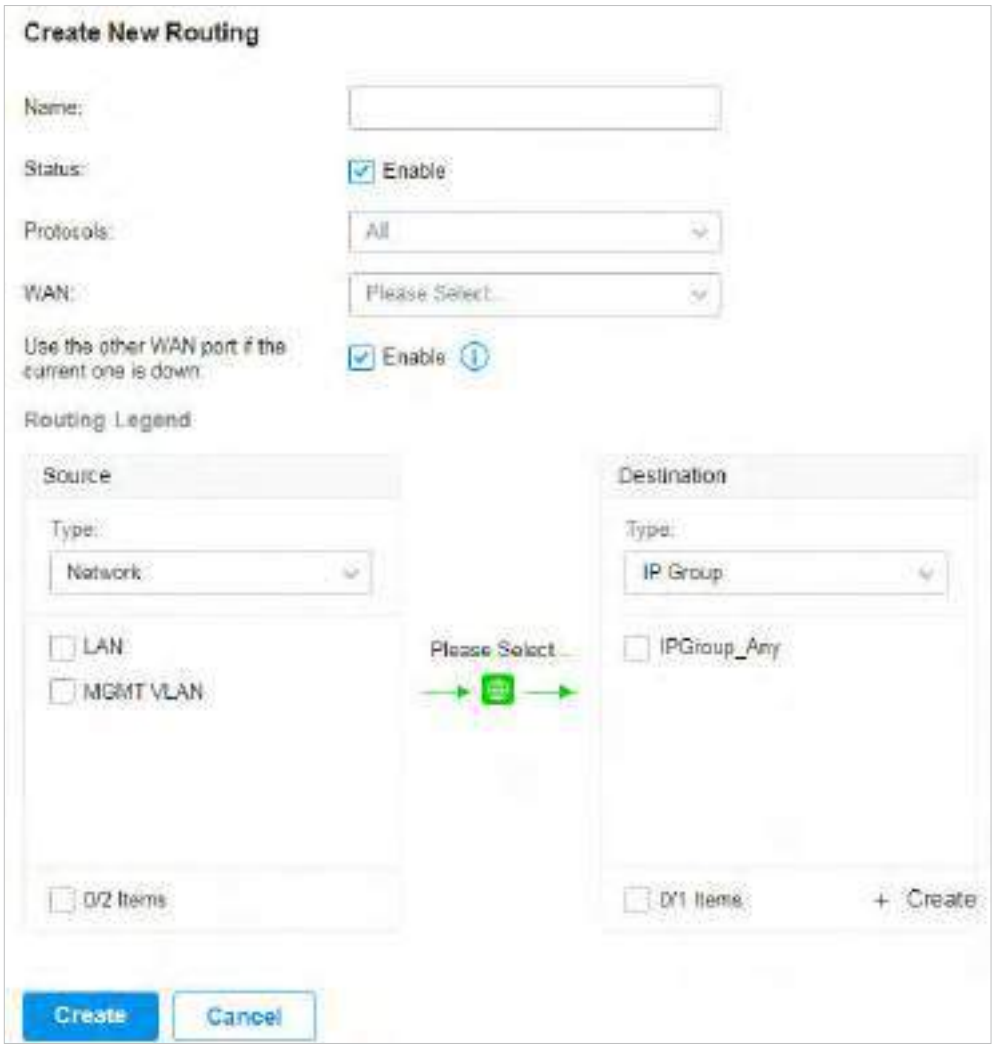
Nume	Introduceți numele pentru a identifica intrarea Static Route.
stare	Activați sau dezactivați intrarea Rută statică.

IP/Subrețea de destinație	Destination IP/Subnet identifică traficul de rețea pe care îl controlează intrarea Static Route. Specificați destinația traficului de rețea în formatul 192.168.0.1/24. Puteți da clic+ Adăugați subrețeapentru a specifica mai multe IP-uri de destinație/ Subrețele și faceți clic pentru a le șterge.
Tip traseu	Următorul pas:Cu Next Hop selectat, dispozitivele dvs. redirecționează traficul de rețea corespunzător către o anumită adresă IP. Trebuie să specificați adresa IP ca Next Hop. Interfata:Cu Interfață selectată, dispozitivele dvs. redirecționează traficul de rețea corespunzător printr-o interfață specifică. Trebuie să specificați interfața în funcție de nevoile dvs.
Metric	Definiți prioritatea intrării Rută statică. O valoare mai mică înseamnă o prioritate mai mare. Dacă mai multe intrări se potrivesc cu IP/Subrețea de destinație a traficului, intrarea cu prioritate mai mare are prioritate. În general, puteți păstra pur și simplu valoarea implicită.

2. Faceți clicCrea. Noua intrare Static Route este adăugată la tabel. Puteți face clic pentru a edita intrarea. Puteți face clic pentru a șterge intrarea.

- Rutarea politicii

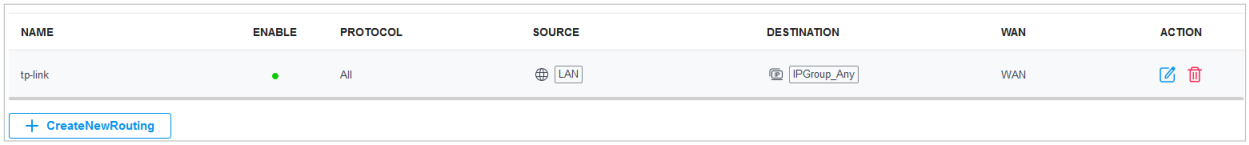
1. AccesațiSetări>Transmitere>Dirijare>Rutarea politicii. Clic+ Creați o nouă rutarepentru a încărca următoarea pagină și a configura parametrii.



Nume	Introduceți numele pentru a identifica intrarea Policy Routing.
stare	Activați sau dezactivați intrarea Policy Routing.
Protocoale	Selectați protocoalele de trafic pe care le controlează intrarea Policy Routing. Intrarea Policy Routing are efect numai atunci când traficul corespunde criteriilor intrării, inclusiv protocoalele.
WAN	Selectați portul WAN prin care să redirecționați traficul. Dacă doriți să redirecționați traficul prin celălalt port WAN atunci când WAN-ul actual este oprit, activațiUtilizați celălalt port WAN dacă WAN-ul actual este oprit.

Legenda de rutare	Intrarea Policy Routing are efect numai atunci când traficul care utilizează protocoalele specificate se potrivește cu sursa și destinația specificate în Legenda de rutare. Selectați tipul sursei și destinației de trafic. Rețea: Selectați interfețele LAN pentru sursa sau destinația de trafic. IP Group: Selectați grupul IP pentru sursa sau destinația de trafic. Puteți da clic+ Creați pentru a crea un nou grup IP. Grup de porturi IP:Selectați grupul de porturi IP pentru sursa sau destinația de trafic. Puteți da clic+ Creațipentru a crea un nou grup de porturi IP.

2. Faceți clicCrea. Noua intrare Policy Routing este adăugată la tabel. Puteți face clic pentru a edita intrarea. Puteți face clic pentru a șterge intrarea.



3. 6. 2 NAT

Prezentare generală

- Port forwarding

  Puteți configura Port Forwarding pentru a permite utilizatorilor de internet să acceseze gazdele locale sau să utilizeze serviciile de rețea care sunt implementate în LAN.

  Port Forwarding ajută la stabilirea conexiunilor de rețea între o gazdă de pe internet și cealaltă din LAN, permițând traficului să treacă prin portul specific al gateway-ului. Fără Port Forwarding, gazdele din LAN sunt de obicei inaccesibile de pe internet de dragul securității.

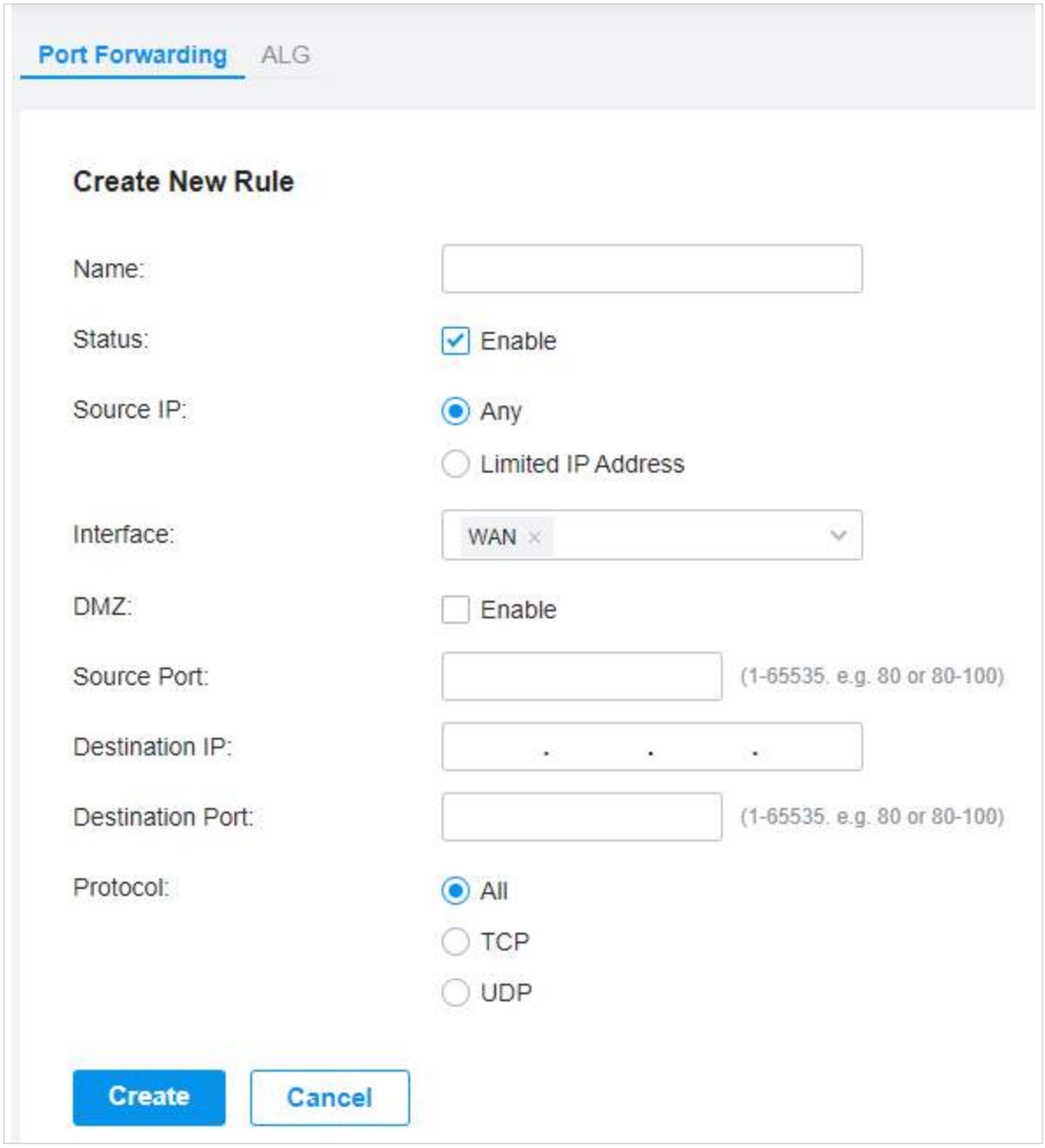
- ALG

  ALG se asigură că anumite protocoale la nivel de aplicație funcționează corespunzător prin gateway-ul dumneavoastră.

Configurare

■ Port forwarding

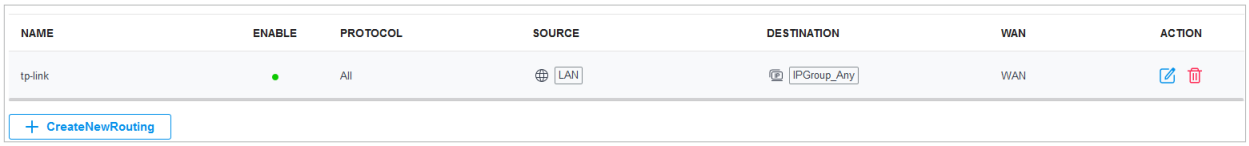
1. AccesațiSetări>Transmitere>NAT>Port forwarding. Clic+ Creați o nouă regulăpentru a încărca următoarea pagină și a configura parametrii.



Nume	Introduceți numele pentru a identifica regula de redirecționare a portului.
stare	Activați sau dezactivați regula Port Forwarding.

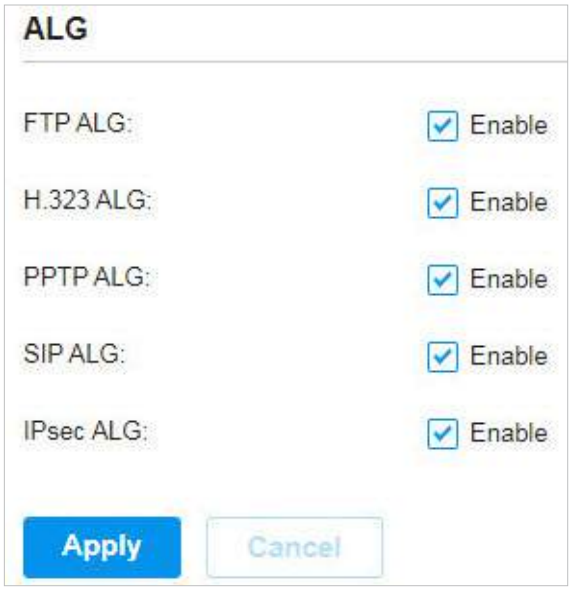
IP sursă	Orice: regula se aplică traficului de la orice adresă IP sursă. Adresă IP limitată: regula se aplică numai traficului de la anumite adrese IP. Cu această opțiune selectată, specificați adresele IP și subrețelele în funcție de nevoile dvs.
Interfață	Selectați interfața căreia i se aplică regula. Traficul care este primit prin interfață este redirecționat conform regulii.
DMZ	Cu DMZ activat, tot traficul este redirecționat cătreIP de destinațieîn LAN, port la port. Trebuie să specificațiIP de destinație. Cu DMZ dezactivat, numai traficul care se potrivește cuPort sursăsi Protocol este transmis. Traficul este redirecționat cătrePortul de destinațieal IP de destinațieîn LAN. Trebuie să specificațiPort sursă,IP de destinație, Portul de destinație, șiProtocol.
Port sursă	Poarta de acces folosesțePort sursăpentru a primi traficul de pe internet. Doar traficul care se potrivește cuPort sursăsiProtocoleste transmis.
IP de destinație	Traficul este redirecționat către gazdaIP de destinațieîn LAN.
Portul de destinație	Traficul este redirecționat cătrePortul de destinațiea gazdei în LAN.
Protocol	Traficul de rețea este transmis folosind fie protocolul TCP, fie UDP. Doar traficul care se potrivește cuPort sursăsiProtocoleste transmis. Dacă doriți să fie redirecționat atât traficul TCP, cât și traficul UDP, selectațiToate.

2. Faceți clicCrea. Noua intrare Port Forwarding este adăugată la tabel. Puteți face clic pentru a edita intrarea. Puteți face clic pentru a șterge intrarea.



ALG

Mergi laSetări>Transmitere>NAT>ALG. Activați sau dezactivați anumite tipuri de ALG în funcție de nevoile dvs. și faceți clicaplica.



FTP ALG	FTP ALG permite serverului FTP și clientului să transfere date utilizând protocolul FTP într-unul dintre următoarele scenarii: • Serverul FTP este în LAN, în timp ce clientul FTP este pe internet. • Serverul FTP este pe internet, în timp ce clientul FTP este în LAN. • Serverul FTP și clientul FTP sunt în rețele LAN diferite.
H.323 ALG	H.323 ALG permite telefoanelor IP și dispozitivelor multimedia să configureze conexiuni folosind protocolul H.323 într-unul dintre următoarele scenarii: • Unul dintre punctele finale se află în LAN, în timp ce celălalt este pe internet. • Punctele finale sunt în rețele LAN diferite.
PPTP ALG	PPTP ALG permite serverului și clientului PPTP să configureze o VPN PPTP într-unul dintre următoarele scenarii: • Serverul PPTP se află în LAN, în timp ce clientul PPTP este pe internet. • Serverul PPTP este pe internet, în timp ce clientul PPTP este în LAN. • Serverul PPTP și clientul PPTP sunt în rețele LAN diferite.
SIP ALG	SIP ALG permite telefoanelor IP și dispozitivelor multimedia să configureze conexiuni folosind protocolul SIP într-unul dintre următoarele scenarii: • Unul dintre punctele finale se află în LAN, în timp ce celălalt este pe internet. • Punctele finale sunt în rețele LAN diferite.
IPsec ALG	IPsec ALG permite punctelor finale IPsec să configureze un VPN IPsec într-unul dintre următoarele scenarii: • Unul dintre punctele finale se află în LAN, în timp ce celălalt este pe internet. • Punctele finale sunt în rețele LAN diferite.

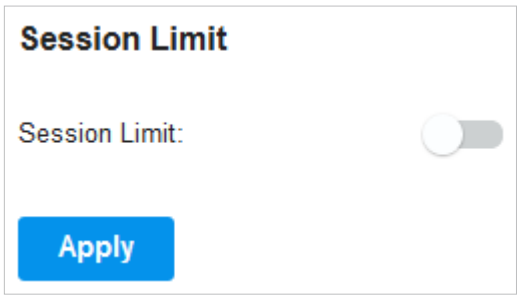
3. 6. 3 Limita sesiunii

Prezentare generală

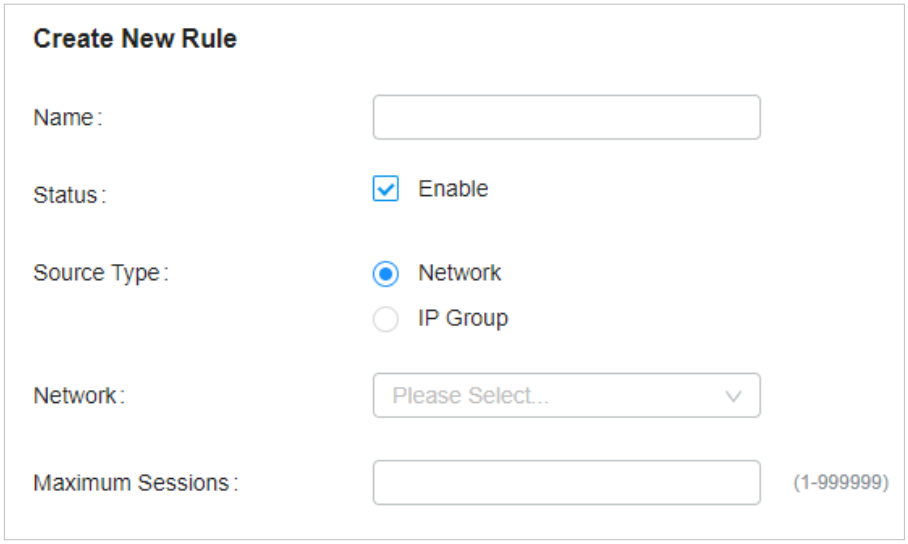
Session Limit optimizează performanța rețelei prin limitarea sesiunilor maxime ale anumitor surse.

Configurare

1. AccesațiSetări>Transmitere>Limită de sesiune. ÎnLimită de sesiune, activați Session Limit global și faceți clicaplica.



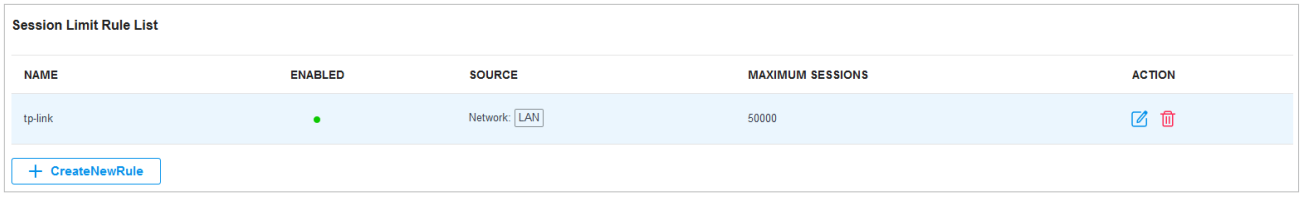
2. ÎnLista de reguli pentru limita de sesiune, faceți clic+ Creați o nouă regulăpentru a încărca următoarea pagină și a configura parametrii.



Nume	Introduceți numele pentru a identifica regula limită de sesiune.
stare	Activați sau dezactivați regula Limita sesiunii.
Tip sursă	Rețea: Limitați sesiunile maxime ale rețelelor LAN specifice. Cu această opțiune selectată, selectați rețelele în care le puteți personalizaRețele cu fir>Rețele LAN. Pentru configurarea detaliată a rețelelor, consultați3. 3. 2 Configurați rețele LAN. IP Group: Limitați sesiunile maxime ale anumitor grupuri IP. Cu această opțiune selectată, selectați grupurile IP, pe care le puteți personalizaProfiluri>Grupuri. Pentru configurarea detaliată a grupurilor IP, consultați3. 8 Creați profiluri.

Sesiuni maxime	Introduceți sesiunile maxime ale surselor specifice.

3. Faceți clicCrea. Noua regulă Limită de sesiune este adăugată la listă. Puteți face clic pentru a edita regula. Puteți face clic pentrula șterge regula.



3. 6. 4 Control lățimea de bandă

Prezentare generală

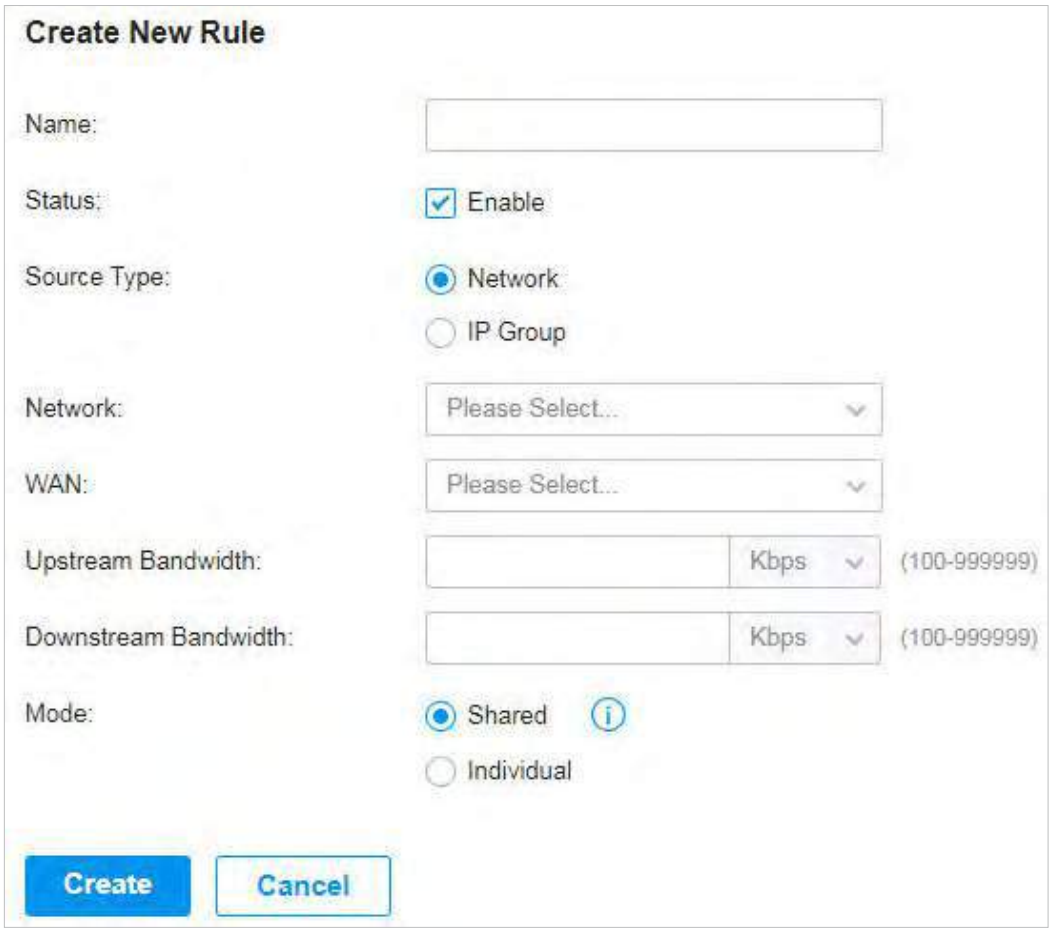
Controlul lățimii de bandă optimizează performanța rețelei prin limitarea lățimii de bandă a anumitor surse.

Configurare

1. AccesațiSetare>Transmitere>Controlul lățimii de bandă. ÎnControlul lățimii de bandă, activați Controlul lățimii de bandă la nivel global și configurați parametrii. Apoi apasaaplica.

Controlul pragului	Cu controlul pragului activat, controlul lățimii de bandă are efect numai atunci când utilizarea totală a lățimii de bandă atinge procentul specificat. Trebuie să specificați lățimea de bandă în amonte totală și lățimea de bandă în aval a porturilor WAN. Se recomandă utilizareaTest de vitezăinstrument pentru a decide lățimea de bandă în amonte și lățimea de bandă în aval.

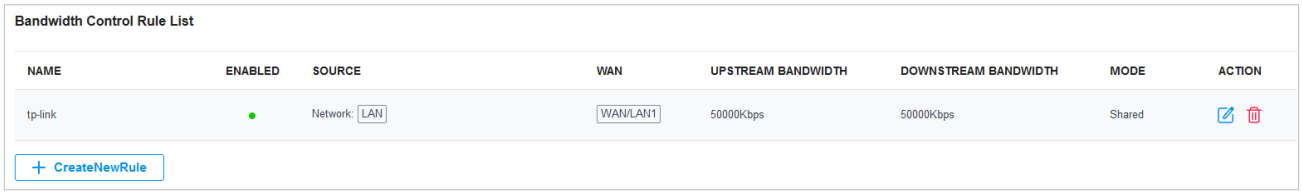
2. ÎnLista regulilor de control al lățimii de bandă, faceți clic+ Creați o nouă regulăpentru a încărca următoarea pagină și a configura parametrii.



Nume	Introduceți numele pentru a identifica regula de control al lățimii de bandă.
stare	Activați sau dezactivați regula de control a lățimii de bandă.
Tip sursă	Rețea: Limitați lățimea de bandă maximă a anumitor rețele LAN. Cu această opțiune selectată, selectați rețelele în care le puteți personalizaRețele cu fir>Rețele LAN. Pentru configurarea detaliată a rețelelor, consultați3. 3. 2 Configurați rețele LAN. IP Group: Limitați lățimea de bandă maximă a anumitor grupuri IP. Cu această opțiune selectată, selectați grupurile IP, pe care le puteți personalizaProfiluri>Grupuri. Pentru configurarea detaliată a grupurilor IP, consultați3. 8 Creați profiluri.
WAN	Selectați portul WAN căruia i se aplică regula.
Lățimea de bandă în amonte	Specificați limita lățimii de bandă în amonte, pe care o folosesc gazdele locale specifice pentru a transmite traficul către internet prin gateway.
Lățimea de bandă în aval	Specificați limita lățimii de bandă în aval, pe care o folosesc gazdele locale specifice pentru a primi trafic de pe internet prin gateway.

Modul	Specificați modul de control al lățimii de bandă pentru anumite gazde locale. Impartit: Lățimea de bandă totală pentru toate gazdele locale este egală cu valorile specificate. Individual: Lățimea de bandă pentru fiecare gazdă locală este egală cu valorile specificate.

3. Faceți clicCrea. Noua regulă de control a lățimii de bandă este adăugată la listă. Puteți face clic pentru a edita regula. Puteți face clic pentru a șterge regula.



3. 7 Configurați VPN

VPN (Virtual Private Network) oferă un mijloc de comunicare securizată între computere la distanță printr-o rețea publică largă (WAN), cum ar fi internetul. Gateway-urile gestionate Omada acceptă diferite tipuri de VPN.

3. 7. 1 VPN

Prezentare generală

VPN (Virtual Private Network) oferă rețelelor LAN de la distanță sau utilizatorilor acces securizat la resursele LAN printr-o rețea publică, cum ar fi internetul. Virtual indică că conexiunea VPN se bazează pe conexiunea logică end-to-end în loc de conexiunea fizică end-to-end. Privat indică că utilizatorii pot stabili conexiunea VPN în funcție de cerințele lor și numai anumiți utilizatori au voie să utilizeze conexiunea VPN.

Miezul conexiunii VPN este realizarea comunicației tunel, care îndeplinește sarcina de încapsulare a datelor, transmitere și decomprimare a datelor prin intermediul protocolului de tunel. Gateway-ul acceptă protocoale comune de tunel pe care le folosește un VPN pentru a menține datele în siguranță:

- IPsec

IPsec (Securitate IP) poate oferi servicii de securitate, cum ar fi confidențialitatea datelor, integritatea datelor și autentificarea datelor la nivelul IP. IPsec folosește IKE (Internet Key Exchange) pentru a gestiona negocierea protocoalelor și a algoritmilor pe baza politicii specificate de utilizator și pentru a genera cheile de criptare și autentificare care vor fi utilizate de IPsec. IPsec poate fi folosit pentru a proteja una sau mai multe căi între o pereche de gazde, între o pereche de gateway-uri de securitate sau între o gateway de securitate și o gazdă.

- PPTP

PPTP (Point-to-Point Tunneling Protocol) este un protocol de rețea care permite transferul securizat de date de la un client la distanță la un server privat de întreprindere prin crearea unui VPN prin rețelele de date bazate pe TCP/IP. PPTP folosește numele de utilizator și parola pentru a valida utilizatorii.

- L2TP

L2TP (Layer 2 Tunneling Protocol) oferă o modalitate pentru un utilizator de dialup de a realiza o conexiune virtuală Point-to-Point Protocol (PPP) la un server de rețea L2TP (LNS), care poate fi o poartă de securitate. L2TP trimite cadre PPP printr-un tunel între un concentrator de acces L2TP (LAC) și LNS. Din cauza lipsei de confidențialitate inerente protocolului L2TP, acesta este adesea implementat împreună cu IPsec. L2TP folosește numele de utilizator și parola pentru a valida utilizatorii.

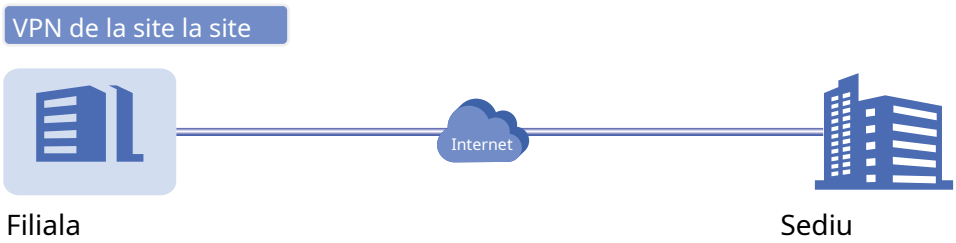
- OpenVPN

OpenVPN folosește OpenSSL pentru criptarea UDP și TCP pentru transmiterea traficului. OpenVPN folosește o conexiune client-server pentru a oferi comunicații sigure între un server și un client la distanță prin internet. Unul dintre cei mai importanți pași în configurarea OpenVPN este obținerea unui certificat care este utilizat pentru autentificare. Controlerul Omada SDN acceptă generarea certificatului care poate fi descărcat ca fișier pe computer. Cu certificatul importat, clienții la distanță sunt verificați de certificat și li se acordă acces la resursele LAN.

Există multe variante ale rețelelor private virtuale, majoritatea bazate pe două modele principale:

■ VPN de la site la site

Un VPN Site-to-Site creează o conexiune între două rețele din locații geografice diferite. În mod obișnuit, sediul central stabilește VPN Site-to-Site cu filiala pentru a oferi sucursalei acces la rețeaua sediului central.



Gateway-ul gestionat Omada acceptă două tipuri de VPN-uri Site-to-Site:

• IPsec automat

Controlerul creează automat un tunel VPN IPsec între două site-uri de pe același controler. Conexiunea VPN este bidirecțională. Adică, crearea unui VPN Auto IPsec de la site-ul A la site-ul B oferă, de asemenea, conectivitate de la site-ul B la site-ul A și nu este nevoie de nimic pentru a fi configurat pe site-ul B.

• IPsec manual

Creați manual un tunel VPN IPsec între două routere peer prin internet, de la un router local la un router de la distanță care acceptă IPsec. Poarta de acces gestionată de Omada pe acest site este routerul peer local.

■ VPN de la client la site

Un VPN de la client la site creează o conexiune la LAN de la o gazdă la distanță. Este util pentru lucrătorii la distanță și călătorii de afaceri să își acceseze rețeaua LAN centrală dintr-o locație la distanță, fără a compromite confidențialitatea și securitatea.

Primul pas pentru a construi o conexiune VPN Client-la-Site este de a determina rolul gateway-urilor și ce protocol de tunel VPN să utilizeze:

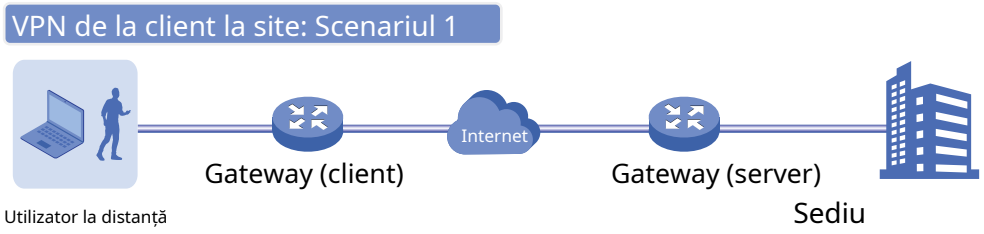
• Server VPN

Gateway-ul de pe LAN central funcționează ca un server VPN pentru a oferi unei gazde la distanță acces la rețeaua locală. Gateway-ul care funcționează ca server VPN poate folosi L2TP, PPTP, IPsec sau OpenVPN ca protocol de tunel.

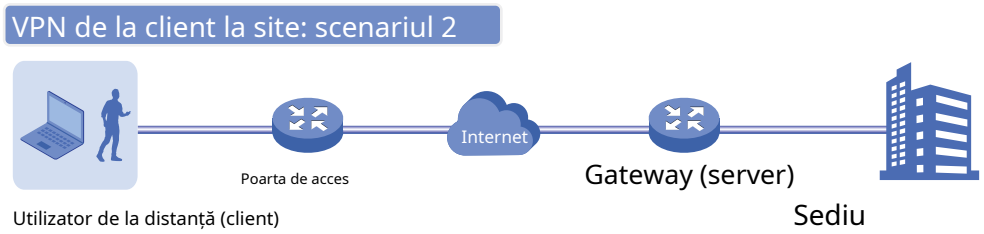
• Client VPN

Fie gateway-ul utilizatorului de la distanță, fie laptopul sau PC-ul utilizatorului de la distanță funcționează ca client VPN.

Când gateway-ul utilizatorului de la distanță funcționează ca client VPN, gateway-ul ajută la crearea tunelurilor VPN între gazdele sale conectate și serverul VPN. Gateway-ul care funcționează ca client VPN poate folosi L2TP, PPTP sau OpenVPN ca protocol de tunel.



Când laptopul sau computerul utilizatorului de la distanță funcționează ca client VPN, laptopul sau computerul utilizează un program software client VPN pentru a crea tuneluri VPN între el și serverul VPN. Programul software client VPN poate folosi L2TP, PPTP, IPsec sau OpenVPN ca protocol de tunel.

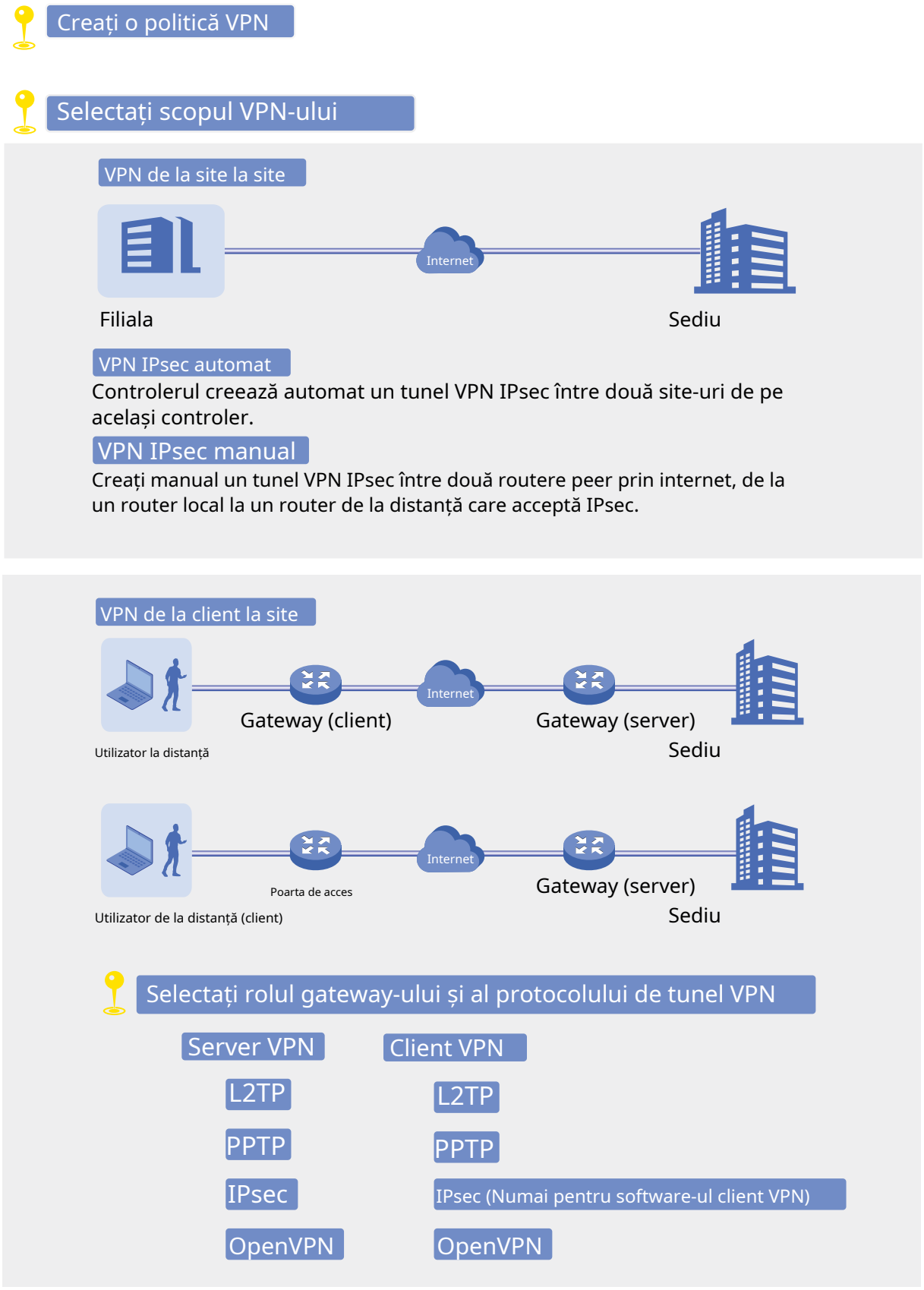


Notă:

În scenariul 1, trebuie să configurați separat clientul VPN și serverul VPN pe gateway-uri, în timp ce gazdele de la distanță pot accesa rețelele locale fără a rula software-ul client VPN.

În scenariul 2, trebuie să configurați serverul VPN pe gateway și apoi să configurați programul software client VPN pe laptopul sau PC-ul utilizatorului la distanță, în timp ce gateway-ul utilizatorului la distanță nu are nevoie de nicio configurație VPN.

Iată infograficul pentru a oferi o imagine de ansamblu rapidă a soluțiilor VPN.



Configurare

Pentru a finaliza configurarea VPN, urmați acești pași:

1)Creați o nouă politică VPN și selectați scopul VPN-ului în funcție de nevoile dvs. Selectați Site-to-Site dacă doriți ca rețeaua să fie conectată la alta. Selectați Client-la-Site dacă doriți ca unele gazde să fie conectate la rețea.

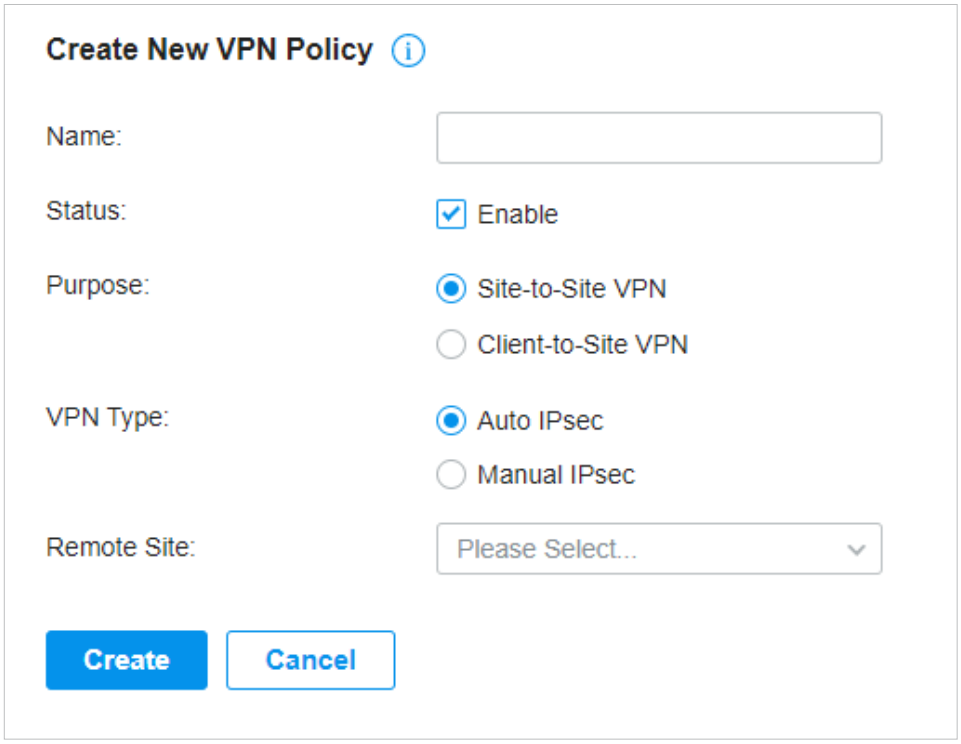
2)Selectați protocolul de tunel VPN și configurați politica VPN pe baza protocolului.

■ Configurarea VPN de la site la site

Gateway-ul gestionat Omada acceptă două tipuri de VPN-uri Site-to-Site:IPsec automat șiIPsec manual .

• Configurarea VPN Auto IPsec

1. Selectați un site din lista derulantă aOrganizare. Mergi laSetări>VPN. Faceți clic pentru a încărca următoarea pagină.



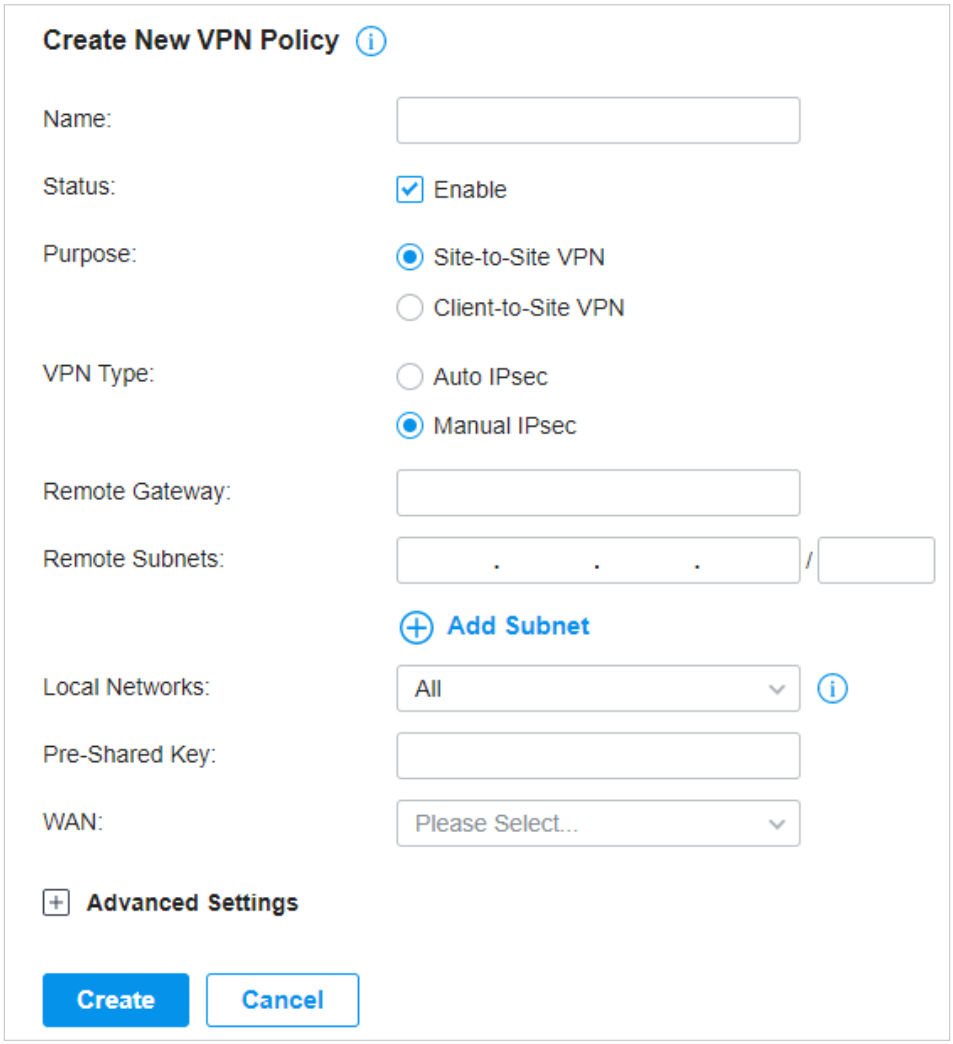
2. Introduceți un nume pentru a identifica politica VPN și selectați scopul ca Site-to-Site VPN. Consultați următorul tabel pentru a configura parametrii necesari și faceți clicCrea.

Nume	Introduceți un nume pentru a identifica politica VPN.
stare	Faceți clic pe caseta de selectare pentru a activa politica VPN.
Scop	Selectați scopul VPN-ului caVPN de la site la site.
Tip VPN	Selectați tipul VPN caIPsec automat. Cu Auto IPsec, controlerul creează automat un tunel VPN IPsec între două site-uri de pe același controler. Conexiunea VPN este bidirecțională. Adică, crearea unui VPN Auto IPsec de la site-ul A la site-ul B oferă, de asemenea, conectivitate de la site-ul B la site-ul A și nu este nevoie de nimic pentru a fi configurat pe site-ul B.

Site la distanță	Selectați site-ul de la celălalt capăt al tunelului Auto IPsec VPN. Asigurați-vă că site-ul la distanță selectat are un gateway online gestionat Omada în cadrul aceluiași controler.

• Configurarea manuală IPsec VPN

1. Selectați un site din lista derulantă aOrganizare. Mergi laSetări>VPN. Faceți clic pentru a încărca următoarea pagină.

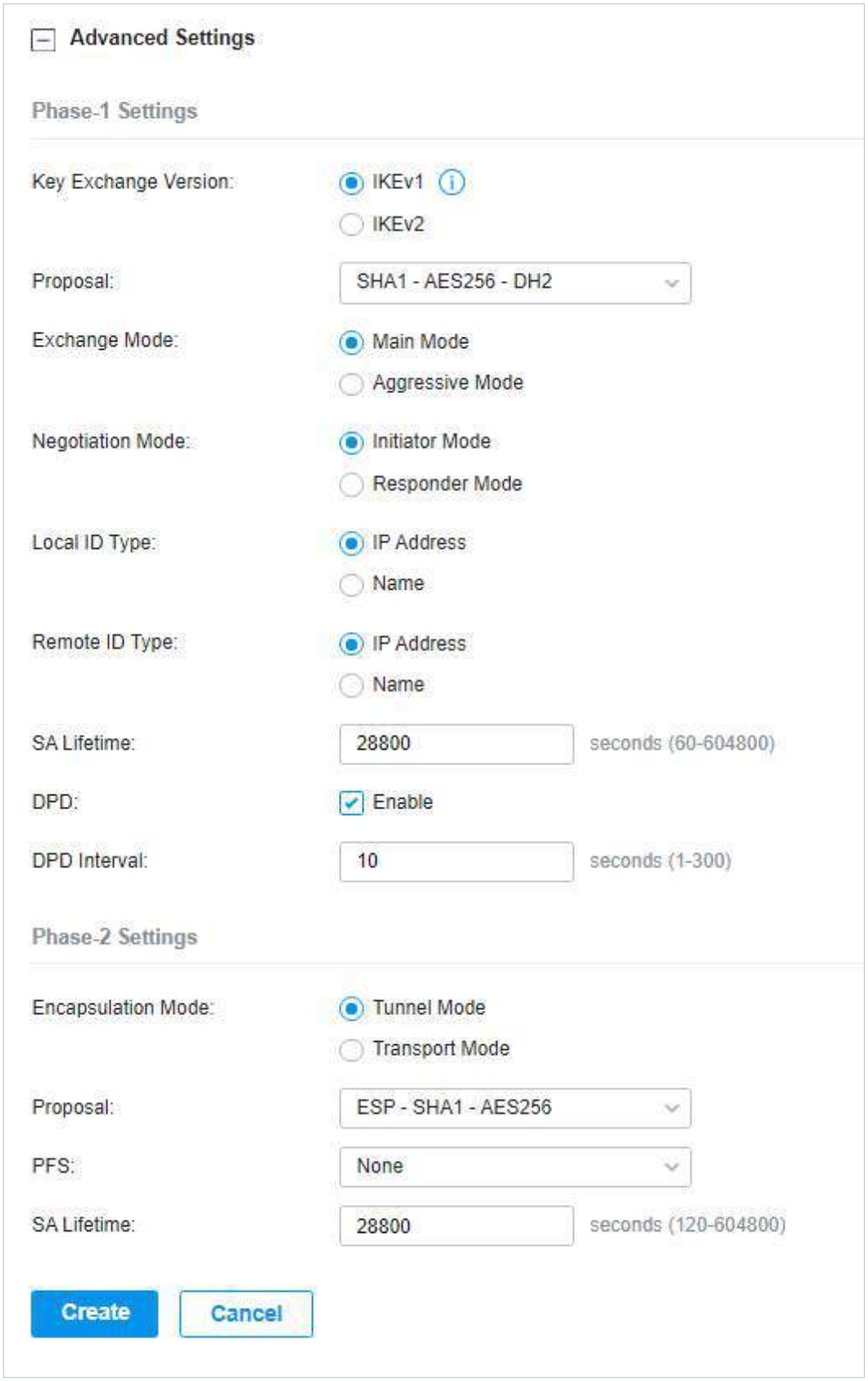


2. Introduceți un nume pentru a identifica politica VPN și selectați scopul ca Site-to-Site VPN. Consultați următorul tabel pentru a configura parametrii de bază și faceți clicCrea.

Nume	Introduceți un nume pentru a identifica politica VPN.
stare	Faceți clic pe caseta de selectare pentru a activa politica VPN.
Scop	Selectați scopul VPN-ului caVPN de la site la site.
Tip VPN	Selectați tipul VPN caIPsec manual.
Gateway la distanță	Introduceți o adresă IP sau un nume de domeniu ca gateway pe peer-ul de la distanță al tunelului VPN.

Subrețele de la distanță	Introduceți intervalul de adrese IP a rețelei LAN pe peer-ul de la distanță al tunelului VPN. Subrețelele de la distanță nu ar trebui să fie în același segment de rețea ca LAN local.
Rețele locale	Selectați rețelele din partea locală a tunelului VPN. Politica VPN va fi aplicată numai rețelelor locale selectate.
Cheie pre-partajată	Introduceți cheia pre-partajată (PSK). Ambele gateway-uri peer trebuie să utilizeze aceeași cheie secretă pre-partajată pentru autentificare. O cheie pre-partajată este un șir de caractere care este folosit ca cheie de autentificare. Ambele gateway-uri peer creează o valoare hash bazată pe aceeași cheie pre-partajată și pe alte informații. Valorile hash sunt apoi schimbate și verificate pentru a autentifica cealaltă parte. Cheile pre-partajate ar trebui să fie lungi și aleatorii pentru securitate. Cheile pre-partajate scurte sau previzibile pot fi sparte cu ușurință în atacurile cu forță brută. Pentru a menține un nivel ridicat de securitate, administratorilor li se recomandă să actualizeze periodic cheia pre-partajată.
WAN	Selectați portul WAN pe care este stabilit tunelul VPN IPsec.

3. Faceți clic pe Setări avansate pentru a încărca următoarea pagină.



Setările avansate includ setările de faza 1 și setările de faza 2. Faza-1 este folosită pentru a configura un canal criptat securizat pe care cei doi colegi să-l poată negocia Faza-2 și apoi să stabilească Asociațiile de Securitate IKE (IKE SA). Faza-2 este folosită pentru a negocia un set de parametri care

definiți ce trafic poate trece prin VPN și cum să criptați și să autentificați traficul, apoi stabiliți asociațiile de securitate IPsec (IPsec SA).

Consultați următorul tabel pentru a finaliza configurațiile în funcție de nevoile dvs. reale și faceți clic Crea.

Pentru setările fazei 1:

Setări Faza-1	Versiunea IKE pe care o selectați determină setările disponibile de Faza 1 și definește procesul de negociere. Ambele gateway-uri VPN trebuie configurate pentru a utiliza aceeași versiune IKE și setări de fază 1.
Schimb de chei pe internet Versiune	Selectați versiunea protocolului Internet Key Exchange (IKE) care este utilizată pentru a configura asocieri de securitate pentru IPsec. Atât IKEv1, cât și IKEv2 sunt acceptate cu gateway-uri gestionate Omada, dar IKEv1 este disponibil numai atunci când politica VPN este aplicată unei singure subrețea la distanță și unei singure rețele locale. Rețineți că ambele gateway-uri peer trebuie configurate pentru a utiliza aceeași versiune IKE.
Propunere	Specificați propunerea pentru etapa 1 de negociere IKE. O propunere IKE listează algoritmul de criptare, algoritmul de autentificare și grupurile Diffie-Hellman (DH) care urmează să fie negociate cu peer-ul IPsec la distanță. Algoritmii de autentificare verifică integritatea datelor și autenticitatea unui mesaj. Algoritmii de criptare protejează datele de a fi citite de o terță parte. Grupurile Diffie-Hellman (DH) determină puterea cheii utilizate în procesul de schimb de chei. Rețineți că ambele gateway-uri peer trebuie configurate pentru a utiliza aceeași propunere.
Modul de schimb	Specificați modul de schimb IKE când este selectat IKEv1. Modul principal:Acest mod oferă protecție identității și schimbă mai multe informații, ceea ce se aplică scenariilor cu cerințe mai mari pentru protecția identității. Modul agresiv:Acest mod stabilește o conexiune mai rapidă, dar cu o securitate mai mică, ceea ce se aplică scenariilor cu cerințe mai scăzute pentru protecția identității.
Modul de negociere	Specificați modul de negociere IKE ca mod inițiator sau mod răspuns. Modul inițiator:Acest mod înseamnă că dispozitivul local inițiază o conexiune cu peer-ul. Modul de răspuns:Acest mod înseamnă că dispozitivul local așteaptă cererea de conectare inițiată de peer.
Tipul ID local	Specificați tipul de ID local care indică identificatorul de autentificare trimis peer-ului pentru negocierea IKE. Adresa IP:Selectați Adresă IP pentru a utiliza adresa IP pentru autentificare. Nume:Selectați Nume, apoi introduceți numele în câmpul Local ID pentru a utiliza numele ca ID pentru autentificare. Rețineți că tipul și valoarea ID local ar trebui să fie aceleași cu ID-ul la distanță dat pentru peer-ul la distanță al tunelului VPN.

ID local	Când Tipul ID local este configurat ca Nume, introduceți un nume pentru dispozitivul local ca ID în negocierea IKE. Numele ar trebui să fie în formatul FQDN (Nume de domeniu complet calificat).
Tip ID de la distanță	Specificați tipul de ID la distanță care indică identificatorul de autentificare primit de la peer pentru negocierea IKE. Adresa IP:Selectați Adresă IP pentru a utiliza adresa IP pentru autentificare. Nume:Selectați Nume, apoi introduceți numele în câmpul Remote ID pentru a utiliza numele ca ID pentru autentificare. Rețineți că tipul și valoarea ID-ului la distanță ar trebui să fie aceleași cu ID-ul local dat pentru peer-ul de la distanță al tunelului VPN.
ID de la distanță	Când Remote ID Type este configurat ca Nume, introduceți un nume al peer-ului la distanță ca ID în negocierea IKE. Numele ar trebui să fie în formatul FQDN (Nume de domeniu complet calificat).
SA Viață	Specificați ISAKMP SA (Asociația de securitate) Durata de viață în negocierea IKE. Dacă durata de viață a SA a expirat, ISAKMP SA aferent va fi șters.
DPD	Bifați caseta pentru a activa funcția DPD (Dead Peer Detect). Dacă este activat, punctul final IKE poate trimite o solicitare DPD către peer pentru a inspecta dacă peer-ul IKE este în viață.
Intervalul DPD	Specificați intervalul dintre trimiterea cererilor DPD cu DPD activat. Dacă punctul final IKE primește un răspuns de la egal în timpul acestui interval, îl consideră peer-ul în viață. Dacă punctul final IKE nu primește un răspuns în timpul intervalului, el consideră peer-ul mort și șterge SA.

Pentru setările fazei 2:

Setări Faza-2	Scopul negocierilor din Faza 2 este de a stabili SA Faza 2 (numită și SA IPsec). IPsec SA este un set de specificații de trafic care îi spun dispozitivului ce trafic să trimită prin VPN și cum să cripteze și să autentifice acel trafic.
Modul de încapsulare	Specificați modul de încapsulare ca mod tunel sau mod de transport. Când ambele capete ale tunelului sunt gazde, se poate alege oricare dintre modurile. Când cel puțin unul dintre punctele terminale ale unui tunel este o poartă de securitate, cum ar fi un router sau un firewall, se recomandă modul Tunnel pentru a asigura siguranța.
Propunere	Specificați propunerea pentru faza 2 de negociere IKE. O propunere IPsec listează algoritmul de criptare, algoritmul de autentificare și protocolul care urmează să fie negociat cu peer-ul IPsec la distanță. Rețineți că ambele gateway-uri peer trebuie configurate pentru a utiliza aceeași propunere.
PFS	Selectați grupul DH pentru a activa PFS (Perfect Forward Security) pentru modul IKE, apoi cheia generată în faza 2 va fi irelevantă cu cheia în faza 1, ceea ce sporește securitatea rețelei. Cu Niciunul selectat, înseamnă că PFS este dezactivat și cheia din faza 2 va fi generată pe baza cheii din faza 1.
SA Viață	Specificați IPsec SA (Asociația de securitate) Durata de viață în negocierea IKE. Dacă durata de viață a SA a expirat, IPsec SA aferent va fi șters.

Configurarea VPN de la client la site

Gateway-ul gestionat Omada acceptă șapte tipuri de VPN-uri client-la-site, în funcție de rolul gateway-ului gestionat Omada și de protocolul pe care l-ați folosit:

Configurarea gateway-ului ca server VPN folosind L2TP

Configurarea gateway-ului ca server VPN folosind PPTP

Configurarea gateway-ului ca server VPN utilizând IPsec

Configurarea gateway-ului ca server VPN folosind OpenVPN

Configurarea gateway-ului ca client VPN folosind L2TP

Configurarea gateway-ului ca client VPN folosind PPTP

Configurarea gateway-ului ca client VPN folosind OpenVPN

• Configurarea gateway-ului ca server VPN folosind L2TP

1. Selectați un site din lista derulantă aOrganizare. Mergi laSetări>VPN. Faceți clic pentru a încărca următoarea pagină.

2. Introduceți un nume pentru a identifica politica VPN și selectați scopul drept VPN Client-Site. Consultați următorul tabel pentru a configura parametrii necesari și faceți clicCrea.

Nume	Introduceți un nume pentru a identifica politica VPN.
stare	Faceți clic pe caseta de selectare pentru a activa politica VPN.
Scop	Selectați scopul VPN-ului caVPN de la client la site.
Tip VPN	Selectați tipul VPN caServer VPN - L2TP.

Criptare IPsec	Specificați dacă activați criptarea pentru tunel. Criptat:Selectați Criptat pentru a cripta tunelul L2TP prin IPsec (L2TP peste IPsec). Cu Criptat selectat, introduceți cheia pre-partajată pentru autentificarea IKE. Serverul VPN și clientul VPN trebuie să utilizeze aceeași cheie secretă pre-partajată pentru autentificare. Necriptat:Cu Necriptat selectat, tunelul L2TP nu va fi criptat de IPsec. Auto:Cu Auto selectat, serverul L2TP va determina dacă să cripteze tunelul conform setărilor de criptare ale clientului. Și introduceți cheia pre-partajată pentru autentificarea IKE. Serverul VPN și clientul VPN trebuie să utilizeze aceeași cheie secretă pre-partajată pentru autentificare.
Rețele locale	Selectați rețelele din partea locală a tunelului VPN. Politica VPN va fi aplicată numai rețelelor locale selectate.
Cheie pre-partajată	Introduceți cheia secretă pre-partajată când Criptarea IPsec este selectată ca Criptat și Auto. Ambele routere peer trebuie să folosească aceeași cheie secretă pre-partajată pentru autentificare.
WAN	Selectați portul WAN pe care este stabilit tunelul VPN L2TP. Fiecare port WAN acceptă un singur tunel VPN L2TP atunci când gateway-ul funcționează ca server L2TP.
Pool IP	Introduceți adresa IP și masca de subrețea pentru a decide intervalul pool-ului de IP VPN. Serverul VPN va atribui o adresă IP gazdei de la distanță atunci când tunelul este stabilit. Puteți specifica orice adresă IP rezonabilă care nu va cauza suprapunerea cu adresa IP a rețelei LAN de pe routerul local de egalitate.

3. Adăugați contul de utilizatori VPN pentru a valida gazdele de la distanță. Pentru a crea utilizatori VPN, consultați3. 7. 2 Utilizator VPN .

• Configurarea gateway-ului ca server VPN utilizând PPTP

1. Selectați un site din lista derulantă aOrganizare. Mergi laSetări>VPN. Faceți clic pentru a încărca următoarea pagină.

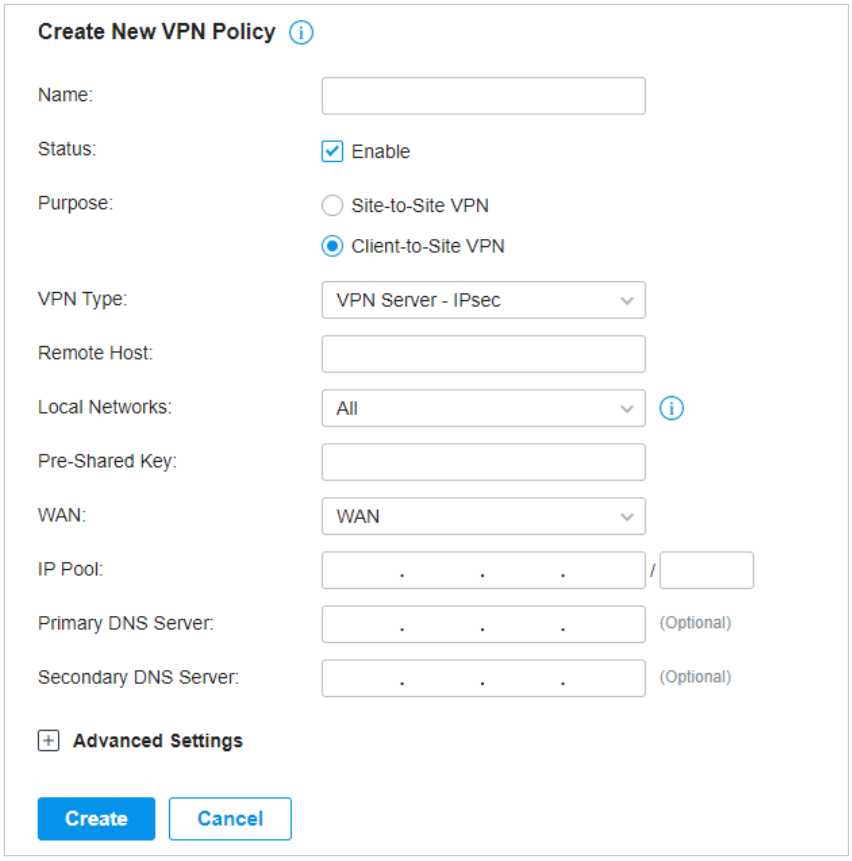
2. Introduceți un nume pentru a identifica politica VPN și selectați scopul drept VPN Client-Site. Consultați următorul tabel pentru a configura parametrii necesari și faceți clicCrea.

Nume	Introduceți un nume pentru a identifica politica VPN.
stare	Faceți clic pe caseta de selectare pentru a activa politica VPN.
Scop	Selectați scopul VPN-ului caVPN de la client la site.
Tip VPN	Selectați tipul VPN caServer VPN - PPTP.
Criptare MPPE	Specificați dacă activați MPPE (Microsoft Point-to-Point Encryption) pentru tunel. Criptat:Cu Criptat selectat, tunelul PPTP va fi criptat de MPPE. Necriptat:Cu Necriptat selectat, tunelul PPTP nu va fi criptat de MPPE.
Rețele locale	Selectați rețelele din partea locală a tunelului VPN. Politica VPN va fi aplicată numai rețelelor locale selectate.
WAN	Selectați portul WAN pe care este stabilit tunelul VPN PPTP. Fiecare port WAN acceptă un singur tunel VPN PPTP atunci când gateway-ul funcționează ca server PPTP.
Pool IP	Introduceți adresa IP și masca de subrețea pentru a decide intervalul pool-ului de IP VPN. Serverul VPN va atribui o adresă IP gazdei de la distanță atunci când tunelul este stabilit. Puteți specifica orice adresă IP rezonabilă care nu va cauza suprapunerea cu adresa IP a rețelei LAN de pe routerul local de egalitate.

3. Adăugați contul de utilizatori VPN pentru a valida gazdele de la distanță. Pentru a crea utilizatori VPN, consultați3. 7. 2 Utilizator VPN .

• Configurarea gateway-ului ca server VPN utilizând IPsec

1. Selectați un site din lista derulantă aOrganizare. Mergi laSetări>VPN. Faceți clic pentru a încărca următoarea pagină.

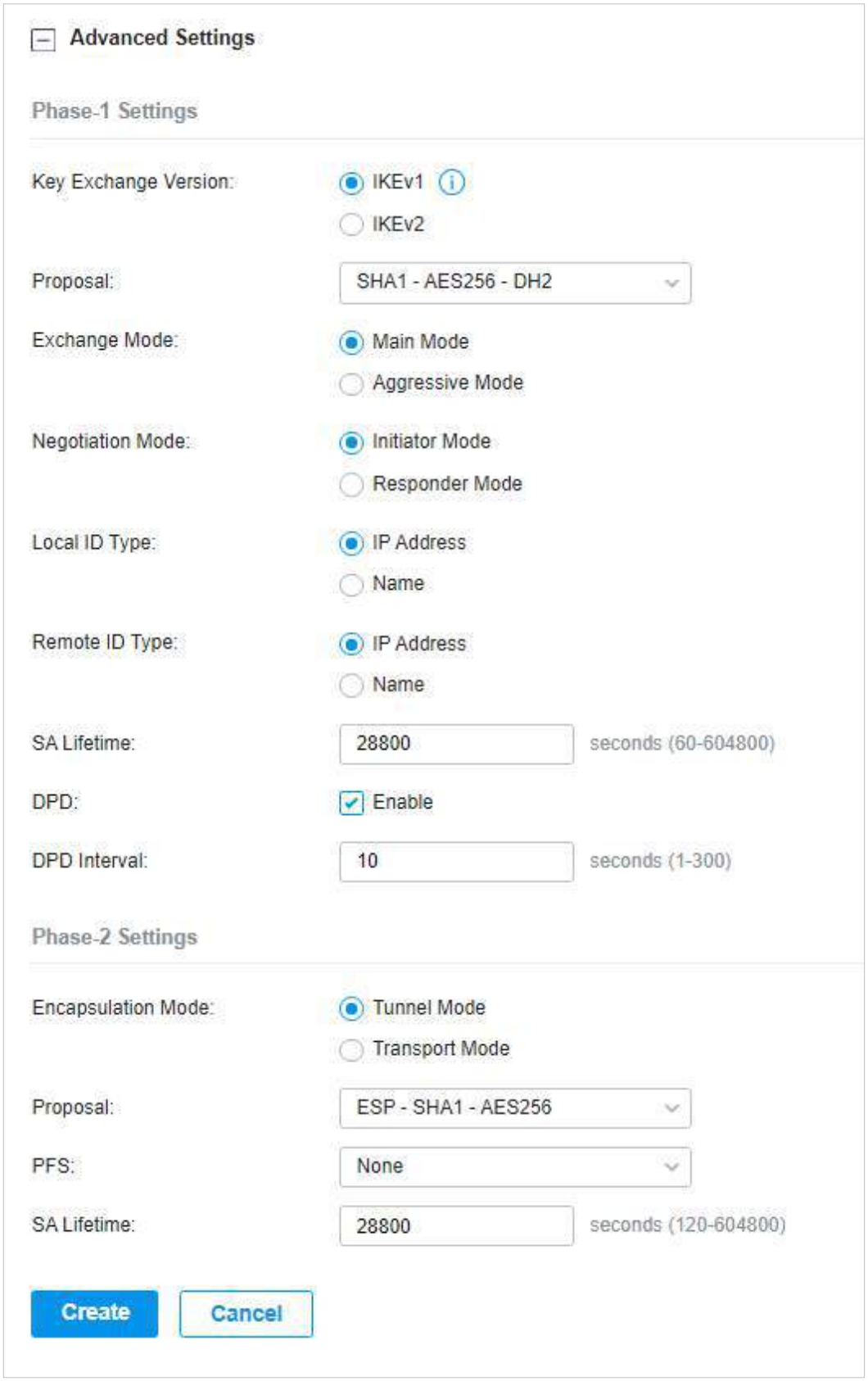


2. Introduceți un nume pentru a identifica politica VPN și selectați scopul drept VPN Client-Site. Consultați următorul tabel pentru a configura parametrii de bază și faceți clicCrea.

Nume	Introduceți un nume pentru a identifica politica VPN.
stare	Faceți clic pe caseta de selectare pentru a activa politica VPN.
Scop	Selectați scopul VPN-ului caVPN de la client la site.
Tip VPN	Selectați tipul VPN caServer VPN - IPsec.
Gazda la distanta	Introduceți o adresă IP sau un nume de domeniu al gazdei pe peer-ul de la distanță al tunelului VPN. 0.0.0.0 reprezintă orice adresă IP.
Rețele locale	Selectați rețelele din partea locală a tunelului VPN. Politica VPN va fi aplicată numai rețelelor locale selectate.

Cheie pre-partajată	Introduceți cheia pre-partajată (PSK). Ambele gateway-uri peer trebuie să utilizeze aceeași cheie secretă pre-partajată pentru autentificare. O cheie pre-partajată este un șir de caractere care este folosit ca cheie de autentificare. Ambii parteneri VPN creează o valoare hash bazată pe aceeași cheie pre-partajată și pe alte informații. Valorile hash sunt apoi schimbate și verificate pentru a autentifica cealaltă parte. Cheile pre-partajate ar trebui să fie lungi și aleatorii pentru securitate. Cheile pre-partajate scurte sau previzibile pot fi sparte cu ușurință în atacurile cu forță brută. Pentru a menține un nivel ridicat de securitate, administratorilor li se recomandă să actualizeze periodic cheia pre-partajată.
WAN	Selectați portul WAN pe care este stabilit tunelul VPN IPsec.
Pool IP	Introduceți adresa IP și masca de subrețea pentru a decide intervalul pool-ului de IP VPN. Serverul VPN va atribui o adresă IP gazdei de la distanță atunci când tunelul este stabilit. Puteți specifica orice adresă IP rezonabilă care nu va cauza suprapunerea cu adresa IP a rețelei LAN de pe routerul local de egalitate.
Server DNS primar	(Opțional) Introduceți adresa IP a serverului DNS principal furnizat de ISP.
Server DNS secundar	(Opțional) Introduceți adresa IP a serverului DNS secundar, care oferă redundanță în cazul în care serverul DNS primar se defectează.

3. Faceți clic pe Setări avansate pentru a încărca următoarea pagină.



Setările avansate includ setările de faza 1 și setările de faza 2. Faza-1 este folosită pentru a configura un canal criptat securizat pe care cei doi colegi să-l poată negocia Faza-2 și apoi să stabilească Asociațiile de Securitate IKE (IKE SA). Faza 2este folosit pentru a negocia despreun set de parametri care

definiți ce trafic poate trece prin VPN și cum să criptați și să autentificați traficul, apoi stabiliți asociațiile de securitate IPsec (IPsec SA).

Consultați următorul tabel pentru a finaliza configurațiile în funcție de nevoile dvs. reale și faceți clic Crea.

Pentru setările fazei 1:

Setări Faza-1	Versiunea IKE pe care o selectați determină setările disponibile de Faza 1 și definește procesul de negociere. Ambele gateway-uri VPN trebuie configurate pentru a utiliza aceeași versiune IKE și setări de fază 1.
Schimb de chei pe internet Versiune	Selectați versiunea protocolului Internet Key Exchange (IKE) care este utilizată pentru a configura asocieri de securitate pentru IPsec. Atât IKEv1, cât și IKEv2 sunt acceptate cu gateway-uri gestionate Omada, dar IKEv1 este disponibil numai atunci când politica VPN este aplicată unei singure subrețea la distanță și unei singure rețele locale. Rețineți că ambii parteneri VPN trebuie configurați pentru a utiliza aceeași versiune IKE.
Propunere	Specificați propunerea pentru etapa 1 de negociere IKE. O propunere IKE listează algoritmul de criptare, algoritmul de autentificare și grupurile Diffie-Hellman (DH) care urmează să fie negociate cu peer-ul IPsec la distanță. Algoritmii de autentificare verifică integritatea datelor și autenticitatea unui mesaj. Algoritmii de criptare protejează datele de a fi citite de o terță parte. Grupurile Diffie-Hellman (DH) determină puterea cheii utilizate în procesul de schimb de chei. Rețineți că ambii parteneri VPN trebuie configurați pentru a utiliza aceeași propunere.
Modul de schimb	Specificați modul de schimb IKE când este selectat IKEv1. Modul principal:Acest mod oferă protecție identității și schimbă mai multe informații, ceea ce se aplică scenariilor cu cerințe mai mari pentru protecția identității. Modul agresiv:Acest mod stabilește o conexiune mai rapidă, dar cu o securitate mai mică, ceea ce se aplică scenariilor cu cerințe mai scăzute pentru protecția identității.
Modul de negociere	Specificați modul de negociere IKE ca mod inițiator sau mod răspuns. Modul inițiator:Acest mod înseamnă că dispozitivul local inițiază o conexiune cu peer-ul. Modul de răspuns:Acest mod înseamnă că dispozitivul local așteaptă cererea de conectare inițiată de peer.
Tipul ID local	Specificați tipul de ID local care indică identificatorul de autentificare trimis peer-ului pentru negocierea IKE. Adresa IP:Selectați Adresă IP pentru a utiliza adresa IP pentru autentificare. Nume:Selectați Nume, apoi introduceți numele în câmpul Local ID pentru a utiliza numele ca ID pentru autentificare. Rețineți că tipul și valoarea ID local ar trebui să fie aceleași cu ID-ul la distanță dat pentru peer-ul la distanță al tunelului VPN.

ID local	Când Tipul ID local este configurat ca Nume, introduceți un nume pentru dispozitivul local ca ID în negocierea IKE. Numele ar trebui să fie în formatul FQDN (Nume de domeniu complet calificat).
Tip ID de la distanță	Specificați tipul de ID la distanță care indică identificatorul de autentificare primit de la peer pentru negocierea IKE. Adresa IP:Selectați Adresă IP pentru a utiliza adresa IP pentru autentificare. Nume:Selectați Nume, apoi introduceți numele în câmpul Remote ID pentru a utiliza numele ca ID pentru autentificare. Rețineți că tipul și valoarea ID-ului la distanță ar trebui să fie aceleași cu ID-ul local dat pentru peer-ul de la distanță al tunelului VPN.
ID de la distanță	Când Remote ID Type este configurat ca Nume, introduceți un nume al peer-ului la distanță ca ID în negocierea IKE. Numele ar trebui să fie în formatul FQDN (Nume de domeniu complet calificat).
SA Viață	Specificați ISAKMP SA (Asociația de securitate) Durata de viață în negocierea IKE. Dacă durata de viață a SA a expirat, ISAKMP SA aferent va fi șters.
DPD	Bifați caseta pentru a activa funcția DPD (Dead Peer Detect). Dacă este activat, punctul final IKE poate trimite o solicitare DPD către peer pentru a inspecta dacă peer-ul IKE este în viață.
Intervalul DPD	Specificați intervalul dintre trimiterea cererilor DPD cu DPD activat. Dacă punctul final IKE primește un răspuns de la egal în timpul acestui interval, îl consideră peer-ul în viață. Dacă punctul final IKE nu primește un răspuns în timpul intervalului, el consideră peer-ul mort și șterge SA.

Pentru setările fazei 2:

Setări Faza-2	Scopul negocierilor din Faza 2 este de a stabili SA Faza 2 (numită și SA IPsec). IPsec SA este un set de specificații de trafic care îi spun dispozitivului ce trafic să trimită prin VPN și cum să cripteze și să autentifice acel trafic.
Modul de încapsulare	Specificați modul de încapsulare ca mod tunel sau mod de transport. Când ambele capete ale tunelului sunt gazde, se poate alege oricare dintre modurile. Când cel puțin unul dintre punctele terminale ale unui tunel este o poartă de securitate, cum ar fi un router sau un firewall, se recomandă modul Tunnel pentru a asigura siguranța.
Propunere	Specificați propunerea pentru faza 2 de negociere IKE. O propunere IPsec listează algoritmul de criptare, algoritmul de autentificare și protocolul care urmează să fie negociat cu peer-ul IPsec la distanță. Rețineți că ambele gateway-uri peer trebuie configurate pentru a utiliza aceeași propunere.
PFS	Selectați grupul DH pentru a activa PFS (Perfect Forward Security) pentru modul IKE, apoi cheia generată în faza 2 va fi irelevantă cu cheia în faza 1, ceea ce sporește securitatea rețelei. Cu Niciunul selectat, înseamnă că PFS este dezactivat și cheia din faza 2 va fi generată pe baza cheii din faza 1.
SA Viață	Specificați IPsec SA (Asociația de securitate) Durata de viață în negocierea IKE. Dacă durata de viață a SA a expirat, IPsec SA aferent va fi șters.

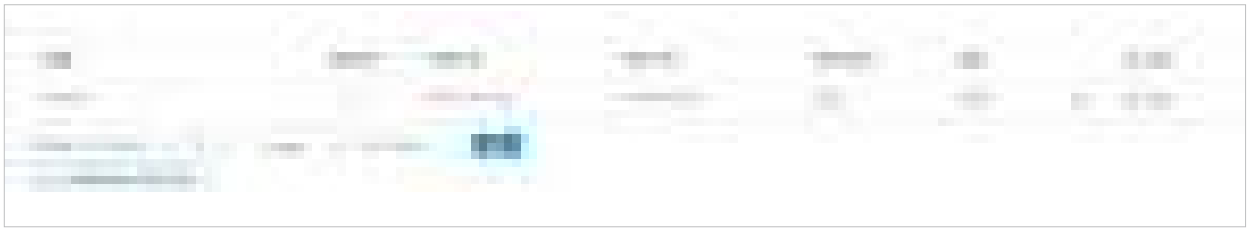
• Configurarea gateway-ului ca server VPN utilizând OpenVPN

1. Selectați un site din lista derulantă aOrganizare. Mergi laSetări>VPN. Faceți clic pentru a încărca următoarea pagină.

2. Introduceți un nume pentru a identifica politica VPN și selectați scopul drept VPN Client-Site. Consultați următorul tabel pentru a configura parametrii necesari și faceți clicCrea.

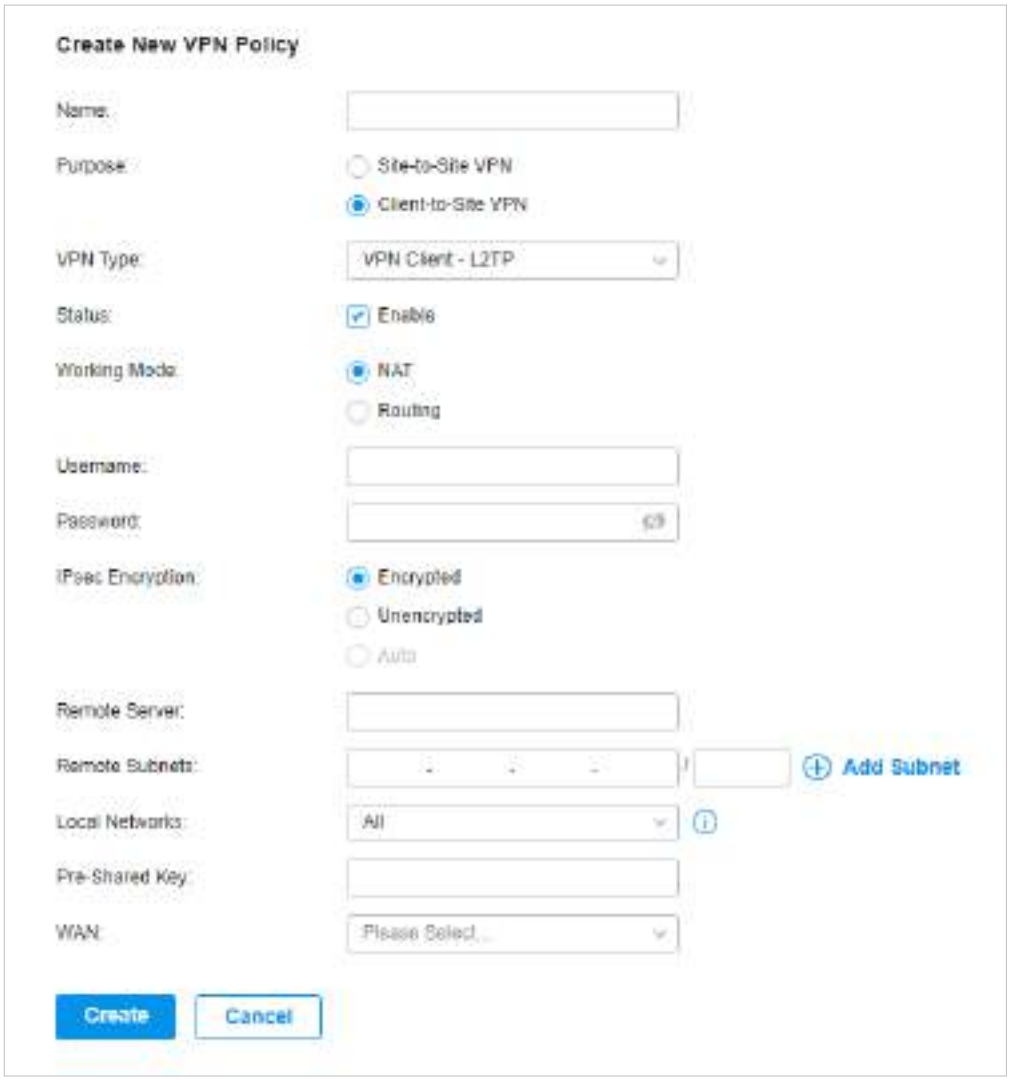
Nume	Introduceți un nume pentru a identifica politica VPN.
stare	Faceți clic pe caseta de selectare pentru a activa politica VPN.
Scop	Selectați scopul VPN-ului caVPN de la client la site.
Tip VPN	Selectați tipul VPN caServer VPN - OpenVPN.
Protocol	Selectați protocolul de comunicare pentru gateway-ul care funcționează ca server OpenVPN. Sunt disponibile două protocoale de comunicare: TCP și UDP.
Port de service	Introduceți un port de serviciu VPN la care se conectează un dispozitiv VPN.
Rețele locale	Selectați rețelele din partea locală a tunelului VPN. Politica VPN va fi aplicată numai rețelelor locale selectate.
WAN	Selectați portul WAN pe care este stabilit tunelul VPN. Fiecare port WAN acceptă un singur tunel OpenVPN atunci când gateway-ul funcționează ca server OpenVPN.
Pool IP	Introduceți adresa IP și masca de subrețea pentru a decide intervalul pool-ului de IP VPN. Serverul VPN va atribui o adresă IP gazdei de la distanță atunci când tunelul este stabilit. Puteți specifica orice adresă IP rezonabilă care nu va cauza suprapunerea cu adresa IP a rețelei LAN de pe routerul local de egalitate.

3. După ce faceți clicCreapentru a salva politica VPN, accesați Lista de politici VPN și faceți clic în Acțiune coloana pentru a exporta fișierul OpenVPN care se termină în .ovpn, care urmează să fie utilizat de clientul de la distanță. Fișierul OpenVPN exportat conține certificatul și informațiile de configurare.



• Configurarea gateway-ului ca client VPN folosind L2TP

1. Selectați un site din lista derulantă aOrganizare. Mergi laSetări>VPN. Faceți clic pentru a încărca următoarea pagină.



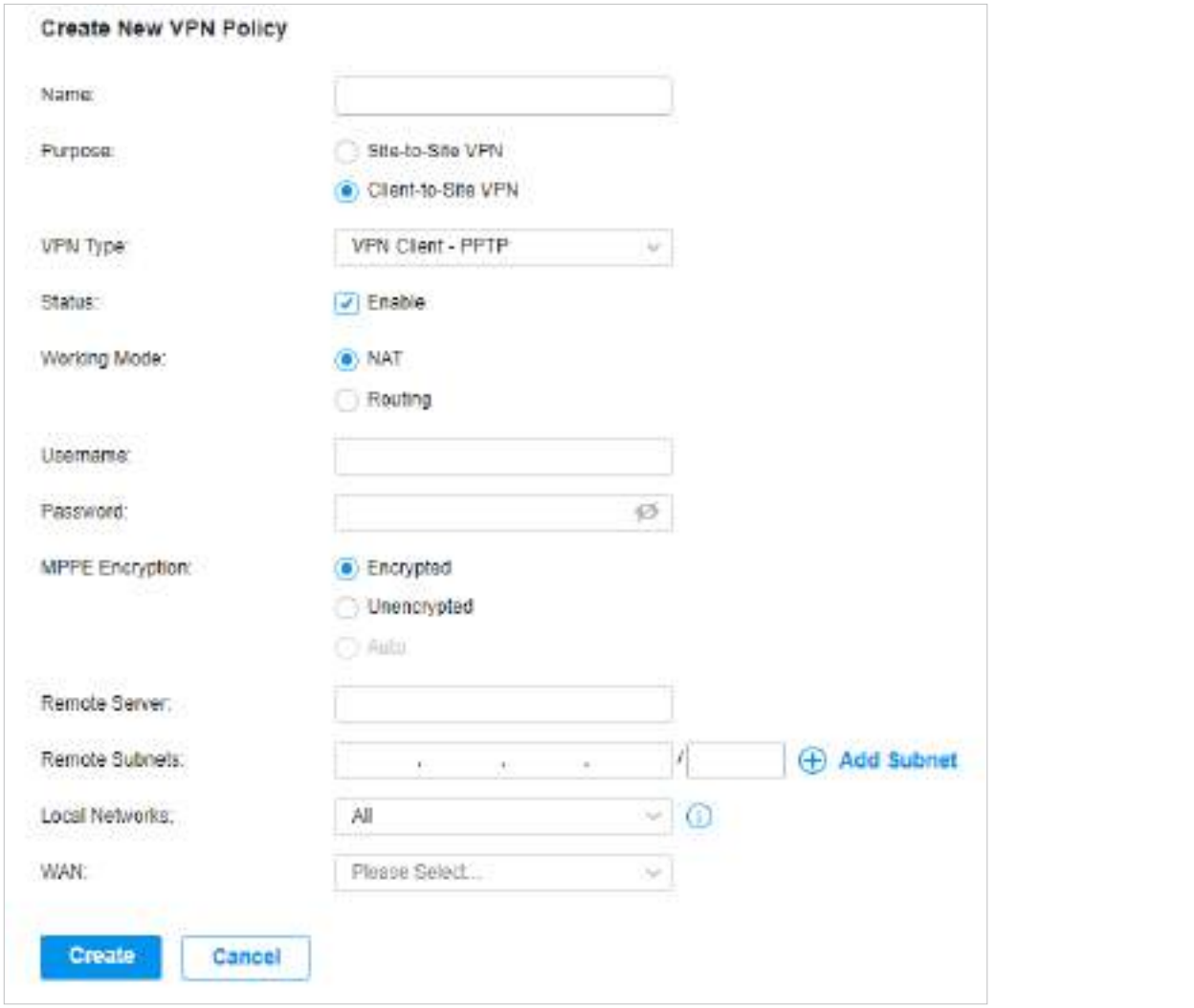
2. Introduceți un nume pentru a identifica politica VPN și selectați scopul drept VPN Client-Site. Consultați următorul tabel pentru a configura parametrii necesari și faceți clicCrea.

Nume	Introduceți un nume pentru a identifica politica VPN.
stare	Faceți clic pe caseta de selectare pentru a activa politica VPN.

Scop	Selectați scopul VPN-ului caVPN de la client la site.
Tip VPN	Selectați tipul VPN caClient VPN - L2TP.
Mod de lucru	Specificați modul de lucru ca NAT sau rutare. NAT:Cu modul NAT (Network Address Translation) selectat, clientul L2TP utilizează adresa IP atribuită ca adrese sursă ale antetului IP original atunci când redirecționează pachetele L2TP. rutare:Cu rutarea selectată, clientul L2TP utilizează propria sa adresă IP ca adrese sursă ale antetului IP original atunci când redirecționează pachetele L2TP.
Nume de utilizator	Introduceți numele de utilizator folosit pentru tunelul VPN. Acest nume de utilizator ar trebui să fie același cu cel al serverului L2TP.
Parola	Introduceți parola utilizatorului. Această parolă ar trebui să fie aceeași cu cea a serverului L2TP.
Criptare IPsec	Specificați dacă activați criptarea pentru tunel. Criptat:Selectați Criptat pentru a cripta tunelul L2TP prin IPsec (L2TP peste IPsec). Cu Criptat selectat, introduceți cheia pre-partajată pentru autentificarea IKE. Serverul VPN și clientul VPN trebuie să utilizeze aceeași cheie secretă pre-partajată pentru autentificare. Necriptat:Cu Necriptat selectat, tunelul L2TP nu va fi criptat de IPsec.
Server la distanta	Introduceți adresa IP sau numele de domeniu al serverului L2TP.
Subrețele de la distanță	Introduceți adresa IP și masca de subrețea pentru a specifica rețeaua de la distanță. Este întotdeauna domeniul de adrese IP a rețelei LAN de peer-ul de la distanță al tunelului VPN.
Rețele locale	Selectați rețelele din partea locală a tunelului VPN. Politica VPN va fi aplicată numai rețelelor locale selectate.
Cheie pre-partajată	Introduceți cheia secretă pre-partajată când tunelul L2TP este criptat de IPsec. Ambele gateway-uri peer trebuie să utilizeze aceeași cheie secretă pre-partajată pentru autentificare.
WAN	Selectați portul WAN pe care este stabilit tunelul VPN.

• Configurarea gateway-ului ca client VPN utilizând PPTP

1. Selectați un site din lista derulantă aOrganizare. Mergi laSetări>VPN. Faceți clic pentru a încărca următoarea pagină.



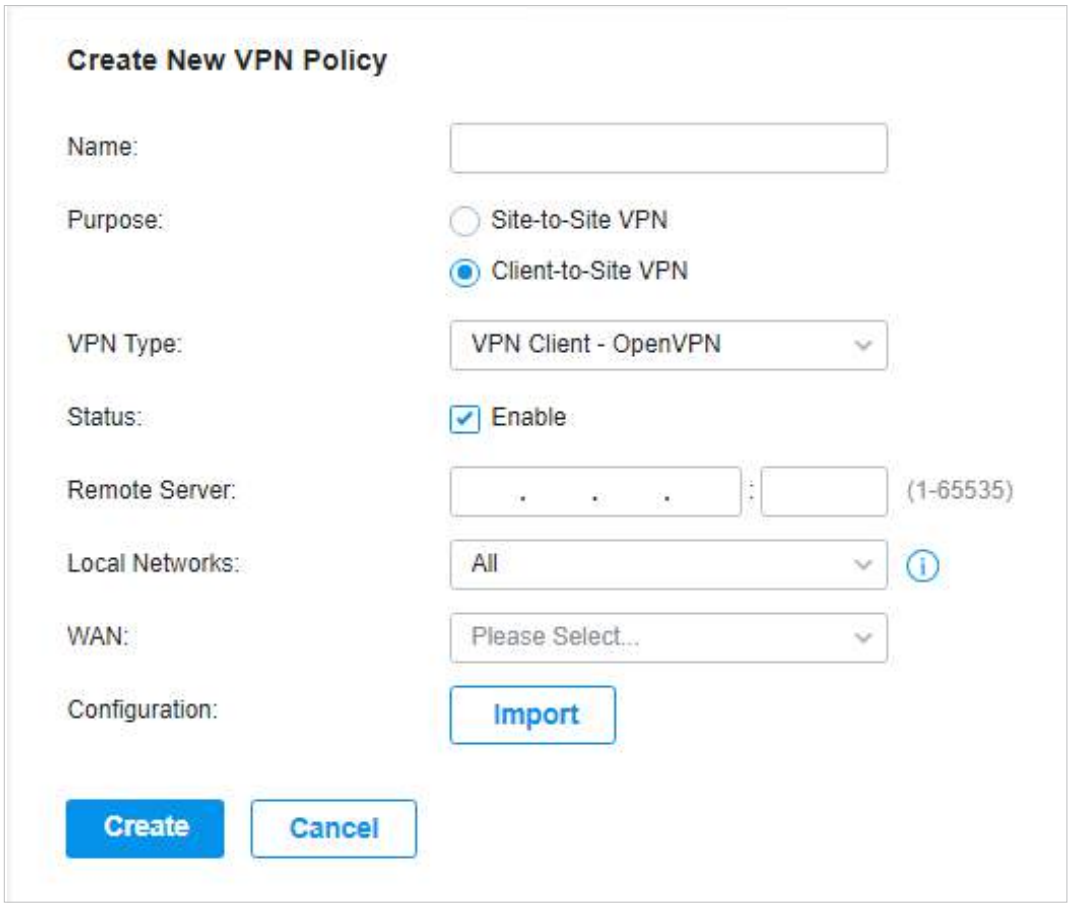
2. Introduceți un nume pentru a identifica politica VPN și selectați scopul drept VPN Client-Site. Consultați următorul tabel pentru a configura parametrii necesari și faceți clicCrea.

Nume	Introduceți un nume pentru a identifica politica VPN.
stare	Faceți clic pe caseta de selectare pentru a activa politica VPN.
Scop	Selectați scopul VPN-ului caVPN de la client la site.
Tip VPN	Selectați tipul VPN caClient VPN - PPTP.
Mod de lucru	Specificați modul de lucru ca NAT sau rutare. NAT:Cu modul NAT (Network Address Translation) selectat, clientul PPTP utilizează adresa IP atribuită ca adrese sursă ale antetului IP original atunci când redirecționează pachetele PPTP. rutare:Cu rutarea selectată, clientul PPTP utilizează propria sa adresă IP ca adrese sursă ale antetului IP original atunci când redirecționează pachetele PPTP.

Nume de utilizator	Introduceți numele de utilizator folosit pentru tunelul VPN. Acest nume de utilizator ar trebui să fie același cu cel al serverului PPTP.
Parola	Introduceți parola utilizatorului. Această parolă ar trebui să fie aceeași cu cea a serverului PPTP.
Criptare MPPE	Specificați dacă activați criptarea pentru tunel. Criptat:Selectați Criptat pentru a cripta tunelul PPTP prin MPPE. Necriptat:Cu Necriptat selectat, tunelul PPTP nu va fi criptat de MPPE.
Server la distanta	Introduceți adresa IP sau numele de domeniu al serverului PPTP.
Subrețele de la distanță	Introduceți adresa IP și masca de subrețea pentru a specifica rețeaua de la distanță. Este întotdeauna domeniul de adrese IP a rețelei LAN de peer-ul de la distanță al tunelului VPN.
Rețele locale	Selectați rețelele din partea locală a tunelului VPN. Politica VPN va fi aplicată numai rețelelor locale selectate.
WAN	Selectați portul WAN pe care este stabilit tunelul VPN.

• Configurarea gateway-ului ca client VPN folosind OpenVPN

1. Selectați un site din lista derulantă aOrganizare. Mergi laSetări>VPN. Faceți clic pentru a încărca următoarea pagină.



2. Introduceți un nume pentru a identifica politica VPN și selectați scopul drept VPN Client-Site. Consultați următorul tabel pentru a configura parametrii necesari și faceți clicCrea.

Nume	Introduceți un nume pentru a identifica politica VPN.
stare	Faceți clic pe caseta de selectare pentru a activa politica VPN.
Scop	Selectați scopul VPN-ului caVPN de la client la site.
Tip VPN	Selectați tipul VPN caClient VPN - OpenVPN.
Server la distanta	Introdu adresa IP sau numele de domeniu al serverului OpenVPN.
Rețele locale	Selectați rețelele din partea locală a tunelului VPN. Politica VPN va fi aplicată numai rețelelor locale selectate.
WAN	Selectați portul WAN pe care este stabilit tunelul VPN.
Configurare	Clic Import pentru a importa fișierul OpenVPN care se termină în .ovpn generat de Server OpenVPN. Un singur fișier poate fi importat. Dacă fișierul de certificat și fișierul de configurare sunt generate individual de serverul OpenVPN, combinați două fișiere și importați întregul fișier.

3. 7. 2 Utilizator VPN

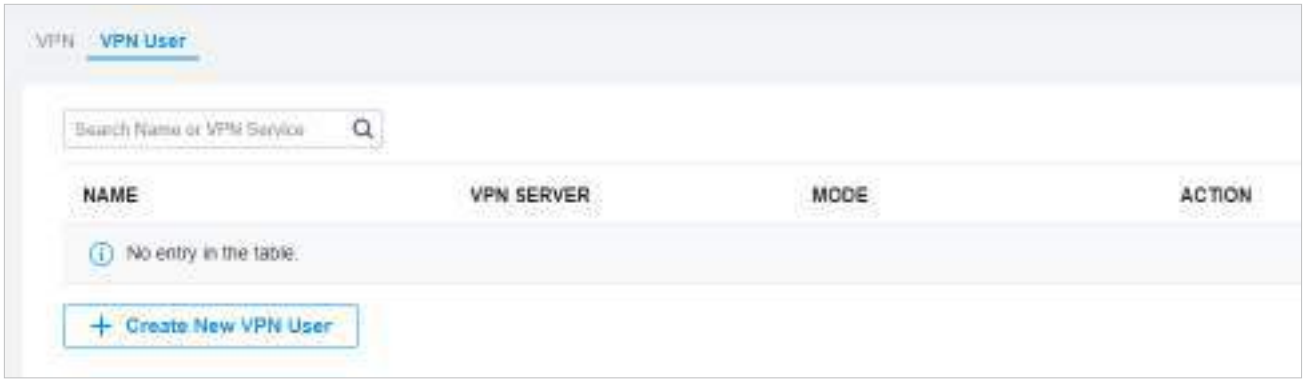
Prezentare generală

Utilizator VPN este folosit pentru a configura și înregistra setările dvs. personalizate pentru configurațiile VPN și vă permite să configurați utilizatori VPN care pot fi utilizați pentru mai multe servere VPN. Vă scutește de setarea în mod repetat a utilizatorilor VPN cu aceleași configurații atunci când doriți să aplicați utilizatorul pe servere VPN diferite.

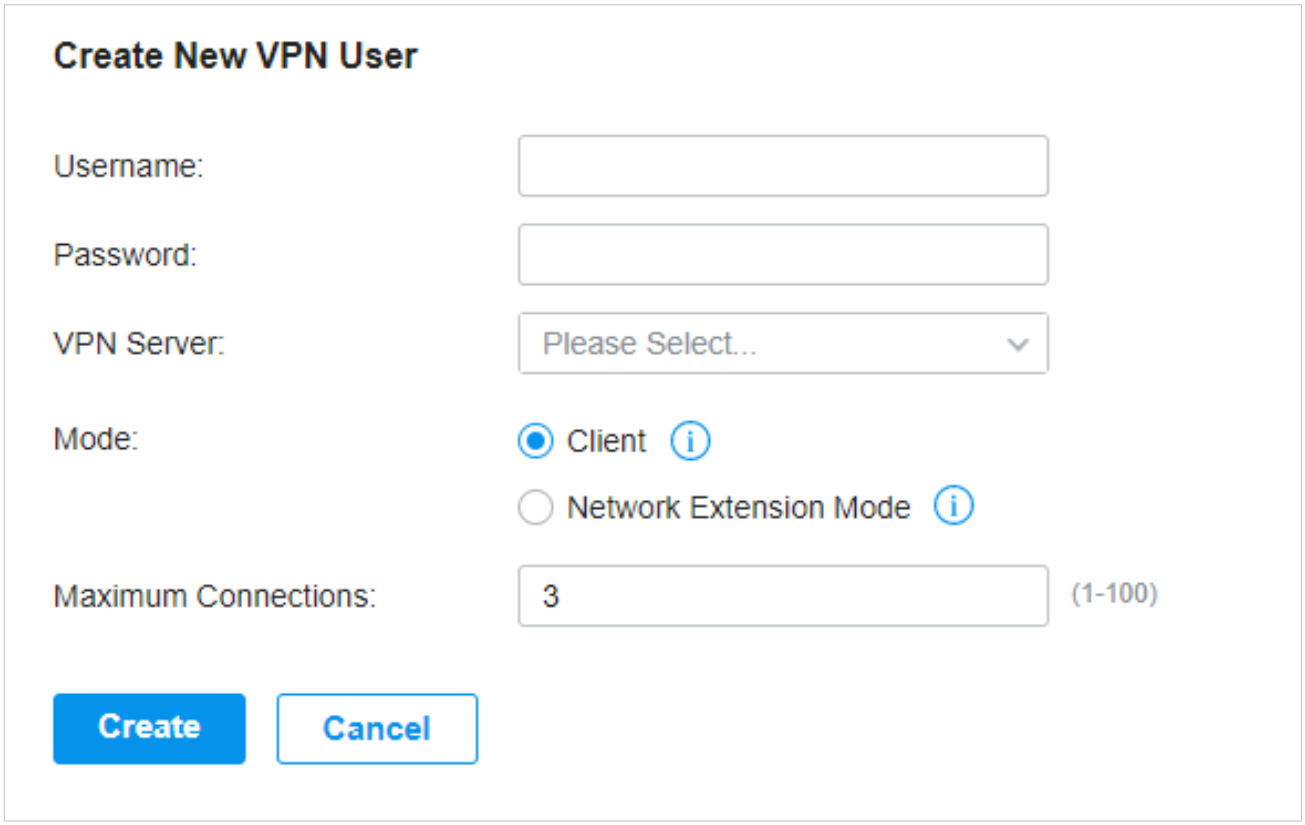
Configurare

Pentru a configura utilizatorii VPN, urmați acești pași:

1. Selectați un site din lista derulantă aOrganizare. Mergi laSetări>VPN>Utilizator VPN. Clic+Creați un utilizator VPN nou pentru a adăuga o nouă intrare de utilizator VPN.

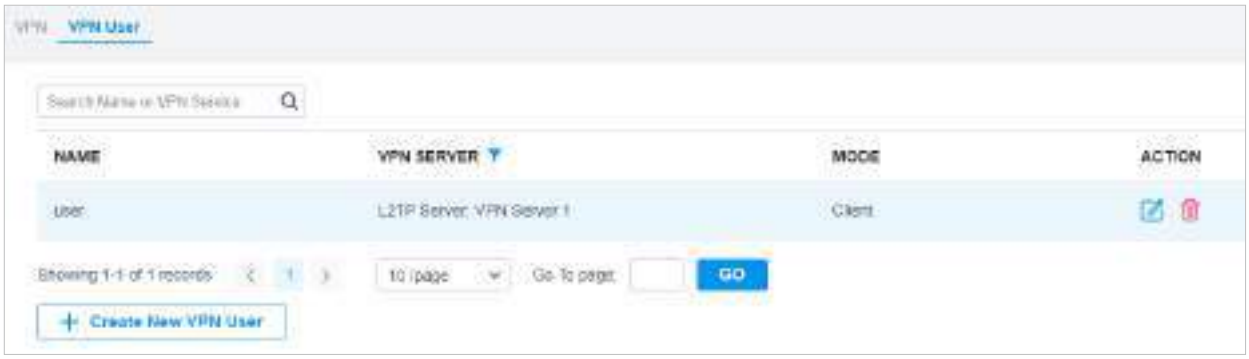


2. Specificați parametrii și faceți clicCrea.



Nume de utilizator	Introduceți numele de utilizator folosit pentru tunelul VPN. Clientul folosește numele de utilizator pentru validare înainte de a accesa rețeaua.
Parola	Introduceți parola utilizatorului. Clientul folosește parola pentru validare înainte de a accesa rețeaua.
Server VPN	Selectați politica VPN cu tipul de server VPN-L2TP/PPTP căruia i se aplică utilizatorul VPN.
Modul	Specificați modul de conectare pentru utilizatorii VPN. Client:Acest mod permite clientului să solicite o adresă IP, iar serverul furnizează adresele IP din pool-ul de IP VPN. Cu acest mod selectat, setați numărul maxim de conexiuni VPN simultane cu același cont în Conexiuni maxime. Modul extensie de rețea:Acest mod permite numai clienților din subrețeaua configurată să se conecteze la server și să obțină servicii VPN. Cu acest mod selectat, specificați subrețeaua în Remote Subnets.
Conexiuni maxime	Cu modul Client selectat, setați numărul maxim de conexiuni VPN simultane cu același cont.
Subrețele de la distanță	Cu Network Extension Mode selectat, doar clienții din subrețeaua configurată sunt permis să se conecteze la server și să obțină servicii VPN. Clic ⊕ Add Subnet la specificați subrețeaua.

Pentru a edita sau șterge utilizatorii VPN, faceți clic pe pictograma din coloana Acțiune. Puteți filtra în continuare intrările pe baza serverului VPN.



	Filtrați intrările.
	Vizualizați și editați informațiile contului utilizatorilor.
	Ștergeți utilizatorul VPN.

3. 8 Creați profiluri

Secțiunea Profiluri este utilizată pentru a configura și înregistra setările dvs. personalizate pentru configurațiile site-ului. Include intervalul de timp și profilurile de grupuri. În secțiunea Interval de timp, puteți configura șabloane de timp pentru programul wireless, programarea PoE etc. În secțiunea Grupuri, puteți configura grupuri pe baza adreselor IP, IP-Port și MAC pentru ACL, Routing, NAT etc. După crearea profilurilor , le puteți aplica pentru a multiplica configurațiile pentru site-uri diferite, evitându-vă să configurați în mod repetat aceleași informații.

3. 8. 1 Interval de timp

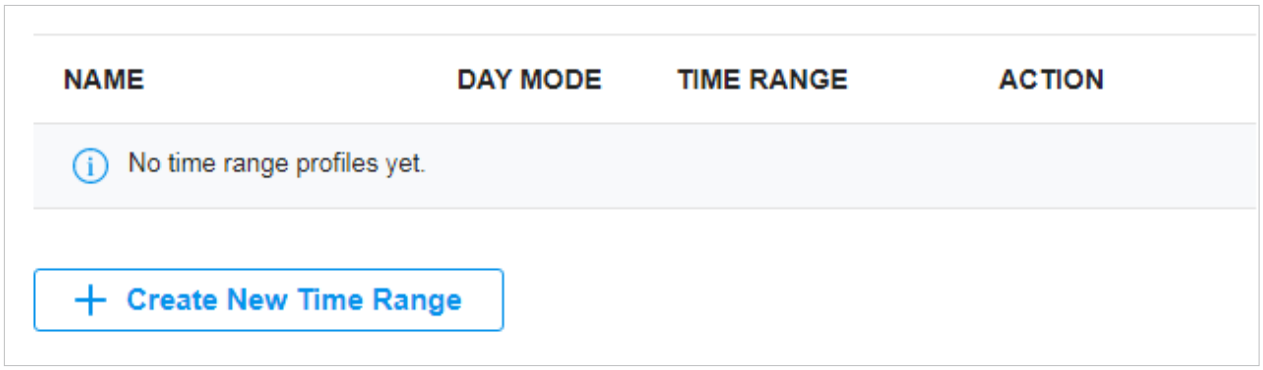
Prezentare generală

Secțiunea Interval de timp vă permite să personalizați configurațiile legate de timp. Puteți seta diferite șabloane de interval de timp care pot fi partajate și aplicate programului wireless, programului PoE etc. în configurația site-ului.

Configurare

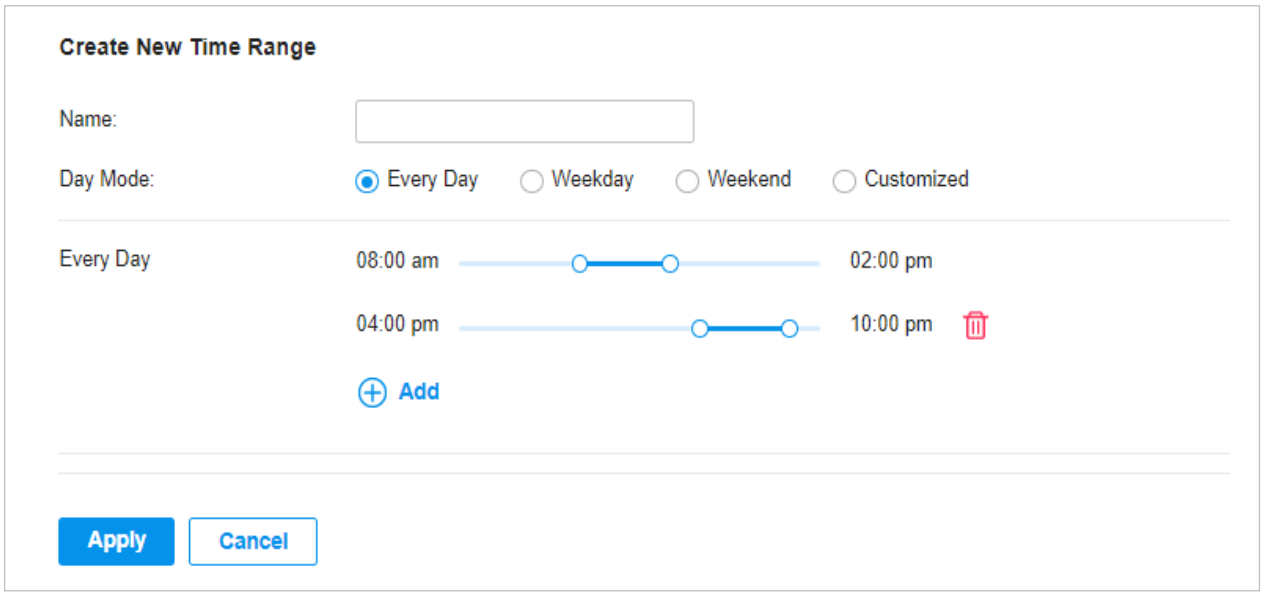
Pentru a configura profilurile intervalului de timp, urmați acești pași:

1. Selectați un site din lista derulantă aOrganizare. Mergi laSetări>Profiluri>Interval de timp. Clic
   + Creați un nou interval de timppentru a adăuga o nouă intrare în intervalul de timp. În mod implicit, nu există nicio intrare în listă.



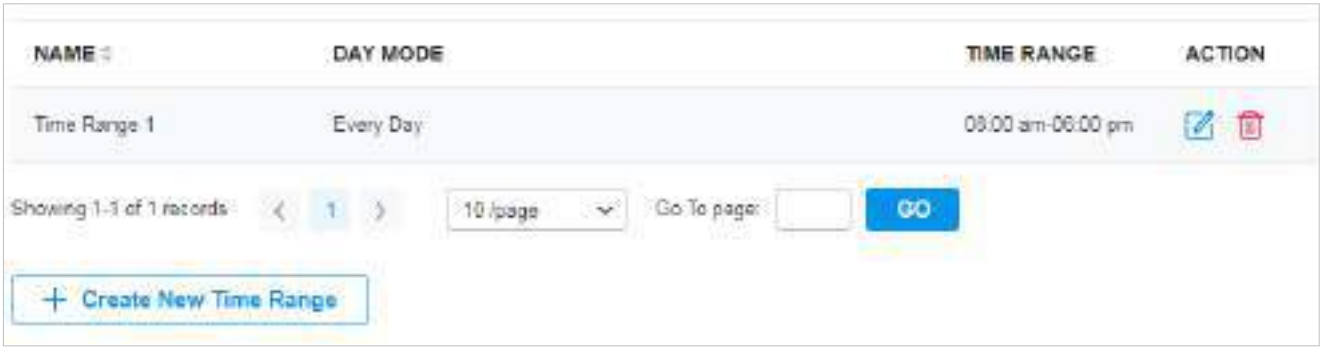
2. Introduceți un Nume pentru noua intrare, selectați Modul Zi și specificați intervalul de timp. Clic+Adăugațipentru a adăuga o nouă perioadă de timp, faceți clicaplicapentru a salva intrarea. După ce salvați intrarea nou adăugată, puteți aplica

la configurarea site-ului. Pentru a aplica profilurile de interval de timp personalizate în configurație, consultați3. 4. 3 Programare WLAN , și3. 10. 8 Program PoE.



Nume	Introduceți un nume pentru noua intrare și este un șir cu 1 până la 64 de simboluri ASCII.
Modul de zi	SelectațiÎn fiecare zi,Ziua săptămânii,Sfârșit de săptămână, sauPersonalizatmai întâi înainte de a specifica intervalul de timp pentru fiecare zi. În fiecare zi: Trebuie să setați intervalul de timp o singură dată și se va repeta în fiecare zi. Ziua săptămânii: Trebuie să setați intervalul de timp o singură dată și se va repeta în fiecare zi a săptămânii, de luni până vineri. Sfârșit de săptămână: Trebuie să setați intervalul de timp o singură dată și se va repeta în fiecare sâmbătă și duminică. Personalizat: Puteți seta un interval de timp diferit pentru zilele alese, în funcție de nevoile dvs. Când nu este aleasă o zi, WiFi este deschis toată ziua în mod implicit.

Puteți vizualiza numele, modul de zi și intervalul de timp în listă.



Pentru a edita sau șterge intrarea în intervalul de timp, faceți clic pe pictograma din coloana Acțiune.

	Editați parametrii din intrare.

	Ștergeți intrarea.

3. 8. 2 Grupe

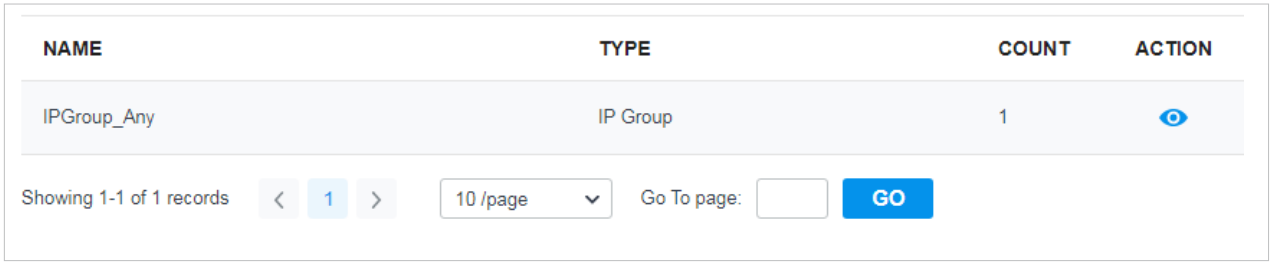
Prezentare generală

Secțiunea Grupuri vă permite să personalizați grupurile de clienți pe baza IP, IP-Port sau adresa MAC. Puteți seta reguli diferite pentru profilurile de grupuri care pot fi partajate și aplicate la ACL, Routing, NAT etc. în configurația site-ului.

Configurare

Pentru a configura profilurile de grup, urmați acești pași:

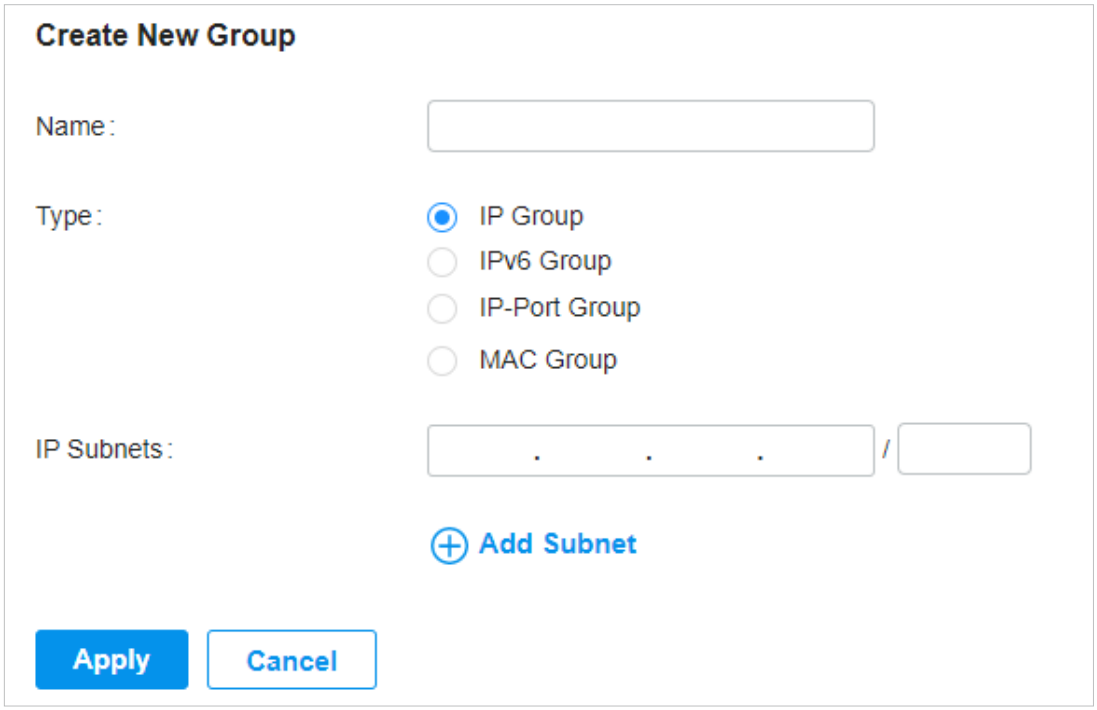
1. Selectați un site din lista derulantă aOrganizare. Mergi laSetări>Profiluri>Grupuri. În mod implicit, există o intrare care acoperă toate IP-urile și nu poate fi editată și ștearsă. Clic+Creează un grup noupentru a adăuga o nouă intrare de grup.



2. Introduceți un nume pentru noua intrare de profil de grup și selectați tipul pentru noua intrare.

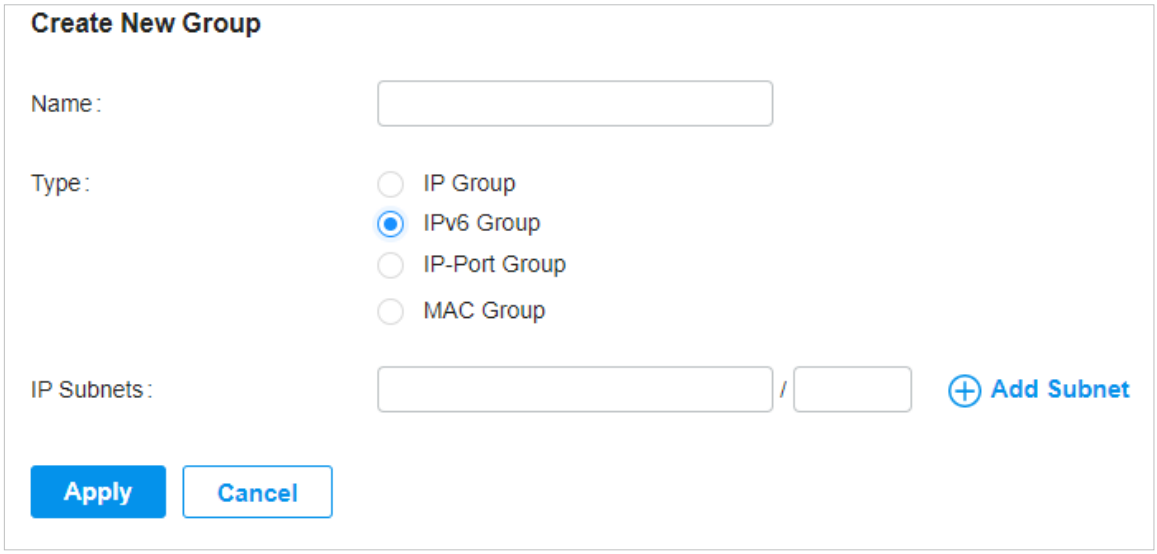
■ Bazat pe IP Group

Pentru a configura un profil de grup bazat pe IP Group, trebuie să specificați subrețelele IP, în timp ce masca de subrețea este opțională. Puteți da clic+ Adăugați subrețeapentru a adăuga subrețele noi și faceți clic pentru a le șterge.



■ Bazat pe grupul IPv6

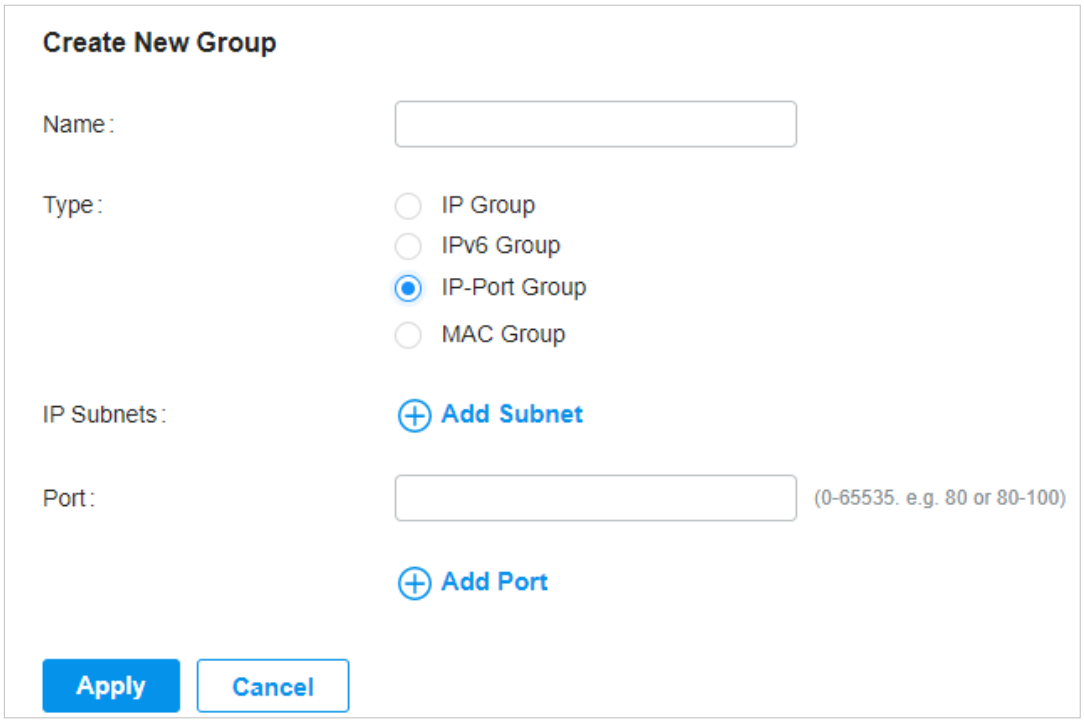
Pentru a configura un profil de grup bazat pe grupul IPv6, trebuie să specificați subrețelele IP, în timp ce masca de subrețea este opțională. Puteți da clic+ Adăugați subrețeapentru a adăuga subrețele noi și faceți clic pentru a le șterge.



■ Bazat pe IP-Port Group

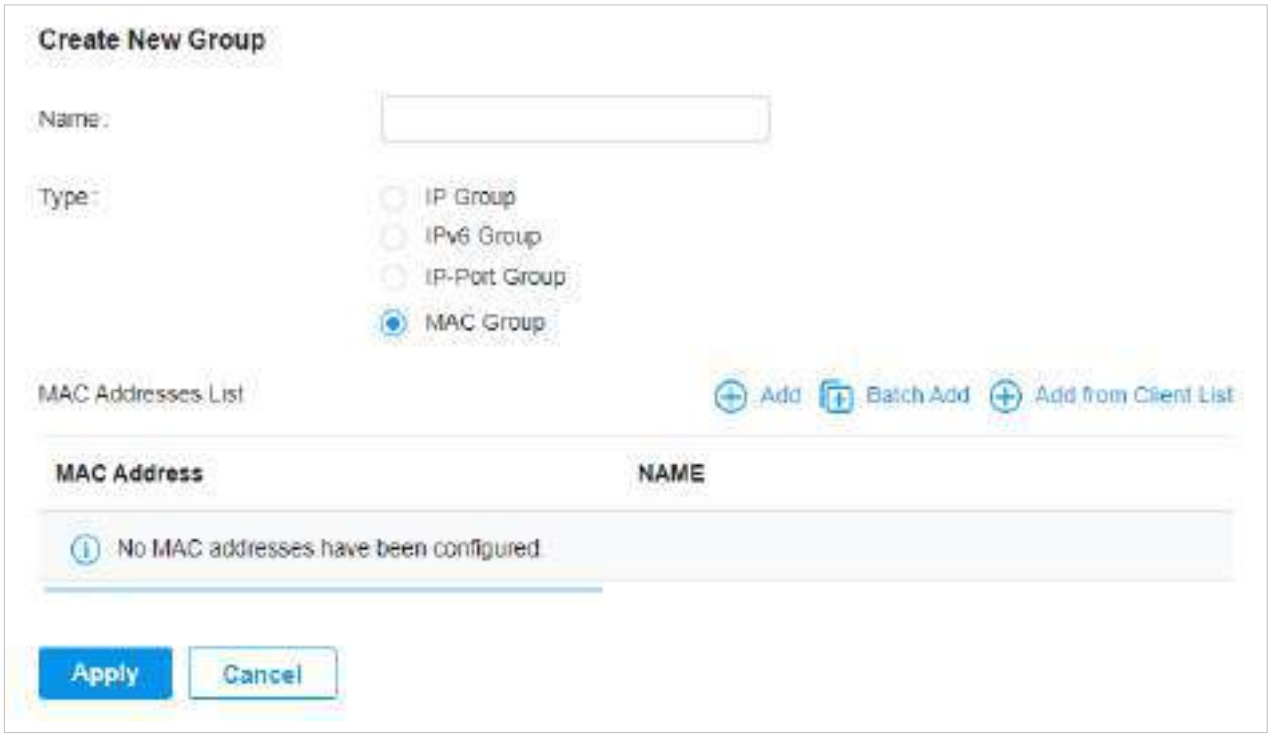
Pentru a configura un profil de grup bazat pe IP-Port Group, trebuie să specificați portul (porturile) pentru intrare, în timp ce este opțional să specificați subrețelele IP. Dacă specificați doar porturile fără a intra

orice subrețea IP, înseamnă că grupul conține porturile specificate pentru toate IP-urile. Puteți da clic+ Adăugați subrețeapentru a adăuga noi subrețele IP, faceți clic+ Adăugați un portpentru a adăuga porturi și faceți clic pentru a le șterge.



■ Bazat pe MAC Group

Pentru a configura un profil de grup bazat pe grupul MAC, trebuie să introduceți adresa(e) MAC în Lista de adrese MAC. Există trei moduri de a adăuga adrese MAC la Lista de adrese MAC.



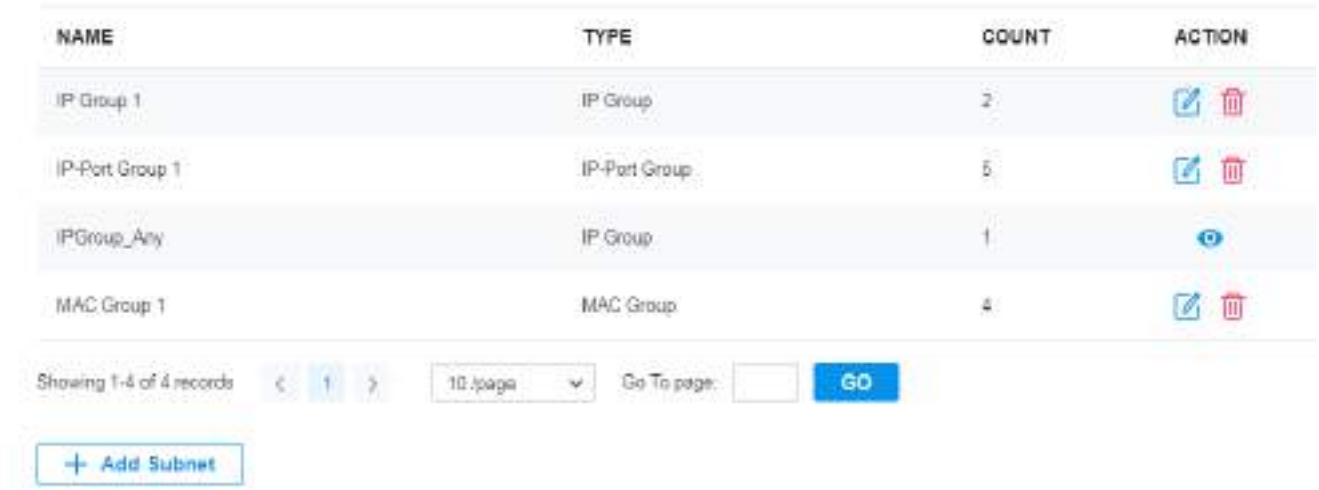
Add	Adăugați individual adresa MAC.

Batch Add	Adăugați adrese MAC în loturi. Puteți introduce adresele MAC și numele în caseta de introducere sau le puteți importa cu fișiere în format Excel, txt și text. Dacă doriți să utilizați adresele și numele MAC nou adăugate atunci când acestea sunt în conflict cu cele existente, faceți clic pe pentru a-i permite să înlocuiască Lista de control al accesului MAC curent. Notă: 1. Fiecare adresă MAC și nume trebuie introduse pe o linie nouă. Adresa MAC și numele trebuie separate printr-un spațiu. 2. Octeții dintr-o adresă MAC trebuie despărțiți printr-o cratimă. De exemplu, AA-BB-CC-DD-EE-FF.
Add from Client List	Adăugați adrese MAC de la clienții care sunt conectați la dispozitivele controlate de Omada SDN Controller.

3. Faceți clicaplicapentru a salva intrarea.

După salvarea intrării nou adăugate, le puteți aplica la configurația site-ului. Pentru a aplica profilurile personalizate în configurație, consultați3. 5. 1 ACL ,3. 6. 1 Traseul ,3. 6. 2 NAT .

Puteți vizualiza numele, tipul și numărarea în listă.



Pentru a vizualiza, edita sau șterge intrarea în grup, faceți clic pe pictograma din coloana Acțiune.

	Vizualizați și editați parametrii din intrare. Nu puteți schimba tipul atunci când editați intrarea.
	Ștergeți intrarea.

3. 8. 3 Rate Limită

Prezentare generală

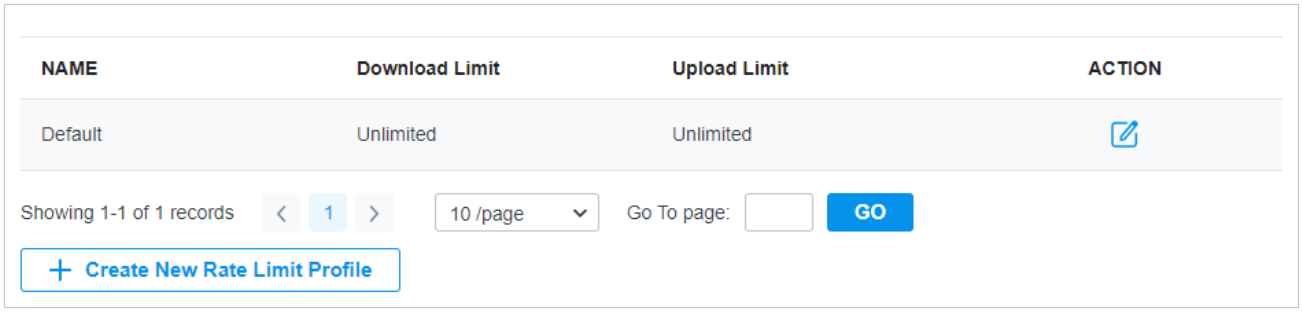
Rate Limit vă permite să personalizați configurațiile legate de rata. Puteți seta diferite șabloane de limită de rată. Acestea pot fi legate cu o rețea fără fir pentru a limita rata de încărcare/descărcare a clienților conectați

SSID și aplicat anumitor tipuri de portal, cum ar fi Utilizator local și Voucher. După crearea profilurilor, le puteți aplica la mai multe configurații, evitându-vă să configurați în mod repetat aceleași informații.

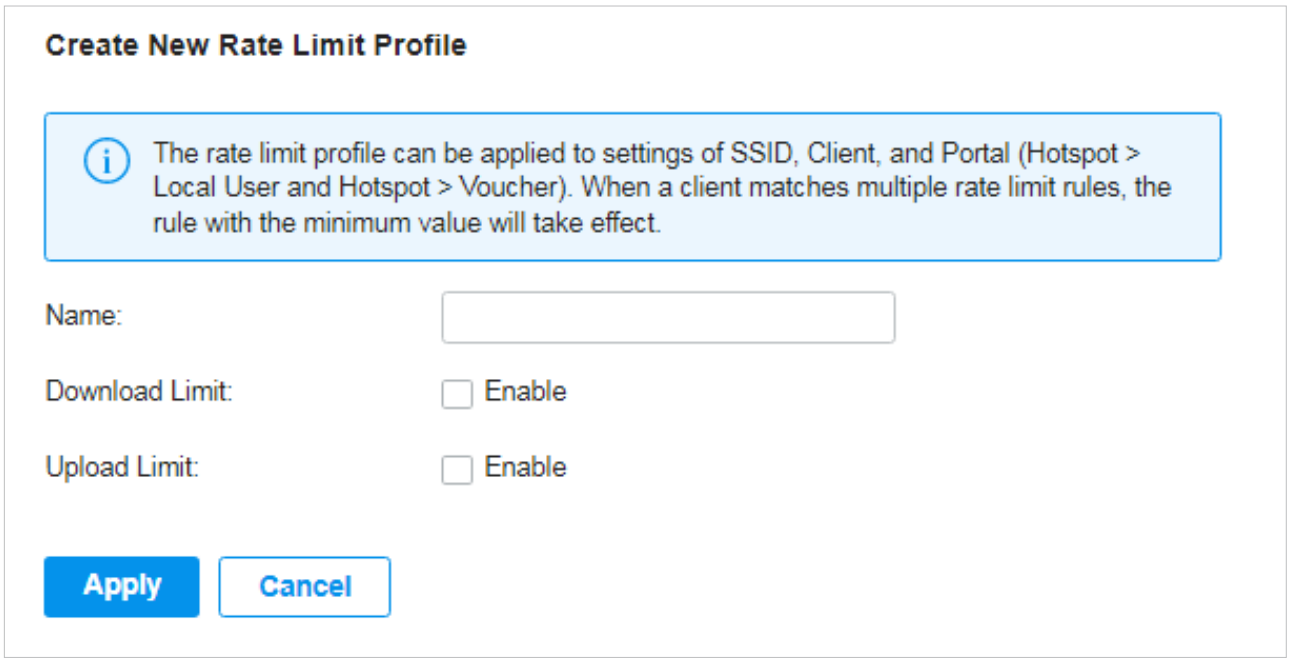
Configurare

Pentru a configura profilurile limită de rată, urmați acești pași:

1. Selectați un site din lista derulantă aOrganizare. Mergi laSetări>Profiluri>Limită de rată. În mod implicit, există o intrare fără limite și nu poate fi ștearsă. Clic+Creați un nou profil de limită de ratepentru a adăuga o nouă intrare de grup.



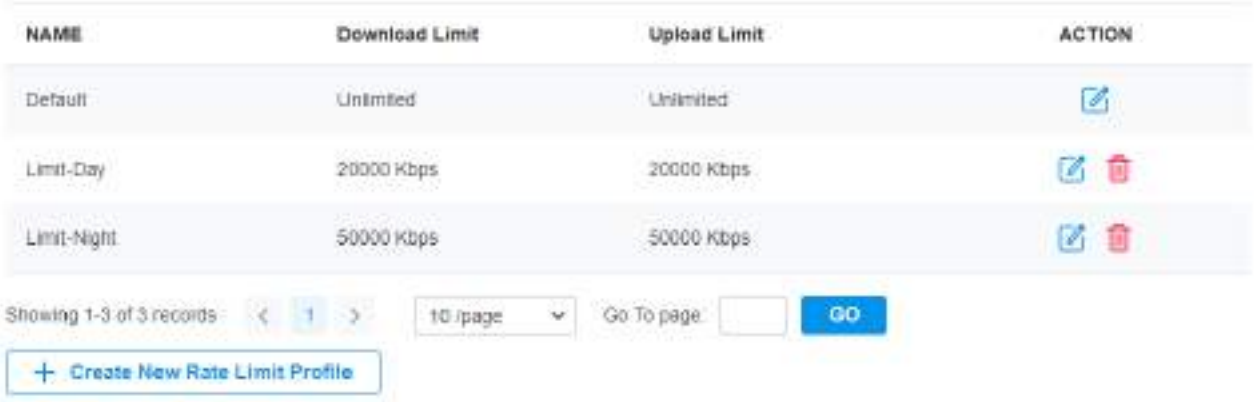
2. Introduceți un nume și specificați limita ratei de descărcare/încărcare pentru noua intrare. După ce salvați intrarea nou adăugată, le puteți aplica altor configurații. Pentru a aplica profilurile de limită de rată personalizate în configurațiile aferente, consultați3. 9. 1 Portal ,3. 4. 1 Configurați rețele wireless de bază, și6. 1. 3 Utilizarea ferestrei de proprietăți pentru a monitoriza și gestiona clienții .



Nume	Introduceți un nume pentru a identifica profilul de limită de rată creat.
Limită de descărcare	Activați limita de descărcare și specificați limita de rată corespunzător în Kbps sau Mbps.
Limită de încărcare	Activați limita de încărcare și specificați limita de rată corespunzător în Kbps sau Mbps.

2. Faceți clicaplicapentru a salva intrarea. După salvarea intrării nou adăugate, le puteți aplica la configurația site-ului. Pentru a aplica profilurile de limită de rată personalizate în configurațiile aferente, consultați3. 9. 1 Portal , și3. 4. 1 Configurați rețele wireless de bază.

Puteți vedea numele, limita de descărcare și limita de încărcare în listă.



Pentru a vizualiza, edita sau șterge profilul limită de rate, faceți clic pe pictograma din coloana Acțiune.

	Vizualizați și editați parametrii din intrare. Nu puteți schimba tipul atunci când editați intrarea.
	Ștergeți intrarea.

3. 8. 4 PPSK

Prezentare generală

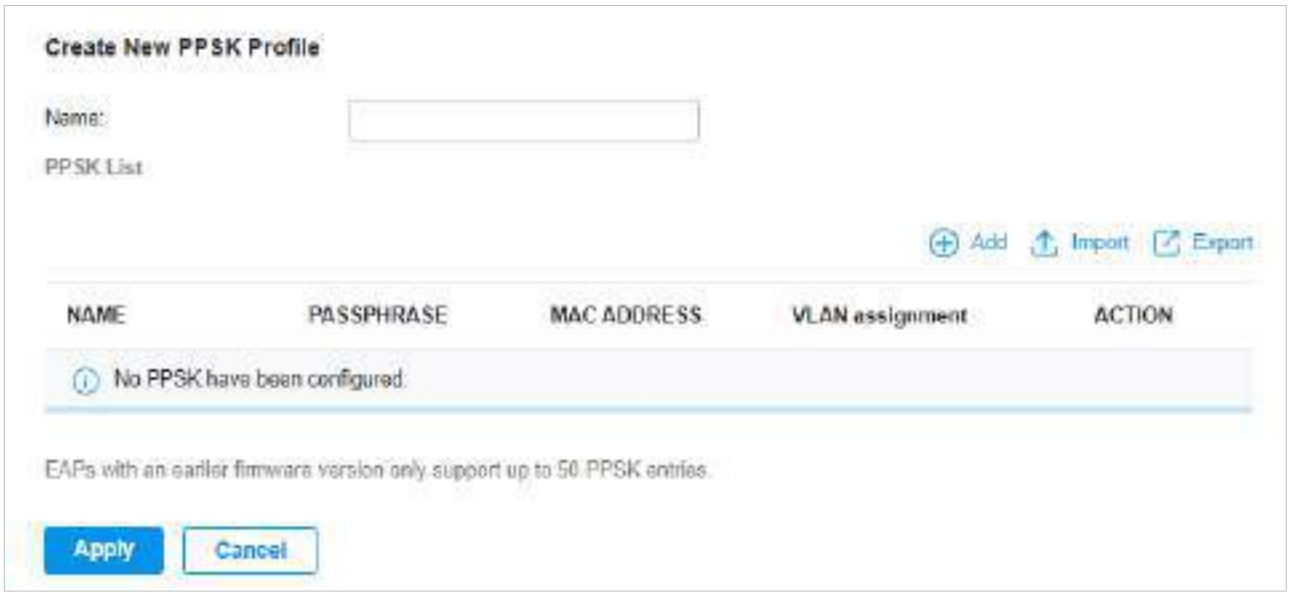
PPSK este o soluție de securitate în care dispozitivele client individuale pot fi gestionate fără prea multă complexitate. Cu PPSK, fiecărui utilizator i se atribuie o frază de acces unică pentru autentificare. De asemenea, permite legarea unei fraze de acces și a adreselor MAC ale dispozitivului și, astfel, numai dispozitivul specificat poate fi autentificat folosind fraza de acces. În PPSK, puteți crea lista PPSK și le puteți aplica mai multor rețele fără fir, evitându-vă să configurați în mod repetat aceleași informații.

Configurare

Pentru a configura profilurile PPSK, urmați acești pași:

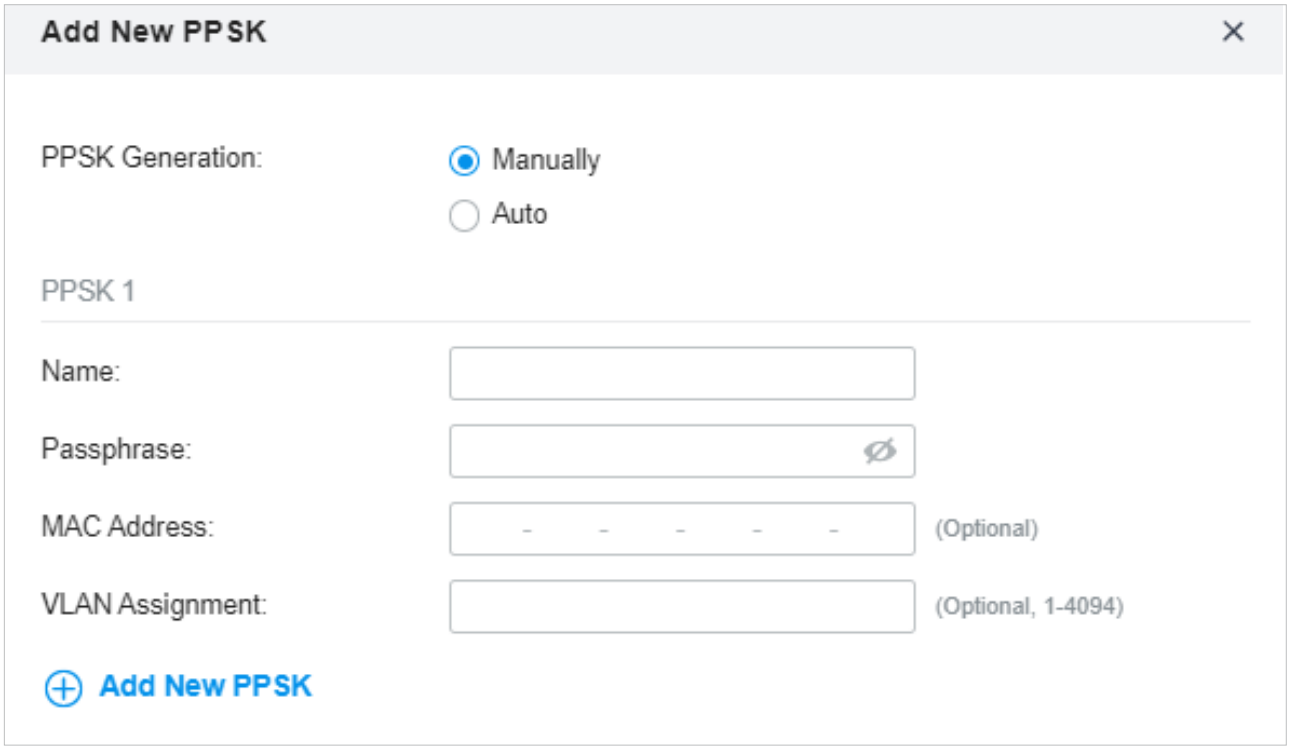
1. Selectați un site din lista derulantă aOrganizare. Mergi laSetări>Profiluri>PPSK. Clic+Creează un profil nou PPSKpentru a adăuga un nou profil PPSK.

2. Introduceți un nume pentru noul profil. Clic+Adăugațipentru a adăuga intrări noi în profilul PPSK sau faceți clicImport pentru a importa intrări în loturi dintr-un fișier.



Introduceți parametrii și faceți clicaplicapentru a salva informațiile PPSK.

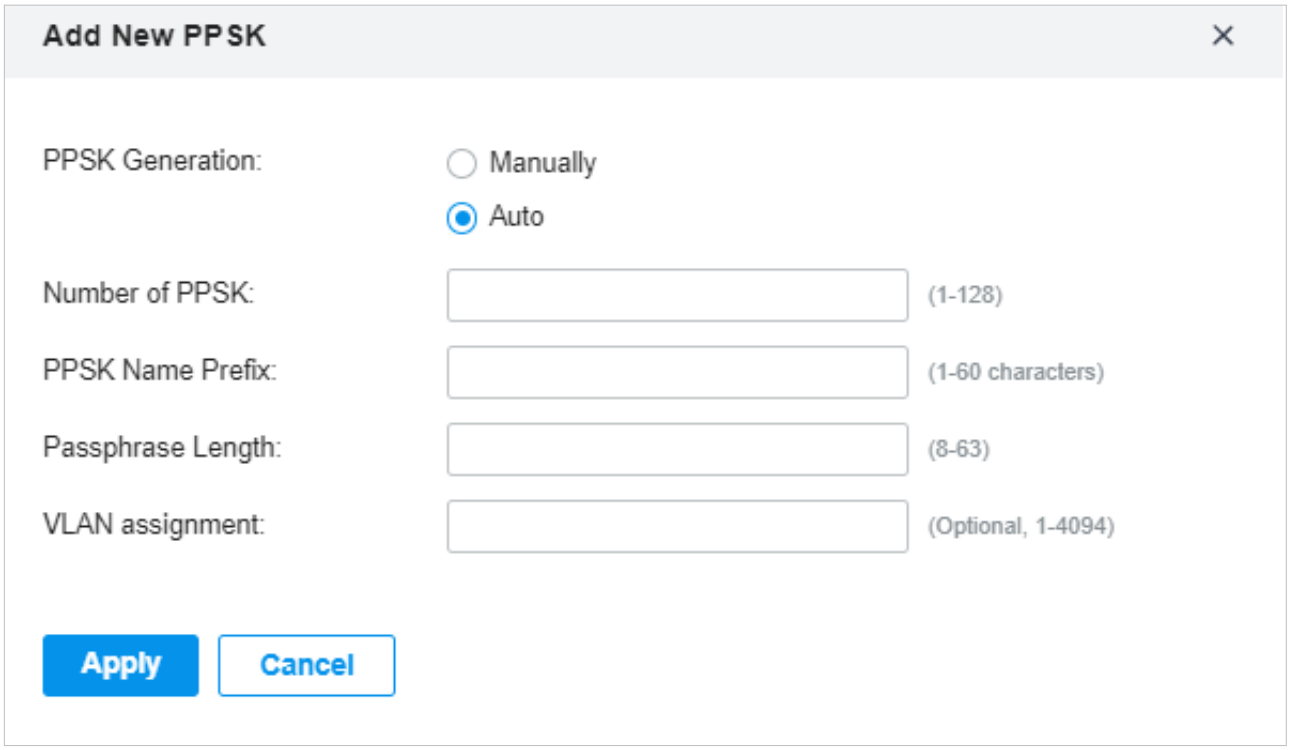
Dacă selectațiManualîn PPSK Generation, configurați parametrii:



Nume	Introduceți un nume pentru a identifica PPSK-ul creat.
Fraza de acces	Introduceți o expresie de acces, iar clientul va folosi expresia de acces pentru autentificare.

Adresa mac	(Opțional) Introduceți adresa MAC a dispozitivului care poate folosi expresia de acces pentru autentificare.
Atribuire VLAN	(Opțional) Introduceți ID-ul VLAN, iar clientul care utilizează fraza de acces pentru autentificare va fi atribuit VLAN-ului specificat.

Dacă selectațiAutoîn PPSK Generation, configurați parametrii, iar intrările PPSK vor fi generate automat.



Numărul de PPSK	Specificați câte intrări PPSK vor fi generate automat.
Prefix de nume PPSK	Specificați un prefix pentru intrările PPSK generate automat.
Lungimea frazei de acces	Specificați cât de lungi sunt frazele de acces generate automat.
Atribuire VLAN	(Opțional) Introduceți ID-ul VLAN, iar clientul care utilizează fraza de acces pentru autentificare va fi atribuit VLAN-ului specificat.

3. Faceți clicaplicapentru a salva profilul. După salvarea profilului nou adăugat, le puteți aplica rețelelor fără fir, consultați3. 4. 1 Configurați rețele wireless de bază.

Puteți vedea numele și rețeaua fără fir (SSID) la care este aplicat profilul PPSK în listă.

Pentru a vizualiza, edita sau șterge profilul PPSK, faceți clic pe pictograma din coloana Acțiune.

	Vizualizați și editați parametrii din intrare.
	Ștergeți intrarea.

3. 9 Autentificare

Autentificarea este un portofoliu de caracteristici concepute pentru a autoriza accesul la rețea clienților, ceea ce sporește securitatea rețelei. Serviciile de autentificare includ3. 9. 1 Portal ,3. 9. 2 802.1X și3. 9. 3 Autentificare bazată pe MAC , acoperind toate nevoile de autentificare atât a clienților cu fir, cât și fără fir.

3. 9. 1 Portal

Prezentare generală

Autentificarea prin portal oferă servicii de autentificare convenabile clienților care au nevoie doar de acces temporar la rețea, cum ar fi clienții dintr-un restaurant sau dintr-un supermarket. Pentru a accesa rețeaua, acești clienți trebuie să intre în pagina de autentificare și să folosească informațiile de conectare corecte pentru a trece autentificarea. În plus, puteți personaliza pagina de autentificare pentru autentificare și puteți specifica o adresă URL către care vor fi redirecționați clienții autentificați.

Autentificarea portalului are efect asupra SSID-urilor și rețelelor LAN. EAP-urile autentifică clienții wireless care se conectează la SSID cu Portal configurat, iar gateway-ul autentifică clienții cu fir care se conectează la rețea cu Portal configurat. Pentru a face autentificarea Portal disponibilă pentru clienții cu fir și fără fir, asigurați-vă că atât gateway-ul, cât și EAP-urile sunt conectate și funcționează corect.

Controlerul oferă șase tipuri de autentificare Portal:

- Fără autentificare

  Cu acest tip de autentificare configurat, clienții pot trece autentificarea și pot accesa rețeaua fără a furniza informații de conectare. Clienții trebuie doar să accepte termenii (dacă sunt configurați) și să facă clic pe butonul Conectare.

- Parolă simplă

  Cu acest tip de autentificare configurat, clienților li se cere să introducă parola corectă pentru a trece autentificarea. Toți clienții folosesc aceeași parolă care este configurată în controler.

- Hotspot

  Cu acest tip de autentificare configurat, clienții pot accesa rețeaua după ce au trecut orice tip de autentificare:

  - Bon

    Clienții pot folosi codurile unice de voucher generate de controlor într-un interval de timp predefinit. Codurile de voucher pot fi tipărite de la controler, astfel încât să puteți imprima codurile și să le distribuiți clienților dvs. pentru a lega accesul la rețea de consum.

  - Utilizator local

    Clienții trebuie să introducă numele de utilizator și parola corecte ale contului de conectare pentru a trece autentificarea.

- SMS

  Clienții pot obține coduri de verificare folosind telefoanele lor mobile și pot introduce codurile primite pentru a trece autentificarea.

- RAZĂ

  Clienții trebuie să introducă numele de utilizator și parola corecte care sunt stocate pe serverul RADIUS pentru a trece autentificarea.

- Form Auth

  Clienții trebuie să completeze un sondaj creat de administratorul de rețea pentru a trece autentificarea. Poate fi folosit pentru a colecta feedback de la clienții dvs.

■ Server RADIUS extern

Clienții trebuie să introducă numele de utilizator și parola corecte create pe serverul RADIUS pentru a trece autentificarea.

■ Server de portal extern

Opțiunea External Portal Server este concepută pentru dezvoltatori. Ei își pot personaliza propriul tip de autentificare, cum ar fi autentificarea contului Google, în funcție de interfața furnizată de Omada Controller.

■ Facebook

Cu Portalul Facebook configurat, atunci când clienții se conectează la Wi-Fi, aceștia vor fi redirecționați către pagina dvs. de Facebook. Pentru a accesa internetul, clienții trebuie să se autentifice în contul lor sau să introducă codul parolei în pagina de Facebook.

Autentificarea portalului poate funcționa cu Politica de control al accesului, care acordă acces la rețea specific utilizatorilor cu identități valide. Puteți determina că clienții care nu au trecut autentificarea Portal pot accesa doar resursele de rețea permise de Politica de control al accesului.

■ Acces de pre-autentificare

Pre-AuthenticationAccess permite clienților neautentificați să acceseze resursele specifice de rețea.

■ Client fără autentificare

Clienții fără autentificare le permit anumitor clienți să acceseze resursele specifice ale rețelei fără autentificare.

Configurare

Pentru a finaliza configurarea portalului, urmați acești pași:

1)Clic + Create New Portal pentru a crea o nouă intrare în Portal.

2)Clic pentru a activa Portal, selectați SSID-urile și rețelele LAN pentru ca portalul să aibă efect și configurați parametrii de bază, inclusiv tipul de autentificare, expirarea timpului de autentificare și așa mai departe.

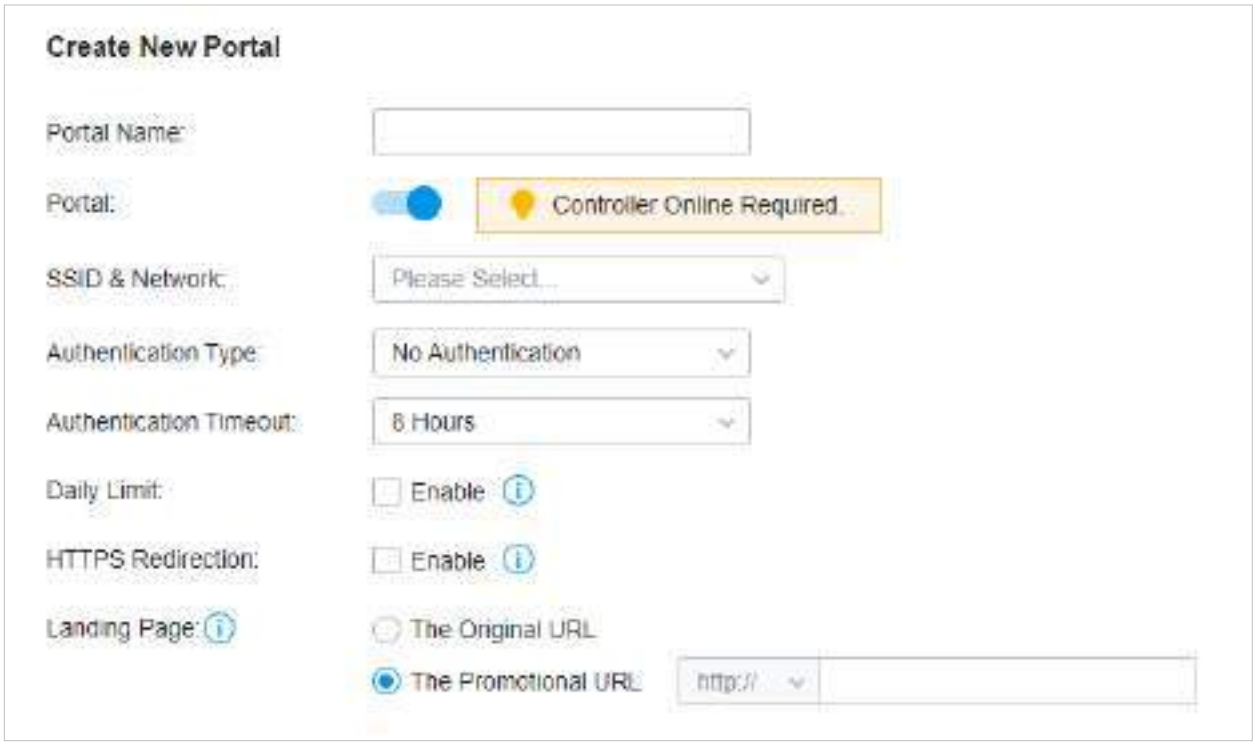
3)Personalizați pagina portalului, inclusiv imaginea de fundal, imaginea siglei și așa mai departe.

4) (Opțional) Configurați politicile de control al accesului, inclusiv accesul pre-autentificare și clienții fără autentificare, dacă este necesar.

Următoarea parte prezintă modul de configurare a fiecărui tip de autentificare Portal:Fără autentificare , Parolă simplă,Hotspot(Voucher, utilizator local, SMS, RADIUS),Server RADIUS extern ,Server de portal extern șiFacebook .

■ Configurarea portalului fără autentificare

1. Selectați un site din lista derulantă aOrganizare. Mergi laSetări>Autentificare>Portal. În fila Portal, faceți clic + Create New Portal pentru a crea o nouă intrare în portal. Apoi faceți clic pentru a activa Portal și încărcați pagina următoare.

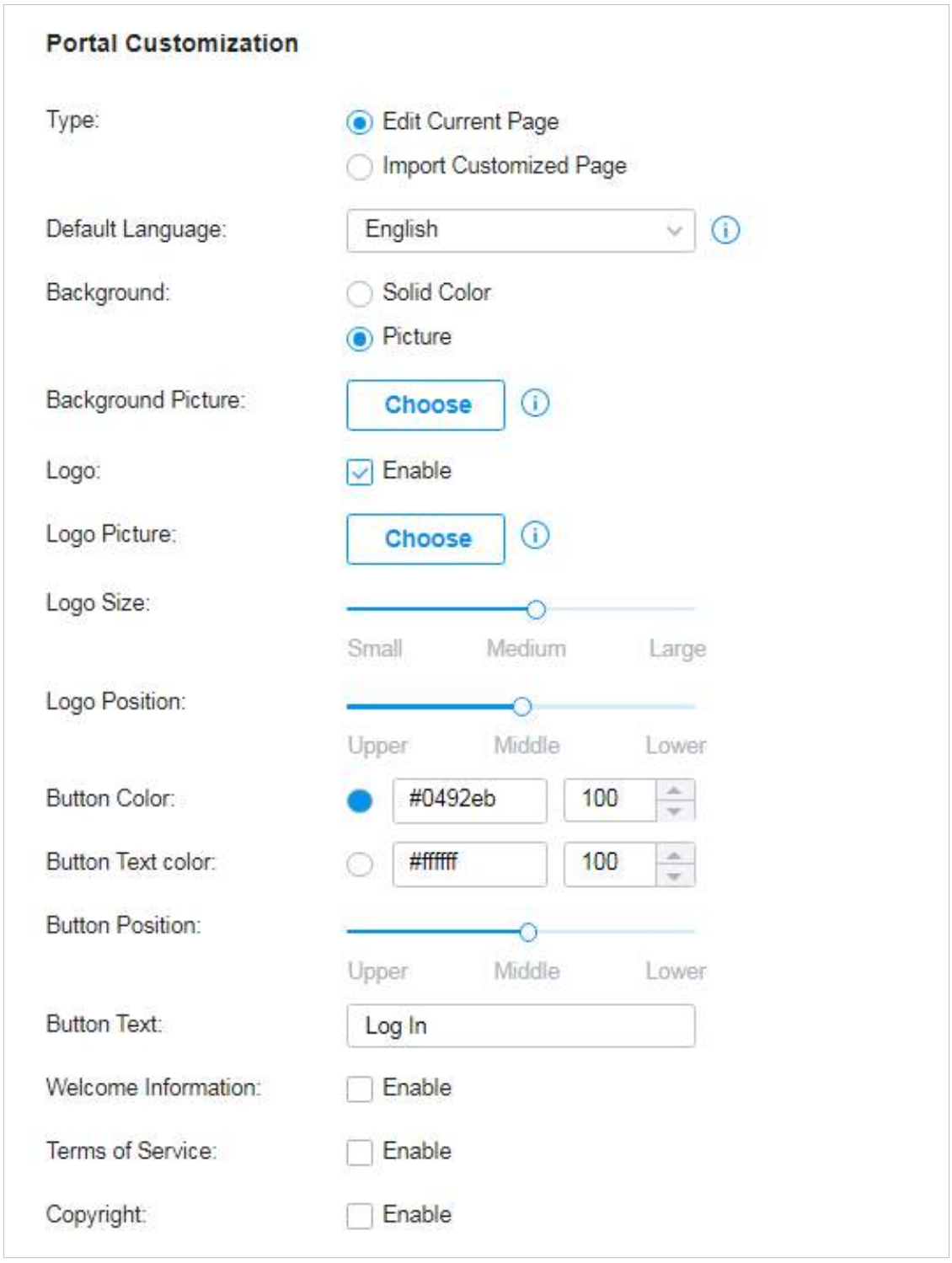


2. Selectați SSID-urile și rețelele LAN pentru care portalul să aibă efect și configurați parametrii de bază, inclusiv tipul de autentificare, expirarea timpului de autentificare și așa mai departe.

Numele portalului	Introduceți un nume pentru a identifica intrarea creată în Portal.
Portal	Clic pentru a activa Portal.
SSID și rețea	Selectați unul sau mai multe SSID-uri sau rețele LAN pentru portal. Clienții conectați la SSID-urile sau rețelele LAN selectate trebuie să se conecteze la o pagină web pentru a stabili verificarea înainte de a accesa rețeaua.
tip de autentificare	Selectați tipul de autentificare Portal ca Fără autentificare.
Timeout autentificare	Selectați durata de conectare. Clienții vor fi offline după expirarea timpului de autentificare.
Limită zilnică	Faceți clic pe caseta de selectare pentru a activa Limita zilnică. Cu această caracteristică activată, după expirarea timpului de autentificare, clienții nu pot fi autentificați din nou până a doua zi. Cu această caracteristică dezactivată, după expirarea timpului de autentificare, clienții se pot autentifica din nou fără limită.

Redirecționare HTTPS	Faceți clic pe caseta de selectare pentru a activa redirecționarea HTTPS. Cu această caracteristică activată, clienții neautorizați vor fi redirecționați către pagina Portal atunci când încearcă să răsfoiască site-urile HTTPS. Cu această caracteristică dezactivată, clienții neautorizați nu pot naviga pe site-uri web HTTPS și nu sunt redirecționați către pagina Portal.
Pagina de destinație	Selectați la ce pagină va fi redirecționat clientul după o autentificare cu succes. Adresa URL originală:Clienții sunt direcționați către adresa URL pe care o solicită după ce trec autentificarea portalului. Adresa URL promoțională:Clienții sunt direcționați către adresa URL specificată după ce trec autentificarea Portal.

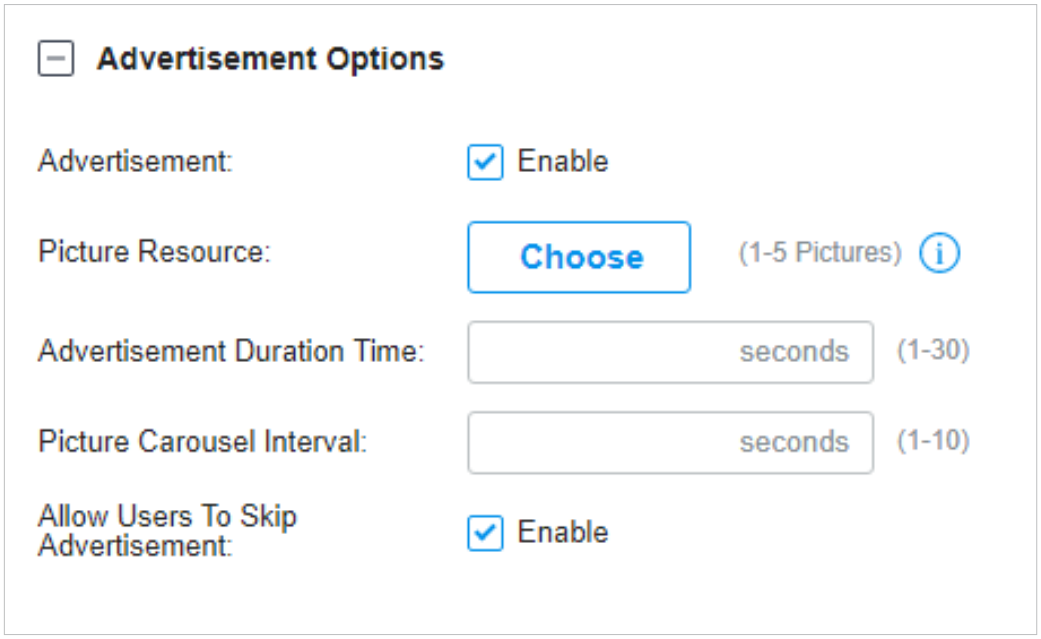
3. În secțiunea Personalizare portal, personalizați pagina Portal, inclusiv imaginea de fundal, imaginea siglei și așa mai departe.



Tip	Selectați tipul paginii Portal. Editați pagina curentă:Editați parametrii aferenți pentru a personaliza pagina Portal pe baza paginii furnizate. Importă pagină personalizată:Faceți clic Import pentru a importa pagina dvs. unică de portal pentru branding pe el conform companiei dvs.

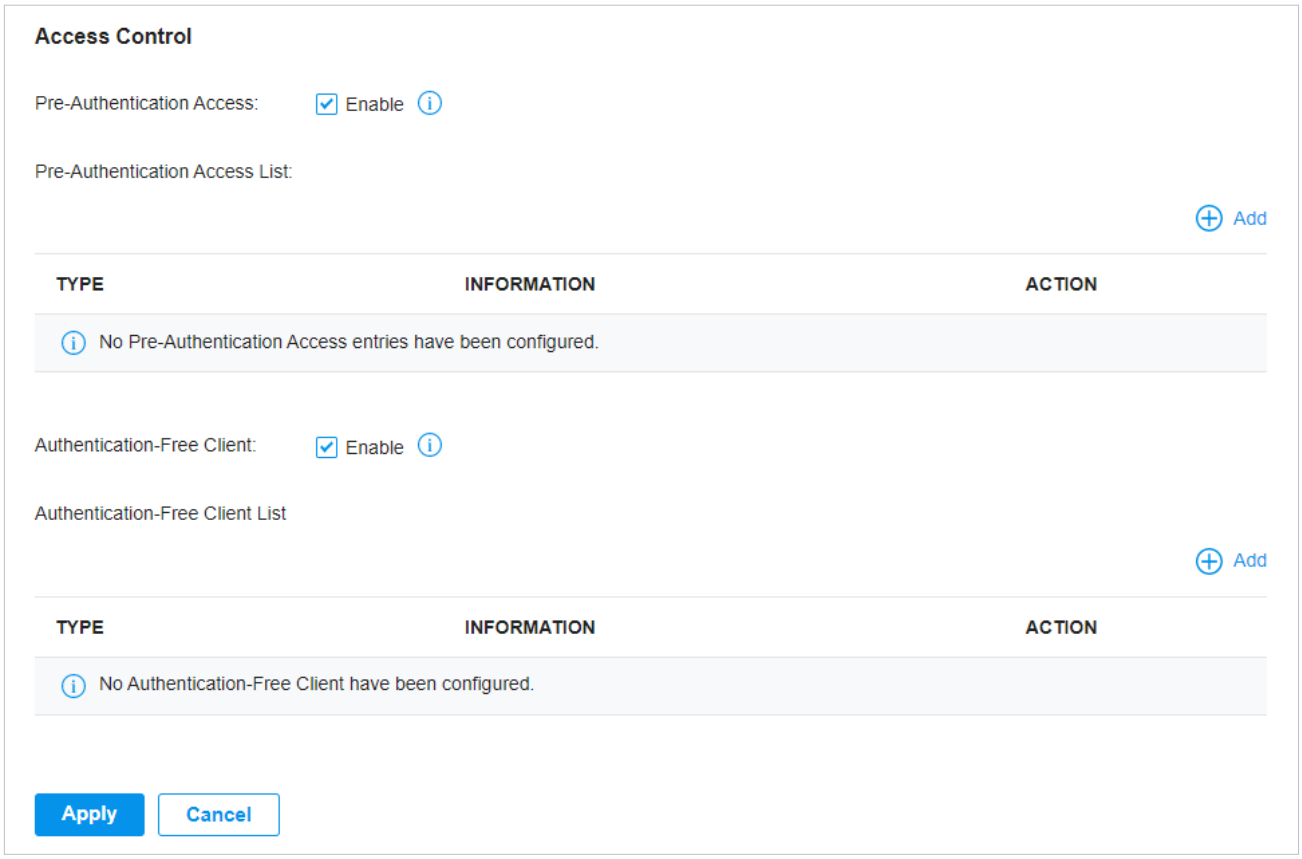
Limba implicita	Selectați limba implicită afișată pe pagina Portal. Controlerul ajustează automat limba afișată pe pagina Portal în funcție de limba sistemului a clienților. Dacă limba nu este acceptată, controlerul va folosi limba implicită specificată aici.
fundal	Selectați tipul de fundal. Culoare solida:Configurați culoarea de fundal dorită introducând manual codul de culoare HTML hexazecimal sau prin selectorul de culori. Imagine:Clic Choose și selectați o imagine de pe computer ca fundal.
Siglă	Faceți clic pentru a afișa sigla pe pagina portalului.
Imagine cu logo	Clic Choose și selectați o imagine de pe computer ca logo.
Dimensiunea logo-ului	Ajustați dimensiunea logo-ului pe pagina portalului.
Poziția logo-ului	Ajustați poziția siglei pe pagina Portal.
Culoarea butonului	Configurați culoarea de fundal dorită pentru buton introducând manual codul de culoare HTML hexazecimal sau prin selectorul de culori.
Culoarea textului butonului	Configurați culoarea textului dorită pentru buton introducând manual codul de culoare HTML hexazecimal sau prin selectorul de culori.
Poziția butonului	Selectați poziția butonului pe pagina portalului.
Buton Text	Introduceți textul pentru buton.
Informații de bun venit	Faceți clic pe caseta de selectare și introduceți text ca informații de bun venit. Puteți specifica dimensiunea dorită a fontului textului și puteți configura culoarea textului introducând manual codul de culoare HTML hexazecimal sau prin selectorul de culori.
Termenii serviciului	Faceți clic pe caseta de selectare și introduceți text ca termeni și condiții în caseta următoare. Clic Adăugați termenipentru a introduce numele și contextul termenilor care vor apărea după ce un client face clic pe linkul din Termenii și condițiile.
Drepturi de autor	Faceți clic pe caseta de selectare și introduceți text ca drepturi de autor în caseta următoare. Puteți specifica dimensiunea dorită a fontului textului și puteți configura culoarea textului introducând manual codul de culoare HTML hexazecimal sau prin selectorul de culori.
Afișați redirecționarea Numărătoarea inversă După Autorizat	Când este activat, sistemul va afișa numărătoarea inversă de redirecționare a portalului.

Faceți clic pe Opțiuni de publicitate și cpersonalizați imaginile publicitare pe pagina de autentificare.



Publicitate	Faceți clic pe caseta de selectare pentru a activa funcția Publicitate. Cu această funcție activată, puteți adăuga imagini publicitare pe pagina de autentificare. Aceste imagini publicitare vor fi afișate înainte ca pagina de conectare să apară.
Resursa de imagine	Clic Choose și selectați imagini de pe computer ca imagini publicitare. Când sunt adăugate mai multe imagini, acestea vor fi redate în buclă.
Durata reclamei Timp	Introduceți durata pentru imaginile publicitare. Pe această perioadă, imaginile vor fi redate în buclă. Dacă durata de timp nu este suficientă pentru toate imaginile, restul nu vor fi afișate.
Carusel de imagini Interval	Introduceți intervalul carusel de imagini. De exemplu, dacă această valoare este setată la 5 secunde, prima imagine va fi afișată timp de 5 secunde, urmată de a doua imagine timp de 5 secunde și așa mai departe.
Permiteți utilizatorilor să omite reclamele	Faceți clic pe caseta de selectare pentru a permite utilizatorilor să omite reclamele.

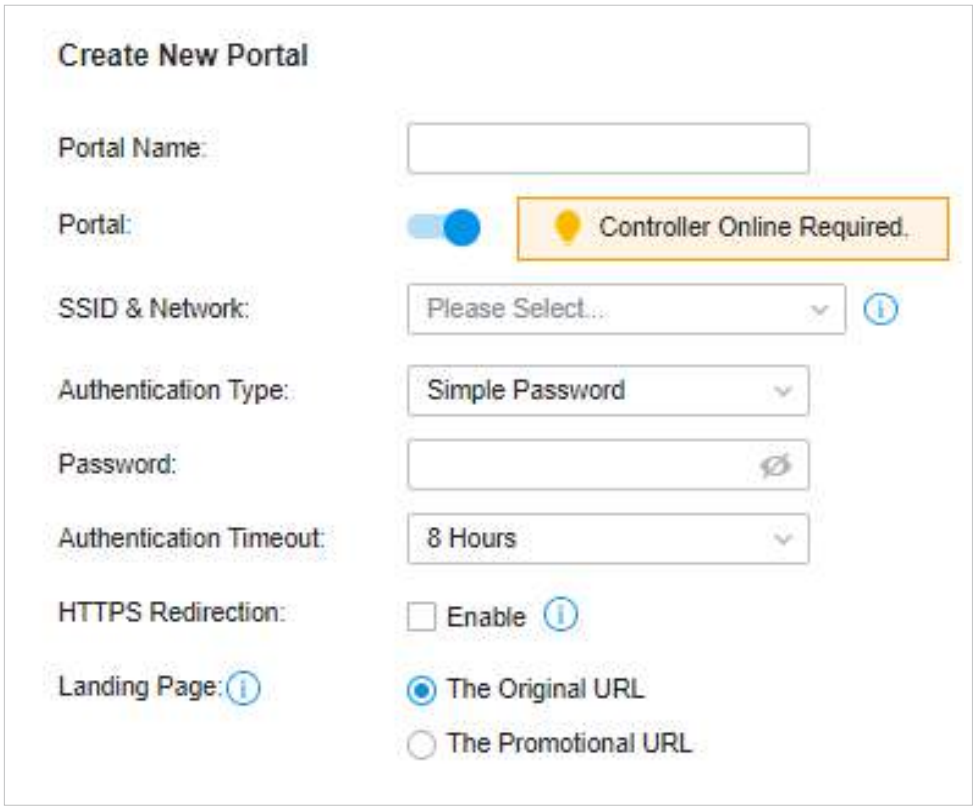
4. (Opțional) Configurați regulile de control al accesului, inclusiv Accesul pre-autentificare și Clientul fără autentificare, dacă este necesar. Mergi laSetări>Autentificare>Portal. În fila Control acces, faceți clic pe caseta de selectare pentru a activa Accesul de pre-autentificare și pentru a seta Clientul fără autentificare.



Preautentificare Acces	Faceți clic pe caseta de selectare pentru a activa Accesul de pre-autentificare. Cu această caracteristică activată, clienților neautentificați li se permite să acceseze subrețelele și resursele web specificate în Lista de acces pre-autentificare de mai jos.
Preautentificare Lista de acces	Clic Add pentru a configura intervalul IP sau adresa URL care sunt clienții neautentificați permis accesul.
Fără autentificare Client	Faceți clic pe caseta de selectare pentru a activa Clientul fără autentificare. Cu această caracteristică activată, puteți permite anumitor clienți să acceseze internetul fără autentificarea portalului.
Fără autentificare Lista de clienti	Clic Add și introduceți adresa IP sau adresa MAC a clienților fără autentificare.

■ Configurarea portalului cu parolă simplă

1. Selectați un site din lista derulantă aOrganizare. Mergi laSetări>Autentificare>Portal. În fila Portal, faceți clic + Create New Portal pentru a crea o nouă intrare în portal. Apoi faceți clic pentru a activa Portal și încărcați pagina următoare.

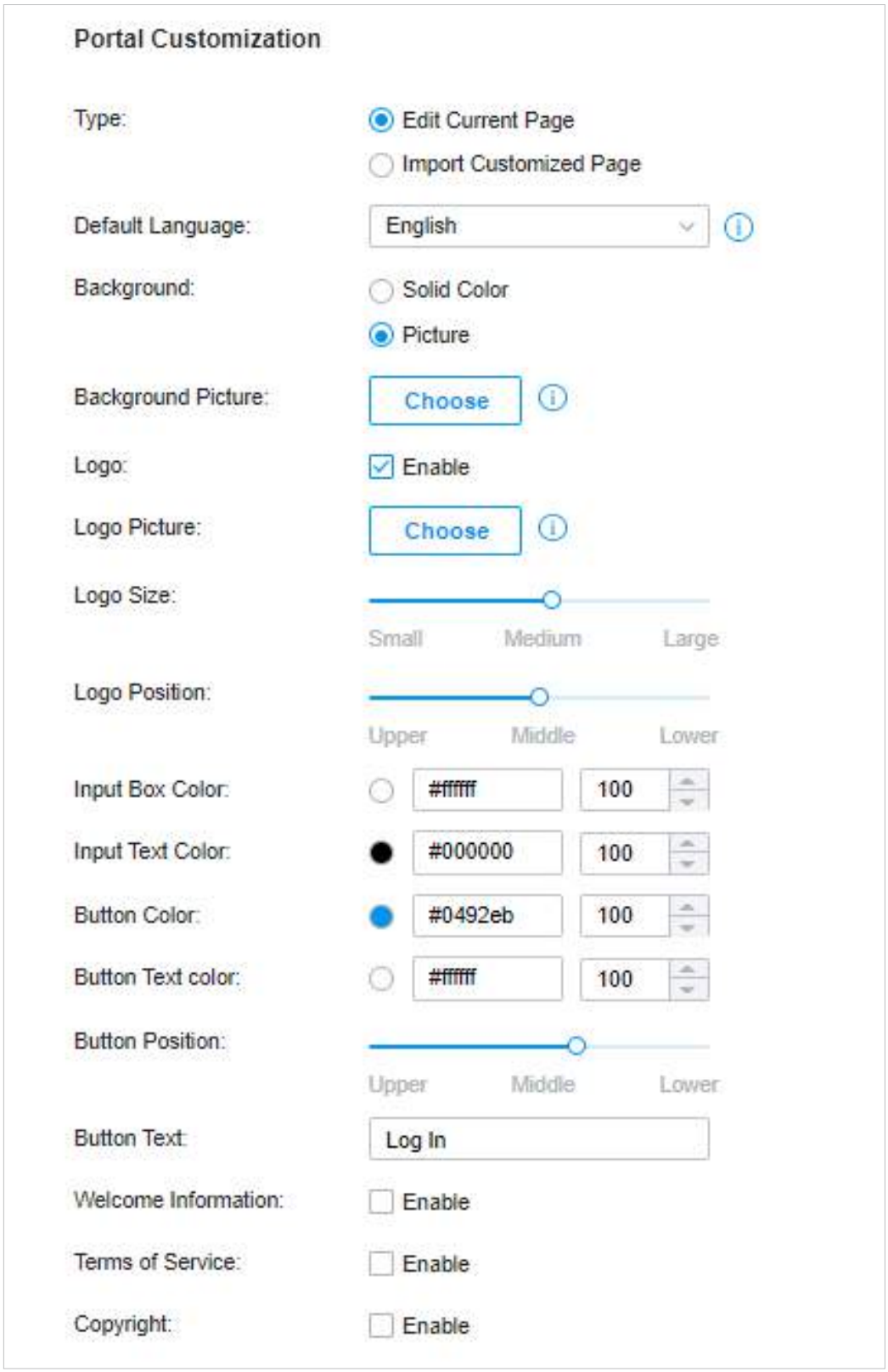


2. Selectați SSID-urile și rețelele LAN pentru care portalul să aibă efect și configurați parametrii de bază, inclusiv tipul de autentificare, expirarea timpului de autentificare și așa mai departe.

SSID și rețea	Selectați unul sau mai multe SSID-uri sau rețele LAN pentru portal. Clienții conectați la SSID-urile sau rețelele LAN selectate trebuie să se conecteze la o pagină web pentru a stabili verificarea înainte de a accesa rețeaua.
tip de autentificare	Selectați tipul de autentificare Portal ca parolă simplă.
Parola	Specificați parola pentru portal.
Timeout autentificare	Selectați durata de conectare. Clienții vor fi offline după expirarea timpului de autentificare.
Redirecționare HTTPS	Faceți clic pe caseta de selectare pentru a activa redirecționarea HTTPS. Cu această caracteristică activată, clienții neautorizați vor fi redirecționați către pagina Portal atunci când încearcă să răsfoiască site-urile HTTPS. Cu această caracteristică dezactivată, clienții neautorizați nu pot naviga pe site-uri web HTTPS și nu sunt redirecționați către pagina Portal.

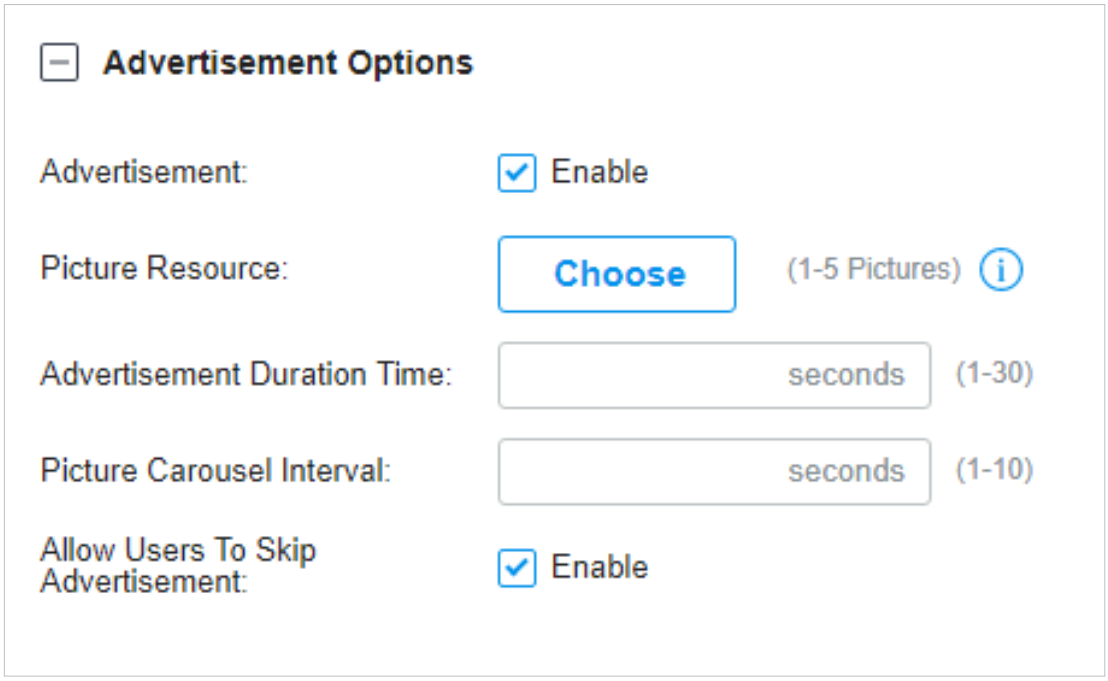
Pagina de destinație	Selectați la ce pagină va fi redirecționat clientul după o autentificare cu succes. Adresa URL originală:Clienții sunt direcționați către adresa URL pe care o solicită după ce trec autentificarea portalului. Adresa URL promoțională:Clienții sunt direcționați către adresa URL specificată aici după ce trec autentificarea portalului.

3. În secțiunea Personalizare portal, personalizați pagina Portal, inclusiv imaginea de fundal, imaginea siglei și așa mai departe.



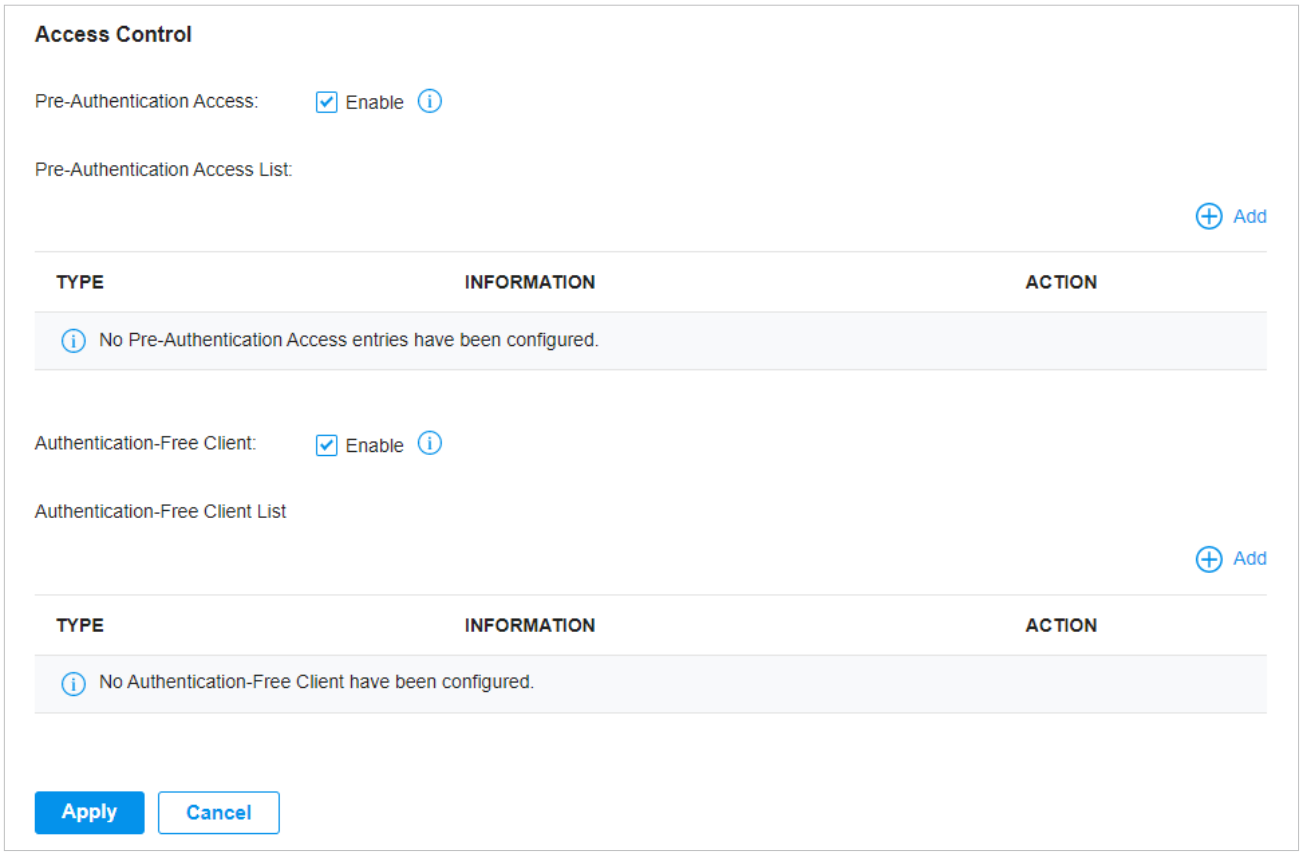
Tip	Selectați tipul paginii Portal. Editați pagina curentă:Editați parametrii aferenți pentru a personaliza pagina Portal pe baza paginii furnizate. Importă pagină personalizată:Faceți clic Import pentru a importa pagina dvs. unică de portal pentru branding pe el conform companiei dvs.
Limba implicita	Selectați limba implicită afișată pe pagina Portal. Controlerul ajustează automat limba afișată pe pagina Portal în funcție de limba sistemului a clienților. Dacă limba nu este acceptată, controlerul va folosi limba implicită specificată aici.
fundal	Selectați tipul de fundal. Culoare solida:Configurați culoarea de fundal dorită introducând manual codul de culoare HTML hexazecimal sau prin selectorul de culori. Imagine:Clic Choose și selectați o imagine de pe computer ca fundal.
Siglă	Faceți clic pentru a afișa sigla pe pagina portalului.
Imagine cu logo	Clic Choose și selectați o imagine de pe computer ca logo.
Dimensiunea logo-ului	Ajustați dimensiunea logo-ului pe pagina portalului.
Poziția logo-ului	Ajustați poziția siglei pe pagina portalului.
Culoarea butonului	Configurați culoarea de fundal dorită pentru buton introducând manual codul de culoare HTML hexazecimal sau prin selectorul de culori.
Culoarea textului butonului	Configurați culoarea textului dorită pentru buton introducând manual codul de culoare HTML hexazecimal sau prin selectorul de culori.
Poziția butonului	Selectați poziția butonului pe pagina portalului.
Buton Text	Introduceți textul pentru buton.
Informații de bun venit	Faceți clic pe caseta de selectare și introduceți text ca informații de bun venit. Puteți specifica dimensiunea dorită a fontului textului și puteți configura culoarea textului introducând manual codul de culoare HTML hexazecimal sau prin selectorul de culori.
Termenii serviciului	Faceți clic pe caseta de selectare și introduceți text ca termeni și condiții în caseta următoare. Clic Adăugați termenipentru a introduce numele și contextul termenilor care vor apărea după ce un client face clic pe linkul din Termenii și condițiile.
Drepturi de autor	Faceți clic pe caseta de selectare și introduceți text ca drepturi de autor în caseta următoare. Puteți specifica dimensiunea dorită a fontului textului și puteți configura culoarea textului introducând manual codul de culoare HTML hexazecimal sau prin selectorul de culori.
Afișați redirecționarea Numărătoarea inversă După Autorizat	Când este activat, sistemul va afișa numărătoarea inversă de redirecționare a portalului.

Faceți clic pe Opțiuni de publicitate și cpersonalizați imaginile publicitare pe pagina de autentificare.



Publicitate	Faceți clic pe caseta de selectare pentru a activa funcția Publicitate. Cu această funcție activată, puteți adăuga imagini publicitare pe pagina de autentificare. Aceste imagini publicitare vor fi afișate înainte ca pagina de conectare să apară.
Resursa de imagine	Clic Choose și selectați imagini de pe computer ca imagini publicitare. Când sunt adăugate mai multe imagini, acestea vor fi redate în buclă.
Durata reclamei Timp	Introduceți durata pentru imaginile publicitare. Pe această perioadă, imaginile vor fi redate în buclă. Dacă durata de timp nu este suficientă pentru toate imaginile, restul nu vor fi afișate.
Carusel de imagini Interval	Introduceți intervalul carusel de imagini. De exemplu, dacă această valoare este setată la 5 secunde, prima imagine va fi afișată timp de 5 secunde, urmată de a doua imagine timp de 5 secunde și așa mai departe.
Permiteți utilizatorilor să omite reclamele	Faceți clic pe caseta de selectare pentru a permite utilizatorilor să omite reclamele.

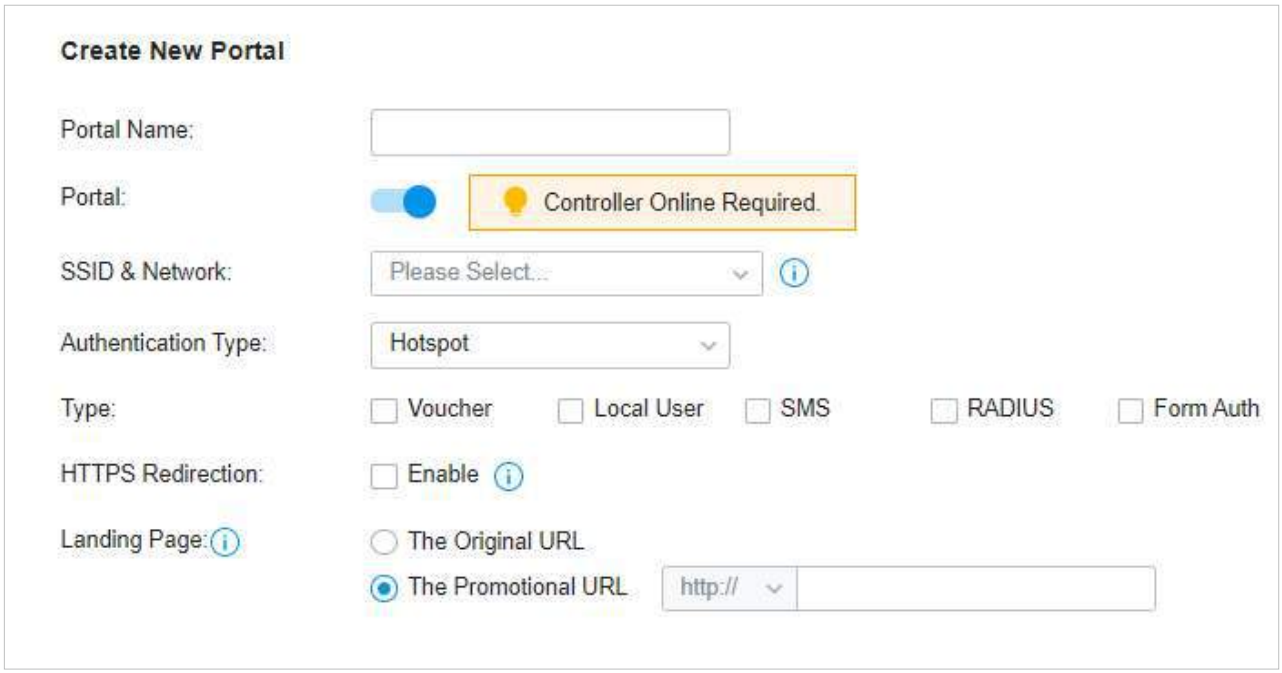
4. (Opțional) Configurați regulile de control al accesului, inclusiv Accesul pre-autentificare și Clientul fără autentificare, dacă este necesar. Mergi laSetări>Autentificare>Portal. În fila Control acces, faceți clic pe caseta de selectare pentru a activa Accesul de pre-autentificare și pentru a seta Clientul fără autentificare.



Preautentificare Acces	Faceți clic pe caseta de selectare pentru a activa Accesul de pre-autentificare. Cu această caracteristică activată, clienților neautentificați li se permite să acceseze subrețelele și resursele web specificate în Lista de acces pre-autentificare de mai jos.
Preautentificare Lista de acces	Clic Add pentru a configura intervalul IP sau adresa URL care sunt clienții neautentificați permis accesul.
Fără autentificare Client	Faceți clic pe caseta de selectare pentru a activa Clientul fără autentificare. Cu această caracteristică activată, puteți permite anumitor clienți să acceseze internetul fără autentificarea portalului.
Fără autentificare Lista de clienti	Clic Add și introduceți adresa IP sau adresa MAC a clienților fără autentificare.

■ Configurarea portalului cu Hotspot

1. Selectați un site din lista derulantă aOrganizare. Mergi laSetări>Autentificare>Portal. În fila Portal, faceți clic + Create New Portal pentru a crea o nouă intrare în portal. Apoi faceți clic pentru a activa Portal și încărcați pagina următoare.



2. Selectați SSID-urile și rețelele LAN pentru ca portalul să aibă efect și să configurați parametrii de bază.

SSID și rețea	Selectați unul sau mai multe SSID-uri sau rețele LAN pentru portal. Clienții conectați la SSID-urile sau rețelele LAN selectate trebuie să se conecteze la o pagină web pentru a stabili verificarea înainte de a accesa rețeaua.
tip de autentificare	Selectați tipul de autentificare Portal ca Hotspot.
Tip	Selectați unul sau mai multe tipuri de autentificare în funcție de nevoile dvs. Clienții pot accesa rețeaua după ce au trecut orice tip de autentificare.
Redirecționare HTTPS	Faceți clic pe caseta de selectare pentru a activa redirecționarea HTTPS. Cu această caracteristică activată, clienții neautorizați vor fi redirecționați către pagina Portal atunci când încearcă să răsfoiască site-urile HTTPS. Cu această caracteristică dezactivată, clienții neautorizați nu pot naviga pe site-uri web HTTPS și nu sunt redirecționați către pagina Portal.
Pagina de destinație	Selectați la ce pagină va fi redirecționat clientul după o autentificare cu succes. Adresa URL originală:Clienții sunt direcționați către adresa URL pe care o solicită după ce trec autentificarea portalului. Adresa URL promoțională:Clienții sunt direcționați către adresa URL specificată după ce trec autentificarea Portal.

3. Cu diferite tipuri de Hotspot selectate, configurați parametrii aferenti.

- Configurarea portalului de voucher

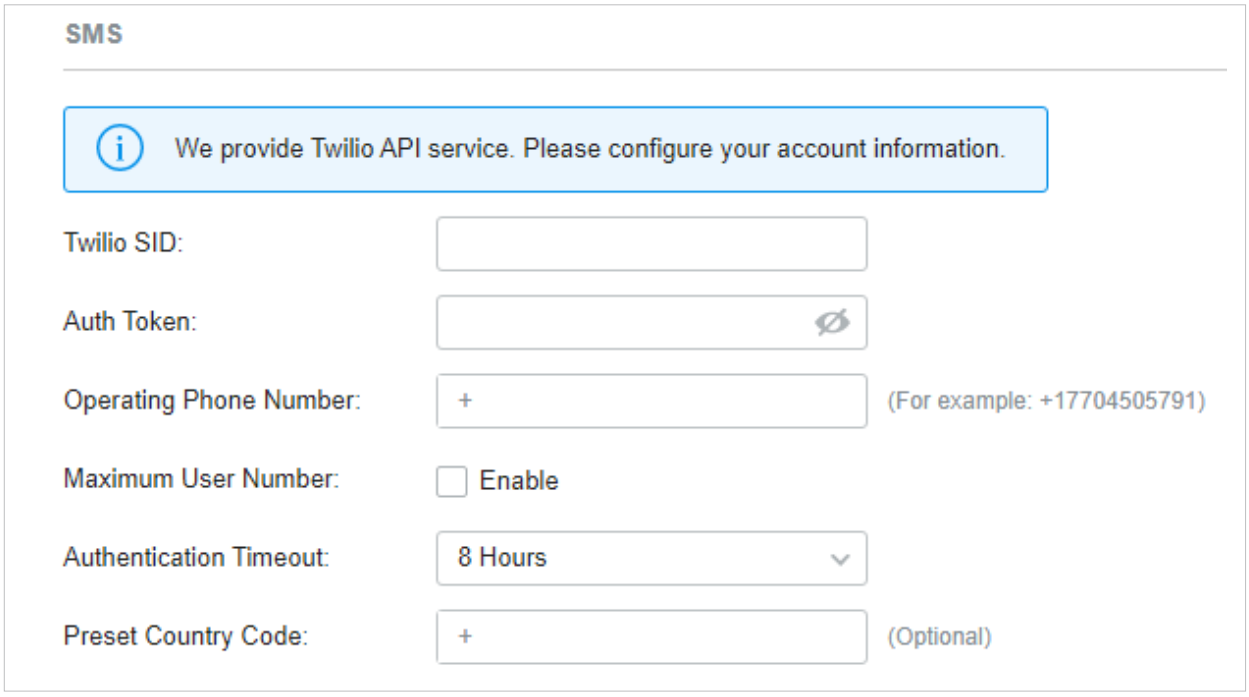
Bon	Selectați Voucher și faceți clic **Voucher Manager** pentru a gestiona codurile voucher. A se referi la6. 2. 3 Vouchere pentru informații detaliate despre cum să creați vouchere.

- Configurarea portalului local

Utilizator local	Selectați Utilizator local și faceți clic pe **User Management** pentru a gestiona informațiile din conturi de conectare. A se referi la6. 2. 4 Utilizatori locali pentru informații detaliate despre cum să creați utilizatori locali.

- Configurarea portalului SMS

Selectați SMS și configurați parametrii necesari în secțiunea SMS.

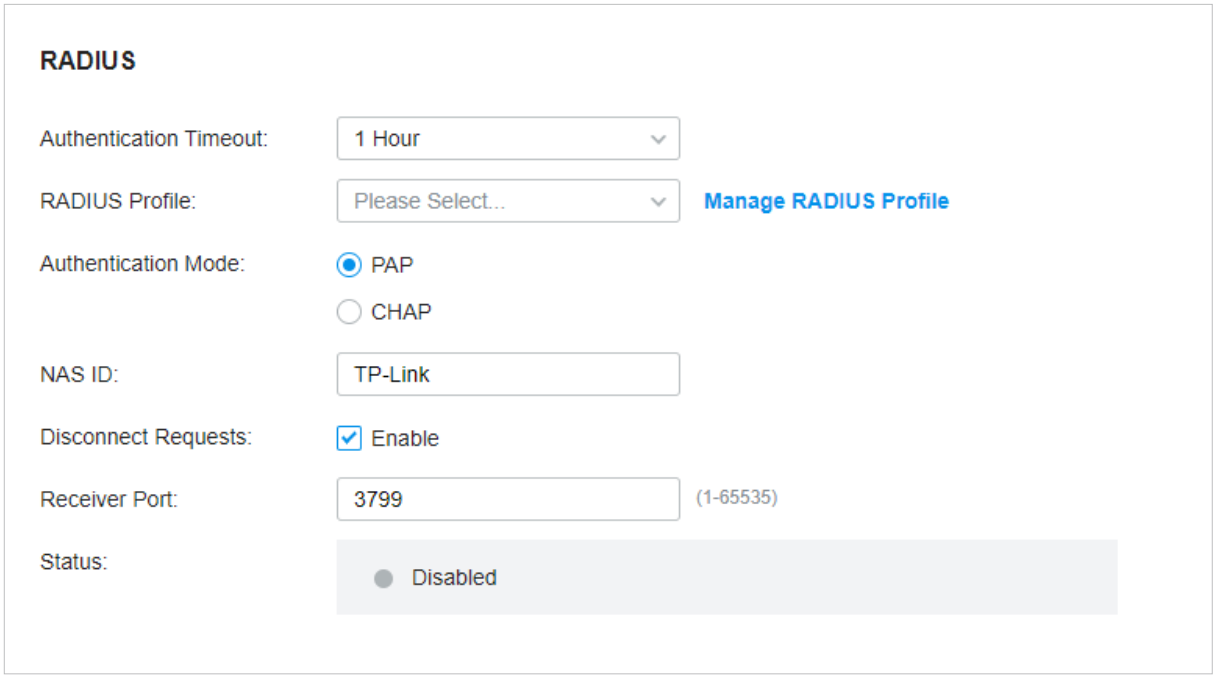


SMS	Clienții pot obține coduri de verificare folosind telefoanele lor mobile și pot introduce codurile primite pentru a trece autentificarea.
Twilio SID	Introduceți SID-ul contului pentru acreditările API Twilio.
Jeton de autentificare	Introduceți simbolul de autentificare pentru acreditările API Twilio.
Telefon de operare Număr	Introduceți numărul de telefon care este utilizat pentru a trimite mesaje de verificare clienților.
Utilizator maxim Numerele	Faceți clic pe caseta de selectare și introduceți numărul maxim de utilizatori care pot fi autentificați folosind același număr de telefon în același timp.

Timeout autentificare	Selectați durata de conectare. Clientul trebuie să se conecteze din nou pe pagina de autentificare web pentru a accesa rețeaua.
Codul de țară prestabilit	Introduceți codul de țară implicit care va fi completat automat pe pagina de autentificare.

- Configurarea portalului RADIUS

Selectați RADIUS și configurați parametrii necesari în secțiunea RADIUS.



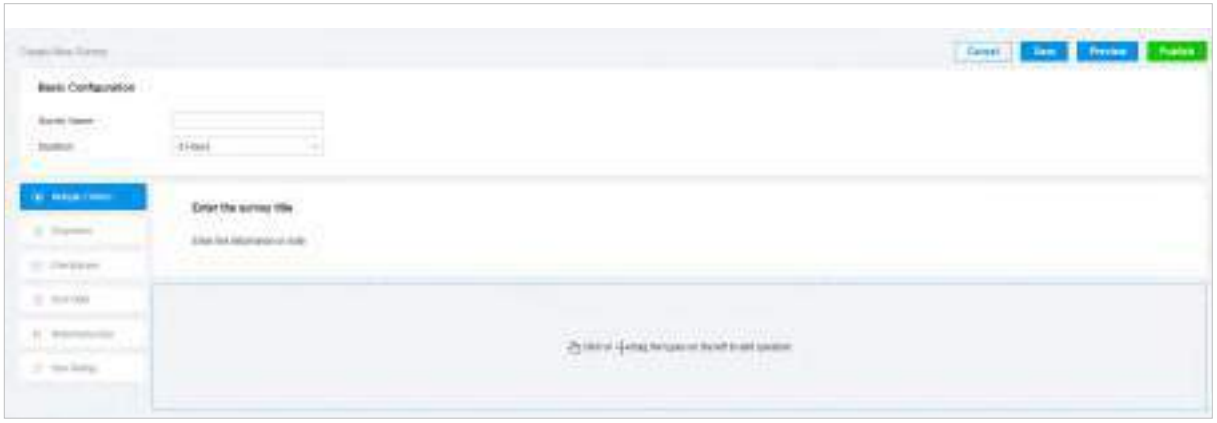
Timeout autentificare	Clienții trebuie să introducă numele de utilizator și parola corecte care sunt stocate pe serverul RADIUS pentru a trece autentificarea.
Profil RADIUS	Selectați profilul RADIUS pe care l-ați creat. Dacă nu au fost create profiluri RADIUS, faceți clic + Create New RADIUS Profile din lista derulantă sau Manage RADIUS Profile pentru a crea unul. Profilul RADIUS înregistrează informațiile al serverului RADIUS care oferă o metodă de stocare centrală a informațiilor de autentificare.
Modul de autentificare	Selectați protocolul de autentificare pentru serverul RADIUS. Sunt disponibile două protocoale de autentificare: PAP și CHAP.
ID NAS	Configurați un identificator de server de acces la rețea (ID NAS) pe portal. Pachetele de solicitare de autentificare de la controler la serverul RADIUS poartă ID-ul NAS. Serverul RADIUS poate clasifica utilizatorii în diferite grupuri pe baza ID-ului NAS și apoi poate alege politici diferite pentru diferite grupuri.
Cereri deconectate	Cu funcția activată, controlerul va asculta pe portul receptor solicitările de deconectare de la serverul RADIUS. Când controlerul primește cererile de deconectare în format corect, controlerul va încheia sesiunea de autentificare RADIUS a clienților. Rețineți că funcția este disponibilă numai atunci când controlerul este accesibil serverului RADIUS.

Port receptor	Specificați portul pe care ascultă controlerul atunci când există solicitări de deconectare de la serverul RADIUS. Asigurați-vă că portul specificat nu este în uz.
stare	Intrarea afișează starea portului receptor, inclusiv Running, Disabled și Error. Rularea înseamnă că portul este disponibil, Disabled înseamnă că portul este închis și Eroare înseamnă că portul este deja în uz.

- Configurarea autentificării formularelor

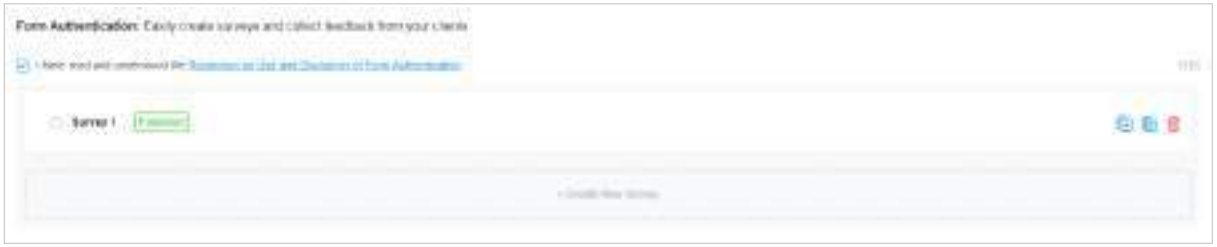
  Selectați Form Auth și faceți clic+ Creați un sondaj nouîn secțiunea Autentificare formular. Apoi urmați instrucțiunile de pe ecran pentru a crea un sondaj adăugând tipul și numărul de întrebări de care aveți nevoie. Puteți da clicprevizualizarepentru a vedea cum arată sondajul pe site-ul web și pe telefon.

  ClicPublicaiar apoi sondajul creat poate fi folosit pentru autentificarea formularelor. Un sondaj nu poate fi editat după ce este publicat.



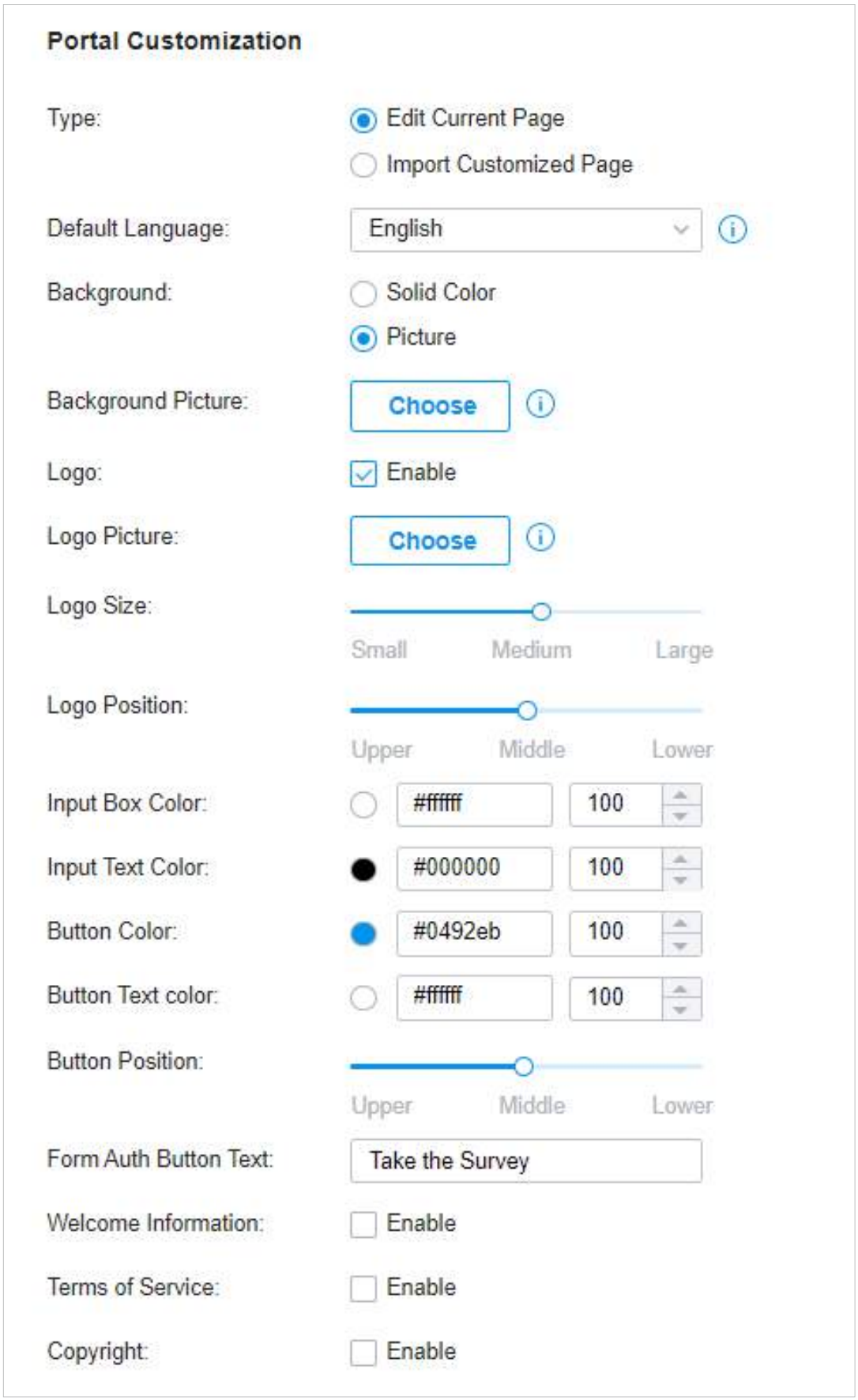
Numele sondajului	Specificați un nume pentru sondaj pentru identificare.
Durată	Specificați cât timp pot folosi clienții rețeaua după ce trec autentificarea prin formular.

Sondajele create vor fi afișate pentru ca dvs. să le alegeți pentru autentificarea formularului.



	Faceți clic pentru a copia sondajul.
	Faceți clic pentru a vizualiza sondajul creat.
	Faceți clic pentru a șterge sondajul..

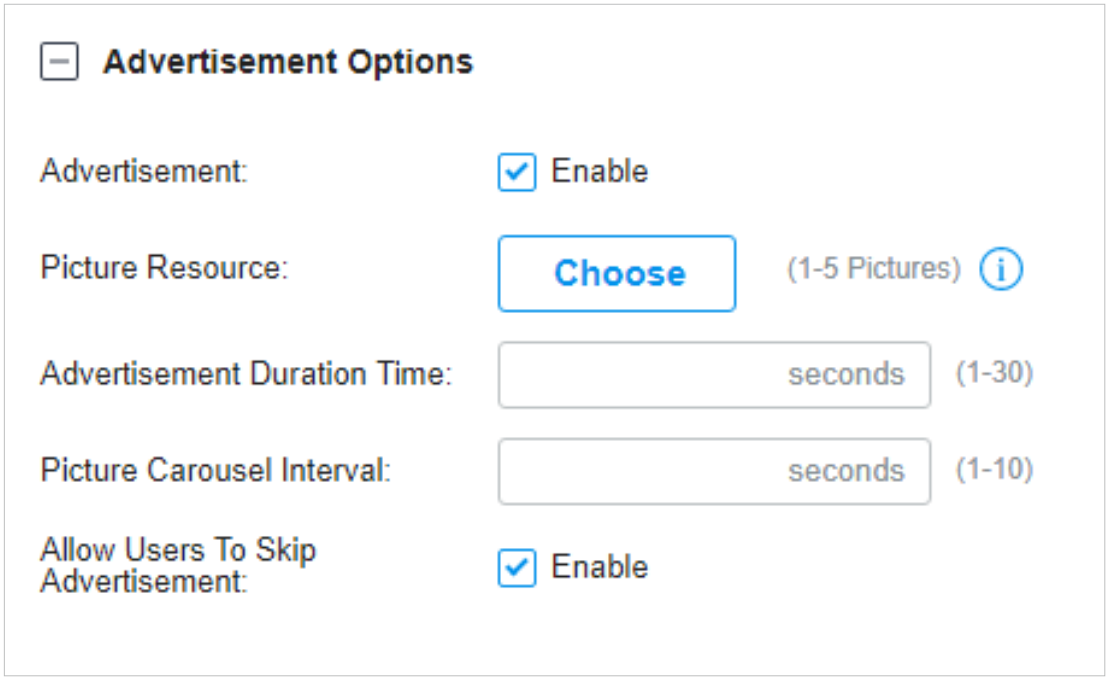
4. În secțiunea Personalizare portal, personalizați pagina Portal, inclusiv imaginea de fundal, imaginea siglei și așa mai departe.



Tip	Selectați tipul paginii Portal. Editați pagina curentă:Editați parametrii aferenți pentru a personaliza pagina Portal pe baza paginii furnizate. Importă pagină personalizată:Faceți clic Import pentru a importa pagina dvs. unică de portal pentru branding pe el conform companiei dvs.
Limba implicita	Selectați limba implicită afișată pe pagina Portal. Controlerul ajustează automat limba afișată pe pagina Portal în funcție de limba sistemului a clienților. Dacă limba nu este acceptată, controlerul va folosi limba implicită specificată aici.
fundal	Selectați tipul de fundal. Culoare solida:Configurați culoarea de fundal dorită introducând manual codul de culoare HTML hexazecimal sau prin selectorul de culori. Imagine:Clic Choose și selectați o imagine de pe computer ca fundal.
Siglă	Faceți clic pentru a afișa sigla pe pagina portalului.
Imagine cu logo	Clic Choose și selectați o imagine de pe computer ca logo.
Dimensiunea logo-ului	Ajustați dimensiunea logo-ului pe pagina portalului.
Poziția logo-ului	Ajustați poziția siglei pe pagina portalului.
Culoarea casetei de intrare	Configurați culoarea de fundal dorită pentru caseta de intrare introducând manual codul de culoare HTML hexazecimal sau prin selectorul de culori.
Introduceți culoarea textului	Configurați culoarea textului dorită pentru caseta de introducere introducând manual codul de culoare HTML hexazecimal sau prin selectorul de culori.
Culoarea butonului	Configurați culoarea de fundal dorită pentru buton introducând manual codul de culoare HTML hexazecimal sau prin selectorul de culori.
Culoarea textului butonului	Configurați culoarea textului dorită pentru buton introducând manual codul de culoare HTML hexazecimal sau prin selectorul de culori.
Poziția butonului	Selectați poziția butonului pe pagina portalului.
Buton Text	Introduceți textul pentru buton.
Informații de bun venit	Faceți clic pe caseta de selectare și introduceți text ca informații de bun venit. Puteți specifica dimensiunea dorită a fontului textului și puteți configura culoarea textului introducând manual codul de culoare HTML hexazecimal sau prin selectorul de culori.
Termenii serviciului	Faceți clic pe caseta de selectare și introduceți text ca termeni și condiții în caseta următoare. Clic Adăugați termenipentru a introduce numele și contextul termenilor care vor apărea după ce un client face clic pe linkul din Termenii și condițiile.

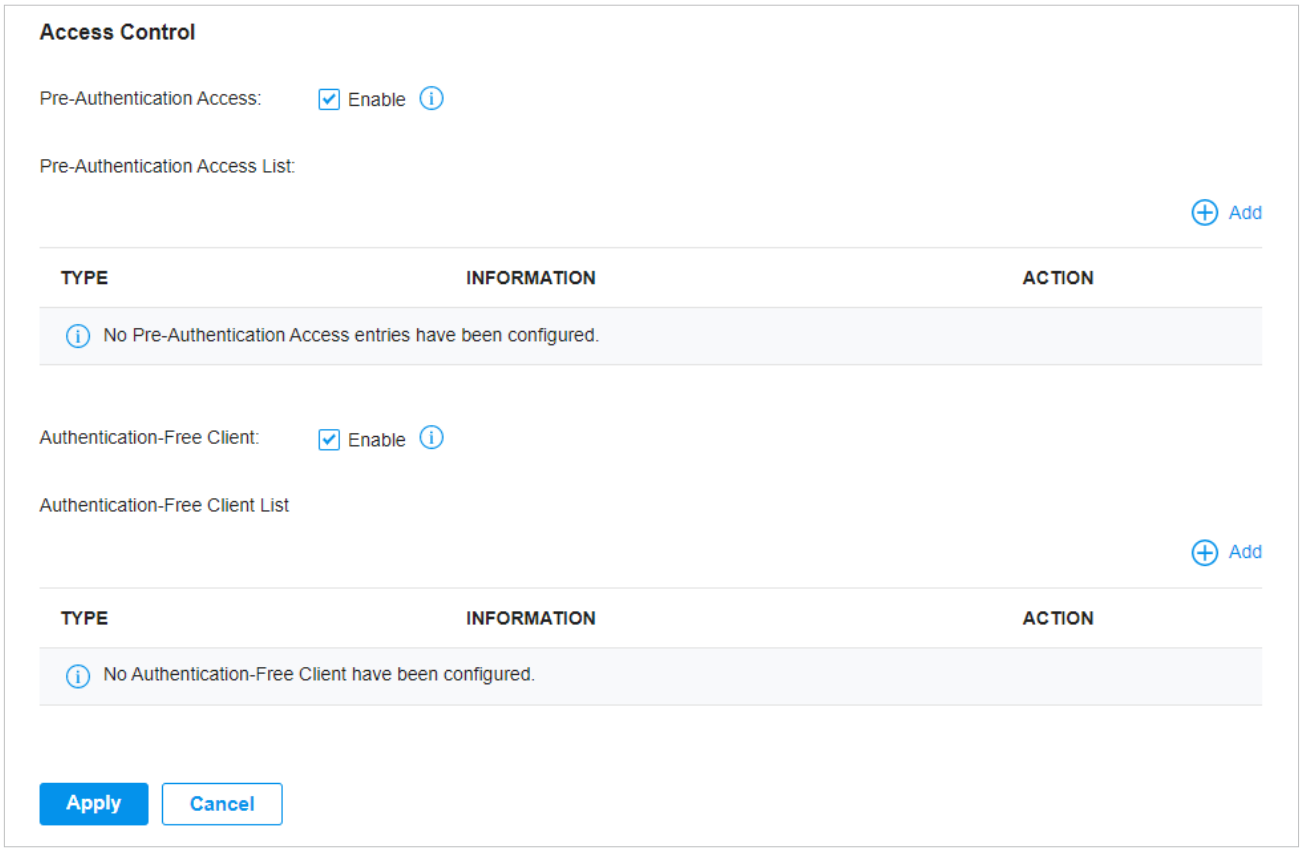
Drepturi de autor	Faceți clic pe caseta de selectare și introduceți text ca drepturi de autor în caseta următoare. Puteți specifica dimensiunea dorită a fontului textului și puteți configura culoarea textului introducând manual codul de culoare HTML hexazecimal sau prin selectorul de culori.
Afișați redirecționarea Numărătoarea inversă După Autorizat	Când este activat, sistemul va afișa numărătoarea inversă de redirecționare a portalului

Faceți clic pe Opțiuni de publicitate și personalizați imaginile publicitare pe pagina de autentificare.



Publicitate	Faceți clic pe caseta de selectare pentru a activa funcția Publicitate. Cu această funcție activată, puteți adăuga imagini publicitare pe pagina de autentificare. Aceste imagini publicitare vor fi afișate înainte ca pagina de conectare să apară.
Resursa de imagine	Clic Choose și selectați imagini de pe computer ca imagini publicitare. Când sunt adăugate mai multe imagini, acestea vor fi redate în buclă.
Durata reclamei Timp	Introduceți durata pentru imaginile publicitare. Pe această perioadă, imaginile vor fi redate în buclă. Dacă durata de timp nu este suficientă pentru toate imaginile, restul nu vor fi afișate.
Carusel de imagini Interval	Introduceți intervalul carusel de imagini. De exemplu, dacă această valoare este setată la 5 secunde, prima imagine va fi afișată timp de 5 secunde, urmată de a doua imagine timp de 5 secunde și așa mai departe.
Permiteți utilizatorilor să omite reclamele	Faceți clic pe caseta de selectare pentru a permite utilizatorilor să omite reclamele.

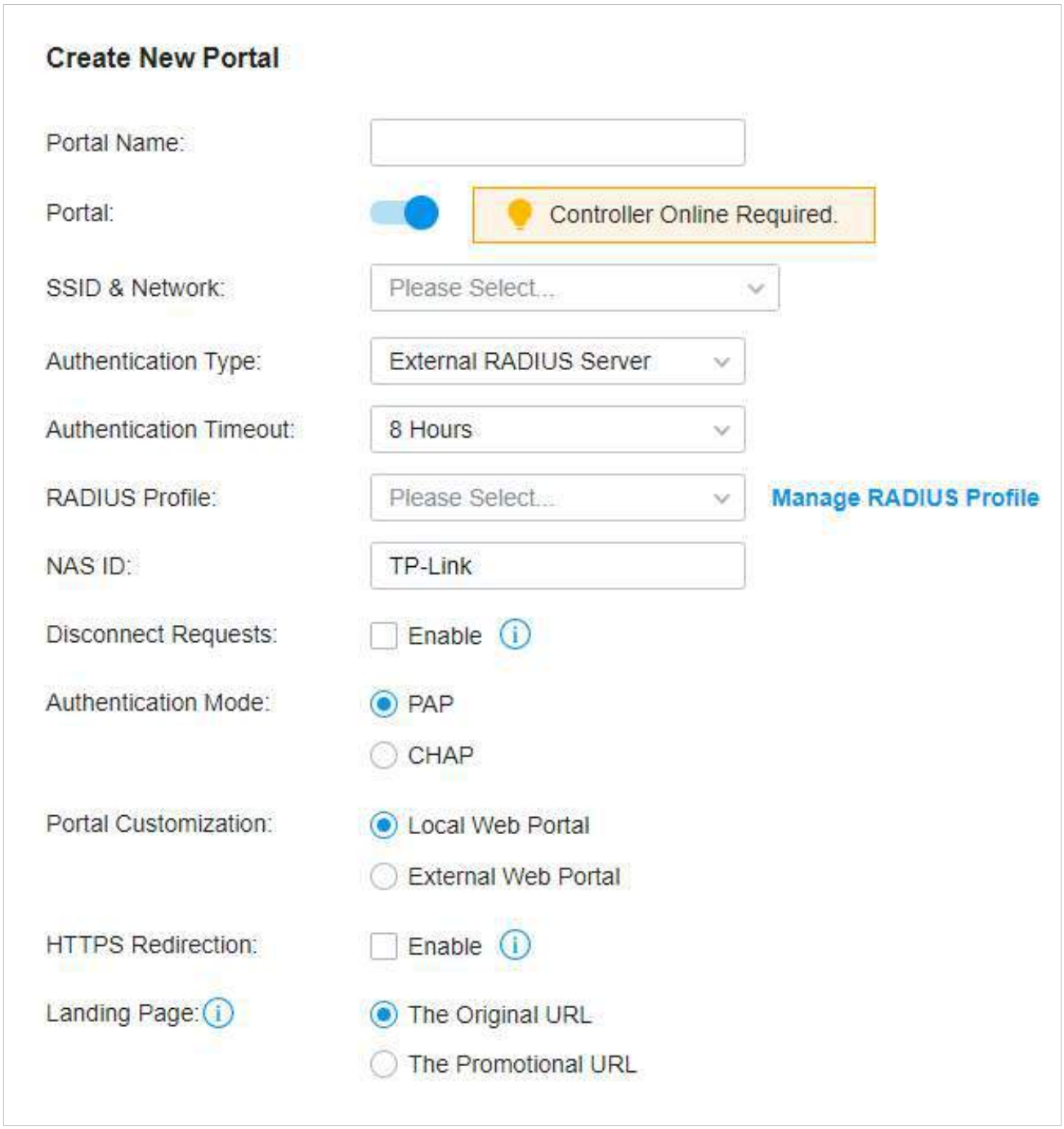
5. (Opțional) Configurați regulile de control al accesului, inclusiv Accesul pre-autentificare și Clientul fără autentificare, dacă este necesar. Mergi laSetări>Autentificare>Portal. În fila Control acces, faceți clic pe caseta de selectare pentru a activa Accesul de pre-autentificare și pentru a seta Clientul fără autentificare.



Preautentificare Acces	Faceți clic pe caseta de selectare pentru a activa Accesul de pre-autentificare. Cu această caracteristică activată, clienților neautentificați li se permite să acceseze subrețelele și resursele web specificate în Lista de acces pre-autentificare de mai jos.
Preautentificare Lista de acces	Clic Add pentru a configura intervalul IP sau adresa URL care sunt clienții neautentificați permis accesul.
Fără autentificare Client	Faceți clic pe caseta de selectare pentru a activa Clientul fără autentificare. Cu această caracteristică activată, puteți permite anumitor clienți să acceseze internetul fără autentificarea portalului.
Fără autentificare Lista de clienti	Clic Add și introduceți adresa IP sau adresa MAC a clienților fără autentificare.

■ Configurarea portalului cu server RADIUS extern

1. Selectați un site din lista derulantă aOrganizare. Mergi laSetări>Autentificare>Portal. Clic pentru a activa Portal și a încărca următoarea pagină.

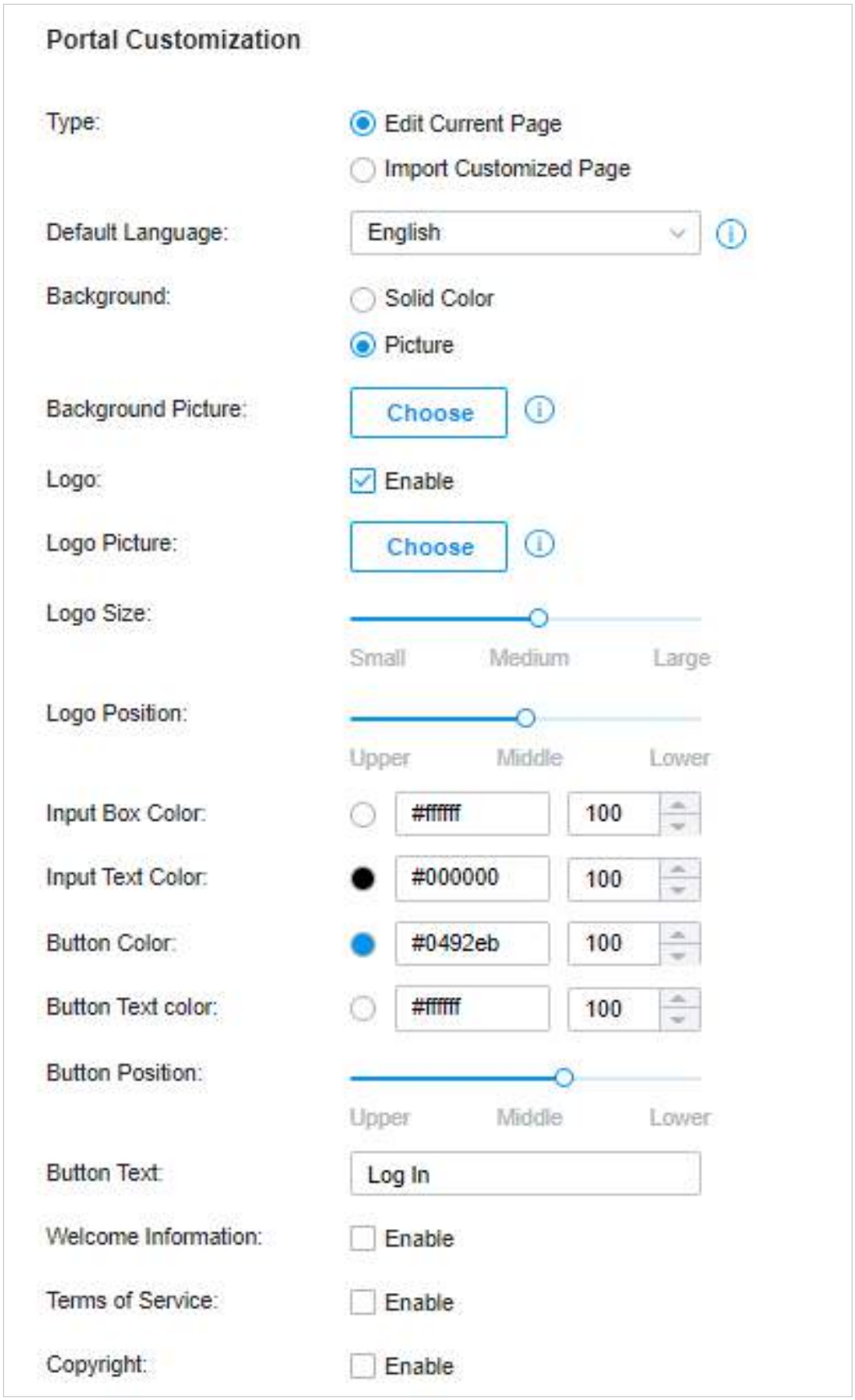


2. Selectați SSID-urile și rețelele LAN pentru care portalul să aibă efect și configurați parametrii de bază, inclusiv tipul de autentificare, expirarea timpului de autentificare și așa mai departe.

SSID și rețea	Selectați unul sau mai multe SSID-uri sau rețele LAN pentru portal. Clienții conectați la SSID-urile sau rețelele LAN selectate trebuie să se conecteze la o pagină web pentru a stabili verificarea înainte de a accesa rețeaua.
tip de autentificare	Selectați tipul de autentificare Portal ca server RADIUS extern.

Timeout autentificare	Selectați durata de conectare. Clienții vor fi offline după expirarea timpului de autentificare.
Profil RADIUS	Selectați profilul RADIUS pe care l-ați creat. Dacă nu au fost create profiluri RADIUS, clic + Create New RADIUS Profile din lista derulantă sau Manage RADIUS Profile pentru a crea unul. Profilul RADIUS înregistrează informații despre serverul RADIUS inclusiv adresa IP, portul și așa mai departe.
ID NAS	Configurați un identificator de server de acces la rețea (ID NAS) pe portal. Pachetele de solicitare de autentificare de la controler la serverul RADIUS poartă ID-ul NAS. Serverul RADIUS poate clasifica utilizatorii în diferite grupuri pe baza ID-ului NAS și apoi poate alege politici diferite pentru diferite grupuri.
Cereri deconectate	Cu funcția activată, controlerul va asculta pe portul receptor solicitările de deconectare de la serverul RADIUS. Când controlerul primește cererile de deconectare în format corect, controlerul va încheia sesiunea de autentificare RAIDIUS a clienților. Rețineți că funcția este disponibilă numai atunci când controlerul este accesibil serverului RADIUS.
Port receptor	Specificați portul pe care ascultă controlerul atunci când există solicitări de deconectare de la serverul RADIUS. Asigurați-vă că portul specificat nu este în uz.
stare	Intrarea afișează starea portului receptor, inclusiv Running, Disabled și Error. Rularea înseamnă că portul este disponibil, Disabled înseamnă că portul este închis și Eroare înseamnă că portul este deja în uz.
Modul de autentificare	Selectați protocolul de autentificare pentru serverul RADIUS.
Personalizare portal	Selectați Portal web local sau Portal web extern. Pagina de autentificare a portalului web local este furnizată de serverul de portal încorporat al controlerului. Portalul web extern este furnizat de un server de portal extern. Introduceți adresa URL a paginii de conectare de autentificare furnizată de serverul portalului extern în câmpul URL extern al portalului web.
Redirecționare HTTPS	Faceți clic pe caseta de selectare pentru a activa redirecționarea HTTPS. Cu această caracteristică activată, clienții neautorizați vor fi redirecționați către pagina Portal atunci când încearcă să răsfoiască site-urile HTTPS. Cu această caracteristică dezactivată, clienții neautorizați nu pot naviga pe site-uri web HTTPS și nu sunt redirecționați către pagina Portal.
Pagina de destinație	Selectați la ce pagină va fi redirecționat clientul după o autentificare cu succes. Adresa URL originală:Clienții sunt direcționați către adresa URL pe care o solicită după ce trec autentificarea portalului. Adresa URL promoțională:Clienții sunt direcționați către adresa URL specificată aici după ce trec autentificarea portalului.

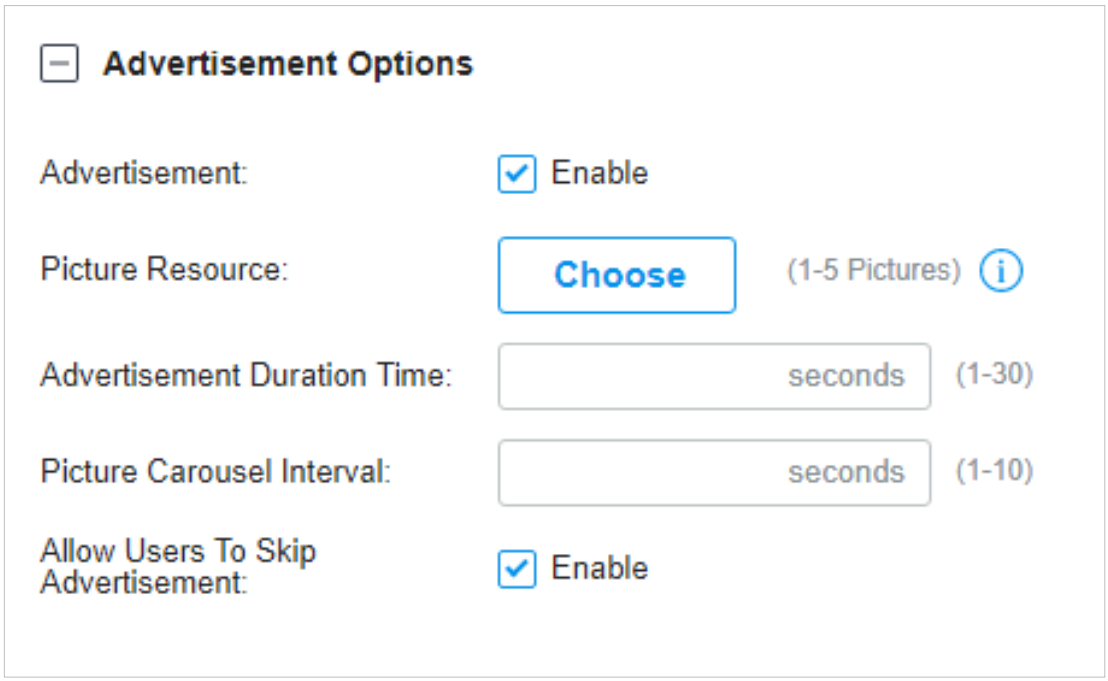
3. Dacă alegeți Local Web Portal, care este furnizat de serverul de portal încorporat al controlerului, personalizați pagina Portal în secțiunea Personalizare portal, inclusiv imaginea de fundal, imaginea siglei și așa mai departe.



Tip	Selectați tipul paginii Portal. Editați pagina curentă:Editați parametrii aferenți pentru a personaliza pagina Portal pe baza paginii furnizate. Importă pagină personalizată:Faceți clic Import pentru a importa pagina dvs. unică de portal pentru branding pe el conform companiei dvs.
Limba implicita	Selectați limba implicită afișată pe pagina Portal. Controlerul ajustează automat limba afișată pe pagina Portal în funcție de limba sistemului a clienților. Dacă limba nu este acceptată, controlerul va folosi limba implicită specificată aici.
fundal	Selectați tipul de fundal. Culoare solida:Configurați culoarea de fundal dorită introducând manual codul de culoare HTML hexazecimal sau prin selectorul de culori. Imagine:Clic Choose și selectați o imagine de pe computer ca fundal.
Siglă	Faceți clic pentru a afișa sigla pe pagina portalului.
Imagine cu logo	Clic Choose și selectați o imagine de pe computer ca logo.
Dimensiunea logo-ului	Ajustați dimensiunea logo-ului pe pagina portalului.
Poziția logo-ului	Ajustați poziția siglei pe pagina portalului.
Culoarea casetei de intrare	Configurați culoarea de fundal dorită pentru caseta de intrare introducând manual codul de culoare HTML hexazecimal sau prin selectorul de culori.
Introduceți culoarea textului	Configurați culoarea textului dorită pentru caseta de introducere introducând manual codul de culoare HTML hexazecimal sau prin selectorul de culori.
Culoarea butonului	Configurați culoarea de fundal dorită pentru buton introducând manual codul de culoare HTML hexazecimal sau prin selectorul de culori.
Culoarea textului butonului	Configurați culoarea textului dorită pentru buton introducând manual codul de culoare HTML hexazecimal sau prin selectorul de culori.
Poziția butonului	Selectați poziția butonului pe pagina portalului.
Buton Text	Introduceți textul pentru buton.
Informații de bun venit	Faceți clic pe caseta de selectare și introduceți text ca informații de bun venit. Puteți specifica dimensiunea dorită a fontului textului și puteți configura culoarea textului introducând manual codul de culoare HTML hexazecimal sau prin selectorul de culori.
Termenii serviciului	Faceți clic pe caseta de selectare și introduceți text ca termeni și condiții în caseta următoare. Clic Adăugați termenipentru a introduce numele și contextul termenilor care vor apărea după ce un client face clic pe linkul din Termenii și condițiile.

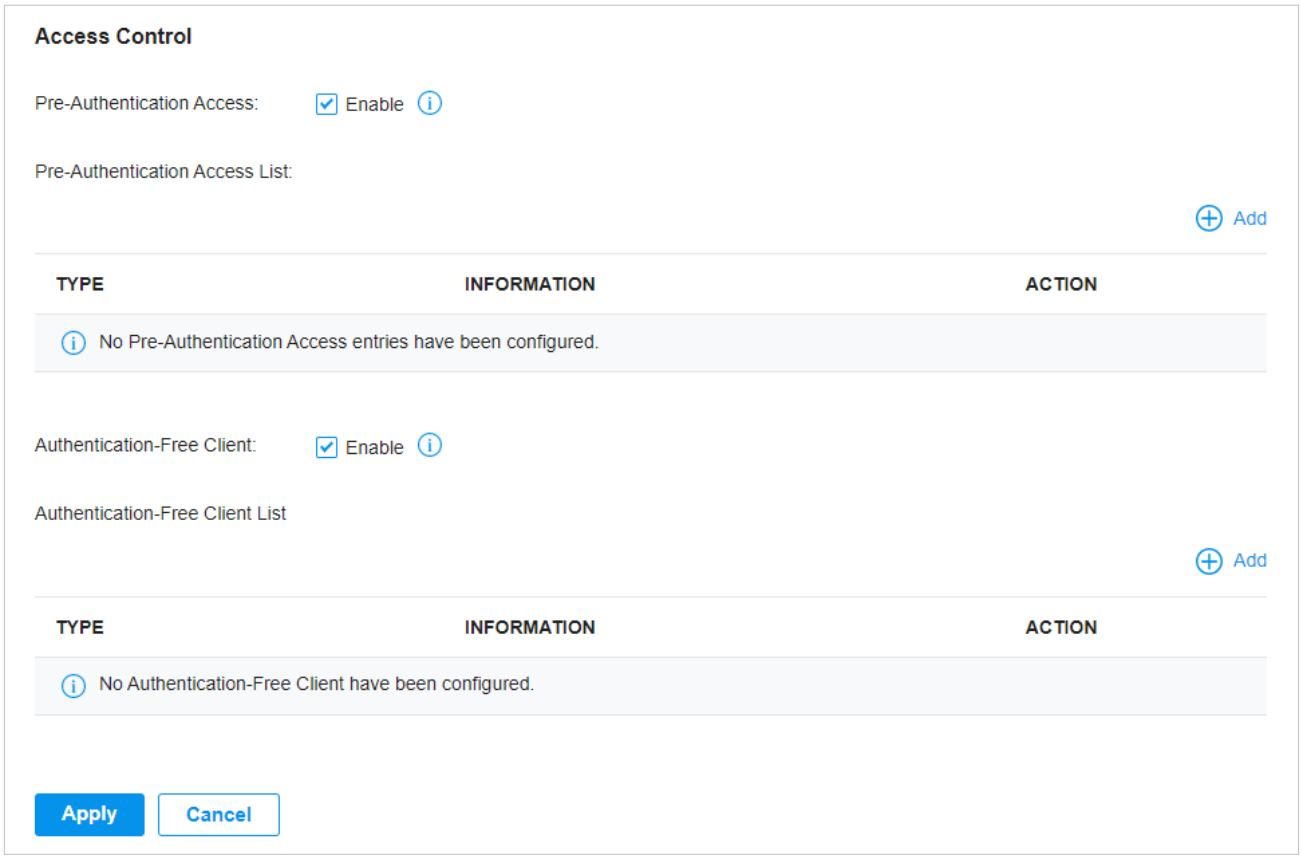
Drepturi de autor	Faceți clic pe caseta de selectare și introduceți text ca drepturi de autor în caseta următoare. Puteți specifica dimensiunea dorită a fontului textului și puteți configura culoarea textului introducând manual codul de culoare HTML hexazecimal sau prin selectorul de culori.
Afișați redirecționarea Numărătoarea inversă După Autorizat	Când este activat, sistemul va afișa numărătoarea inversă de redirecționare a portalului.

Faceți clic pe Opțiuni de publicitate și personalizați imaginile publicitare pe pagina de autentificare.



Publicitate	Faceți clic pe caseta de selectare pentru a activa funcția Publicitate. Cu această funcție activată, puteți adăuga imagini publicitare pe pagina de autentificare. Aceste imagini publicitare vor fi afișate înainte ca pagina de conectare să apară.
Resursa de imagine	Clic Choose și selectați imagini de pe computer ca imagini publicitare. Când sunt adăugate mai multe imagini, acestea vor fi redate în buclă.
Durata reclamei Timp	Introduceți durata pentru imaginile publicitare. Pe această perioadă, imaginile vor fi redate în buclă. Dacă durata de timp nu este suficientă pentru toate imaginile, restul nu vor fi afișate.
Carusel de imagini Interval	Introduceți intervalul carusel de imagini. De exemplu, dacă această valoare este setată la 5 secunde, prima imagine va fi afișată timp de 5 secunde, urmată de a doua imagine timp de 5 secunde și așa mai departe.
Permiteți utilizatorilor să omite reclamele	Faceți clic pe caseta de selectare pentru a permite utilizatorilor să omite reclamele.

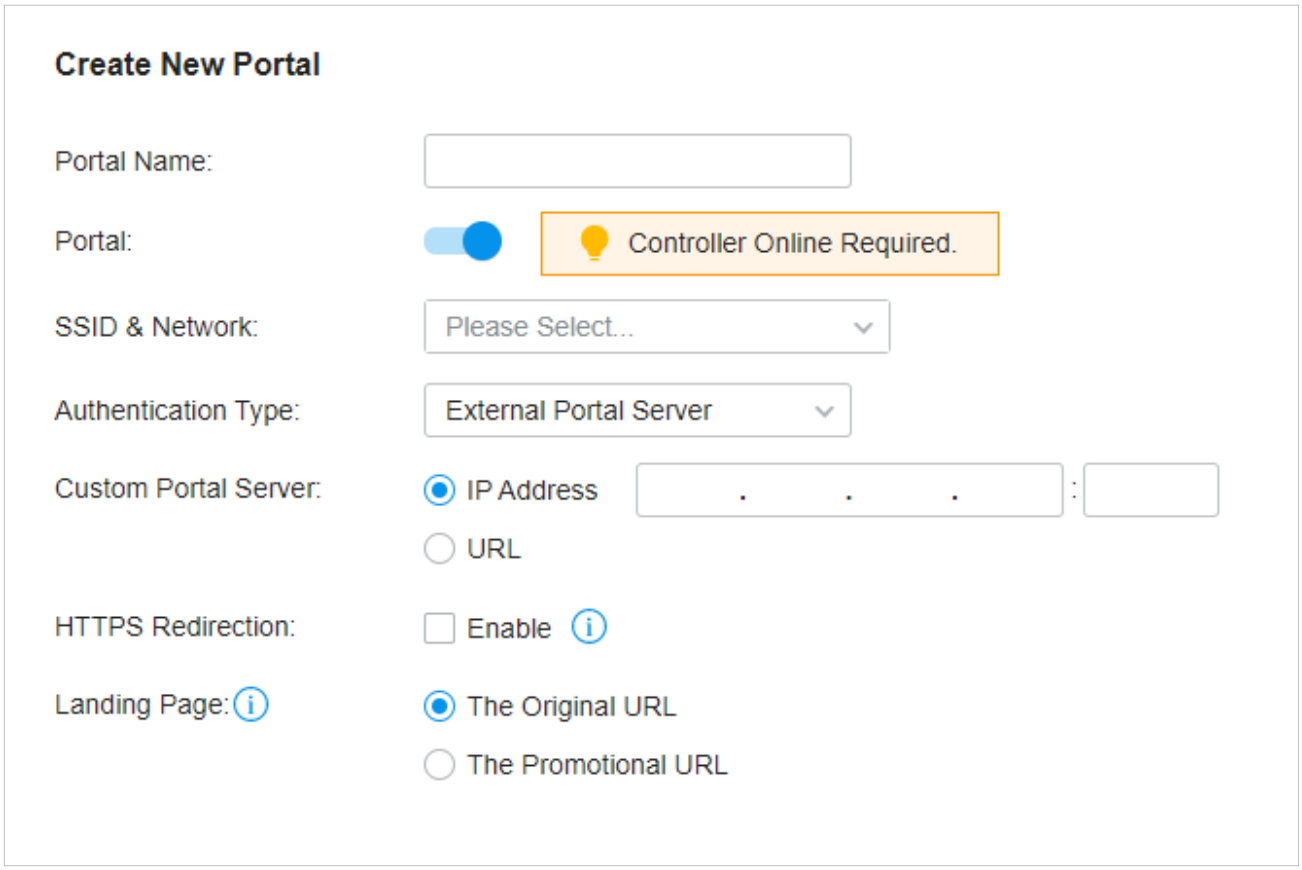
4. (Opțional) Configurați regulile de control al accesului, inclusiv Accesul pre-autentificare și Clientul fără autentificare, dacă este necesar. Mergi laSetări>Autentificare>Portal. În fila Control acces, faceți clic pe caseta de selectare pentru a activa Accesul de pre-autentificare și pentru a seta Clientul fără autentificare.



Preautentificare Acces	Faceți clic pe caseta de selectare pentru a activa Accesul de pre-autentificare. Cu această caracteristică activată, clienților neautentificați li se permite să acceseze subrețelele și resursele web specificate în Lista de acces pre-autentificare de mai jos.
Preautentificare Lista de acces	Clic Add pentru a configura intervalul IP sau adresa URL care sunt clienții neautentificați permis accesul.
Fără autentificare Client	Faceți clic pe caseta de selectare pentru a activa Clientul fără autentificare. Cu această caracteristică activată, puteți permite anumitor clienți să acceseze internetul fără autentificarea portalului.
Fără autentificare Lista de clienti	Clic Add și introduceți adresa IP sau adresa MAC a clienților fără autentificare.

■ Configurarea portalului cu serverul portal extern

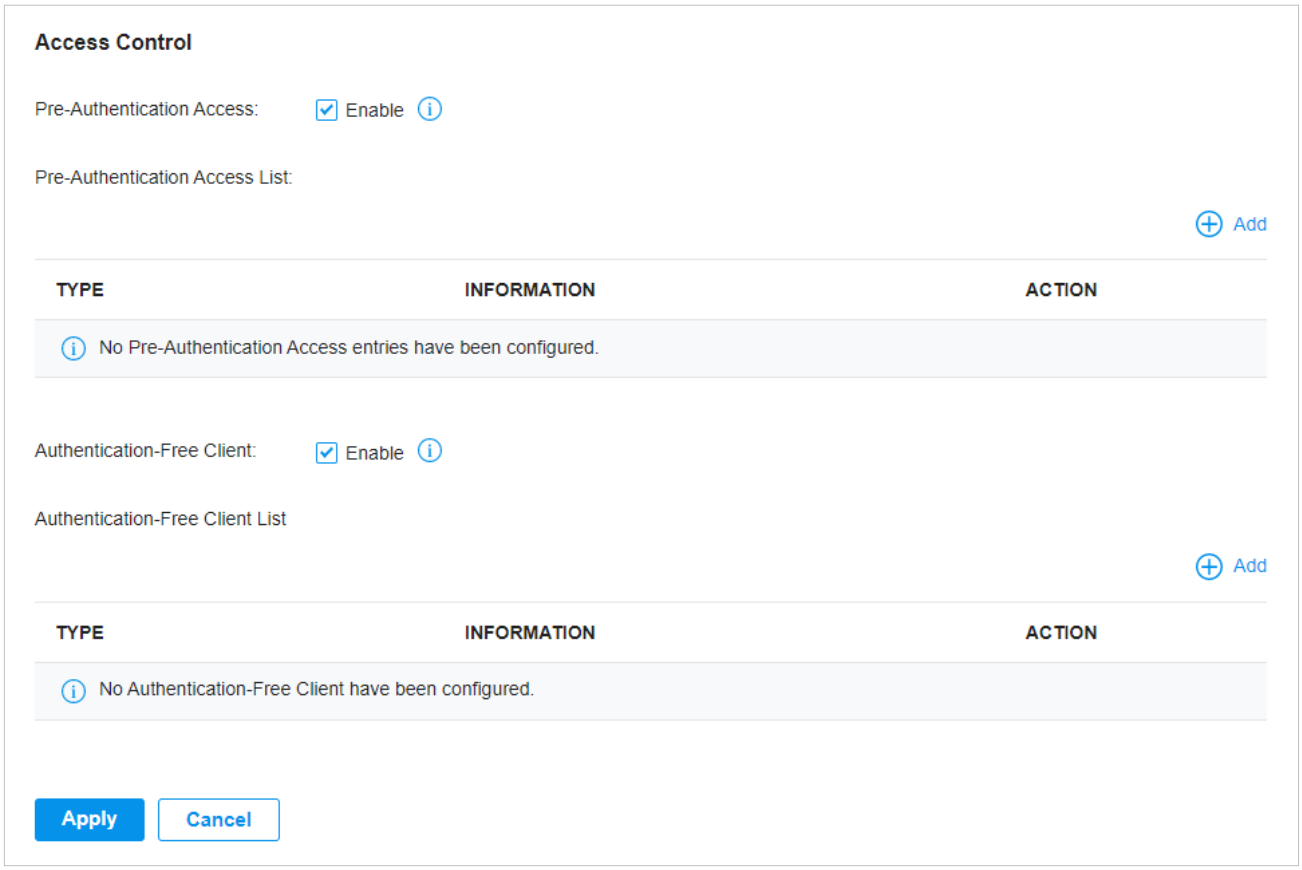
1. Selectați un site din lista derulantă aOrganizare. Mergi laSetări>Autentificare>Portal. În fila Portal, faceți clic + Create New Portal pentru a crea o nouă intrare în portal. Apoi faceți clic pentru a activa Portal și încărcați pagina următoare.



2. Selectați SSID-urile și rețelele LAN pentru care portalul să aibă efect și configurați parametrii de bază, inclusiv tipul de autentificare, serverul de portal personalizat și așa mai departe.

SSID și rețea	Selectați unul sau mai multe SSID-uri sau rețele LAN pentru portal. Clienții conectați la SSID-urile sau rețelele LAN selectate trebuie să se conecteze la o pagină web pentru a stabili verificarea înainte de a accesa rețeaua.
tip de autentificare	Selectați tipul de autentificare portal ca server de portal extern.
Server Portal personalizat	Specificați adresa IP sau adresa URL care redirecționează către un server de portal extern.
Redirecționare HTTPS	Faceți clic pe caseta de selectare pentru a activa redirecționarea HTTPS. Cu această caracteristică activată, clienții neautorizați vor fi redirecționați către pagina Portal atunci când încearcă să răsfoiască site-urile HTTPS. Cu această caracteristică dezactivată, clienții neautorizați nu pot naviga pe site-uri web HTTPS și nu sunt redirecționați către pagina Portal.
Pagina de destinație	Selectați la ce pagină va fi redirecționat clientul după o autentificare cu succes. Adresa URL originală:Clienții sunt direcționați către adresa URL pe care o solicită după ce trec autentificarea portalului. Adresa URL promoțională:Clienții sunt direcționați către adresa URL specificată aici după ce trec autentificarea portalului.

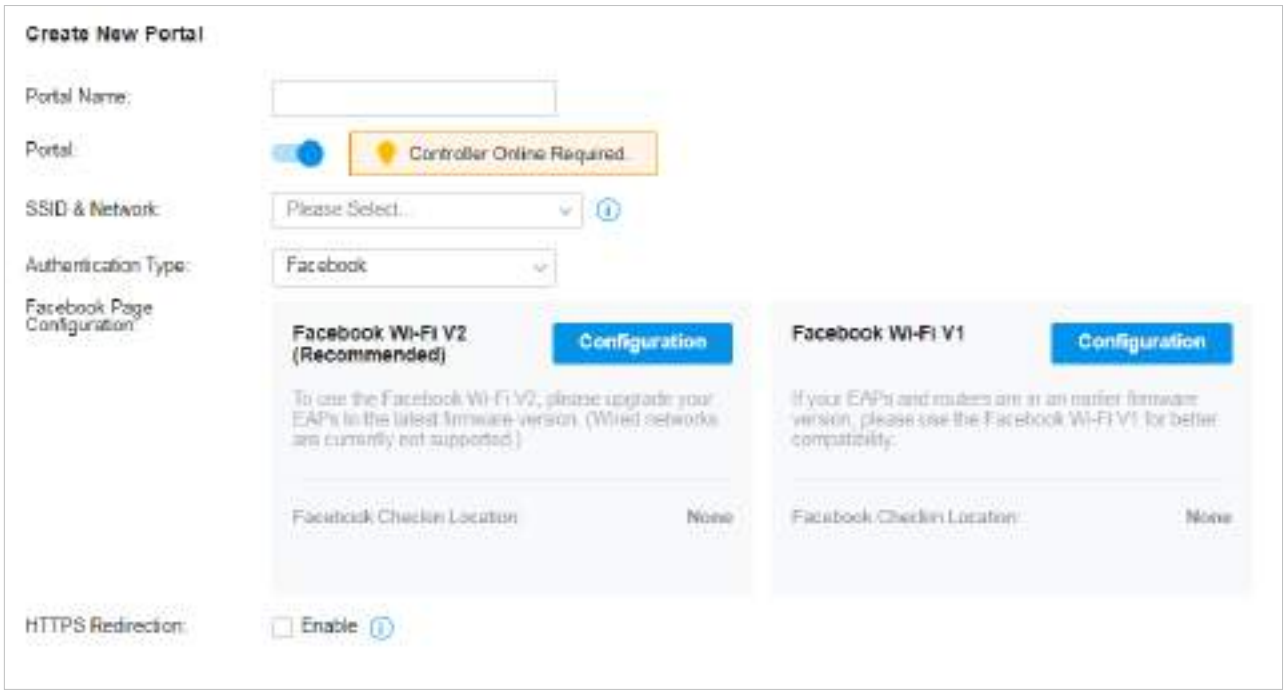
3. (Opțional) Configurați regulile de control al accesului, inclusiv Accesul pre-autentificare și Clientul fără autentificare, dacă este necesar. Mergi laSetări>Autentificare>Portal. În fila Control acces, faceți clic pe caseta de selectare pentru a activa Accesul de pre-autentificare și pentru a seta Clientul fără autentificare.



Preautentificare Acces	Faceți clic pe caseta de selectare pentru a activa Accesul de pre-autentificare. Cu această caracteristică activată, clienților neautentificați li se permite să acceseze subrețelele și resursele web specificate în Lista de acces pre-autentificare de mai jos.
Preautentificare Lista de acces	Clic Add pentru a configura intervalul IP sau adresa URL care sunt clienții neautentificați permis accesul.
Fără autentificare Client	Faceți clic pe caseta de selectare pentru a activa Clientul fără autentificare. Cu această caracteristică activată, puteți permite anumitor clienți să acceseze internetul fără autentificarea portalului.
Fără autentificare Lista de clienti	Clic Add și introduceți adresa IP sau adresa MAC a clienților fără autentificare.

■ Configurarea portalului cu Facebook

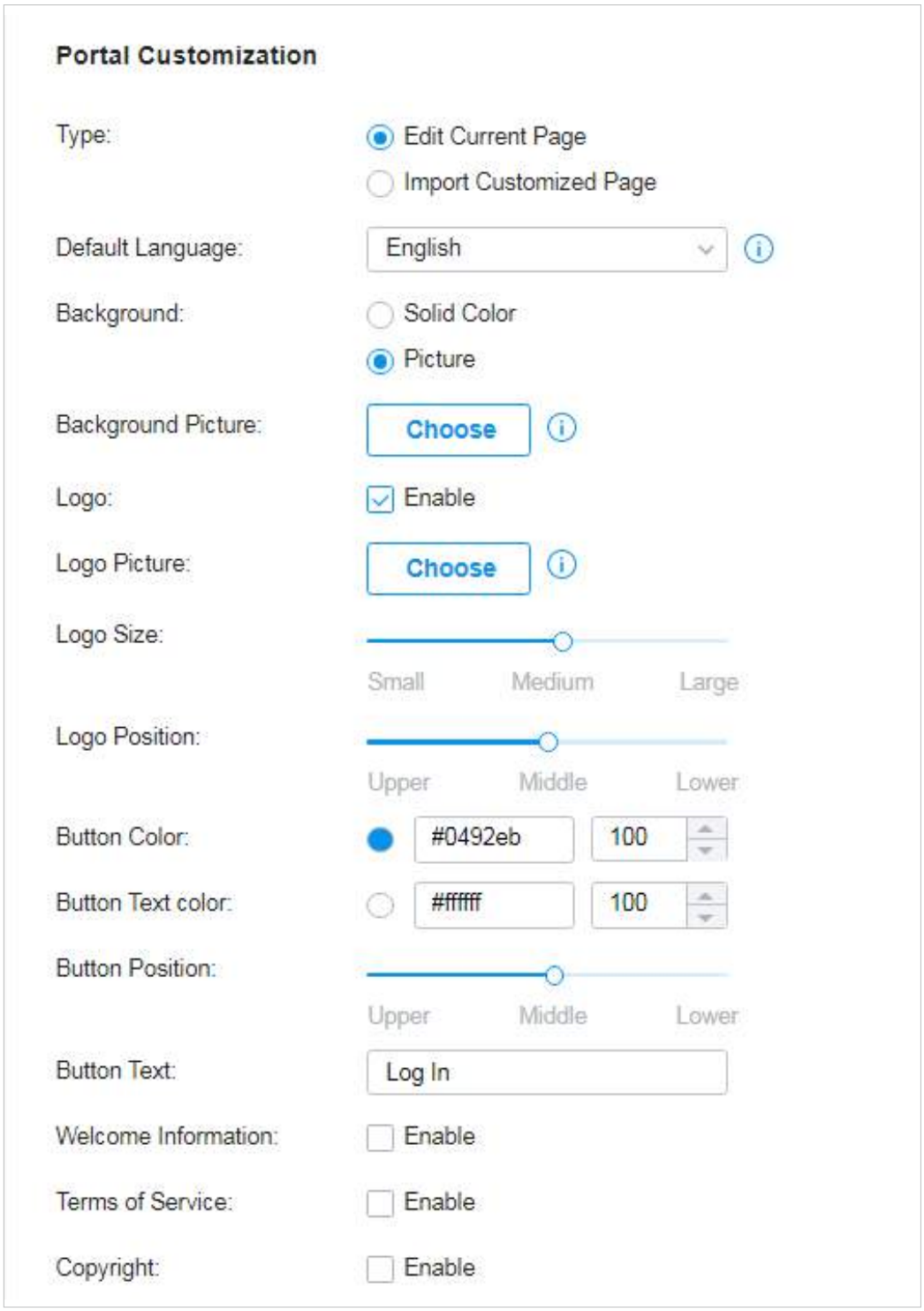
1. Selectați un site din lista derulantă aOrganizare. Mergi laSetări>Autentificare>Portal. Clic pentru a activa Portal și a încărca următoarea pagină.



2. Selectați SSID-urile și rețelele LAN pentru ca portalul să aibă efect și să configurați parametrii de bază.

SSID și rețea	Selectați unul sau mai multe SSID-uri sau rețele LAN pentru portal. Clienții conectați la SSID-urile sau rețelele LAN selectate trebuie să se conecteze la o pagină web pentru a stabili verificarea înainte de a accesa rețeaua.
tip de autentificare	Selectați tipul de autentificare Portal ca Facebook.
Pagina de Facebook Configurare:	Clic Configuration pentru a specifica Pagina de Facebook. Pentru Facebook Wi-Fi V1, clienți pot folosi contul Facebook pentru a se autentifica, iar pentru Facebook Wi-Fi V2, clienții pot folosi Cont Facebook sau Instagram pentru autentificare.
Înregistrare Facebook Locație	Când controlerul Omada obține cu succes pagina de Facebook, va afișa aici numele paginii de Facebook.
Redirecționare HTTPS	Faceți clic pe caseta de selectare pentru a activa redirecționarea HTTPS. Cu această caracteristică activată, clienții neautorizați vor fi redirecționați către pagina Portal atunci când încearcă să răsfoiască site-urile HTTPS. Cu această caracteristică dezactivată, clienții neautorizați nu pot naviga pe site-uri web HTTPS și nu sunt redirecționați către pagina Portal.

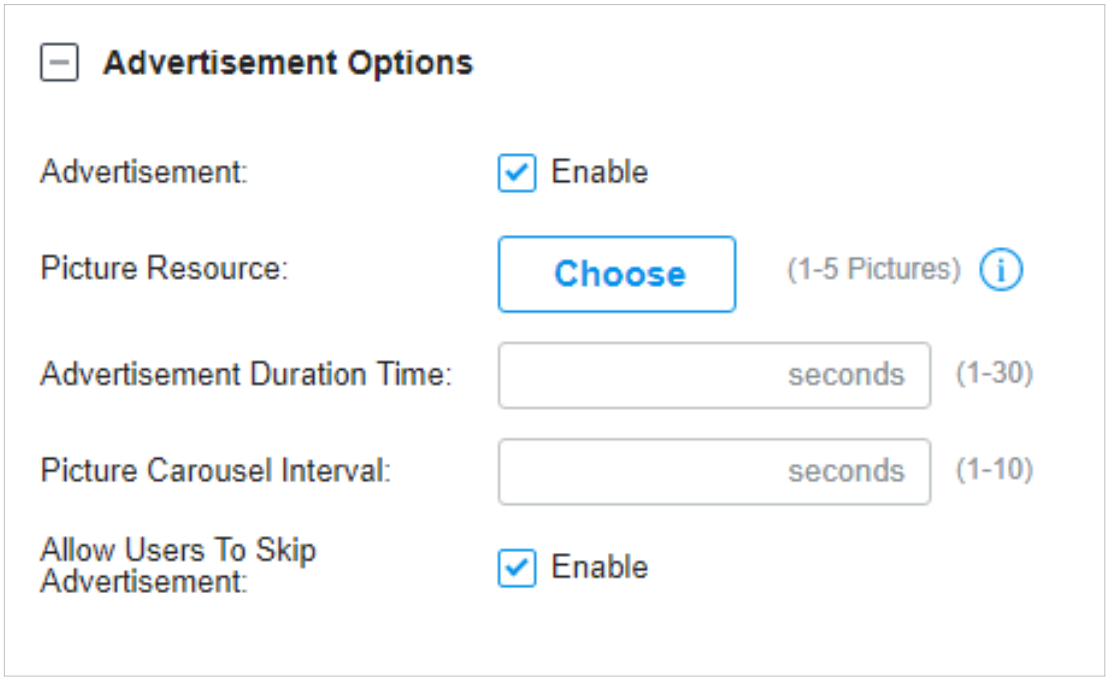
3. În secțiunea Personalizare portal, personalizați pagina Portal, inclusiv imaginea de fundal, imaginea siglei și așa mai departe.



Tip	Selectați tipul paginii Portal. Editați pagina curentă:Editați parametrii aferenți pentru a personaliza pagina Portal pe baza paginii furnizate. Importă pagină personalizată:Faceți clic Import pentru a importa pagina dvs. unică de portal pentru branding pe el conform companiei dvs.

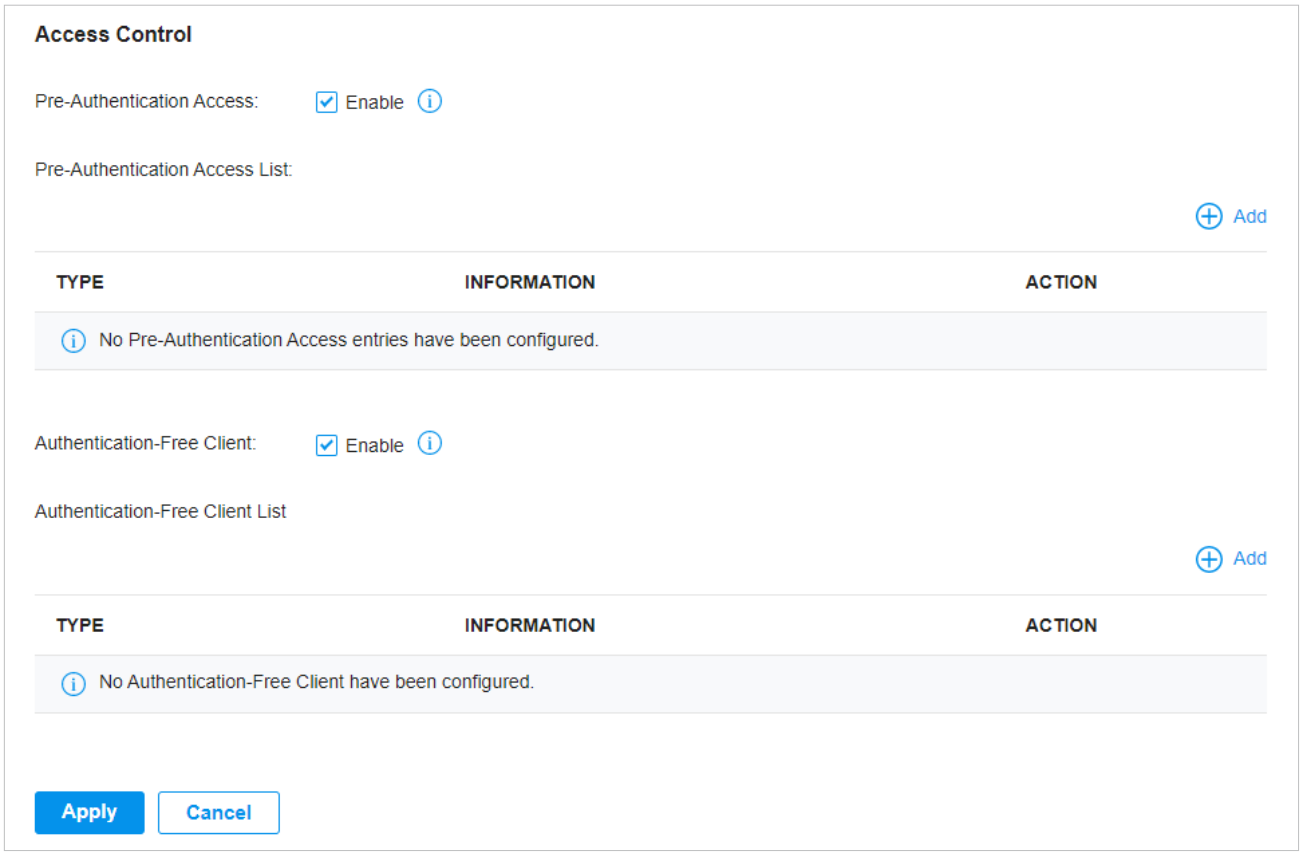
Limba implicita	Selectați limba implicită afișată pe pagina Portal. Controlerul ajustează automat limba afișată pe pagina Portal în funcție de limba sistemului a clienților. Dacă limba nu este acceptată, controlerul va folosi limba implicită specificată aici.
fundal	Selectați tipul de fundal. Culoare solida:Configurați culoarea de fundal dorită introducând manual codul de culoare HTML hexazecimal sau prin selectorul de culori. Imagine:Clic Choose și selectați o imagine de pe computer ca fundal.
Siglă	Faceți clic pentru a afișa sigla pe pagina portalului.
Imagine cu logo	Clic Choose și selectați o imagine de pe computer ca logo.
Dimensiunea logo-ului	Ajustați dimensiunea logo-ului pe pagina portalului.
Poziția logo-ului	Ajustați poziția siglei pe pagina portalului.
Culoarea butonului	Configurați culoarea de fundal dorită pentru buton introducând manual codul de culoare HTML hexazecimal sau prin selectorul de culori.
Culoarea textului butonului	Configurați culoarea textului dorită pentru buton introducând manual codul de culoare HTML hexazecimal sau prin selectorul de culori.
Poziția butonului	Selectați poziția butonului pe pagina portalului.
Buton Text	Introduceți textul pentru buton.
Informații de bun venit	Faceți clic pe caseta de selectare și introduceți text ca informații de bun venit. Puteți specifica dimensiunea dorită a fontului textului și puteți configura culoarea textului introducând manual codul de culoare HTML hexazecimal sau prin selectorul de culori.
Termenii serviciului	Faceți clic pe caseta de selectare și introduceți text ca termeni și condiții în caseta următoare. Clic Adăugați termenipentru a introduce numele și contextul termenilor care vor apărea după ce un client face clic pe linkul din Termenii și condițiile.
Drepturi de autor	Faceți clic pe caseta de selectare și introduceți text ca drepturi de autor în caseta următoare. Puteți specifica dimensiunea dorită a fontului textului și puteți configura culoarea textului introducând manual codul de culoare HTML hexazecimal sau prin selectorul de culori.
Afișați redirecționarea Numărătoarea inversă După Autorizat	Când este activat, sistemul va afișa numărătoarea inversă de redirecționare a portalului.

ClicOpțiuni de publicitateși cpersonalizați imaginile publicitare pe pagina de autentificare.



Publicitate	Faceți clic pe caseta de selectare pentru a activa funcția Publicitate. Cu această funcție activată, puteți adăuga imagini publicitare pe pagina de autentificare. Aceste imagini publicitare vor fi afișate înainte ca pagina de conectare să apară.
Resursa de imagine	Clic Choose și selectați imagini de pe computer ca imagini publicitare. Când sunt adăugate mai multe imagini, acestea vor fi redate în buclă.
Durata reclamei Timp	Introduceți durata pentru imaginile publicitare. Pe această perioadă, imaginile vor fi redate în buclă. Dacă durata de timp nu este suficientă pentru toate imaginile, restul nu vor fi afișate.
Carusel de imagini Interval	Introduceți intervalul carusel de imagini. De exemplu, dacă această valoare este setată la 5 secunde, prima imagine va fi afișată timp de 5 secunde, urmată de a doua imagine timp de 5 secunde și așa mai departe.
Permiteți utilizatorilor să omite reclamele	Faceți clic pe caseta de selectare pentru a permite utilizatorilor să omite reclamele.

4. (Opțional) Configurați regulile de control al accesului, inclusiv Accesul pre-autentificare și Clientul fără autentificare, dacă este necesar. Mergi laSetări>Autentificare>Portal. În fila Control acces, faceți clic pe caseta de selectare pentru a activa Accesul de pre-autentificare și pentru a seta Clientul fără autentificare.



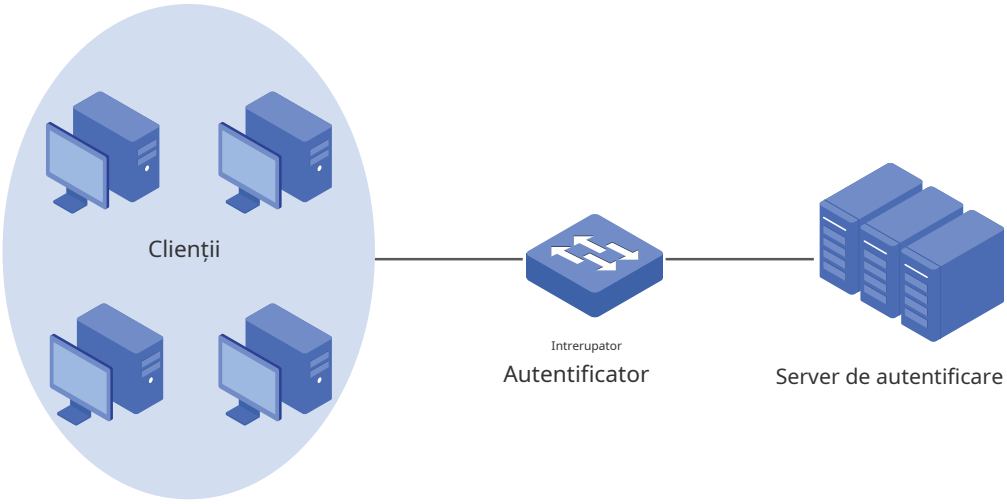
Preautentificare Acces	Faceți clic pe caseta de selectare pentru a activa Accesul de pre-autentificare. Cu această caracteristică activată, clienților neautentificați li se permite să acceseze subrețelele și resursele web specificate în Lista de acces pre-autentificare de mai jos.
Preautentificare Lista de acces	Clic Add pentru a configura intervalul IP sau adresa URL care sunt clienții neautentificați permis accesul.
Fără autentificare Client	Faceți clic pe caseta de selectare pentru a activa Clientul fără autentificare. Cu această caracteristică activată, puteți permite anumitor clienți să acceseze internetul fără autentificarea portalului.
Fără autentificare Lista de clienti	Clic Add și introduceți adresa IP sau adresa MAC a clienților fără autentificare.

3. 9. 2 802.1X

Prezentare generală

802.1X oferă un serviciu de autentificare bazat pe porturi pentru a restricționa accesul clienților neautorizați la rețea prin porturi de comutare accesibile public. An802.1X-enabledport permite doar mesaje de autentificare și interzice traficul normal până când clientul trece de autentificare.

Autentificarea 802.1X utilizează modelul client-server care conține trei roluri de dispozitiv: client/solicitant, autentificare și server de autentificare. Acest lucru este descris în figura de mai jos:



- Client

  Un client, de obicei un computer, este conectat la autentificator printr-un port fizic. Vă recomandăm să instalați software-ul client de autentificare TP-Link 802.1X pe gazdele client, permițându-le să solicite autentificarea 802.1X pentru a accesa LAN.

- Autentificator

  Un autentificator este de obicei un dispozitiv de rețea care acceptă protocolul 802.1X. După cum arată figura de mai sus, comutatorul este un autentificator.

  Autentificatorul acționează ca un proxy intermediar între client și serverul de autentificare. Autentificatorul solicită informații despre utilizator de la client și le trimite către serverul de autentificare; de asemenea, autentificatorul obține răspunsuri de la serverul de autentificare și le trimite clientului. Autentificatorul permite clienților autentificați să acceseze LAN prin porturile conectate, dar refuză clienții neautentificați.

- Server de autentificare

  Serverul de autentificare este de obicei gazda care rulează programul server RADIUS. Stochează informații despre clienți, confirmă dacă un client este legal și informează autentificatorul dacă un client este autentificat.

Bazat pe identitatea autentificată, 802.1X poate oferi și servicii personalizate. De exemplu, 802.1X și VLAN Assignment împreună fac posibilă atribuirea automată a diferiților utilizatori autentificați la diferite VLAN-uri.

Configurare

Pentru a finaliza configurația 802.1X, urmați acești pași:

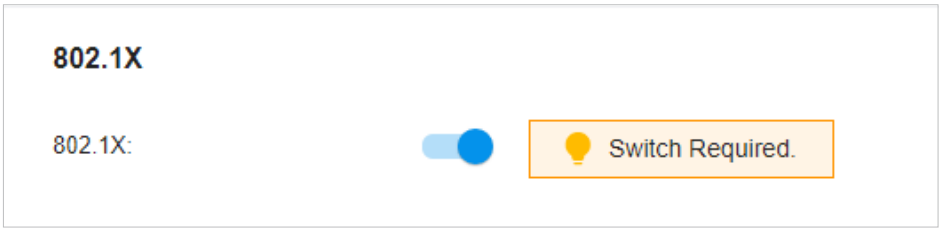
1)Faceți clic pentru a activa 802.1X.

2)Selectați profilul RADIUS pe care l-ați creat și configurați alți parametri.

3)Selectați porturile pe care va avea efect autentificarea 802.1X.

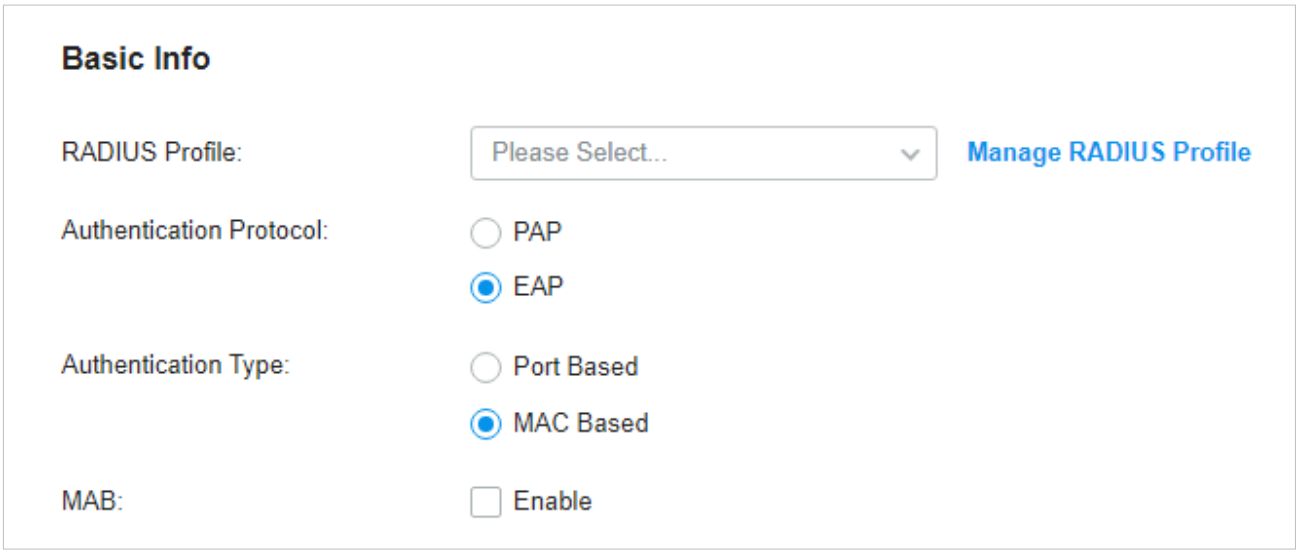
Activați 802.1X > Configurați profilul și parametrii RADIUS > Selectați porturile

Selectați un site din lista derulantă aOrganizare. Mergi laSetări>Autentificare>802.1X. Clic pentru a activa 802.1X.



Activați 802.1X > Configurați profilul și parametrii RADIUS > Selectați porturile

Selectați profilul RADIUS pe care l-ați creat. Dacă nu au fost create profiluri RADIUS, faceți clic + Create New RADIUS Profile din lista derulantă sau Manage RADIUS Profile pentru a crea unul. RAZA profil înregistrează informațiile serverului RADIUS care acționează ca server de autentificare în timpul autentificării 802.1X.



Protocol de autentificare	Selectați protocolul de autentificare pentru schimbul de mesaje între comutator și serverul RADIUS. Ca o punte între client și serverul RADIUS, comutatorul redirecționează mesajele pentru ei. Utilizează pachete EAP pentru a schimba mesaje cu clientul și procesează mesajele conform protocolului de autentificare specificat înainte de a le redirecționa către serverul RADIUS. PAP:Pachetele EAP sunt convertite în alte pachete de protocol (cum ar fi RADIUS) și transmise serverului RADIUS. EAP:Pachetele EAP sunt încapsulate în alte pachete de protocol (cum ar fi RADIUS) și transmise la serverul de autentificare. Pentru a utiliza acest mecanism de autentificare, serverul RADIUS ar trebui să accepte atribute EAP.

tip de autentificare	Selectați tipul de autentificare 802.1X. Bazat pe port:După ce un client conectat la port este autentificat cu succes, alți clienți pot accesa rețeaua prin port fără autentificare. Bazat pe MAC:Clienții conectați la port trebuie să fie autentificați individual. Serverul RADIUS distinge clienții după adresele lor MAC.
Atribuire VLAN	Această caracteristică permite serverului RADIUS să trimită configurațiile VLAN către port în mod dinamic. După ce portul este autentificat, serverul RADIUS atribuie VLAN-ul pe baza numelui de utilizator al clientului care se conectează la portul. Mapările nume de utilizator la VLAN trebuie să fie deja stocate în baza de date a serverului RADIUS. Această caracteristică este disponibilă numai când tipul de autentificare 802.1X este bazat pe port.
MAB	MAB (MAC Authentication Bypass) permite clienților să fie autentificați fără a fi instalat niciun software client. MAB este util pentru autentificarea dispozitivelor fără capacitate 802.1X, cum ar fi telefoanele IP. Când MAB este activat pe un port, comutatorul va învăța automat adresa MAC a clientului și va trimite serverului de autentificare un cadru de solicitare de acces RADIUS cu adresa MAC a clientului ca nume de utilizator și parolă. MAB are efect numai atunci când autentificarea 802.1X este activată pe port.

Activați 802.1X > Configurați profilul și parametrii RADIUS > Selectați porturile

Selectați porturile pentru a activa autentificarea 802.1X sau MAB pentru ele. Pentru a activa autentificarea 802.1X, faceți clic pe porturile neselectate. Porturile 802.1X activate vor fi marcate cu . Pentru a activa MAB, faceți clic pe porturile marcate cu . Puteți activa MAB numai pe porturile 802.1X activate. Porturile activate pentru MAB vor fi marcate cu .

Notă:

- Nu vi se recomandă să activați autentificarea 802.1X pe porturile switch-ului care se conectează la dispozitivele de rețea fără capacitatea 802.1X, cum ar fi routerul și AP-urile.
- Comutatorul autentifică clienții cu fir care se conectează la portul cu 802.1X activat. Și gateway-ul autentifică clienții cu fir care se conectează la rețea cu Portal configurat. Clienții cu fir ar trebui să treacă autentificarea Portal și 802.1X pentru a accesa internetul atunci când ambele sunt configurate.

3. 9. 3 Autentificare bazată pe MAC Prezentare

generală

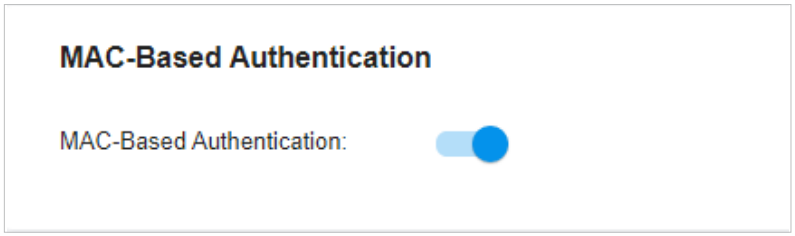
Autentificarea bazată pe MAC permite sau interzice accesul clienților la rețelele wireless pe baza adreselor MAC ale clienților. În această metodă de autentificare, controlerul ia adresele MAC ale clienților fără fir drept nume de utilizator și parole pentru autentificare. Serverul RADIUS autentifică adresele MAC în baza de date care stochează adresele MAC permise. Clienții pot accesa rețelele wireless configurate cu autentificarea bazată pe MAC după ce au trecut cu succes autentificarea.

Notă:

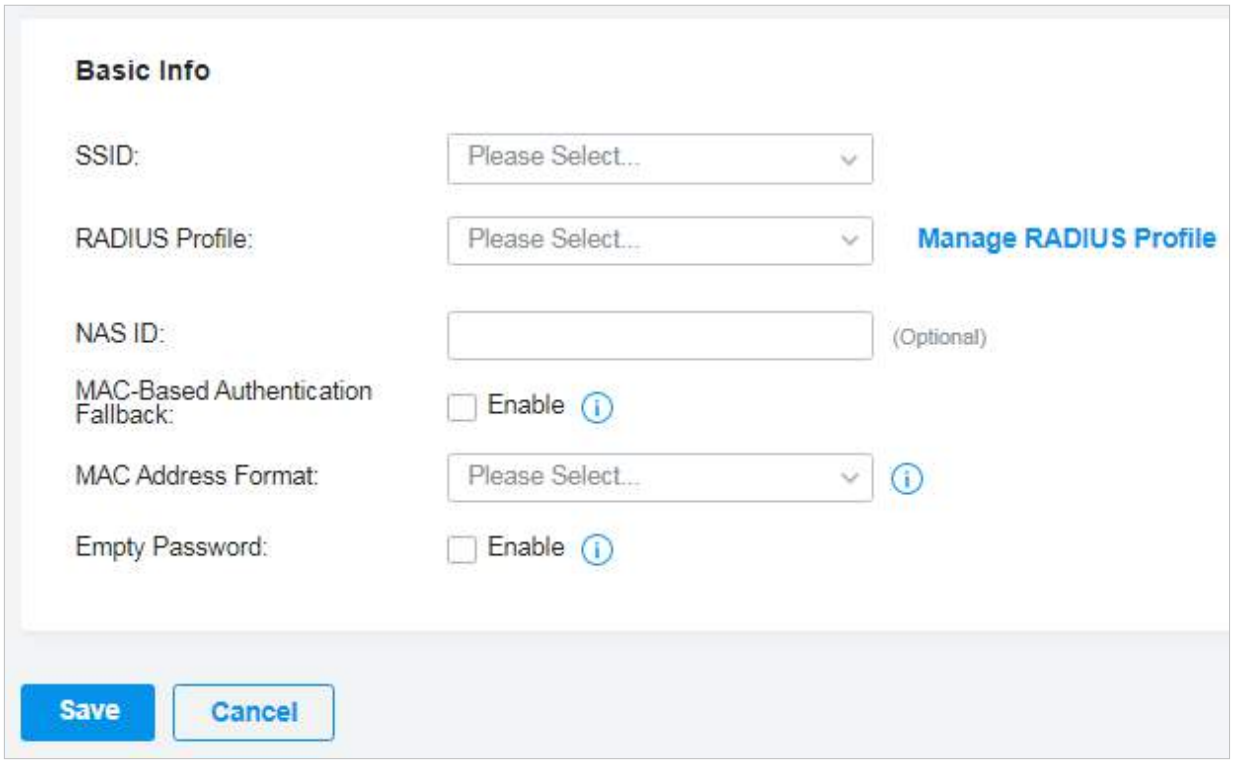
Atât Autentificarea bazată pe MAC, cât și autentificarea Portal pot autentifica clienții wireless. Dacă ambele sunt configurate într-o rețea fără fir, un client wireless trebuie să treacă mai întâi autentificarea bazată pe MAC și apoi autentificarea portal pentru acces la internet. Puteți activa autentificarea bazată pe MAC pentru a permite clienților să ocolească autentificarea bazată pe MAC, ceea ce înseamnă că clientul trebuie să treacă oricare dintre cele două autentificare. Clientul încearcă mai întâi autentificarea bazată pe MAC și are voie să încerce autentificarea portal dacă a eșuat autentificarea bazată pe MAC.

Configurare

1. Selectați un site din lista derulantă aOrganizare. Mergi laSetări>Autentificare>Autentificare bazată pe MAC. Faceți clic pentru a activa autentificarea bazată pe MAC.



2. În Informații de bază, selectați SSID-urile, Profilul RADIUS și alți parametri necesari. Consultați următorul tabel pentru a configura parametrii necesari și faceți clicSalvați.



SSID	Selectați unul sau mai multe SSID-uri pentru ca autentificarea bazată pe MAC să aibă efect.
Profil RADIUS	Selectați profilul RADIUS pe care l-ați creat. Dacă nu au fost create profiluri RADIUS, clic + Create New RADIUS Profile din lista derulantă sau Manage RADIUS Profile pentru a crea unul. Profilul RADIUS înregistrează informațiile serverului RADIUS care acționează ca server de autentificare în timpul autentificării bazate pe MAC.

ID NAS	Configurați un identificator de server de acces la rețea (ID NAS) pentru autentificare. Pachetele de solicitare de autentificare de la controler la serverul RADIUS poartă ID-ul NAS. Serverul RADIUS poate clasifica utilizatorii în diferite grupuri pe baza ID-ului NAS și apoi poate alege politici diferite pentru diferite grupuri.
Bazat pe MAC Fallback de autentificare	Pentru rețeaua wireless configurată atât cu autentificare bazată pe MAC, cât și cu portal, dacă activați această caracteristică, un client wireless trebuie să treacă o singură autentificare. Clientul încearcă mai întâi autentificarea bazată pe MAC și are voie să încerce autentificarea portal dacă a eșuat autentificarea bazată pe MAC. Dacă dezactivați această caracteristică ca implicit, un client wireless trebuie să treacă atât Autentificarea bazată pe MAC, cât și autentificarea portalului pentru acces la internet și va fi refuzat dacă nu reușește oricare dintre autentificare.
Formatul adresei MAC	Selectați formatul adresei MAC al clienților pe care îl folosește controlerul pentru autentificare. Apoi configurați adresele MAC în formatul specificat ca nume de utilizator pentru clienții de pe serverul RADIUS.
Parola goală	Faceți clic pentru a permite o parolă goală pentru autentificarea bazată pe MAC. Cu această opțiune dezactivată, parola va fi aceeași cu numele de utilizator.

3. 9. 4 Profil RADIUS Prezentare

generală

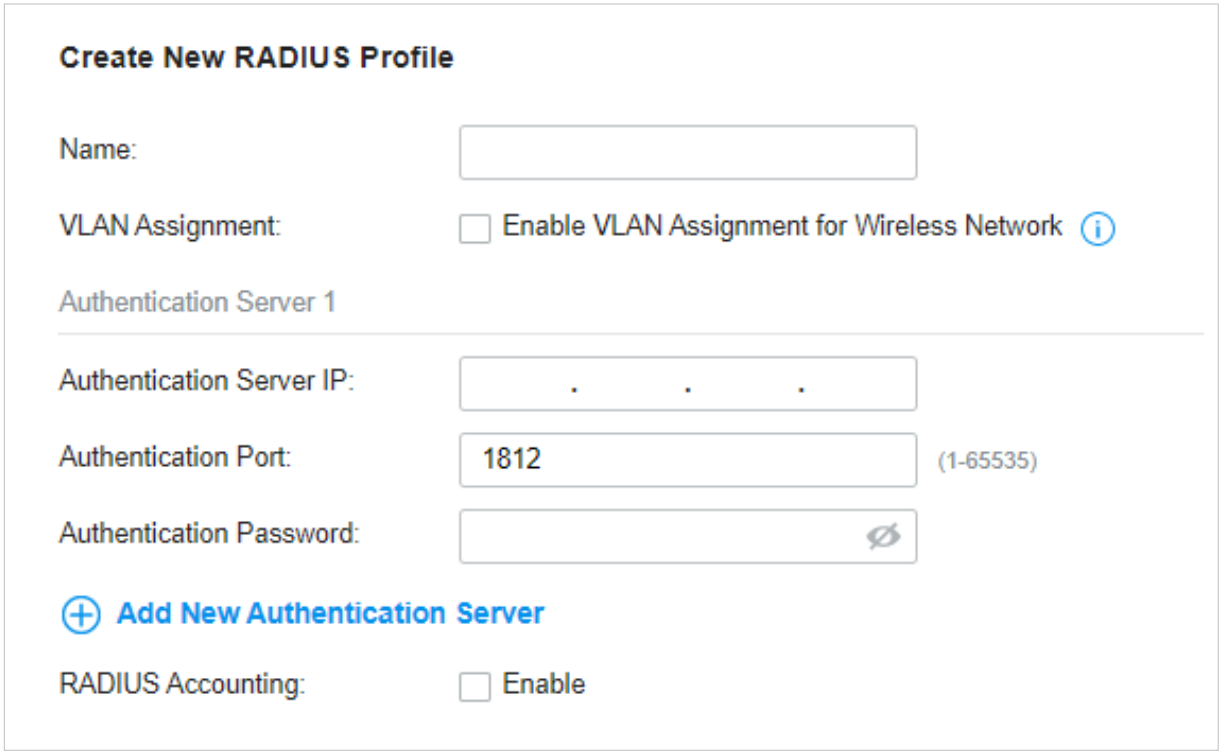
RADIUS (Remote Authentication Dial In User Service) este un protocol client/server care asigură nevoile AAA (Autentificare, Autorizare și Contabilitate) în mediile IT moderne.

În serviciile de autentificare, inclusiv 802.1X, Portal și autentificarea bazată pe MAC, dispozitivele Omada funcționează ca clienți ai RADIUS pentru a transmite informații despre utilizator către serverele RADIUS desemnate. Un server RADIUS menține o bază de date care stochează informațiile de identitate ale utilizatorilor legali. Autentifică utilizatorii în baza de date atunci când utilizatorii solicită accesul la rețea și le oferă servicii de autorizare și contabilitate.

Un profil RADIUS înregistrează setările dvs. personalizate ale unui server RADIUS. După crearea unui profil RADIUS, îl puteți aplica mai multor politici de autentificare precum Portal și 802.1X, evitându-vă să introduceți în mod repetat aceleași informații.

Configurare

1. Selectați un site din lista derulantă aOrganizare. Mergi laSetări>Autentificare>Profil RADIUS. Clic + Create New RADIUS Profile pentru a încărca următoarea pagină.



2. Introduceți informațiile serverelor RADIUS. Consultați următorul tabel pentru a configura parametrii necesari și faceți clicSalvați.

Nume	Introduceți un nume pentru a identifica profilul RADIUS.
Atribuire VLAN	Această caracteristică permite serverului RADIUS să plaseze un utilizator fără fir într-un anumit VLAN pe baza acreditărilor furnizate de utilizator. Pentru a utiliza funcția, ar trebui să creați mai întâi VLAN-ul specific. Iar mapările de la utilizator la VLAN trebuie să fie deja stocate în baza de date a serverului RADIUS. Notă: 1. Atribuirea VLAN nu este acceptată în prezent când un client este autentificat de Portal cu Server RADIUS extern sau Hotspot RADIUS. 2. Atribuirea VLAN este aplicabilă numai atunci când dispozitivul acceptă caracteristica. Pentru ca această caracteristică să funcționeze corect, se recomandă să actualizați dispozitivele la cea mai recentă versiune de firmware.
Server de autentificare IP	Introduceți adresa IP a serverului de autentificare.
Port de autentificare	Introduceți portul de destinație UDP pe serverul de autentificare pentru solicitările de autentificare.
Autentificare Parola	Introduceți parola care va fi folosită pentru a valida comunicarea dintre dispozitivele Omada și serverul de autentificare RADIUS.

Contabilitate RADIUS	Faceți clic pe caseta de selectare pentru a activa Contabilitatea RADIUS pentru a satisface nevoile de facturare. Această caracteristică este disponibilă numai pentru EAP-urile Omada cu Portal pentru a contabiliza clienții wireless.
Actualizare intermediară	Faceți clic pe caseta de selectare pentru a activa Actualizarea intermediară. În mod implicit, procesul de contabilitate RADIUS are nevoie doar de mesaje de pornire și oprire către serverul de contabilitate RADIUS. Cu Actualizarea intermediară activată, dispozitivele Omada vor trimite periodic o actualizare intermediară (un pachet de solicitare de contabilitate RADIUS care conține o valoare „actualizare intermediară”) către serverul RADIUS. O actualizare intermediară actualizează durata sesiunii utilizatorului și utilizarea curentă a datelor.
Interval de actualizare interimar	Introduceți un interval adecvat între actualizările duratei sesiunii utilizatorilor și utilizarea curentă a datelor.
IP server de contabilitate	Introduceți adresa IP a serverului de contabilitate RADIUS.
Port de contabilitate	Introduceți portul de destinație UDP pe serverul RADIUS pentru solicitările de contabilitate.
Parola de contabilitate	Introduceți parola care va fi folosită pentru a valida comunicarea dintre dispozitivele Omada și serverul de contabilitate RADIUS.

3. 10 Servicii

Serviciile oferă servicii de rețea convenabile și facilitează gestionarea rețelei. Puteți seta o adresă IP fixă pentru anumite dispozitive în Rezervare DHCP, puteți configura servere sau terminale în DDNS, SNMP, UPnP și SSH, puteți programa dispozitivele în Programul de repornire, Programul PoE și Programul de actualizare și puteți exporta informațiile din Export Data.

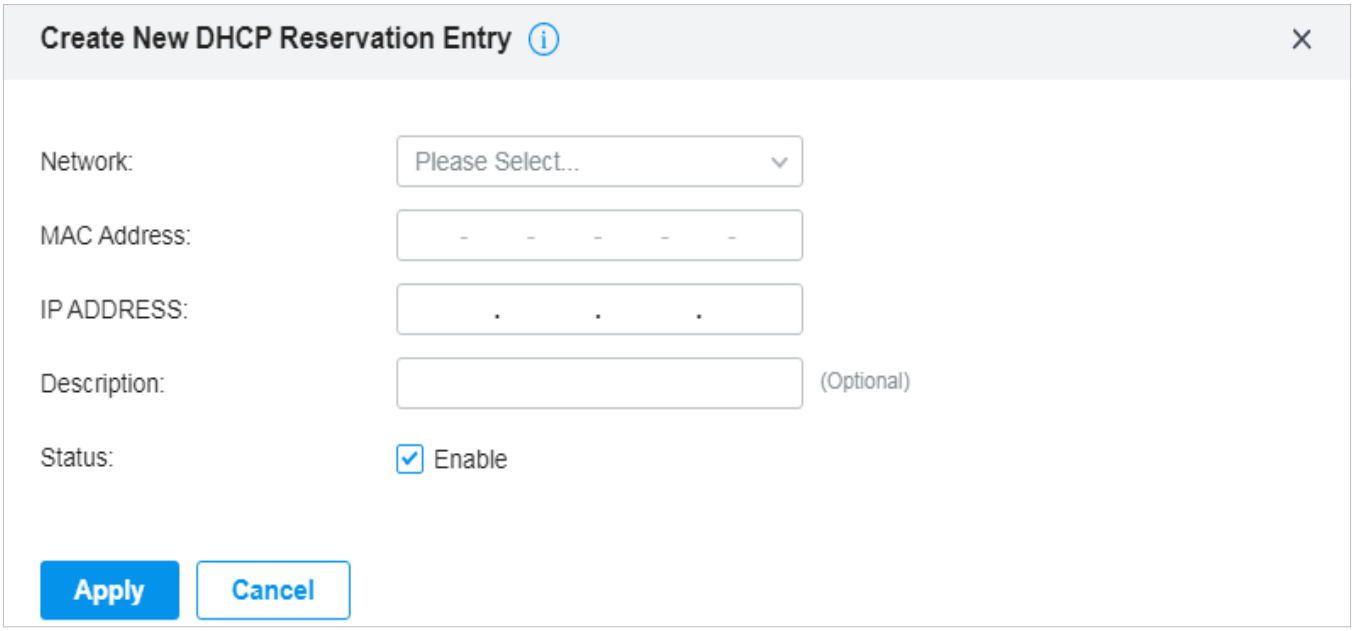
3. 10. 1 Rezervare DHCP

Prezentare generală

Este convenabil ca rețelele să utilizeze adrese IP dinamice atribuite prin Protocolul de configurare dinamică a gazdei (DHCP), totuși, pentru dispozitivele care trebuie accesate în mod fiabil, este ideal să setați adrese IP fixe pentru acestea. Rezervarea DHCP vă permite să rezervați adrese IP specifice pentru dispozitivele din rețeaua dvs. și să gestionați la nivel central adresele IP.

Configurare

Selectați un site din lista derulantă aOrganizare. Mergi laSetări>Servicii>Rezervare DHCP, faceți clic +Creează o nouă intrare de rezervare DHCPși configurați parametrii. Apoi apasaaplica.



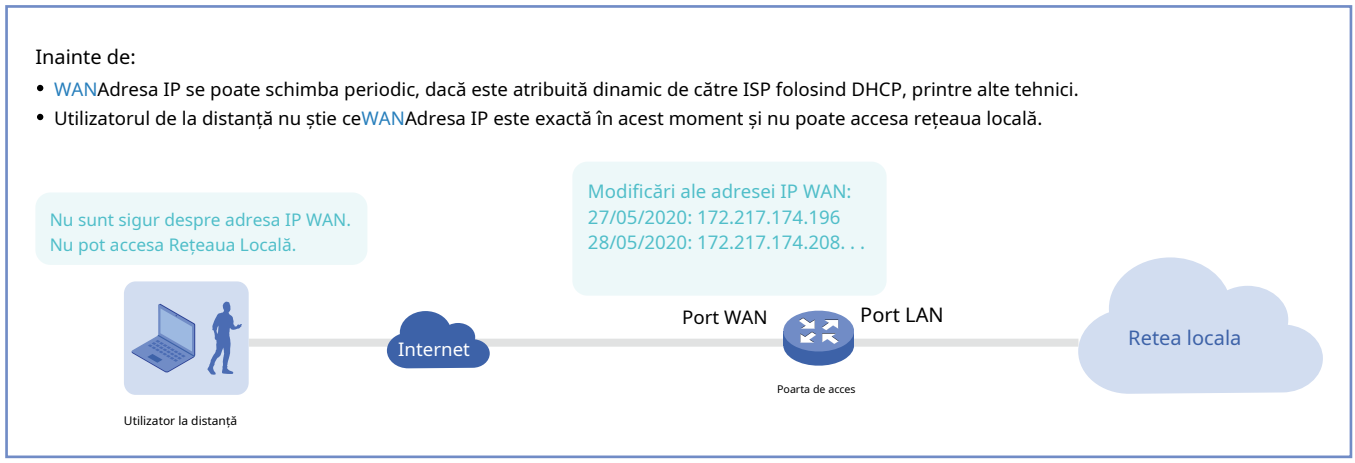
Rețea	Selectați rețeaua pentru care este utilizată intrarea de rezervare DHCP.
Adresa mac	Specificați adresa MAC a dispozitivului pentru care doriți să rezervați o adresă IP.
Adresa IP	Specificați adresa IP fixă pentru dispozitiv.
Descriere	Introduceți descrierea intrării pentru identificare.
stare	Activați sau dezactivați intrarea.

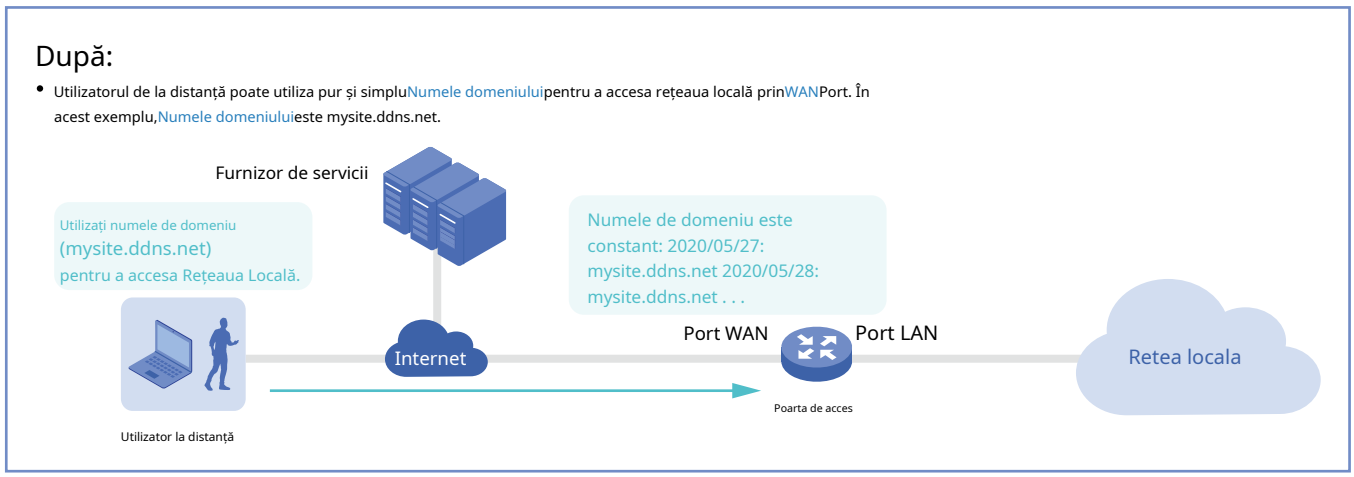
3. 10. 2 DNS dinamic

Prezentare generală

Adresa IP WAN a gateway-ului dvs. se poate schimba periodic, deoarece ISP-ul dvs. utilizează de obicei DHCP, printre alte tehnici. Aici intervine Dynamic DNS. Dynamic DNS atribuie un nume de domeniu fix portului WAN al gateway-ului, ceea ce facilitează utilizatorilor la distanță să acceseze rețeaua locală prin portul WAN.

Să ilustrăm cum funcționează DNS dinamic cu următoarele figuri.



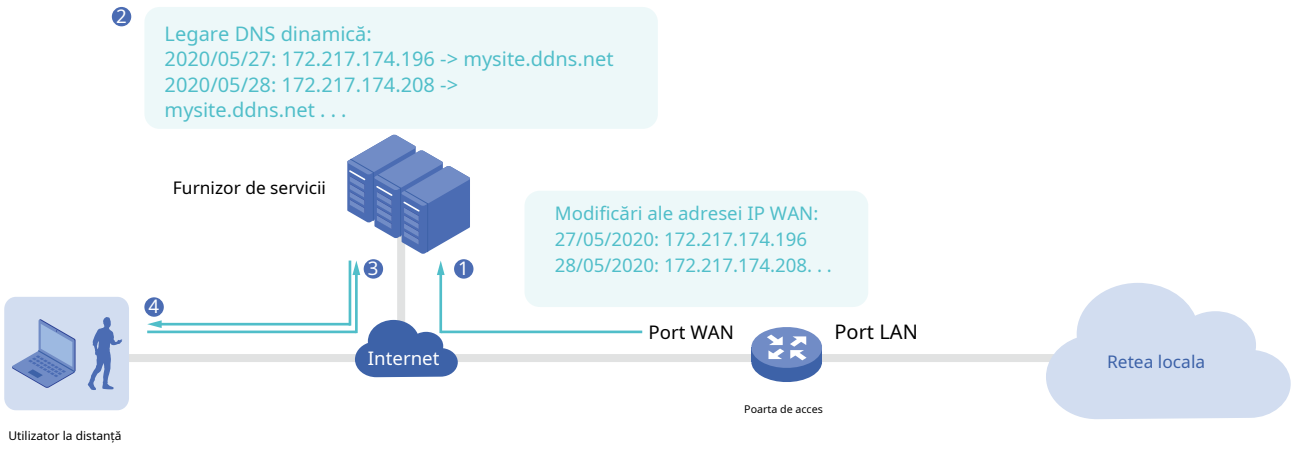


Condiție preliminară:

- Alege unaFurnizor de serviciidin cele patru pe care le suportă controlerul, adicăDynDNS,Fără IP,Peanuthull,Comexe.
- Înregistrați-vă la dvsFurnizor de servicii, atunci îți ieiNume de utilizatorșiParola. Ia-tiNumele domeniuluide la tine
- Furnizor de servicii.

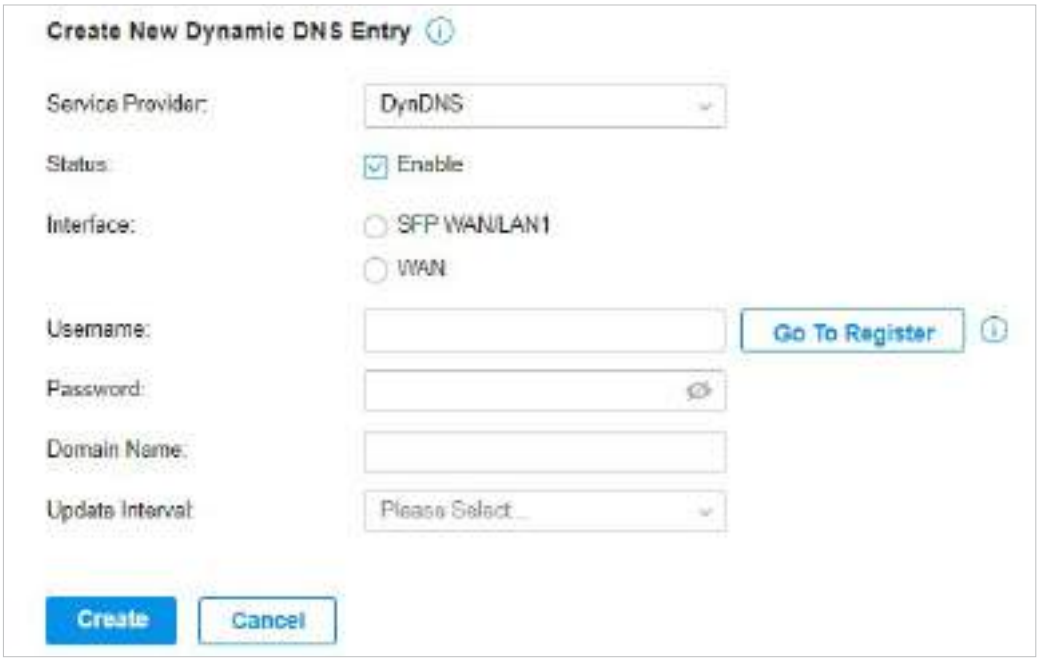
Cum funcționează DNS dinamic:

1. Gateway informeazăFurnizor de serviciideWANAdresa IP.
2. Furnizor de serviciileagăWANAdresa IP cuNumele domeniuluiși îl menține actualizat pe măsură ce se modifică adresa IP WAN.
3. Solicitările utilizatorilor de la distanță pentruWANAdresa IP prin trimitereNumele domeniuluilaFurnizor de servicii.
4. Furnizor de serviciiraspunde cuWANAdresa IP, pe care utilizatorul la distanță o folosește de fapt pentru a accesa rețeaua localăWANPort.



Configurare

Selectați un site din lista derulantă aOrganizare. Mergi laSetări>Servicii>DNS dinamic. Clic+ Creați o nouă intrare DNS dinamică, pentru a încărca următoarea pagină. Configurați parametrii și faceți clicCrea.



Furnizor de servicii	Selectați furnizorul de servicii cu care funcționează Dynamic DNS.

stare	Activați sau dezactivați intrarea DNS dinamic.
Interfață	Selectați portul WAN căruia i se aplică intrarea Dynamic DNS.
Nume de utilizator	Introduceți numele dvs. de utilizator pentru furnizorul de servicii. Dacă nu v-ați înregistrat la furnizorul de servicii, faceți clicMergi la Înregistrare.
Parola	Introduceți parola pentru furnizorul de servicii.
Numele domeniului	Introduceți numele de domeniu furnizat de furnizorul dvs. de servicii. Utilizatorii de la distanță pot folosi numele de domeniu pentru a accesa rețeaua locală prin portul WAN.
Interval de actualizare	Selectați cât de des este actualizată adresa IP WAN cu Nume de domeniu.

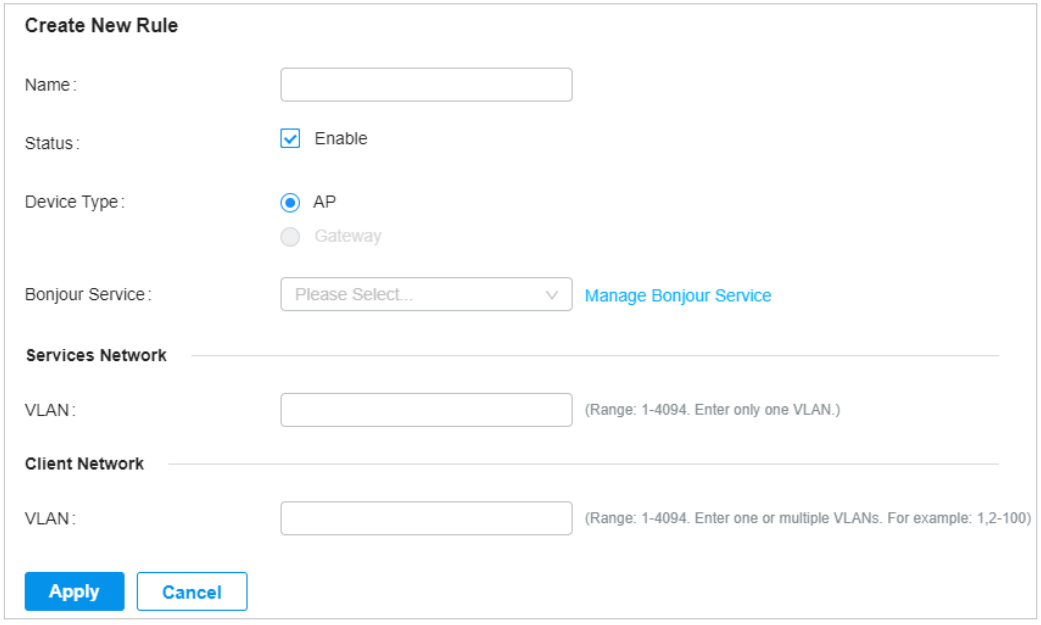
3. 10. 3 mDNS

Prezentare generală

Repeatorul mDNS (Multicast DNS) poate ajuta pachetele de solicitare/răspuns mDNS răspândite în diferite segmente de rețea. Cu această funcție, serviciile publicate folosind protocolul mDNS pot fi descoperite pe segmente de rețea.

Configurare

1. Selectați un site din lista derulantă aOrganizare. Mergi laSetări>Servicii>mDNS.
2. Faceți clic + Create New Rule pentru a crea o nouă regulă de redirecționare mDNS și a configura parametrii.
3. Aplicați setările.



Nume	Specificați numele regulii pentru identificare.

stare	Activați sau dezactivați această regulă.
Tip de dispozitiv	Specificați tipul de dispozitiv pentru care regula intră în vigoare.
Serviciu Bonjour:	Serviciu Bonjour: Specificați serviciile care vor fi redirecționate.
Rețea de servicii > VLAN	Specificați VLAN-urile unde se află serviciile mDNS. Puteți introduce intervale VLAN sau ID-uri VLAN separate prin virgulă.
Rețea client > VLAN	Specificați VLAN-urile unde se află dispozitivele Client. Puteți introduce intervale VLAN sau ID-uri VLAN separate prin virgulă.

3. 10. 4 SNMP

Prezentare generală

SNMP (Simple Network Management Protocol) oferă o metodă convenabilă și flexibilă pentru configurarea și monitorizarea dispozitivelor de rețea. Odată ce ați configurat SNMP pentru dispozitive, le puteți gestiona central cu un NMS (Network Management Station).

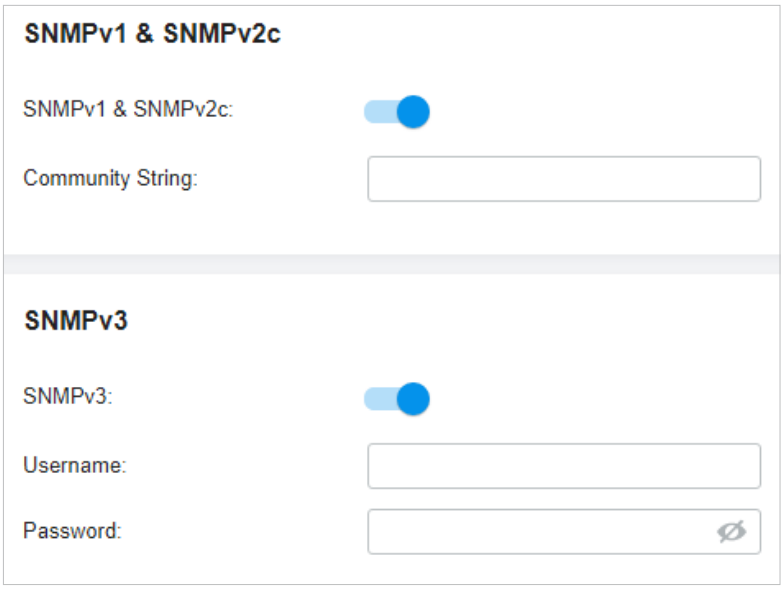
Controlerul acceptă mai multe versiuni SNMP, inclusiv SNMPv1, SNMPv2c și SNMPv3.

Notă:

Dacă utilizați un NMS pentru a gestiona dispozitivele care sunt gestionate de controler, puteți doar să citiți, dar nu să scrieți obiecte SNMP.

Configurare

Selectați un site din lista derulantă aOrganizare. Mergi laSetări>Servicii>SNMPși configurați parametrii. Apoi apasaaplica.



SNMPv1 și SNMPv2c	Activați sau dezactivați SNMPv1 și SNMPv2c la nivel global.

șir de comunitate	Cu SNMPv1 și SNMPv2c activate, specificați șirul de comunitate, care este folosit ca parolă pentru NMS pentru a accesa agentul SNMP. Trebuie să configurați șirul comunității în mod corespunzător pe NMS.
SNMPv3	Activați sau dezactivați SNMPv3 la nivel global.
Nume de utilizator	Cu SNMPv3 activat, specificați numele de utilizator pentru NMS-ul dvs. pentru a accesa agentul SNMP. Trebuie să configurați numele de utilizator corespunzător pe NMS.
Parola	Cu SNMPv3 activat, specificați parola pentru NMS pentru a accesa agentul SNMP. Trebuie să configurați parola în mod corespunzător pe NMS.

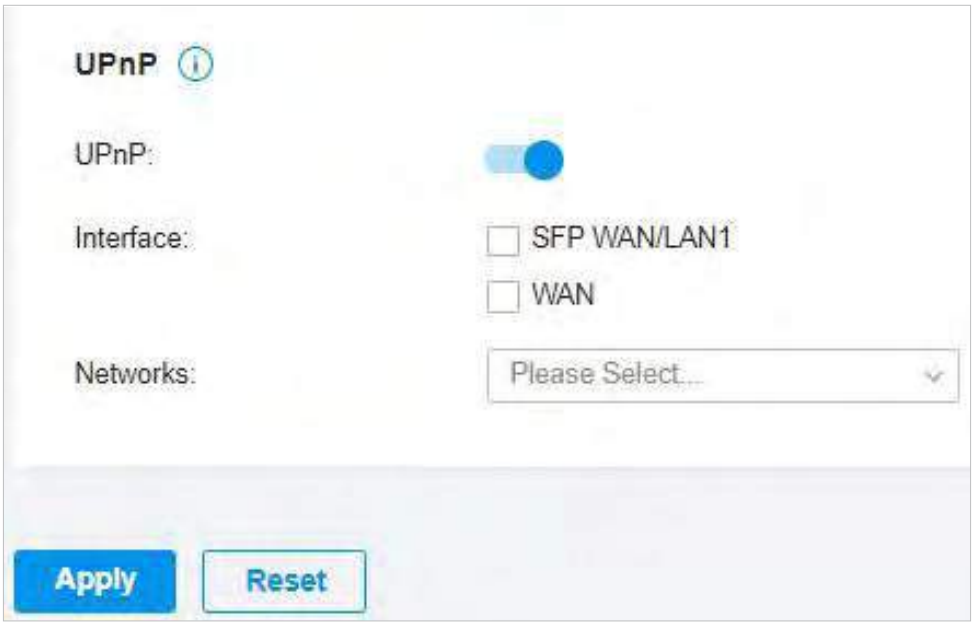
3. 10. 5 UPnP

Prezentare generală

UPnP (Universal Plug and Play) este esențial pentru aplicații, inclusiv jocuri multiplayer, conexiuni peer-to-peer, comunicare în timp real (cum ar fi VoIP sau conferință telefonică) și asistență la distanță etc. Cu ajutorul UPnP, traficul dintre punctele finale ale acestor aplicații pot trece liber de gateway, realizând astfel conexiuni fără întreruperi.

Configurare

Selectați un site din lista derulantă aOrganizare. Mergi laSetări>Servicii>UPnP. Activați UPnP la nivel global și configurați parametrii. Apoi apasaaplica.



Interfață	Selectați portul WAN unde UPnP are efect.
Rețele	Selectați interfața LAN unde UPnP are efect.

3. 10. 6 SSH

Prezentare generală

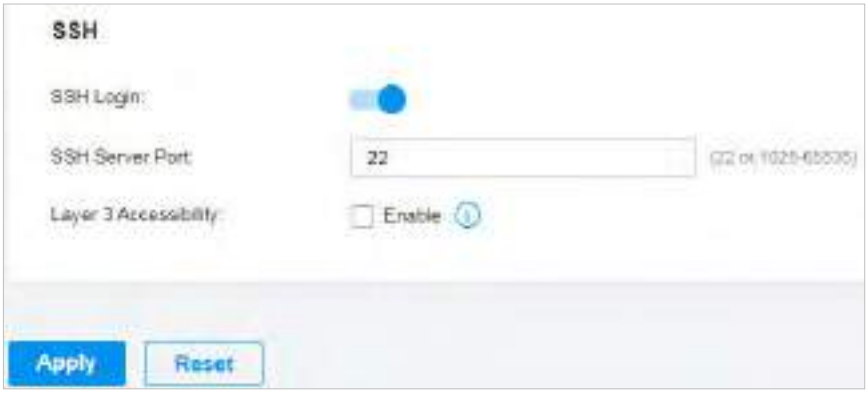
SSH (Secure Shell) vă oferă o metodă pentru a configura și monitoriza în siguranță dispozitivele de rețea printr-o interfață de utilizator de linie de comandă pe terminalul SSH.

Notă:

Dacă utilizați un terminal SSH pentru a gestiona dispozitivele care sunt gestionate de controler, puteți obține doar privilegiul de utilizator.

Configurare

Selectați un site din lista derulantă aOrganizare. Mergi laSetări>Servicii>SSH. Activați SSH Login la nivel global și configurați parametrii. Apoi apasaaplica.



Portul serverului SSH	Specificați portul serverului SSH pe care dispozitivele dvs. de rețea îl folosesc pentru conexiunile SSH. Trebuie să configurați portul serverului SSH în mod corespunzător pe terminalul dvs. SSH.
Stratul 3 Accesibilitate	Cu această caracteristică activată, terminalul SSH dintr-o subrețea diferită vă poate accesa dispozitivele prin SSH. Cu această funcție dezactivată, numai terminalul SSH din aceeași subrețea vă poate accesa dispozitivele prin SSH.

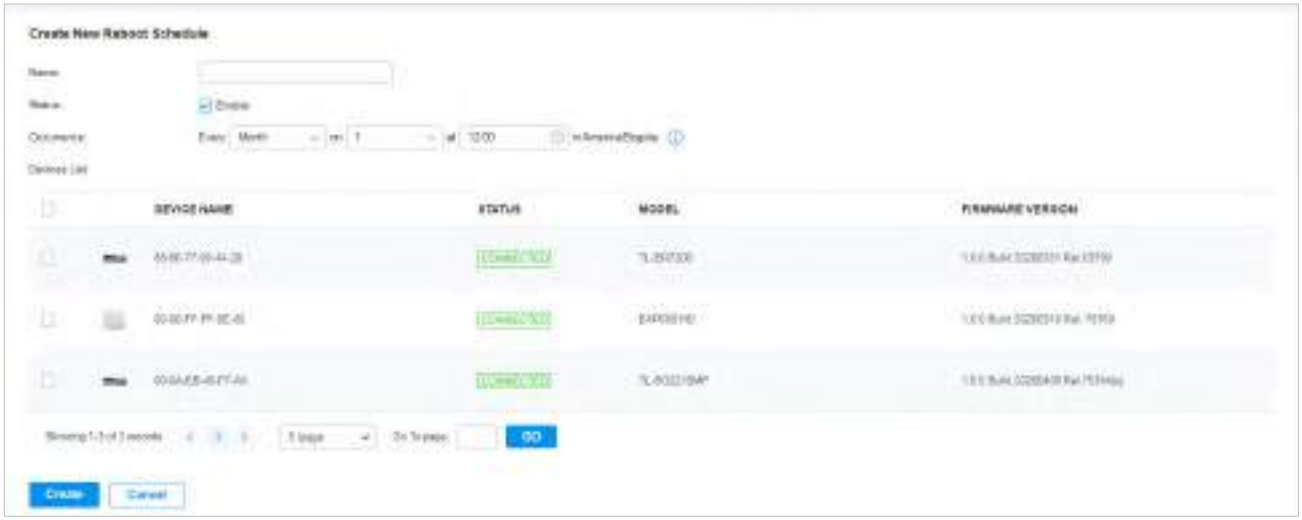
3. 10. 7 Programul de repornire

Prezentare generală

Programul de repornire poate face ca dispozitivele să se repornească periodic, în funcție de nevoile dvs. Puteți configura programul de repornire în mod flexibil creând mai multe intrări în programul de repornire.

Configurare

1. Selectați un site din lista derulantă aOrganizare. Mergi laSetări>Servicii>Programul de repornire. Clic+ Creați un nou program de repornirepentru a încărca următoarea pagină și a configura parametrii.



Nume	Introduceți numele pentru a identifica intrarea Programului de repornire.
stare	Activați sau dezactivați intrarea Programul de repornire.
Apariția	Specificați data și ora pentru repornirea dispozitivelor.
Lista de dispozitive	Selectați dispozitivele cărora li se aplică Programul de repornire.

2. Faceți clicCrea. Noua intrare Program de repornire este adăugată la tabel. Puteți face clic pentru a edita intrarea. Puteți face clic pentru a șterge intrarea.

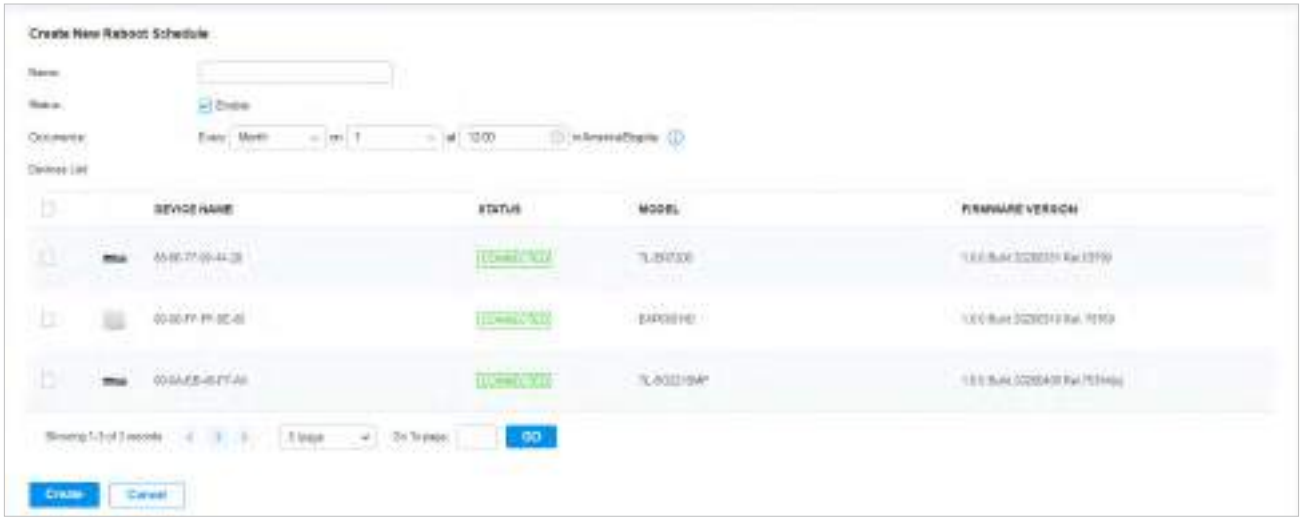
3. 10. 8 Program PoE

Prezentare generală

PoE Schedule poate face ca dispozitivele PoE care sunt conectate la comutatoarele dvs. PoE să se pornească și să funcționeze numai în perioada de timp specifică dorită. Puteți configura PoE Schedule în mod flexibil creând mai multe intrări PoE Schedule.

Configurare

1. Selectați un site din lista derulantă aOrganizare. Mergi laSetări>Servicii>Programul de repornire. Clic+ Creați un nou program de repornirepentru a încărca următoarea pagină și a configura parametrii.



Nume	Introduceți numele pentru a identifica intrarea Programului de repornire.
stare	Activați sau dezactivați intrarea Programul de repornire.
Apariția	Specificați data și ora pentru repornirea dispozitivelor.
Lista de dispozitive	Selectați dispozitivele cărora li se aplică Programul de repornire.

2. Faceți clicCrea. Noua intrare Program de repornire este adăugată la tabel. Puteți face clic pentru a edita intrarea. Puteți face clic pentru a șterge intrarea.

3. 10. 8 Program PoE

Prezentare generală

PoE Schedule poate face ca dispozitivele PoE care sunt conectate la comutatoarele dvs. PoE să se pornească și să funcționeze numai în perioada de timp specifică dorită. Puteți configura PoE Schedule în mod flexibil creând mai multe intrări PoE Schedule.

Configurare

1. Selectați un site din lista derulantă aOrganizare. Mergi laSetări>Servicii>Program PoE. Clic+ Creați un nou program PoEpentru a încărca următoarea pagină și a configura parametrii.

Nume	Introduceți numele pentru a identifica intrarea PoE Schedule.
stare	Activați sau dezactivați intrarea PoE Schedule.
Interval de timp	Selectați intervalul de timp când funcționează dispozitivele PoE. Puteți crea o intrare de interval de timp făcând clic+ Creați o nouă intrare în intervalul de timpdin lista derulantă a intervalului de timp. Pentru detalii, consultațiProfiluri.
Lista de dispozitive	Selectați comutatoarele PoE și porturile PoE cărora li se aplică Programul PoE. Dispozitivele dumneavoastră PoE conectate la porturile selectate ale comutatoarelor funcționează conform programului PoE.

2. Faceți clicCrea. Noua intrare PoE Schedule este adăugată la tabel. Puteți face clic pentru a edita intrarea. Puteți face clic pentru a șterge intrarea.

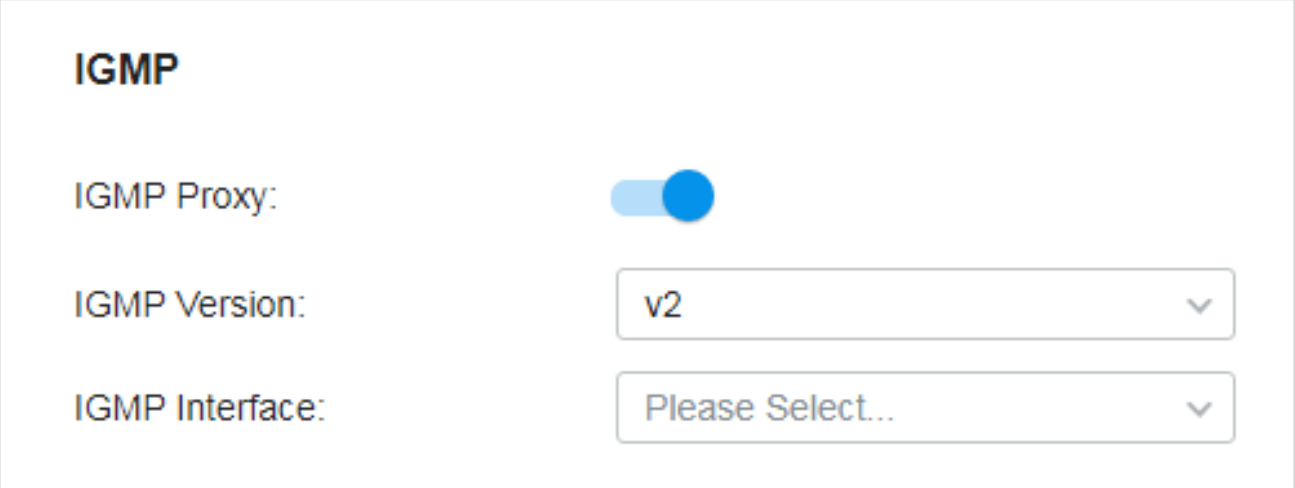
3. 10. 9 IPTV

Prezentare generală

IPTV include două secțiuni: IGMP și IPTV. În setările IGMP, puteți activa proxy-ul IGMP pentru a detecta informațiile despre apartenența la grupul multicast și astfel routerul poate redirecționa pachete multicast pe baza informațiilor. Setările IPTV vă permit să activați serviciul Internet/IPTV/Telefon oferit de ISP-ul dumneavoastră.

Configurare

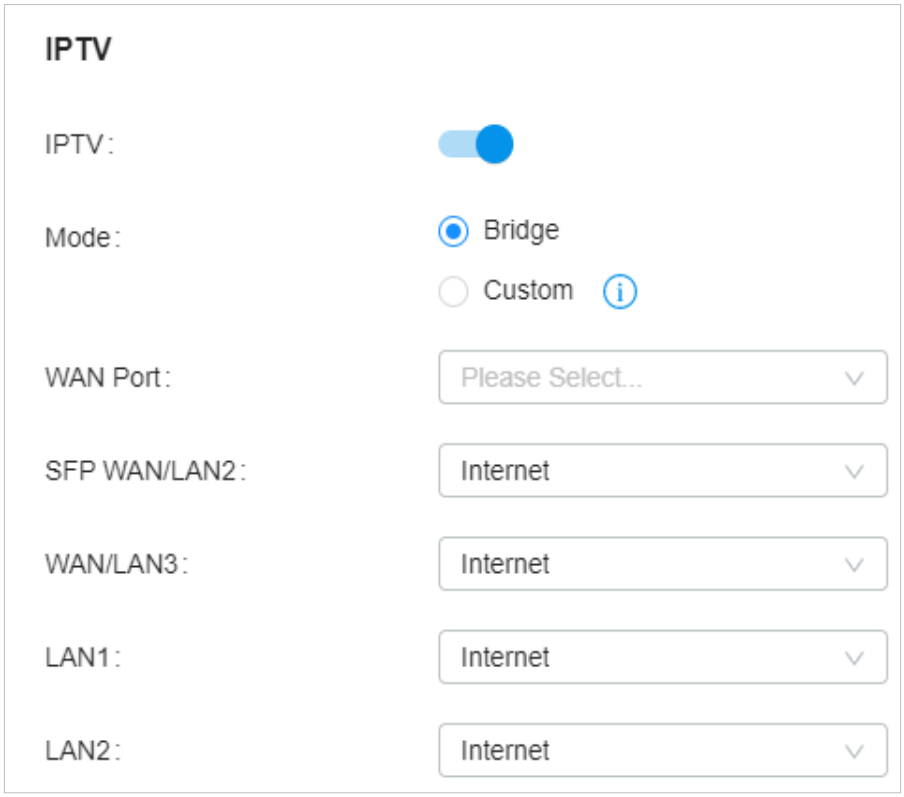
1. Selectați un site din lista derulantă aOrganizare. Mergi laSetări>Servicii>IPTV>IGMP, configurați parametrii. Dacă doriți să configurați setările IPTV, treceți la pasul următor; dacă nu doriți să configurați setările IPTV, faceți clic peAplica.



Proxy IGMP	Activați proxy IGMP. IGMP Proxy trimite pachete de interogare IGMP către porturile LAN pentru a detecta dacă există vreun membru multicast conectat la porturile LAN.
Versiunea IGMP	Selectați versiunea IGMP ca V2 sau V3. Valoarea implicită este IGMP V2.
Interfață IGMP	Selectați portul WAN pe care are efect proxy-ul IGMP.

2. AccesațiSetări>Servicii>IPTV>IPTV, activați funcțiile IPTV și alegeți modul Bridge sau Personalizat, în funcție de ISP-ul dvs. Apoi configurați parametrii corespunzători. Clicaplica.

Rețineți că secțiunea IPTV va fi ascunsă dacă dispozitivul dvs. este o versiune anterioară care nu acceptă această caracteristică.



IPTV	Activați funcția IPTV.
Modul	Selectați modul potrivit în funcție de ISP-ul dvs. Pod:Selectați acest mod dacă ISP-ul dvs. nu necesită alți parametri. Personalizat: Selectați acest mod dacă ISP-ul dumneavoastră furnizează parametrii necesari și configurați parametrii conform cerințelor ISP-ului dumneavoastră.
Port WAN	Selectați portul WAN pe care intră în vigoare setările IPTV.
Modul Port	Selectați modul de port corespunzător pentru a determina ce port este utilizat pentru a susține serviciul de Internet, serviciul IPTV sau serviciul IP Phone.

3. 10. 10 Program de actualizare

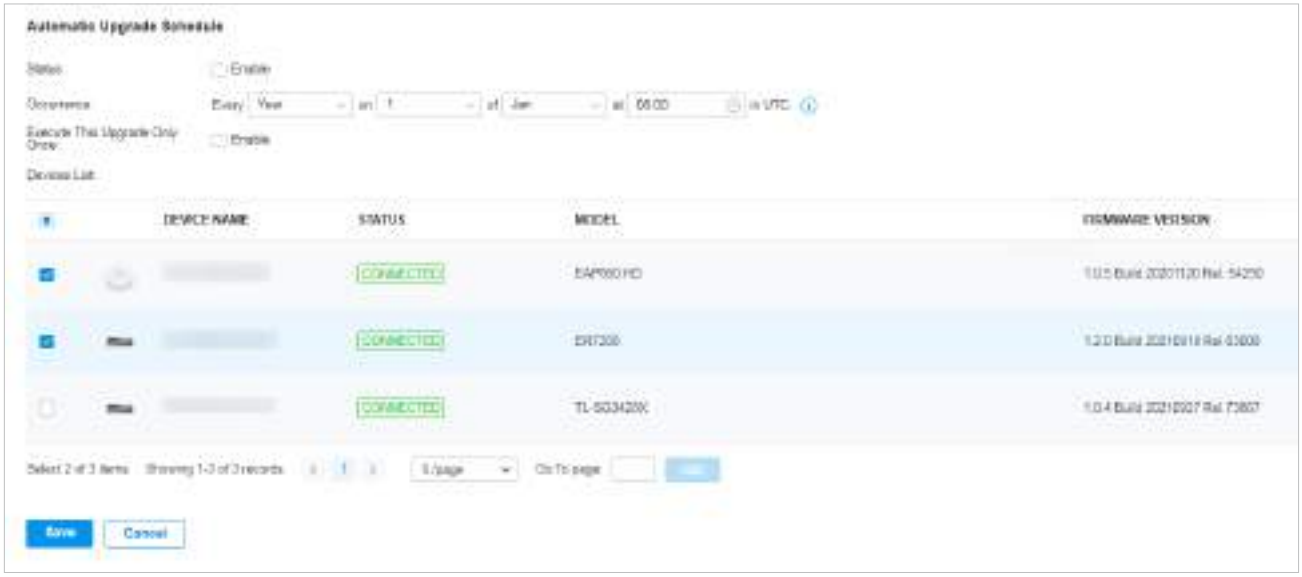
Prezentare generală

Upgrade Schedule vă permite să programați upgrade-ul dispozitivului după cum doriți. Puteți seta upgrade-uri recurente sau un program unic.

Configurare

Selectați un site din lista derulantă aOrganizare. Mergi laSetări>Servicii>Program de upgrade.

Setați programul de actualizare automată și selectați dispozitivele. ClicAplica.



stare	Activați sau dezactivați programul de actualizare.
Apariția	Specificați ora pentru upgrade automat.
Executați această actualizare Doar o data	Activați această opțiune dacă doriți să executați o singură dată programul setat.
Lista de dispozitive	Selectați dispozitivele care vor face upgrade conform programului stabilit.

3. 10. 11 Export date

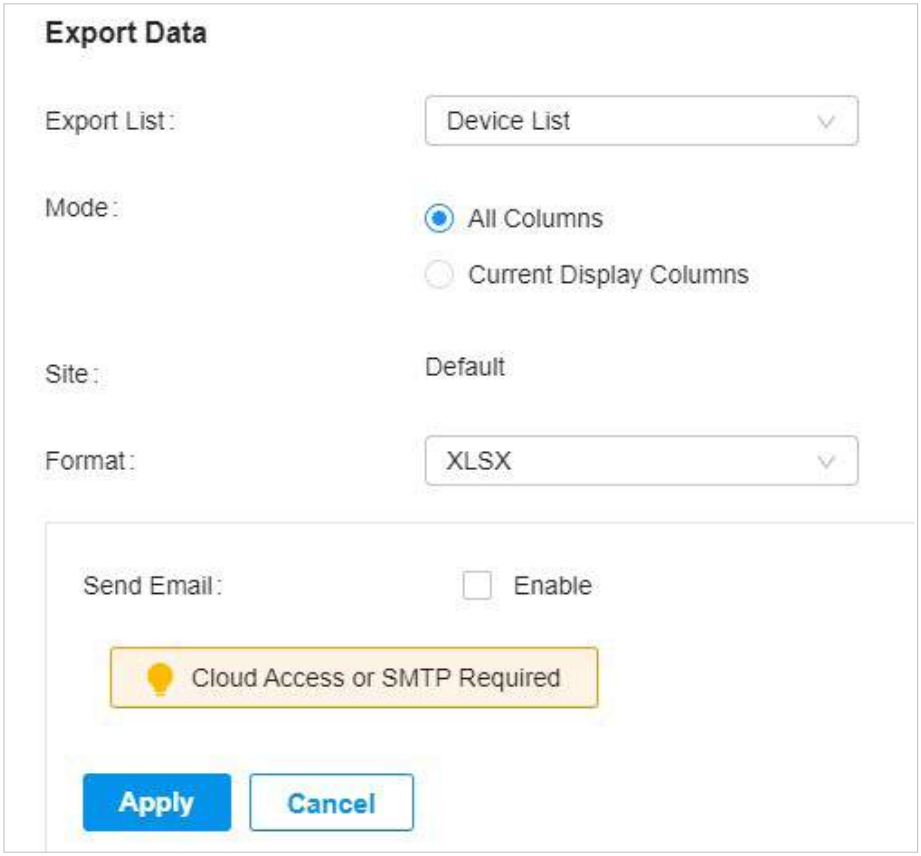
Prezentare generală

Puteți exporta date pentru a vă monitoriza sau depana dispozitivele.

Configurare

1. SelectațiVedere globalădin lista derulantă aOrganizare. Dacă doriți să exportați datele unui singur site, puteți selecta și site-ul pentru a accesa vizualizarea site-ului.

2. AccesațiSetări>Servicii>Export de date. Selectați tipul de date din lista de export și faceți clic Export.



Lista de export	Lista de dispozitive: Exportați lista dispozitivelor gestionate. Lista de clienti: Exportați lista tuturor clienților care sunt conectați la rețele. Lista AP Insight-Rogue: Exportați lista AP-urilor necinstite scanate anterior. Pentru informații detaliate, consultați7. 5. 9 AP-uri necinstiți. Listă de jurnal: Exportați lista jurnalelor generate de controler. Lista de clienți autorizați: Exportați lista clienților autorizați. Coduri voucher: Exportați lista codurilor voucher.
Modul	Toate Coloanele: Exportați lista de date care conține toate coloanele. Coloane de afișare curente: Exportați lista de date care conține numai coloanele afișate în prezent.
Site	Alegeți site-urile, iar datele specificate ale site-ului ales vor fi exportate. Notă: În vizualizarea site-ului, numai datele site-ului curent pot fi exportate.
Format	Datele pot fi exportate în fișier în formatul .CSV sau .XLSX.

Trimite email	Dacă doriți să trimiteți datele exportate prin e-mail, activați Trimitere e-mail și configurați parametrii de mai jos: Numele raportului: specificați numele raportului e-mailului de trimis. Apariția: Specificați când să trimiteți e-mailul. Trimite catre: Specificați adresele de e-mail la care să trimiteți datele exportate.

Configurați controlerul Omada SDN

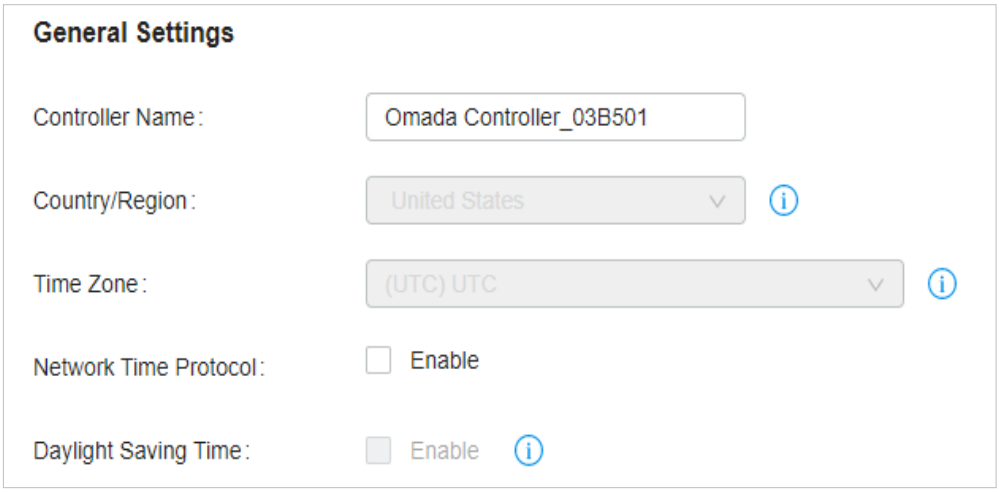
Setările controlerului controlează aspectul și comportamentul controlerului și oferă metode de backup, restaurare și migrare a datelor:

4. 1 Gestionați controlerul

4. 1. 1 Setări generale

Configurare

Selectați Global din lista derulantă aOrganizareîn colțul din dreapta sus. Mergi laSetări> Setări controler. Însetari generale, configurați parametrii și faceți clicSalvați.



Numele controlerului	Specificați un nume pentru a identifica controlerul.
Fus orar	Pentru setările și statisticile controlerului, ora este afișată pe baza fusului orar. Setările de fus orar ale acestui controler sunt aceleași cu cele ale site-ului implicit.
Network Time Protocol	Activați și introduceți adresa(ele) IP ale serverului NTP (Network Time Protocol). Serverul NTP atribuie ora rețelei dispozitivelor EAP și controlerului.
Ora de vară	Setările pentru ora de vară ale acestui controler sunt aceleași cu cele ale site-ului implicit.

4. 1. 2 Capacitatea controlerului

Selectați Global din lista derulantă aOrganizareîn colțul din dreapta sus. Mergi laSetări> Setări controler. În Capacitatea controlerului, verificați numărul de dispozitive pe care controlerul le gestionează și cantitatea maximă de dispozitive pe care controlerul le poate gestiona.

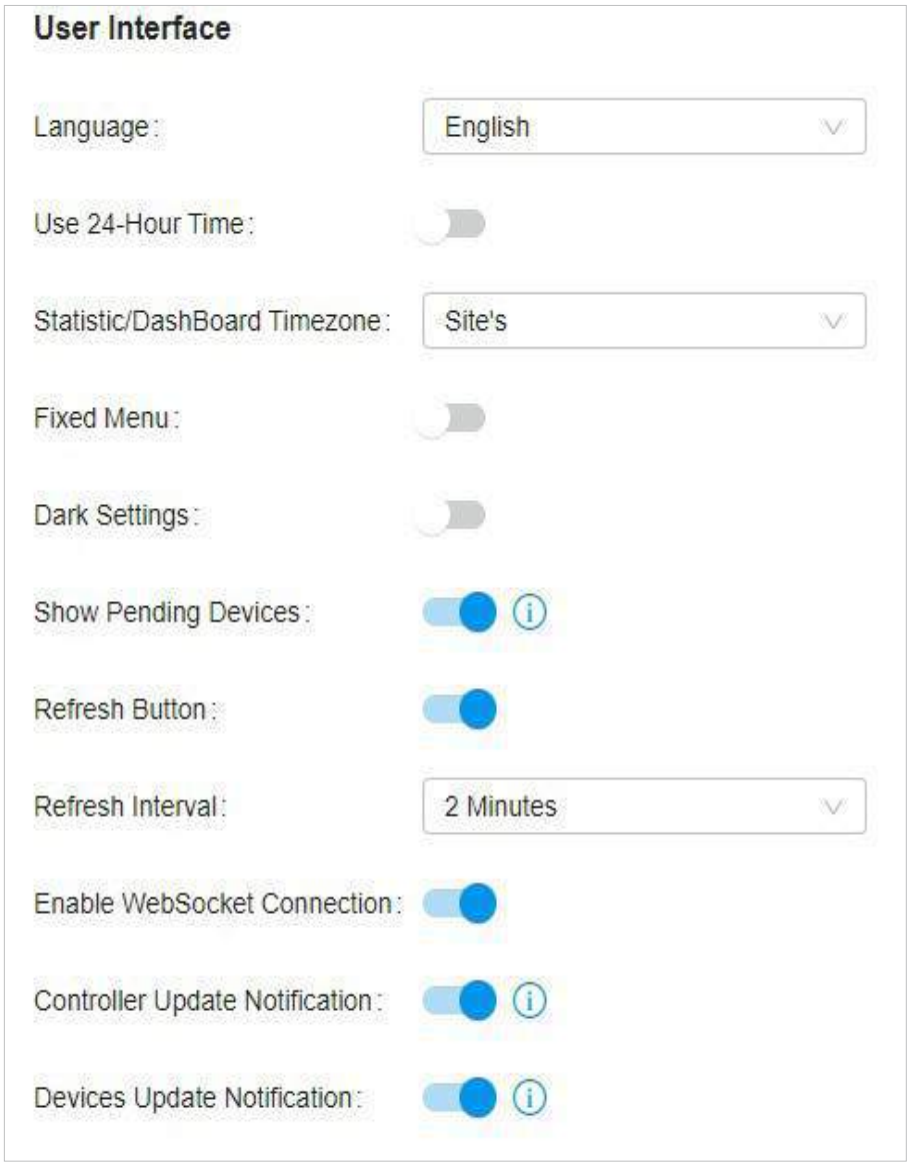
4. 1. 3 Interfata utilizator

Prezentare generală

În Interfața cu utilizatorul, puteți activa funcțiile sau puteți selecta modul preferat pentru interfața cu utilizatorul a controlerului.

Configurare

Selectați Global din lista derulantă aOrganizareîn colțul din dreapta sus. Mergi laSetări> Setări controler. ÎnInterfața cu utilizatorul, configurați parametrii și faceți clicSalvațiÎn josul paginii.



Limba	Selectați limba pentru a afișa paginile.
Utilizați 24 de ore	Cu Utilizarea orei de 24 de ore activată, ora este afișată într-un format de 24 de ore. Cu utilizarea timpului de 24 de ore dezactivată, ora este afișată într-un format de 12 ore.

Statistică/Fus orar al tabloului de bord	Selectați pe ce fus orar se bazează ora statisticilor și tabloul de bord. Site-uri: Fusul orar al site-ului este setat în Configurarea site-ului site-ului corespunzător. Browser-ul: fusul orar al browserului este sincronizat cu configurația browserului. Controllerului: Fusul orar al controlerului este setat în Setările generale ale controlerului. UTC: UTC (Coordinated Universal Time) este standardul orar comun în întreaga lume.
Meniu fix	Cu meniul fix activat, pictogramele meniului sunt fixe și nu solicită texte de meniu atunci când mouse-ul trece pe ele.
Setări întunecate	Când este activat, sistemul va trece la o temă întunecată.
Afișați dispozitivele în așteptare	Cu această opțiune activată, dispozitivele în starea În așteptare vor fi afișate și puteți determina dacă să le adoptați. Cu această opțiune dezactivată, acestea nu vor fi afișate și, prin urmare, nu puteți adopta niciun dispozitiv nou.
Butonul de reîmprospătare	Cu această opțiune activată, butonul de reîmprospătare va fi afișat în colțul din dreapta sus al paginii de configurare.
Interval de reîmprospătare	Selectați cât de des controlerul reîmprospătează automat datele afișate pe pagină.
E enable We b Socket Connection	Cu această opțiune activată, controlerul își actualizează o parte din datele de pe interfața web în timp real, care sunt transmise folosind serviciul WebSocket, astfel încât să nu fie nevoie să le reîmprospătați manual.
Notificare de actualizare a controlorului	Cu Notificarea de actualizare a controlerului activată, controlerul va solicita în cloud actualizări de firmware ale controlerului.
Dispozitivele Actualizați Notificare	Cu Programul de actualizare/Notificarea actualizării dispozitivelor activată, controlerul va solicita în cloud actualizări de firmware ale dispozitivului.

4. 1. 4 Server de e-mail

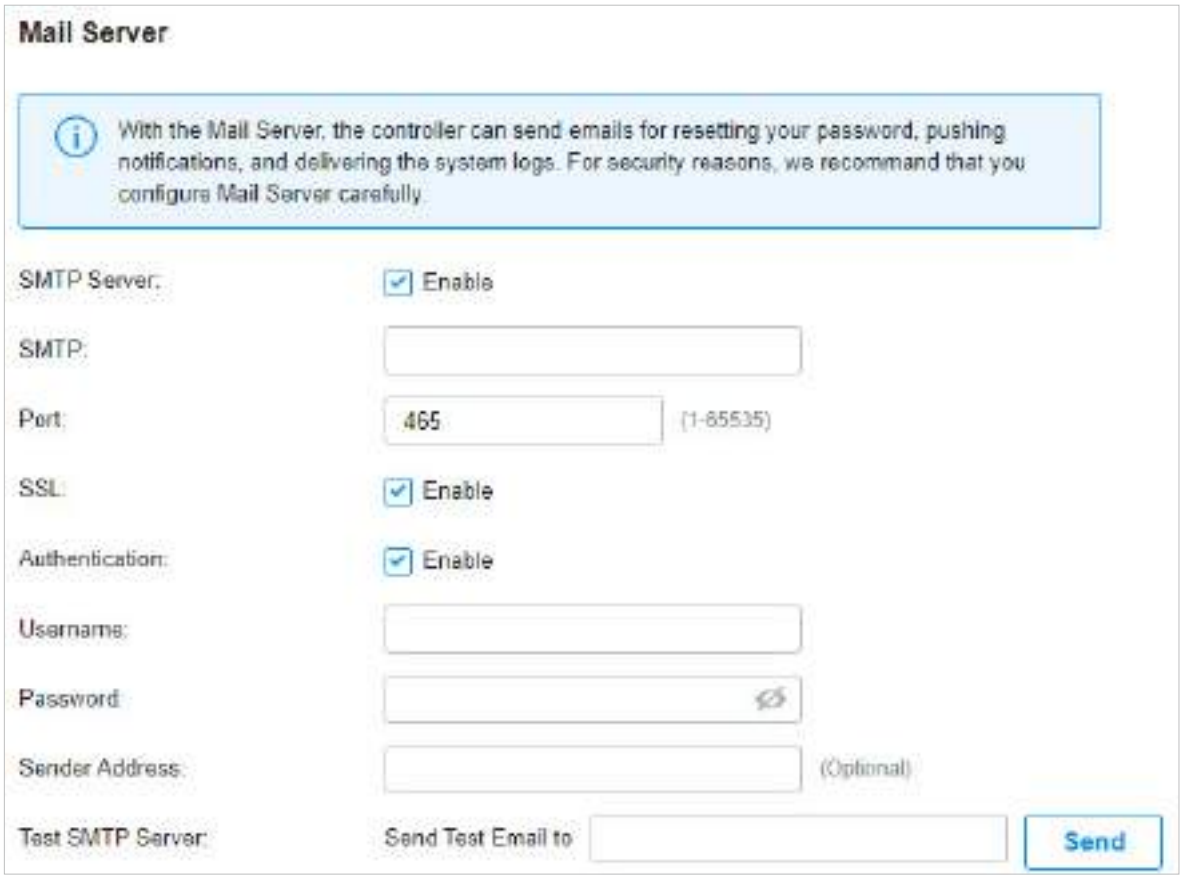
Prezentare generală

Cu serverul de e-mail, controlerul poate trimite e-mailuri pentru resetarea parolei, trimiterea de notificări și livrarea jurnalelor de sistem. Caracteristica Mail Server funcționează cu serviciul SMTP (Simple Mail Transfer Protocol) oferit de un furnizor de servicii de e-mail.

Configurare

1. Conectați-vă la contul dvs. de e-mail și activați serviciul SMTP (Simple Mail Transfer Protocol). Pentru detalii, consultați instrucțiunile furnizorului dvs. de servicii de e-mail.

2. Selectați Global din lista derulantă aOrganizareîn colțul din dreapta sus. Mergi laSetări> Setări controler. ÎnServer de e-mail, activați Serverul SMTP și configurați parametrii. Apoi apasa Salvați.



SMTP	Introduceți adresa URL sau adresa IP a serverului SMTP conform instrucțiunilor furnizorului de servicii de e-mail.
Port	Configurați portul utilizat de serverul SMTP conform instrucțiunilor furnizorului de servicii de e-mail.
SSL	Activați sau dezactivați SSL conform instrucțiunilor furnizorului de servicii de e-mail. SSL (Secure Sockets Layer) este folosit pentru a crea o legătură criptată între controler și serverul SMTP.
Autentificare	Activați sau dezactivați autentificarea conform instrucțiunilor furnizorului de servicii de e-mail. Dacă autentificarea este activată, serverul SMTP necesită numele de utilizator și parola pentru autentificare.
Nume de utilizator	Când autentificarea este activată, introduceți adresa dvs. de e-mail ca nume de utilizator.
Parola	Când autentificarea este activată, introduceți codul de autentificare ca parolă, care este furnizat de furnizorul de servicii de e-mail când activați serviciul SMTP.
Adresa expeditorului	(Opțional) Specificați adresa expeditorului e-mailului. Dacă îl lăsați necompletat, controlerul vă folosește adresa de e-mail ca adresă expeditorului.

Testați serverul SMTP	Testați configurația serverului de e-mail trimițând un e-mail de test la o adresă de e-mail pe care o specificați.

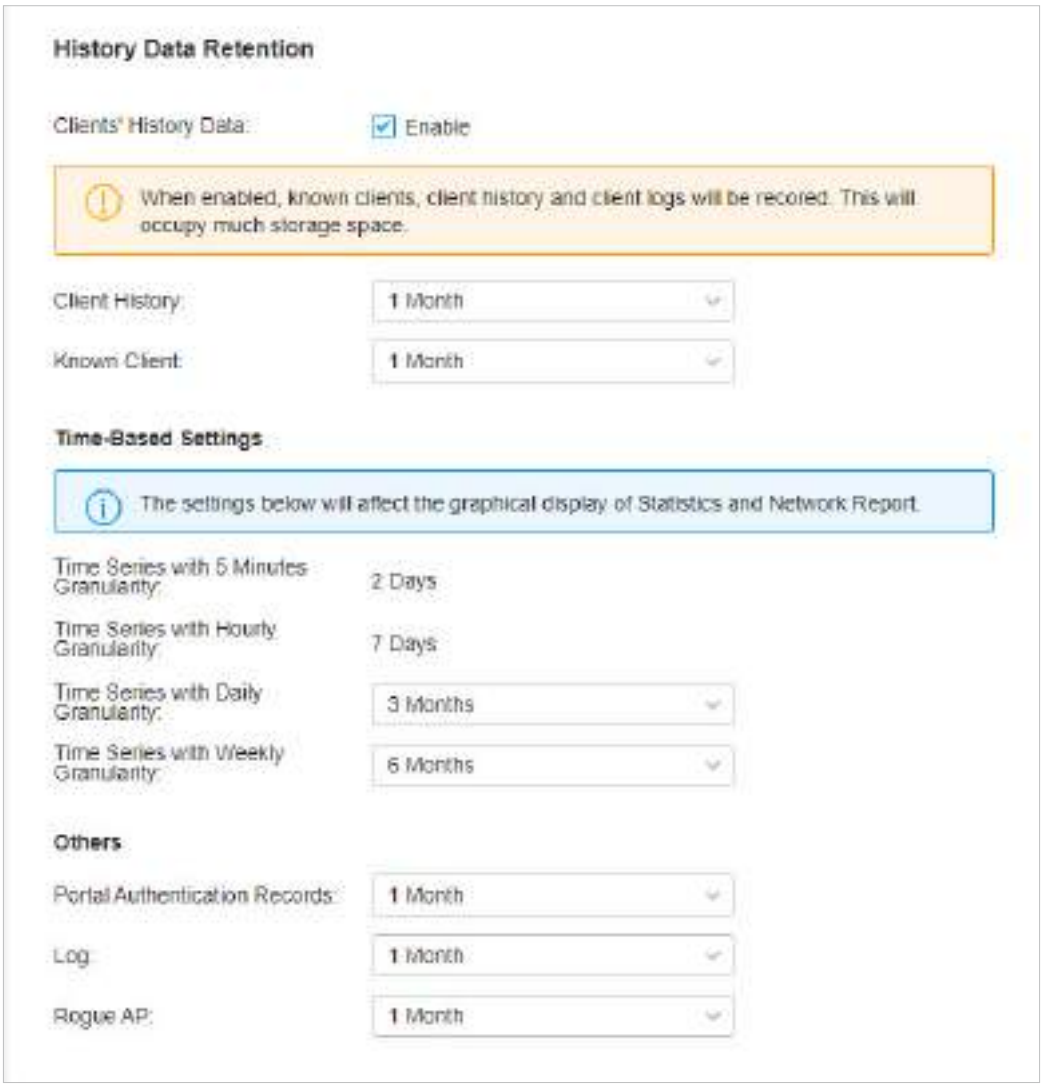
4. 1. 5 Istoric Păstrarea datelor

Prezentare generală

Cu reținerea datelor istorice, puteți specifica modul în care operatorul își păstrează datele.

Configurare

Selectați Global din lista derulantă aOrganizareîn colțul din dreapta sus. Mergi laSetări> Setări controler. ÎnPăstrarea datelor istorice, configurați parametrii și faceți clicSalvați.



Datele istorice ale clienților	Când este activat, clienții cunoscuți, istoricul clienților și jurnalele clienților vor fi înregistrați. Acest lucru va ocupa mult spațiu de stocare.

Istoricul clientului	Specificați timpul de păstrare a înregistrărilor clienților online și offline. Corespunzător conexiunii Insight-Past.
Client cunoscut	Specificați timpul de păstrare a datelor cunoscute despre client. Corespunzător clienților Insight-Known.
Serii temporale cu granularitate de 5 minute	Afișează timpul de păstrare al datelor AP, switch, gateway și client. Corespunzător statisticilor de 5 minute.
Serii temporale cu granularitate orară	Afișează timpul de păstrare al datelor AP, switch, gateway și client. Corespunzător statisticilor orare.
Serii temporale cu granularitate zilnică	Specificați timpul de păstrare al datelor AP, switch, gateway și client. Corespunzător statisticilor zilnice.
Serii temporale cu granularitate săptămânală	Specificați timpul de păstrare a datelor clientului. Corespunzător statisticilor săptămânale.
Autentificare portal Înregistrări	Specificați timpul de păstrare a înregistrărilor de autorizare a portalului. Corespunzător Autorizării Portal Insight-Past.
Buturuga	Specificați timpul de păstrare a jurnalelor.
Rogue AP	Specificați timpul de reținere al AP-urilor Rogue scanate. Corespunzător AP-urilor Insight-Rogue.

4. 1. 6 Alăturați-vă programului de îmbunătățire a experienței utilizatorului

Configurare

Faceți clic pe caseta de selectare dacă sunteți de acord să participați la programul de îmbunătățire a experienței utilizatorului și să ajutați la îmbunătățirea calității și a performanței produselor TP-Link prin trimiterea de statistici și informații de utilizare.

4. 1. 7 Stare controler

Selectați Global din lista derulantă aOrganizareîn colțul din dreapta sus. Mergi laSetări>Setarile sistemului. ÎnStarea controlerului, puteți vizualiza informațiile și starea controlerului.

Numele controlerului	Afișează numele controlerului, care îl identifică. Puteți specifica numele controlerului în4. 1. 1 Setări generale.
Adresa mac	Afișează adresa MAC a controlerului.
Timpul sistemului	Afișează ora de sistem a controlerului. Ora sistemului se bazează pe fusul orar.
Timp de funcționare	Afișează cât timp a funcționat controlerul.
Versiunea controlerului	Afișează versiunea software a controlerului.
Model	Afișează modelul controlerului.
Versiunea softului	Afișează versiunea de firmware a controlerului.
Stocare internă	Afișează stocarea internă a controlerului.

4. 1. 8 Certificat HTTPS

Prezentare generală

Dacă ați atribuit controlorului un nume de domeniu pentru autentificare, pentru a elimina mesajul de eroare „certificat neîncrezut” care va apărea în procesul de conectare, puteți importa aici certificatul SSL și cheia privată corespunzătoare. Certificatul și cheia privată sunt emise de autoritatea de certificare.

Notă:

- Trebuie să reporniți controlerul pentru ca certificatul SSL importat să intre în vigoare.

Configurare

Selectați Global din lista derulantă aOrganizareîn colțul din dreapta sus. Mergi laSetări>Setarile sistemului. ÎnCertificat HTTPS, selectați formatul de fișier, importați certificatul SSL și configurați parametrii. Apoi apasaSalvați.

Tipul fisierului	Selectați formatul certificatului dvs. și importați fișierul certificatului.
Parola pentru depozitul de chei	(Pentru JKS) Introduceți parola depozitului de chei dacă certificatul dvs. SSL are parola depozitului de chei. În caz contrar, lăsați-l necompletat.
Parolă cheie privată	(Pentru PFX) Introduceți parola cheii private dacă certificatul dvs. SSL are parola cheii private. În caz contrar, lăsați-l necompletat.

Notă:

Pentru certificatul format PEM:

- Începe cu: -----BEGIN CERTIFICAT-----
- Se termină cu: -----CERTIFICAT DE sfârșit-----
- Lanțul de certificate este acceptat și nu este permisă nicio linie goală între două lanțuri de certificate.

Pentru cheia formatată în PEM:

- Este necesară criptarea RSA.
- Începe cu: -----BEGIN RSA PRIVATE KEY-----
- Se termină cu: -----END RSA PRIVATE KEY -----
- Cheia poate fi plasată în spatele fișierului de certificat și pot fi importate împreună.

4. 1. 9 Accesați Config

Prezentare generală

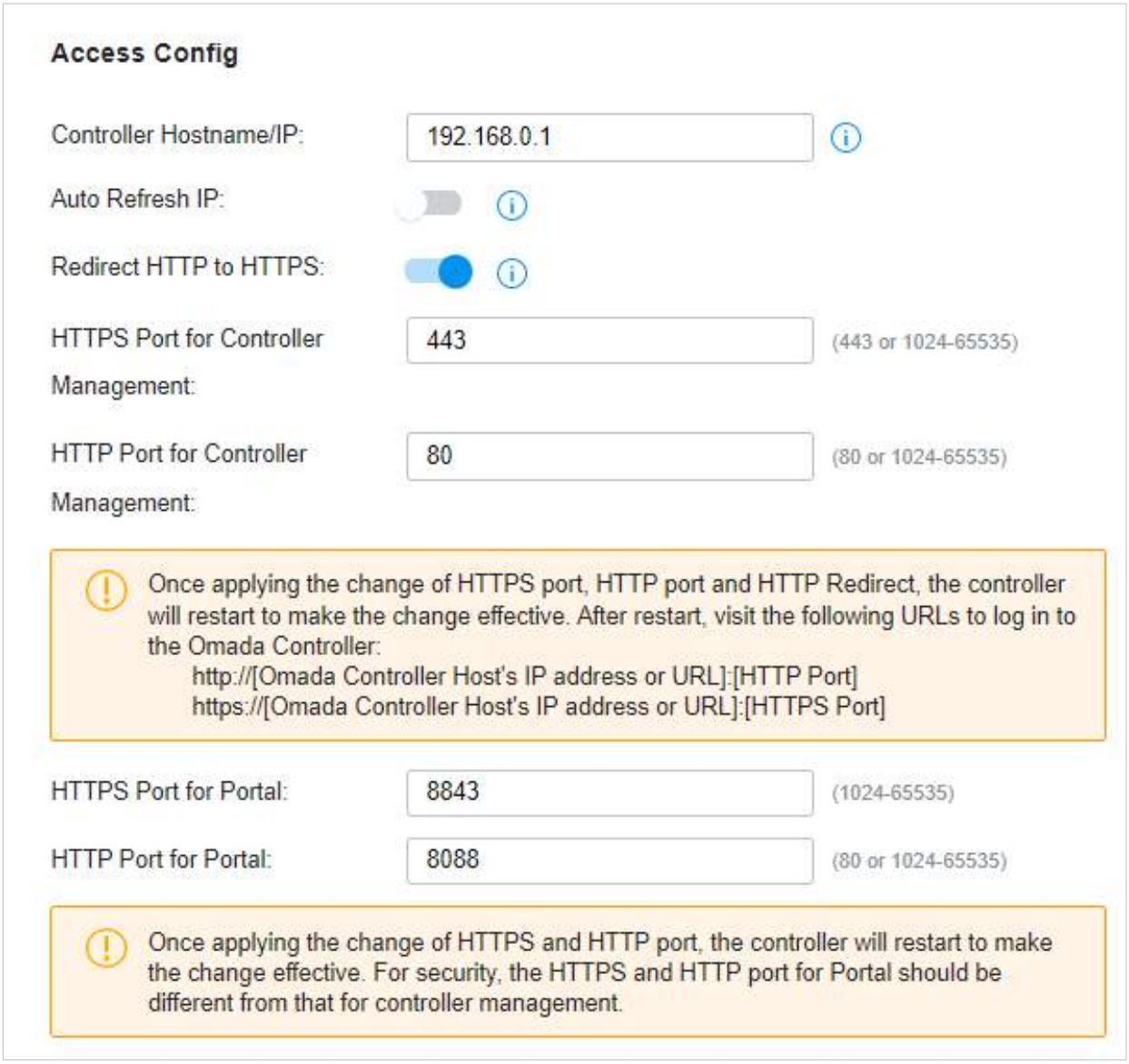
Cu Access Config, puteți specifica portul folosit de controler pentru management și portal.

Notă:

- Odată aplicată modificarea HTTPS și a portului HTTP, reporniți controlerul pentru ca modificarea să fie efectivă.
- Pentru securitate, portul HTTPS și HTTP pentru Potal ar trebui să fie diferit de cel pentru gestionarea controlerului.

Configurare

Selectați Global din lista derulantă aOrganizareîn colțul din dreapta sus. Mergi laSetări>Setarile sistemului. ÎnAccesați Config, configurați parametrii și faceți clicSalvați.



Nume gazdă/IP controler	Introduceți numele de gazdă sau adresa IP a controlerului, care va fi folosită ca URL a controlerului în e-mailul de notificare pentru resetarea parolei controlerului. Îl puteți păstra implicit și adresa IP recunoscută de controler va fi folosită ca URL a controlorului.
Reîmprospătare automată IP	Activați funcția și controlerul își va reîmprospăta adresa IP automat.
Redirecționare HTTP către HTTPS	Cu această opțiune activată, solicitările HTTP vor fi redirecționate către conexiuni HTTPS.
Port HTTPS pentru managementul controlerului	Specificați portul HTTPS utilizat de controler pentru gestionare. După setarea portului, puteți vizita https://[Adresa IP sau URL a gazdei Controller Omada]:[Port HTTPS] pentru a vă conecta la Controlerul Omada.

Port HTTP pentru managementul controlerului	Specificați portul HTTP utilizat de controler pentru gestionare. După setarea portului, puteți accesa https://[Adresa IP sau URL a gazdei Controller Omada]:[Port HTTP] pentru a vă conecta la Controlerul Omada.
Port HTTPS pentru portal	Specificați portul HTTPS utilizat de controler pentru Portal.
Port HTTP pentru portal	Specificați portul HTTP utilizat de controler pentru Portal.

4. 1. 10 Router integrat

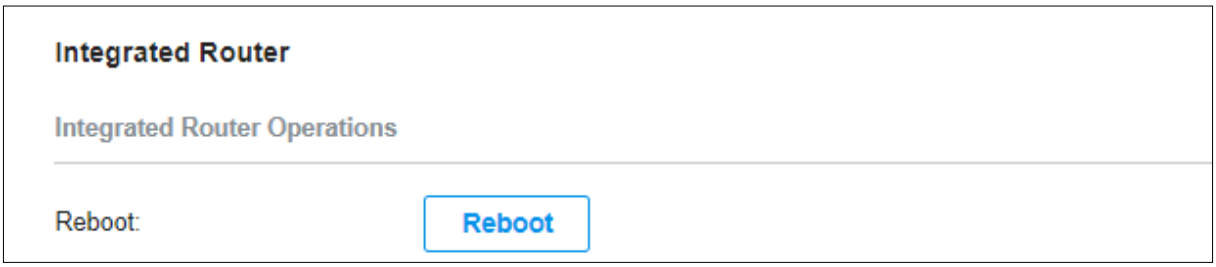
Prezentare generală

Puteți face configurații pentru routerul integrat (acest controler), inclusiv repornirea, resetarea și actualizarea firmware-ului routerului integrat.

Configurare

- Reporniți

Selectați Global din lista derulantă aOrganizareîn colțul din dreapta sus. Mergi laSetări>Setarile sistemului>Router integrat>Operații de router integrate. ClicReporniți și urmați instrucțiunile pentru a reporni routerul integrat. Repornirea poate dura câteva minute, vă rugăm să așteptați fără nicio operațiune.



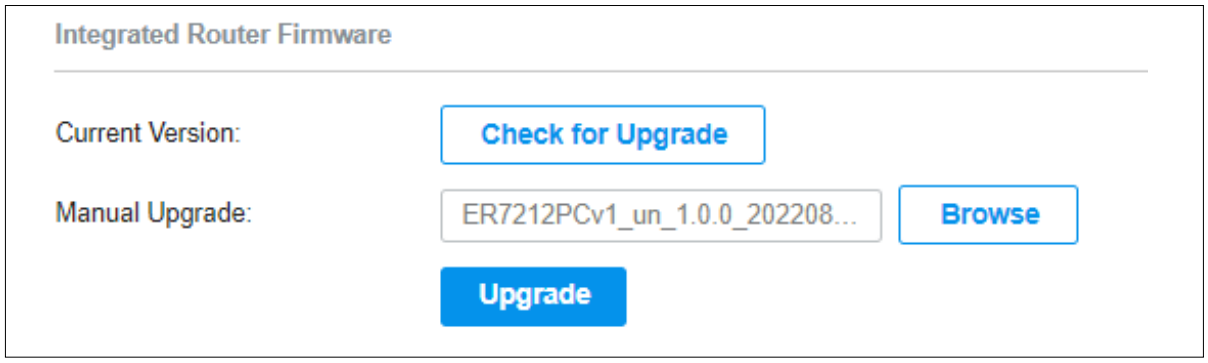
- Resetare din fabrică

Selectați Global din lista derulantă aOrganizareîn colțul din dreapta sus. Mergi laSetări>Setarile sistemului>Router integrat>Operații de router integrate. ClicResetare din fabrică și urmați instrucțiunile pentru a restabili routerul integrat la setările implicite din fabrică. Resetarea poate dura câteva minute, vă rugăm să așteptați fără nicio operațiune.

- Upgrade de firmware

Selectați Global din lista derulantă aOrganizareîn colțul din dreapta sus. Mergi laSetări>Setarile sistemului>Router integrat>Firmware pentru router integrat. ClicVerificați pentru Upgradepentru a vizualiza curentul

versiunea de firmware și pentru a verifica dacă trebuie să fie actualizat. Pentru a actualiza firmware-ul, faceți clic peNaviga, selectați un fișier firmware și faceți clicActualizare.



4. 2 Gestionați controlerul de la distanță prin CloudAccess

Prezentare generală

Cu Cloud Access, vă este convenabil să vă gestionați controlerul de oriunde.

Configurare

■ Permite legarea de la distanță

Notă:

- Înainte de a începe, asigurați-vă că controlerul a fost configurat cu succes și că poate accesa internetul.

1)SelectațiGlobaldin lista derulantă aOrganizareîn colțul din dreapta sus. Mergi laSetări> Acces la cloud .

2)PermitePermite legarea de la distanțăpentru controlor.

3)Mergi lahttps://omada.tplinkcloud.comși conectați-vă cu ID-ul și parola TP-Link, faceți clic pe +Add Controller și urmați instrucțiunile pentru a adăuga controlerul în Omada Cloud.

■ Acces la cloud

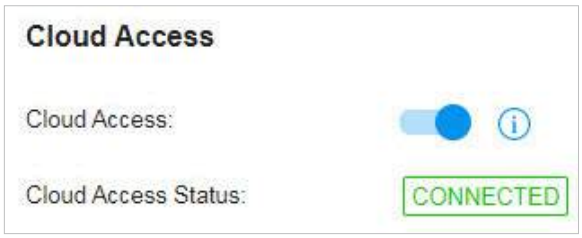
1. Pregătiți-vă controlerul pentru Cloud Access.

Notă:

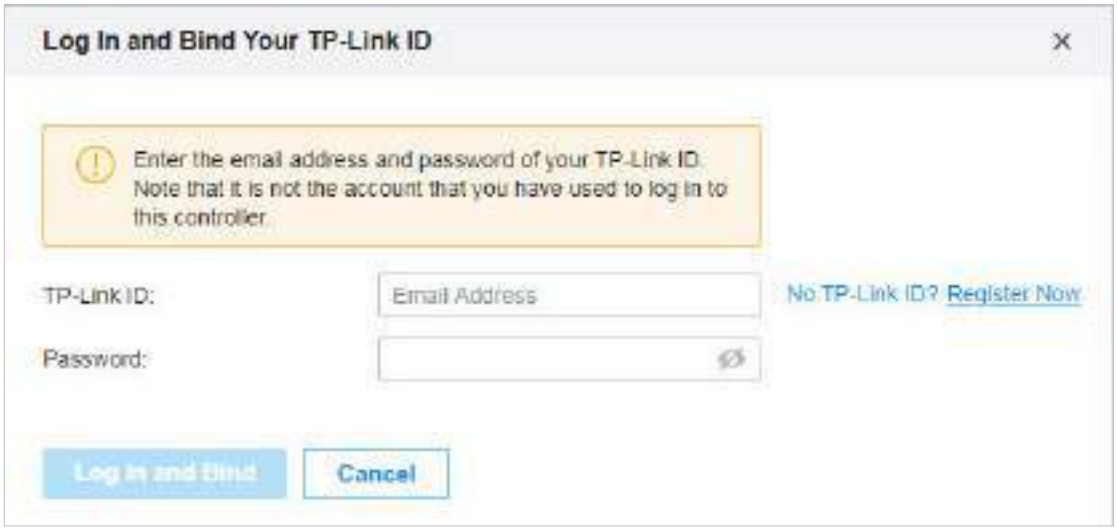
- Înainte de a începe, asigurați-vă că controlerul are acces la internet.
- Dacă ați activat accesul la cloud și ați legat ID-ul TP-Link în asistentul de configurare rapidă, săriți peste acest pas.

1)SelectațiGlobaldin lista derulantă aOrganizareîn colțul din dreapta sus. Mergi laSetări> Acces la cloud .

2)PermiteAcces la cloud.



3)Introduceți ID-ul și parola TP-Link. Apoi apasaConectați-vă și legați.



2. Accesați controlerul dvs. prin Serviciul Cloud

Mergi lahttps://omada.tplinkcloud.comși autentificați-vă cu ID-ul și parola TP-Link. Va apărea o listă de controlere care au fost legate cu ID-ul dvs. TP-Link. Apoi apasaLanuchpentru a gestiona controlerul.

4. 3 Întreținere

4. 3. 1 Backup & Restore

Prezentare generală

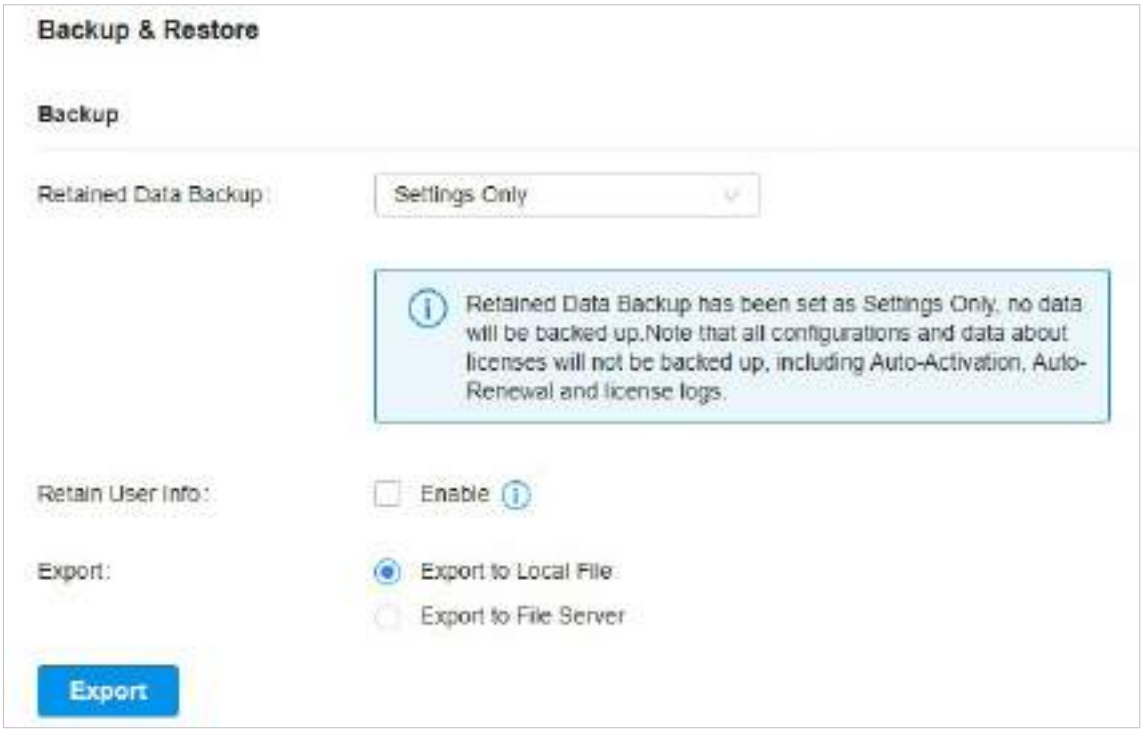
Puteți face backup pentru configurația și datele controlerului pentru a preveni orice pierdere de informații importante. Dacă este necesar, restaurați controlerul la o stare anterioară folosind fișierul de rezervă.

Configurare

■ Backup

Selectați Global din lista derulantă aOrganizareîn colțul din dreapta sus. Mergi laSetări> întreținere>Backup și restaurare>Backup, faceți clicExportpentru a exporta și salva fișierul de rezervă.

Dacă doriți să exportați datele pe un server de fișiere, configurați parametrii corespunzător și faceți clicExport.

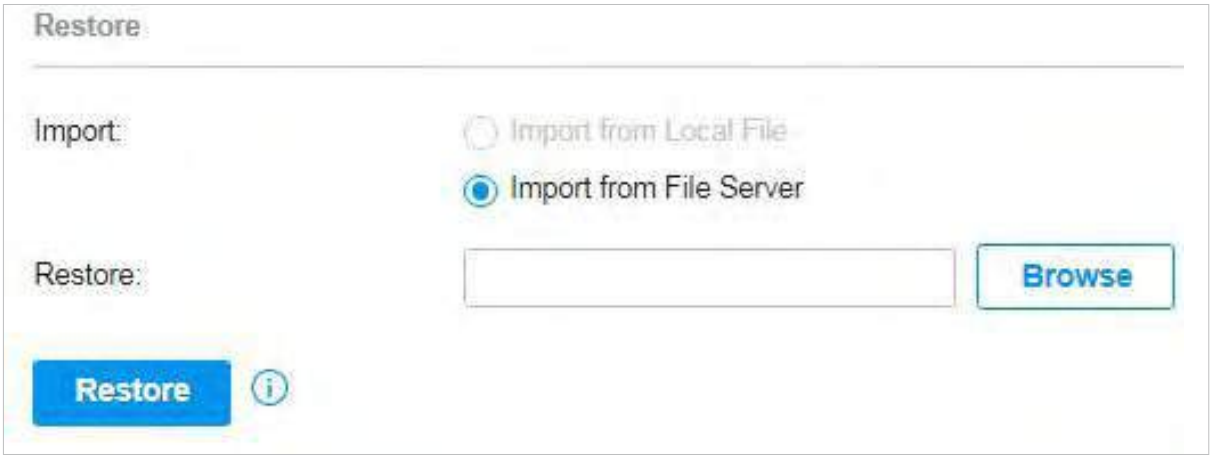


Backup de date reținute	Selectați intervalul de timp din meniul derulant al Backup-ului datelor reținute. Numai configurația și datele din intervalul de timp sunt salvate. Dacă selectați Numai setări, se face copii de rezervă numai pentru configurație (fără date).
Păstrați informațiile despre utilizator	Selectați această opțiune dacă doriți să păstrați informațiile despre utilizatorul local și din cloud.

Export	Selectați unde doriți să exportați datele. Exportați în fișierul local:Exportați și salvați datele local. Nu este acceptat la accesarea controlerului prin cloud. Exportați pe serverul de fișiere:Exportați și salvați datele pe un server de fișiere. Selectați tipul de server de fișiere dorit (FTP / TFTP / SFTP / SCP) și configurați parametrii.

■ Restabili

Mergi laSetări>întreținere>Backup și restaurare>Restabili. ÎnBackup și restauraresecțiune, faceți clicNaviga și selectați un fișier de rezervă de pe computer sau server de fișiere. ClicRestabili.



Import	Selectați unde stocați fișierul de restaurare. Import din fișierul local:Importați datele local. Nu este acceptat la accesarea controlerului prin cloud. Import de pe serverul de fișiere:Importați datele de pe un server de fișiere. Selectați tipul de server de fișiere dorit (FTP / TFTP / SFTP / SCP) și configurați parametrii.
Restabili	Selectați fișierul de rezervă pentru a restaura informațiile.

Notă:

- Un router integrat poate doar restaura fișierul de configurare al routerelor integrate.
- Gateway-ul se poate reporni dacă se modifică setările de internet. În acest caz, controlerul va fi inaccesibil până la repornirea gateway-ului.

4. 3. 2 Backup automat

Prezentare generală

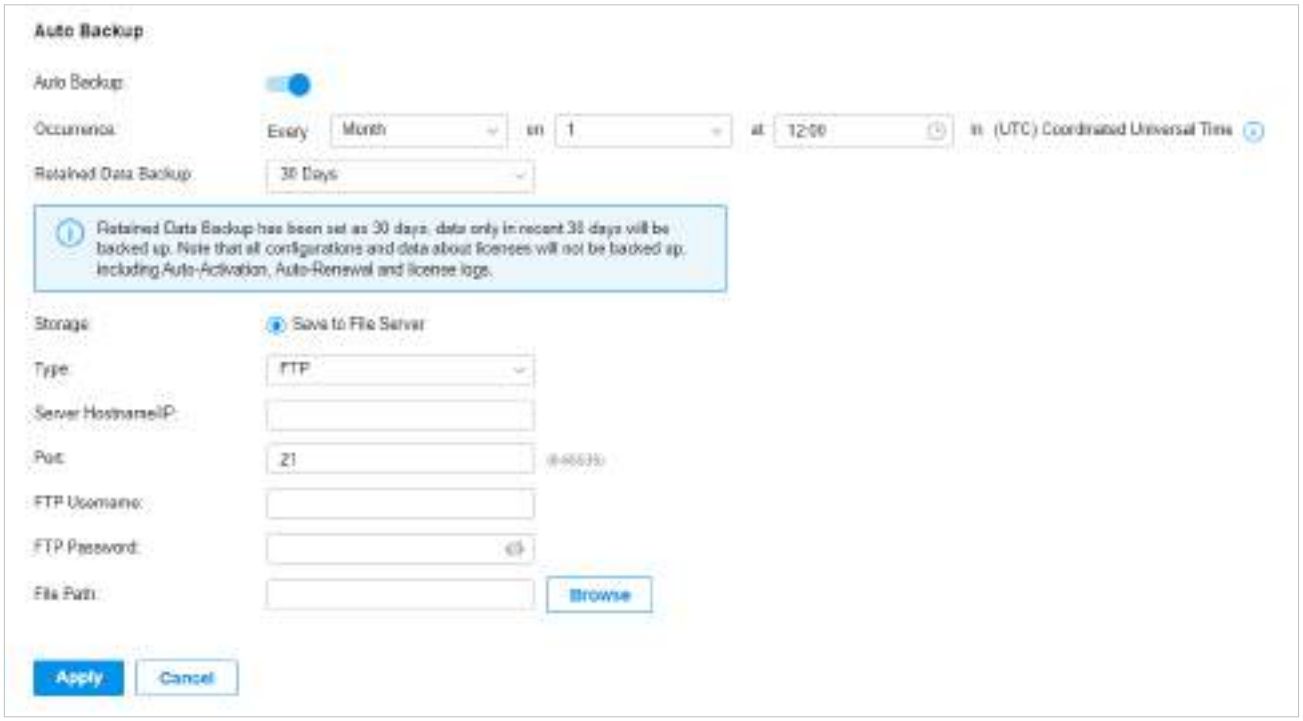
Cu Backup automat activat, controlerul va fi programat să facă backup automat pentru configurații și date, la ora specificată. Puteți restaura cu ușurință configurațiile și datele atunci când este necesar.

Configurare

Pentru a configura Backup automat, urmați acești pași:

1. Selectați Global din lista derulantă aOrganizareîn colțul din dreapta sus. Mergi laSetări> întreținere.ÎnCopie de siguranta automata. Faceți clic pentru a activa Backup automat.

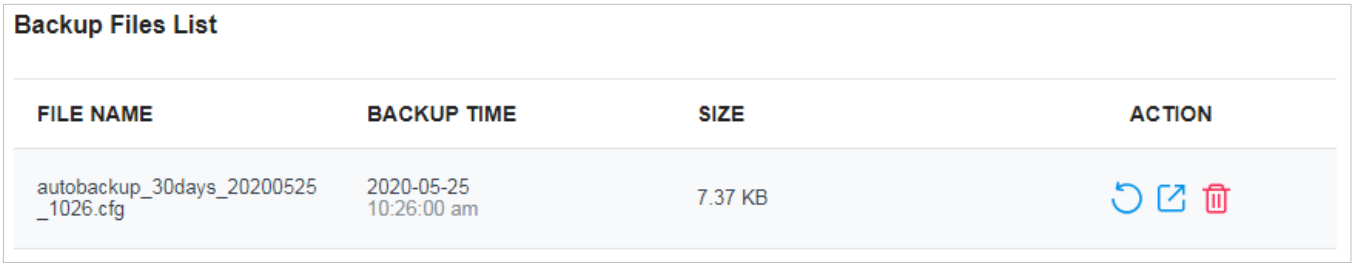
2. Configurați următorii parametri pentru a specifica regulile Auto Backup. Clicaplica.



Apariția	Specificați când să efectuați în mod regulat Backup automat. SelectațiÎn fiecare zi,Săptămână,Lună, sau Anmai întâi și apoi setați o oră pentru a face backup fișierelor. Rețineți disponibilitatea timpului atunci când alegețiIn fiecare luna. De exemplu, dacă alegeți să faceți o copie de rezervă automată a datelor în data de 31 a fiecărei luni, Backup automat nu va intra în vigoare atunci când vine vorba de luna fără 31, cum ar fi februarie, aprilie și iunie.
Backup de date reținute	Selectați perioada de timp în care se va face backup pentru datele. Numai setări: Faceți copii de rezervă numai pentru setările controlerului. 7 zile/30 de zile/60 de zile/90 de zile/180 de zile: Faceți o copie de rezervă a datelor din ultimele 7 zile/30 de zile/60 de zile/90 de zile/180 de zile.

Depozitare	Selectați unde doriți să salvați fișierul de rezervă. Salvare pe serverul de fișiere:Fișierul de rezervă va fi salvat pe serverul de fișiere specificat. Sunt disponibile patru tipuri de server de fișiere: FTP, TFTP, SFTP și SCP.

Puteți vizualiza numele, timpul de rezervă și dimensiunea fișierelor de rezervă înLista de fișiere de rezervă.



Pentru a restaura, exporta sau șterge fișierul de rezervă, faceți clic pe pictograma dinAcțiunecoloană.

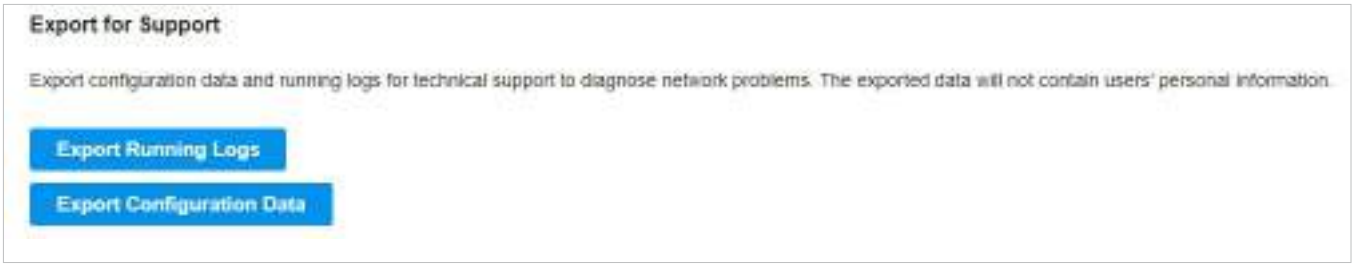
	Restaurați configurațiile și datele din fișierul de rezervă. Toate configurațiile curente vor fi înlocuite după restaurare. Pentru a păstra datele de rezervă în siguranță, așteptați până la finalizarea operațiunii. Acest lucru va dura câteva minute.
	Exportați fișierul de rezervă. Fișierul exportat va fi salvat în calea de salvare a browserului dvs. web.
	Ștergeți fișierul de rezervă.

Notă:

- Dacă fișierul de rezervă este salvat pe serverul de fișiere și este selectat tipul SCP / TFTP, acesta nu va fi inclus în Lista de fișiere de rezervă și nu poate fi exportat, restaurat sau șters.
- Pentru a face o copie de rezervă manuală a datelor și a restabili datele către controler, consultați4. 3. 1 Backup & Restorepentru a configura Backup & Restore.
- Configurația utilizatorilor cloud nu poate fi nici salvată, nici restaurată. Pentru a adăuga utilizatori cloud, vă rugăm să consultați8. 3 Gestionați și creați conturi de utilizator locale.

4. 3. 3 Export pentru asistență

Clic Export Running Logs sau Export Configuration Data pentru a exporta jurnalele de rulare sau datele de configurare pentru tehnice suport pentru diagnosticarea problemelor de rețea. Datele exportate nu vor conține informații personale ale utilizatorilor.



4. 4 Migrația

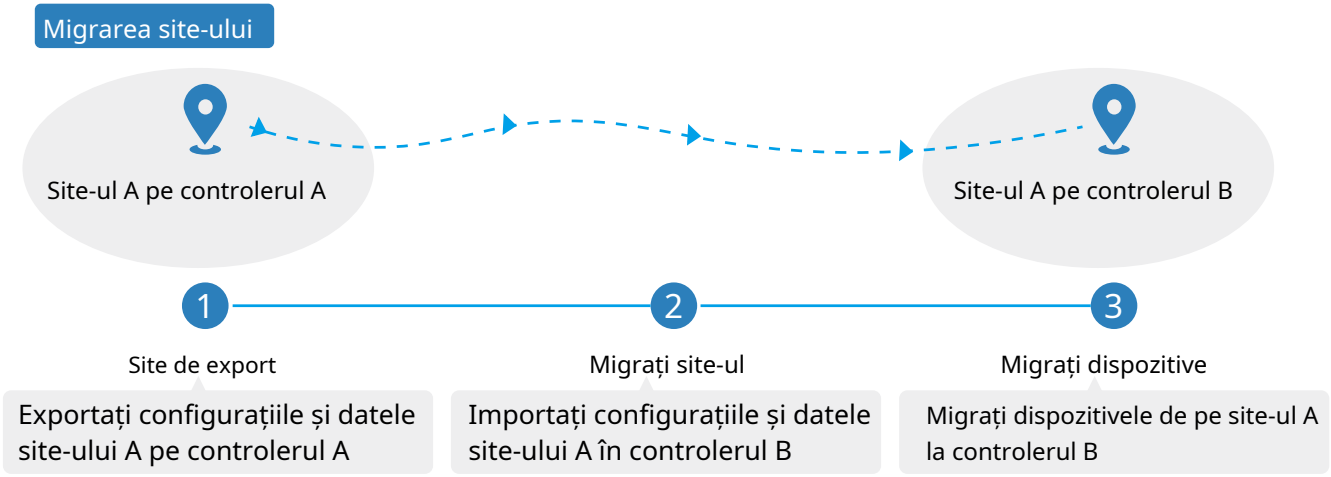
Serviciile de migrare permit utilizatorilor să migreze configurațiile și datele către orice alt controler. Serviciile de migrare includ4. 4. 1 Migrarea site-ului și4. 4. 2 Migrarea controlerului , acoperind toate nevoile de migrare atât a unui singur site, cât și a întregului controler.

4. 4. 1 Migrarea site-ului

Prezentare generală

Migrarea site-ului permite administratorilor să exporte un site de la controlerul actual la orice alt controler care are aceeași versiune. Toate configurațiile și datele site-ului vor fi migrate către controlerul țintă.

Procesul de migrare a configurațiilor și a datelor de la un site la un alt controlor poate fi rezumat în trei pași: Export Site, Migrate Site și Migrate Devices.



Pasul 1: Exportați site-ul

Exportați configurațiile și datele site-ului de migrat ca fișier de rezervă.

Pasul 2: Migrați site-ul

În controlerul țintă, importați fișierul de rezervă al site-ului original.

Pasul 3: Migrați dispozitivele

Migrați dispozitivele care se află pe site-ul original la controlerul țintă.

Configurare

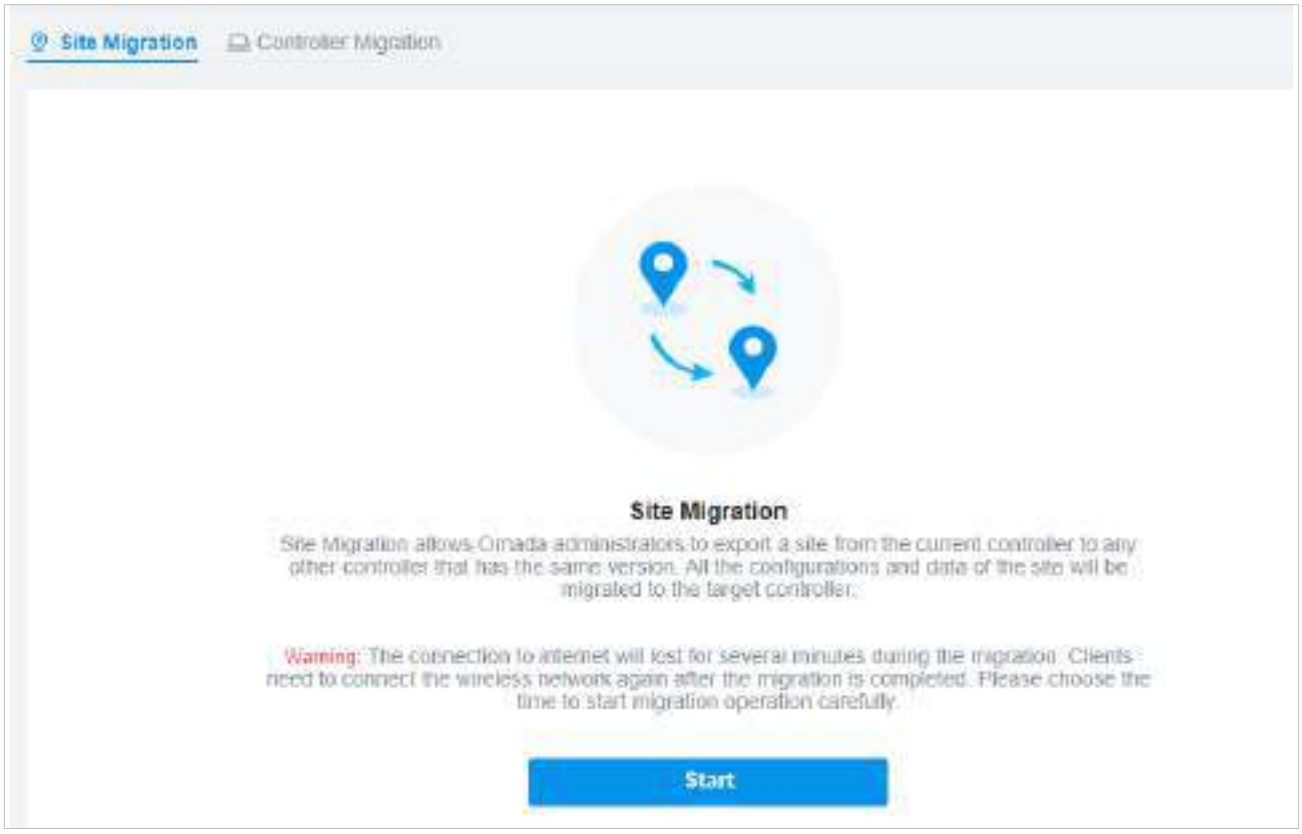
Pentru a migra un site la un controler anther, urmați acești pași de mai jos.

Notă:

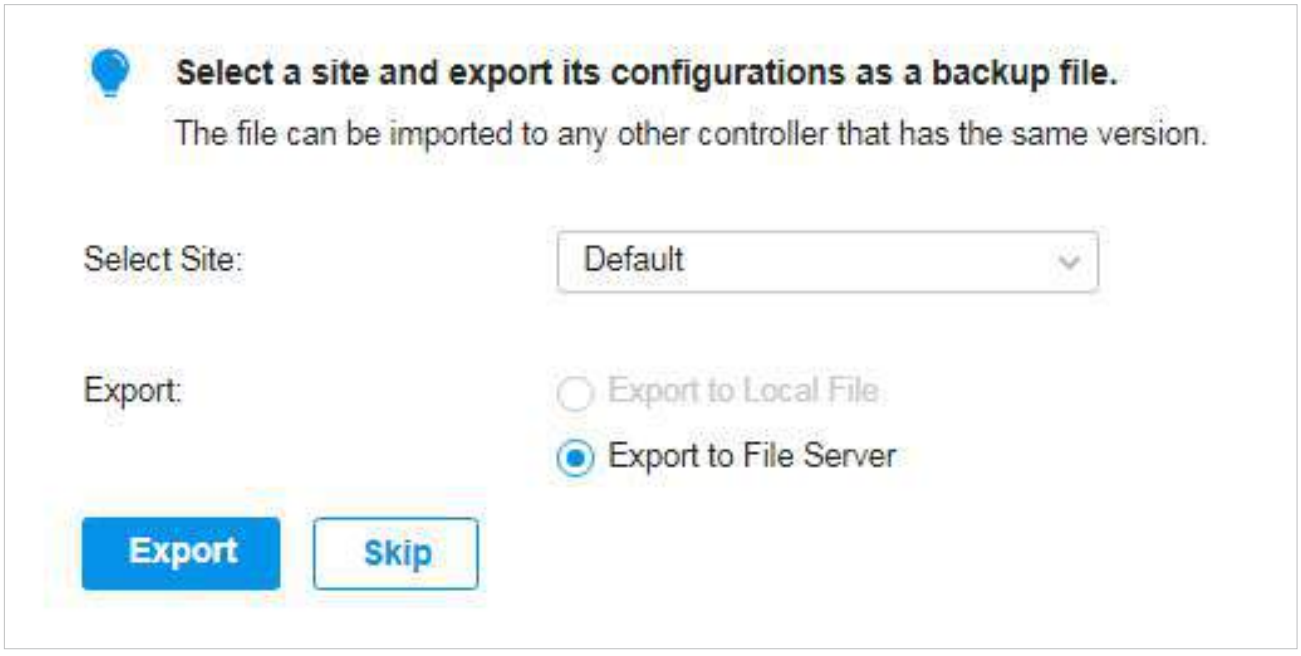
Conexiunea la internet se va pierde timp de câteva minute în timpul migrării. Clienții trebuie să se conecteze din nou la rețeaua wireless după finalizarea migrării. Vă rugăm să alegeți cu atenție momentul pentru a începe operațiunea de migrare.

Site de export | Migrați site-ul | Migrați dispozitive

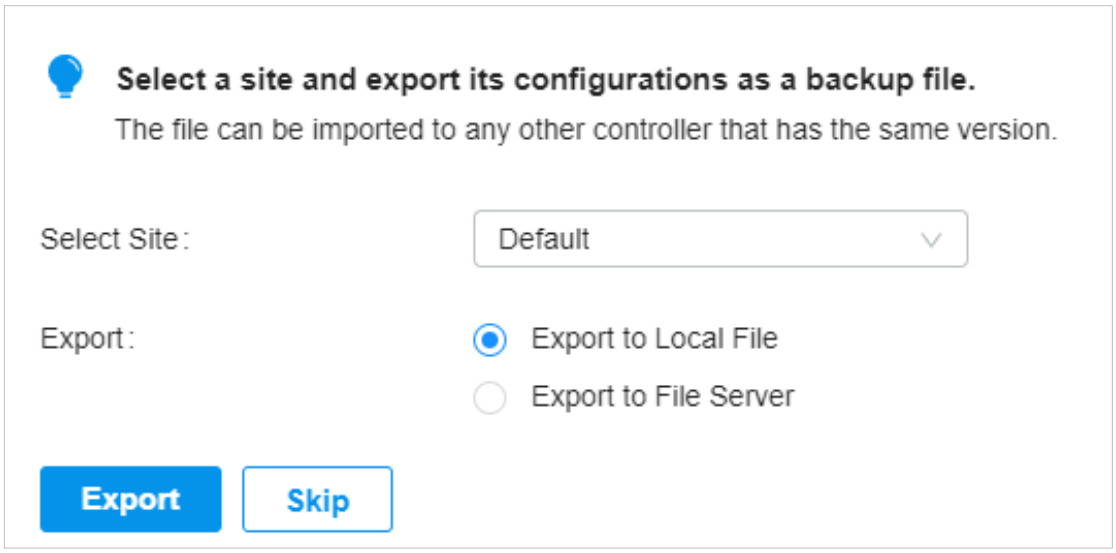
1. SelectațiGlobaldin lista derulantă aOrganizareîn colțul din dreapta sus. Mergi laSetări> Migrația. În fila Migrare site, faceți clic pe butonul Start de pe pagina următoare.



2. Selectați site-ul care urmează să fie importat în al doilea controler dinSelectați Sitelista verticală. Selectați unde doriți să exportați și salvați fișierul de rezervă. ClicExportpentru a descărca fișierul site-ului curent. Dacă ați făcut o copie de rezervă a fișierului, faceți clicOcolire.

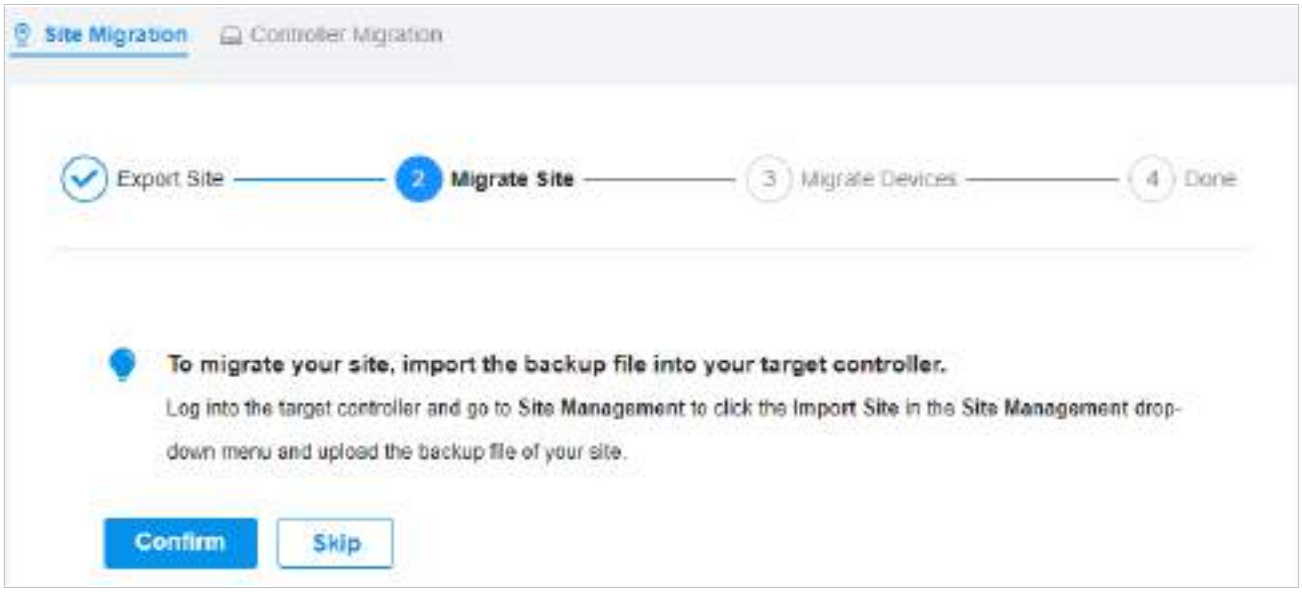


1. Porniți și conectați-vă la controlerul țintă, faceți clic pe Sites: Site A colțul din dreapta sus al ecran și selectați Import Site, iar apoi va apărea următoarea fereastră. Rețineți că pentru controler v 4.3.0 și versiuni ulterioare, numai fișierul de la controler cu același număr de versiune majoră și minoră poate fi importat.



2. Introduceți un nume unic pentru noul site. ClicNavigapentru a încărca fișierul site-ului de importat și faceți clicImport pentru a importa site-ul.

3. După ce fișierul a fost importat în controlerul țintă, reveniți la controlerul anterior și faceți clic A confirma.



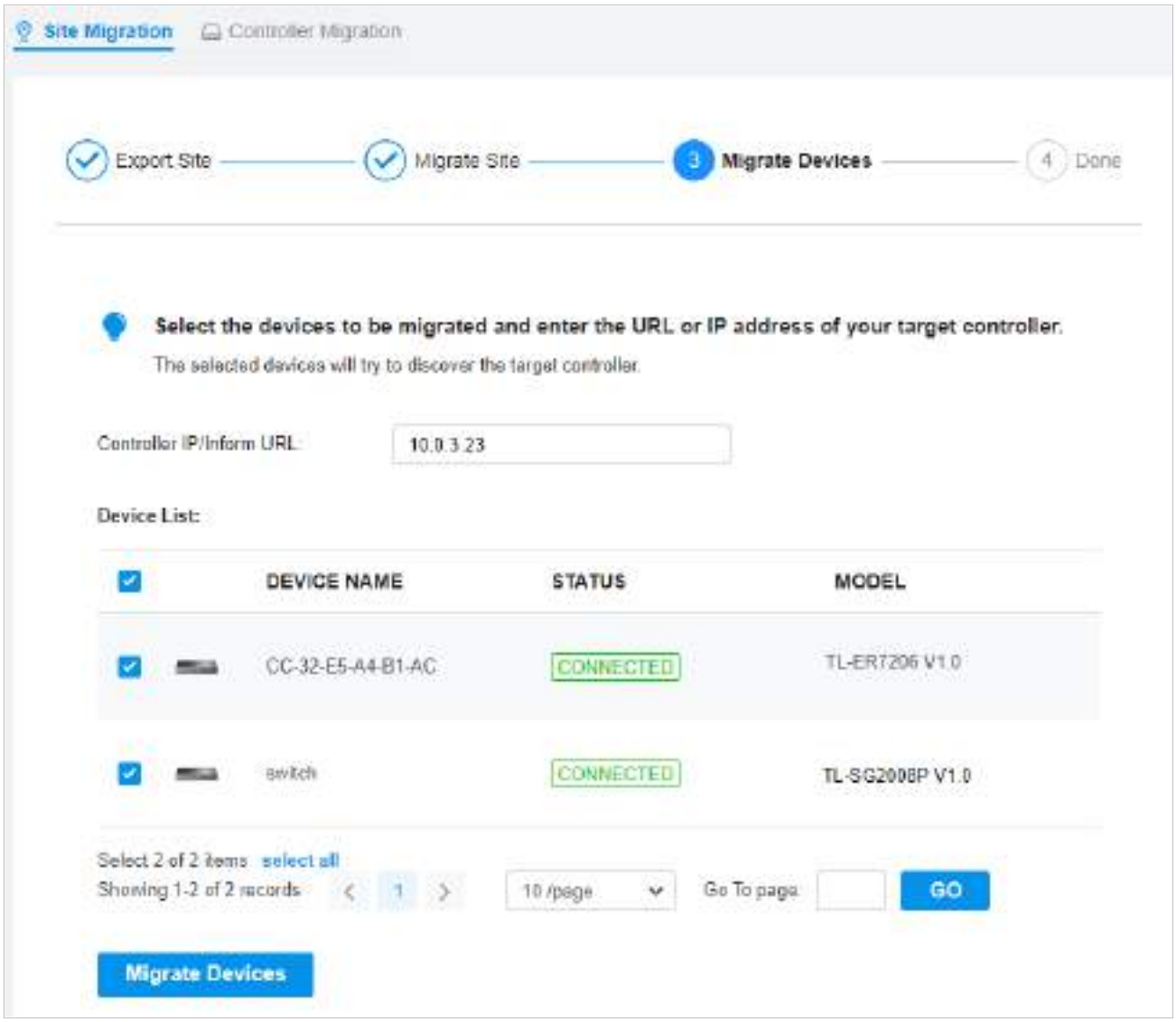
Site de export > Migrați site-ul > Migrați dispozitive

1. Introduceți adresa IP sau URL-ul controlerului dvs. țintă în IP controler/Inform URL introdus. În acest caz, adresa IP a controlerului țintă este 10.0.3.23.

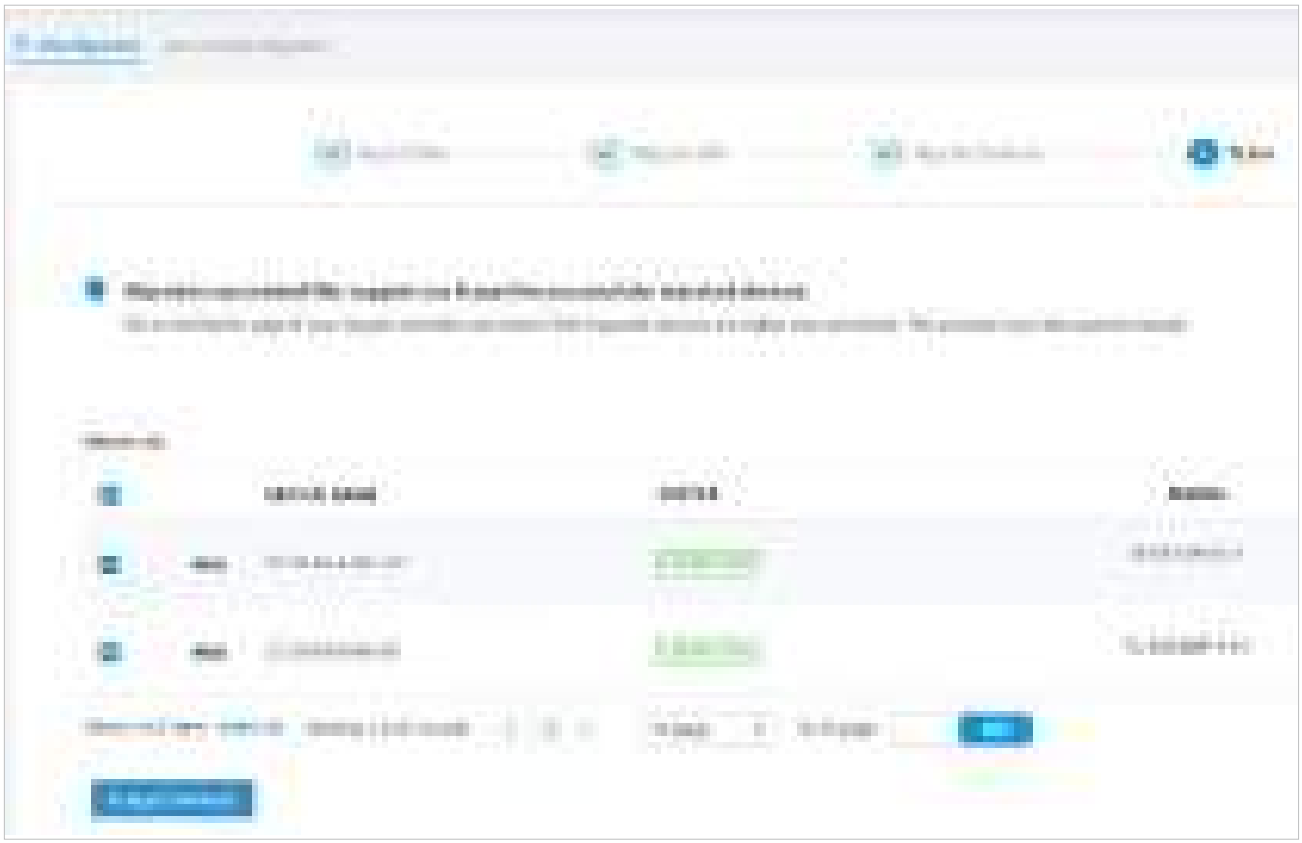
Notă:

Asigurați-vă că introduceți adresa IP corectă sau URL-ul controlerului țintă pentru a stabili comunicarea între dispozitivele gestionate de Omada și controlerul țintă. În caz contrar, dispozitivele gestionate de Omada nu pot fi adoptate de controlerul țintă.

2. Selectați dispozitivele care urmează să fie migrate făcând clic pe caseta de lângă fiecare dispozitiv. În mod implicit, toate dispozitivele sunt selectate. ClicMigrați dispozitivepentru a migra dispozitivele selectate către controlerul țintă.



3. Verificați dacă toate dispozitivele migrate sunt vizibile și conectate pe controlerul țintă. Când toate dispozitivele migrate sunt în starea Conectat pe pagina Dispozitiv a controlerului țintă, faceți clicUitați de dispozitive pentru a finaliza procesul de migrare.



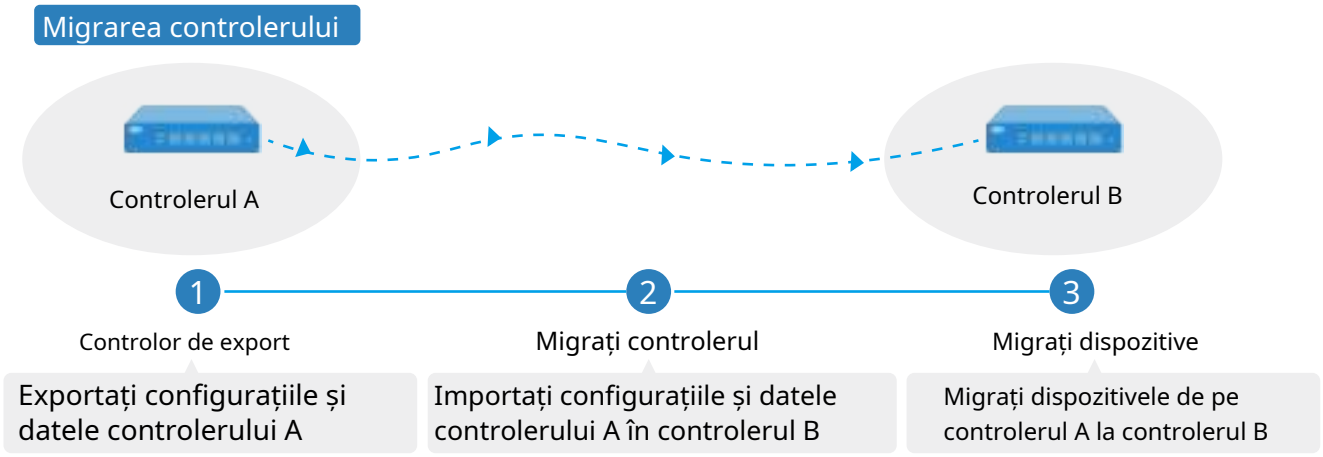
4. Când procesul de migrare este finalizat, toate configurațiile și datele sunt migrate către controlerul țintă. Dacă este necesar, puteți șterge site-ul anterior.

4. 4. 2 Migrarea controlerului

Prezentare generală

Migrarea controlerului permite administratorilor Omada să migreze configurațiile și datele de la controlerul actual la orice alt controler care are aceeași versiune.

Procesul de migrare a configurațiilor și a datelor de la controlerul actual la un alt controler poate fi rezumat în trei pași: Export Controller, Migrate Controller și Migrate Devices.



Pasul 1: Export Controller

Exportați configurațiile și datele controlerului curent ca fișier de rezervă.

Pasul 2: Migrați controlerul

În controlerul țintă, importați fișierul de rezervă al controlerului curent.

Pasul 3: Migrați dispozitivele

Migrați dispozitivele de pe controlerul curent la controlerul țintă.

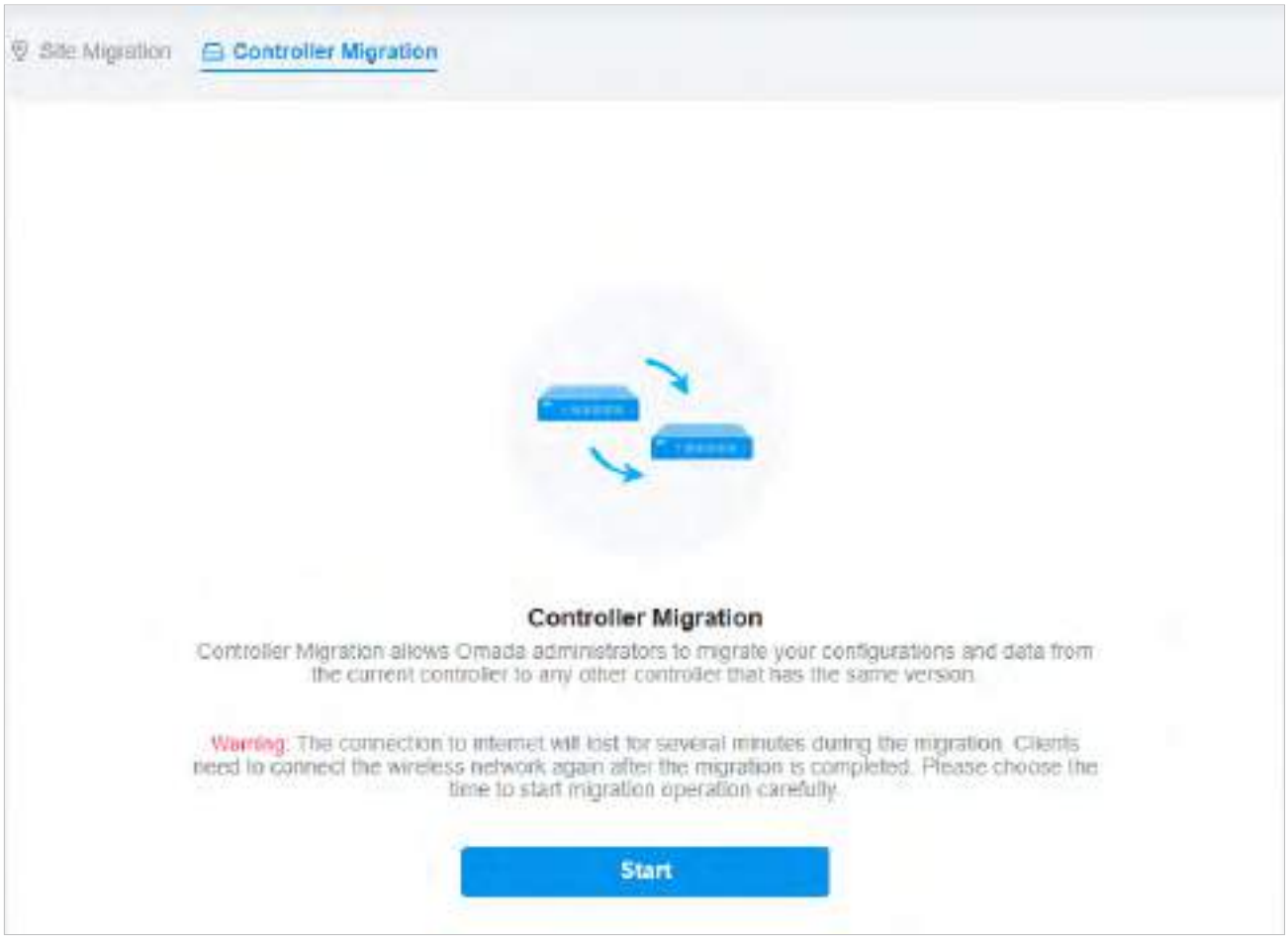
Configurare

Pentru a migra controlerul, urmați acești pași de mai jos.

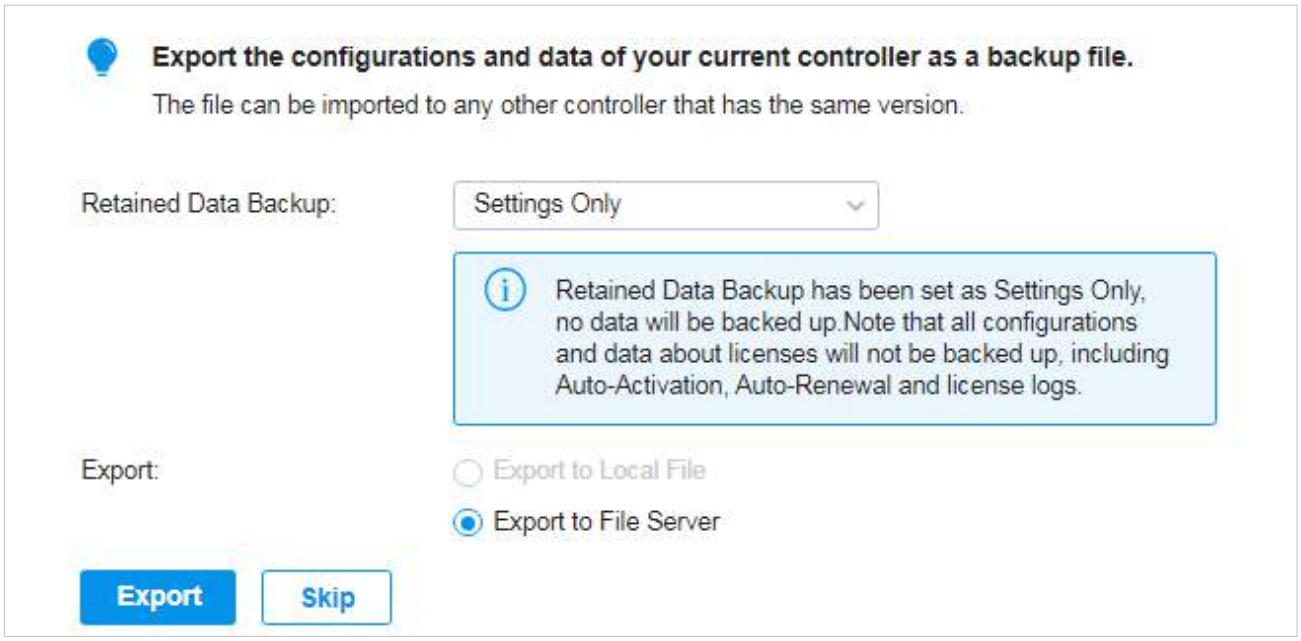
Notă:

Conexiunea la internet se va pierde timp de câteva minute în timpul migrării. Clienții trebuie să se conecteze din nou la rețeaua wireless după finalizarea migrării. Vă rugăm să alegeți cu atenție momentul pentru a începe operațiunea de migrare.

1. SelectațiGlobaldin lista derulantă aOrganizareîn colțul din dreapta sus. Mergi laSetări> Migrația. În fila Migrare controler, faceți clic pe butonul Start de pe pagina următoare.

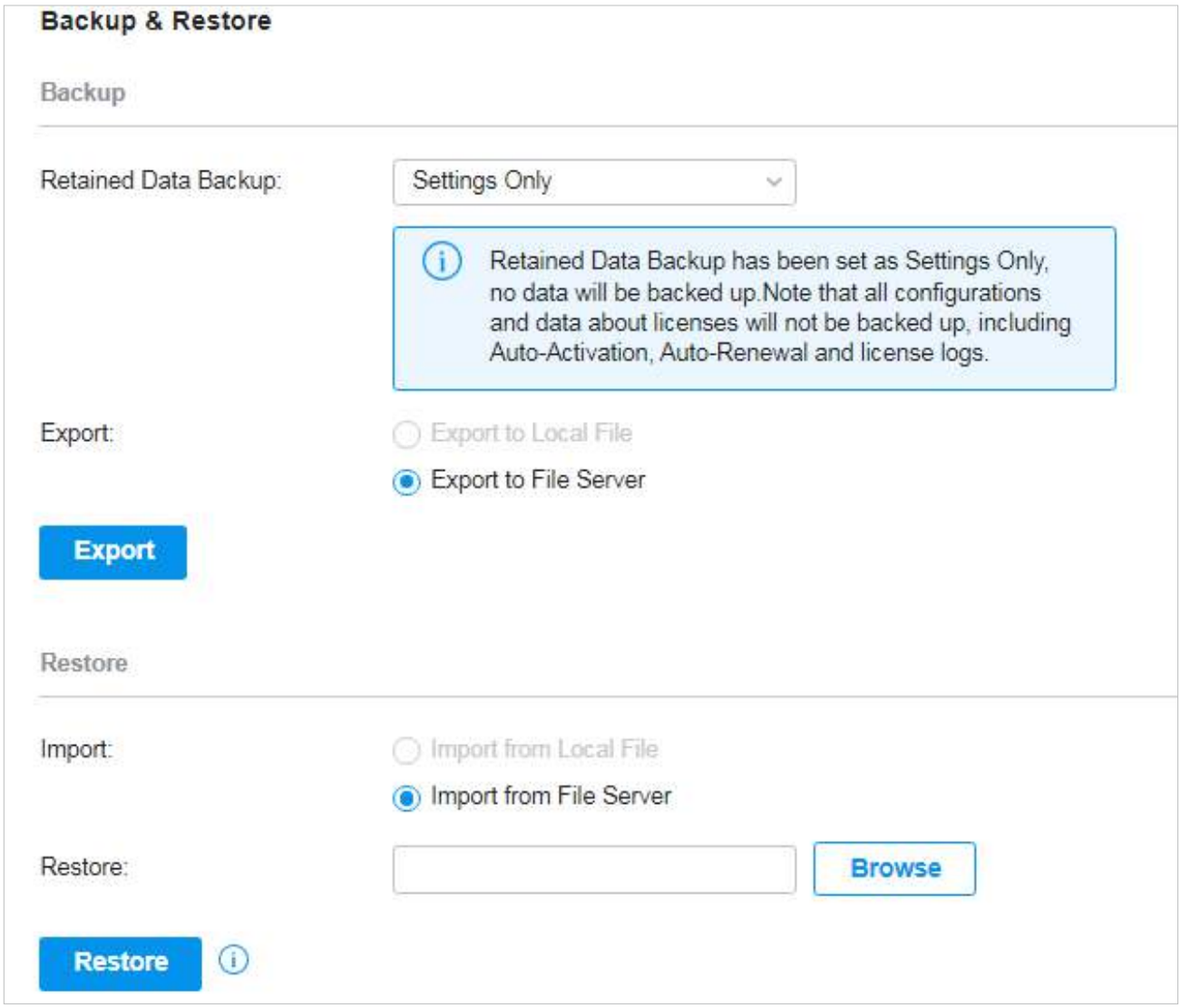


2. Selectați durata de timp în zile în care se va face backup pentru datele înBackup de date reținute, și unde doriți să exportați și să salvați datele. ClicExportpentru a exporta configurațiile și datele actualului controler ca fișier de rezervă. Dacă ați făcut o copie de rezervă a fișierului, faceți clicOcolire.



Controlor de export | Migrați controlerul | Migrați dispozitive

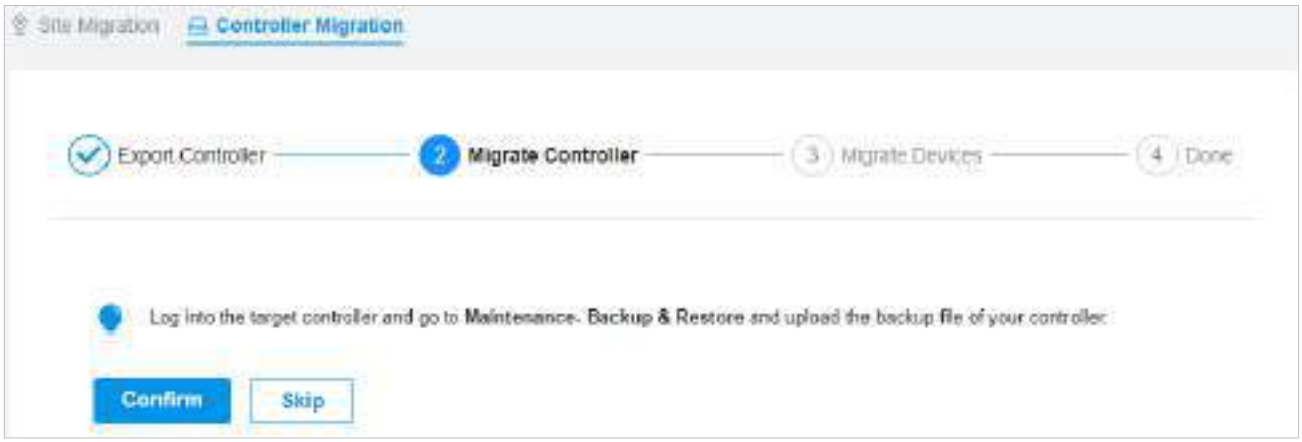
1. Conectați-vă la controlerul țintă. SelectațiGlobaldin lista derulantă aOrganizareîn colțul din dreapta sus. Mergi laSetări>întreținere>Backup și restaurare. ClicNavigapentru a localiza și alege fișierul de rezervă al controlerului anterior. Apoi apasaRestabilipentru a încărca fișierul.



Notă:

În ceea ce privește migrarea controlerului, routerul integrat poate importa doar fișiere de configurare ale routerelor integrate cu aceeași versiune sau versiunea anterioară. Routerele integrate nu pot importa alte tipuri de controlere (OC200/OC300/Software Controller/Cloud-Base Controller).

2. După ce fișierul a fost importat în controlerul țintă, reveniți la controlerul anterior și faceți clic A confirma.



Controlor de export | Migrați controlerul | **Migrați dispozitive**

1. Introduceți adresa IP sau URL-ul controlerului dvs. țintă în IP controler/Inform URL introdus. În acest caz, adresa IP a controlerului țintă este 10.0.3.23.

Notă:

Asigurați-vă că introduceți adresa IP corectă sau URL-ul controlerului țintă pentru a stabili comunicarea între dispozitivele gestionate de Omada și controlerul țintă. În caz contrar, dispozitivele gestionate de Omada nu pot fi adoptate de controlerul țintă.

2. Selectați dispozitivele care urmează să fie migrate făcând clic pe caseta de lângă fiecare dispozitiv. În mod implicit, toate dispozitivele sunt selectate. ClicMigrați dispozitivepentru a migra dispozitivele selectate către controlerul țintă.

3. Verificați dacă toate dispozitivele migrate sunt vizibile și conectate pe controlerul țintă. Când toate dispozitivele migrate sunt în starea Conectat pe pagina Dispozitiv de pe controlerul țintă, faceți clicUitați de dispozitive pentru a finaliza procesul de migrare.

Când procesul de migrare este finalizat, toate configurațiile și datele sunt migrate către controlerul țintă. Puteți dezinstala controlerul anterior dacă este necesar.

Configurați și monitorizați dispozitivele gestionate Omada

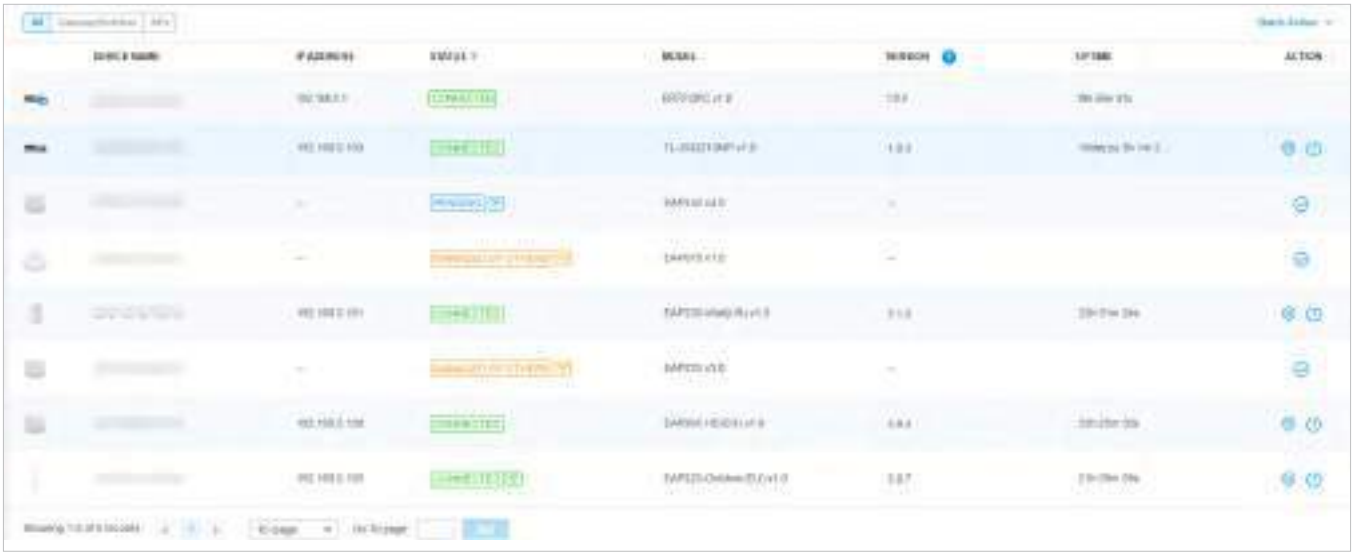
Acest capitol vă îndrumă despre cum să configurați și să monitorizați dispozitivele gestionate de Omada, inclusiv gateway-uri, comutatoare și EAP-uri. Puteți configura dispozitivele individual sau în loturi pentru a modifica configurațiile anumitor dispozitive. Capitolul include următoarele secțiuni:

5. 1 Introducere în pagina Dispozitive

Prezentare generală

Pagina Dispozitive afișează toate dispozitivele TP-Link descoperite de controler și informațiile generale ale acestora.

Pentru o monitorizare ușoară a dispozitivelor, puteți personaliza coloana și filtra dispozitivele pentru o imagine de ansamblu mai bună a informațiilor despre dispozitiv. De asemenea, operațiunile rapide și Batch Edit sunt disponibile pentru configurații.



În funcție de starea conexiunii, dispozitivele au următoarea stare: În așteptare, Izolat, Conectat, Gestionat de alții, Bătăi cardiace ratate și Deconectat. Pictogramele din coloana Stare sunt explicate după cum urmează:

PENDING	Dispozitivul este în modul Standalone sau cu setările din fabrică și nu a fost adoptat de către controlor. Pentru a adopta dispozitivul, faceți clic pe , iar controlerul va folosi numele de utilizator și parola implicite pentru a-l adopta. La adoptare, statutul său se va schimba din Adoptare, Provisioning, Configurare, la Connected eventual.
ISOLATED	(Pentru AP-urile din rețeaua mesh) AP-ul administrat cândva de controler printr-o conexiune fără fir acum nu poate ajunge la gateway. Puteți reconstrui rețeaua mesh conectându-l la un AP în starea Conectat, apoi AP-ul izolat se va transforma într-unul conectat. Pentru configurarea detaliată, consultațiPlasă.
CONNECTED	Dispozitivul a fost adoptat de controler și îl puteți gestiona central. Un dispozitiv conectat se va transforma într-unul în așteptare după ce îl uitați.
MANAGED BY OTHERS	Dispozitivul a fost deja gestionat de un alt controler. Puteți reseta dispozitivul sau puteți furniza numele de utilizator și parola pentru a-l deconecta de la un alt controler și a-l adopta în controlerul actual.

HEARTBEAT MISSED	O stare de tranziție între Conectat și Deconectat. Odată conectat la controler, dispozitivul va trimite pachete de informare către controler la un interval regulat pentru a menține conexiunea. Dacă controlerul nu primește pachetele de informare în 30 de secunde, dispozitivul se va transforma în starea Heartbeat Missed. Pentru un dispozitiv care a ratat bătăile inimii, dacă controlerul primește un pachet de informare de la dispozitiv în 5 minute, starea acestuia va deveni din nou Conectat; în caz contrar, starea acestuia va deveni Deconectat.
DISCONNECTED	Dispozitivul conectat și-a pierdut conexiunea cu controlerul pentru mai mult de 5 minute.
	(Pentru AP-urile din rețeaua mesh) Când această pictogramă apare cu o pictogramă de stare, indică că EAP are funcție de plasă și controlerul nu detectează nicio conexiune prin cablu. Îl puteți conecta la un AP uplink prin intermediulPlasă.
	Când această pictogramă apare cu o pictogramă de stare, indică că dispozitivul în starea Conectat, Bătăi inimii ratate, Izolat sau Deconectat migrează. Pentru mai multe informații despre migrare, consultați4. 4 Migrația.

Configurare

■ Personalizați coloana

Pentru a personaliza coloanele, faceți clic chiar lângăAcțiuneși bifați casetele de tip de informații.

Pentru a modifica ordinea listei, faceți clic pe capul coloanei și pe va apărea pentru a indica creşterea sau ordinea descendentă.

■ Filtrați dispozitivele

Utilizați caseta de căutare și bara de file de deasupra tabelului pentru a filtra dispozitivele.

Pentru a căuta dispozitive, introduceți textul în caseta de căutare sau selectați o etichetă din lista verticală. În ceea ce privește eticheta dispozitivului, consultați configurația generală aîntrerupătoare șiEAP-uri .

Pentru a filtra dispozitivele, o bară de file  este deasupra tabelului pentru a filtra dispozitivele după tip de dispozitiv. De asemenea, puteți filtra dispozitivele după starea lor făcând clic în coloana Stare.

Dacă selectațiAP-urifilă, o altă bară de file  va fi disponibil pentru schimbă rapid coloana.

Prezentare generală	Afișează numele dispozitivului, adresa IP, starea, modelul, versiunea firmware, timpul de funcționare, canalul și puterea Tx în mod implicit.
Plasă	Afișează informațiile despre dispozitivele din rețeaua mesh, inclusiv numele dispozitivului, adresa IP, starea, modelul, dispozitivul uplink, canalul, puterea Tx și numărul de dispozitive downlink, clienți și hopuri în mod implicit.
Performanţă	Afișează numele dispozitivului, adresa IP, starea, timpul de funcționare, canalul, puterea Tx, numărul de clienți de 2,4 GHz și 5 GHz, rata Rx și rata Tx în mod implicit.
Config	Afișează numele dispozitivului, starea, versiunea, grupul WLAN și setările radio pentru 2,4 GHz și 5 GHz în mod implicit.

■ Operații rapide

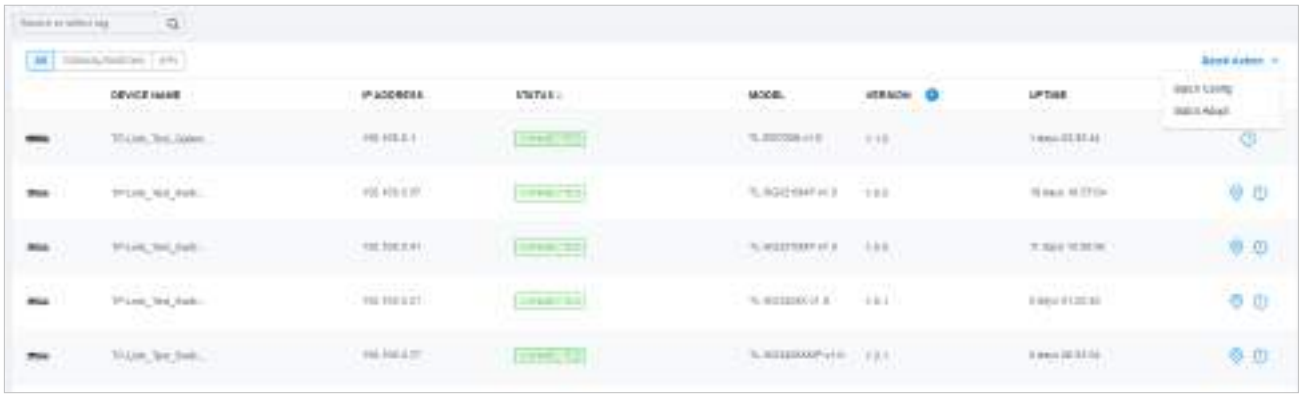
Faceți clic pe pictogramele din Antet sau peAcțiunepentru a adopta, localiza, face upgrade sau reporni rapid dispozitivul.

Start Rolling Upgrade	Faceți clic pentru a actualiza dispozitivele gestionate în loturi.
	Faceți clic pentru a verifica dacă există firmware nou pentru dispozitivele gestionate.
	(Pentru dispozitivele în așteptare) Faceți clic pentru a adopta dispozitivul.
	(Pentru comutatoarele și AP-urile conectate) Faceți clic pe această pictogramă și LED-urile dispozitivului vor clipi pentru a indica locația dispozitivului. LED-urile vor continua să clipească timp de 10 minute sau puteți face clic pe pictogramă pentru a opri clipirea.
	(Pentru dispozitivele conectate) Faceți clic pentru a reporni dispozitivul.
	Faceți clic pentru a actualiza versiunea de firmware a dispozitivului. Această pictogramă apare atunci când dispozitivul are o nouă versiune de firmware.

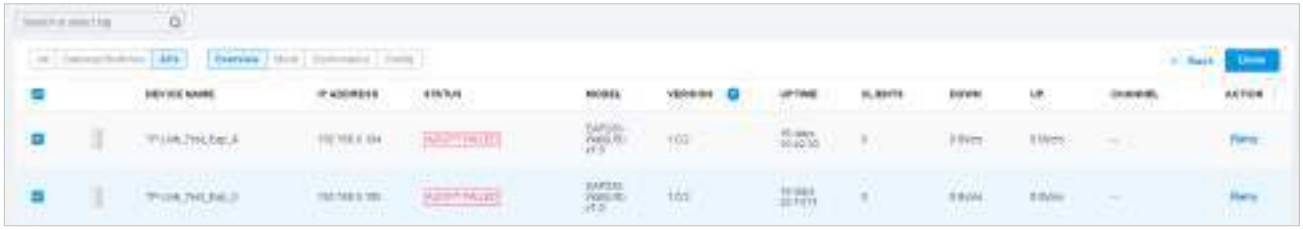
■ Editare lot (pentru comutatoare și EAP)

După selectareaGateway/Switch-urisauAP-urifila, puteți adopta sau configura comutatoarele sau EAP-urile în loturi. Batch Config este disponibilă numai pentru dispozitivele din Connected/Disconnected/Heartbeat

Starea Pierdut/Izolat, în timp ce Adoptarea lotului este disponibilă pentru dispozitivele în starea În așteptare/ Gestionat de alții.



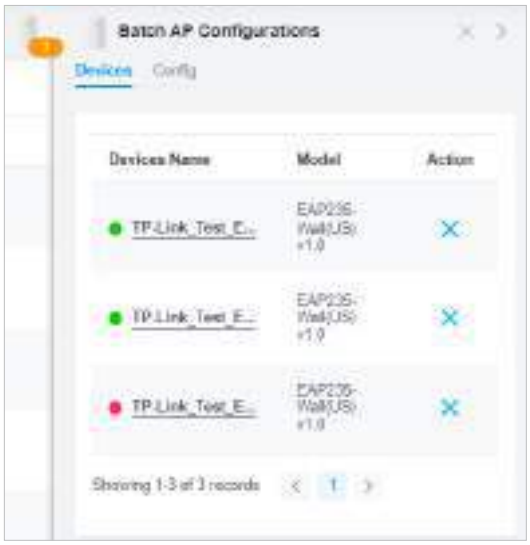
ClicAcțiune în lot. SelectațiAdoptarea lotului, faceți clic pe casetele de selectare ale dispozitivelor și faceți clicTerminat. Dacă dispozitivele selectate sunt toate în starea În așteptare, controlerul le va adopta cu numele de utilizator și parola implicite. Dacă nu, introduceți manual numele de utilizator și parola pentru a adopta dispozitivele.



ClicAcțiune în lot, SelectațiConfigurare lot, faceți clic pe casetele de selectare ale dispozitivelor și faceți clicTerminat. Apoi apare fereastra Proprietăți. Există două file în fereastră: Dispozitive și Config.

În Dispozitive, puteți face clic pentru a elimina dispozitivul din configurația curentă a lotului.

În Config, toate setările sunt în mod prestabilit Keep Existing. Pentru configurații detaliate, consultați configurația deîntrerupătoare șiEAP-uri .



	Faceți clic pentru a minimiza fereastra Proprietăți la o pictogramă. Pentru a redeschide fereastra de Proprietăți minimizată, faceți clic pe .
	Faceți clic pentru a maximiza fereastra Proprietăți. De asemenea, puteți utiliza pictograma în alte pagini decât pagina Dispozitive.
	Faceți clic pentru a închide fereastra Proprietăți a dispozitivelor alese. Rețineți că configurația nesalvată se va pierde.
	Numărul din dreapta jos arată tipul și numărul de dispozitive din configurarea lotului.

5. 2 Configurați și monitorizați Gateway-ul

În fereastra Proprietăți, puteți configura gateway-ul gestionat de controler și puteți monitoriza performanța și statisticile. În mod implicit, toate configurațiile sunt sincronizate cu site-ul curent.

Notă:

- Fiecare site poate adopta doar un router. Dacă adoptați un nou router la routerul integrat, trebuie să adoptați noul router sub un alt site decât cel care a adoptat routerul integrat.
- Funcțiile disponibile în fereastră vor varia în funcție de modelul și starea dispozitivului. Acest router integrat este adaptat special pentru utilizare cu SDN Controller v5.5. Dacă utilizați acest router integrat pentru a adopta și gestiona un router de un alt model, routerul nou adoptat va fi adaptat la SDN Controller v5.8.
- Acest ghid folosește acest router integrat ca exemplu pentru a demonstra cum să configurați și să monitorizați gateway-ul. Pentru a adopta și monitoriza un nou router, consultați ghidul utilizatorului Omada Software Controller, care poate fi descărcat de la https://www.tp-link.com/support/download/.

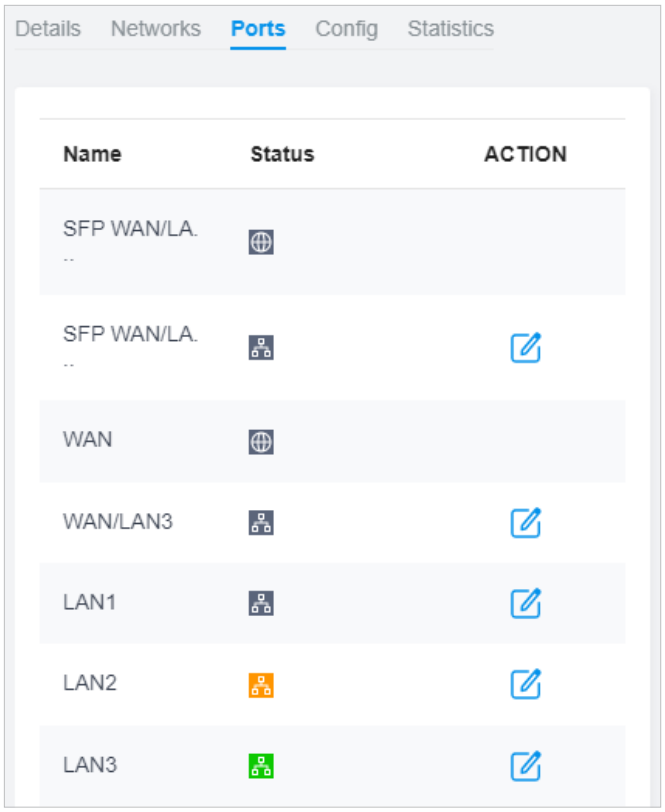
Pentru a deschide fereastra Proprietăți, faceți clic pe intrarea unui router. Un panou de monitor și mai multe file sunt listate în fereastra Proprietăți. Cele mai multe caracteristici care trebuie configurate sunt adunate în fila Configurare, cum ar fi IP, SNMP și descărcare hardware, în timp ce alte file sunt utilizate în principal pentru a monitoriza dispozitivele.

5. 2. 1 Configurați Gateway-ul

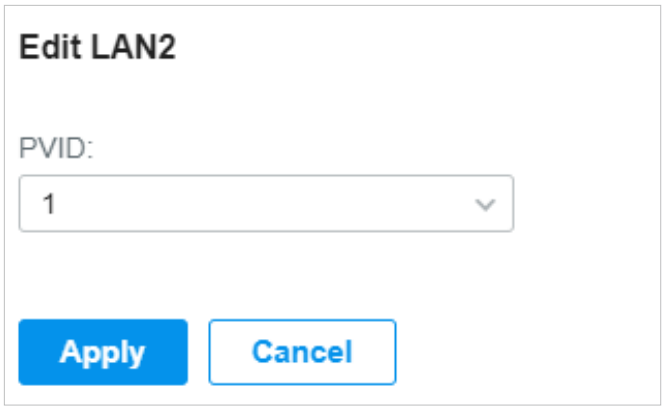
În fereastra Proprietăți, faceți clicConfigapoi faceți clic pe secțiuni pentru a configura caracteristicile, inclusiv setările generale, SNMP și funcțiile avansate.

- Porturi

  În Porturi, puteți vedea starea și edita setările porturilor.



Pentru a configura un port, faceți clic in masa.



PVID	Specificați pentru a desemna un VLAN pentru un port.

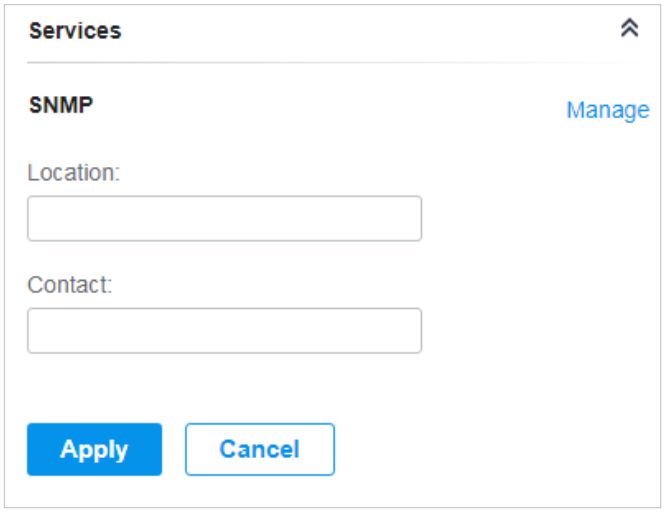
General

În general, puteți specifica numele dispozitivului și setările LED ale routerului.

Nume	Specificați un nume pentru dispozitiv.
LED	Selectați modul în care funcționează LED-urile dispozitivului respectiv. Utilizați Setările site-ului: LED-ul dispozitivului va funcționa urmând setările site-ului. Pentru a vizualiza și modifica setările site-ului, consultați3. 2. 2 Servicii. Pe/Oprit: LED-ul dispozitivului va rămâne aprins/stins.
Longitudine / Latitudine / Adresă	Configurați parametrii în funcție de locul în care se află site-ul. Aceste câmpuri sunt opționale.

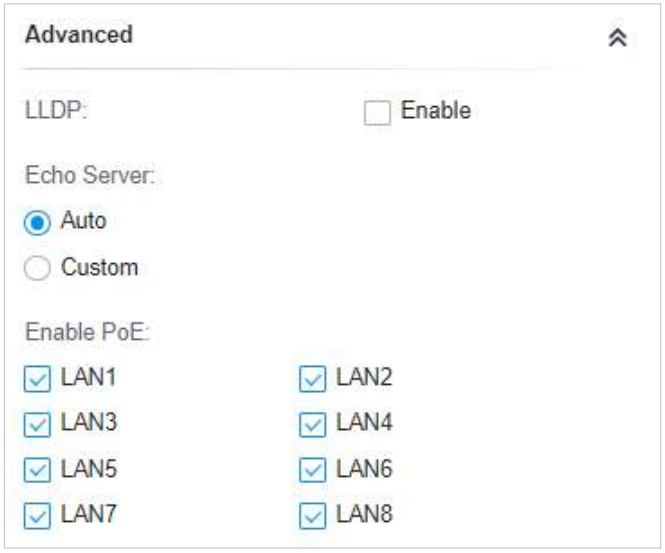
■ Servicii

În Servicii, puteți configura SNMP pentru a nota locația și detaliile de contact. De asemenea, puteți face clicAdministraa sari laSetări>Servicii>SNMP, iar pentru configurarea detaliată a serviciului SNMP, consultați3. 10. 4 SNM P.



■ Avansat

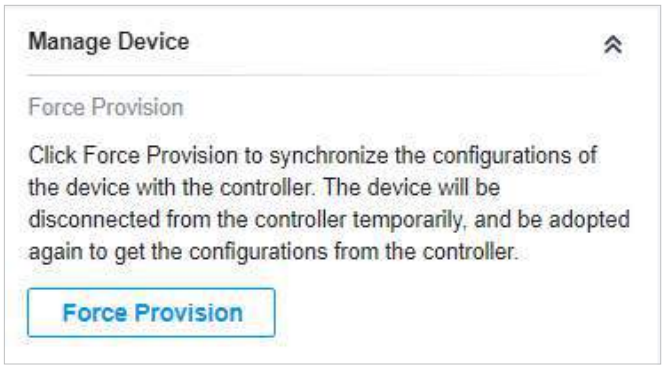
În Advanced, puteți configura Hardware Offload, LLDP (Link Layer Discovery Protocol), Echo Server și PoE pentru a utiliza mai bine resursele rețelei.



LLDP	LLDP poate ajuta la descoperirea dispozitivelor.
Echo Server	Echo Server este folosit pentru a testa conectivitatea și pentru a monitoriza latența rețelei automat sau manual. Dacă dai clicPersonalizat, introduceți adresa IP sau numele de gazdă al serverului dvs. personalizat.
PoE	(Pentru routerele cu porturi PoE+) Cu PoE activat, routerul poate furniza energie dispozitivelor conectate prin cabluri cu perechi răsucite. Pentru a activa PoE, accesațiAvansat, și bifați caseta de selectare din partea stângă a porturilor LAN corespunzătoare.

Gestionați dispozitivul

În Manage Device, puteți sincroniza configurațiile cu controlerul.



Furnizare de forță	ClicFurnizare de forțăpentru a sincroniza configurațiile dispozitivului cu controlerul. Dispozitivul își va pierde temporar conexiunea și va fi adoptat din nou la controler pentru a obține configurațiile de la controler.

- Setările comune

  În Setări comune, puteți face clic pe cale pentru a trece rapid la modulele corespunzătoare.

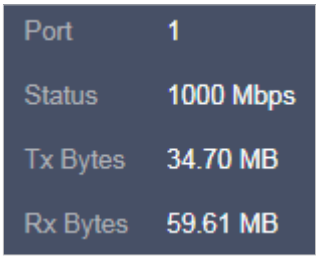
5. 2. 2 Monitorizați Gateway-ul

Un panou și trei file sunt furnizate pentru a monitoriza dispozitivul în fereastra Proprietăți: Panou monitor, Detalii, Rețele și Statistici.

Panoul de monitorizare

Panoul de monitor afișează porturile routerului și folosește culori și pictograme pentru a indica diferitele stări de conexiune și tipuri de porturi. Când routerul este în așteptare sau este deconectat, toate porturile sunt dezactivate.

Puteți trece cursorul peste pictograma portului pentru mai multe detalii.

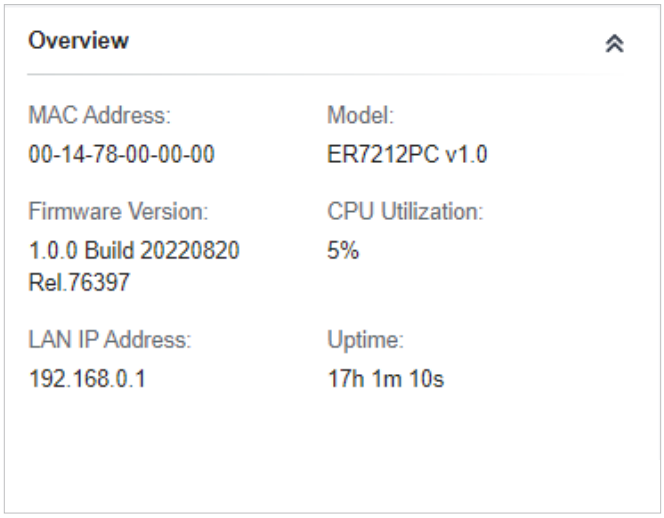


Detalii

În Detalii, puteți vizualiza informațiile de bază ale routerului și statisticile porturilor WAN pentru a afla pe scurt starea de funcționare a dispozitivului.

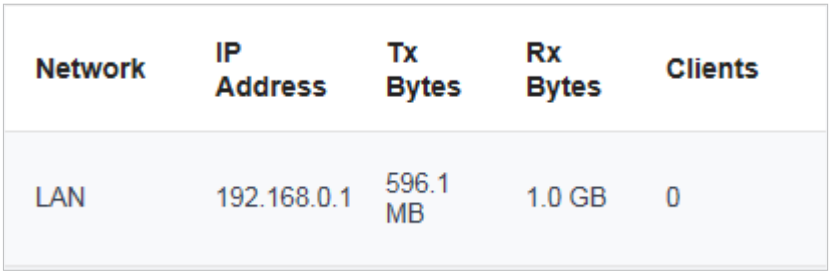
- Prezentare generală

  În Prezentare generală, puteți vizualiza informațiile de bază ale dispozitivului. Informațiile listate variază în funcție de starea dispozitivului.

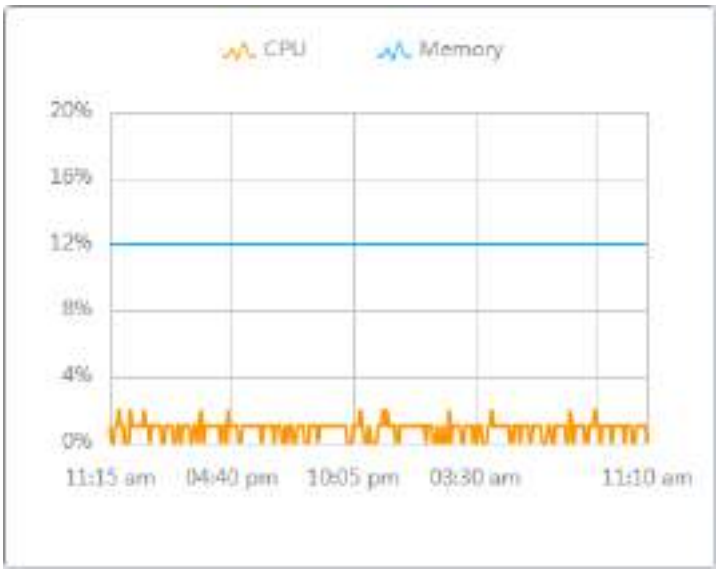
Rețele

În Rețele, puteți vizualiza informațiile de rețea ale routerului, inclusiv numele rețelei, adresa IP, traficurile transmise și primite ale interfețelor LAN din rețea și numărul de clienți.



Statistici

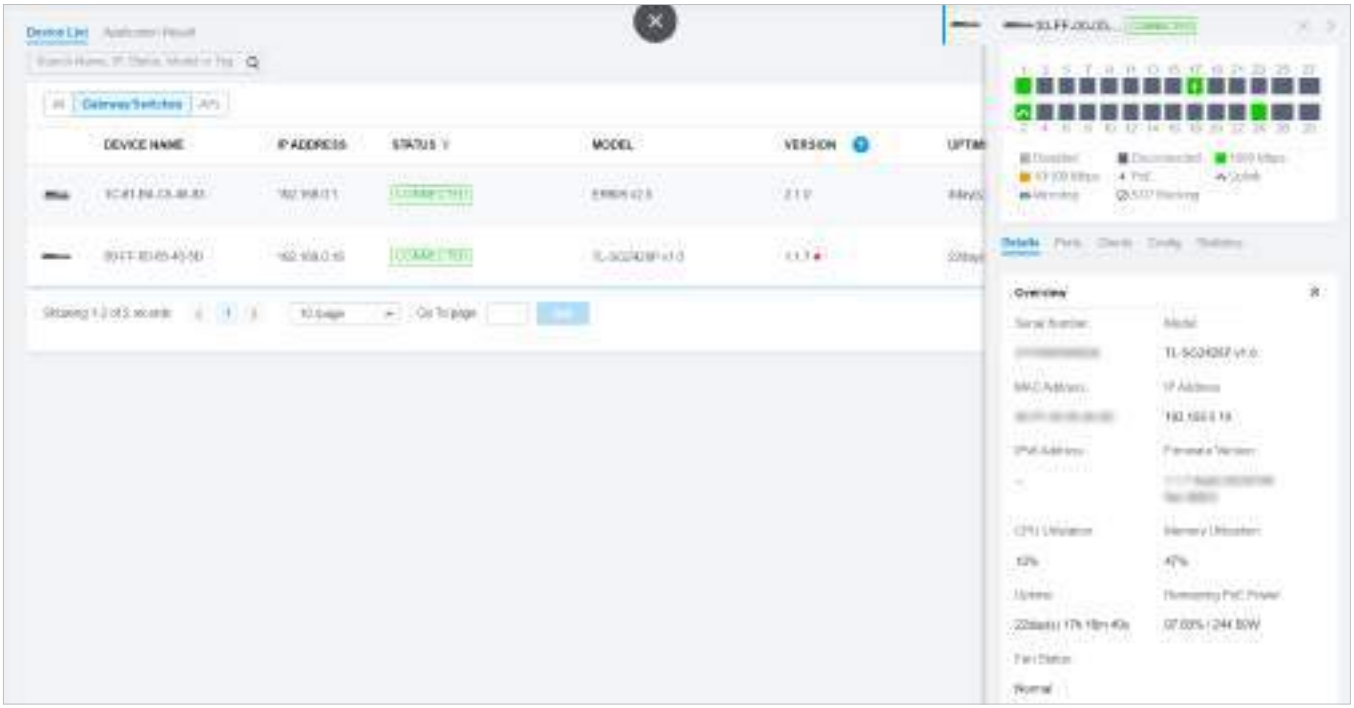
În Statistică, puteți monitoriza CPU și memoria dispozitivului în ultimele 24 de ore prin diagrame. Pentru a vizualiza statisticile dispozitivului într-o anumită perioadă, faceți clic pe diagramă la care sări7. 2 Vizualizați Statisticile rețelei .



5. 3 Configurați și monitorizați comutatoarele

În fereastra Proprietăți, puteți configura unul sau câteva comutatoare conectate la controler și puteți monitoriza performanța și statisticile. Configurațiile modificate în fereastra Proprietăți vor fi aplicate numai comutatoarelor selectate. În mod implicit, toate configurațiile sunt sincronizate cu site-ul curent.

Pentru a deschide fereastra Proprietăți, faceți clic pe intrarea unui comutator sau faceți clicAcțiune în lot, și apoiConfigurare lot pentru a selecta comutatoarele pentru configurarea lotului. Un panou de monitor și mai multe file sunt listate în fereastra Proprietăți. Cele mai multe caracteristici care trebuie configurate sunt adunate în fila Porturi și configurare, cum ar fi oglindirea portului, adresa IP și VLAN de gestionare, în timp ce alte file sunt utilizate în principal pentru a monitoriza dispozitivele.



Notă:

- Funcțiile disponibile în fereastră variază în funcție de modelul și starea dispozitivului.
- În Batch Config, puteți configura doar dispozitivele selectate, iar configurațiile nealterate vor păstra setările curente.

5. 3. 1 Configurați comutatoarele

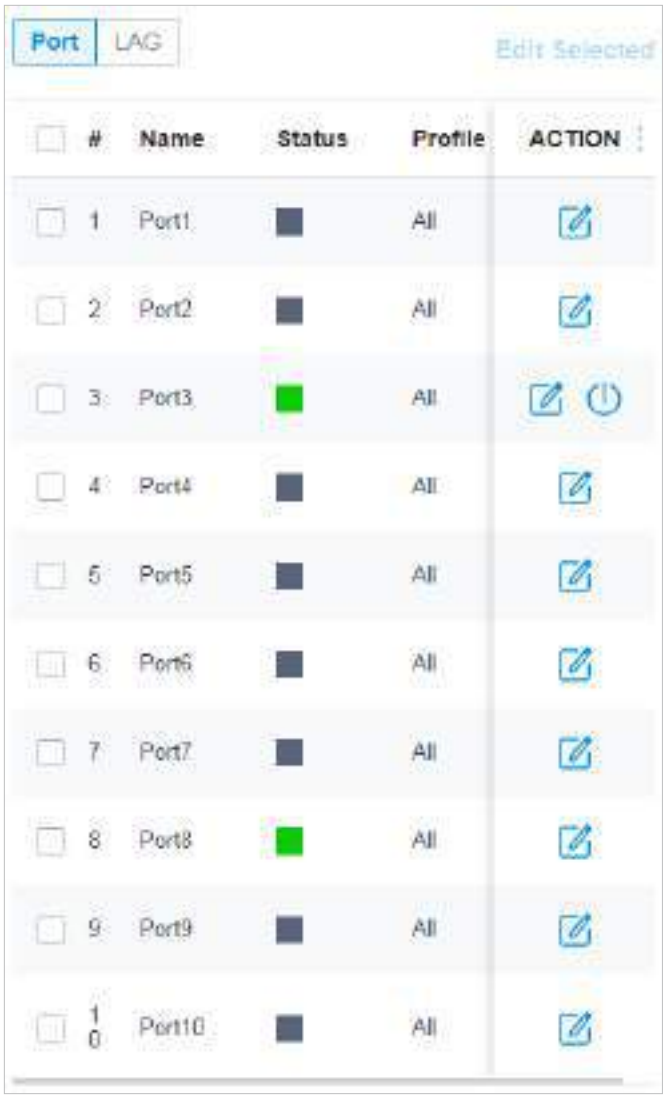
În fereastra Proprietăți, puteți vizualiza și configura profilurile aplicate porturilor în Ports, iar în Config, puteți configura caracteristicile comutatorului.

Porturi

Port și LAG sunt două file concepute pentru porturi fizice și, respectiv, LAG-uri (Grupuri de agregare a legăturilor). Sub eticheta Port, sunt listate toate porturile, dar puteți configura numai porturile fizice, inclusiv suprascrierea profilurilor aplicate, configurarea Port Mirroring și specificarea porturilor ca LAG-uri. Sub eticheta LAG, sunt listate toate LAG-urile și puteți vizualiza și modifica configurațiile LAG-urilor existente.

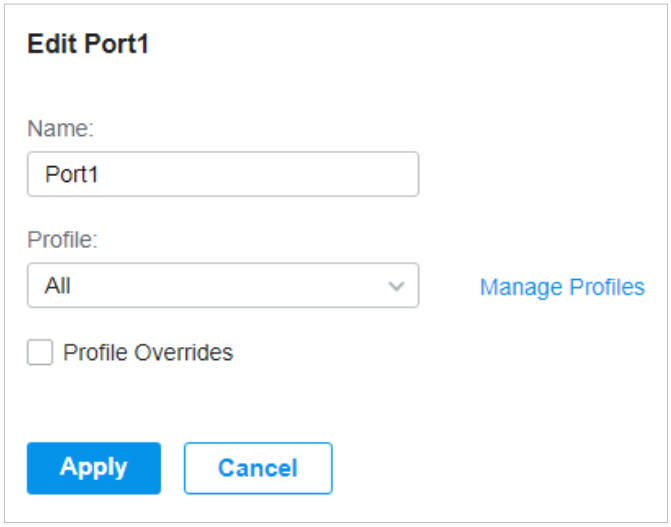
Port

În Port, puteți vizualiza și configura numele tuturor porturilor și profilurile aplicate.

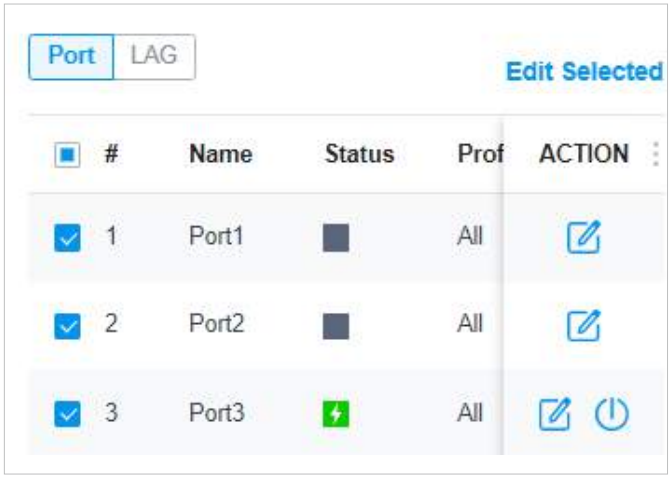


stare	Afișează starea portului în diferite culori. : Profilul portului este Dezactivat. Pentru a-l activa, faceți clic pentru a schimba profilul. : Portul este activat, dar niciun dispozitiv sau client nu este conectat la el. : portul rulează la 1000 Mbps. : portul rulează la 10/100 Mbps.
Profil	Afișează profilul aplicat portului.
Acțiune	: Faceți clic pentru a edita numele portului și a configura profilul aplicat portului. : (Pentru porturile PoE) Faceți clic pentru a reporni dispozitivele alimentate (PD) conectate.

Pentru a configura un singur port, faceți clic in masa.



Pentru a configura porturile în loturi, faceți clic pe casetele de selectare și apoi faceți clicEditați selectat. Apoi puteți configura numele și profilul portului. În mod implicit, toate setările sunt Păstrați existente pentru configurarea lotului.

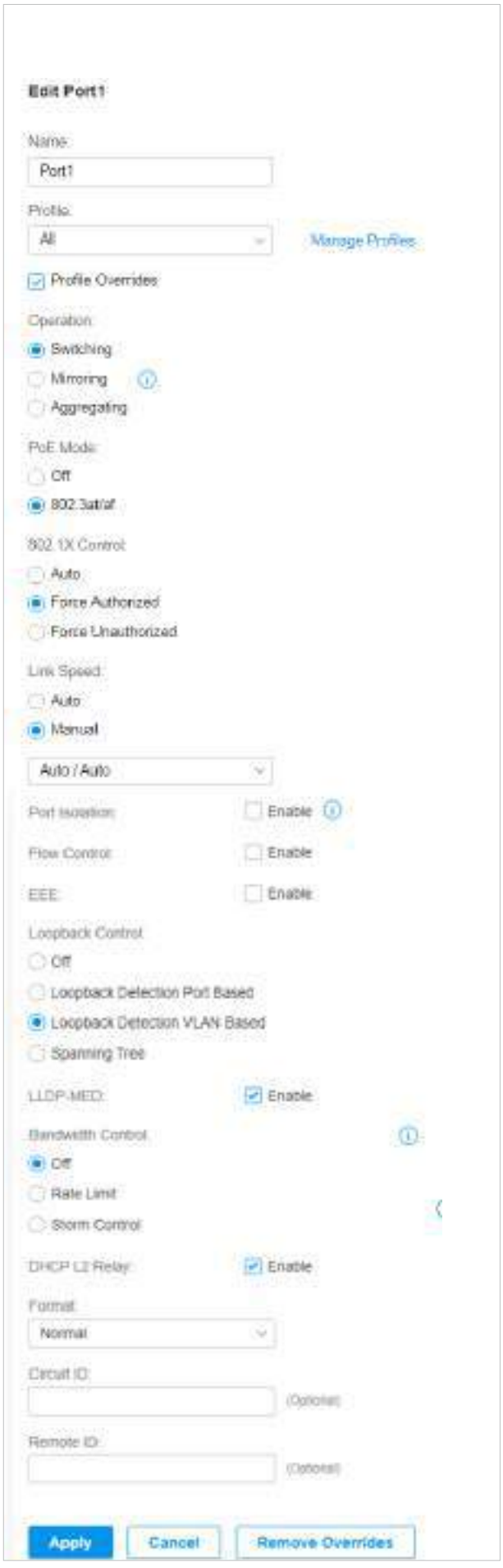


Nume	Introduceți numele portului.
Profil	Selectați profilul aplicat portului din lista verticală. ClicGestionați profiluripentru a sări pentru a vizualiza și gestiona profilurile. Pentru detalii, consultați3. 3 Configurați rețelele cu fir.
Anulări de profil	Faceți clic pe caseta de selectare pentru a înlocui profilul aplicat. Parametrii care trebuie configurați variază în modurile de funcționare,

Cu Profile Overrides activate, selectați un mod de funcționare și configurați următorii parametri pentru suprascrie profilul aplicat ,configurați un port de oglindire , sauconfigurați un LAG .

- Ignorați profilul aplicat

  Dacă selectațiComutarepentru Operare, configurați următorii parametri și faceți clicaplicapentru a suprascrie profilul aplicat. Pentru a renunța la modificări, faceți clicEliminați anulărișI toate configurațiile profilului vor deveni aceleași cu profilul aplicat.


Edit Port1
Name:
Port1
Profile:
All
Manage Profiles
Profile Overrides
Operation:
Switching
Mirroring
Aggregating
PoE Mode:
Off
802.3at/af
802.1X Control:
Auto
Force Authorized
Force Unauthorized
Link Speed:
Auto
Manual
Auto / Auto
Port Isolation:
Enable
Flow Control:
Enable
EEE:
Enable
Loopback Control:
Off
Loopback Detection Port Based
Loopback Detection VLAN Based
Spanning Tree
LLDP-MED:
Enable
Bandwidth Control:
Off
Rate Limit
Storm Control
DHCP L2 Relay:
Enable
Format:
Normal
Circuit ID:
(Optional)
Remote ID:
(Optional)
Apply
Cancel
Remove Overrides

Modul PoE	(Numai pentru porturile PoE) Selectați modul PoE (Power over Ethernet) pentru port. Oprit: Dezactivați funcția PoE pe portul PoE. 802.3at/af: Activați funcția PoE pe portul PoE.
Control 802.1X	Selectați modul de control 802.1X pentru porturi. Pentru a configura autentificarea 802.1X la nivel global, accesațiSetări>Autentificare>802.1X. Auto:Portul este neautorizat până când clientul este autentificat cu succes de către serverul de autentificare. Forțat autorizat:Portul rămâne în starea autorizată, trimite și primește trafic normal fără autentificarea 802.1X a clientului. Forțat neautorizat:Portul rămâne în starea neautorizată, iar clientul conectat la port nu se poate autentifica prin niciun mijloc. Switch-ul nu poate furniza servicii de autentificare clientului prin port.
Viteza legăturii	Selectați modul de viteză pentru port. Auto: Portul negociază automat viteza și duplexul. Manual: Specificați manual viteza și duplexul din lista verticală.
Izolarea portului	Faceți clic pe caseta de selectare pentru a activa Izolarea portului. Un port izolat nu poate comunica direct cu niciun alt port izolat, în timp ce portul izolat poate trimite și primi trafic către porturi neizolate.
Controlul debitului	Cu această opțiune activată, atunci când un dispozitiv este supraîncărcat, va trimite un cadru PAUSE pentru a anunța dispozitivul egal să nu mai trimită date pentru o perioadă de timp specificată, evitând astfel pierderea de pachete cauzată de congestie.
EEE	Faceți clic pe caseta de selectare pentru a activa EEE (Energy Efficient Ethernet) pentru a permite reducerea puterii.
Control Loopback	Loopback se referă la rutarea fluxurilor de date înapoi la sursa lor în rețea. Puteți dezactiva controlul loopback-ului pentru rețea sau puteți alege o metodă pentru a preveni producerea buclei înapoi în rețea. Oprit: Dezactivează controlul loopback pe port. Detectare Loopback: Selectați detecția loopback și ajută la prevenirea buclelor pe port. Este folosit pentru a detecta buclele care apar pe un anumit port. Când este detectată o buclă pe un port, comutatorul va bloca portul corespunzător. STP: Selectați STP (Spanning Tree Protocal) pentru a preveni buclele în rețea. STP ajută la blocarea anumitor porturi ale comutatoarelor pentru a construi o topologie fără buclă și pentru a detecta modificările topologiei și pentru a genera automat o nouă topologie fără buclă. Pentru a vă asigura că Spanning Tree are efect asupra portului, accesațiConfigfila și activați Spanning Tree pe comutator.
LLDP-MED	Faceți clic pe caseta de selectare pentru a activa LLDP-MED (Link Layer Discovery Protocol-Media Endpoint Discovery) pentru descoperirea dispozitivelor și configurarea automată a dispozitivelor VoIP (Voice over Internet Protocol).

Controlul lățimii de bandă	Selectați tipul de funcții de control al lățimii de bandă pentru a controla rata de trafic și specificați pragul de trafic pe fiecare port pentru a utiliza bine lățimea de bandă a rețelei. Off:Dezactivați Controlul lățimii de bandă pentru port. Limita ratei:Selectați Rate limit pentru a limita rata de trafic de intrare/ieșire pe fiecare port. Cu această funcție, lățimea de bandă a rețelei poate fi distribuită și utilizată în mod rezonabil. Controlul furtunii:Selectați Storm Control pentru a permite comutatorului să monitorizeze cadrele de difuzare, cadrele multicast și cadrele UL (cadre unicast necunoscute) în rețea. Dacă viteza de transmisie a cadrelor depășește rata specificată, cadrele vor fi eliminate automat pentru a evita furtuna de transmisie în rețea.
Limita ratei de intrare	Cu Rate Limit selectată, faceți clic pe caseta de selectare și specificați limita superioară a ratei pentru primirea pachetelor pe port.
Limita ratei de ieșire	Când este selectată Rate Limit, faceți clic pe caseta de selectare și specificați limita superioară a ratei pentru trimiterea de pachete pe port.
Pragul de difuzare	Cu Storm Control selectat, faceți clic pe caseta de selectare și specificați limita superioară a ratei pentru recepția cadrelor de difuzare. Traficul de difuzare care depășește limita va fi procesat conform configurațiilor Acțiunii.
Prag multicast	Cu Storm Control selectat, faceți clic pe caseta de selectare și specificați limita superioară a ratei pentru primirea cadrelor multicast. Traficul multicast care depășește limita va fi procesat conform configurațiilor Action.
Unicast necunoscut Prag	Cu Storm Control selectat, faceți clic pe caseta de selectare și specificați limita superioară a ratei pentru primirea cadrelor unicast necunoscute. Traficul care depășește limita va fi procesat conform configurațiilor Acțiunii.
Acțiune	Când este selectat Storm Control, selectați acțiunea pe care o va întreprinde comutatorul atunci când traficul depășește limita corespunzătoare. cădere brusca: Cu Drop selectat, portul va renunța la cadrele ulterioare când traficul depășește limita. Închide: Cu Oprire selectată, portul va fi oprit atunci când traficul depășește limita.
Recuperează Timp	Cu Shutdown selectat ca Acțiune, specificați timpul de recuperare și portul va fi deschis după timpul specificat.
Releu DHCP L2	Faceți clic pe caseta de selectare pentru a activa DHCP L2 Relay pentru rețea.
Format	Selectați formatul câmpului pentru valoarea subopțiunii 82. Normal: Formatul câmpului de valoare a sub-opțiunii este TLV (tip-lungime-valoare). Privat: Formatul câmpului valoare sub-opțiune este doar valoare.

ID circuit	(Opțional) Introduceți ID-ul circuitului personalizat. Configurațiile de identificare a circuitului ale comutatorului și ale serverului DHCP ar trebui să fie compatibile între ele. Dacă nu este specificat, comutatorul va folosi ID-ul de circuit implicit atunci când inserează Opțiunea 82 în pachetele DHCP.
ID de la distanță	(Opțional) Introduceți ID-ul personalizat de la distanță. Configurațiile ID la distanță ale comutatorului și ale serverului DHCP ar trebui să fie compatibile între ele. Dacă nu este specificat, comutatorul va folosi propria sa adresă MAC ca ID la distanță.

- Configurați un port de oglindire

  Dacă selectațiOglindireca Operație, portul editat poate fi configurat ca port de oglindire. Specificați alte porturi ca port în oglindă, iar comutatorul trimite o copie a traficurilor care trec prin portul în oglindă către portul de oglindire. Puteți utiliza oglindirea pentru a analiza traficul de rețea și a depana problemele de rețea.

  Pentru a configura Mirroring, selectați portul în oglindă sau LAG, specificați următorii parametri și faceți clicaplica. Pentru a renunța la modificări, faceți clicEliminați anulărișsi toate configurațiile profilului devin aceleași cu profilul aplicat.

Rețineți că porturile de oglindire și porturile membre ale LAG nu pot fi selectate ca porturi în oglindă.

Modul PoE	(Numai pentru porturile PoE) Selectați modul PoE pentru port. Oprit: Dezactivați PoE pe portul PoE. 802.3at/af: Activați PoE pe portul PoE.
Viteza legăturii	Selectați modul de viteză pentru port. Auto: Portul negociază automat viteza și duplexul. Manual: Specificați manual viteza și duplexul din lista verticală.

Controlul lățimii de bandă	Controlul lățimii de bandă optimizează performanța rețelei prin limitarea lățimii de bandă a anumitor surse. Oprit: Dezactivează controlul lățimii de bandă pe port. Limită de rată: Activați controlul lățimii de bandă pe port și trebuie să specificați limita ratei de intrare și/sau ieșire.
Limita ratei de intrare	CuLimită de ratăselectat, faceți clic pe caseta de selectare și specificați limita superioară a ratei pentru primirea pachetelor pe port. Cu această funcție, lățimea de bandă a rețelei poate fi distribuită și utilizată în mod rezonabil.
Limita ratei de ieșire	CuLimită de ratăselectat, faceți clic pe caseta de selectare și specificați limita superioară a ratei pentru trimiterea de pachete pe port. Cu această funcție, lățimea de bandă a rețelei poate fi distribuită și utilizată în mod rezonabil.

- Configurați un LAG

  Dacă selectațiAgregareaca operație, puteți agrega mai multe porturi fizice într-o interfață logică, care poate crește lățimea de bandă a conexiunii și poate spori fiabilitatea conexiunii.

  Ghid de configurare:

  - Asigurați-vă că ambele capete ale legăturii de agregare funcționează în același mod LAG. De exemplu, dacă capătul local funcționează în modul LACP, capătul egal ar trebui, de asemenea, setat ca mod LACP.
  - Asigurați-vă că dispozitivele de la ambele capete ale conexiunii de agregare utilizează același număr de porturi fizice cu aceeași viteză, duplex, jumbo și mod de control al fluxului.
  - Un port nu poate fi adăugat la mai mult de un LAG în același timp.
  - LACP nu acceptă legături semi-duplex.
  - Un LAG static acceptă până la opt porturi membre. Toate porturile membre împart lățimea de bandă în mod egal. Dacă o legătură activă eșuează, celelalte legături active împart lățimea de bandă în mod egal.
  - Un LACP LAG acceptă mai multe porturi membre, dar cel mult opt dintre ele pot funcționa simultan, iar celelalte porturi membre sunt copii de rezervă. Folosind protocolul LACP, comutatoarele negociază parametrii și determină porturile de lucru. Când un port de funcționare eșuează, portul de rezervă cu cea mai mare prioritate va înlocui portul defect și va începe să transmită datele.
  - Portul membru al unui LAG urmează configurația LAG, dar nu pe propria sa. Odată eliminat, membrul LAG va fi configurat ca implicit Toate profilurile și operația de comutare.
  - Portul activat cu Port Security, Port Mirror, MAC Address Filtering sau 802.1X nu poate fi adăugat la un LAG, iar portul membru al unui LAG nu poate fi activat cu aceste funcții.

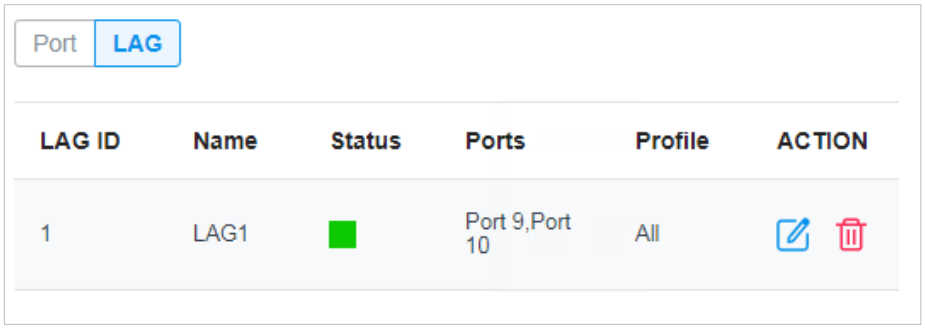
  Pentru a configura un nou LAG, selectați alte porturi pentru a fi adăugate la LAG, specificați ID-ul LAG și alegeți un tip de LAG. Clicaplica. Pentru a renunța la modificări, faceți clicEliminați anulărisi tot

configurațiile profilului devin aceleași cu profilul aplicat. Pentru alți parametri, configurați-i în fila LAG.

ID LAG	Specificați ID-ul LAG al LAG-ului. Rețineți că ID-ul LAG ar trebui să fie unic. Valoarea validă a ID-ului LAG este determinată de numărul maxim de LAG-uri acceptate de comutatorul dvs. De exemplu, dacă comutatorul dvs. acceptă până la 14 LAG-uri, valoarea validă variază de la 1 la 14.
LAG static	Selectați tipul LAG ca LAG static, iar porturile membre sunt adăugate manual la LAG.
LACP	Selectați tipul LAG ca LACP (Link Aggregation Control Protocol), iar comutatorul utilizează LACP pentru a implementa agregarea și dezagregarea legăturilor dinamice. LACP extinde flexibilitatea configurațiilor LAG.
Act i ve LACP/Pass i ve LACP	LACP extinde flexibilitatea configurațiilor LAG. În LACP, comutatorul folosește LACPDU (Link Aggregation Control Protocol Data Unit) pentru a negocia parametrii cu capătul egal. În acest fel, cele două capete selectează porturile active și formează legătura de agregare. LACP activ: În acest mod, portul va lua inițiativa de a trimite LACPDU. LACP pasiv: În acest mod, portul nu va trimite LACPDU înainte de a primi LACPDU de la capătul egal.

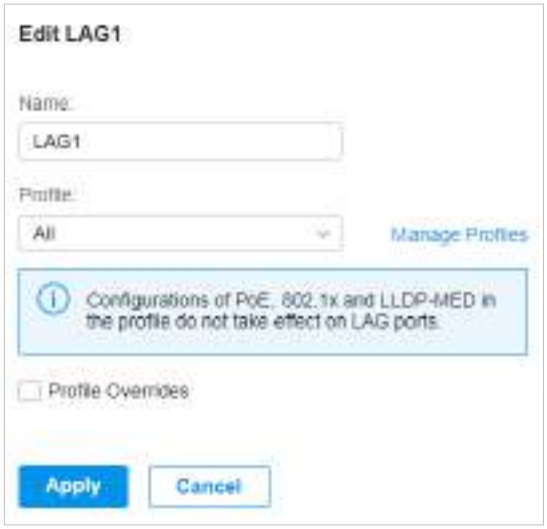
LAG

LAG-urile (Link Aggregation Groups) sunt interfețe logice agregate, care pot crește lățimea de bandă a conexiunii și pot spori fiabilitatea conexiunii. Puteți vizualiza și edita LAG-urile în fila LAG. Pentru a configura porturile fizice ca LAG, consultațiConfigurați un LAG .



stare	Afișează starea în diferite culori. : Profilul LAG este Dezactivat. Pentru a-l activa, faceți clic pentru a schimba profilul. : Portul este activat, dar niciun dispozitiv sau client nu este conectat la el. : Porturile LAG rulează la 1000 Mbps. : portul LAG rulează la 10/100 Mbps.
Porturi	Afișează numărul portului de porturi LAG.
Profil	Afișează profilul aplicat portului.
Acțiune	: Faceți clic pentru a edita numele portului și a configura profilul aplicat portului. : Faceți clic pentru a șterge LAG. Odată șterse, porturile vor fi configurate ca implicit Toate profilurile și operația de comutare. Puteți configura porturile în fila Port.

Clic pentru a configura numele LAG și profilul aplicat.



Nume	Introduceți numele portului.
Profil	Selectați profilul aplicat portului din lista verticală. ClicGestionați profiluripentru a sări pentru a vizualiza și gestiona profilurile. Pentru detalii, consultați3. 3 Configurați rețelele cu fir.
Anulări de profil	Faceți clic pe caseta de selectare pentru a înlocui profilul aplicat. Parametrii care trebuie configurați variază în modurile de operare.

Cu opțiunile de înlocuire a profilului activate, puteți reselecta membrii LAG și puteți configura următorii parametri.

Viteza legăturii	Selectați modul de viteză pentru port. Auto: Portul negociază automat viteza și duplexul. Manual: Specificați manual viteza și duplexul din lista verticală.
Izolarea portului	Faceți clic pe caseta de selectare pentru a activa Izolarea portului. Un port izolat nu poate comunica direct cu niciun alt port izolat, în timp ce portul izolat poate trimite și primi trafic către porturi neizolate.
Controlul debitului	Cu această opțiune activată, atunci când un dispozitiv este supraîncărcat, va trimite un cadru PAUSE pentru a anunța dispozitivul egal să nu mai trimită date pentru o perioadă de timp specificată, evitând astfel pierderea de pachete cauzată de congestie.
EEE	Faceți clic pe caseta de selectare pentru a activa EEE (Energy Efficient Ethernet) pentru a permite reducerea puterii.

Control Loopback	Loopback se referă la rutarea fluxurilor de date înapoi la sursa lor în rețea. Puteți dezactiva controlul loopback-ului pentru rețea sau puteți alege o metodă pentru a preveni producerea buclei înapoi în rețea. Oprit: Dezactivează controlul loopback pe port. Loopback Detection Port Bazat:Loopback Detection Port Based ajută la detectarea buclelor care apar pe un anumit port. Când este detectată o buclă pe un port, portul va fi blocat. Loopback Detection bazat pe VLAN:Loopback Detection VLAN Based ajută la detectarea buclelor care apar pe un anumit VLAN. Când este detectată o buclă pe un VLAN, VLAN-ul va fi blocat. STP: Selectați STP (Spanning Tree Protocal) pentru a preveni buclele în rețea. STP ajută la blocarea anumitor porturi ale comutatoarelor pentru a construi o topologie fără buclă și pentru a detecta modificările topologiei și pentru a genera automat o nouă topologie fără buclă. Pentru a vă asigura că Spanning Tree are efect asupra portului, accesațiConfigfila și activați Spanning Tree pe comutator.
Controlul lățimii de bandă	Selectați tipul de funcții de control al lățimii de bandă pentru a controla rata de trafic și pragul de trafic pe fiecare port pentru a asigura performanța rețelei. Off:Dezactivați Controlul lățimii de bandă pentru port. Limita ratei:Selectați Rate limit pentru a limita rata de trafic de intrare/ieșire pe fiecare port. Cu această funcție, lățimea de bandă a rețelei poate fi distribuită și utilizată în mod rezonabil. Controlul furtunii:Selectați Storm Control pentru a permite comutatorului să monitorizeze cadrele de difuzare, cadrele multicast și cadrele UL (cadre unicast necunoscute) în rețea. Dacă viteza de transmisie a cadrelor depășește rata specificată, cadrele vor fi eliminate automat pentru a evita furtuna de transmisie în rețea.
Limita ratei de intrare	Cu Rate Limit selectată, faceți clic pe caseta de selectare și specificați limita superioară a ratei pentru primirea pachetelor pe port.
Limita ratei de ieșire	Cu Rate Limit selectată, faceți clic pe caseta de selectare și specificați limita superioară a ratei pentru trimiterea de pachete pe port.
Pragul de difuzare	Cu Storm Control selectat, faceți clic pe caseta de selectare și specificați limita superioară a ratei pentru recepția cadrelor de difuzare. Traficul de difuzare care depășește limita va fi procesat conform configurațiilor Acțiunii.
Prag multicast	Cu Storm Control selectat, faceți clic pe caseta de selectare și specificați limita superioară a ratei pentru primirea cadrelor multicast. Traficul multicast care depășește limita va fi procesat conform configurațiilor Action.
Unicast necunoscut Prag	Cu Storm Control selectat, faceți clic pe caseta de selectare și specificați limita superioară a ratei pentru primirea cadrelor unicast necunoscute. Traficul care depășește limita va fi procesat conform configurațiilor Acțiunii.
Releu DHCP L2	Faceți clic pe caseta de selectare pentru a activa DHCP L2 Relay pentru rețea.

Acțiune	Cu Storm Control selectat, selectați acțiunea pe care o va întreprinde comutatorul atunci când traficul depășește limita corespunzătoare. cădere brusca: Cu Drop selectat, portul va renunța la cadrele ulterioare când traficul depășește limita. Închide: Cu Oprire selectată, portul va fi oprit atunci când traficul depășește limita.
Recuperează Timp	Cu Shutdown selectat ca Acțiune, specificați timpul de recuperare și portul va fi deschis după timpul specificat.

Config

ÎnConfig, faceți clic pe secțiuni pentru a configura caracteristicile aplicate comutatoarelor selectate, inclusiv setările generale, serviciile și rețelele.

■ General

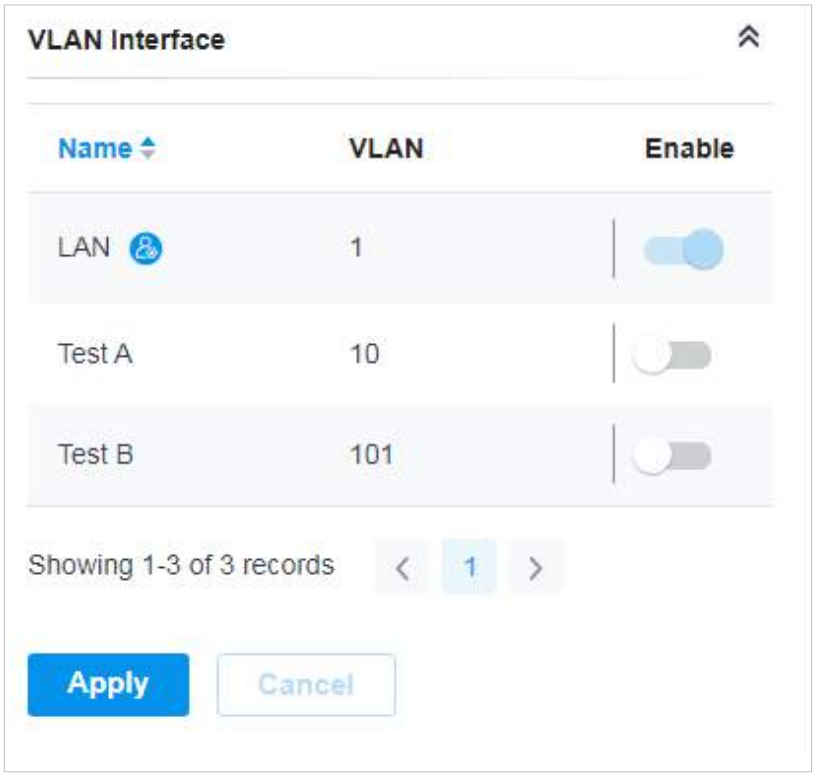
În general, puteți specifica numele dispozitivului și setările LED ale comutatorului și le puteți clasifica prin etichete de dispozitiv.

Nume	(Numai pentru configurarea unui singur dispozitiv) Specificați un nume pentru dispozitiv.

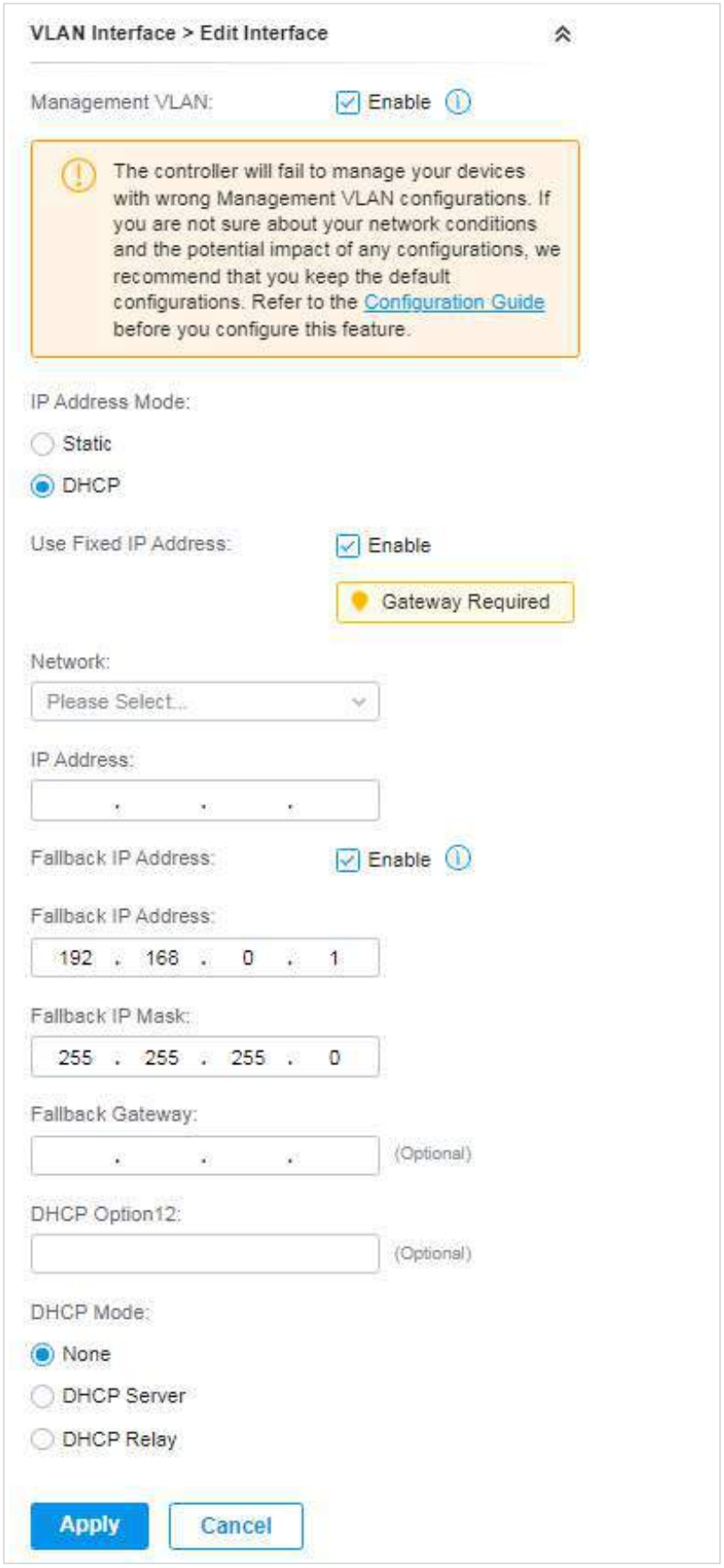
LED	Selectați modul în care funcționează LED-urile dispozitivului respectiv. Utilizați Setările site-ului: LED-ul dispozitivului va funcționa urmând setările site-ului. Pentru a vizualiza și modifica setările site-ului, consultați3. 2. 2 Servicii. Pe/Oprit: LED-ul dispozitivului va rămâne aprins/stins.
Etichete dispozitiv	Selectați o etichetă din lista derulantă sau creați o nouă etichetă pentru a clasifica dispozitivul.
Jumbo	Configurați dimensiunea cadrelor jumbo. În mod implicit, este de 1518 octeți. În general, dimensiunea MTU (Maximum Transmission Unit) a unui cadru normal este de 1518 octeți. Dacă doriți ca comutatorul să transmită cadre a căror dimensiune MTU este mai mare de 1518 octeți, puteți configura manual dimensiunea MTU aici.
Algoritmul Hash	Selectați algoritmul Hash, pe baza căruia comutatorul poate alege portul pentru a redirecționa pachetele primite. În acest fel, diferite fluxuri de date sunt transmise pe diferite legături fizice pentru a implementa echilibrarea sarcinii. SRC MAC: Calculul se bazează pe adresele MAC sursă ale pachetelor. DST MAC: Calculul se bazează pe adresele MAC de destinație ale pachetelor. SRC MAC+DST MAC: Calculul se bazează pe adresele MAC sursă și destinație ale pachetelor. SRC IP: Calculul se bazează pe adresele IP sursă ale pachetelor. IP DST: Calculul se bazează pe adresele IP de destinație ale pachetelor. SRC IP+DST IP: Calculul se bazează pe adresele IP sursă și destinație ale pachetelor.

- Interfață VLAN

  În VLAN Interface, puteți configura Management VLAN și diferite interfețe VLAN pentru comutator. Informațiile generale ale interfeței VLAN existente sunt afișate în tabel.



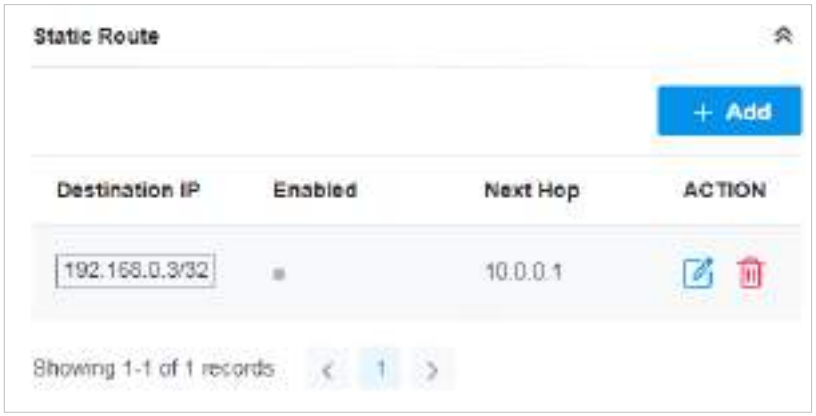
Pentru a configura o singură interfață VLAN, plasați mouse-ul pe intrare și faceți clic pentru a edita setările.



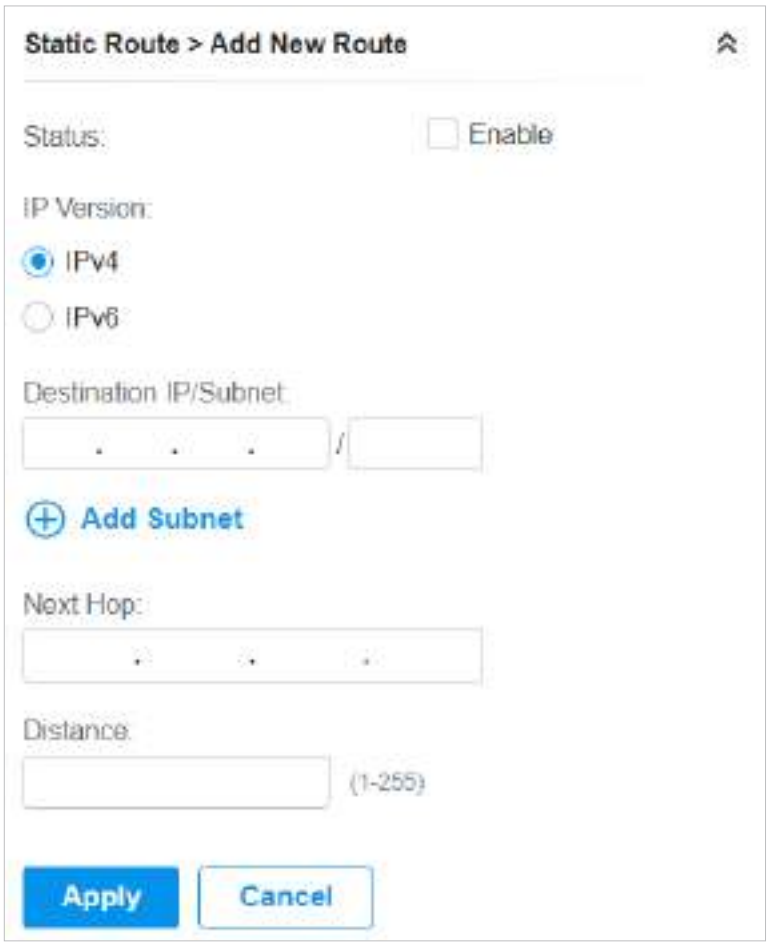
VLAN de management	Faceți clic pe caseta de selectare dacă doriți să utilizați interfața VLAN ca VLAN de gestionare. Rețineți că controlerul nu va reuși să vă gestioneze dispozitivele cu configurații de management VLAN greșite. Dacă nu sunteți sigur de condițiile rețelei dvs. și de impactul potențial al oricăror configurații, vă recomandăm să păstrați configurațiile implicite. VLAN-ul de management este un VLAN creat pentru a spori securitatea rețelei. Fără Management VLAN, comenzile de configurare și pachetele de date sunt transmise în aceeași rețea. Există riscuri ca utilizatorii neautorizați să acceseze pagina de management și să modifice configurațiile. Un VLAN de management poate separa rețeaua de management de rețeaua de date și poate reduce riscurile.
Modul Adresă IP (când Managementul VLAN activat)	Selectați un mod pentru ca interfața să obțină adresa IP, iar VLAN-ul va comunica cu alte rețele, inclusiv VLAN-uri cu adresa IP. Static: Atribuiți manual o adresă IP interfeței, specificațiAdresa IPșiMască de rețeapentru interfata. Când interfața VLAN este setată ca Management VLAN, este opțional să specificațiGateway implicitșiDNS primar/secundarpentru interfata. DHCP: Atribuiți o adresă IP interfeței printr-un server DHCP. Când doriți să permiteți dispozitivului să utilizeze o adresă IP fixă, activațiUtilizați o adresă IP fixă și specificațiRețeașiAdresa IPpe baza nevoilor. Când interfața VLAN este setată ca Management VLAN, puteți activa în continuare Adresă IP de rezervă, și specificațiAdresă IP de rezervă,Mască IP de rezervă, șiGateway de rezervă (opțional). Dacă interfața VLAN nu reușește să obțină o adresă IP de la serverul DHCP, adresa IP de rezervă va fi utilizată pentru interfață.
Opțiunea DHCP 12	Când DHCP este selectat ca Mod Adresă IP, puteți specifica numele de gazdă al clientului DHCP în câmp. Clientul DHCP va folosi opțiunea 12 pentru a-i spune serverului DHCP numele de gazdă.
Modul DHCP	Selectați un mod pentru clienții din VLAN pentru a obține adresa lor IP. Nici unul: Nu utilizați DHCP pentru a atribui adrese IP. Server DHCP: Atribuiți o adresă IP clienților printr-un server DHCP. Când este selectat Server DHCP, puteți specificaInterval DHCP, iar adresele IP din interval pot fi atribuite clienților din VLAN. De asemenea, este opțional să specificațiOpțiunea DHCP 138,DNS primar/secund,Gateway implicit, șiTimp de închiriere. Opțiunea DHCP 138 informează clientul DHCP despre adresa IP a controlerului atunci când clientul trimite o solicitare către serverul DHCP și specificați Opțiunea 138 ca adresa IP a controlerului aici. Lease Time decide cât timp clientul poate folosi adresa IP atribuită. DHCP Relay: permite clienților din VLAN să obțină adrese IP de la un server DHCP din subrețea diferită. Când este selectat DHCP Relay, specificați adresa IP a serverului DHCP în Adresa serverului.

Traseu Static

În Static Route, puteți configura intrările de rută statică pentru comutator. Informațiile generale ale intrărilor de rută statică existente sunt afișate în tabel. Pentru o rută statică existentă, faceți clic pentru a edita setările și faceți clic pentru a o șterge.



Pentru a adăuga o nouă intrare de rută statică, faceți clic + Add și configurați parametrii.

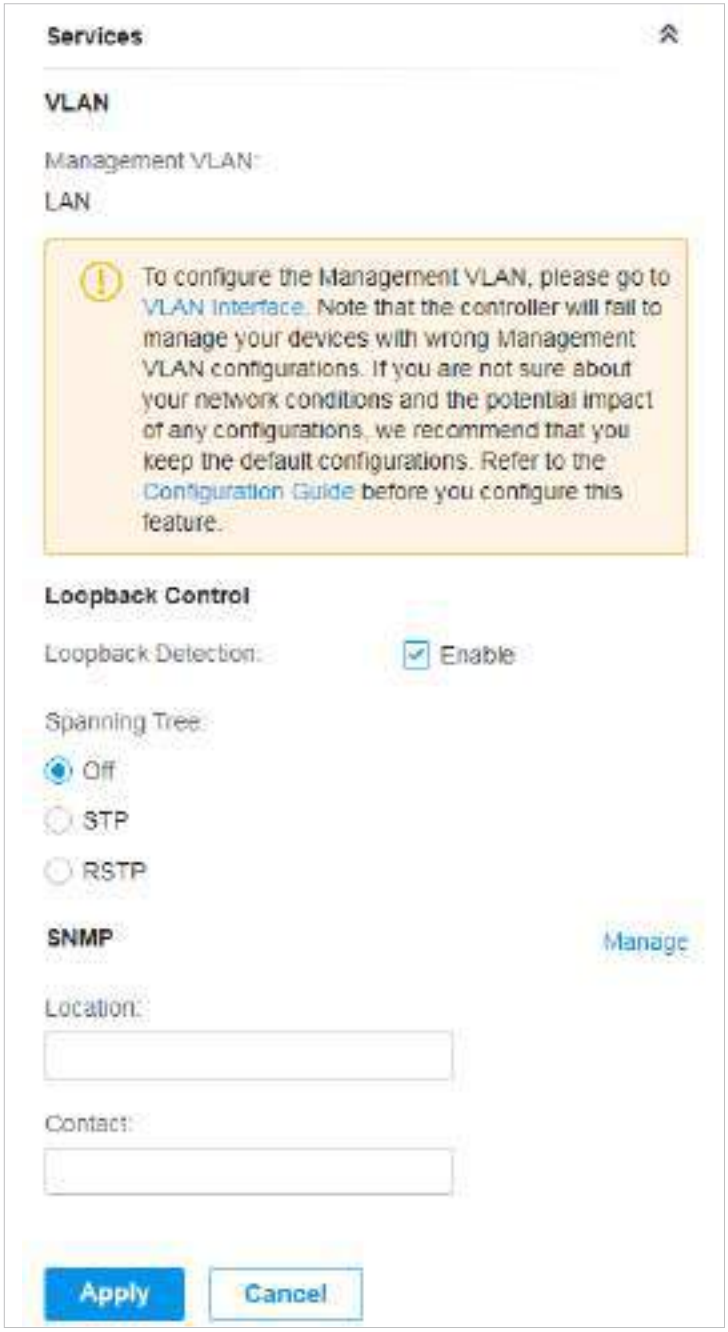


stare	Faceți clic pe caseta de selectare pentru a activa sau dezactiva ruta statică.
Versiunea IP	Selectați IPv4 sau IPv6.

IP destinație/ Subrețea	Când Versiunea IP este IPv4, specificațiIP/Subrețea de destinație. Când Versiunea IP este IPv6, specificați IP destinație/lungime prefix. Ele identifică traficul de rețea pe care îl controlează intrarea Static Route.
IP destinație/ Lungimea prefixului	Puteți da clic+ Adăugați subrețeapentru a specifica mai multe IP/Subrețele de destinație și faceți clic pe la ștergeți-le.
Următorul pas	Specificați adresa IP pentru dispozitivele dvs. pentru a redirecționa traficul de rețea corespunzător.
Distanţă	Specificați prioritatea unei rute statice. Este folosit pentru a decide prioritatea dintre rutele către aceeași destinație. Dintre rutele către aceeași destinație, ruta cu cea mai mică valoare a distanței va fi înregistrată în tabelul de rutare.

■ Servicii

În Servicii, puteți configura Management VLAN, Loopback Control și SNMP.



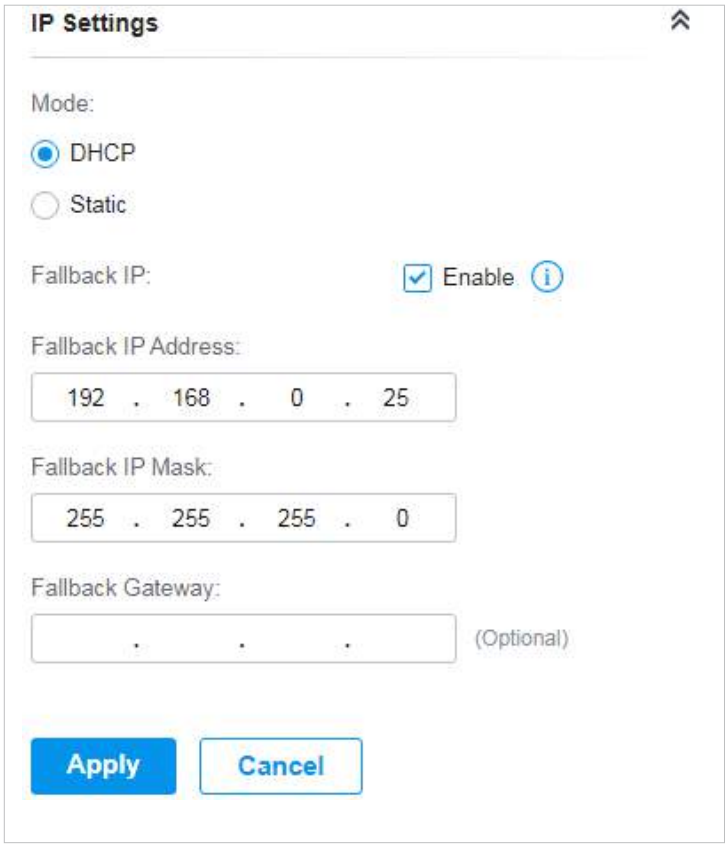
VLAN de management	Afișați numele VLAN-ului de management curent. Pentru a configura managementul VLAN, accesațiConfig>Interfață VLAN. Rețineți că controlerul nu va reuși să vă gestioneze dispozitivele cu configurații de management VLAN greșite. Dacă nu sunteți sigur de condițiile rețelei dvs. și de impactul potențial al oricăror configurații, vă recomandăm să păstrați configurațiile implicite. VLAN-ul de management este un VLAN creat pentru a spori securitatea rețelei. Fără Management VLAN, comenzile de configurare și pachetele de date sunt transmise în aceeași rețea. Există riscuri ca utilizatorii neautorizați să acceseze pagina de management și să modifice configurațiile. Un VLAN de management poate separa rețeaua de management de rețeaua de date și poate reduce riscurile.
Detectare Loopback	Când este activat, comutatorul verifică rețeaua în mod regulat pentru a detecta loopback-ul. Rețineți că Lopback Detection și Spanning Tree nu sunt disponibile în același timp.
Spanning Tree	Selectați un mod pentru Spanning Tree. Această caracteristică este disponibilă numai când Detectarea buclei este dezactivată. Oprit: Dezactivează Spanning Tree pe comutator. STP: Activați STP (Spanning Tree Protocol) pentru a preveni buclele în rețea. STP ajută la blocarea anumitor porturi ale comutatoarelor pentru a construi o topologie fără bucle și pentru a detecta modificările de topologie și pentru a genera automat o nouă topologie fără bucle. RSTP: Activați RSTP (Rapid Spanning Tree Protocol) pentru a preveni buclele în rețea. RSTP oferă aceleași caracteristici ca și STP, cu o convergență mai rapidă a arborelui. Prioritate: Când STP/RSTP este activat, specificați prioritatea comutatorului în Spanning Tree. În STP/RSTP, comutatorul cu cea mai mare prioritate va fi selectat ca rădăcină a arborelui spanning. Comutatorul cu valoarea mai mică are prioritate mai mare.
SNMP	(Numai pentru configurarea unui singur dispozitiv) Configurați SNMP pentru a nota locația și detaliile de contact. De asemenea, puteți face clicAdministraa sari laSetări>Servicii>SNMP, iar pentru configurarea detaliată a serviciului SNMP, consultați3. 10. 4 SNMP.

■ Setări IP (Numai pentru configurarea unui singur dispozitiv)

În Setări IP, selectați un mod IP și configurați parametrii pentru dispozitiv.

Dacă selectațiDHCPca mod, asigurați-vă că există un server DHCP în rețea și apoi dispozitivul va obține automat adresa IP dinamică de la serverul DHCP. Puteți seta un IP alternativ

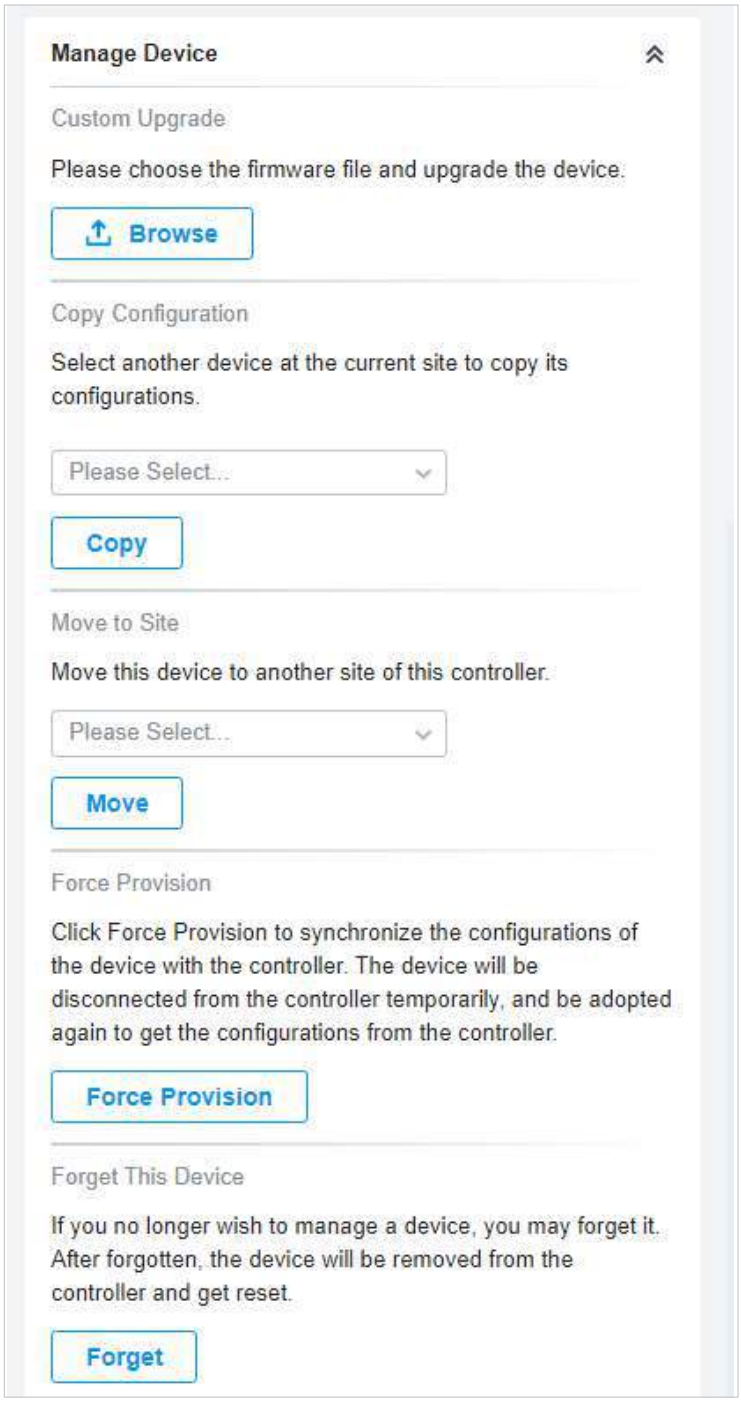
adresa pentru a păstra o adresă IP în rezervă pentru situația în care dispozitivul nu reușește să obțină o adresă IP dinamică. Activați IP de rezervă și apoi setați adresa IP, masca IP și gateway-ul.



Dacă selectațiStaticca mod, setați adresa IP, masca IP, gateway-ul și serverul DNS pentru adresa statică.

Gestionați dispozitivul

În Manage Device, puteți actualiza manual versiunea de firmware a dispozitivului, o puteți muta pe alt site, puteți sincroniza configurațiile cu controlerul și uitați comutatorul.



Upgrade personalizat	ClicNavigași alegeți un fișier de pe computer pentru a actualiza dispozitivul. La actualizare, dispozitivul va fi repornit și readoptat de controler. De asemenea, puteți bifa caseta deActualizați toate dispozitivele de același modelpe site după ce fișierul firmware este încărcat.
Copiați configurația	Selectați alt dispozitiv de pe site-ul curent pentru a-i copia configurațiile.

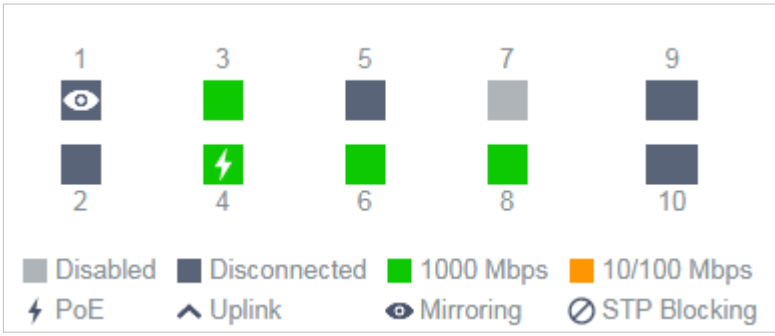
Mutați pe site	Selectați un site în care va fi mutat dispozitivul. După mutarea pe alt site, configurațiile dispozitivului de pe site-ul anterior vor fi înlocuite cu cele de pe noul site, iar istoricul traficului acestuia va fi șters.
Furnizare de forță	(Numai pentru configurarea unui singur dispozitiv) Faceți clicFurnizare de forțăpentru a sincroniza configurațiile dispozitivului cu controlerul. Dispozitivul își va pierde temporar conexiunea și va fi adoptat din nou la controler pentru a obține configurațiile de la controler.
Uitați acest dispozitiv	ClicA uitaiar apoi dispozitivul va fi scos din controler. Odată uitate, toate configurațiile și istoricul legat de dispozitiv vor fi șterse.

5. 3. 2 Comutatoare monitor

Un panou și patru file sunt furnizate pentru a monitoriza dispozitivul în fereastra Proprietăți: Panou monitor, Detalii, Clienți și Statistici.

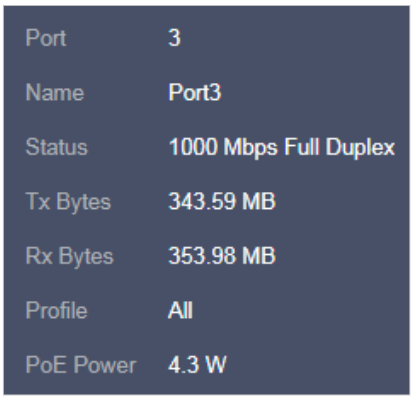
Panoul de monitorizare

Panoul monitorului afișează porturile comutatorului și folosește culori și pictograme pentru a indica starea conexiunii și tipul portului. Când comutatorul este în așteptare sau este deconectat, toate porturile sunt dezactivate.



PoE	Un port PoE conectat la un dispozitiv alimentat (PD).
Uplink	Un port uplink conectat la WAN.
Oglindire	Un port de oglindire care reflectă un alt port de comutare.
Blocare STP	Un port în starea Blocare în Spanning Tree. Acesta primește și trimite pachete BPDU (Bridge Protocol Data Unit) pentru a menține arborele de acoperire. Alte pachete sunt aruncate.

Puteți trece cursorul peste pictograma portului (cu excepția porturilor dezactivate) pentru mai multe detalii. Informațiile afișate variază în funcție de starea conexiunii și tipul de port.



stare	Afișează viteza de negociere a portului.
Tx Bytes	Afișează cantitatea de date transmisă ca octeți.
Rx Bytes	Afișează cantitatea de date primite ca octeți.
Profil	Afișează numele profilului aplicat portului, care definește modul în care sunt gestionate pachetele atât în direcțiile de intrare, cât și de ieșire. Pentru configurarea detaliată, consultați3. 8 Creați profiluri.
Putere PoE	Afișează sursa de alimentare PoE pentru dispozitivul PD.
Uplink	Afișează numele dispozitivului conectat la portul uplink.
Oglindirea de la	Afișează numele portului care este reflectat.
ID LAG	Afișează numele porturilor care sunt agregate într-o interfață logică.

Detalii

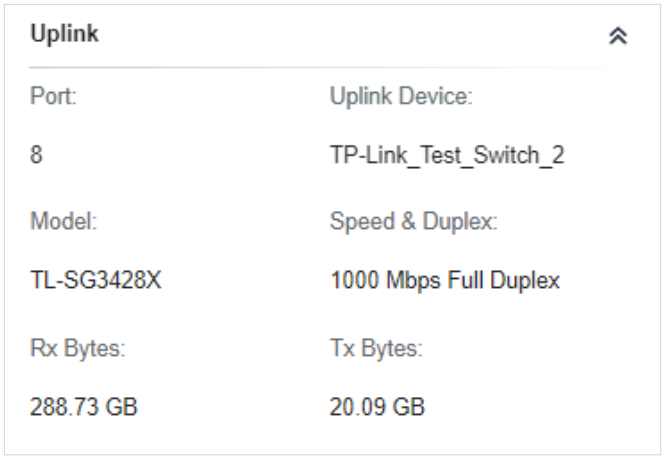
În Detalii, puteți vizualiza informațiile de bază, informațiile despre trafic și informațiile radio ale dispozitivului pentru a afla starea de funcționare a dispozitivului.

- Prezentare generală

  În Prezentare generală, puteți vizualiza informațiile de bază ale dispozitivului. Informațiile enumerate vor fi variate în funcție de modelul și starea dispozitivului.

- Uplink (Numai pentru comutatorul conectat la un router/switch gestionat de Omada în starea Conectat)

  ClicUplinkpentru a vizualiza informațiile uplink, inclusiv portul uplink, dispozitivul uplink, viteza de negociere și rata de transmisie.

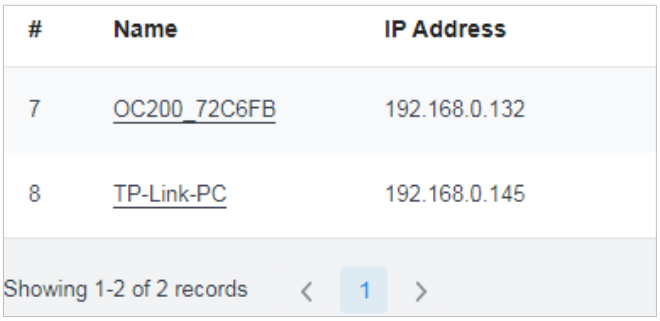


- Legătură în jos (numai pentru comutatorul conectat la dispozitivele gestionate de Omada în starea Conectat)

  ClicLegătură în jospentru a vizualiza informațiile downlink, inclusiv porturile downlink, numele și modelul dispozitivelor, precum și viteza de negociere.

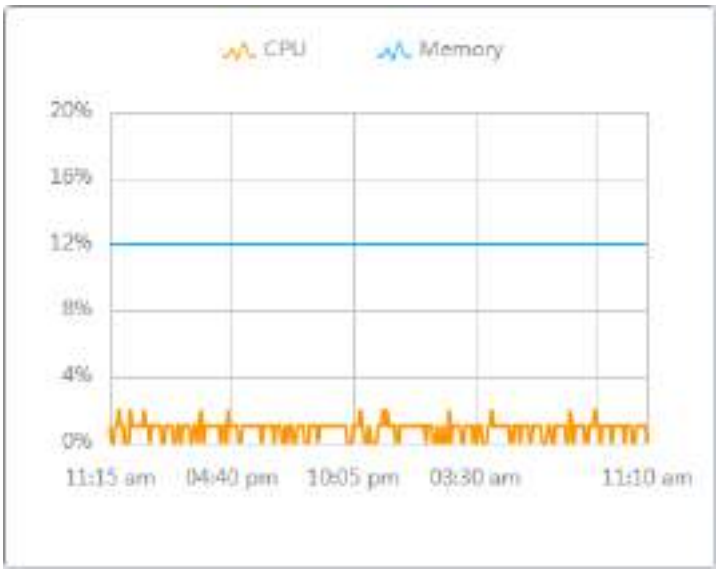
Clienții

În Clienți, puteți vizualiza informațiile clienților conectați la comutator, inclusiv numele clientului, adresa IP și portul conectat. Puteți face clic pe numele clientului pentru a deschide fereastra de Proprietăți.



Statistici

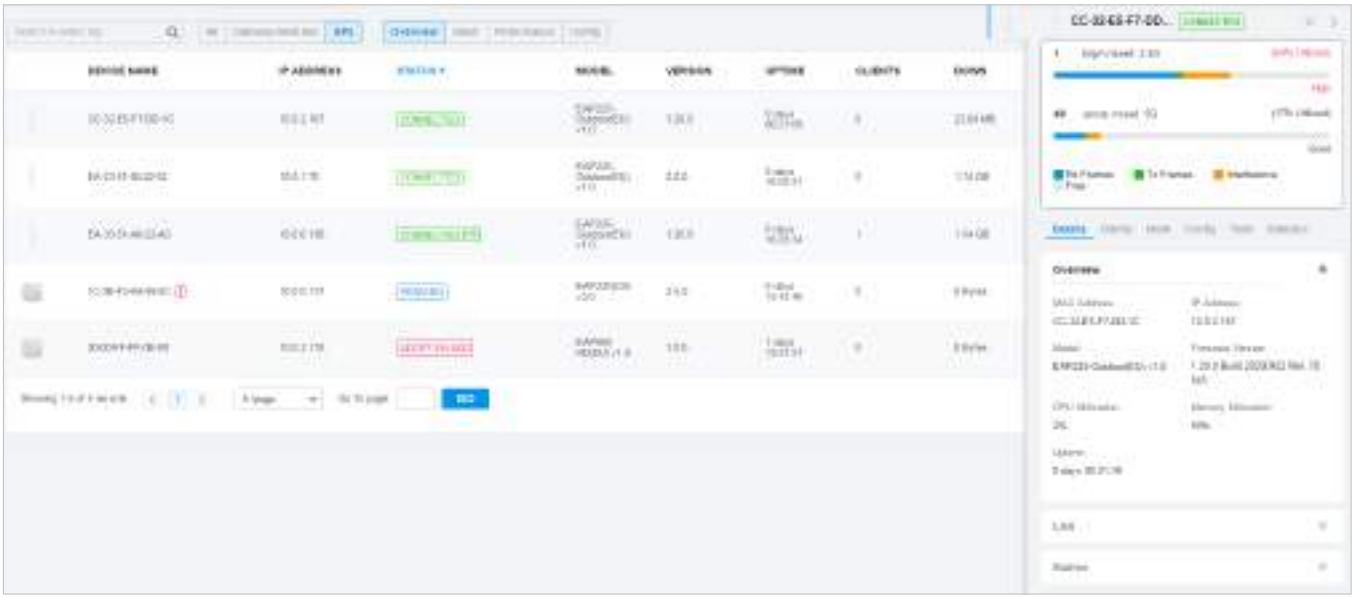
În Statistică, puteți monitoriza CPU și memoria dispozitivului în ultimele 24 de ore prin diagrame. Pentru a vizualiza statisticile dispozitivului într-o anumită perioadă, faceți clic pe diagramă la care săriți7. 2 Vizualizați Statisticile rețelei .



5. 4 Configurați și monitorizați EAP-urile

În fereastra Proprietăți, puteți configura unul sau câteva EAP-uri conectate la controler și puteți monitoriza performanța și statisticile. Configurațiile modificate în fereastra Proprietăți vor fi aplicate numai AP-urilor selectate. În mod implicit, toate configurațiile sunt sincronizate cu site-ul curent.

Pentru a deschide fereastra Proprietăți, faceți clic pe intrarea unui AP sau faceți clicAcțiune în lot, și apoiConfigurare lotpentru a selecta AP-uri pentru configurarea lotului. Un panou de monitor și mai multe file sunt listate în fereastra Proprietăți. Cele mai multe caracteristici care trebuie configurate sunt adunate în fila Config, cum ar fi IP, radiouri, SSID și VLAN, în timp ce alte file sunt utilizate în principal pentru a monitoriza dispozitivul.



Notă:

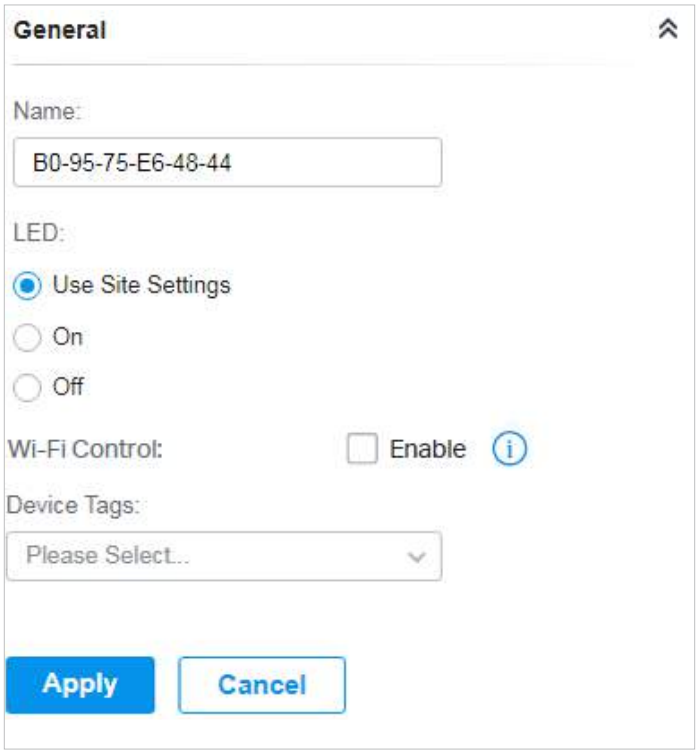
- Funcțiile disponibile în fereastră variază în funcție de modelul și starea dispozitivului.
- În Batch Config, puteți configura doar dispozitivele selectate, iar configurațiile nealterate vor păstra setările curente.
- În Batch Config, dacă unele funcții, cum ar fi banda de 5 GHz, sunt disponibile numai pe anumite EAP-uri selectate, configurațiile corespunzătoare nu vor avea efect. Pentru a le configura cu succes, verificați mai întâi modelul dispozitivelor selectate.

5. 4. 1 Configurați EAP-urile

În fereastra Proprietăți, faceți clicConfigapoi faceți clic pe secțiuni pentru a configura caracteristicile aplicate AP-urilor selectate.

General

În general, puteți specifica numele dispozitivului și setările LED-ului AP și le puteți clasifica prin etichete de dispozitiv.



Nume	(Numai pentru configurarea unui singur dispozitiv) Specificați un nume pentru dispozitiv.
LED	Selectați modul în care funcționează LED-urile dispozitivului respectiv. Utilizați Setările site-ului: LED-ul dispozitivului va funcționa urmând setările site-ului. Pentru a vizualiza și modifica setările site-ului, consultați3. 2. 2 Servicii. Pe/Oprit: LED-ul dispozitivului va rămâne aprins/stins.
Control Wi-Fi	(Numai pentru anumite puncte de acces pentru plăci de perete) Activați controlul Wi-Fi și va intra în vigoare numai când caracteristica LED este activată. După activarea controlului Wi-Fi, puteți apăsa butonul LED de pe AP pentru a porni/dezactiva simultan Wi-Fi și LED-ul.
Etichete dispozitiv	Selectați o etichetă din lista derulantă sau creați o nouă etichetă pentru a clasifica dispozitivul.

Setări IP (Numai pentru configurarea unui singur dispozitiv)

În Setări IP, selectați un mod IP și configurați parametrii pentru dispozitiv.

Dacă selectațiDHCPca mod, asigurați-vă că există un server DHCP în rețea și apoi dispozitivul va obține automat adresa IP dinamică de la serverul DHCP. Dacă doriți să lăsați dispozitivul să utilizeze o adresă IP fixă, puteți activa Utilizare adresă IP fixă și puteți seta rețeaua și adresa IP în funcție de nevoi. De asemenea, puteți seta o adresă IP de rezervă pentru a păstra o adresă IP în rezervă

situația în care dispozitivul nu reușește să obțină o adresă IP dinamică. Activați IP de rezervă și apoi setați adresa IP, masca IP și gateway-ul.

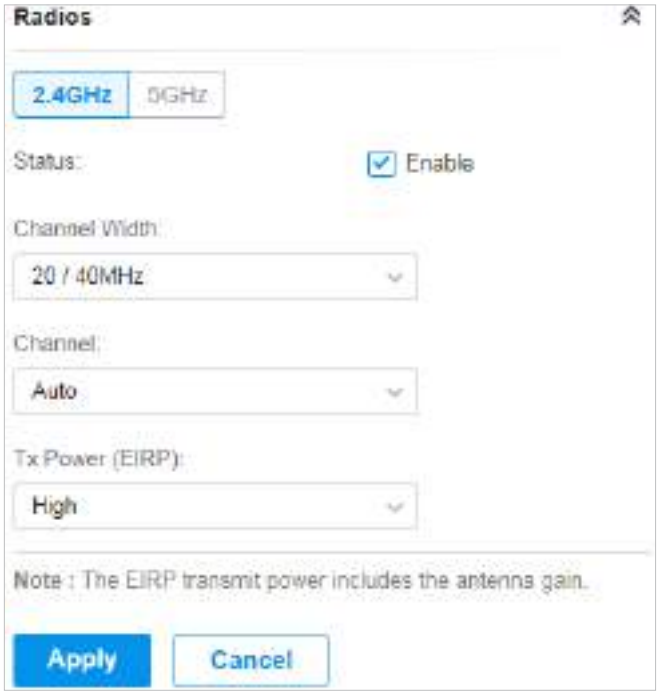
Dacă selectațiStaticca mod, setați adresa IP, masca IP, gateway-ul și serverul DNS pentru adresa statică.

Radiouri

În Radiouri, puteți controla cum și ce tip de semnale radio emite EAP. Selectați banda de frecvență  și configurați următorii parametri.

Notă:

Banda de 6 GHz este disponibilă numai pentru anumite dispozitive.



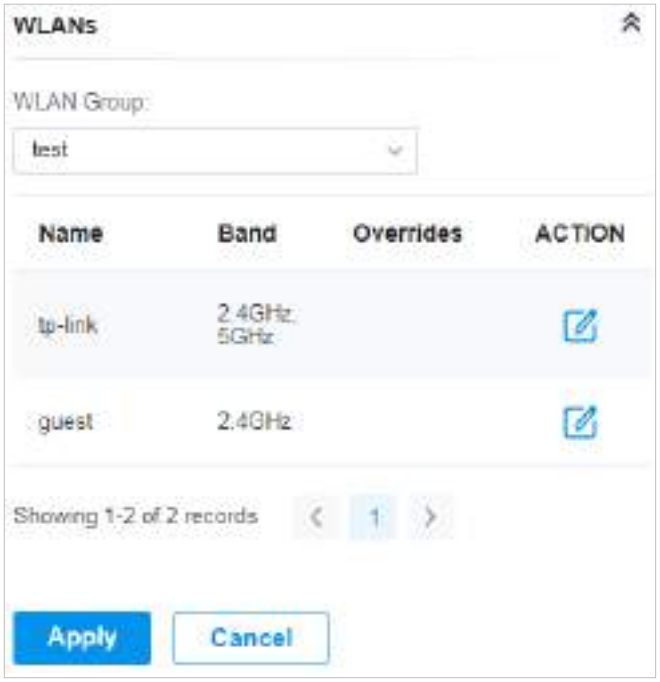
stare	Dacă dezactivați banda de frecvență, radioul de pe ea se va opri.
latimea canalului	Specificați lățimea canalului benzii. Diferitele benzi au diferite opțiuni disponibile. Vă recomandăm să utilizați valoarea implicită.
Canal	Specificați canalul de operare al EAP pentru a îmbunătăți performanța wireless. Dacă selectați Autopentru setarea canalului, EAP scanează canalele disponibile și selectează canalul unde este detectat cel mai mic trafic.
Putere Tx	Specificați Tx Power (Transmit Power) în cele 4 opțiuni: Low, Medium, High și Custom. Puterea reală a scăzut, mediu și ridicat se bazează pe puterea minimă de transmisie (Min. Txpower) și puterea maximă de transmisie (Max. TxPower), care pot varia în diferite țări și regiuni. Scăzut: Min. TxPower + (Max. TxPower-Min. TxPower) * 20% (rotunjește valoarea) Mediu: Min. TxPower + (Max. TxPower-Min. TxPower) * 60% (rotunjește valoarea) Înalt: Max. TxPower Personalizat: Specificați manual valoarea.

rețele WLAN

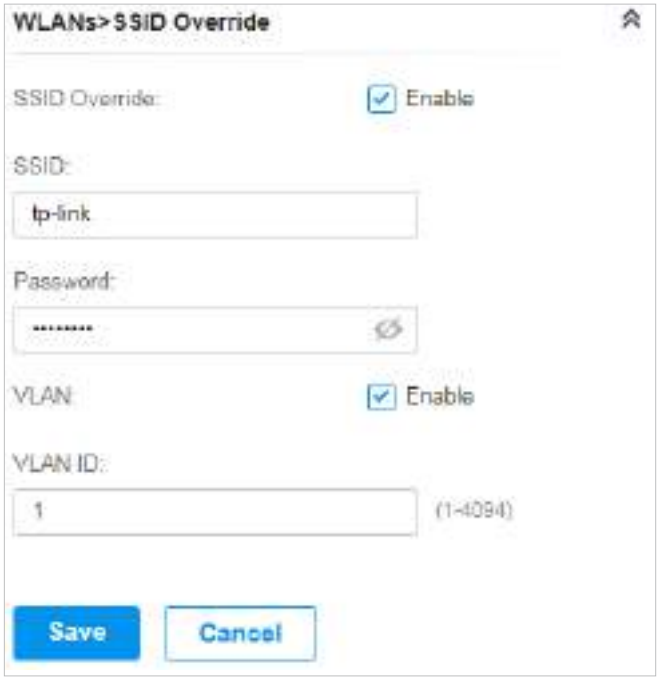
În rețele WLAN, puteți aplica grupul WLAN la EAP și puteți specifica un nume și o parolă SSID diferite pentru a înlocui SSID-ul din grupul WLAN. După aceea, clienții pot vedea doar noul SSID și pot folosi noua parolă pentru a accesa rețeaua. Pentru a crea sau edita grupuri WLAN, consultați3. 4 Configurați rețele wireless .

Notă:

Banda de 6 GHz este disponibilă numai pentru anumite dispozitive.



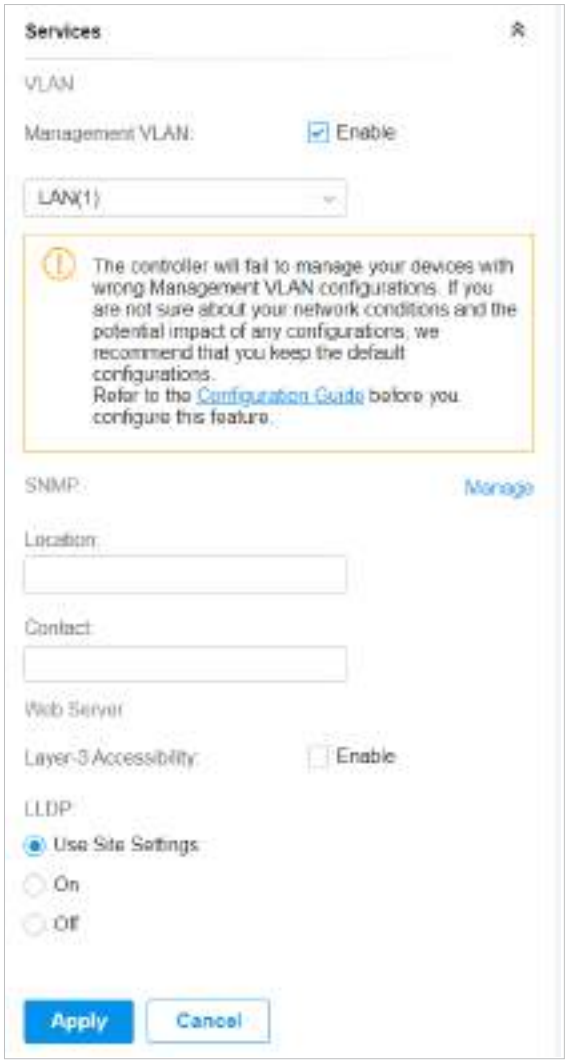
(Numai pentru configurarea unui singur dispozitiv) Pentru a suprascrie SSID, selectați un grup WLAN, în intrare faceți clic și apoi apare următoarea pagină.



Suprascriere SSID	Activați sau dezactivați anularea SSID pe EAP. Dacă SSID Override este activată, specificați noul SSID și parola pentru a o înlocui pe cea actuală.
VLAN	Activați sau dezactivați VLAN. Dacă VLAN este activat, introduceți un ID VLAN pentru a adăuga noul SSID la VLAN.

■ Servicii

În Servicii, puteți configura Management VLAN pentru a vă proteja rețeaua și SNMP pentru a nota locația și detaliile de contact.

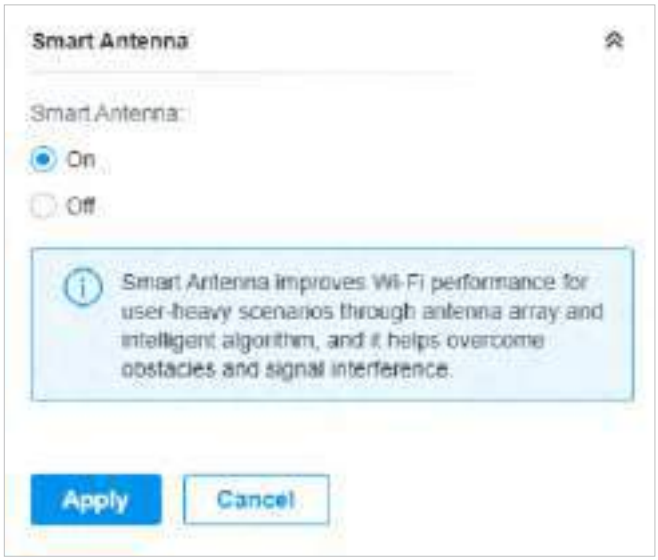


VLAN de management	Pentru a configura Management VLAN, creați o rețea înLANmai întâi, apoi selectați-l ca VLAN de gestionare pe această pagină. Pentru detalii, consultați3. 3 Configurați rețelele cu fir. VLAN-ul de management este un VLAN creat pentru a spori securitatea rețelei. Fără Management VLAN, comenzile de configurare și pachetele de date sunt transmise în aceeași rețea. Există riscuri ca utilizatorii neautorizați să acceseze pagina de management și să modifice configurațiile. Un VLAN de management poate separa rețeaua de management de rețeaua de date și poate reduce riscurile.

SNMP	(Numai pentru configurarea unui singur dispozitiv) Configurați SNMP pentru a nota locația și detaliile de contact. De asemenea, puteți face clicAdministraa sari laSetări>Servicii>SNMP, iar pentru configurarea detaliată a serviciului SNMP, consultați3. 10. 4 SNMP.
Accesibilitate layer-3	Cu această caracteristică activată, dispozitivele dintr-o subrețea diferită pot accesa dispozitivele gestionate de Omada.
LLDP	LLDP (Link Layer Discovery Protocol) poate ajuta la descoperirea dispozitivelor.

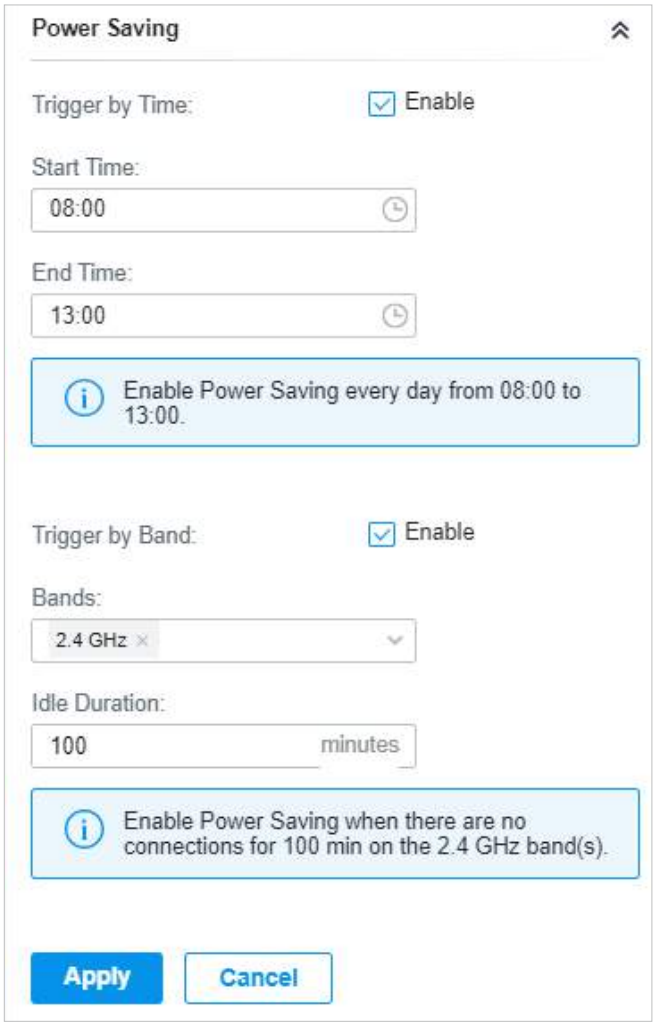
■ Antenă inteligentă

În Smart Antenna, puteți activa funcția pentru a îmbunătăți performanța Wi-Fi pentru scenarii grele de utilizator prin matrice de antene și algoritm inteligent. Acest lucru ajută la depășirea obstacolelor și la semnalizarea interferențelor.



■ Economisire de energie

În Power Saving, puteți personaliza la ce perioadă sau bandă pentru a economisi consumul de energie al AP-ului. Setați următorii parametri în funcție de nevoile dvs.

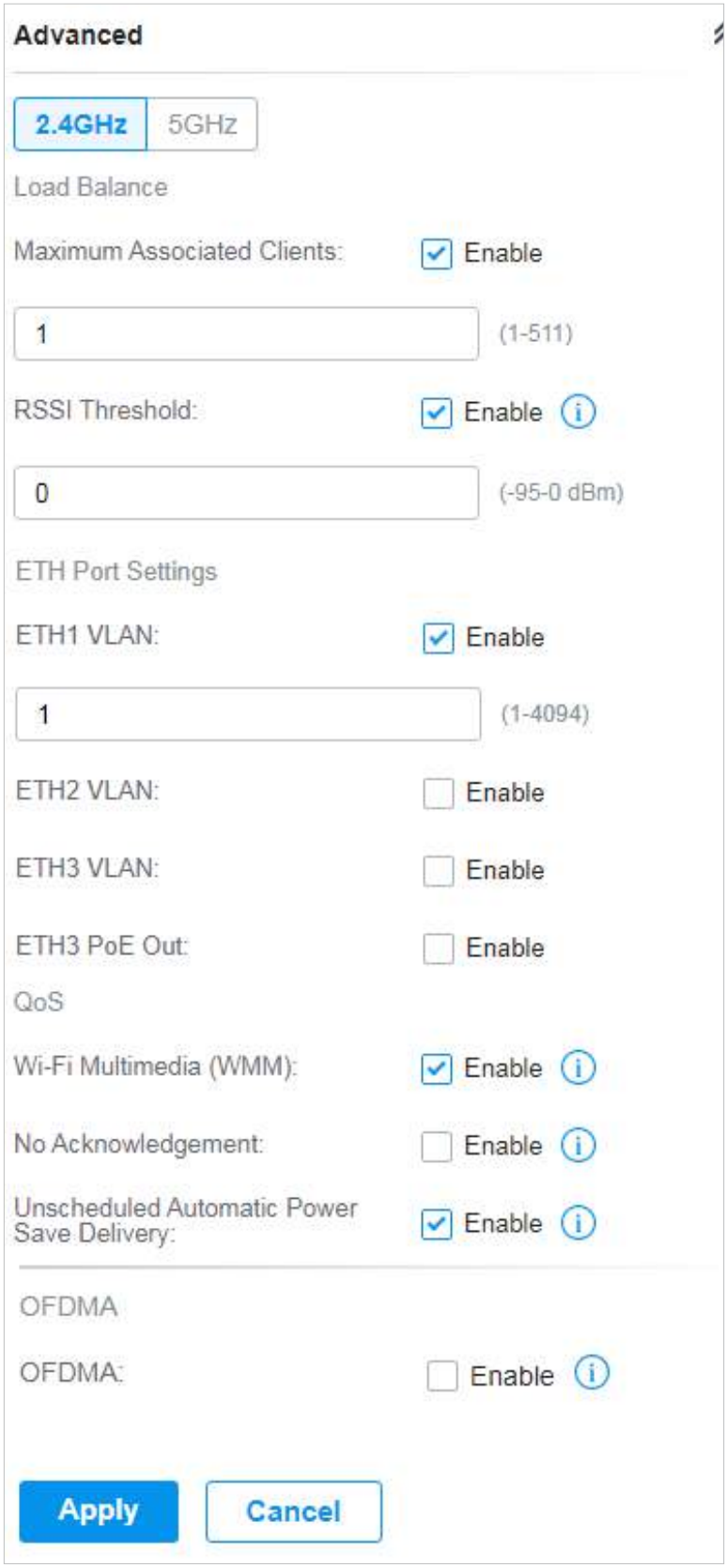


Declanșează de timp	PermiteDeclanșează de timp, și specificațiTimpul de începereșiSfârșitul timpuluipentru a economisi energia zilnic.
Declanșare după bandă	PermiteDeclanșare după bandăși configurați parametrii: Benzi:Selectați banda pentru Economisire energie. Durata inactiv:Introduceți un număr nu mai mic de 60. Dacă perioada de deconectare a AP-ului depășește Durata Idle, va fi declanșată Economisirea energiei benzii prestabilite.

■ Avansat

În Advanced, configurați Load Balance și QoS pentru a utiliza mai bine resursele rețelei. Load Balance poate controla numărul de client asociat EAP, în timp ce QoS poate optimiza performanța atunci când gestionează traficuri wireless diferențiate, inclusiv date IP tradiționale, VoIP (Voice-over Internet Protocol) și alte tipuri de media audio, video, streaming.

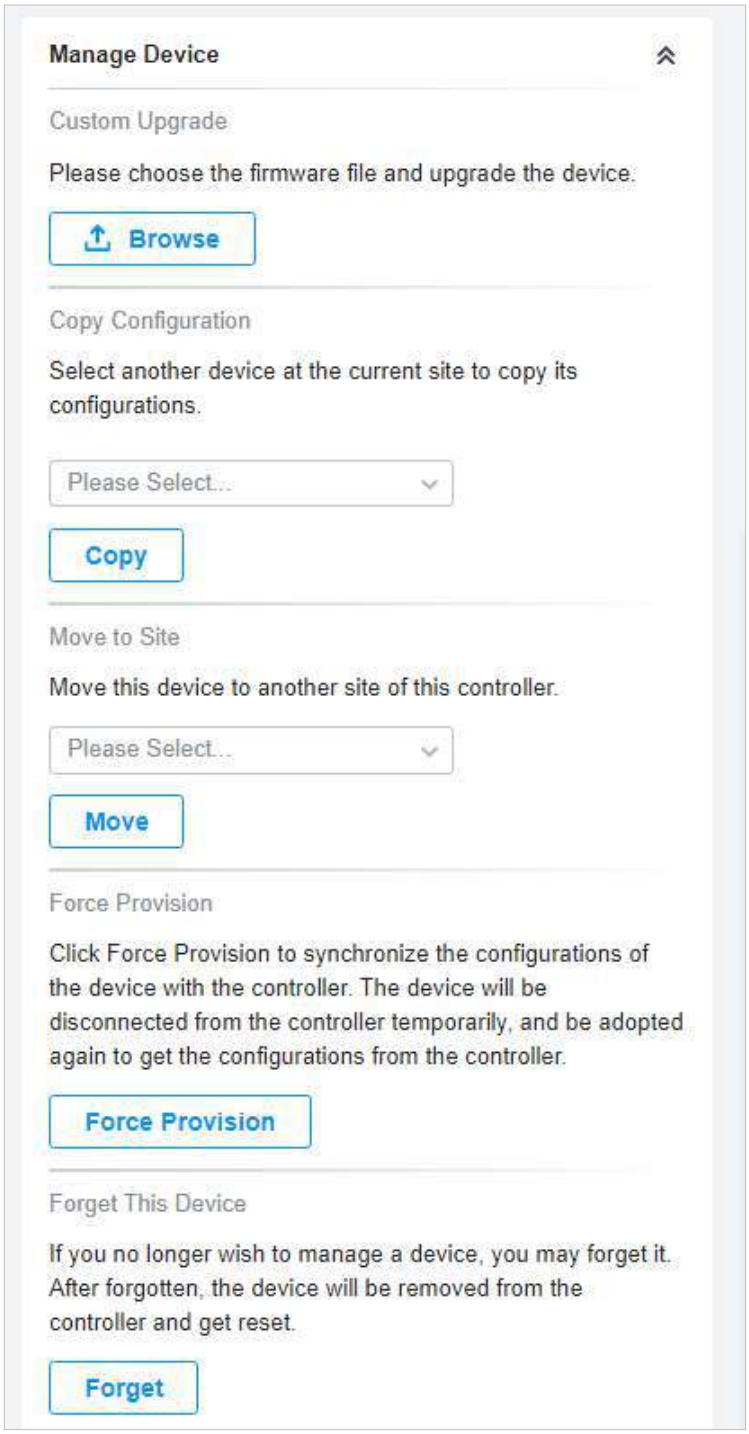
Selectați banda de frecvență 2.4GHz 5GHz și configurați următorii parametri și caracteristici.



Max Clienți Asociați	Activați această funcție și specificați numărul maxim de clienți conectați. Dacă clientul conectat atinge numărul maxim, EAP-ul îi va deconecta pe cei cu semnale mai slabe pentru a face loc altor clienți care solicită conexiuni.
Pragul RSSI	Activați această funcție și introduceți pragul RSSI (Received Signal Strength Indication). Dacă puterea semnalului clientului este mai slabă decât pragul, clientul va pierde conexiunea cu EAP.
ETH VLAN/ETH2 VLAN/ ETH3 VLAN	(Numai pentru Wall Plate AP) Activați această funcție și adăugați portul LAN al AP-ului corespunzător la VLAN-ul specificat aici. Apoi, gazdele conectate la acest EAP pot comunica doar cu dispozitivele din acest VLAN.
ETH3 PoE Out	(Numai pentru Wall Plate AP cu portul de ieșire PoE) Activați această funcție pentru a furniza energie dispozitivului conectat pe acest port.
Wi-Fi Multimedia (WMM)	Cu WMM activat, EAP menține prioritatea pachetelor audio și video pentru o performanță media mai bună.
Fără recunoaștere	Activați această funcție pentru a specifica că EAP-urile nu vor confirma cadre cu QoS No Ack. Activarea No Acknowledgement poate aduce un debit mai eficient, dar poate crește ratele de eroare într-un mediu zgomotos de radiofrecvență (RF).
Automat neprogramat Livrare cu economie de energie	Când este activată, această funcție poate îmbunătăți considerabil capacitatea de economisire a energiei a clienților.
OFDMA	(Numai pentru AP care acceptă 802.11 ax) Activați această caracteristică pentru a permite mai multor utilizatori să transmită date simultan și va îmbunătăți considerabil viteza și eficiența. Rețineți că beneficiile OFDMA pot fi profitate pe deplin numai atunci când clienții acceptă OFDMA.

Gestionați dispozitivul

În Manage Device, puteți actualiza manual versiunea de firmware a dispozitivului, o puteți muta pe alt site, puteți sincroniza configurațiile cu controlerul și uitați de AP.



Upgrade personalizat	ClicNavigași alegeți un fișier de pe computer pentru a actualiza dispozitivul. La actualizare, dispozitivul va fi repornit și readoptat de controler. De asemenea, puteți bifa caseta deActualizați toate dispozitivele de același modelpe site după ce fișierul firmware este încărcat.
Copiați configurația	Selectați alt dispozitiv de pe site-ul curent pentru a-i copia configurațiile.

Mutați pe site	Selectați un site în care va fi mutat dispozitivul. După mutarea pe alt site, configurațiile dispozitivului de pe site-ul anterior vor fi înlocuite cu cele de pe noul site, iar istoricul traficului acestuia va fi șters.
Furnizare de forță	(Numai pentru configurarea unui singur dispozitiv) Faceți clicFurnizare de forțăpentru a sincroniza configurațiile dispozitivului cu controlerul. Dispozitivul își va pierde temporar conexiunea și va fi adoptat din nou la controler pentru a obține configurațiile de la controler.
Uitați acest AP	ClicA uitaiar apoi dispozitivul va fi scos din controler. Odată uitate, toate configurațiile și istoricul legat de dispozitiv vor fi șterse.

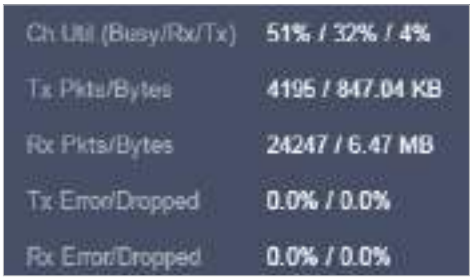
5. 4. 2 Monitorizați EAP-urile

Un panou și patru file sunt furnizate pentru a monitoriza dispozitivul în fereastra Proprietăți: Panou monitor, Detalii, Clienți, Mesh și Statistici.

Panoul de monitorizare

Panoul de monitor ilustrează informațiile despre canalul activ pe fiecare bandă radio, inclusiv canalul de operare al EAP, modul radio și utilizarea canalului. Patru culori sunt folosite pentru a indica procentul de cadre Rx (albastru), Cadre Tx (verde), Interferență (portocaliu) și lățime de bandă liberă (gri).

Puteți trece cursorul peste bara de canal pentru mai multe detalii.



Ch.Util.(Ocupat/Rx/Tx)	Afișează statisticile de utilizare a canalului. **Ocupat**: Afișează suma Tx, Rx și, de asemenea, interferențe non-WiFi, care indică cât de ocupat este canalul. **Rx**: Indică cât de des se află radioul în modul de recepție activ. **Tx**: Indică cât de des se află radioul în modul de transmisie activ.
Tx Pkts/Bytes	Afișează cantitatea de date transmise ca pachete și octeți.
Rx Pkts/Bytes	Afișează cantitatea de date primite ca pachete și octeți.
Eroare Tx/Scăpat	Afișează procentul de pachete transmise care au erori și procentul de pachete care au fost abandonate.
Eroare Rx/Scăpat	Afișează procentul de pachete de primire care au erori și procentul de pachete care au fost abandonate.

Detalii

În Detalii, puteți vizualiza informațiile de bază, informațiile despre trafic și informațiile radio ale dispozitivului pentru a afla starea de funcționare a dispozitivului.

■ Prezentare generală

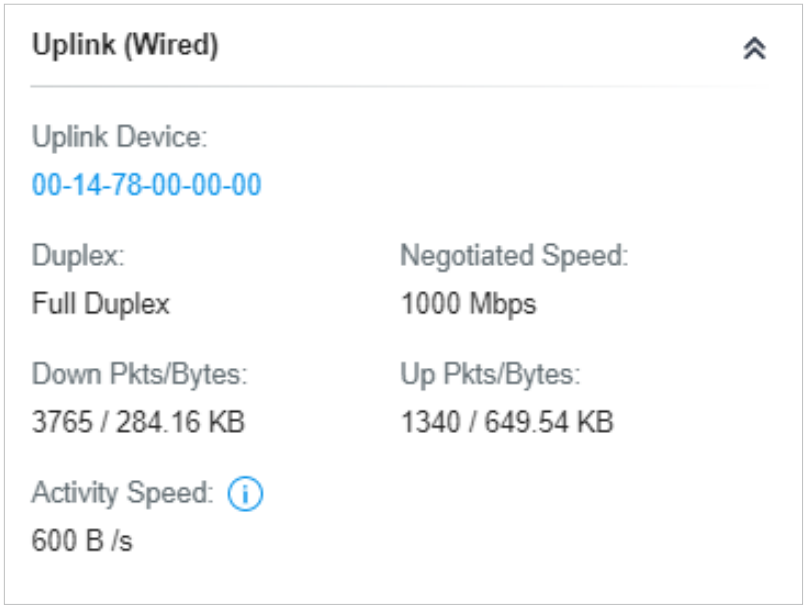
În Prezentare generală, puteți vizualiza informațiile de bază ale dispozitivului. Informațiile listate variază în funcție de starea dispozitivului.

■ LAN (Numai pentru dispozitivele în starea Conectat)

ClicLANpentru a vizualiza informațiile de trafic ale portului LAN, inclusiv numărul total de pachete, dimensiunea totală a datelor, numărul total de pierderi de pachete și dimensiunea totală a datelor de eroare în procesul de primire și transmitere a datelor.

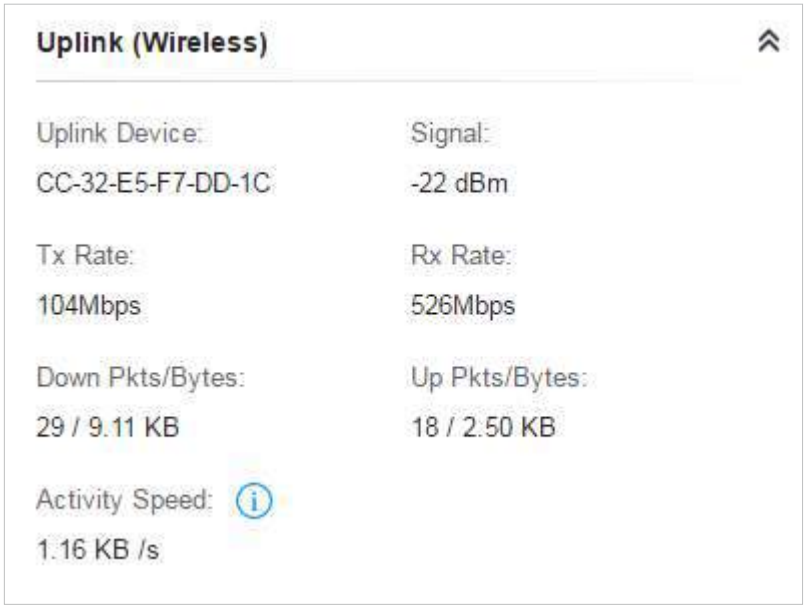
- Uplink (prin cablu) (numai pentru dispozitivele în starea Conectat)

  Dacă EAP este conectat la controler prin cablu, faceți clicUplink (prin cablu)pentru a vizualiza informațiile de trafic legate de dispozitivul uplink, inclusiv modul de transmisie a datelor (Duplex), viteza negociată, raportul dintre numărul și dimensiunea pachetelor și rata dinamică în aval.



- Uplink (Wireless) (Numai pentru dispozitivele în starea Conectat)

  Dacă EAP este conectat la un uplink AP fără fir, faceți clicUplink (Wireless)pentru a vizualiza informațiile de trafic legate de AP-ul uplink, inclusiv puterea semnalului, rata de transmisie, raportul dintre numărul și dimensiunea pachetelor și rata dinamică în aval.



- Radiouri (Numai pentru dispozitivele în starea Conectat)

  ClicRadiouripentru a vizualiza informațiile radio, inclusiv banda de frecvență, modul wireless, lățimea canalului, canalul și puterea de transmisie. De asemenea, puteți vizualiza parametrii de recepție/transmitere a datelor pe fiecare bandă radio.

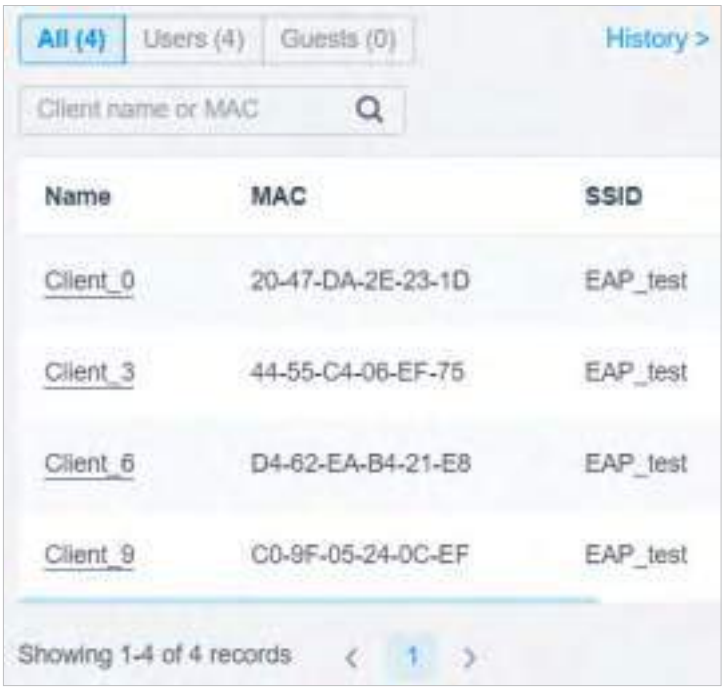
  Notă:

  Banda de 6 GHz este disponibilă numai pentru anumite dispozitive.

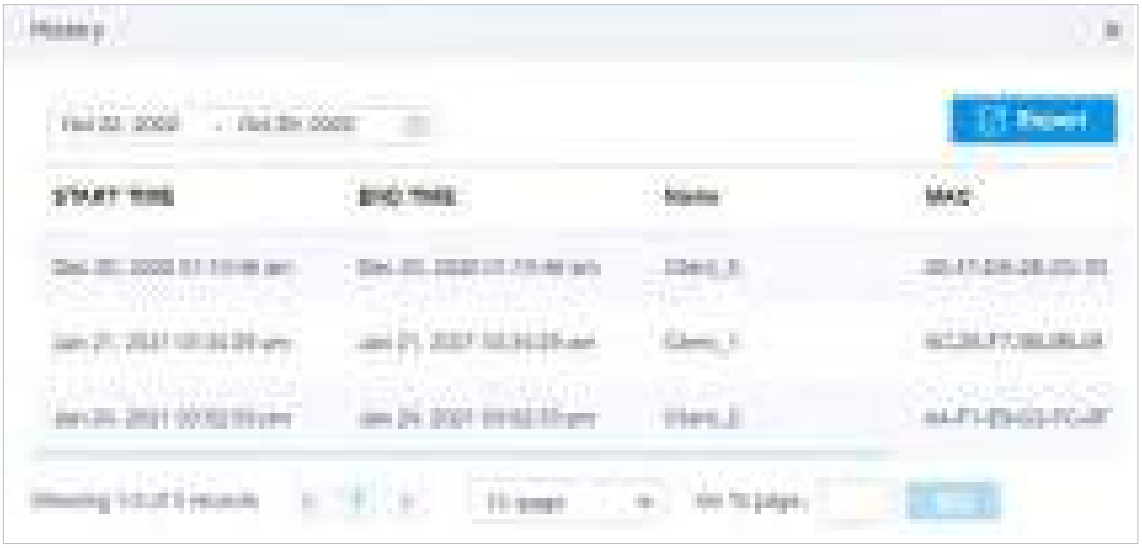
Clienții

În Clienți, puteți vizualiza informațiile utilizatorilor și oaspeților care se conectează la AP, inclusiv numele clientului, adresa MAC și SSID-ul conectat. Utilizatorii sunt clienți conectați la SSID-ul AP-ului cu Guest

Rețeaua dezactivată, în timp ce oaspeții sunt clienți conectați cu rețeaua pentru oaspeți activată. Puteți face clic pe numele clientului pentru a deschide fereastra de Proprietăți.



Faceți clic pe Istoric pentru a vedea istoricul clienților. În pagina Istoric, puteți specifica data sau perioada de timp pentru a vizualiza clienții conectați într-un anumit timp și faceți clic pe Export pentru a descărca lista de clienți.



Mesh (Numai pentru dispozitivele în așteptare/conectate/izolate care acceptă Mesh)

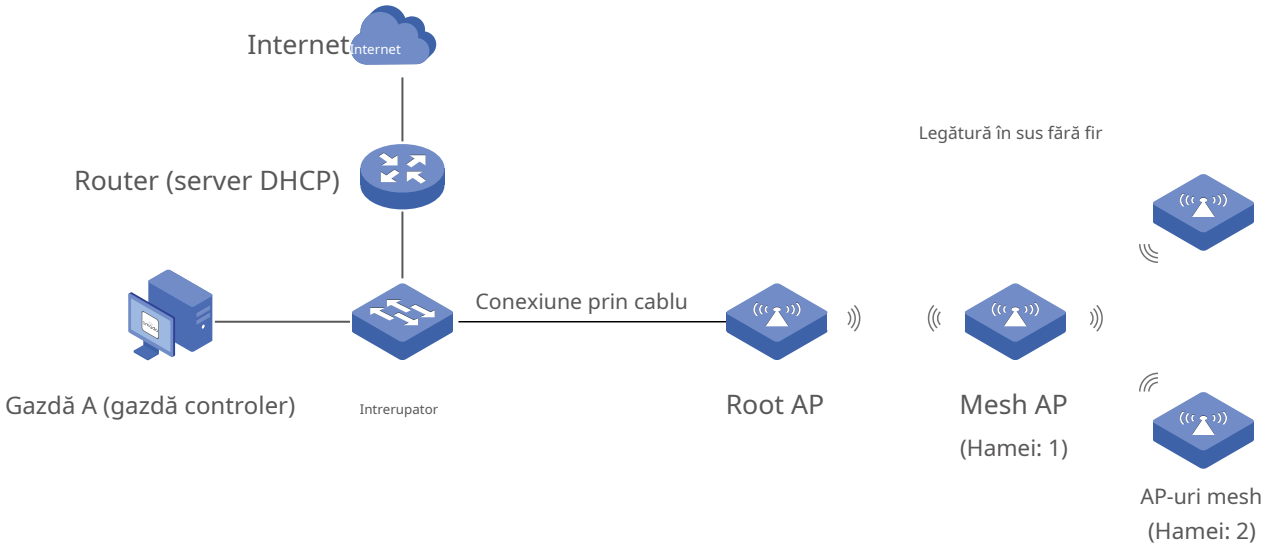
Mesh este utilizat pentru a stabili o rețea fără fir sau a extinde o rețea cu fir prin conexiune fără fir pe banda radio de 5 GHz. În aplicații practice, poate ajuta utilizatorii să implementeze în mod convenabil AP-uri fără a necesita cablu Ethernet. După ce rețeaua mesh se stabilește, EAP-urile pot fi configurate și gestionate în controlerul Omada în același mod ca EAP-urile cu fir. Între timp, datorită capacității de auto-organizare și autoconfigurare, mesh-ul poate reduce eficient configurația.

Rețineți că numai anumite modele EAP acceptă Mesh, iar EAP-urile ar trebui să fie în același site pentru a stabili o rețea Mesh.

Pentru a înțelege cum poate fi utilizată plasa, vor fi introduși următorii termeni folosiți în Omada Controller:

Root AP	AP-ul este gestionat de Omada Controller cu o conexiune de date prin cablu care poate fi configurată pentru a transmite date către și de la AP-uri mesh (AP downlink).
AP izolat	Când EAP-ul care a fost gestionat de Omada Controller înainte se conectează la rețea fără fir și nu poate ajunge la gateway, acesta intră în starea Izolat.
Mesh AP	Un AP izolat va deveni un AP mesh după stabilirea unei conexiuni wireless la AP cu acces la rețea.
Uplink AP/Downlink AP	Printre AP-urile mesh, AP-ul care oferă conexiunea fără fir pentru alte AP-uri se numește AP uplink. Un AP rădăcină sau un AP intermediar poate fi AP-ul uplink. Iar AP-ul care se conectează la AP-ul uplink se numește AP-ul downlink. Un AP uplink poate oferi conexiune wireless directă pentru cel mult 4 AP-uri downlink.
Legătură în sus fără fir	Acțiunea pe care un AP pe legătură în jos se conectează la AP pe legătură în sus.
Hamei	Într-o implementare care utilizează un AP rădăcină și mai mult de un nivel de uplink wireless cu AP-uri intermediare, nivelurile de uplink pot fi denumite prin rădăcină, primul hop, al doilea hop și așa mai departe. Hameiul nu trebuie să fie mai mare de 3.

O rețea mesh comună este prezentată mai jos. Doar AP-ul rădăcină este conectat printr-un cablu Ethernet, în timp ce alte AP-uri nu au conexiune de date prin cablu. Mesh permite AP-urilor izolate să comunice cu AP-ul rădăcină preconfigurat în rețea. Odată pornit, EAP-urile implicite din fabrică sau neadoptate pot detecta EAP-ul în raza de acțiune și pot fi disponibile pentru adoptare în controler.



După ce toate EAP-urile sunt adoptate, se stabilește o rețea mesh. EAP-urile conectate la rețea prin conexiune fără fir pot, de asemenea, să difuzeze SSID-uri și să transmită traficul de rețea către și dinspre rețea prin AP-ul uplink.

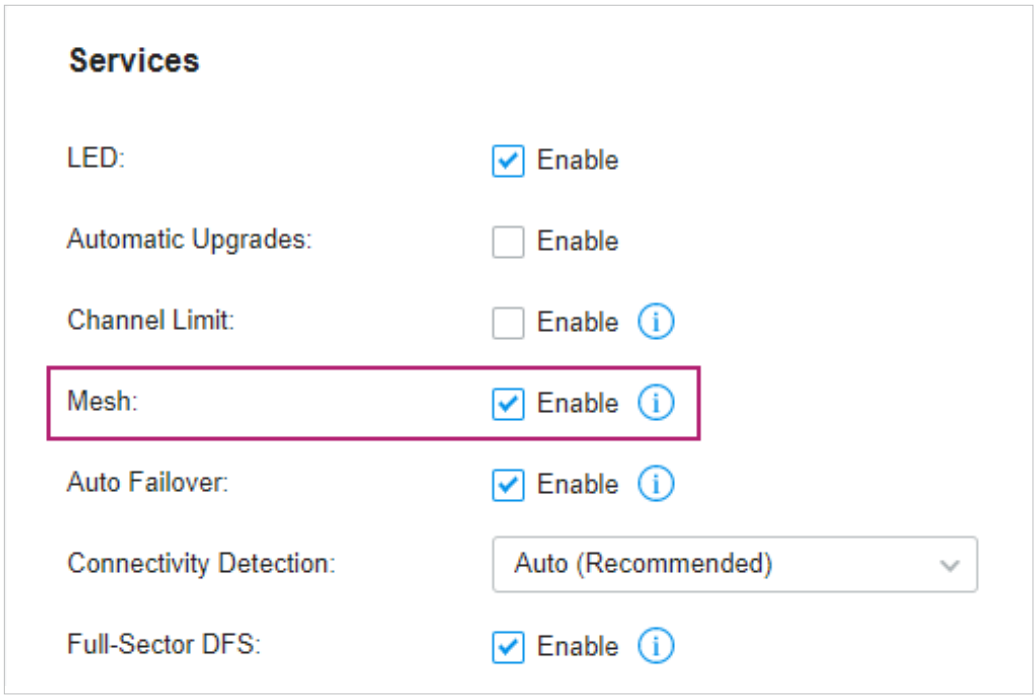
Pentru a construi o rețea mesh, urmați pașii de mai jos:

1)Activați funcția Mesh.

2)Adoptă AP-ul rădăcină.

3)Configurați legătura în sus fără fir adoptând AP-uri în starea În așteptare (Wireless) sau Izolat.

1. AccesațiSetări>Sitepentru a vă asigura că Mesh este activat.



2. AccesațiDispozitivepentru a vă asigura că Root AP a fost adoptat de controler. Starea AP-ului rădăcină este Conectat.

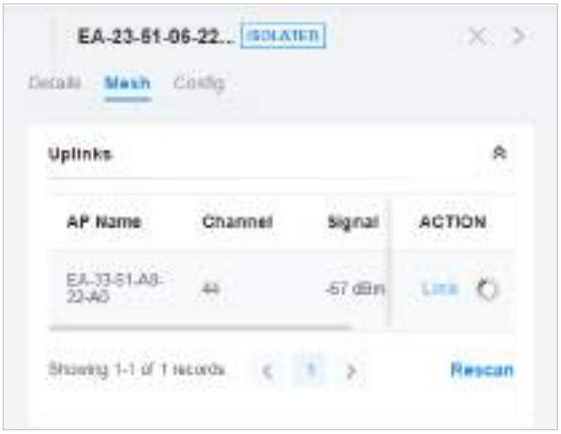
3. Instalați EAP-ul care va conecta wireless AP-ul rădăcină. Asigurați-vă că locația dorită se află în raza de acțiune a Root AP. EAP-urile care așteaptă Wireless Uplink includ două cazuri: EAP-uri implicite din fabrică și EAP-uri care au mai fost gestionate de controler. Mergi laDispozitivepentru a adopta un EAP în starea Pending (Wireless) sau pentru a conecta un AP izolat.

1) Pentru EAP implicit din fabrică, după pornirea dispozitivului, EAP va fi în starea În așteptare (Wireless) cu pictograma PENDING în controler. Faceți clic pentru a adopta EAP în Pending (Wireless) starea înDispozitivelistă.

După începerea adoptării, starea EAP în așteptare (Wireless) va deveni Adoptare (Wireless) și apoi Conectat (Wireless). Ar trebui să dureze aproximativ 2 minute pentru a afișa Conectat (Wireless) cu pictograma CONNECTED în controlerul tău.

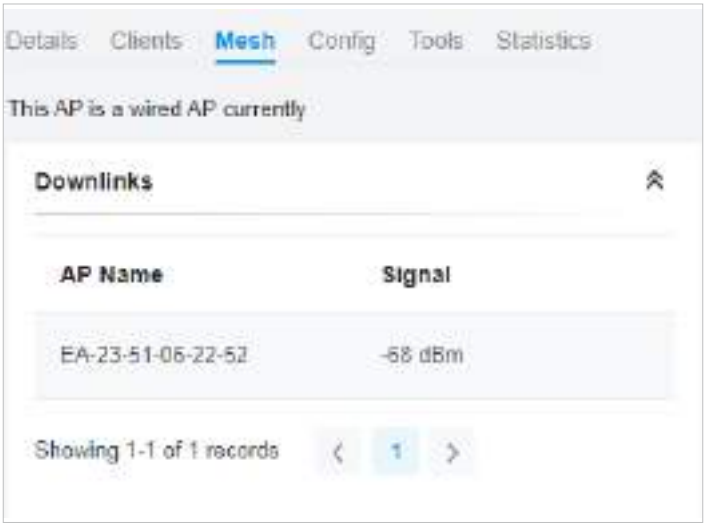
2) Pentru EAP-ul care a fost gestionat de Omada Controller înainte și nu poate ajunge la gateway, acesta intră în starea Izolat atunci când este descoperit din nou de către controler. Faceți clic pentru a conecta AP-ul Uplink înDispozitivelistă.

Următoarea pagină va fi afișată ca mai jos, faceți clicLegăturăpentru a conecta Uplink AP.

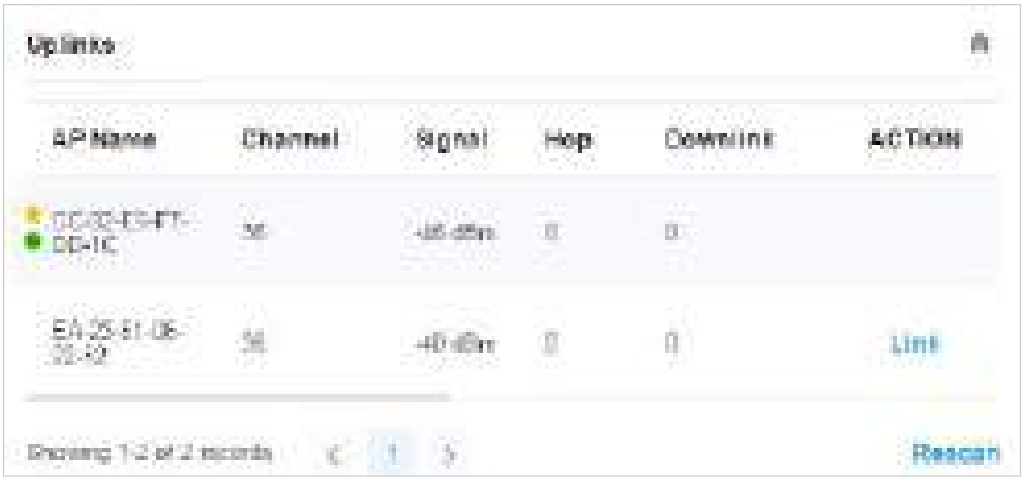


Odată ce rețeaua mesh a fost stabilită, EAP poate fi gestionat de controler în același mod ca un EAP cu fir. Puteți face clic pe numele EAP înDispozitivelistă și faceți clicPlasăpentru a vizualiza și configura parametrii de plasă ai EAP în fereastra Proprietăți.

ÎnPlasă, dacă AP-ul selectat este un AP cu legătură în sus, această pagină listează toate AP-urile pe legătura în jos conectate la AP.



Dacă AP-ul selectat este un AP pe legătură în jos, această pagină listează toate AP-urile pe legătura în sus disponibile și canalul lor, puterea semnalului, hop și numărul de AP-uri pe legătura în jos. Puteți da clicRescanațipentru a căuta AP-urile uplink disponibile și pentru a reîmprospăta lista și faceți clicLegăturăpentru a conecta AP-ul uplink și a construi o rețea mesh.



★	Pictograma apare înaintea AP-ului de uplink prioritar al AP-ului de downlink. Dacă doriți să setați un alt AP ca AP prioritar, faceți clicLegăturăîn coloana Acțiune.
●	Pictograma apare înaintea AP-ului de uplink curent al AP-ului de downlink.

Sfaturi:

- Puteți selecta manual AP-ul de uplink prioritar pe care doriți să îl conectați în lista de AP-uri de uplink. Pentru a construi o rețea mesh cu performanțe mai bune, vă recomandăm să selectați AP-ul de uplink cu cel mai puternic semnal, cel mai puțin hop și cel mai puțin downlink AP.
- Auto Failover este activat în mod implicit și permite controlerului să selecteze automat un AP pentru legătura în sus pentru AP-ul izolat pentru a stabili legătura în sus fără fir. Și controlerul va selecta automat un nou AP pentru legătura ascendentă pentru EAP-urile mesh atunci când legătura ascendentă originală eșuează. Pentru mai multe detalii despre configurațiile globale Mesh, consultați caracteristica Mesh în3. 2. 2 Servicii.

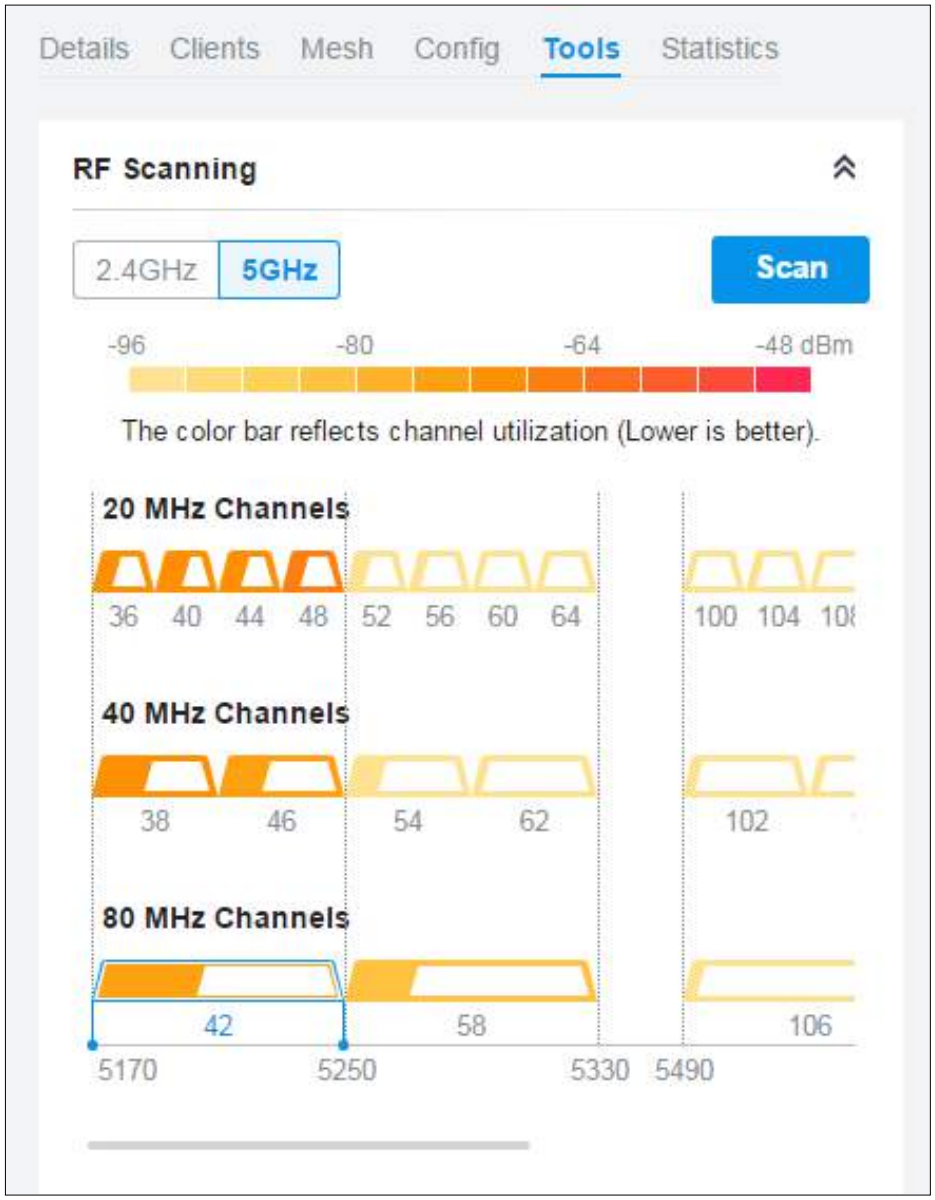
Instrumente

În Instrumente, puteți activa Scanarea RF pentru a scana mediile RF (frecvență radio) din jurul AP, ceea ce este util pentru analiza spectrală în selectarea și planificarea canalelor.

Notă:

- Scanarea RF poate dura câteva minute. În timpul scanării, toți clienții care folosesc acest AP vor fi deconectați, iar AP-ul va fi offline. Ar trebui să selectați un timp liber de rețea pentru a începe scanarea.
- AP-urile din rețeaua mesh nu acceptă scanarea RF.

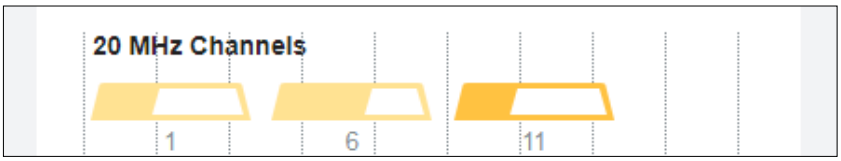
Selectați fiecare bandă de frecvență pentru a vizualiza și analiza rezultatele scanării.



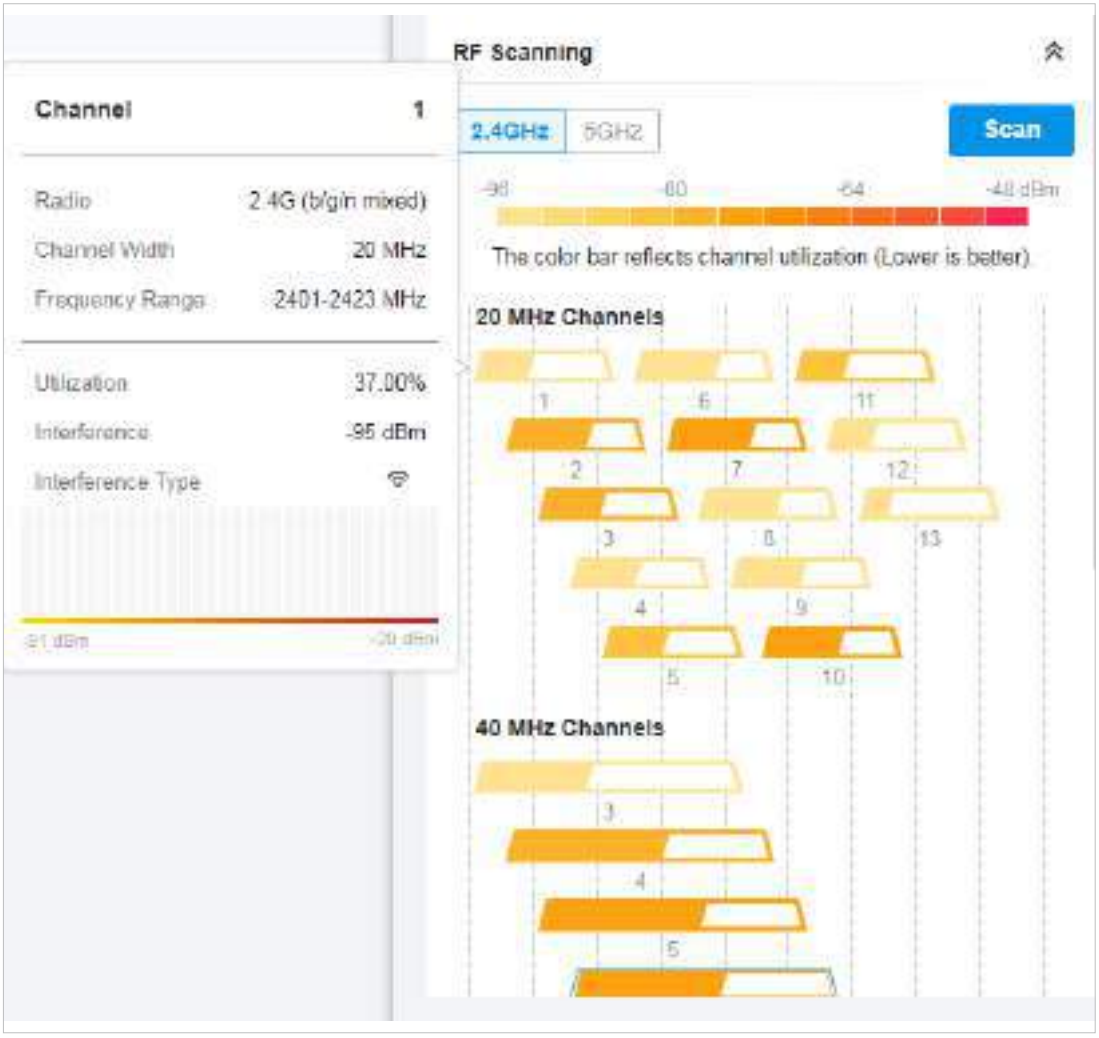
Fiecare grafic cu bare colorat afișează informații despre utilizarea canalului și interferența pe un canal. Zona de umplere a barei reprezintă utilizarea canalului. Iar suprafața de umplere mai mare înseamnă o utilizare mai mare, ceea ce indică că canalul este mai ocupat în transmiterea datelor. Nuanța de culoare reprezintă nivelul de interferență. Și legenda este afișată în partea de sus.

Rezultatele de 2,4 GHz sunt afișate în lățimi de canal de 20 și 40 MHz. Rezultatele de 5 GHz sunt afișate în lățimi de canal de 20, 40 și 80 MHz.

Numărul de sub graficul cu bare afișează numărul de canal corespunzător pentru fiecare opțiune de lățime a canalului. De exemplu, canalele 42, 58 și 106 sunt trei dintre canalele de 80 MHz. Și conturul canalului în albastru este în uz în prezent.



Puteți trece cursorul peste o opțiune de canal pentru mai multe detalii.

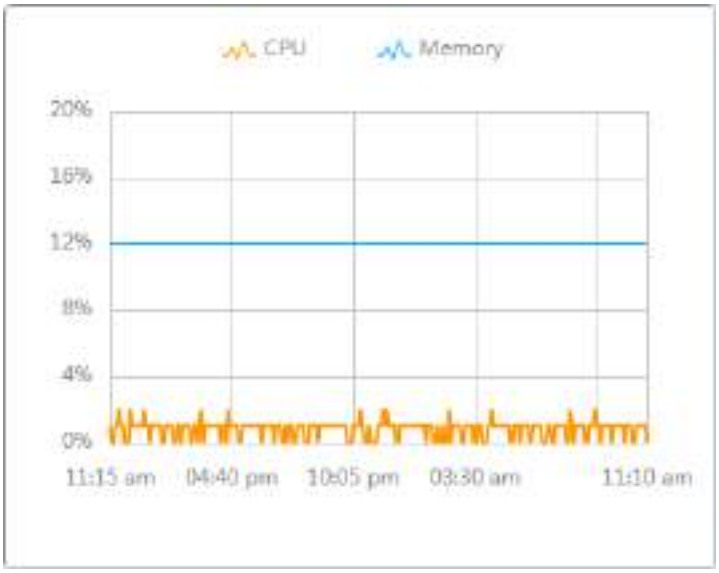


Radio	Afișează radioul pe care îl folosește AP.
latimea canalului	Afișează lățimea canalului.
Canale folosite	Afișează canalele în uz.
Gama de frecvente	Afișează gama de frecvențe.

Utilizare	Afișează procentul din intervalul de frecvență deja utilizat.
Interferență	Afișează nivelul de interferență.
Tip de interferență	Afișează tipul de interfață, inclusiv MWO (cuptor cu microunde), CW (undă continuă), WLAN (semnale Wi-Fi) și FHSS (spectru răspândit cu salt de frecvență).

Statistici

În Statistică, puteți monitoriza utilizarea dispozitivului în ultimele 24 de ore prin diagrame, inclusiv monitorizarea procesorului/memoriei, utilizarea canalului, pachetele abandonate și pachetele reîncercate. Pentru a vizualiza statisticile dispozitivului într-o anumită perioadă, faceți clic pe diagramă la care sări7. 2 Vizualizați Statisticile rețelei .



6

Monitorizați și gestionați clienții

Acest capitol vă ghidează despre cum să monitorizați și să gestionați clienții prin pagina Clienți folosind tabelul clienți și fereastra de proprietăți și sistemul Hotspot Manager. Pentru a vedea clienții care s-au conectat la rețea în trecut, consultațiVizualizați statisticile în perioada specificată cu Insight . Acest capitol include următoarele secțiuni:

6. 1 Gestionați clienții cu fir și fără fir în Pagina Clienți

6. 1. 1 Pagina de introducere a clienților

Pagina Clienți oferă o modalitate simplă de a gestiona și monitoriza clienții. Afișează toți clienții cu fir și fără fir conectați în site-ul ales și informațiile generale ale acestora. De asemenea, puteți deschide fereastra Proprietăți pentru informații și configurații detaliate.

PENDING	Clientul nu a trecut de autentificarea portalului și nu este conectat la internet.
AUTHORIZED	Clientul a fost autorizat și este conectat la internet.
CONNECTED	Clientul este conectat la internet printr-o rețea non-portală.
AUTHENTICATION-FREE	Clientul nu trebuie autorizat și este conectat la internet.

6. 1. 2 Utilizarea tabelului Clienți pentru a monitoriza și gestiona clienții

Pentru a monitoriza și gestiona rapid clienții, puteți personaliza coloanele și filtra clienții pentru o imagine de ansamblu mai bună a informațiilor lor. De asemenea, sunt disponibile operațiuni rapide și configurarea loturilor.

■ Personalizați coloanele de informații

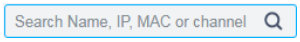
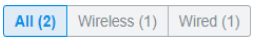
Faceți clic lângă coloana Acțiune și aveți trei opțiuni: Coloane implicite, Toate coloanele și Personalizați coloanele. Pentru a personaliza informațiile afișate în tabel, faceți clic pe casetele de selectare ale tipului de informații.

Pentru a schimba ordinea listei, faceți clic pe capul coloanei și pe pictograma în apare pentru ca dvs. să alegeți ordine ascendentă sau descendentă.

Când această icoană apare în coloana Conexiune fără fir, indică că clientul este în modul de salvare.

Filtrați clienții

Pentru a căuta anumiți clienți, utilizați caseta de căutare de deasupra tabelului. Pentru a filtra clienții după tipul lor de conexiune, utilizați barele de file de deasupra tabelului. Pentru clienții fără fir, îi puteți filtra în continuare după banda de frecvență și tipul de rețea wireless conectată.

	Filtrați clienții folosind caseta de căutare în funcție de numele de utilizator, adresa IP, adresa MAC sau canal.
	Filtrați clienții în funcție de tipul lor de conexiune.
	(Pentru clienții fără fir) Filtrați clienții fără fir în funcție de banda de frecvență pe care o folosesc.
	(Pentru clienții fără fir) Filtrați clienții fără fir în funcție de tipul de rețea wireless conectată. Oaspeții sunt clienți conectați la rețeaua de oaspeți, pe care o puteți seta în timpulInstalare rapida,crearea de rețele fără fir, etc.

Operații rapide

Pentru operațiuni rapide pe un singur client, faceți clic pe pictogramele din coloana Acțiune. Pictogramele disponibile variază în funcție de starea clientului și tipul de conexiune.

	Faceți clic pentru a bloca clientul în site-ul ales. Puteți vizualiza clienții blocați în7. 5. 1 Clienți cunoscuți.
	(Cu autentificarea portalului activată) Faceți clic pentru a autoriza manual clientul care nu a trecut autentificarea portalului.
	(Cu autentificarea portalului activată) Faceți clic pentru a neautoriza clientul care a trecut autentificarea portalului.
	(Pentru clienți fără fir) Faceți clic pentru a reconecta clientul fără fir la rețeaua fără fir.

Selectare multiplă pentru configurarea lotului

Pentru a selecta mai mulți clienți și a-i adăuga la fereastra Proprietăți, faceți clic în dreapta sus și apoi bifați casetele. Când ați terminat de ales clienții, faceți clicEditați selectatiar clientul (clienții) aleși vor fi adăugați la fereastra Proprietăți pentru configurarea clientului în lot.

6. 1. 3 Utilizarea ferestrei de proprietăți pentru a monitoriza și gestiona clienții

În fereastra Proprietăți, puteți vizualiza informații mai detaliate despre clienții conectați și le puteți gestiona. Pentru a deschide fereastra Proprietăți, faceți clic pe intrarea unui singur client sau faceți clic pe pictograma pentru a selecta mai mulți clienți pentru configurarea lotului. Utilizați următoarele pictograme pentru fereastra Proprietăți.

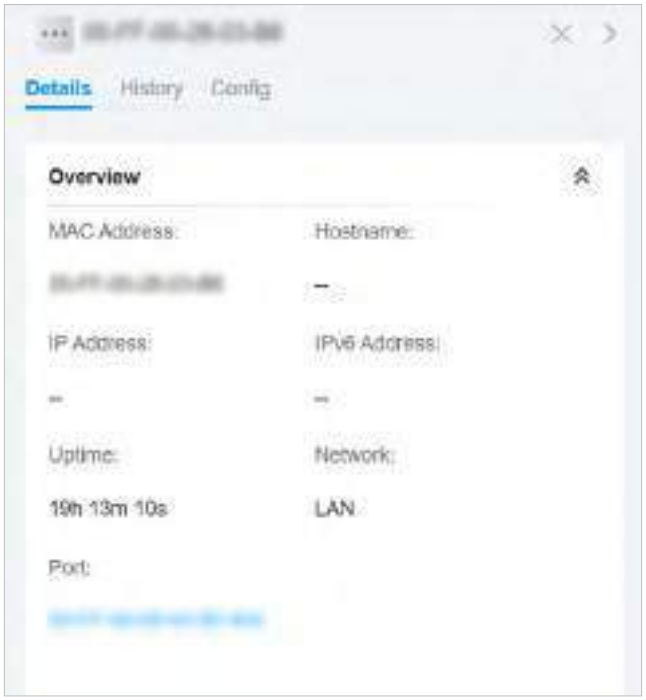
	Faceți clic pentru a selecta mai mulți clienți și adăugați-i în fereastra Proprietăți pentru monitorizarea și gestionarea loturilor.
	Faceți clic pentru a minimiza fereastra Proprietăți la o pictogramă. Pentru a redeschide fereastra de Proprietăți minimizată, faceți clic pe .
	Faceți clic pentru a maximiza fereastra Proprietăți. Puteți folosi pictograma și în alte pagini decât pagina Clienți.
	Faceți clic pentru a închide fereastra Proprietăți a clientului(ilor) aleși(i). Rețineți că configurația nesalvată pentru client(i) se va pierde.
	Numărul din dreapta jos arată numărul de clienți din configurația client lot.

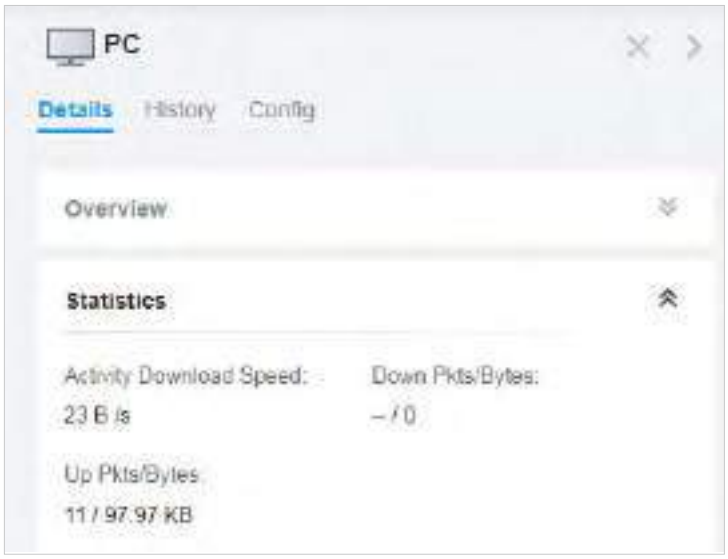
Monitorizați și gestionați un singur client

- Monitorizați un singur client

  După deschiderea ferestrei Proprietăți a unui singur client, puteți vizualiza informațiile de bază, statisticile de trafic și istoricul conexiunilor în filele Detalii și Istoric.

  Sub fila Detalii, Prezentare generală și Statistici afișează informațiile de bază și, respectiv, statisticile de trafic ale clientului. Informațiile listate variază în funcție de starea clientului și tipul de conexiune.





Sub fila Istoric, puteți vizualiza istoricul conexiunilor clientului.

■ Gestionați un singur client

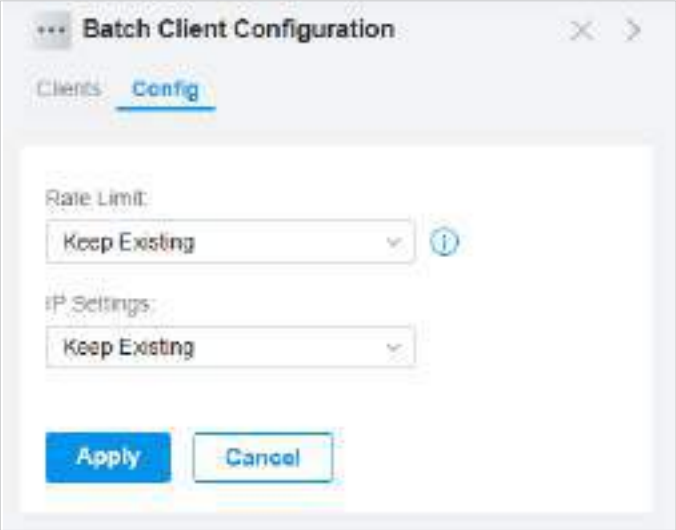
În Config, puteți configura următorii parametri:

Nume	Specificați numele clientului pentru a identifica mai bine diferiți clienți, iar numele clientului este afișat în tabelul de pe pagina Clienți.

Limită de rată	Selectați un profil de limită de tarif existent, creați un nou profil de limită de tarif sau personalizați limita de tarif pentru client. Personalizat: specificați limita ratei de descărcare/încărcare în funcție de nevoi. Notă: Rate Limit de pe această pagină este disponibilă numai pentru clienții conectați la EAP-uri. Pentru a limita rata clienților conectați la gateway sau la comutator, accesați pagina Bandwidth Control.
Limită de descărcare/încărcare	Faceți clic pe caseta de selectare și specificați limita ratei de descărcare/încărcare pentru clienții wireless utilizând codurile voucherului. Valoarea ratei de descărcare și încărcare poate fi setată în Kbps sau Mbps.
Utilizați o adresă IP fixă	Faceți clic pe caseta de selectare pentru a configura o adresă IP fixă pentru client. Cu această funcție activată, selectați o rețea și specificați o adresă IP pentru client. Pentru a vizualiza și configura rețelele, consultați3. 3 Configurați rețelele cu fir.
Blocare la AP	Activați funcția și selectați unul sau mai multe AP-uri, apoi clientul va fi blocat la AP-urile selectate. Această caracteristică ajută la prevenirea unui client static să se deplaseze frecvent între mai multe AP-uri.

Monitorizați și gestionați mai mulți clienți

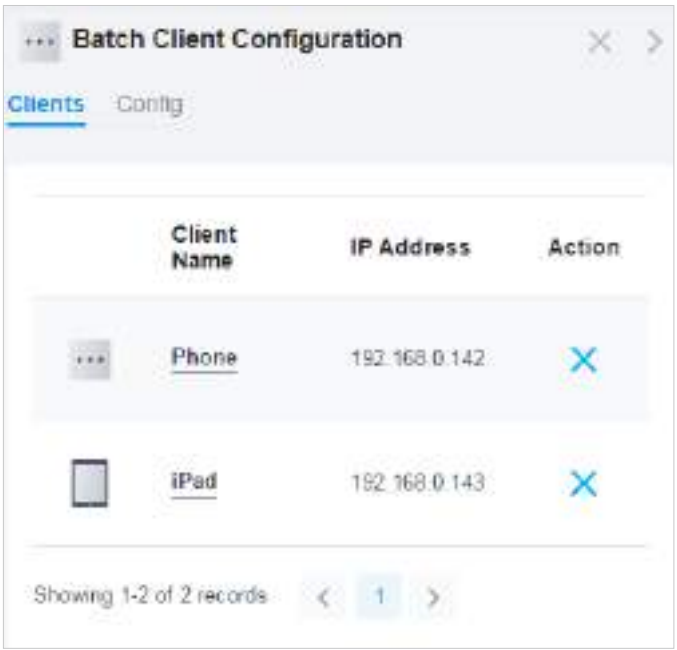
Pentru a gestiona mai mulți clienți în același timp, faceți clic pe , selectați mai mulți clienți și faceți clicEditați selectat. Apoi puteți configura următorii parametri în fila Config.



Limită de rată	Selectați un profil de limită de tarif existent, creați un nou profil de limită de tarif sau personalizați limita de tarif pentru clienți. Păstrarea existenței: Limita de tarife a clienților aleși va rămâne setările lor curente. Personalizat: specificați limita ratei de descărcare/încărcare în funcție de nevoi. Dezactivat:Limita de tarife a clienților aleși va fi dezactivată. Notă: Rate Limit de pe această pagină este disponibilă numai pentru clienții conectați la EAP-uri. Pentru a limita rata clienților conectați la gateway sau la comutator, accesați pagina Bandwidth Control.

Limită de descărcare/încărcare	Faceți clic pe caseta de selectare și specificați limita ratei de descărcare/încărcare pentru clienții wireless utilizând codurile voucherului. Valoarea ratei de descărcare și încărcare poate fi setată în Kbps sau Mbps.
Setări IP	Păstrarea existenței: Setările IP ale clienților aleși rămân setările lor curente. Utilizați DHCP: Adresele IP ale clienților sunt atribuite automat de serverul DHCP, cum ar fi gateway-ul sau comutatorul. Utilizați adresa IP fixă:Selectați o rețea și atribuiți manual adrese IP fixe clienților aleși. Pentru a vizualiza și configura rețelele, consultați3. 3 Configurați rețelele cu fir.
Blocare la AP	Blocarea la AP ajută la prevenirea clienților statici să roaming frecvent între mai multe AP. Păstrarea existenței:Păstrați setările curente ale clienților aleși. Dezactivat:Dezactivați Blocarea la AP a clienților aleși. Permite:Activați Blocarea la AP și selectați unul sau mai multe AP-uri, apoi clienții aleși vor fi blocați la AP-urile selectate.

Puteți vedea numele și adresele IP ale acestora în fila Clienți și puteți elimina clienții din Configurarea clientului în lot făcând clic în coloana Acțiune.



6. 2 Gestionați autentificarea clientului în Hotspot Manager

Hotspot Manager este un sistem de management al portalului pentru monitorizarea și gestionarea centrală a clienților autorizați prin autentificarea portalului. Următoarele patru file sunt prevăzute în sistem pentru o gestionare ușoară și directă.

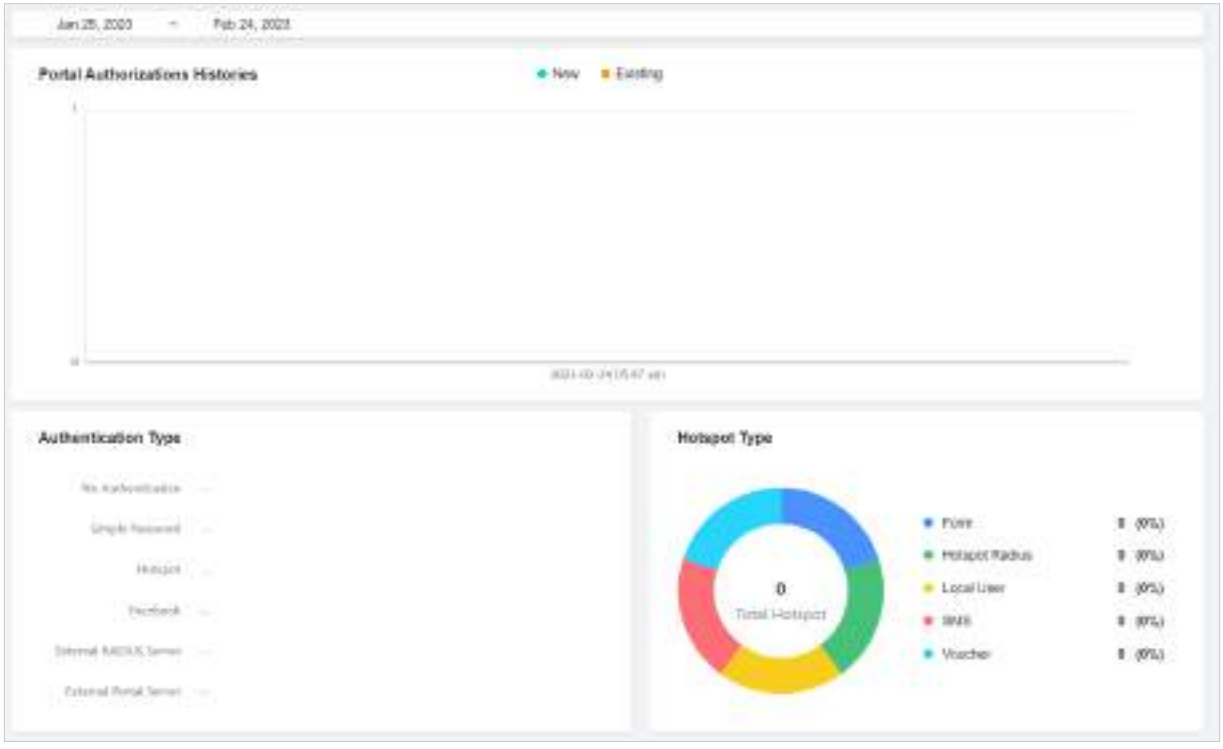
Bord	Monitorizați autorizațiile portalului dintr-o privire prin diferite vizualizări.
Clienți autorizați	Vizualizați înregistrările clienților portalului conectați și expirați.
Bonuri	Creați vouchere pentru autentificarea portalului și vizualizați și gestionați informațiile aferente.
Utilizatori locali	Creați conturi de utilizator locale pentru autentificarea portalului, vizualizați informațiile acestora și gestionați-le.
Date de autentificare formular	Personalizați conținutul sondajului și publicați-l pentru a colecta date.
Operatori	Creați conturi de operator pentru gestionarea Hotspot-ului, vizualizați informațiile acestora și gestionați-le.

Pentru a accesa sistemul, faceți clicManager hotspotdin lista derulantă aOrganizare. Pentru a vă deconecta din sistem, faceți clic pe pictograma contului din colțul din dreapta sus, apoi faceți clicDeconectați-vă.

6. 2. 1 Tabloul de bord

În tabloul de bord, puteți monitoriza autorizațiile portalului dintr-o privire prin diferite vizualizări.

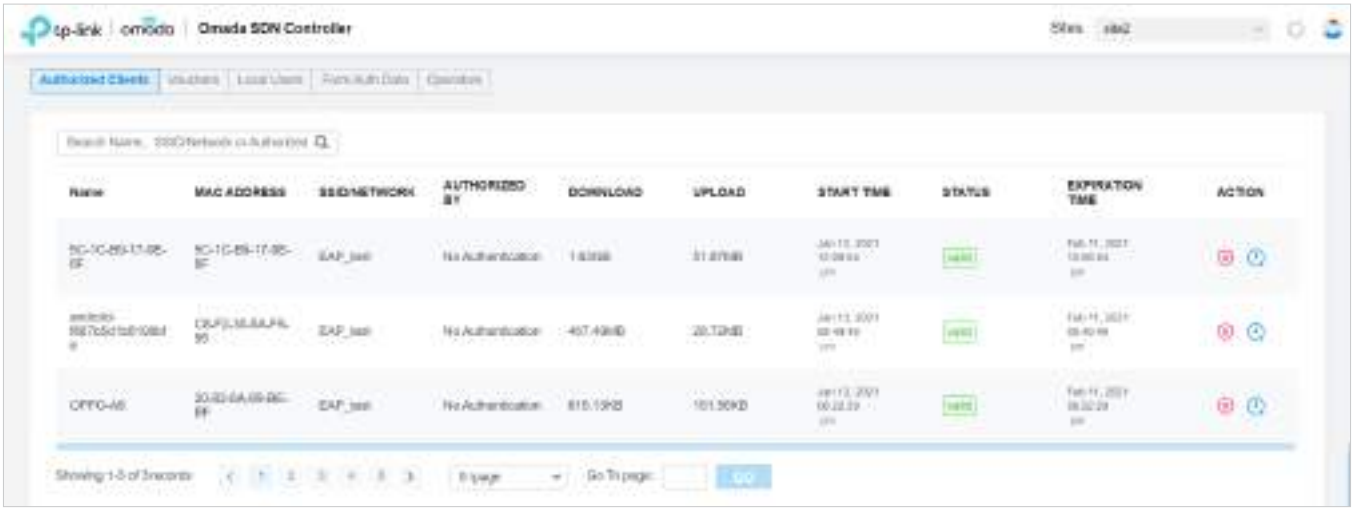
Pentru a deschide tabloul de bord, faceți clicManager hotspotdin lista derulantă aOrganizareși faceți clic Bordîn pagina pop-up. Specificați perioada de timp pentru a vizualiza istoricul de autorizare a portalului.



6. 2. 2 Clienți autorizați

Fila Clienți autorizați este utilizată pentru a vizualiza și gestiona clienții autorizați de sistemul portal, inclusiv clienții expirați și clienții în perioada valabilă.

Pentru a deschide lista de Clienți Autorizați, faceți clic peManager hotspotdin lista derulantă aOrganizare și faceți clicClienți autorizațiîn pagina pop-up. Puteți căuta anumiți clienți utilizând caseta de căutare, puteți vizualiza informațiile detaliate ale acestora în tabel și îi puteți gestiona folosind coloana de acțiuni.



	Faceți clic pentru a prelungi perioada de valabilitate a clientului autorizat. Puteți alege durata de timp prestabilită sau puteți seta o perioadă personalizată în funcție de nevoi.
	Faceți clic pentru a deconecta clienții autorizați. Dacă deconectați un client autorizat, clientul trebuie să fie re-autentificat pentru următoarea conexiune.
	Faceți clic pentru a șterge clientul expirat din listă.

6. 2. 3 Vouchere

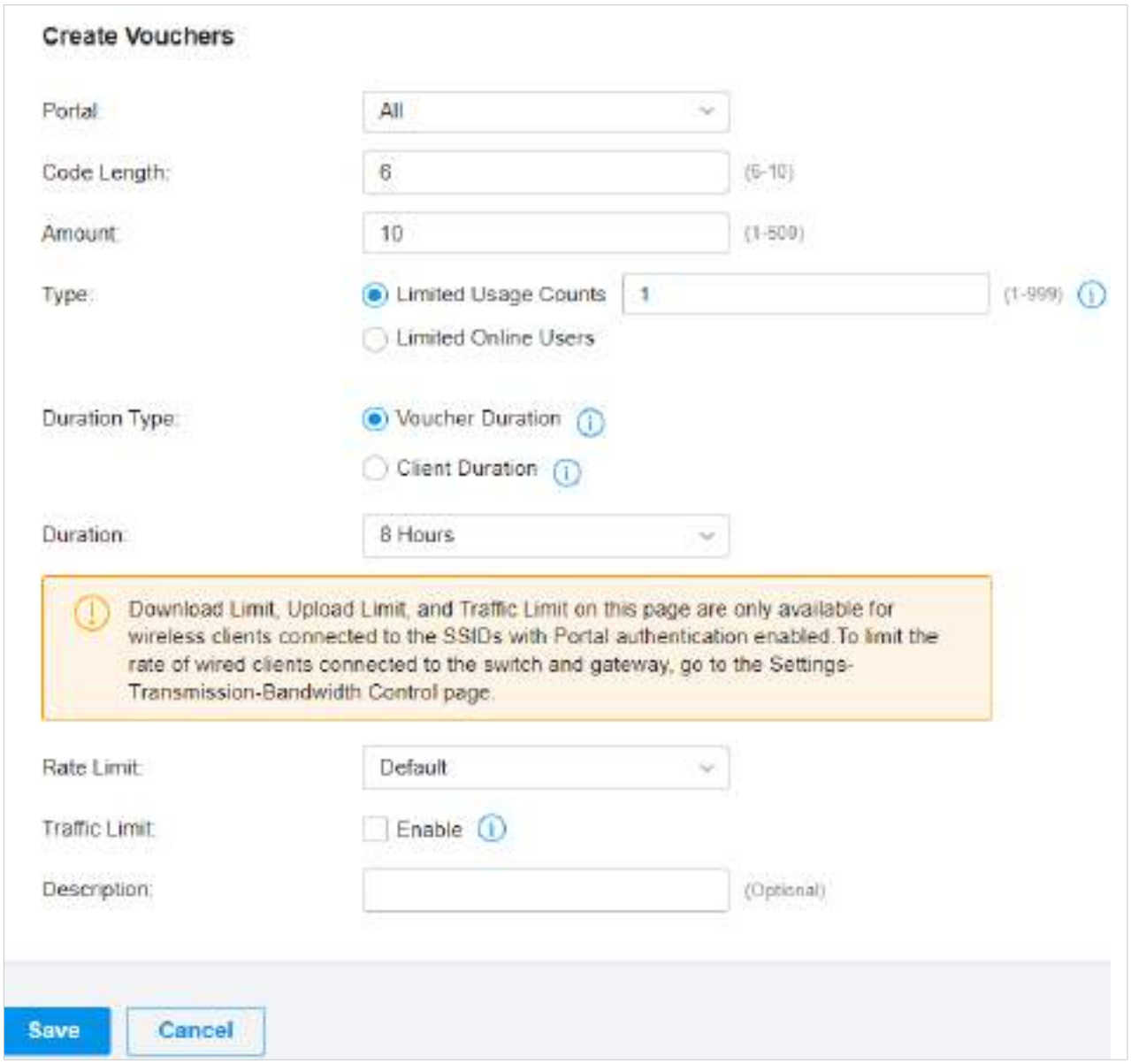
Fila Vouchere este folosită pentru a crea vouchere și pentru a gestiona codurile voucher neutilizate. Cu voucherul configurat și codurile create, puteți distribui codurile voucher generate de controlor către clienți pentru ca aceștia să acceseze rețeaua prin autentificarea portalului. Pentru configurații detaliate, consultați3. 9. 1 Portal .

Creați vouchere

Urmați pașii de mai jos pentru a crea vouchere pentru autentificare:

1. Faceți clicManager hotspotdin lista derulantă aSite-uriși faceți clicBonuriîn pagina pop-up.

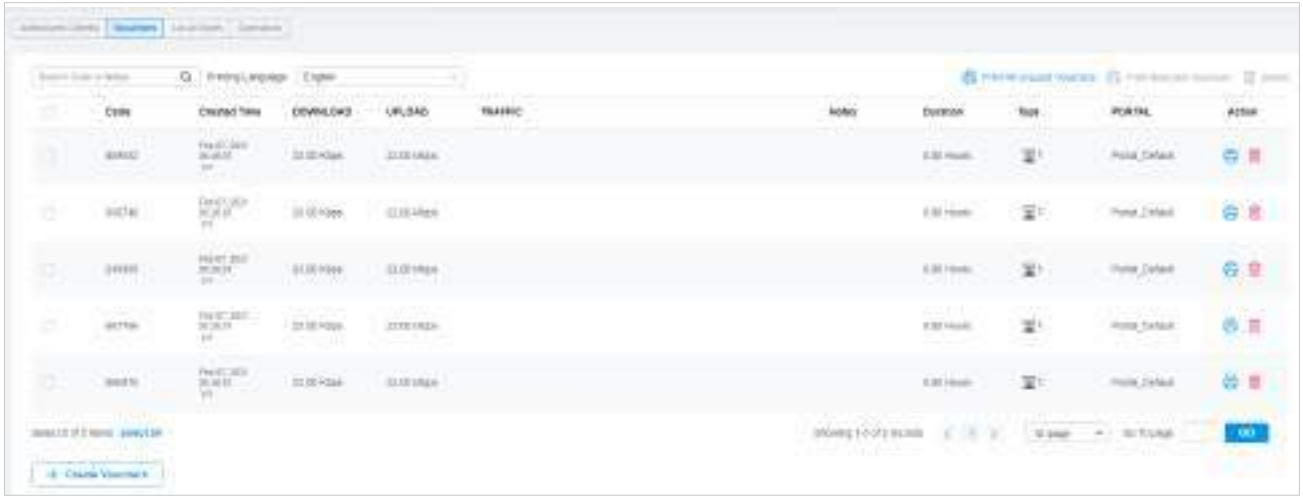
2. Faceți clic+ Creați voucheredin stânga jos și apare următoarea fereastră. Configurați următorii parametri și faceți clicSalvați.



Portal	Selectați portalul pentru care vor intra în vigoare voucherele.
Lungimea codului	Specificați lungimea codurilor de la 6 la 10 cifre.
Cantitate	Specificați numărul de coduri voucher pe care doriți să le creați.
Tip	Selectați un tip pentru a limita numărul de utilizare sau numărul de utilizatori autorizați ai unui cod voucher. Număr limitat de utilizare: Codul voucher poate fi folosit doar pentru un număr limitat de ori în perioada de valabilitate. Utilizatori online limitati: Codul voucher poate fi folosit de un număr nelimitat de ori în perioada sa de valabilitate, dar doar un număr limitat de clienți wireless pot accesa rețeaua cu acest cod voucher în același timp.

Tip de durată	Specificați dacă limitați durata voucherului sau durata clientului.
Durată	Selectați perioada valabilă pentru codul (codul) voucherului.
Limită de rată	Selectați un profil de limită de tarif existent, creați un nou profil de limită de tarif sau personalizați limita de tarif pentru codurile voucher. Personalizat: specificați limita ratei de descărcare/încărcare în funcție de nevoi.
Limită de descărcare/încărcare	Faceți clic pe caseta de selectare și specificați limita ratei de descărcare/încărcare pentru clienții wireless utilizând codurile voucherului. Valoarea ratei de descărcare și încărcare poate fi setată în Kbps sau Mbps. Notă: Limita de descărcare/încărcare de pe această pagină este disponibilă numai pentru clienții wireless conectați la SSID-urile cu autentificarea portalului activată. Pentru a limita rata de cablu clienții conectați la switch și gateway, accesațiSetări>Transmitere>Controlul lățimii de bandă.
Limita de trafic	Faceți clic pe caseta de selectare și specificați limita de trafic zilnic/săptămânal/lunar/total pentru voucher, iar valoarea limitei de trafic poate fi setată în MB sau GB. Odată atins limita, clientul (clienții) nu mai poate accesa rețeaua folosind voucherul. Notă: Limita de trafic de pe această pagină este disponibilă numai pentru clienții wireless conectați la SSID-urile cu autentificarea portalului activată. Pentru a limita rata de clienți conectați prin cablu la comutator și gateway, mergeți laSetări>Transmitere>Controlul lățimii de bandă.
Descriere (optional)	Introduceți notele pentru codurile de voucher create, iar descrierea introdusă este afișată în lista de voucher sub fila voucher.

3. Codurile voucher sunt generate și afișate în tabel.



2	Codul voucher poate fi folosit de un număr nelimitat de ori în perioada sa de valabilitate, dar doar un număr limitat de clienți wireless pot accesa internetul cu acest cod voucher în același timp. Numărul din dreapta arată numărul limitat de utilizatori.
2	Codul voucher poate fi folosit doar pentru un număr limitat de ori în perioada de valabilitate a acestuia. Numărul din dreapta arată numărul limitat de ori de autentificare.

4. Imprimați voucherele. Clic pentru a imprima un singur voucher sau faceți clic pe casetele de selectare ale bonurilor și faceți clic Imprimați voucherele selectatepentru a imprima voucherele selectate. Și poți face clic Tipăriți toate neutilizate Bonuripentru a tipări toate bonurile neutilizate.

307690 Valid for 8h Limited Usage Counts One	**084520** Valid for 8h Limited Usage Counts One
924665 Valid for 8h Limited Usage Counts One	**232608** Valid for 8h Limited Usage Counts One
701945 Valid for 8h Limited Usage Counts One	**473875** Valid for 8h Limited Usage Counts One
141716 Valid for 8h Limited Usage Counts One	**999934** Valid for 8h Limited Usage Counts One
825813 Valid for 8h Limited Usage Counts One	**180815** Valid for 8h Limited Usage Counts One

5. Distribuiți voucherele clienților, iar apoi aceștia pot folosi codurile pentru a trece autentificarea. Dacă un cod voucher expiră, acesta va fi eliminat automat din listă.

6. Pentru a șterge manual anumite bonuri, faceți clic pentru a șterge un singur voucher sau Ștergepentru a șterge mai multe coduri voucher în același timp.

6. 2. 4 Utilizatori locali

Fila Utilizatori locali este folosită pentru a crea conturi de utilizator pentru autentificare. Cu utilizatorul local configurat, clienților li se cere să introducă numele de utilizator și parola pentru a trece autentificarea. Puteți crea mai multe conturi și le puteți atribui diferiților utilizatori. Pentru configurații detaliate, consultați3. 9. 1 Portal .

Creați utilizatori locali

Există două moduri de a crea conturi de utilizator locale: creați conturi pe pagină și importați dintr-un fișier.

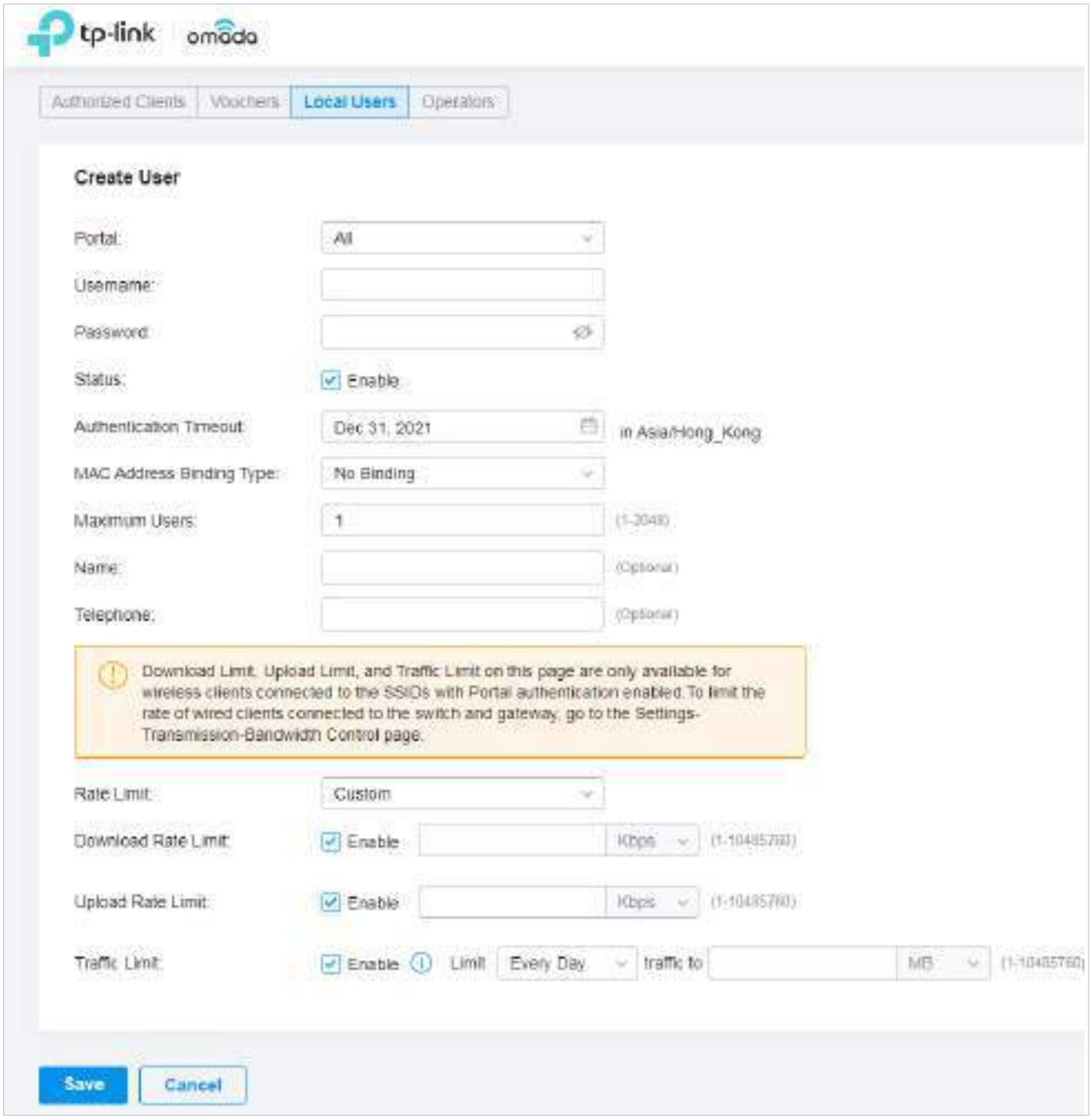
Pentru a crea conturi de utilizator locale, urmați pașii de mai jos.

1. Faceți clicManager hotspotdin lista derulantă aOrganizareși faceți clicUtilizatori localiîn pagina pop-up.

2. Creați conturi de utilizator local prin două moduri diferite.

■ Creați conturi de utilizator local

Clic+Creați utilizatordin stânga jos și apare următoarea fereastră. Configurați următorii parametri și faceți clicSalvați.

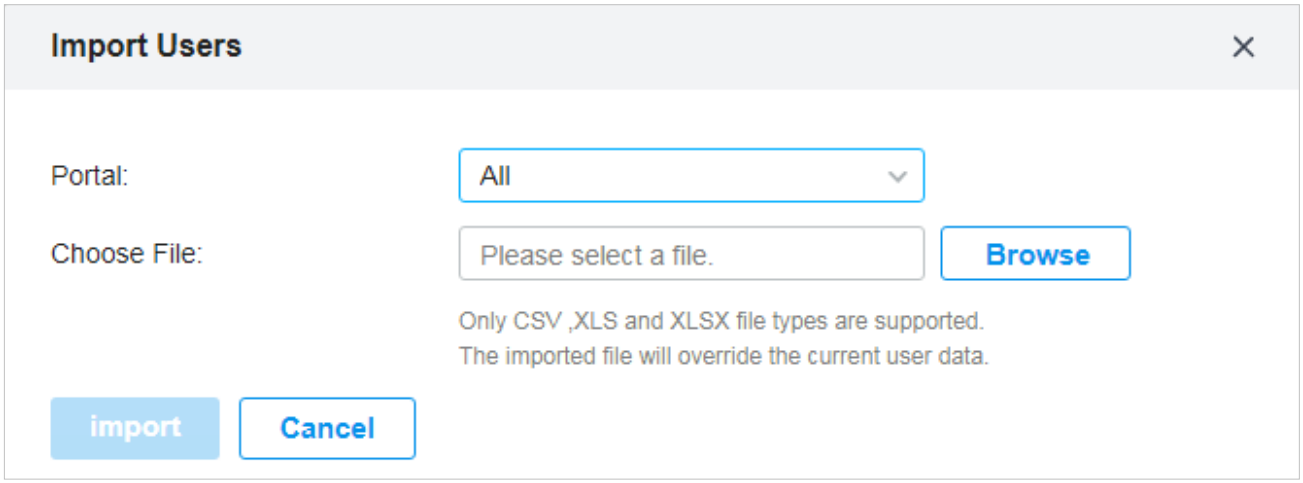


Portal	Selectați portalul pentru care utilizatorii locali vor intra în vigoare.
Nume de utilizator	Specificați numele de utilizator. Numele de utilizator ar trebui să fie diferit de cel existent și nu poate fi editat odată ce este creat.

Parola	Specificați parola. Utilizatorii locali trebuie să introducă numele de utilizator și parola pentru a trece autentificarea și a accesa rețeaua.
stare	Când starea este activată, înseamnă că contul de utilizator este valid. Puteți dezactiva contul de utilizator și îl puteți activa mai târziu, atunci când este necesar.
Timeout autentificare	Specificați timpul de expirare a autentificării pentru utilizatorii locali. După expirarea timpului, utilizatorii trebuie să se conecteze din nou pe pagina de autentificare pentru a accesa rețeaua.
Legarea adresei MAC Tip	Există trei tipuri de legare MAC: No Binding, Static Binding și Dynamic Binding. Fără legare:Nicio adresă MAC nu este legată de contul de utilizator local. Legare statică: legați manual o adresă MAC la acest cont de utilizator. Apoi, numai utilizatorul cu această adresă MAC poate folosi numele de utilizator și parola pentru a trece autentificarea. Legare dinamică: Adresa MAC a primului utilizator care trece autentificarea va fi legată de acest cont. Atunci numai acest utilizator poate folosi numele de utilizator și parola pentru a trece autentificarea.
Numărul maxim de utilizatori	Specificați numărul maxim de utilizatori care pot folosi acest cont pentru a trece autentificarea.
Nume (opțional)	Specificați un nume pentru identificare.
Telefon (optional)	Specificați un număr de telefon pentru identificare.
Limită de rată	Selectați un profil de limită de tarif existent, creați un nou profil de limită de tarif sau personalizați limita de tarif pentru utilizatorii locali. Personalizat: specificați limita ratei de descărcare/încărcare în funcție de nevoi.
Limită de descărcare/încărcare	Faceți clic pe caseta de selectare și specificați limita ratei de descărcare/încărcare pentru utilizatorii contului de utilizator local. Valoarea ratei de descărcare/încărcare poate fi setată în Kbps sau Mbps. Notă: Limita de descărcare/încărcare de pe această pagină este disponibilă numai pentru clienții wireless conectați la SSID-urile cu autentificarea portalului activată. Pentru a limita rata clienților cu fir conectați la comutator și la gateway, accesațiSetări>Transmitere>Controlul lățimii de bandă.
Limita de trafic	Faceți clic pe caseta de selectare și specificați limita de trafic zilnic/săptămânal/lunar/total pentru contul de utilizator local, iar valoarea limitei de trafic poate fi setată în MB sau GB. Odată ce limita este atinsă, utilizatorii nu mai pot accesa rețeaua folosind acest cont. Notă: Limita de trafic de pe această pagină este disponibilă numai pentru clienții wireless conectați la SSID-urile cu autentificarea portalului activată. Pentru a limita rata clienților cu fir conectați la comutator și la gateway, accesațiSetări>Transmitere>Controlul lățimii de bandă.

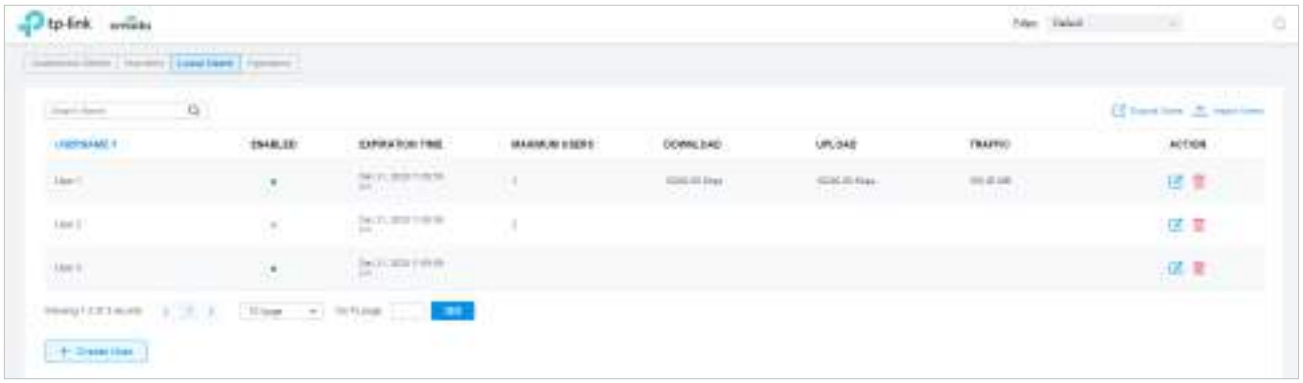
- Creați conturi de utilizator local din fișiere.

  Clic Import Users în dreapta sus și apare următoarea fereastră. Selectați un fișier în format de CVS sau Excel și faceți clicImport. Pentru a vedea parametrii necesari și explicația corespunzătoare, consultați Creați conturi de utilizator local . Rețineți că fișierul importat va suprascrie datele curente ale utilizatorului.



Portal	Selectați portalul în care vor fi importați utilizatorii locali.

3. Conturile de utilizator local vor fi create și afișate în modul. Puteți vizualiza informațiile utilizatorilor locali creați, puteți căuta anumite conturi prin nume și puteți utiliza pictograme pentru administrare.



Import Users	Faceți clic pentru a adăuga utilizatori locali din fișiere în format CVS sau Excel. Este recomandat atunci când trebuie să creați utilizatori locali în loturi. Selectați portalurile în funcție de nevoi, iar utilizatorii locali vor fi importați în portalul ales. Rețineți că fișierul importat va suprascrie datele curente ale utilizatorului.
Export Users	Faceți clic pentru a exporta utilizatorii locali în fișiere în format CVS sau Excel. Selectați portalurile în funcție de nevoi, iar utilizatorii locali ai portalului ales vor fi exportați.
	Faceți clic pentru a edita parametrii pentru utilizatorul local.
	Faceți clic pentru a șterge utilizatorul local.

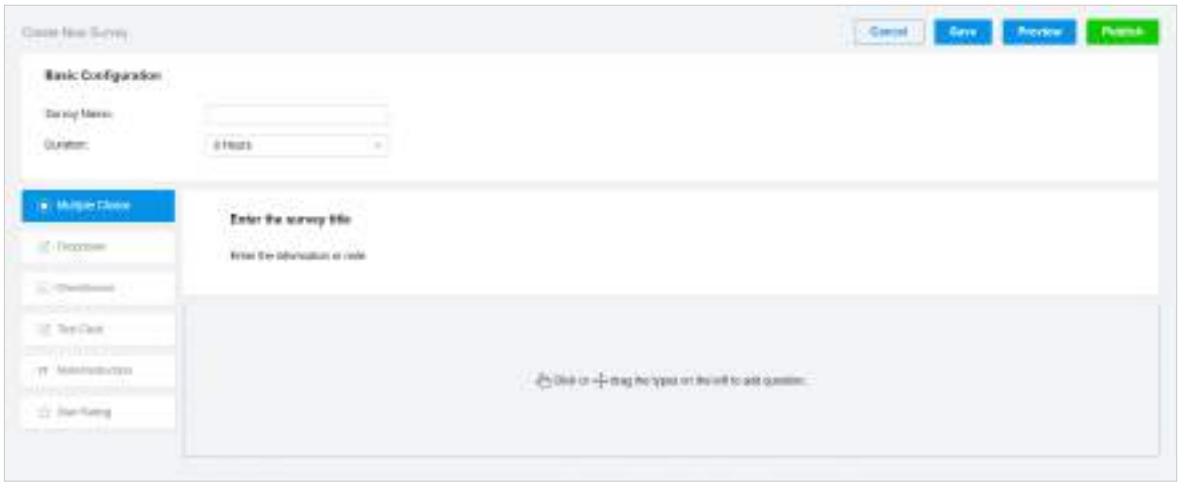
6. 2. 5 Date Auth Form

Fila Date Auth Form este folosită pentru a crea și gestiona sondaje. Puteți personaliza conținutul sondajului și îl puteți publica pentru a colecta date.

Creați sondaje

Pentru a crea sondaje, urmați pașii de mai jos.

1. Faceți clicManager hotspotdin lista derulantă aOrganizareși faceți clicDate de autentificare formularîn pagina pop-up.
2. Faceți clicCreați un sondaj nouși apare următoarea fereastră.



3. Specificați numele și durata sondajului, apoi personalizați conținutul.
4. Previzualizați și salvați setările sau publicați sondajul.
5. Sondajele sunt create și afișate în tabel. Puteți folosi pictograme pentru management.

	Faceți clic pentru a edita parametrii pentru intrare.
	Faceți clic pentru a șterge intrarea.
	Faceți clic pentru mai multe opțiuni de gestionare: copiați, exportați date și ștergeți.

6. 2. 6 Operatori

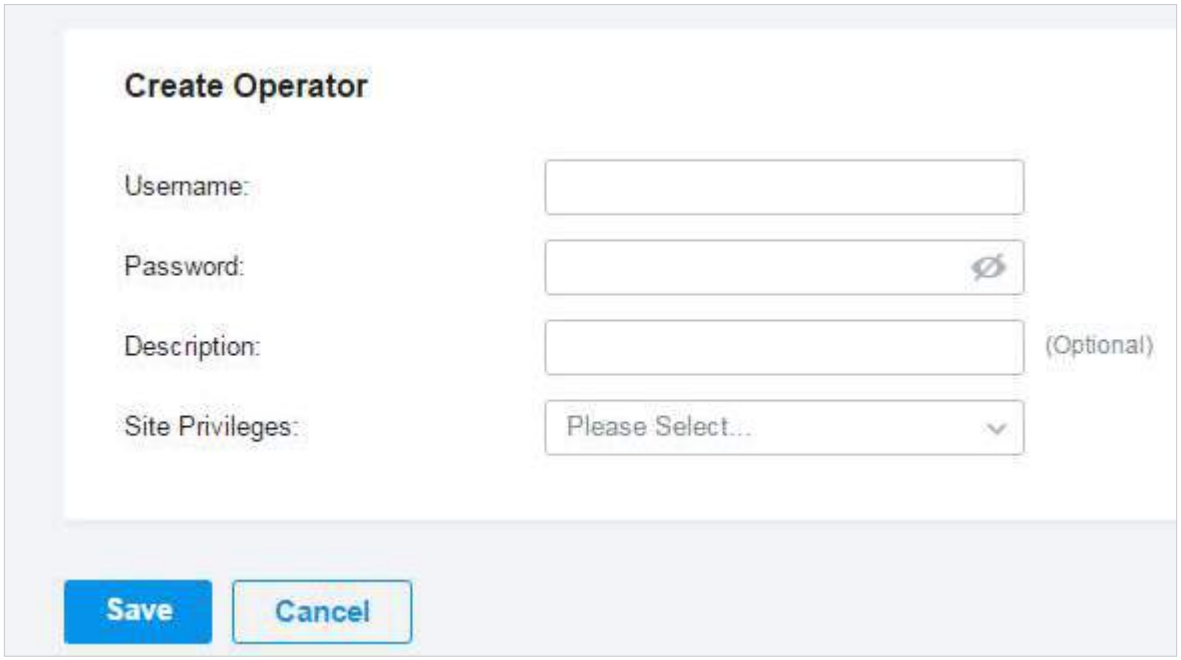
Fila Operatori este folosită pentru a gestiona și a crea conturi de operator care pot fi folosite doar pentru a vă conecta de la distanță la sistemul Hotspot Manager și pentru a gestiona vouchere și utilizatori locali pentru site-urile specificate. Operatorii nu au privilegii de a crea conturi de operator, ceea ce oferă confort și asigură securitatea pentru autentificarea clientului.

Creați operatori

Pentru a crea conturi de operator, urmați pașii de mai jos.

1. Faceți clicManager hotspotdin lista derulantă aOrganizareși faceți clicOperatoriîn pagina pop-up.

2. Faceți clic + Create Operator din stânga jos și apare următoarea fereastră.



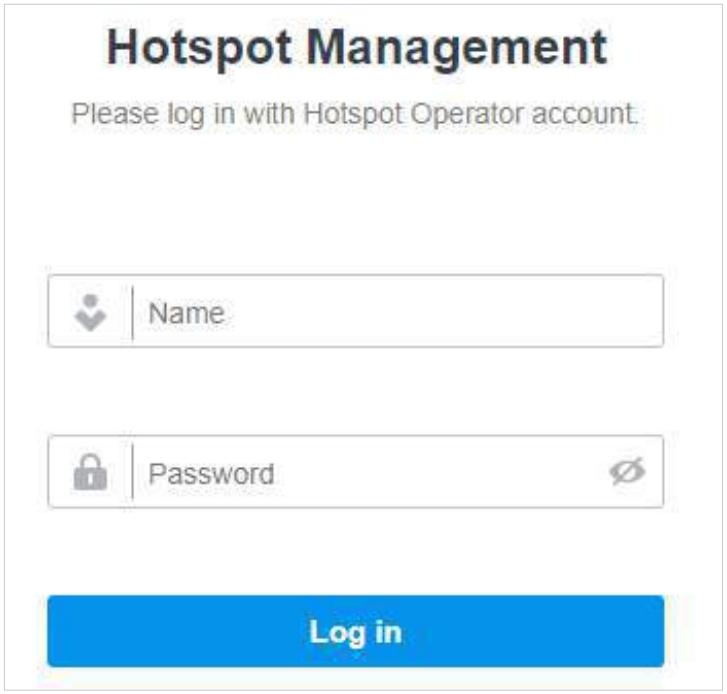
3. Specificați numele de utilizator, parola și descrierea (opțional) pentru contul de operator. Apoi selectați site-uri din lista derulantă aPrivilegii site. ClicSalvați.

4. Conturile de operator sunt create și afișate în tabel. Puteți vizualiza informațiile conturilor de operator create pe pagină, puteți căuta anumite conturi prin nume și note și puteți utiliza pictograme pentru administrare.

	Faceți clic pentru a edita parametrii pentru contul de operator.
	Faceți clic pentru a șterge contul de operator.

5. Apoi puteți utiliza un cont de operator pentru a vă conecta la sistemul Hotspot Manager:

Accesați adresa URLhttps://Adresa IP a gazdei controlerului Omada:443/ControllerID/login/#hotspot (de exemplu: https://192.168.0.174:443/4d4ede7983bb983545d017c628feaa3d/login/#hotspot), și utilizați contul de operator pentru a intra în sistemul de gestionare a hotspot-ului.



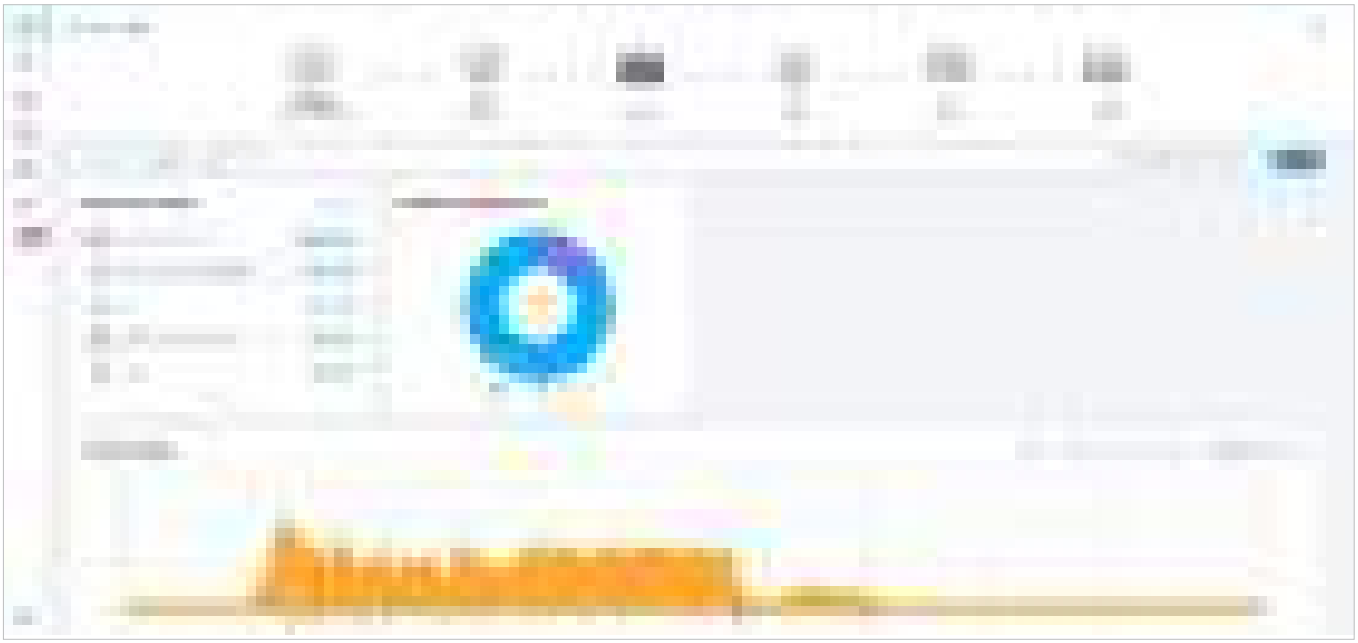
Monitorizați rețeaua

Acest capitol vă ghidează despre cum să monitorizați dispozitivele de rețea, clienții și statisticile acestora. Prin prezentări vizuale și în timp real, Omada SDN Controller vă ține la curent cu privire la starea exactă a rețelei gestionate. Acest capitol include următoarele secțiuni:

7. 1 Vizualizați starea rețelei cu tabloul de bord

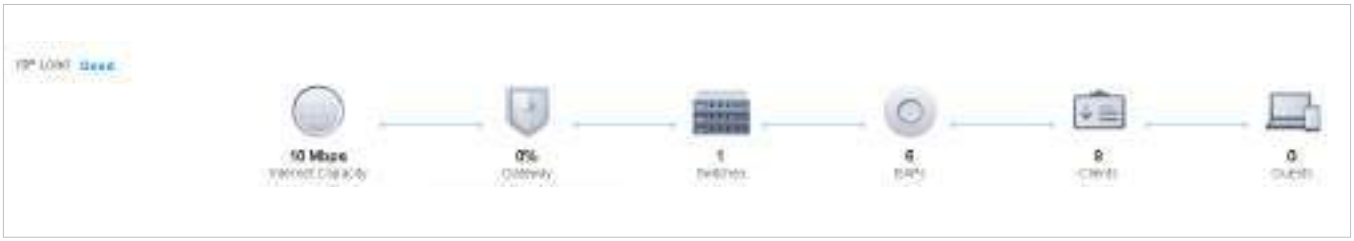
7. 1. 1 Aspect de pagină a tabloului de bord

Tabloul de bord este conceput pentru o monitorizare rapidă în timp real a rețelei site-ului. O prezentare generală a topologiei rețelei este în partea de sus a Tabloului de bord, iar mai jos este o bară de file urmată de widget-uri personalizate.



Prezentare generală a topologiei

Prezentare generală a topologiei în partea de sus arată starea ISP Load și numărul de dispozitive, clienți și oaspeți. ISP Load are patru stări: Necunoscut, Bun, Mediu, Slab.



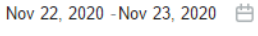
Puteți trece cursorul peste pictogramele gateway, switch, AP, client sau invitat pentru a verifica starea acestora. Pentru informații detaliate, faceți clic pe pictograma aici pentru a sări laDispozitivesauClienții secțiune.

Bara de file

Puteți personaliza widget-urile afișate în fila pentru pagina Tablou de bord. Trei file sunt create implicit și nu pot fi șterse.

Prezentare generală	Afișează în mod implicit prezentarea generală a controlerului și erorile de asociere.
Rețea	Afișează în mod implicit Alerte, Distribuția traficului Wi-Fi, Rezumatul Wi-Fi și Activitățile de trafic.
Clienții	Afișează cei mai mulți clienți activi, distribuția frecvenței clienților și activitățile clientului în mod implicit.

În bara de file, puteți efectua următoarea acțiune pentru a edita filele și a personaliza widgetul care urmează să fie afișat.

	Faceți clic pe pictogramă pentru a edita filele. Pentru filele implicite, le puteți reseta la setările implicite. Pentru o filă creată, îi puteți edita numele sau o puteți șterge.
	Faceți clic pe pictogramă și introduceți numele în fereastra pop-up pentru a crea o filă nouă.
	Faceți clic pe dată pentru a afișa un calendar. Pentru a afișa rapid statisticile de azi, ieri, ultimele 24 de ore sau ultimele câteva zile, faceți clic pe data/perioada implicită din partea dreaptă a calendarului. Pentru a afișa statisticile unei anumite date, faceți clic pe data de două ori în calendar. Pentru a afișa statisticile pentru un anumit interval de timp, faceți clic pe data de început și data de încheiere din calendar.
	Faceți clic pe o filă, apoi faceți clic pe widget-ul din pagina pop-up pentru a-l adăuga la această filă sau pentru a-l elimina.

7. 1. 2 Explicația widgeturilor

Widgeturile sunt împărțite în două categorii:Rețea,Client. Puteți face clic pe pictogramă pentru a adăuga sau a elimina widget-uri.

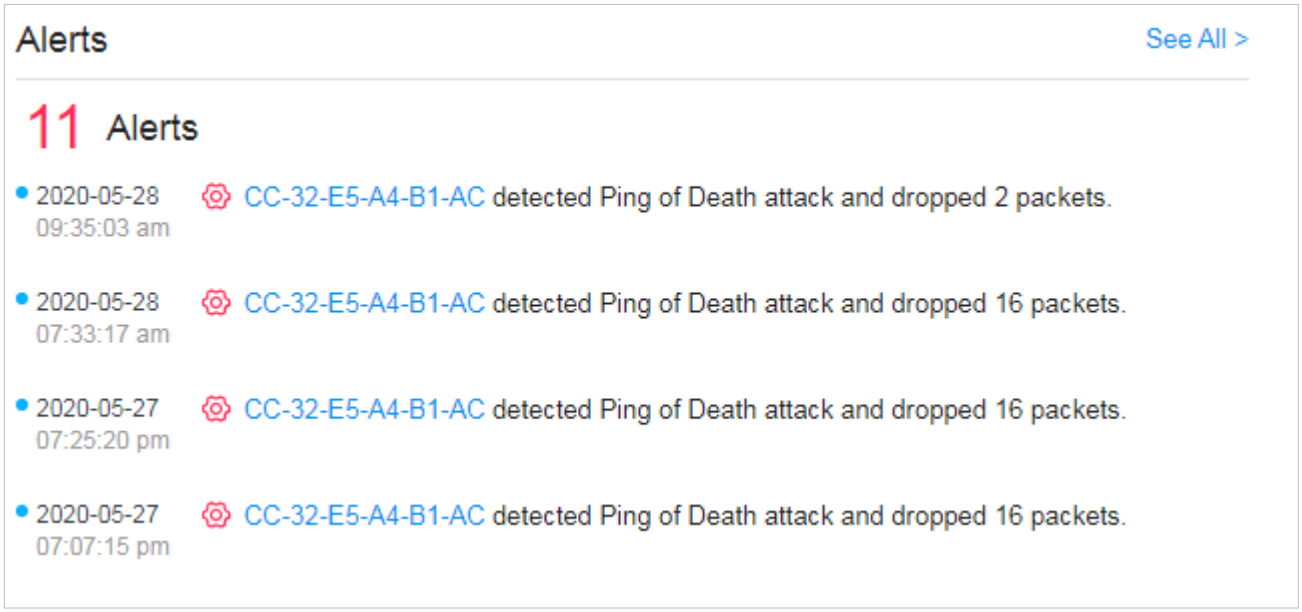
Reţea	Alerte, Încărcare ISP, VPN-uri, Cele mai active EAP-uri, Cele mai active comutatoare, Rezumat Wi-Fi, Rezumat comutare, Distribuție trafic, Distribuție clienți, Activități de trafic, Rată reîncercată/ Rată scăzută, Utilizare de top dispozitive, Utilizare PoE, Interferență de top
Client	Cei mai activi clienți, cel mai lung timp de funcționare al clienților, distribuție frecvență clienți, activități clienți, activități de asociere clienți, eșecuri de asociere, distribuire SSID clienți, clienți cu timpi de îmbarcare, clienți cu RSSI

Reţea

Widgeturile din Rețea folosesc liste și diagrame pentru a ilustra starea traficului rețelelor cu fir și fără fir din site, inclusiv statistici de trafic, cele mai active dispozitive, conexiune VPN, distribuție, utilizarea PoE și interferențe.

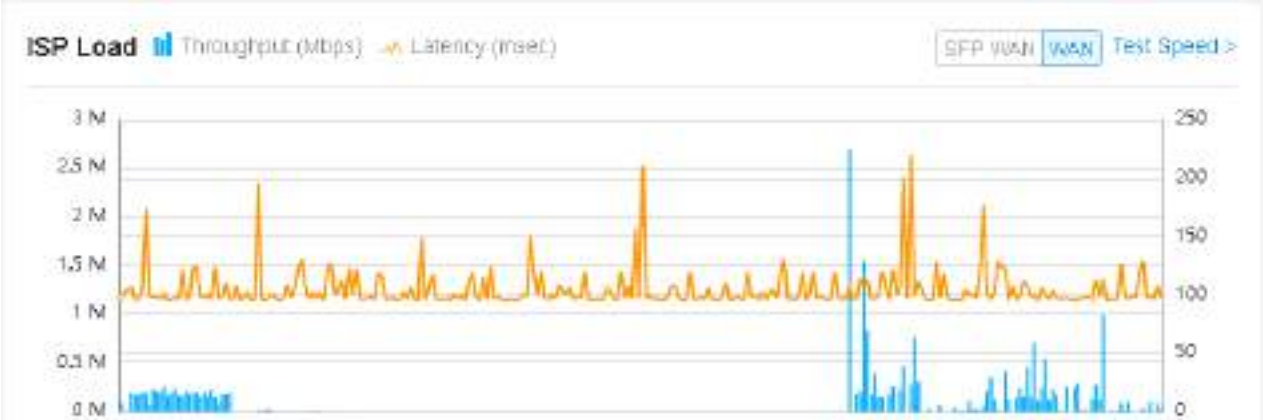
- Alerte

  Widgetul Alerte afișează numărul total de alerte nearhivate care au avut loc pe site și detalii despre ultimele cinci. Pentru a vizualiza toate alertele și pentru a le arhiva, faceți clic peVezi toatea sari laButuruga>Alerte. Pentru a specifica evenimentele apărute în Alerte, accesațiButuruga>Notificărișsi configurați evenimentele ca nivel de alertă. Pentru detalii, consultați7. 6 Vizualizați și gestionați jurnalele .



- Încărcare ISP

ISP Load utilizați o diagramă cu linii pentru a afișa debitul și latența portului WAN al gateway-ului în intervalul de timp. Faceți clic pe fila din dreapta pentru a vizualiza statisticile fiecărui port WAN și mutați cursorul pe diagrama cu linii pentru a vizualiza valori specifice ale debitului și al latenței. Pentru statistici detaliate despre portul WAN al anumitor gateway-uri într-un interval de timp, consultați7. 2 Vizualizați Statisticile rețelei .



Pentru a testa viteza actuală de descărcare și descărcare și latența portului WAN, faceți clicTest de vitezăpe widget pentru a afișa rezultatul testului de viteză.

- VPN-uri

VPN-urile afișează informațiile despre serverele VPN și clienții VPN. Faceți clic pe fila corespunzătoare pentru a afișa statisticile.

Nume	Afișează numele serverului/clientului VPN.
stare	Afișează starea conexiunii serverului/clientului VPN.
Tuneluri	Afișează numărul de tuneluri VPN pentru serverul VPN.
Date Tx medii	Afișează traficul transmis mediu al serverului/clientului VPN.
Date medii Rx	Afișează traficul mediu primit al serverului/clientului VPN.
Statistici	Afișează traficul în amonte și în aval al serverului/clientului VPN.

IP de conectare	Afișează IP-ul de conectare al VPN-ului SSL.
ID-ul tunelului	Afișează direcția tunelului VPN IPSec.
Flux de date	Afișează fluxul de date al tunelului VPN IPSec.

- Cele mai active EAP-uri/ Cele mai active comutatoare

  Aceste două widget-uri pot afișa, respectiv, 15 EAP-uri și switch-uri cele mai active din site în funcție de numărul total de trafic din intervalul de timp. Vor fi afișate doar dispozitivele care au fost adoptate de controler.

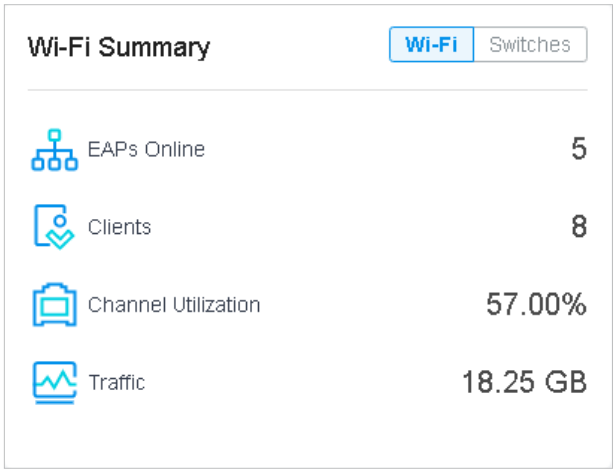
  Pentru a vizualiza toate dispozitivele descoperite de controler, faceți clicVezi toatea sari laDispozitivesecțiune. De asemenea, puteți face clic pe numărul de trafic din widget pentru a deschide fereastra Proprietăți a dispozitivului pentru configurații și monitorizare suplimentare. Pentru detalii, consultați5 Configurați și monitorizați dispozitivele gestionate Omada .

- Distribuția traficului Wi-Fi

  Wi-Fi-ul Wi-Fi Traffic Distribution afișează distribuția canalelor tuturor EAP-urilor conectate de pe site. Bine, Normal și Slab sunt folosite pentru a descrie starea canalului, care indică interferența canalului de la scăzut la ridicat. Puteți trece cursorul peste bandă pentru a vedea numărul de EAP și clienți de pe canal.

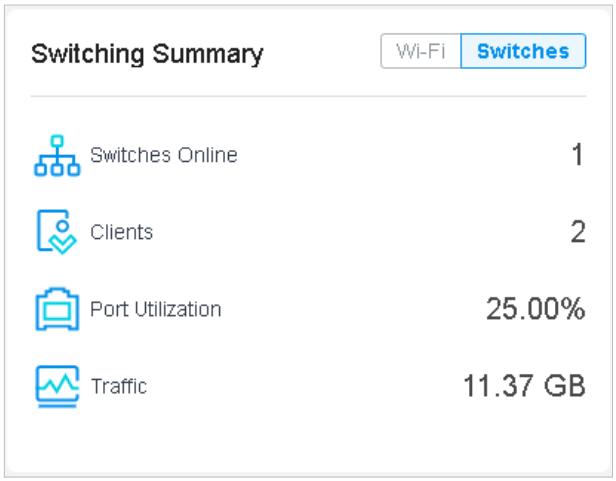
- Rezumat Wi-Fi

  Wi-Fi-ul Rezumat Wi-Fi rezumă starea în timp real a rețelelor fără fir din site, inclusiv numărul de EAP-uri și clienți conectați, utilizarea canalului și numărul total de trafic în intervalul de timp.



- Rezumatul comutării

  Widgetul Switching Summary rezumă starea în timp real a switch-urilor de pe site, inclusiv numărul de switch-uri și clienți conectați, utilizarea portului și cantitatea totală de trafic în intervalul de timp.



- Distribuția traficului

  Widgetul Distribuția traficului folosește o diagramă circulară pentru a afișa distribuția traficului pe EAP-uri și comutatoare din site în intervalul de timp. Faceți clic pe fila pentru a afișa statistica EAP-urilor sau a comutatoarelor și faceți clic pe segment pentru a vedea numărul total de trafic, proporția acestuia și numele dispozitivului.

- Distribuția clienților

  Widgetul Client Distribution folosește o diagramă sunburst pentru a afișa distribuția în timp real a clienților conectați pe site. Graficul are până la trei niveluri. Cercul interior este împărțit la categoria de dispozitiv la care clienții sunt conectați, mijlocul este după numele dispozitivului, iar cel exterior este după banda de frecvență. Puteți trece cursorul peste felie pentru a vedea anumite valori.

- Activități de trafic

  Widgetul Activități de trafic afișează datele Tx și Rx ale EAP-urilor și comută în intervalul de timp. Vor fi contorizate doar activitățile dispozitivelor aflate în starea conectate în prezent.

Faceți clic pe fila pentru a afișa statistica EAP-urilor sau a comutatoarelor și mutați cursorul pe diagrama cu linii pentru a vizualiza anumite valori ale traficului. Pentru statistici detaliate ale anumitor dispozitive într-un interval de timp, consultați 7. 2 Vizualizați Statisticile rețelei .

- Rata reîncercată/Rata renunțată

Widgetul Rata reîncercată/Rata renunțată afișează rata pachetelor reîncercate și abandonate ale EAP-urilor conectate în intervalul de timp. Selectați un AP din listă și faceți clic pe fila pentru a afișa graficul ratei reîncercate sau ratei renunțate. Puteți muta cursorul pe punct pentru a vizualiza anumite valori.

Rata reîncercată	Afișează procentul de pachete care au trebuit să fie retrimise deoarece au fost corupte la sosirea la destinația potrivită.
Rata scăzută	Afișează procentul de pachete care au fost abandonate înainte de a ajunge la destinația dorită.

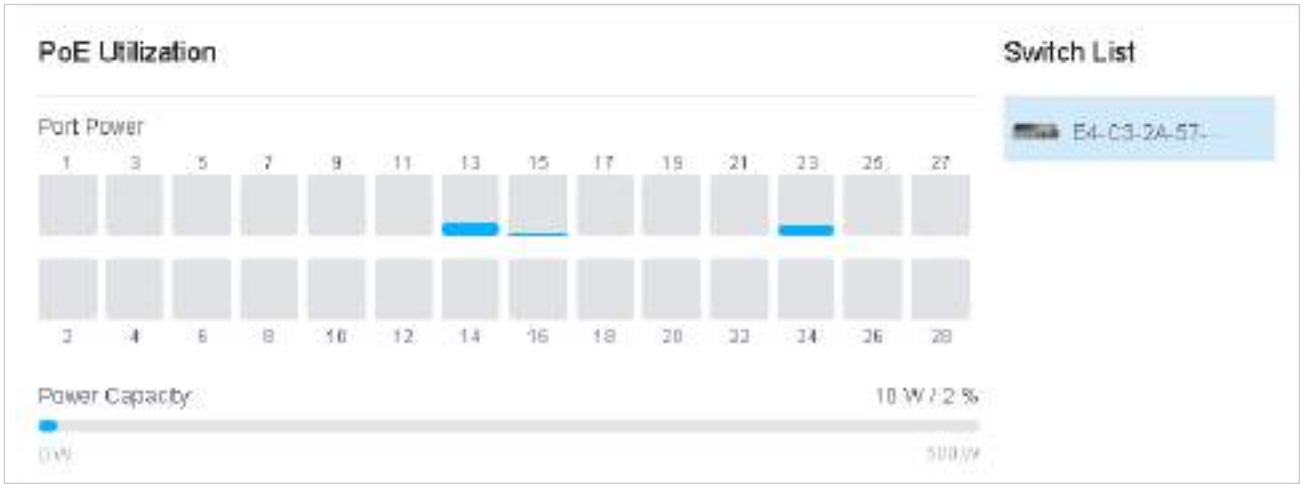
- Top Utilizare Dispozitive

Widgetul Top Devices Usage afișează utilizarea CPU și utilizarea memoriei dispozitivelor în intervalul de timp. Faceți clic pe fila pentru a selecta procesorul sau memoria pentru afișare. Faceți clic pe numărul de trafic în

widget-ul pentru a deschide fereastra Proprietăți a dispozitivului pentru configurații și monitorizare ulterioare. Pentru detalii, consultați5 Configurați și monitorizați dispozitivele gestionate Omada .

■ Utilizare PoE

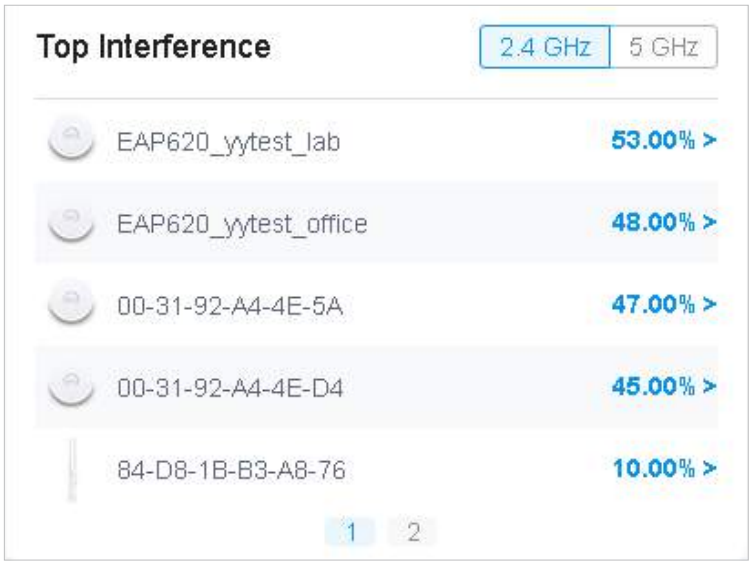
Widgeturile de utilizare PoE descrie utilizarea PoE a unui comutator. Selectați un comutator din lista de comutatoare pentru a afișa porturile conectate la dispozitivele PoE. Puteți trece cursorul peste un anumit port pentru a vedea anumite valori. Bara de mai jos afișează capacitatea curentă de alimentare furnizată de PoE și proporția acesteia din bugetul PoE.



■ Top Interferență

Widgetul Top Interference afișează interferențele de mediu ale produselor wireless. Faceți clic pe fila pentru a selecta banda de 2,4 GHz sau banda de 5 GHz. Faceți clic pe numărul de trafic din widget pentru a deschide

fereastra Proprietăți a dispozitivului pentru configurații și monitorizare ulterioare. Pentru detalii, consultați5 Configurați și monitorizați dispozitivele gestionate Omada .



Client

Widgeturile din Clienți folosesc liste și diagrame pentru a ilustra starea traficului clienților cu fir și fără fir din site, inclusiv cei mai activi clienți, statistici de activitate și distribuție.

- Cei mai activi clienti

  Widgetul Cei mai activi clienți poate afișa 15 cei mai activi clienți. Vor fi afișați doar clienții în starea conectată în prezent.

  Pentru a vedea toți clienții conectați la rețea, faceți clic peVezi toatea sari laCliențiisecțiune. De asemenea, puteți face clic pe numărul de trafic din widget pentru a deschide fereastra Proprietăți a clientului pentru configurații și monitorizare ulterioare. Pentru detalii, consultați„6. 1 Gestionați clienții cu fir și fără fir în pagina Clienți” .

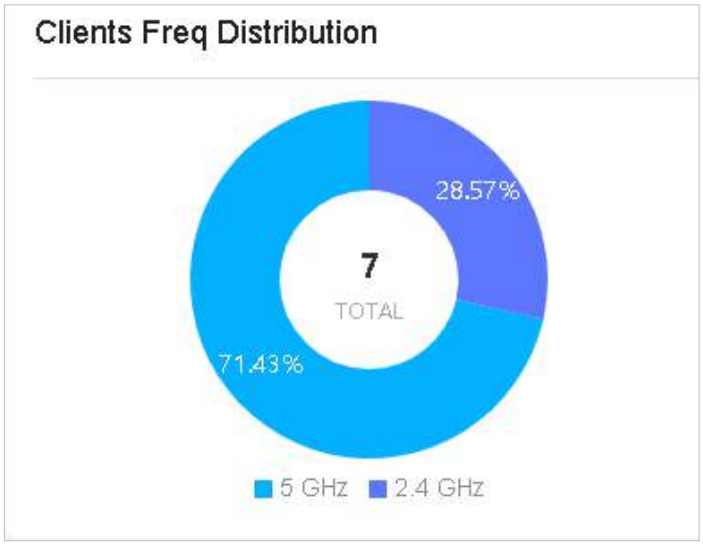
- Cel mai lung timp de funcționare a clientului

  Widgetul Cel mai lung timp de funcționare a clientului poate afișa până la 15 clienți sortați în funcție de timpul de funcționare. Vor fi afișați doar clienții în starea conectată în prezent. De asemenea, puteți face clic pe timpul de funcționare din widget pentru

deschide fereastra Proprietăți a clientului pentru configurații și monitorizări suplimentare. Pentru detalii, consultați „6. 1 Gestionați clienții cu fir și fără fir în pagina Clienți” .

- Distribuția frecvenței clienților

  Widgetul Clients Freq Distribution folosește o diagramă donut pentru a afișa distribuția clienților wireless conectați la banda de 5 GHz și banda de 2,4 GHz în site. Graficul are două niveluri. Cercul interior arată numărul total de clienți wireless, iar cel exterior afișează proporția de clienți care se conectează la cele două benzi. Puteți trece cursorul peste secțiune pentru a vedea numărul de clienți în banda de 2,4 GHz sau 5 GHz.



- Activități ale Asociației Clienților

  Widgetul Activități Asociația Clienților afișează modul în care numărul de clienți conectați la EAP-uri se modifică în timp și durata în care clienții comunică cu EAP-urile. În graficul stivuit, puteți compara cu ușurință numărul total de clienți și puteți analiza variația fiecărei perioade de timp.

Valoarea totală a unei coloane arată numărul total de clienți conectați la EAP-uri în această perioadă de timp, iar segmentele în patru culori reprezintă numărul de clienți cu durate diferite într-un anumit timp.

- Activități ale clienților

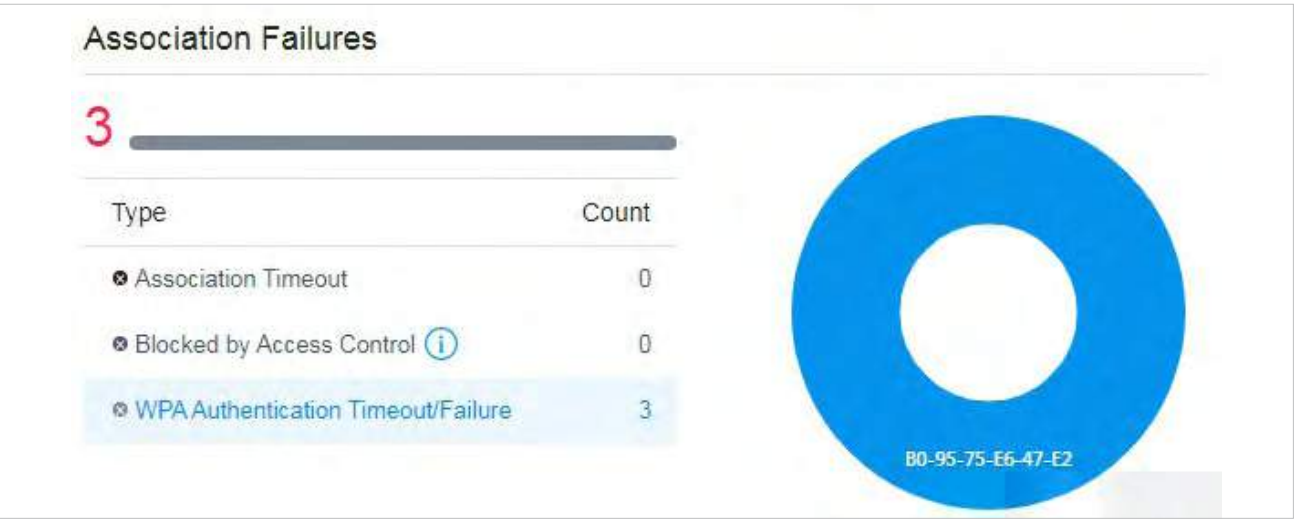
Widgetul Activități client afișează modul în care numărul de clienți conectați se modifică în timp în intervalul de timp. În graficul stivuit, puteți compara cu ușurință numărul total de clienți și puteți analiza variația fiecărei perioade de timp.

Valoarea totală a unei coloane arată numărul total de clienți conectați în această perioadă de timp, iar segmentele în trei culori arată modificarea numărului de client în comparație cu ultima perioadă de timp. Albastru reprezintă clienții nou conectați, portocaliu este clienții care au fost conectați în ultima perioadă, iar gri este clienții nou deconectați.

- Eșecurile Asociației

Widgetul Eșecuri de asociere listează trei tipuri de defecțiuni și perioadele în care clienții nu au reușit să se conecteze la rețelele EAP-urilor din site. O singură bară este lângă numărătoare pentru a arăta proporția dintre

trei motive de eșec folosind culorile gri de la întunecat la deschis. Faceți clic pe motivul din listă pentru a vedea distribuția eșecurilor pe EAP.



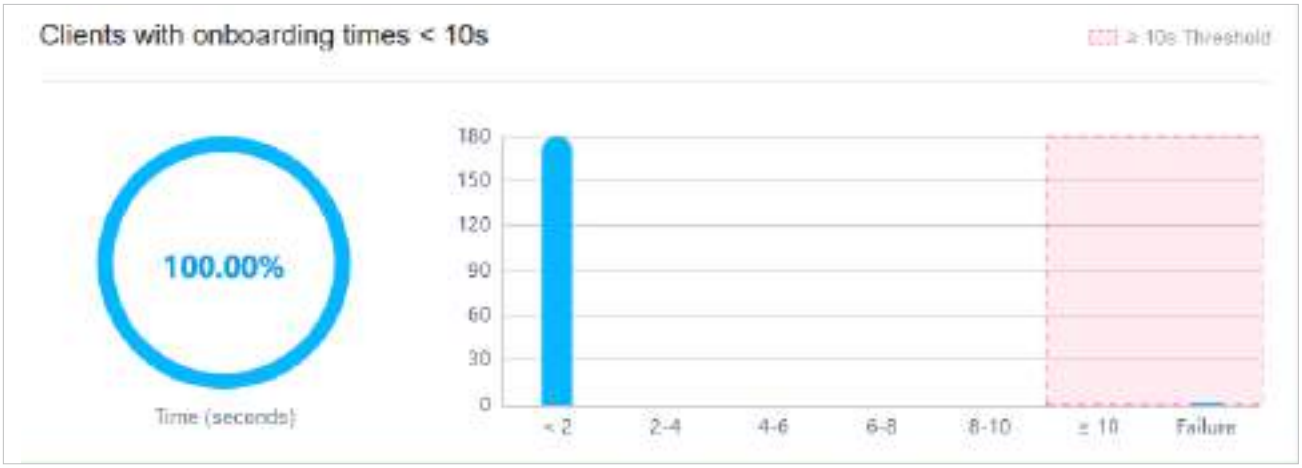
Timp de asociere	Conexiunea a eșuat din cauza expirării sesiunii.
Blocat de controlul accesului	Conexiunea a eșuat deoarece clientul a fost blocat. Pentru detalii despre clienții blocați, consultați7. 5. 1 Clienți cunoscuți.
Timeout/Eșec de autentificare WPA	Conexiunea a eșuat deoarece clientul nu a trecut autentificarea din cauza expirării timpului de autentificare sau a parolei greșite.

■ Distribuție SSID clienți

Widgetul SSID Distribution folosește o diagramă sunburst pentru a afișa distribuția clienților wireless conectați la diferitele SSID-uri din site. Graficul are două niveluri. Cercul interior este împărțit la SSID-ul EAP la care s-au conectat clienții, iar cel exterior este de banda de frecvență. Puteți trece cursorul peste secțiune pentru a vedea numărul de clienți conectați la SSID în banda de 2,4 GHz sau 5 GHz. Faceți clic pe un anumit SSID pentru a afișa în continuare statisticile distribuției sale de frecvență a benzii.

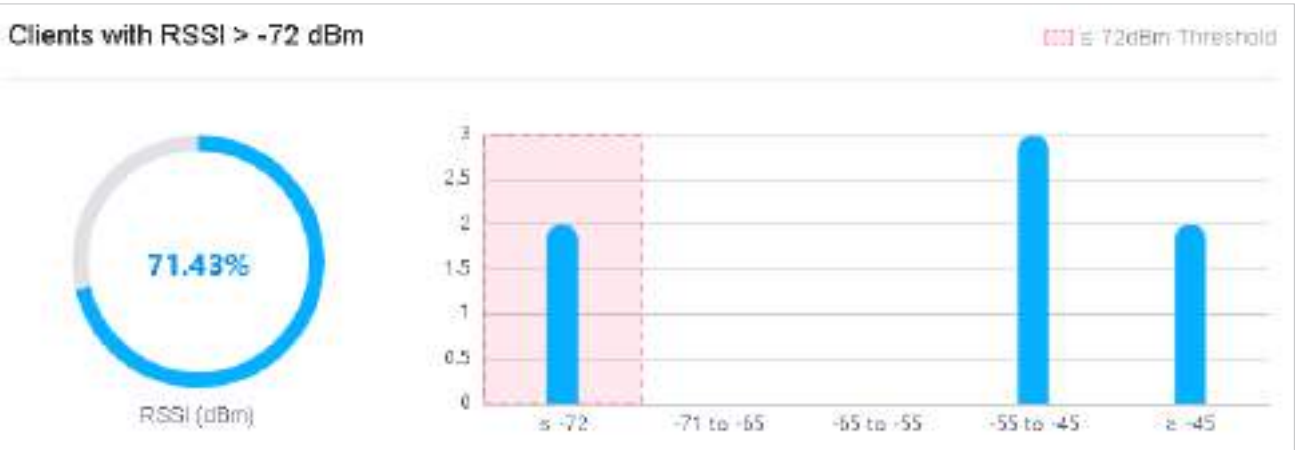
- Clienți cu timp de îmbarcare

  Widgetul Clienți cu orele de îmbarcare descrie timpul pe care clienții fără fir îl folosesc atunci când se conectează la un anumit SSID. Graficul donut din stânga arată proporția de clienți care folosesc mai puțin de 10 secunde pentru a se conecta la dispozitive. Graficul cu linii din dreapta afișează numărul de clienți în funcție de timpul diferit pe care clienții îl au pentru a se conecta la SSID-urile.



- Clienți cu RSSI

  Widgetul Clienți cu RSSI descrie RSSI (indicație de putere a semnalului primit) pe care clienții wireless îl experimentează în mediu. RSSI este o valoare negativă care măsoară nivelul de putere primit după orice posibilă pierdere la nivelul antenei și cablului. Cu cât valoarea RSSI este mai mare, cu atât semnalul este mai puternic. Graficul gogoși din stânga arată proporția clienților a căror valoare RSSI este mai mare de -72 dBm. Graficul cu linii din dreapta afișează numărul de clienți în funcție de diferitele valori ale intervalului RSSI.



7. 2 Vizualizați Statisticile rețelei

Statisticile oferă o reprezentare vizuală a datelor dispozitivului în Omada SDN Controller. Puteți monitoriza cu ușurință traficul și performanța rețelei în următoarele file, Performanță, Statistici comutatoare și Statistici test de viteză.

7. 2. 1 Performanță

În Performanță, puteți vizualiza performanța dispozitivului într-o perioadă specificată prin grafice, cum ar fi numărul de utilizatori, CPU și utilizarea memoriei și pachetele transmise și primite. Graficele variază în funcție de tipul și starea dispozitivului.

Bara de file

Filele și calendarul din partea de sus sunt folosite pentru a specifica statisticile afișate, iar legendele din dreapta contează elementele din grafice.

	Faceți clic pentru a selecta un dispozitiv din lista derulantă pentru a vedea statisticile acestuia. Filele variază în funcție de tipul dispozitivului selectat.
	Faceți clic pe dată pentru a afișa un calendar. Faceți clic pe o anumită dată de două ori în calendar pentru ca widget-urile să-și afișeze statisticile. Pentru a afișa statistica unui interval de timp, faceți clic pe data de început și data de încheiere din calendar sau selectați direct intervalul de timp din dreapta. Intervalul de timp disponibil este limitat de intervalul de timp. Înainte de a selecta un interval de timp lung, selectați Orară sau Zilnic ca interval de timp.
	Selectați5 minute,Orar, sauZilnicpentru a specifica intervalul de timp al datelor. Când selectați un interval de timp lung, se recomandă un interval de timp mai lung pentru o vizualizare mai bună.
	(Pentru gateway) Faceți clic pentru a selecta portul gateway-ului din fila pentru a vizualiza statisticile.
	(Pentru AP) Faceți clic pentru a selecta banda AP pentru a vizualiza statisticile.

Grafice statistice

Graficele statistice variază în funcție de tipul de dispozitive. Graficul de mai jos prezintă graficele statistice care corespund gateway-ului, comutatorului și AP.

Poarta de acces	Număr de utilizatori, utilizare, trafic, pachete
Intrerupator	Număr de utilizatori, utilizare
AP	Număr de utilizatori, utilizare, trafic, pachete, scăpat, erori, reîncercări

■ Numărul de utilizatori

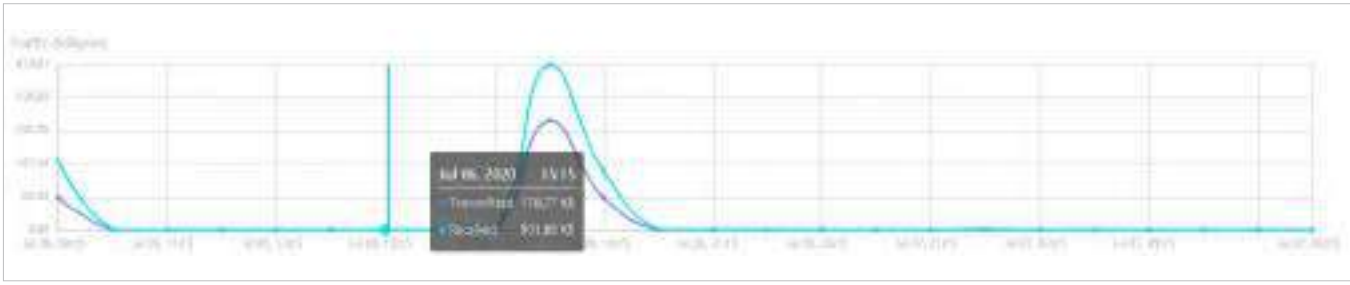
Graficul User Counts afișează numărul de utilizatori conectați la dispozitive în intervalul de timp selectat. Treceți cursorul peste linie pentru a afișa valorile specifice.

■ Utilizare

Graficul de utilizare folosește linia portocalie și linia galbenă pentru a afișa procentul de utilizare a CPU și, respectiv, memoria utilizată în intervalul de timp selectat. Treceți cursorul peste linii pentru a afișa valorile specifice.

■ Trafic

Graficul Trafic utilizează linia albastră închisă și linia albastră deschisă pentru a afișa octeții de date transmise și recepționate în intervalul de timp selectat. Treceți cursorul peste linii pentru a afișa valorile specifice.



■ Pachete

Graficul Pachete utilizează linia albastru închis și linia albastru deschis pentru a afișa numărul de pachete transmise și primite în intervalul de timp selectat. Treceți cursorul peste linii pentru a afișa valorile specifice.

■ Scăzut

Graficul Dropped folosește linia albastră închisă și linia albastră deschisă pentru a afișa numărul de pachete Tx și, respectiv, de pachete Rx abandonate în intervalul de timp selectat. Treceți cursorul peste linii pentru a afișa valorile specifice.

■ Erori

Graficul Erori folosește linia albastru închis și linia albastru deschis pentru a afișa numărul de pachete de eroare trimise către AP și primite de AP în intervalul de timp selectat, respectiv. Treceți cursorul peste linie pentru a afișa valorile specifice.

■ Reîncercări

Graficul Retries folosește linia albastră închisă și linia albastru deschis pentru a afișa numărul de ori în care pachetele de date sunt transmise din nou și, respectiv, primite din nou în perioada selectată. Treceți cursorul peste linii pentru a afișa valorile specifice.

7. 2. 2 Comutare Statistici

În Switch Statistics, puteți vizualiza starea curentă a porturilor și statisticile de trafic ale comutatorului selectat în intervalul de timp specificat, printr-un panou de monitor și grafice.

Bara de file

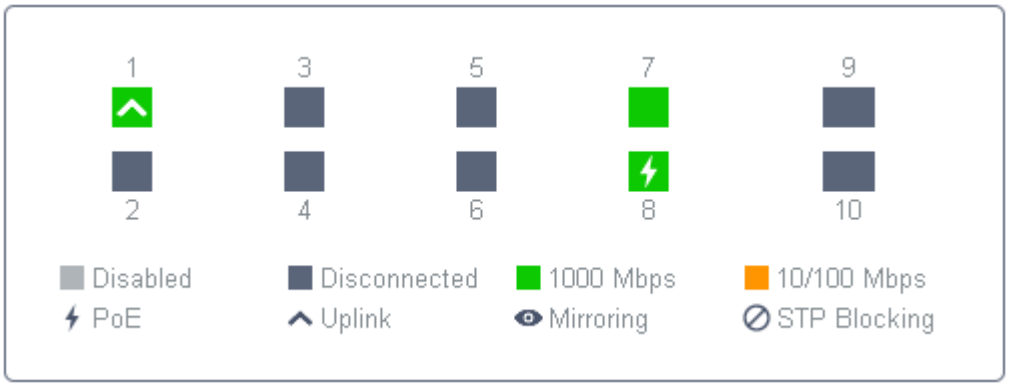
Filele și calendarul din partea de sus sunt folosite pentru a specifica statisticile afișate, iar legendele din dreapta contează elementele din grafice.

switch	Faceți clic pentru a selecta un comutator din lista derulantă pentru a vedea statisticile acestuia.
Jul 06, 2020 - Jul 07, 2020	Faceți clic pe dată pentru a afișa un calendar. Faceți clic pe o anumită dată de două ori în calendar pentru ca widget-urile să-și afișeze statisticile. Pentru a afișa statistica unui interval de timp, faceți clic pe data de început și data de încheiere din calendar sau selectați direct intervalul de timp din dreapta. Intervalul de timp disponibil este limitat de intervalul de timp. Înainte de a selecta un interval de timp lung, selectați Orară sau Zilnic ca interval de timp.
Hourly	Selectați5 minute,Orar, sauZilnicpentru a specifica intervalul de timp al datelor. Când selectați un interval de timp lung, se recomandă un interval de timp mai lung pentru o vizualizare mai bună.
Sort: Natural	Selectați Natural, Transmis, Received sau All pentru a specifica ordinea grafică a porturilor. Natural:Afișează graficele cu linii în ordinea crescătoare a numărului portului. Transmis:Afișează graficele de linii în ordine descrescătoare în funcție de volumul de trafic al pachetelor transmise. Primit:Afișează graficele de linii în ordine descrescătoare în funcție de volumul de trafic al pachetelor primite. Toate:Afișează graficele de linii în ordine descrescătoare pe baza volumului total de trafic al pachetelor transmise și primite.

	Selectați bps, octeți sau pachete pentru a specifica tipul de date și unitatea de măsură. bps: Afișează rata de trafic în bps. octeți: Afișează statisticile de trafic în octeți. Pachete: Afișează numărul total de pachete.
	Dacă selectațiPachet, faceți clic pe fila pentru a specifica ce tip de statistici de pachete vor fi afișate. Toate:Afișează statistici pentru toate pachetele, inclusiv pachetele de difuzare și multicast. Difuzare:Afișează numai statisticile pachetelor de difuzare. Multicast:Afișează numai statisticile pachetelor multicast.

Panoul de monitorizare

Panoul de monitor de sub bara de file afișează starea curentă a porturilor de pe comutatorul selectat.

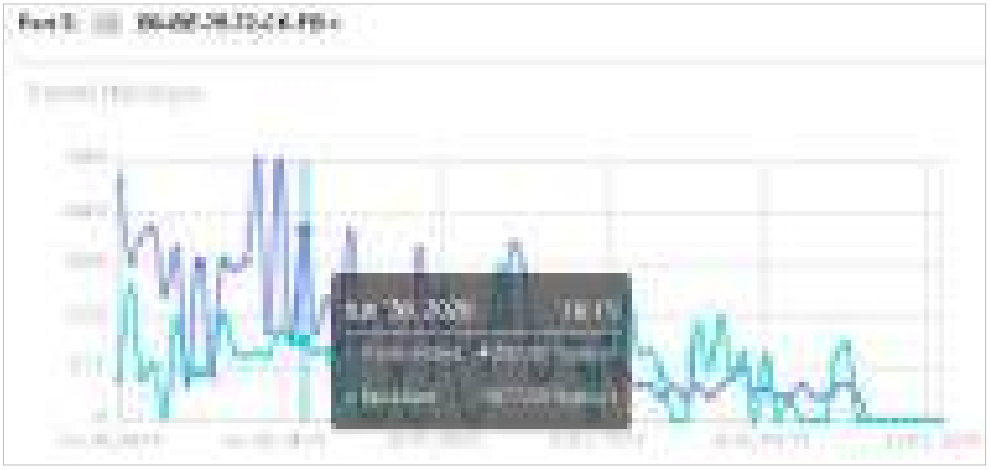


Dezactivat	Profilul portului este Dezactivat. Pentru a-l activa, consultați5. 3 Configurați și monitorizați comutatoarele.
Deconectat	Portul este activat, dar nu se conectează la niciun dispozitiv sau client.
1000 Mbps	Portul rulează la 1000 Mbps.
10/100 Mbps	Portul rulează la 10/100 Mbps.
PoE	Un port PoE conectat la un dispozitiv alimentat (PD).
Uplink	Un port uplink conectat la WAN.
Oglindire	Un port de oglindire care reflectă un alt port de comutare.
Blocare STP	Un port în starea Blocare în Spanning Tree. Acesta primește și trimite pachete BPDU (Bridge Protocal Data Unit) pentru a menține arborele de acoperire. Alte pachete sunt aruncate.

Grafice statistice

Graficele statistice de sub panoul monitorului afișează statisticile de trafic ale porturilor active.

Puteți specifica tipul de date și unitatea de măsură făcând clic pe bps Bytes Packets fila. Albastrul închis și albastru deschis sunt folosite pentru a indica statisticile transmise, respectiv primite. Treceți cursorul peste linii pentru a afișa valorile specifice. Pentru a vizualiza și configura dispozitivul conectat la port, faceți clic pe numele dispozitivului de lângă numărul portului.



7. 3 Monitorizați rețeaua cu Hartă

În secțiunea Hartă, puteți consulta topologia și furnizarea dispozitivelor rețelei înTopologieși personalizează o reprezentare vizuală a rețelei dvs. înHarta termograficași afișați vizual locația geografică a fiecărui dispozitiv și site înHarta dispozitivuluișiHarta site-ului.

7. 3. 1 Topologie

Mergi laHartă>Topologie, și puteți vizualiza automat topologia generată de controler. Puteți face clic pe pictograma dispozitivelor pentru a deschide fereastra Proprietăți. Pentru configurarea și monitorizarea detaliată în fereastra Proprietăți, consultați5 Configurați și monitorizați dispozitivele gestionate Omada .

Pentru o imagine de ansamblu mai bună a topologiei rețelei, puteți controla afișarea ramurilor, dimensiunea diagramei și etichetele legăturilor.

Afișarea ramurilor

Vizualizarea implicită arată toate dispozitivele conectate prin linii continue și punctate. Faceți clic pe pictograma grupului de clienți pentru a vedea clienții conectați la același dispozitiv. Faceți clic pe încuviințări pentru a desfășura sau a îndoi ramurile.

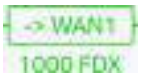
Dimensiunea diagramei

Faceți clic pe pictogramele din colțul din dreapta pentru a ajusta dimensiunea topologiei și pentru a vedea legendele.

	Faceți clic pentru a potrivi topologia paginii web.
	Faceți clic pentru a mări topologia.
	Faceți clic pentru a micșora topologia.
	Faceți clic pentru a vedea semnificația liniilor din topologie. Liniile continue și punctate sunt folosite pentru a indica conexiunile cu fir și, respectiv, fără fir, iar patru culori sunt folosite pentru a indica viteza conexiunii.

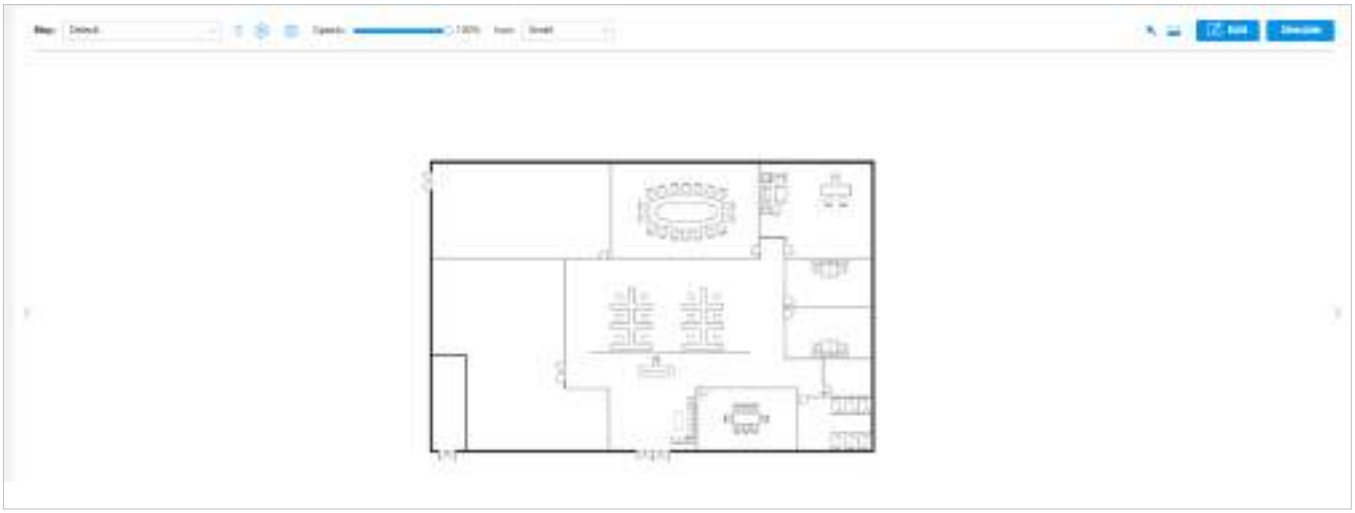
- Link Etichete

  ClicLink Etichetteîn colțul din stânga și vor apărea etichete pentru a afișa starea legăturii. Informațiile de pe etichete variază din cauza conexiunilor de legătură.

	(Pentru portul WAN al routerului conectat la internet) Afișează numele portului, viteza conexiunii și tipul duplex.
	(Pentru conexiuni simple prin cablu) Afișează numărul portului conectat, viteza conexiunii și tipul duplex. Rețineți că numai numărul portului comutatorului poate fi afișat pe etichetă.
	(Pentru Link Aggregation) Afișează ID-ul LAG, numărul de port al membrilor LAG, viteza LAG și tipul duplex.
	(Pentru conexiunile wireless între AP-uri) Afișează rata de negociere a uplink și downlink și RSSI (afișat în procente și dBm).
	(Pentru conexiunile fără fir între AP-uri și clienți)) Afișează SSID-ul conectat, canalul wireless al AP-ului și puterea semnalului acestuia.

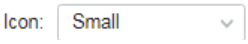
7. 3. 2 Harta termică

Mergi laHartă>Harta termografica, iar o hartă implicită este afișată ca mai jos. Puteți încărca imaginile hărții locale și puteți adăuga dispozitive și diferite tipuri de pereți pentru a personaliza o reprezentare vizuală a rețelei dvs.



Faceți clic pe următoarele pictograme pentru a adăuga, edita și selecta harta. După ce ați selectat o hartă, faceți clic și trageți în dispozitivele dinDispozitivelistă pentru a o plasa pe hartă în funcție de locațiile reale.

	Faceți clic pentru a selecta o hartă din lista derulantă pentru a plasa dispozitivele.

	Faceți clic pentru a edita hărți în fereastra pop-up. Clic  pentru a edita descrierea și aspectul hărții. Clic  pentru a șterge harta.
	Faceți clic pentru a adăuga o hartă. În fereastra pop-up, introduceți descrierea, selectați aspectul și încărcați o imagine în format .jpg, .jpeg, .gif, .png, .bmp, .tiff.
	Reglați opacitatea hărții.
	Faceți clic pentru a selecta dimensiunea pictogramei afișată pe hartă.
	Faceți clic pentru a utiliza instrumentul de selecție pentru a selecta elementele, inclusiv pereții și dispozitivele de pe hartă.
	Faceți clic pentru a utiliza instrumentul de măsurare. Desenați o linie pe hartă pentru a măsura distanța reală în funcție de scara hărții.
	Faceți clic pentru a edita elementele, inclusiv pereții și dispozitivele de pe hartă.
	Faceți clic pe simulați harta termică a rețelei. Rețineți că este necesar să faceți clicSimulapentru a genera o nouă hartă termică după editarea elementelor de pe hartă.
	Faceți clic pentru a potrivi harta pe pagina web.
	Faceți clic pentru a mări harta.
	Faceți clic pentru a micșora harta.
	Faceți clic pentru a seta scara hărții. Desenați o linie pe hartă făcând clic și trăgând, apoi definiți distanța liniei.
	Faceți clic pentru a seta înălțimea implicită a dispozitivelor adăugate și informațiile afișate pe hartă.
	Faceți clic pentru a exporta raportul de acoperire a rețelei.

Configurare

Pentru a genera o reprezentare vizuală și o hartă termică a rețelei dvs., urmați acești pași:

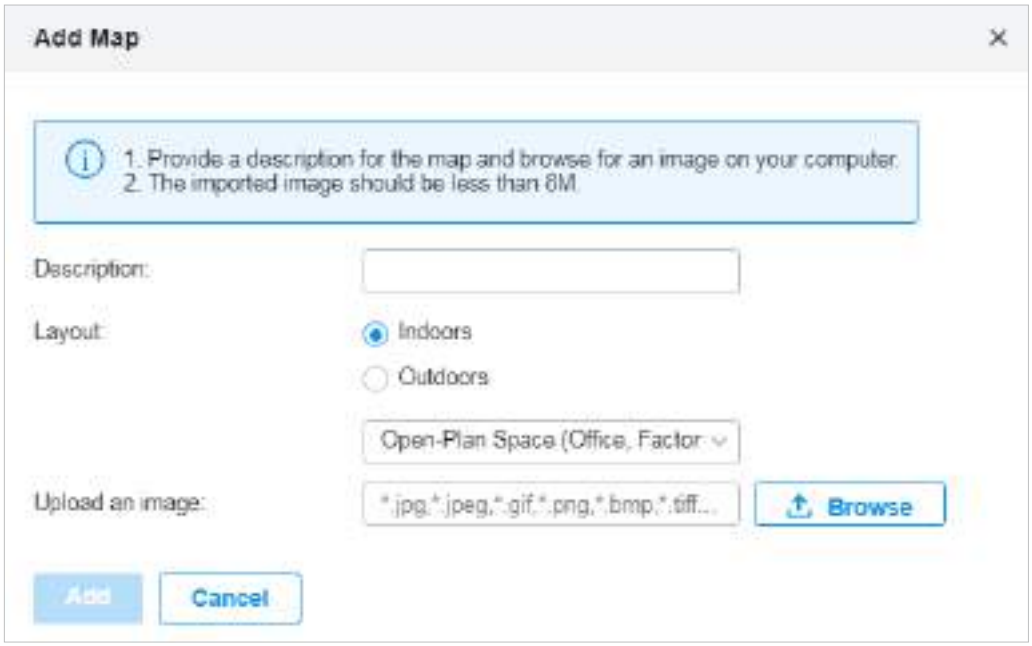
1)Adăugați o hartă și configurați parametrii generali pentru hartă.

2)Adăugați dispozitive și pereți și configurați parametrii.

3)Vedeți rezultatele simulării.

Adăugați o hartă | Adăugați dispozitive și pereți | Vizualizați și exportați rezultatele

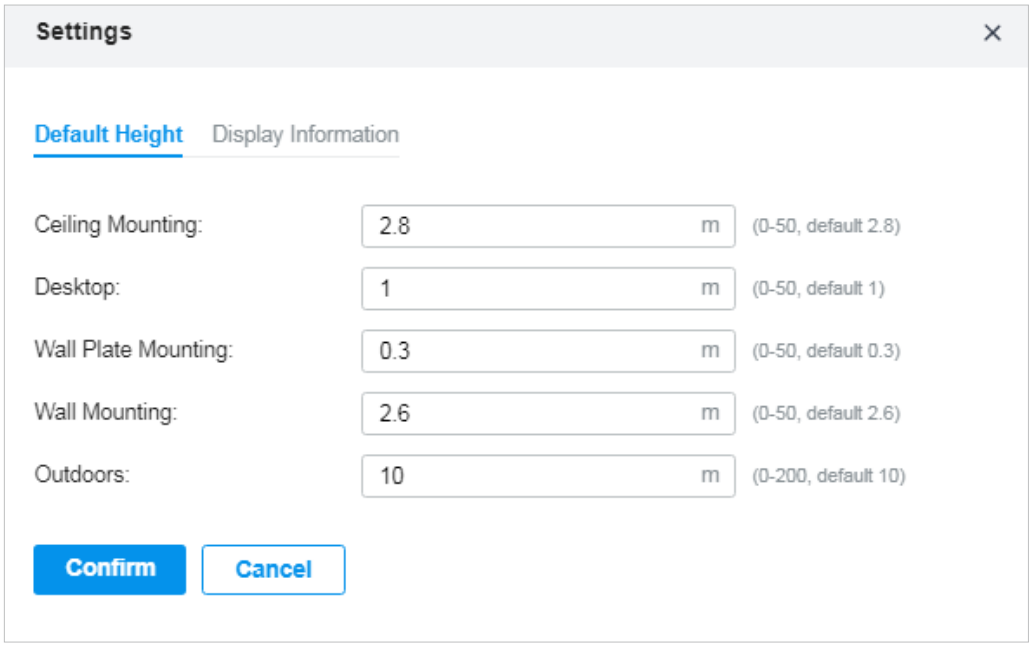
1. AccesațiHartă>Harta termograficași faceți clic pentru a adăuga o nouă hartă. Apoi apasaAdăuga.

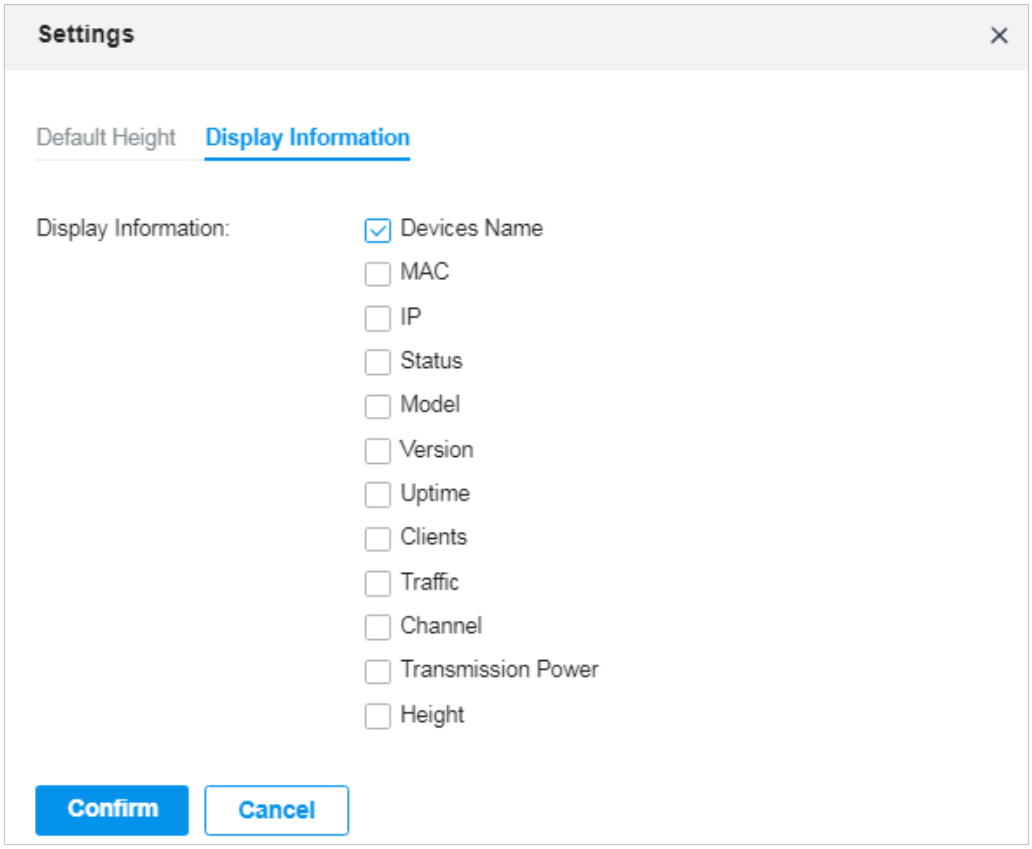


Descriere	Introduceți o descriere pentru hartă.
Aspect	Selectați aspectul general al hărții, ceea ce va face simularea mai precisă.
Încărcați o imagine	Încărcați harta în format .jpg, .jpeg, .gif, .png, .bmp, .tiff, .dxf.

2. Faceți clic 10.73m în dreapta sus pentru a seta o scară a hărții. Desenați o linie pe hartă făcând clic pe și tragerea și apoi definiți distanța liniei.

3. Faceți clic pentru a seta înălțimea implicită a dispozitivelor adăugate și informațiile afișate pe hartă. Apoi apasaA confirma.

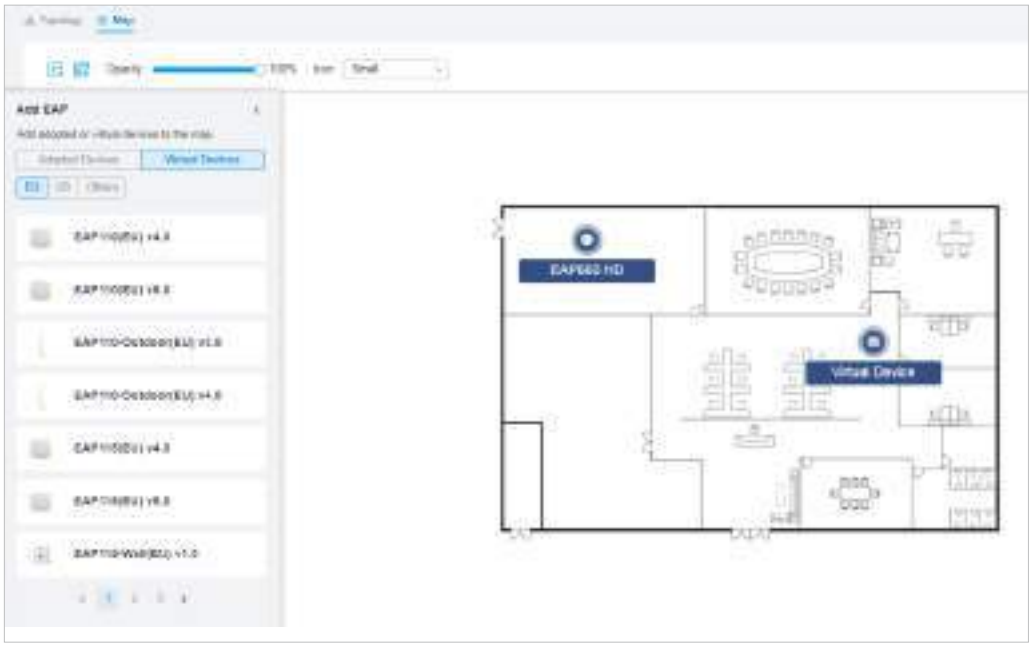




Înălțime implicită	Specificați înălțimea implicită pentru dispozitive. Puteți modifica ulterior înălțimea pentru fiecare dispozitiv.
Afișează informații	Selectați informațiile pe care doriți să le vedeți pe hartă.

Adăugați o hartă | Adăugați dispozitive și pereți | Vizualizați și exportați rezultatele

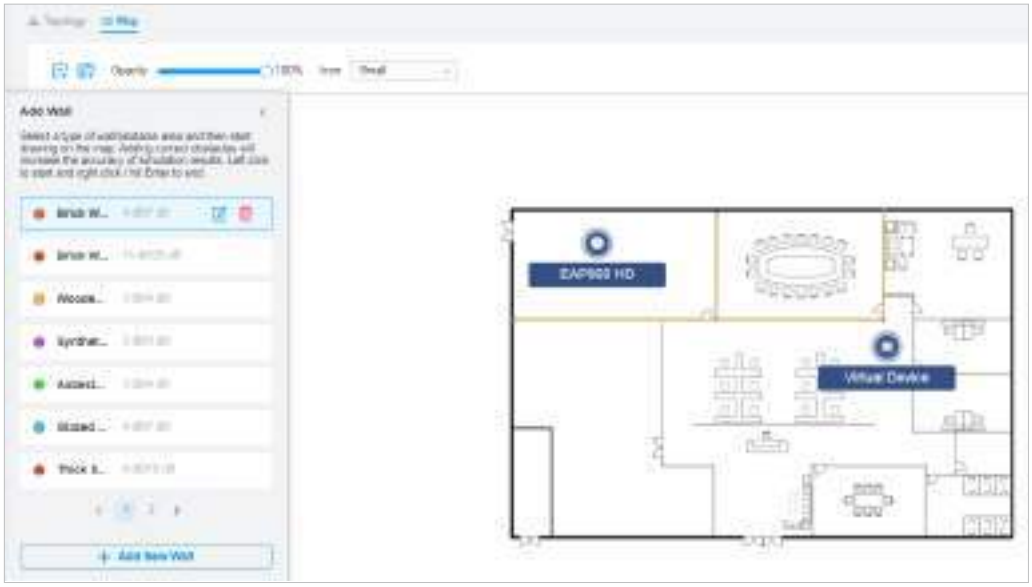
1. Faceți clic Edit pentru a intra în starea de editare a hărții.
2. Faceți clic în stânga sus și va apărea lista dispozitivelor adoptate și a dispozitivelor virtuale. Trageți dispozitive la locul dorit de pe hartă.



3. Faceți clic în stânga sus. Selectați un tip de zonă de perete/obstacol și apoi începeți să desenați pe hartă.

Faceți clic stânga pentru a începe și faceți clic dreapta / apăsați Enter pentru a termina.

De asemenea, puteți edita parametrii detaliați ai pereților și obstacolelor, puteți șterge și adăuga pereți. Adăugarea de obstacole corecte va crește acuratețea rezultatelor simulării.



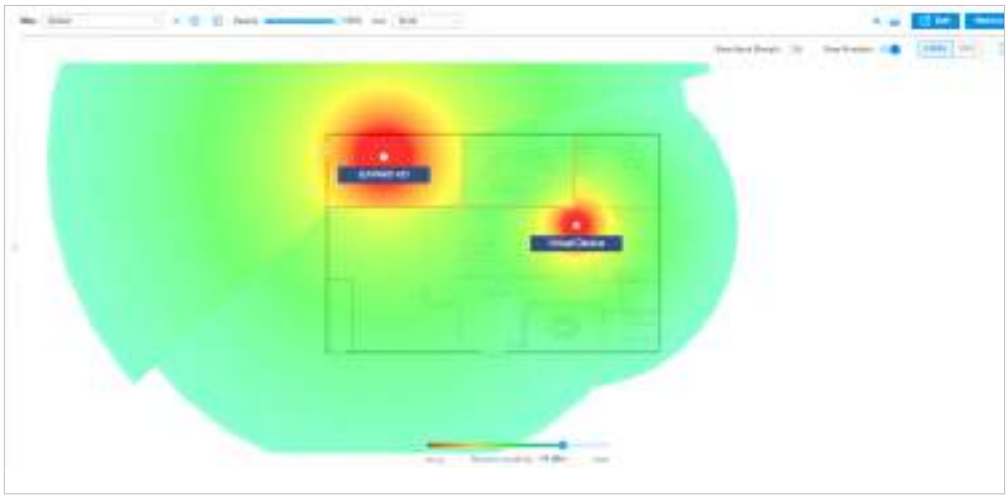
4. Faceți clic Done pentru a ieși din starea de editare a hărții.

Adăugați o hartă > Adăugați dispozitive și pereți > Vizualizați și exportați rezultatele

Notă:

Este necesar să faceți clicSimulapentru a genera o nouă hartă termică după editarea elementelor de pe hartă.

1. Faceți clic Simulate pentru a genera harta termică. Puteți regla sensibilitatea receptorului, puteți afișa puterea semnalului, și vizualizați rezultatele simulării 2,4 GHz/5GHz în funcție de nevoile dvs.



Show Signal Strength:	Activați funcția și puteți muta cursorul pentru a vedea puterea semnalului unei anumite locații.
Show Simulation:	Activați sau dezactivați afișarea rezultatelor simulării pe hartă.
2.4GHz 5GHz	Selectați 2,4 GHz sau 5 GHz pentru a vizualiza rezultatele simulării benzii.
	Faceți clic și urmați instrucțiunile pentru a specifica o zonă pentru a vedea puterea semnalului și procentul corespunzător.
	Reglați sensibilitatea receptorului, iar noile setări vor intra în vigoare după reîmprospătarea simulării.

2. (Opțional) Dacă doriți să exportați un raport de acoperire a rețelei, faceți clic în dreapta sus pentru a exporta un raport în format .docx.

7. 3. 3 Harta dispozitivului

Condiție prealabilă

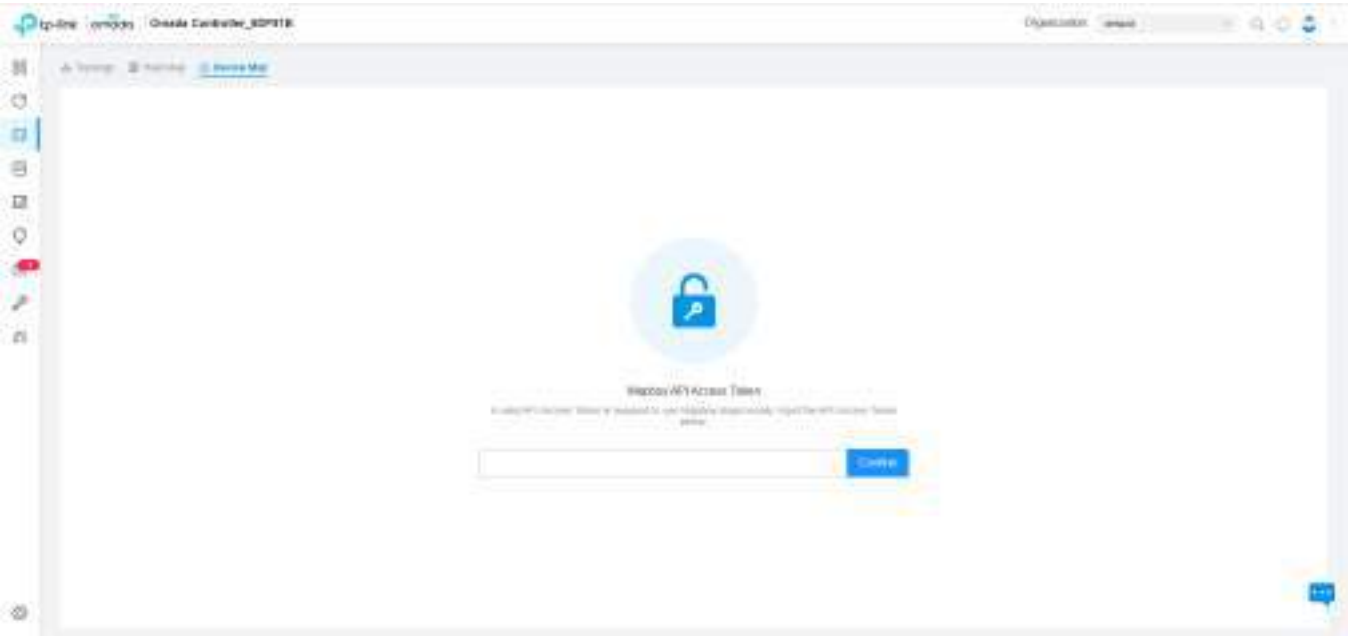
Este necesar un token de acces Mapbox API valid pentru a utiliza funcția Device Map.

Vizitahttps://www.mapbox.com , înregistrați un cont și obțineți simbolul implicit pe pagina contului.

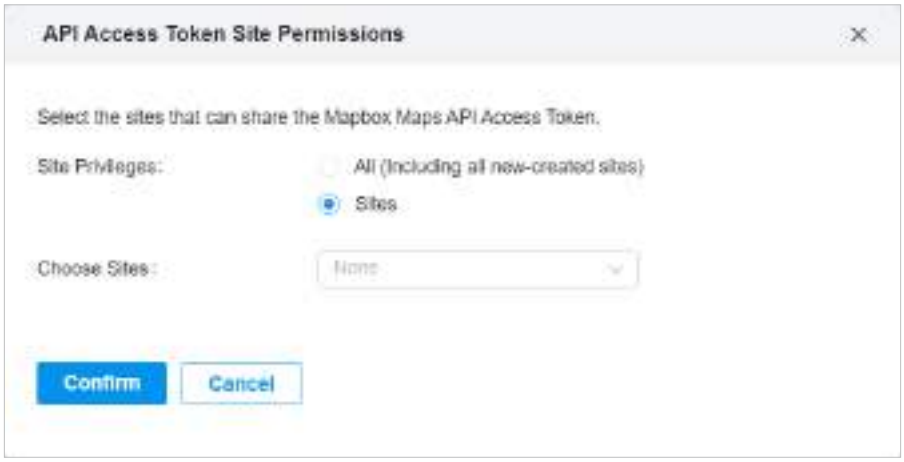
Configurare

1. Selectați un site din lista verticală aOrganizareîn colțul din dreapta sus. Mergi laHartă>Harta dispozitivului .

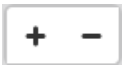
2. Introduceți codul de acces Mapbox API pe care l-ați obținut, apoi faceți clicA confirma.



3. Selectați site-urile care pot partaja simbolul, apoi faceți clicA confirma.



4. Utilizați harta pentru a vă gestiona dispozitivele.

Dispozitiv neplasat Listă	Afișează o listă de site-uri care nu sunt marcate pe hartă. Puteți trage și plasa un site pentru a-l adăuga pe hartă.
Bara de căutare	Selectați o categorie și introduceți cuvântul cheie pentru a căuta un site sau o adresă.
	Localizați în locația curentă.
	Măriți și micșorați harta.

Faceți clic dreapta pe pictograma unui dispozitiv pentru a edita locația sau pentru a o elimina de pe hartă.

Faceți clic pe pictograma unui dispozitiv pentru a vedea informațiile despre dispozitiv și pentru a edita setările.

7. 3. 4 Harta site-ului

Condiție prealabilă

Este necesar un token de acces Mapbox API valid pentru a utiliza funcția Hartă site.

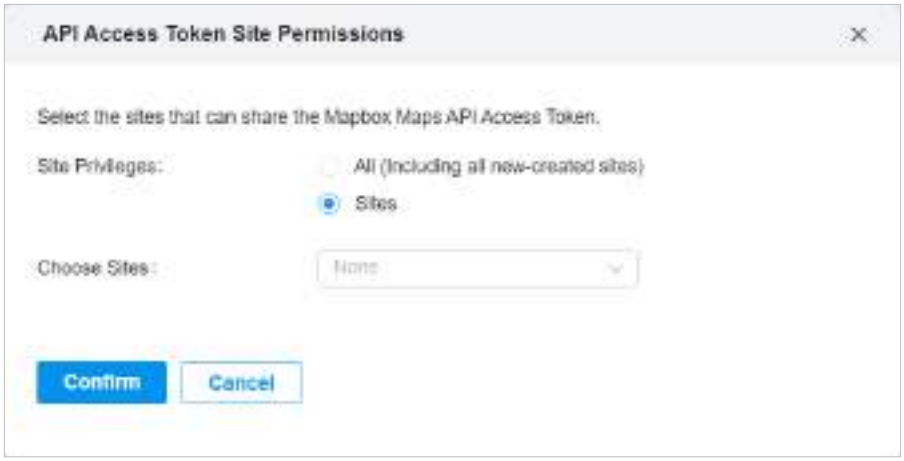
Vizitahttps://www.mapbox.com , înregistrați un cont și obțineți simbolul implicit pe pagina contului.

Configurare

1. SelectațiGlobaldin lista derulantă aOrganizareîn colțul din dreapta sus. Mergi laBord> Harta site-ului .

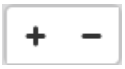
2. Introduceți codul de acces Mapbox API pe care l-ați obținut, apoi faceți clicA confirma.

3. Selectați site-urile care pot partaja simbolul, apoi faceți clicA confirma.



4. Utilizați harta pentru a vă gestiona site-urile.

Lista de site-uri nelocate	Afișează o listă de site-uri care nu sunt marcate pe hartă. Puteți trage și plasa un site pentru a-l adăuga pe hartă.
Bara de căutare	Selectați o categorie și introduceți cuvântul cheie pentru a căuta un site sau o adresă.

	Localizați în locația curentă.
	Măriți și micșorați harta.

Faceți clic dreapta pe hartă pentru a adăuga un site nou.

Faceți clic dreapta pe pictograma unui site pentru a edita locația sau pentru a o elimina de pe hartă.

Faceți clic pe un site pentru a vedea informații despre site și faceți clic pe Lansare pentru a accesa site-ul.

7. 4 Monitorizați rețeaua cu raport

Network Report arată statisticile diferiților indicatori de rețea și modificările acestora de-a lungul timpului, ajutând administratorii de rețea să înțeleagă în mod intuitiv și cuprinzător starea de funcționare curentă și istorică a rețelei lor. Astfel, facilitează administratorii de rețea să decidă dacă controlerul și dispozitivele trebuie să fie actualizate și optimizate. De asemenea, oferă administratorilor de rețea și SI suport de date pentru raportarea condițiilor rețelei.

Mergi laRaport, și puteți vizualiza datele de conectare ale dispozitivelor din topologie și statisticile diferiților indicatori de rețea și modificările acestora în timp. Faceți clic pe filele din partea de sus pentru a vizualiza statisticile unei anumite secțiuni a rețelei.

rezumat	Afișează rezumatul statisticilor întregii rețele.
Rezumat wireless	Afișați rezumatul statisticilor wireless pentru întreaga rețea, inclusiv datele legate de AP-uri, clienții wireless și traficul wireless.
Rezumat prin cablu	Afișați rezumatul statisticilor cu fir pentru întreaga rețea, inclusiv date legate de gateway, switch-uri, clienți cu fir și trafic prin cablu.
Dispozitive fără fir	Afișați detalii despre AP-urile din rețea, inclusiv traficul AP, utilizarea CPU, utilizarea memoriei, numărul total de clienți, alertele și timpii de repornire.
Dispozitive cu fir	Afișați detalii despre gateway-uri și switch-uri din rețea, inclusiv Trafic, Utilizarea CPU, Utilizarea memoriei, Numărul total de clienți, Alertele și Timpii de repornire.
SSID	Afișați statisticile SSID-urilor din rețea, inclusiv Trafic, Total Clienți și Activități.
Clienții	Afișați statisticile clienților din rețea, inclusiv distribuția, activitățile clienților și numerele clienților.

7. 5 Vizualizați statisticile în timpul perioadei specificate cu Insight

ÎnPerspectivăpagina, puteți monitoriza istoricul site-ului clienților conectați, autorizațiile portalului și AP-urile rouge. Pentru o monitorizare mai bună, puteți specifica perioada de timp și clasifica clienții și AP-urile.

7. 5. 1 Clienți cunoscuți

În Clienți cunoscuți, un tabel listează toți clienții care s-au conectat la rețea înainte pe site.

În tabel, puteți vizualiza informațiile de bază ale clientului, rolul și statisticile de conectare, inclusiv traficul de descărcare și încărcare, durata conexiunii și ultima conectare la rețea.

O bară de căutare, un selector de timp și trei file sunt deasupra tabelului pentru căutare și filtrare.

Search Name or MAC Address	Introduceți numele clientului sau adresa MAC pentru a căuta clienții.
Start date - End date	Filtrați clienții în funcție de Last Seen. Faceți clic pe selector pentru a deschide calendarul. Faceți clic pe o anumită dată de două ori în calendar pentru a afișa înregistrările din ziua respectivă. Pentru a afișa înregistrările unui interval de timp, faceți clic pe data de început și data de încheiere din calendar.

	Faceți clic pe file pentru a filtra clienții enumerați în tabel. Cele trei file pot avea efect simultan.
	Toate/Fără fir/Cablat: Faceți clicToatepentru a afișa atât clienții wireless, cât și clienții cu fir. ClicFără fir sauCablatpentru a afișa numai clienți fără fir sau cu fir.
	Toate/Utilizatori/Vizitatori: Faceți clicToatepentru a afișa atât utilizatorii, cât și oaspeții. ClicUtilizatorisauGusets pentru a afișa numai utilizatori sau oaspeți. Oaspeții sunt utilizatori conectați la rețeaua wireless pentru oaspeți. Pentru a configura rețeaua pentru oaspeți, consultați3. 4 Configurați rețele wireless. Toate/Tarif limitat/Blocat: Faceți clicToatepentru a afișa atât clienții cu tarif limitat, cât și clienții blocați. ClicTarif limitatsauBlocatpentru a afișa doar clienții cu rată limitată sau blocați. Pentru a configura Rate Limit, consultați3. 8. 3 Rate Limită. Pentru a bloca clienții, faceți clic pe pictograma din tabel.

De asemenea, puteți lua măsuri pentru a bloca sau uita clientul. Pentru monitorizare și management detaliat, faceți clic pe intrarea din tabel pentru a deschide fereastra Proprietăți a clientului. Pentru mai multe detalii, consultați6. 1. 2 Utilizarea tabelului Clienți pentru a monitoriza și gestiona clienții .

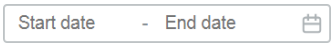
	(Pentru clienții deblocați) Faceți clic pentru a bloca clientul în site. Odată blocat, clientului i se interzice conectarea la rețeaua din site.
	(Pentru clienții blocați) Faceți clic pentru a debloca clientul în site.
	Faceți clic pentru a uita clientul. Odată uitat, toate statisticile și istoricul clientului de pe site sunt eliminate.

7. 5. 2 Conexiuni trecute

În Conexiuni anterioare, un tabel afișează informații despre sesiunile anterioare de conexiune client.

În tabel, puteți vizualiza numele clientului, adresa MAC, timpul și durata asocierii, descărcarea și încărcarea traficului, adresa IP și rețeaua/portul la care s-a conectat.

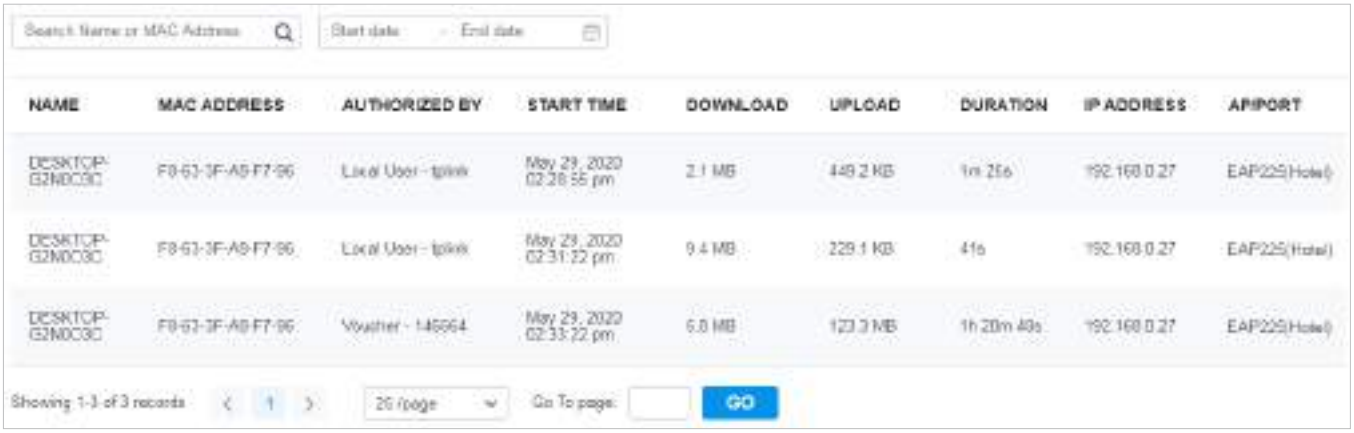
O bară de căutare și un selector de timp sunt deasupra tabelului pentru căutare și filtrare.

	Introduceți numele clientului, SSID sau adresa MAC pentru a căuta clienții.
	Filtrați clienții în funcție de Ora de începere. Faceți clic pe selector pentru a deschide calendarul. Faceți clic pe o anumită dată de două ori în calendar pentru a afișa sesiunile de conectare la client în ziua respectivă. Pentru a afișa sesiunile de conectare la client într-un interval de timp, faceți clic pe data de început și data de încheiere din calendar.

7. 5. 3 Autorizări anterioare ale portalului

În Autorizările anterioare ale portalului, un tabel listează toți clienții care au trecut anterior autorizarea portalului.

În tabel, puteți vedea numele clientului, adresa MAC, acreditările de autorizare, traficul uplink și downlink, timpul și durata autorizației, adresa IP și rețeaua/portul la care s-a conectat. Pentru monitorizare și management detaliat, consultați6. 2 Gestionați autentificarea clientului în Hotspot Manager .



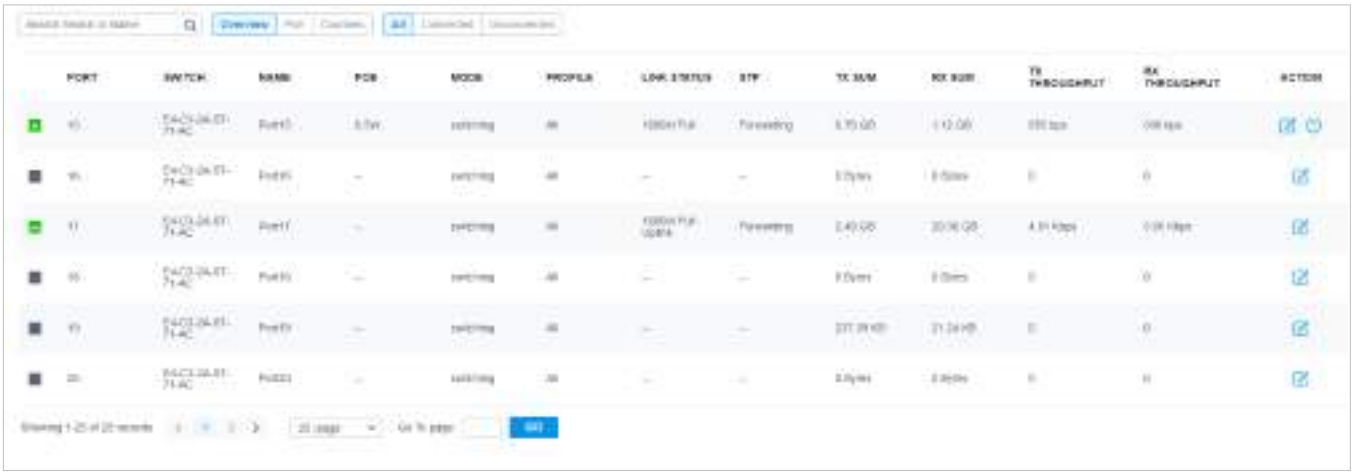
O bară de căutare și un selector de timp sunt deasupra tabelului pentru căutare și filtrare.

Search Name or MAC Address	Introduceți numele clientului sau adresa MAC pentru a căuta clienții.
Start date - End date	Filtrați clienții în funcție de Ora de începere. Faceți clic pe selector pentru a deschide calendarul. Faceți clic pe o anumită dată de două ori în calendar pentru a afișa clienții autorizați în ziua respectivă. Pentru a afișa clienții autorizați într-un interval de timp, faceți clic pe data de început și data de încheiere din calendar.

7. 5. 4 Comutare stare

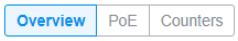
În Stare comutatoare, un tabel afișează informații despre starea comutatoarelor gestionate de controler.

În tabel, puteți vedea porturile, starea PoE, modul și activitatea de trafic a comutatoarelor.



O bară de căutare și două file sunt deasupra tabelului pentru căutare și filtrare. De asemenea, puteți face clic pe pictogramele din coloana Acțiune pentru o operare rapidă.

Search Switch or Name	Introduceți comutatorul sau numele pentru a căuta.

	Faceți clic pe file pentru a filtra porturile de comutare enumerate în tabel. Cele două file pot avea efect simultan.
	Prezentare generală/PoE/Contoare: Faceți clicPrezentare generalăpentru a afișa starea generală a fiecărui port. ClicPoEpentru a afișa configurațiile PoE și starea fiecărui port. ClicContoare pentru a afișa ratele TX și RX pentru fiecare port. Toate/Conectat/Deconectat: filtrează porturile după starea conexiunii. ClicToatepentru a afișa informații despre toate porturile. ClicConectatsauDeconectatpentru a afișa toate porturile conectate sau deconectate.
	Faceți clic pentru a edita configurațiile portului.
	(Numai pentru portul PoE care este conectat la un PD) Faceți clic pe butonul și portul se va opri pentru a furniza curent PD-ului conectat pentru a reporni PD-ul.

Informațiile listate atunci când selectațiPrezentare generalăpe prima filă este explicat după cum urmează.

Port	Afișați numărul și starea portului. 10/100 Mbps:Portul rulează la 10/100 Mbps. 1000 Mbps:Portul rulează la 1000 Mbps. 2,5 Gbps:Portul rulează la 2,5 Gbps. 10 Gbps:Portul rulează la 10 Gbps. Dezactivat:Portul este dezactivat. Deconectat:Portul este activat, dar nu se conectează la niciun dispozitiv sau client. PoE:Portul PoE este conectat la un dispozitiv alimentat (PD). Uplink:Portul este un port uplink conectat la WAN. Oglindire:Portul este un port de oglindire care reflectă un alt port de comutare. Blocare STP:Portul este în starea Blocare în Spanning Tree. Acesta primește și trimite pachete BPDU (Bridge Protocal Data Unit) pentru a menține arborele de acoperire. Alte pachete sunt aruncate.
Intrerupator	Afișați adresa MAC sau aliasul comutatorului.
Nume	Afișează numele portului.
PoE	Afișează starea PoE a portului. - - :PoE este dezactivat _W:Afișați puterea de ieșire a portului în wați.

Modul	Afișează modul de funcționare al portului. Comutare:Modul implicit. Oglindire:Traficul de rețea al acestui port va primi traficul în oglindă de la portul în oglindă. Agregare:Portul este o parte a unei legături agregate
Profil	Afișați profilul portului de comutare care are efect asupra portului.
Stare link	Afișați viteza conexiunii și modul duplex al portului.
STP	Afișați modul Spanning Tree Protocol (STP).
Suma TX	Afișează cantitatea de date transmise.
Suma RX	Afișează cantitatea de date primite.
Debitul TX	Afișează rata de transmisie.
Debitul RX	Afișați rata de transfer de recepție.

Informațiile listate atunci când selectațiPoEpe prima filă este explicat după cum urmează.

Port	Afișați numărul și starea portului. 10/100 Mbps:Portul rulează la 10/100 Mbps. 1000 Mbps:Portul rulează la 1000 Mbps. 2,5 Gbps:Portul rulează la 2,5 Gbps. 10 Gbps:Portul rulează la 10 Gbps. Dezactivat:Portul este dezactivat. Deconectat:Portul este activat, dar nu se conectează la niciun dispozitiv sau client. PoE:Portul PoE este conectat la un dispozitiv alimentat (PD). Uplink:Portul este un port uplink conectat la WAN. Oglindire:Portul este un port de oglindire care reflectă un alt port de comutare. Blocare STP:Portul este în starea Blocare în Spanning Tree. Acesta primește și trimite pachete BPDU (Bridge Protocal Data Unit) pentru a menține arborele de acoperire. Alte pachete sunt aruncate.
Intrerupator	Afișați adresa MAC sau aliasul comutatorului.
Nume	Afișează numele portului.

PoE	Afișează starea PoE a portului. - - :PoE este dezactivat. _W:Afișați puterea de ieșire a portului în wați.
Clasa PD	Afișați necesarul de energie al PD conectat la portul PoE.
Putere	Afișați puterea de ieșire a portului în wați.
Voltaj	Afișează tensiunea de ieșire în volți.
Actual	Afișează ieșirea curentă în amperi.

Informațiile listate atunci când selectațiContoarepe prima filă este explicat după cum urmează.

Port	Afișați numărul și starea portului. 10/100 Mbps:Portul rulează la 10/100 Mbps. 1000 Mbps:Portul rulează la 1000 Mbps. 2,5 Gbps:Portul rulează la 2,5 Gbps. 10 Gbps:Portul rulează la 10 Gbps. Dezactivat:Portul este dezactivat. Deconectat:Portul este activat, dar nu se conectează la niciun dispozitiv sau client. PoE:Portul PoE este conectat la un dispozitiv alimentat (PD). Uplink:Portul este un port uplink conectat la WAN. Oglindire:Portul este un port de oglindire care reflectă un alt port de comutare. Blocare STP:Portul este în starea Blocare în Spanning Tree. Acesta primește și trimite pachete BPDU (Bridge Protocal Data Unit) pentru a menține arborele de acoperire. Alte pachete sunt aruncate.
Intrerupator	Afișați adresa MAC sau aliasul comutatorului.
TX octeți	Afișează numărul de octeți transmisi.
Cadre TX	Afișează numărul de cadre transmise.
TX Multicast	Afișează numărul de pachete multicast transmise.
Difuzare TX	Afișează numărul de pachete transmise de difuzare.
Erori TX	Afișează numărul de pachete de eroare transmise.
Octeți RX	Afișează numărul de octeți primiți.
Cadre RX	Afișează numărul de cadre primite.

RX Multicast	Afișează numărul de pachete multicast primite.
Difuzare RX	Afișează numărul de pachete de difuzare primite.
Erori RX	Afișează numărul de pachete de eroare primite.

7. 5. 5 Stare redirecționare port

În Port Forwarding Status, un tabel afișează informații despre intrările de port forwarding utilizate de gateway-ul gestionat de controler.

O filă este deasupra tabelului pentru filtrare. De asemenea, puteți face clic pe pictogramele din coloana Acțiune pentru o operare rapidă.

User Defined UPnP	Faceți clic pe fila pentru a filtra intrările de redirecționare porturi enumerate în tabel. Definit de utilizator/UPnP: Faceți clicDefinit de utilizatorpentru a afișa intrările de redirecționare porturi create de utilizator. ClicUPnPpentru a afișa intrările de redirecționare a portului UPnP.
	Faceți clic pentru a edita configurațiile intrării de redirecționare a portului.

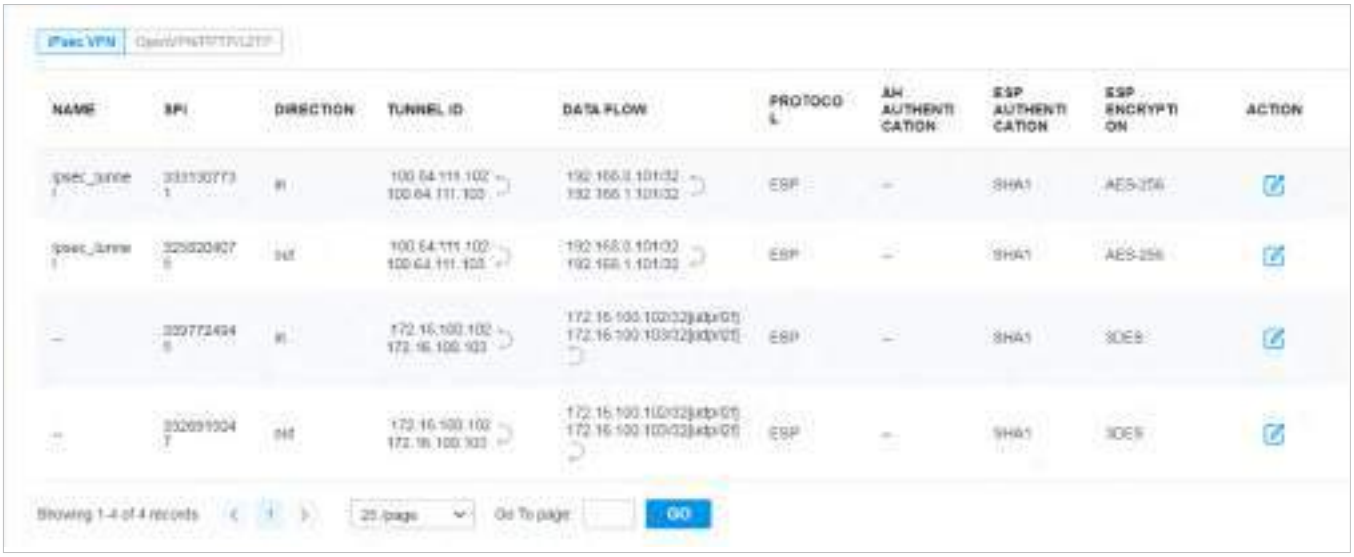
Informațiile enumerate sunt explicate după cum urmează.

Nume	Afișați numele intrării de redirecționare a portului.
Interfață	Afișați rețelele WAN utilizate de intrarea de redirecționare a portului.
IP sursă	(Numai pentru intrările definite de utilizator) Afișează adresa IP sursă. O anumită adresă IP/Mască:Adresa IP sursă specificată. 0.0.0.0/0:Toate adresele IP sunt setate ca adresă IP sursă.
Port sursă	Traficul prin portul sursă, cunoscut și ca port intern, va fi redirecționat către LAN.
IP de destinație	Afișați adresa IP de destinație și va primi traficul portului redirecționat.
Portul de destinație	Afișați portul de destinație, cunoscut și ca port intern, care va primi traficul redirecționat.
Protocol	Afișați protocolul care va fi redirecționat.

Pachete	Afișează numărul de pachete transferate.
octeți	Afișează numărul de octeți transferați.
Durata de închiriere	(Numai pentru redirecționarea portului UPnP) Afișează timpul de funcționare al intrării de redirecționare a portului.

7. 5. 6 Stare VPN

În Stare VPN, un tabel afișează tunelurile VPN existente și informațiile corespunzătoare.



O filă este deasupra tabelului pentru filtrare. De asemenea, puteți face clic pe pictograme pentru o operare rapidă.

IPsec VPN OpenVPN/PPTP/L2TP	Faceți clic pe fila pentru a filtra informațiile de rutare listate în tabel. Când selectați OpenVPN/PPTP/L2TP, puteți alege în continuare Server sau Client.
	(Numai pentru OpenVPN/PPTP/L2TP) Filtrați intrările.
	Faceți clic pentru a configura intrarea.
	(Numai pentru OpenVPN/PPTP/L2TP) Faceți clic pentru a încheia tunelul VPN.
	(Numai pentru OpenVPN/PPTP/L2TP) Faceți clic pentru a alege mai multe informații listate care vor fi afișate în tabel.

Informațiile listate din tabelul IPsec VPN sunt explicate după cum urmează.

Nume	Afișați numele intrării VPN IPsec.
SPI	Afișați indexul parametrilor de securitate.
Direcţie	Afișați direcția procesului VPN IPsec.

ID-ul tunelului	Afișați adresa/numele IP local și la distanță. Săgeata indică sensul de circulație.
Flux de date	Afișează subrețeaua locală și la distanță. Săgeata indică direcția.
Protocol	Afișează protocolul de autentificare și criptare al intrării.
Autentificare AH	Afișează algoritmii de sumă de control ai intrării.
Autentificare ESP	Afișați algoritmii pentru autentificarea ESP.
Criptare ESP	Afișați algoritmii pentru criptarea ESP.

Informațiile listate din tabelul OpenVPN/PPTP/L2TP (Server) sunt explicate după cum urmează (unele informații enumerate mai jos sunt ascunse în mod implicit). Puteți filtra în continuare intrările în funcție de tipul lor.

Utilizator	Afișați numele de utilizator al utilizatorului de la distanță.
Interfață	Afișează interfața prin care trece traficul.
Tip	Afișați tipul de conexiune.
IP local	Afișați adresa IP locală a tunelului VPN.
IP local la distanță	Afișați adresa IP a utilizatorului de la distanță al tunelului VPN.
DNS	Afișați adresa DNS a tunelului VPN.
Descărcați Pkts	Afișați cantitatea de date descărcate ca pachete.
Descărcați octeți	Afișați cantitatea de date descărcate ca octeți.
Încărcați Pkts	Afișează cantitatea de date încărcate ca octeți.
Încărcați octeți	Afișează cantitatea de date încărcate ca octeți.

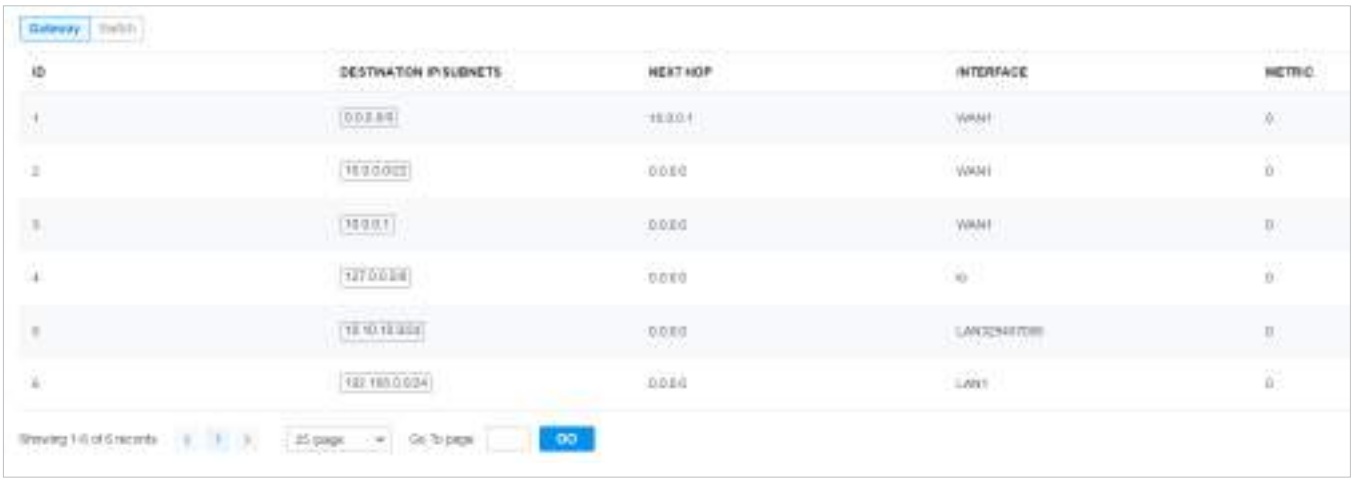
Timp de funcționare	Afișați durata de timp în care tunelul VPN a fost activ.

Informațiile listate din tabelul OpenVPN/PPTP/L2TP (Client) sunt explicate după cum urmează (unele informații enumerate mai jos sunt ascunse în mod implicit). Puteți filtra în continuare intrările în funcție de tipul lor.

Interfață	Afișează interfața prin care trece traficul.
Tunel	Afișați numele clientului VPN.
Tip	Afișați tipul de conexiune.
IP local la distanță	Afișați adresa IP a utilizatorului de la distanță al tunelului VPN.
DNS	Afișați adresa DNS a tunelului VPN.
Descărcați Pkts	Afișați cantitatea de date descărcate ca pachete.
Descărcați octeți	Afișați cantitatea de date descărcate ca octeți.
Încărcați Pkts	Afișează cantitatea de date încărcate ca octeți.
Încărcați octeți	Afișează cantitatea de date încărcate ca octeți.
Timp de funcționare	Afișați durata de timp în care tunelul VPN a fost activ.

7. 5. 7 Tabel de rutare

Tabel de rutare afișează informații despre intrările de rutare care au intrat în vigoare.



O filă este deasupra tabelului pentru filtrare. De asemenea, puteți face clic pe pictogramele din coloana Acțiune pentru o operare rapidă.

Gateway Switch	Faceți clic pe fila pentru a filtra informațiile de rutare listate în tabel. Poarta de acces/Intrerupator: Faceți clic pentru a afișa informațiile de rutare ale gateway-ului sau ale comutatorului.
	(Numai pentru comutare) Faceți clic pentru a configura rutele statice.

Informațiile enumerate sunt explicate după cum urmează.

IP/Subrețele de destinație	Afișați adresele IP de destinație ale intrării de rutare.
Următorul pas	Afișați adresa IP a următorului hop.
Interfață	(Numai pentru Gateway) Afișează interfața prin care trece traficul intrării.
Metric	(Numai pentru Gateway) Afișați numărul de hop înainte de a ajunge la destinație. În general, dacă există câteva intrări de rutare cu aceeași destinație, va fi folosită rutarea cu cea mai mică valoare.
Distanţă	(Numai pentru Switch) Afișează distanța administrativă a intrării de rutare. Este folosit pentru a decide prioritatea dintre rutele către aceeași destinație. Dintre rutele către aceeași destinație, se va utiliza traseul cu cea mai mică valoare a distanței.

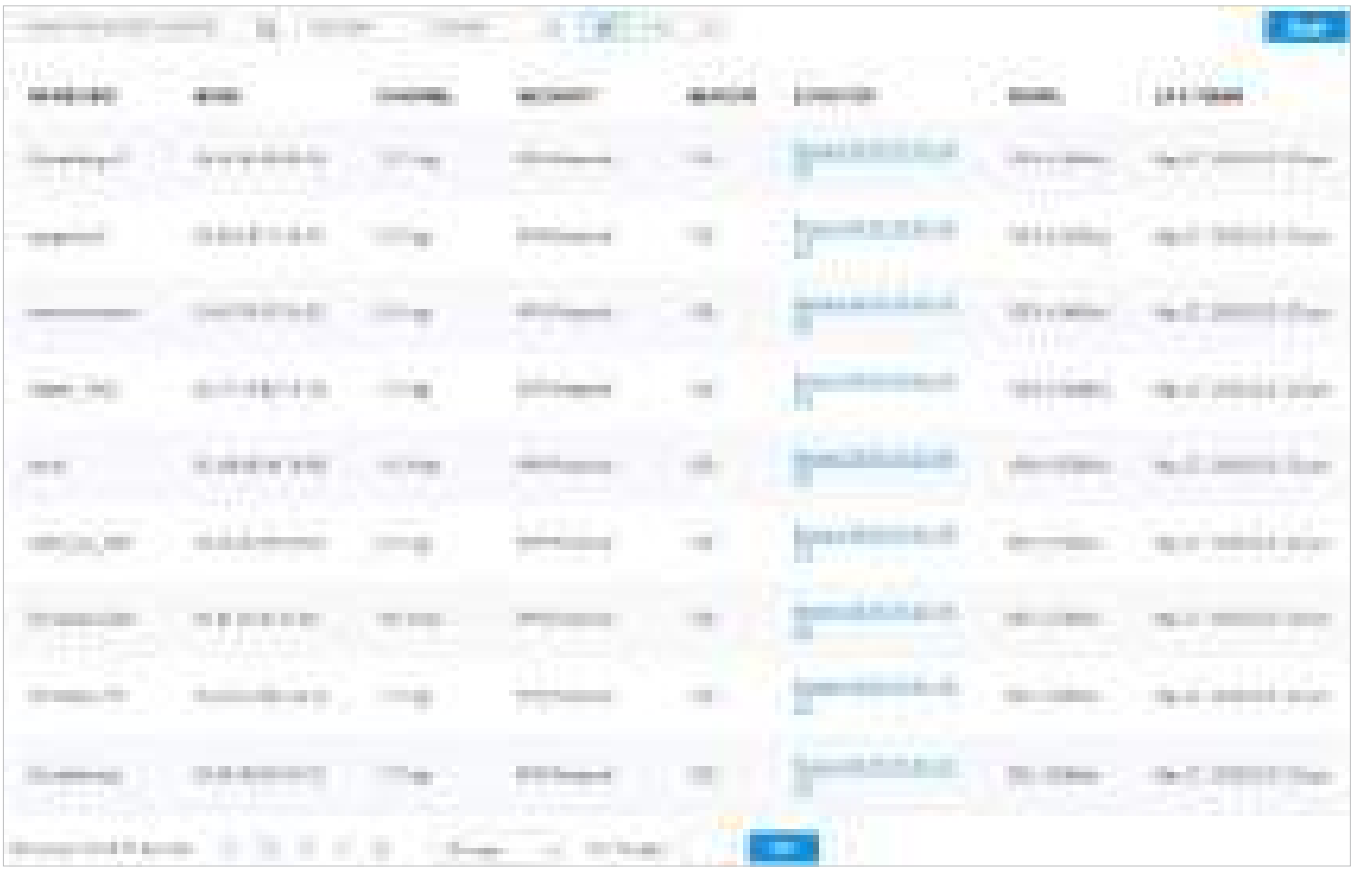
7. 5. 8 DNS dinamic

În DNS dinamic, un tabel afișează informații despre utilizările serviciilor DNS dinamice. Puteți face clic în coloana Acțiune pentru a edita intrarea.

Serviciu	Afișează numele serviciului DDNS.
Interfață	Afișați rețelele WAN utilizate de intrarea DDNS.
stare	Afișează starea celei mai recente actualizări DDNS.
Nume de utilizator	Afișați numele de utilizator al contului DDNS.
Numele domeniului	Afișează numele de domeniu înregistrat cu serviciul DDNS.
IP	Afișați adresa IP a numelui de domeniu.
Ultima actualizare	Afișați ora la care adresa IP a numelui de domeniu a fost actualizată ultima dată.

7. 5. 9 AP-uri necinstiți

Un AP necinstit este un punct de acces care a fost instalat într-o rețea securizată fără autorizarea explicită a unui administrator de sistem. În Rogue AP-uri, puteți scana AP-uri necinstiți și puteți vizualiza AP-urile necinstite scanate anterior.



Search Name or MAC Address	Introduceți numele clientului sau adresa MAC pentru a căuta clienții.
Start date - End date	Filtrați AP-urile necinstite în funcție de Last Seen. Faceți clic pe selector pentru a deschide calendarul. Faceți clic pe o anumită dată de două ori în calendar pentru a afișa AP-urile necinstite scanate în acea zi. Pentru a afișa AP-ul scanat într-un interval de timp, faceți clic pe data de început și data de încheiere din calendar.
All 2.4G 5G	Faceți clic pe fila pentru a filtra AP-urile necinstite enumerate în tabel pe baza benzii de frecvență.
Scan	Faceți clic pentru a scana AP-uri necinstite. Poate dura câteva minute, iar serviciul wireless poate fi influențat în timpul scanării.
BSSID	Un șir cu o formă similară cu adresa MAC pentru a recunoaște punctele de acces.
Canal	Afișează canalul de operare și standardul AP-ului necinstiți.
Securitate	Afișează strategia de securitate a AP necinstiți.
Far	Afișează intervalul de semnalizare al AP necinstiți. Beacon-urile sunt transmise periodic de către EAP pentru a anunța prezența unei rețele wireless pentru clienți, iar intervalul înseamnă cât de des AP trimite un beacon către clienți.
Locație	Afișează AP-ul gestionat cel mai apropiat de AP necinstit. Puteți face clic pe cel mai apropiat AP pentru a deschide fereastra de Proprietăți.

Semnal	Afișează puterea semnalului în procente și dBm.
Vazut ultima data	Afișați ultima dată când AP-ul necinstiți a fost scanat de controler.

7. 6 Vizualizați și gestionați jurnalele

Controlerul folosește jurnalele pentru a înregistra activitățile sistemului, dispozitivelor, utilizatorilor și administratorilor, ceea ce oferă suporturi puternice pentru monitorizarea operațiunilor și diagnosticarea anomaliilor. Pe pagina Jurnal, puteți monitoriza în mod convenabil conectările7. 6. 1 Alerte și7. 6. 2 Evenimente și configurați nivelurile de notificare în 7. 6. 3 Notificări .

Toate jurnalele pot fi clasificate după următoarele patru aspecte.

- Ierarhii apărute

  Două categorii în ierarhiile apărute sunt Controller și Site, care indică activitățile de jurnal care au avut loc, respectiv, la nivelul controlorului și, respectiv, pe un anumit site. Numai Administratorii Maeștri pot vedea jurnalele care au avut loc la nivel de controler.

- Notificări

  Două categorii în notificări sunt Evenimente și Alertă și puteți clasifica jurnalele în ele singur.

- Severități

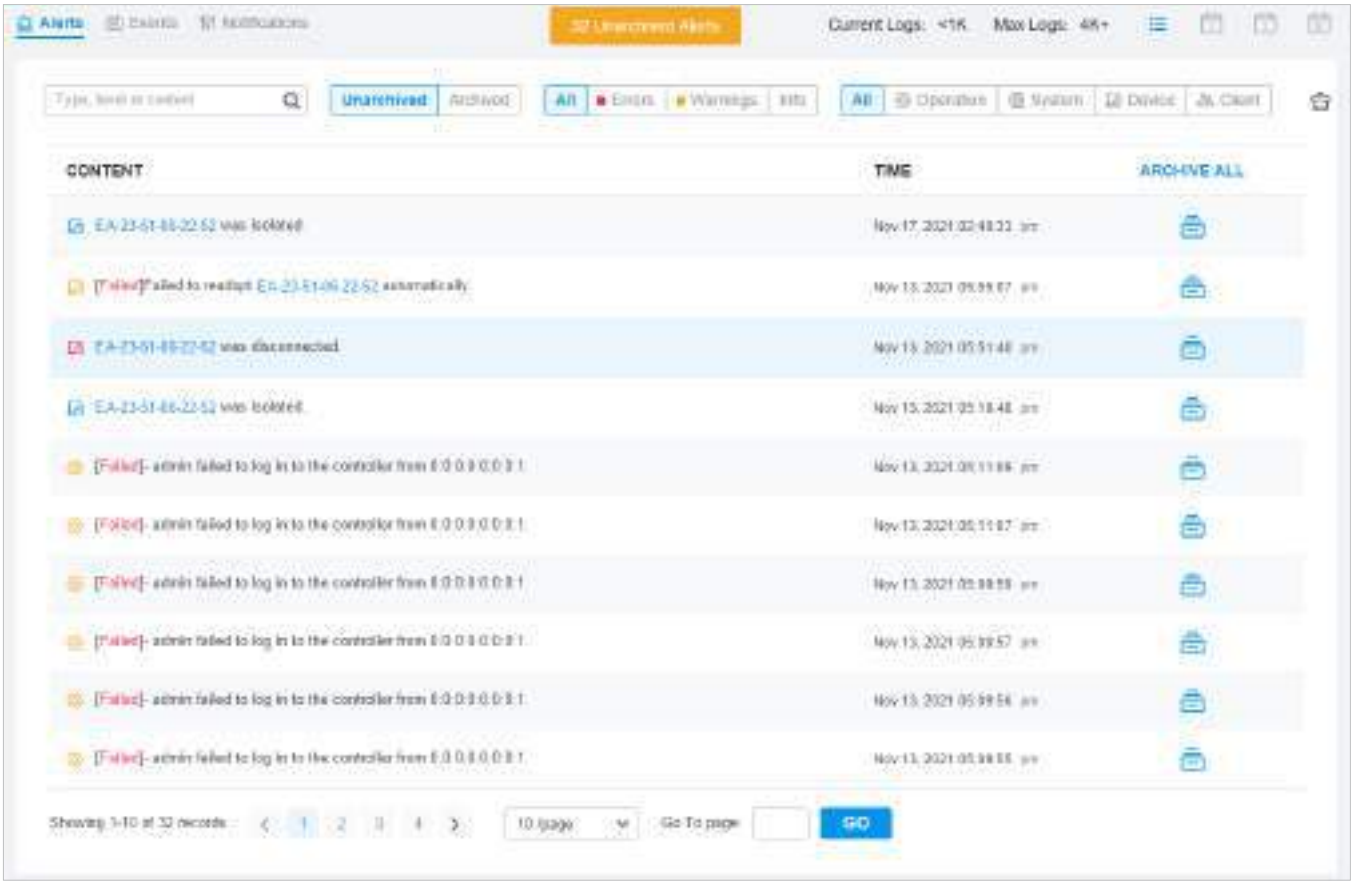
  Trei niveluri de severitate sunt Eroare, Avertizare și Informații, ale căror influențe sunt clasificate de la mare la scăzut.

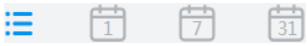
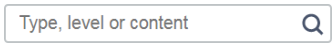
- Cuprins

  Patru tipuri de conținut sunt Operație, Sistem, Dispozitiv și Client, care indică conținutul jurnalului referitor la.

7. 6. 1 Alerte

Alertele sunt jurnalele care trebuie observate și arhivate special. Puteți configura jurnalele ca Alerte în Notificări, iar toate jurnalele configurate ca Alerte sunt listate în fila Alerte pentru a le căuta, filtra și arhiva.

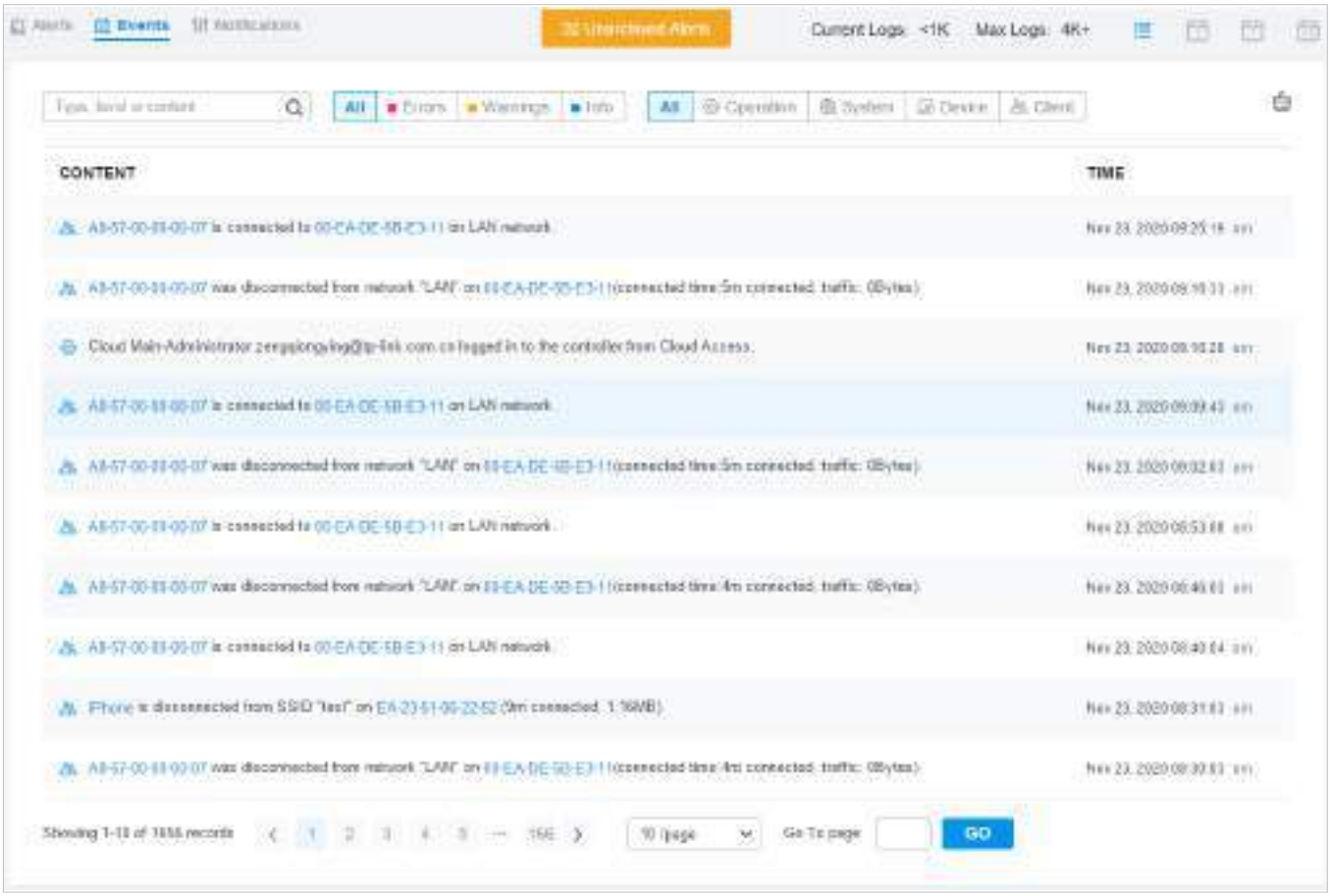


	Faceți clic pentru a schimba modul de vizualizare pentru o imagine de ansamblu mai bună. : Afișează jurnalele într-un tabel. / / : Afișează jurnalele într-o zi/săptămână/lună. Pentru a schimba ora, faceți clic pe sau . La sari înapoi la cea actuală, dă clicAstăzi/În această săptămână/Luna aceasta.
	Introduceți tipurile de conținut, nivelurile de severitate sau cuvintele cheie pentru a căuta în jurnalele.
	Faceți clic pe file pentru a filtra jurnalele listate în tabel. Cele două file pot avea efect simultan.
	Dezarhivat/Arhivat: faceți clic pe fila pentru a filtra jurnalele nearhivate și arhivate. Puteți da clic și Arhiveaza-pe toatepentru a arhiva un singur jurnal și, respectiv, toate. Toate/Erori/Avertizări: Faceți clicToatepentru a afișa jurnalele atât la nivelurile de eroare, de avertizare, cât și de informații. ClicErorisauAvertizăripentru a afișa jurnalele numai la nivelurile de eroare sau de avertizare.
Conținut	Afișează tipurile de jurnal și mesajul detaliat. Puteți face clic pe numele dispozitivului, numele clientului pentru a deschide fereastra Proprietăți pentru informații detaliate.
Timp	Afișează când a avut loc activitatea.

Arhiveaza-le pe toate	Faceți clic pentru a arhiva toate jurnalele dezarhivate.
	Faceți clic pentru a arhiva intrarea în jurnal.
	Faceți clic și selectați tipurile de jurnal pentru a șterge jurnalele de alertă corespunzătoare. Odată șterse, alertele arhivate nu pot fi recuperate. Alertele dezarhivate nu pot fi șterse.

7. 6. 2 Evenimente

Evenimentele sunt jurnalele care pot fi vizualizate, dar nu au notificări. Puteți configura jurnalele ca Evenimente în Notificări, iar toate jurnalele configurate ca Evenimente sunt listate în fila Evenimente pentru a le căuta și filtra.

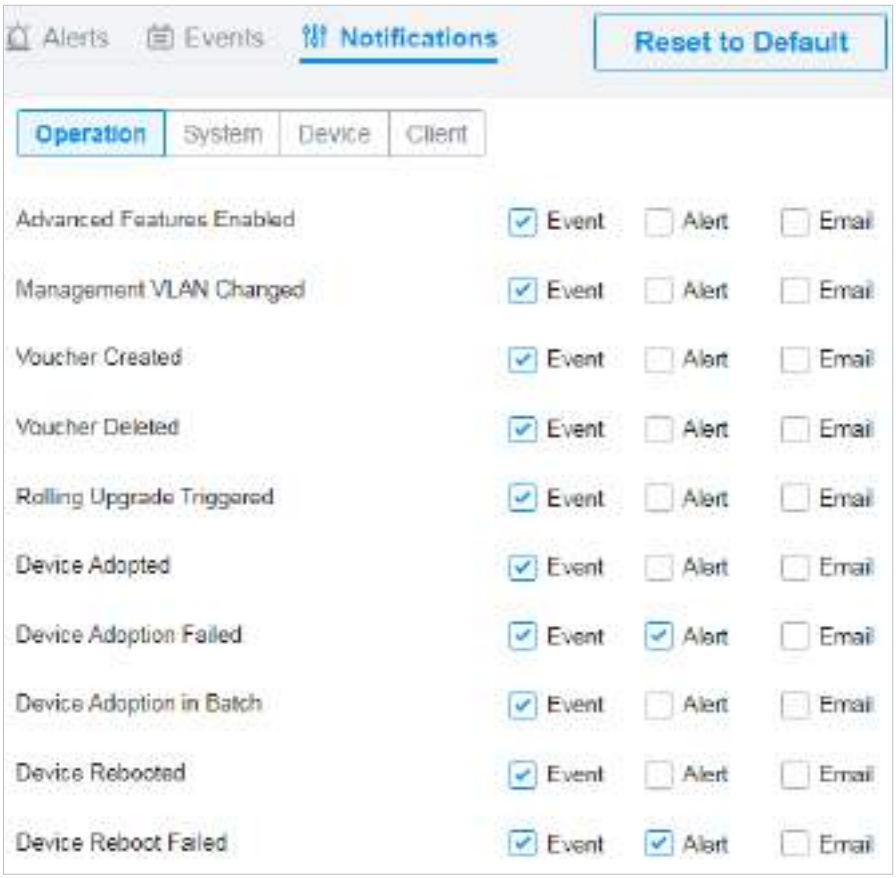


	Faceți clic pentru a schimba modul de vizualizare. : Afișează jurnalele într-un tabel. / / : Afișează jurnalele într-o zi/săptămână/lună. Pentru a schimba ora, faceți clic sau . Pentru a reveni la cea actuală, faceți clicAstăzi/În această săptămână/Luna aceasta.
Type, level or content	Introduceți tipurile de conținut, nivelurile de severitate sau cuvintele cheie pentru a căuta în jurnalele.
	Faceți clic și selectați tipurile de jurnal pentru a șterge jurnalele de evenimente corespunzătoare.

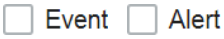
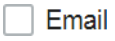
 	Faceți clic pe file pentru a filtra jurnalele listate în tabel. Cele două file pot avea efect simultan. Toate/Erori/Avertizări/Info: Faceți clicToatepentru a afișa jurnalele atât la nivel de eroare, cât și la nivel de avertizare. ClicErori,AvertizărisauInfopentru a afișa jurnalele numai la nivelul corespunzător. Toate/Operațiune/Sistem/Dispozitiv/Client: Faceți clicToatepentru a afișa toate tipurile de jurnal. Clic OperațiunesauSistemsauDispozitivsauClientpentru a afișa numai tipul corespunzător de jurnal.
Conținut	Afișează tipurile de jurnal și mesajul detaliat. Puteți face clic pe numele dispozitivului, numele clientului pentru a deschide fereastra Proprietăți pentru informații detaliate.
Timp	Afișează când a avut loc activitatea.

7. 6. 3 Notificări

În Notificări, puteți găsi tot felul de jurnale de activitate clasificate după conținut și să specificați categoriile de notificare ale acestora ca Eveniment și Alertă pentru site-ul curent. De asemenea, puteți activa e-mail pentru jurnalele. Cu configurații adecvate, controlerul va trimite e-mail-uri administratorilor atunci când înregistrează jurnalele.



Pentru a specifica jurnalele ca Alertă/Eveniment, faceți clic pe casetele de selectare corespunzătoare ale jurnalelor și faceți clicaplica. Următoarele pictograme și filă sunt furnizate ca auxiliare.

Resetare la valorile implicite	Faceți clic pentru a reseta toate configurațiile de notificări din site-ul curent la valorile implicite.
	Faceți clic pe file pentru a afișa configurațiile tipurilor de jurnal corespunzătoare.
	Activați casetele de selectare pentru a specifica jurnalele de activitate ca Evenimente/Alerte, iar apoi jurnalele înregistrate vor fi afișate în fila Evenimente/Alerte. Dacă ambele sunt dezactivate, controlerul nu va înregistra jurnalele de activitate.
	Activați casetele de selectare pentru a specifica jurnalele de activitate ca jurnale de alerte. Cu setările corespunzătoare în Site și Admin, controlorul poate trimite e-mailuri pentru a notifica administratorii și spectatorii despre jurnalele de alertă ale site-ului odată generate.
	Această pictogramă apare atunci când configurația unui jurnal este modificată, dar nu a fost aplicată. Faceți clic pe acesta pentru a reseta configurația jurnalului la valoarea implicită.

Casetele de selectare E-mail sunt folosite pentru a activa e-mailurile de alertă pentru jurnalele. Pentru a vă asigura că administratorii și spectatorii pot primi e-mailuri de alertă ale site-ului, urmați următorii pași:

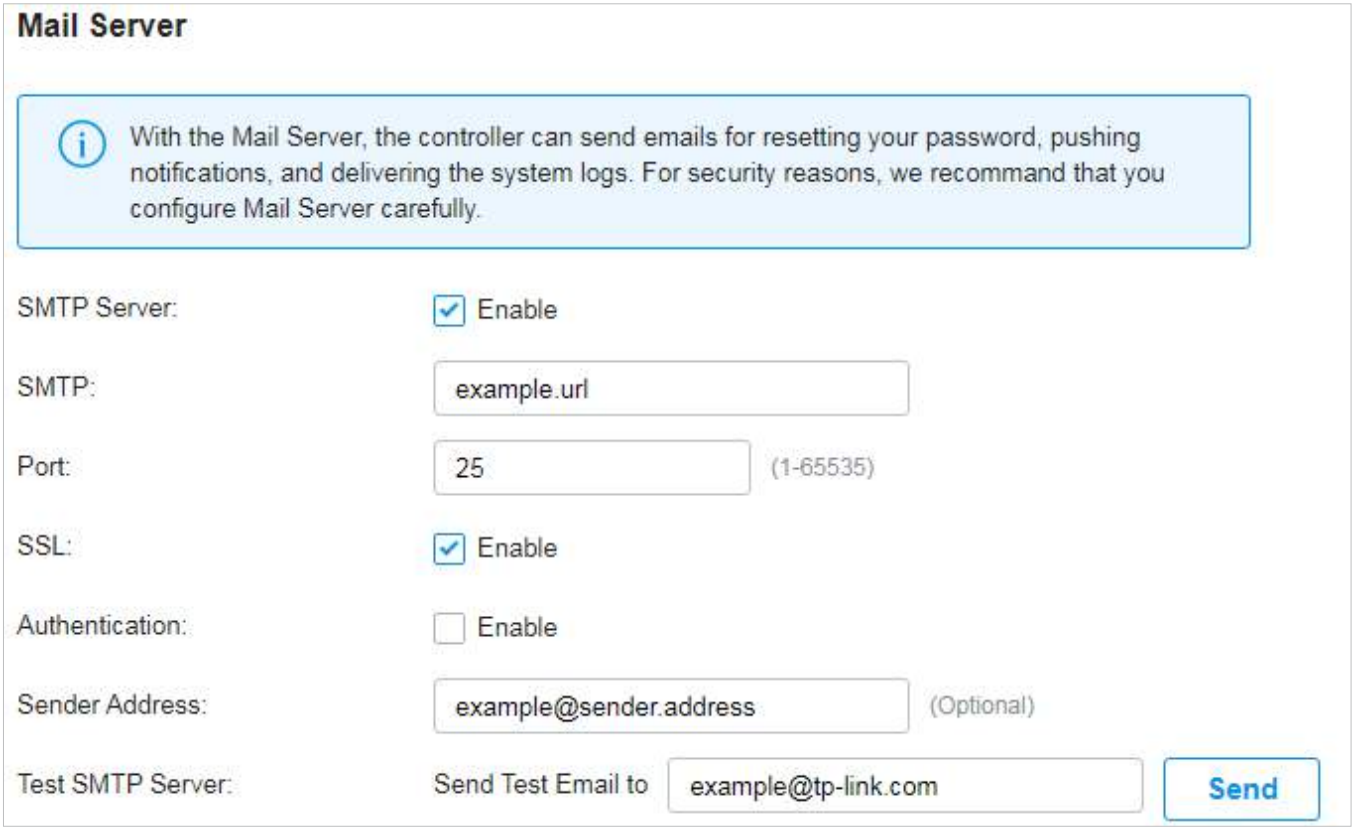
1)Activați serverul de e-mail

2)Activați e-mailurile de alertă pe site

3)Activați e-mailurile de alertă în Admin

4)Activați e-mailurile de alertă în jurnal

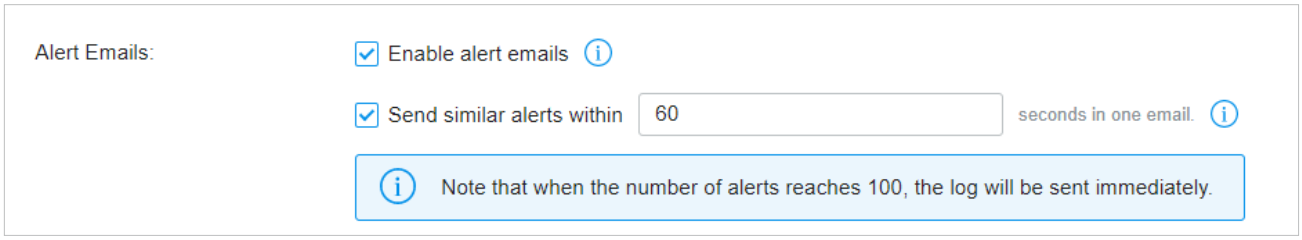
SelectațiGlobaldin lista derulantă aOrganizareîn colțul din dreapta sus. Mergi laSetări> Setări controler. ÎnServer de e-mailsecțiunea, activați Serverul SMTP și configurați parametrii. Apoi apasaSalvați.



SMTP	Introduceți adresa URL sau adresa IP a serverului SMTP conform instrucțiunilor furnizorului de servicii de e-mail.
Port	Configurați portul utilizat de serverul SMTP conform instrucțiunilor furnizorului de servicii de e-mail.
SSL	Activați sau dezactivați SSL conform instrucțiunilor furnizorului de servicii de e-mail. SSL (Secure Sockets Layer) este folosit pentru a crea o legătură criptată între controler și serverul SMTP.
Autentificare	Activați sau dezactivați autentificarea conform instrucțiunilor furnizorului de servicii de e-mail. Dacă autentificarea este activată, serverul SMTP necesită numele de utilizator și parola pentru autentificare.
Nume de utilizator	Când autentificarea este activată, introduceți adresa dvs. de e-mail ca nume de utilizator.
Parola	Când autentificarea este activată, introduceți codul de autentificare ca parolă, care este furnizat de furnizorul de servicii de e-mail când activați serviciul SMTP.
Adresa expeditorului	(Opțional) Specificați adresa expeditorului e-mailului. Dacă îl lăsați necompletat, controlerul vă folosește adresa de e-mail ca adresă expeditorului.
Testați serverul SMTP	Testați configurația serverului de e-mail trimițând un e-mail de test la o adresă de e-mail pe care o specificați.

Activați serverul de e-mail | Activați e-mailurile de alertă pe site | Activați e-mailurile de alertă în Admin

1. Selectați un site din lista derulantă aOrganizareîn colțul din dreapta sus. Mergi laSetări site> Buturuga> Notificărișiactivațiși activațiE-mailuri de alertă.



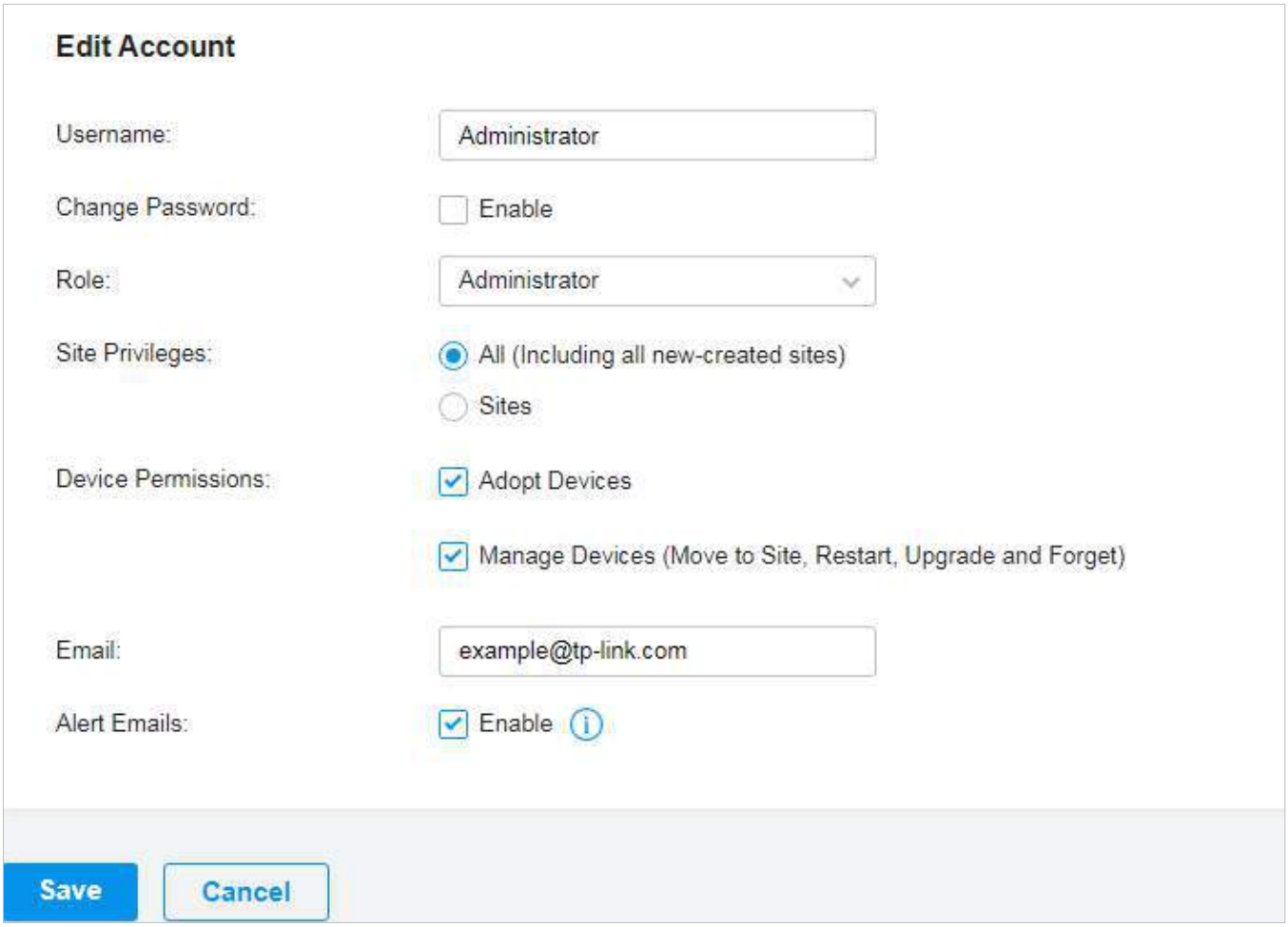
2. (Opțional) Pe aceeași pagină, activațiTrimiteți alerte similare în câteva secunde într-un singur e-mailși specificați intervalul de timp. Când este activată, alertele similare generate în fiecare perioadă de timp sunt colectate și trimise administratorilor și spectatorilor într-un singur e-mail.

3. Faceți clicSalvați.

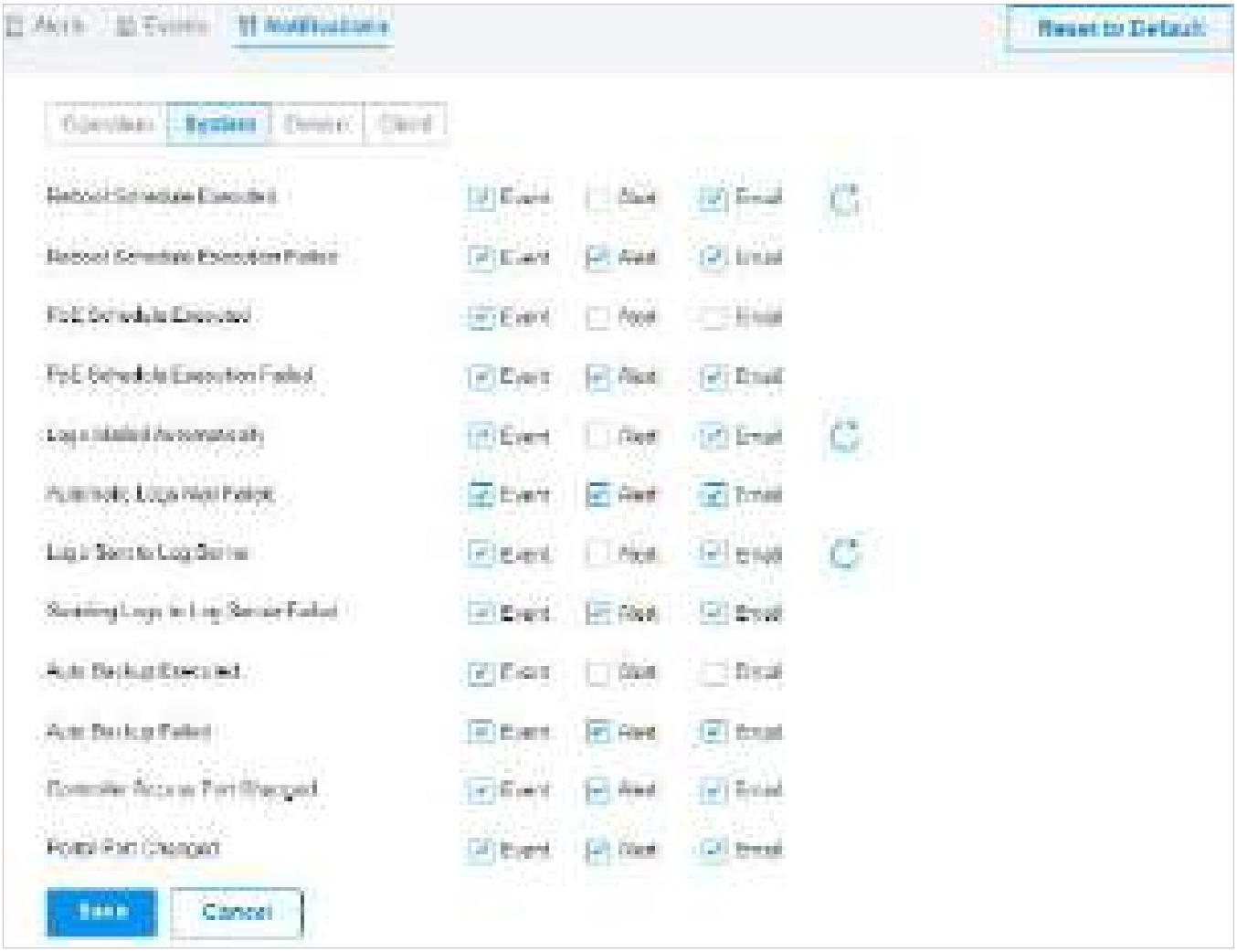
Activați e-mailurile de alertă pe site | Activați e-mailurile de alertă în Admin | Activați e-mailurile de alertă în jurnal

SelectațiGlobaldin lista derulantă aOrganizareîn colțul din dreapta sus. Mergi laAdminși configurați e-mailuri de alertă pentru ca administratorii și spectatorii să primească e-mailurile. Clic+ Adăugați un nou administrator

Contpentru a crea un cont sau faceți clic pentru a edita un cont. Introdu adresa de e-mail înE-mailși activați E-mailuri de alertă. ClicCreasauSalvați.



Mergi laButuruga și faceți clicNotificări. Faceți clic pe o filă de tipuri de conținut și activațiE-mailpentru jurnalele de activitate pe care controlorul le trimite prin e-mail administratorilor. ClicSalvați.



Gestionați conturile de administrator ale Omada SDN Controller

Acest capitol oferă o introducere la diferite niveluri de utilizator ale conturilor de administrator și vă îndrumă despre cum să le creați și să le gestionați în pagina Administrator. Capitolul include următoarele secțiuni:

8. 1 Introducere în Conturile de utilizator

Omada SDN Controller oferă trei niveluri de acces disponibile pentru utilizatori:administrator principal, administrator și vizualizator.De asemenea, puteți crea noi roluri de cont și le puteți personaliza permisiunile pentru a accesa diferite funcții.

Deoarece controlerul poate fi accesat atât local, cât și prin acces la cloud, utilizatorii pot fi grupați în continuare în utilizatori locali și utilizatori în cloud.

Contul administrativ pe mai multe niveluri prezintă o ierarhie de permisiuni pentru diferite niveluri de acces la controlor, după cum este necesar. Această abordare asigură securitatea și oferă confort pentru management.

Mai mult, în lista de conturi de utilizator a administratorului principal vor fi afișate toate conturile create de administratorul principal, inclusiv administratorii și vizualizatorii. Conturile de vizualizare create de fiecare administrator vor fi ascunse implicit, făcând interfața mai sistematică și la obiect.

■ Master Administrator

Administratorul principal are acces la toate funcțiile.

Contul care lansează primul controler va fi administratorul principal. Nu poate fi schimbat și șters.

■ Administrator

Administratorii nu au permisiunea pentru unele module, inclusiv accesul la cloud, migrarea, backupul automat și jurnalele de vizualizare globală. Ei au permisiunea de numai citire pentru unele module, cum ar fi gestionarea licențelor de vizualizare globală și roluri personalizate de cont.

Administratorii pot fi creați și șterși numai de administratorul principal.

■ Vizualizator

Spectatorii pot vedea starea și setările rețelei și pot modifica setările în Hotspot Manager. Intrarea în pagina Cont este ascunsă pentru spectatori și pot fi create sau șterse de administratorul și administratorul principal.

■ Roluri personalizate

Rolurile personalizate pot fi configurate pentru a accesa diferite funcții.

Acestea pot fi create sau șterse numai de administratorul principal.

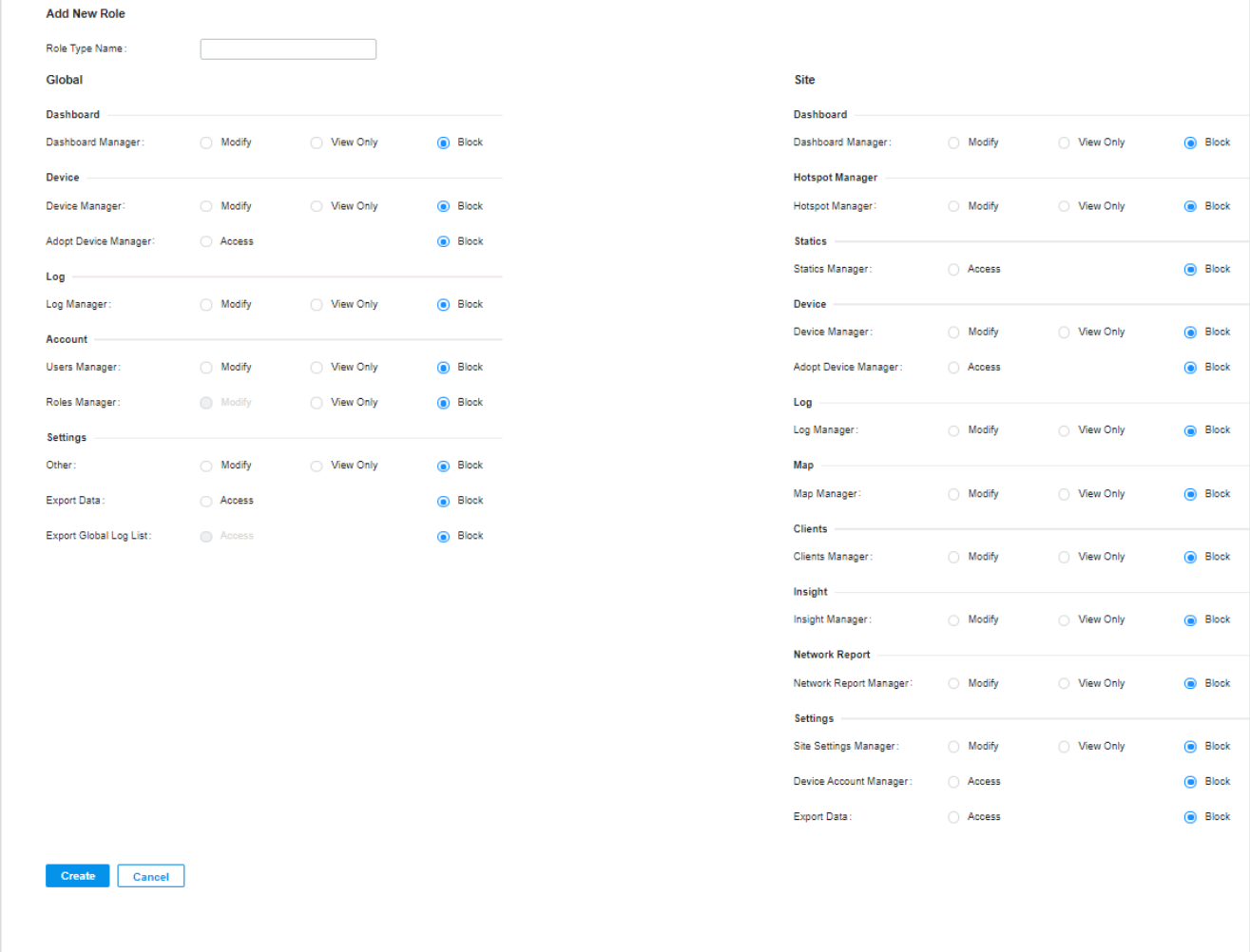
Notă:

Vă rugăm să actualizați aplicația Omada la versiunea 4.6 sau o versiune ulterioară, altfel este posibil să nu vă puteți conecta cu conturile asociate cu roluri personalizate.

8. 2 Creați și gestionați rolurile personalizate ale conturilor

1. SelectațiGlobaldin lista derulantă aOrganizareîn colțul din dreapta sus. Mergi laCont>Rol.

2. Faceți clicAdăugați un rol nou. Specificați numele tipului de rol și personalizați permisiunile pentru rol.



3. Faceți clicCrea. Noul rol va fi afișat în lista de roluri.

8. 3 Gestionați și creați conturi de utilizator locale

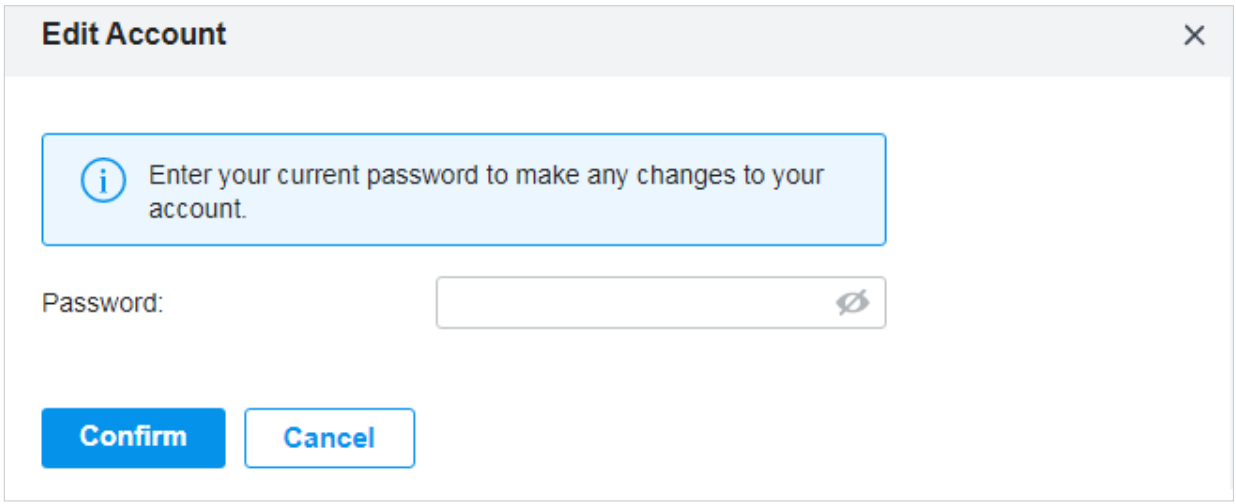
În mod implicit, Omada SDN Controller configurează automat un utilizator local cu rolul numit administrator principal ca administrator principal. Numele de utilizator și parola administratorului principal

sunt identice cu cele ale contului de controlor în mod implicit. Administratorul principal nu poate fi șters și poate crea, edita și șterge alte niveluri de conturi de utilizator.

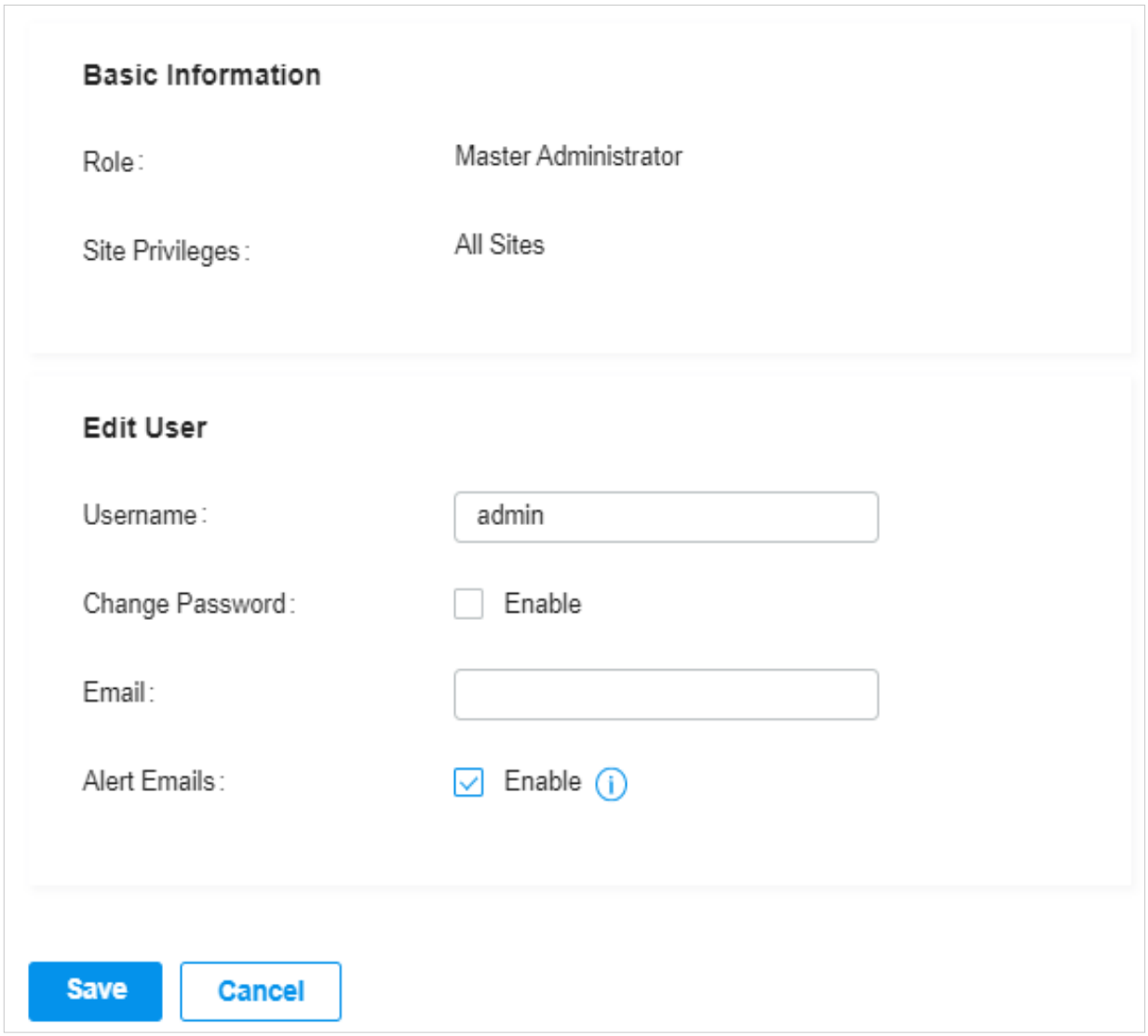
8. 3. 1 Editați contul de administrator principal

Pentru a vizualiza informațiile de bază și a edita contul de administrator principal, urmați acești pași:

1. SelectațiGlobaldin lista derulantă aOrganizareîn colțul din dreapta sus. Mergi laCont>Utilizator.
2. Faceți clic în coloana Acțiune. Introduceți parola și faceți clicA confirma(în mod implicit, parola administratorului principal este aceeași cu contul de controler).



3. Verificați informațiile de bază, modificați parola sau activați e-mailurile de alertă în funcție de nevoile dvs. Clic Salvați.



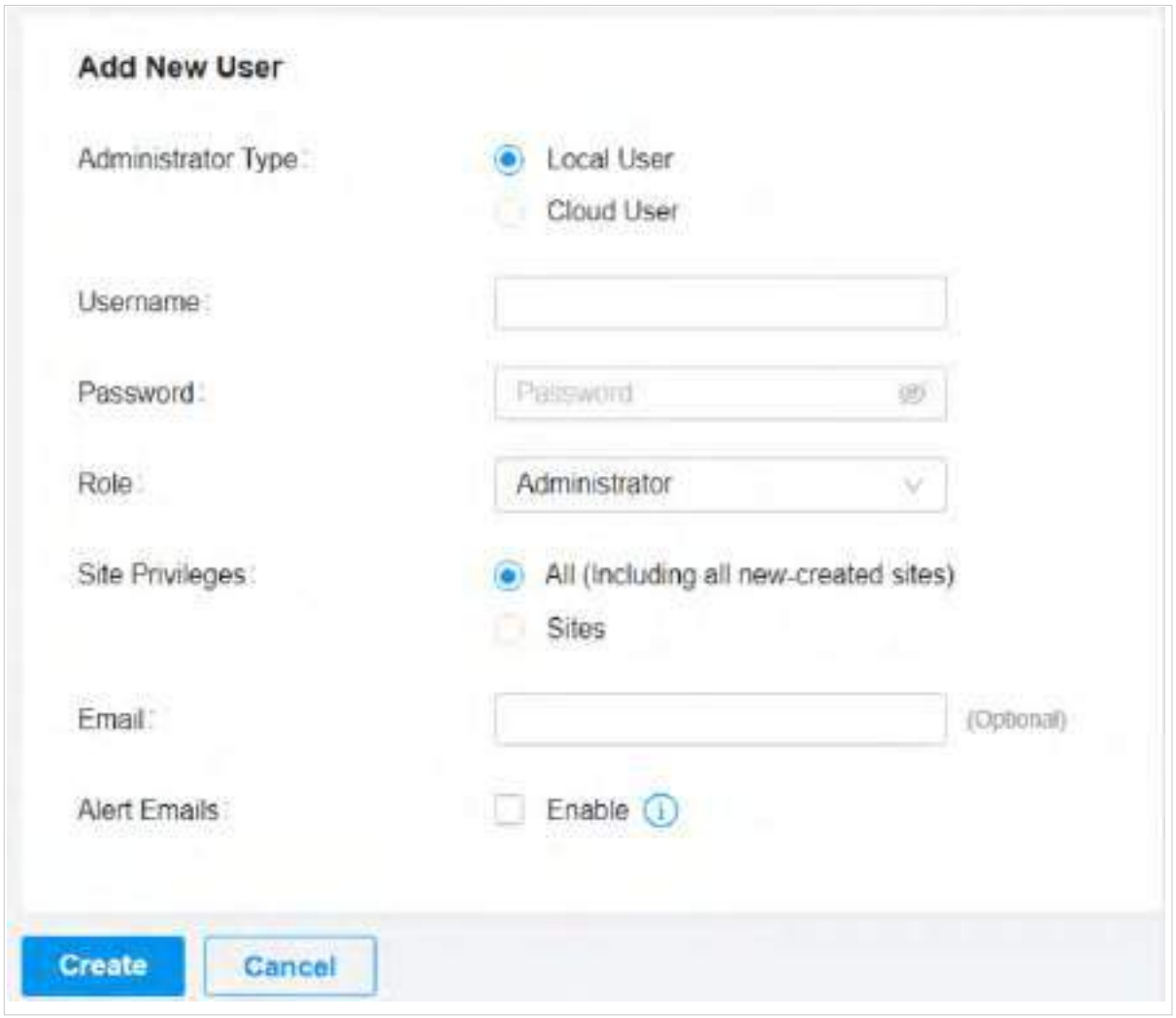
8. 3. 2 Creați și gestionați alte conturi locale

Pentru a crea și gestiona contul de utilizator local, urmați acești pași:

1. SelectațiGlobaldin lista derulantă aOrganizareîn colțul din dreapta sus. Mergi laCont>Utilizator.

2. Faceți clicAdăugați un utilizator nou.

3. SelectațiUtilizator localpentru administrator tastați în fereastra pop-out. Specificați parametrii și faceți clic Crea.



Nume de utilizator	Specificați numele de utilizator. Numele de utilizator ar trebui să fie diferit de cel existent.
Parola	Specificați parola.
Rol	Selectați un rol pentru contul de utilizator creat. Administrator: Acest rol are permisiuni de a adopta și/sau de a gestiona dispozitivele site-urilor alese în privilegiile site-ului, de a se edita, de a crea/edita/șterge conturi de vizualizare în site-urile sale privilegiate. Cu toate acestea, nu se poate șterge singur sau edita/șterge conturile de administrator principal și alte conturi de administrator. Vizualizator: Acest rol poate vizualiza informațiile site-urilor alese în privilegiile site-ului. Se poate edita doar singur. Roluri personalizate: Dacă ați creat roluri personalizate, acestea vor fi afișate în listă. Pentru a crea roluri personalizate, consultați8. 2 Creați și gestionați rolurile personalizate ale conturilor.

Privilegii site	Atribuiți permisiunile site-ului utilizatorului local creat. Toate: utilizatorul creat are permisiuni pentru dispozitive pe toate site-urile, inclusiv pe toate site-urile nou-create. Site-uri: Utilizatorul creat are permisiunea de dispozitiv în site-urile selectate. Selectați site-urile bifând caseta dinaintea lor.
E-mail (opțional)	Introduceți o adresă de e-mail pentru a primi e-mailuri de alertă.
E-mailuri de alertă	Bifați caseta dacă doriți ca utilizatorul creat să primească e-mailuri despre alertele site-urilor privilegiate.

Pentru a edita și șterge conturile, faceți clic pe pictograme din coloana de acțiuni.

	Pentru a edita parametrii pentru utilizator. Administratorul principal poate edita toate conturile de utilizator. Administratorul se poate edita singur și conturile de vizualizare ale site-urilor sale privilegiate, iar vizualizatorul se poate edita doar singur.
	Pentru a șterge contul. Administratorul principal poate șterge toate conturile de utilizator în afară de el, administratorul poate șterge conturile de vizualizator de pe site-urile sale privilegiate, iar vizualizatorul nu poate șterge niciun cont.

8. 4 Gestionați și creați conturi de utilizator Cloud

Controlerul dvs. configurează automat administratorul principal de cloud dacă ați activat accesul la cloud și ați legat contul de controler cu un ID TP-Link. Numele de utilizator și parola sunt aceleași cu cele ale ID-ului TP-Link. Administratorul cloud master nu poate fi șters și poate crea, edita și șterge alte niveluri de conturi de utilizator.

8. 4. 1 Configurați Cloud Master Administrator

Dacă nu ați activat accesul la cloud și ați legat controlerul cu un ID TP-Link, pentru a configura administratorul cloud master, urmați acești pași:

1. SelectațiGlobaldin lista derulantă aOrganizareîn colțul din dreapta sus. Mergi laSetări>Acces la cloudpentru a activa Cloud Access și pentru a vă lega ID-ul TP-Link.

2. AccesațiCont>Utilizator. Va fi creat automat un administrator cloud master cu același nume de utilizator ca ID-ul TP-Link. Administratorul Cloud Master nu poate fi șters. Vă puteți autentifica cu administratorul cloud master când accesul la cloud este activat.

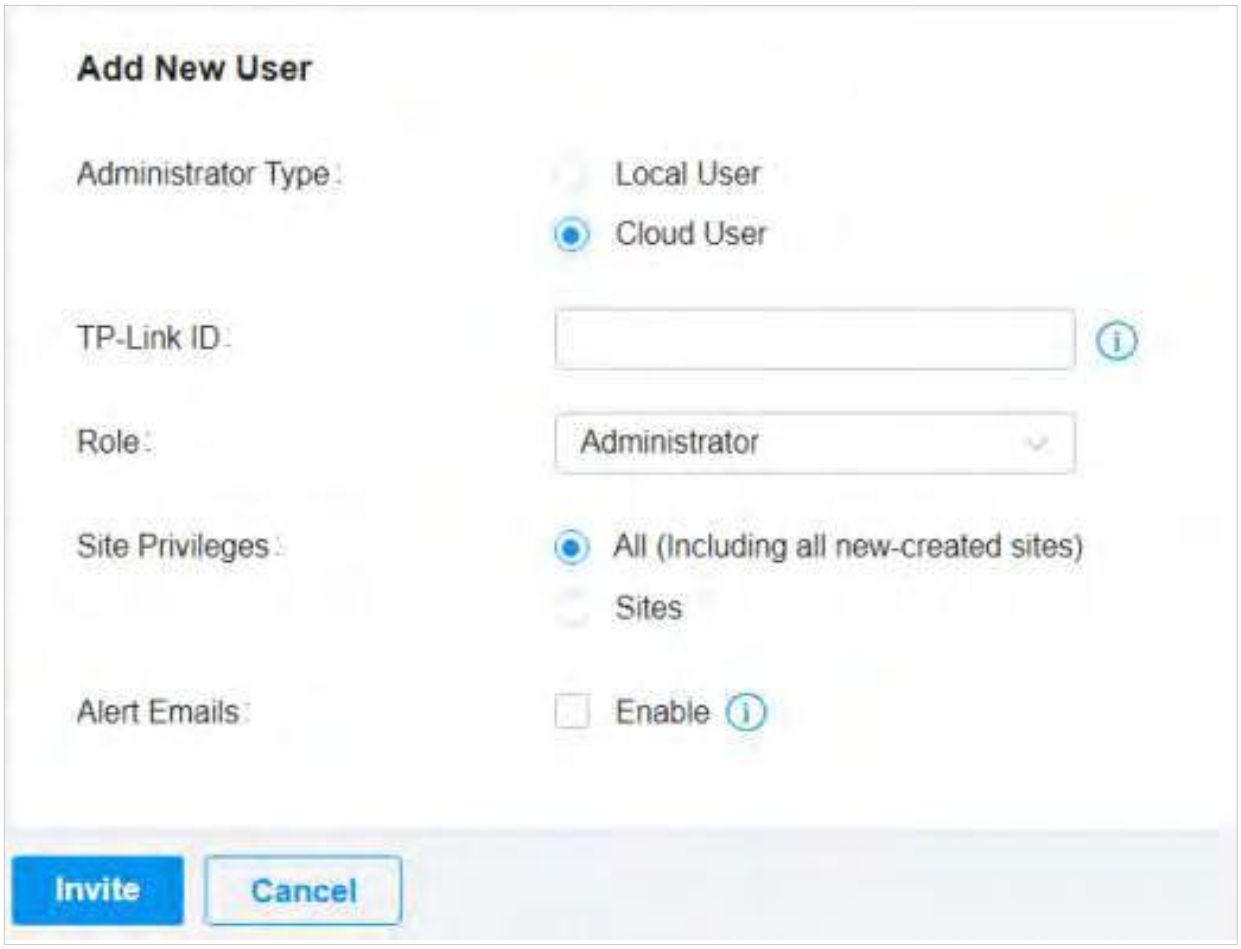
8. 4. 2 Creați și gestionați Cloud Administrator și Cloud Viewer

Pentru a crea și gestiona contul de utilizator cloud, urmați acești pași:

1. SelectațiGlobaldin lista derulantă aOrganizareîn colțul din dreapta sus și accesațiCont> Utilizator.

2. Faceți clicAdăugați un utilizator nou.

3. SelectațiUtilizator cloudpentru administrator tastați în fereastra pop-out. Specificați parametrii și faceți clicA invita.



ID TP-Link	Introduceți o adresă de e-mail a utilizatorului cloud creat și apoi un e-mail de invitație va fi trimis la adresa de e-mail. Dacă adresa de e-mail a fost deja înregistrată ca ID TP-Link, aceasta va deveni un utilizator cloud valid după acceptarea invitației. Dacă adresa de e-mail nu a fost înregistrată, va primi un e-mail de invitație pentru înregistrare. După terminarea înregistrării, acesta va deveni automat un utilizator cloud valid.
Rol	Selectați un rol pentru utilizatorul cloud creat. Administrator: Acest rol are permisiuni de a adopta și/sau de a gestiona dispozitivele site-urilor alese în privilegiile site-ului, de a se edita, de a crea/edita/șterge conturi de vizualizare în site-urile sale privilegiate. Cu toate acestea, nu se poate șterge singur sau edita/șterge conturile de administrator principal și alte conturi de administrator. Vizualizator: Acest rol poate vizualiza informațiile site-urilor alese în privilegiile site-ului. Se poate edita doar singur. Roluri personalizate: Dacă ați creat roluri personalizate, acestea vor fi afișate în listă. Pentru a crea roluri personalizate, consultați8. 2 Creați și gestionați rolurile personalizate ale conturilor.

Privilegii site	Atribuiți permisiunea site-ului utilizatorului cloud creat. Toate: utilizatorul creat are permisiunea pe toate site-urile, inclusiv pe toate site-urile nou-create. Site-uri: Utilizatorul creat are permisiunea pe site-urile selectate. Selectați site-urile bifând caseta dinaintea lor.
E-mailuri de alertă	Bifați caseta dacă doriți ca utilizatorul creat să primească e-mailuri despre alertele site-urilor privilegiate.

Pentru a edita și șterge conturile, faceți clic pe pictograme din coloana de acțiuni.

	Pentru a edita parametrii pentru utilizator. Administratorul principal Cloud poate edita toate conturile de utilizator, administratorul se poate edita singur și conturile de vizualizare ale site-urilor sale privilegiate, vizualizatorul se poate edita doar singur.
	Pentru a șterge contul. Administratorul principal cloud poate șterge toate conturile de utilizator, cu excepția administratorului principal și el însuși, administratorul poate șterge conturile de vizualizare ale site-urilor sale privilegiate, vizualizatorul nu poate șterge niciun cont.