Guide de l’utilisateur

Contrôleur Omada SDN

12/10/2020

À propos de ce guide

Ce guide d'utilisation fournit des informations pour la gestion centralisée des périphériques TP-Link via le contrôleur SDN d'Omada. Veuillez lire attentivement ce guide avant l'opération.

Lecteurs visés

Ce guide d'utilisation est destiné aux gestionnaires de réseau familiers avec les concepts informatiques et les terminologies réseau.

Conventions

Lorsque vous utilisez ce guide, notez que :

■Les fonctionnalités disponibles dans le contrôleur SDN Omada peuvent varier en fonction de votre région, de votre version de contrôleur et du modèle de périphérique. Toutes les images, les étapes et les descriptions de ce guide ne sont que des exemples et peuvent ne pas refléter votre expérience réelle.

■Les informations contenues dans ce document peuvent être modifiées sans préavis. Tous les efforts ont été faits dans la préparation de ce document pour assurer l'exactitude du contenu, mais toutes les déclarations, informations et recommandations contenues dans le présent document ne constituent aucune garantie de quelque nature que ce soit, expresse ou implicite. Les utilisateurs doivent assumer l'entière responsabilité de leur application de tous les produits.

■Ce guide utilise les formats spécifiques pour mettre en évidence des messages spéciaux. Le tableau suivant répertorie les icônes d'avis utilisées dans ce guide.

Note	Rappelez-vous de prendre note. La note contient les informations utiles pour une meilleure utilisation du contrôleur
Recommandations de configuration	Fournit des conseils pour vous renseigner sur la fonctionnalité et ses configurations.

Plus d'informations

■Pour obtenir un soutien technique, la dernière version du Guide de l'utilisateur et d'autres informations, veuillez visiter https://www.tp-link.com/support.

■Pour poser des questions, trouver des réponses et communiquer avec les utilisateurs ou les ingénieurs de TP-Link, veuillez visiter https://community.tp-link.com pour rejoindre la communauté TP-Link.

CONTENU

À propos de ce guide 2

Conventions 2

Plus d'informations 2

CONTENU 3

Vue d'ensemble de la solution de contrôleur Omada SDN 9

1. 1 Vue d'ensemble de la solution de contrôleur SDN d'Omada 2

1. 2 Composants de base 3

Contrôleur Omada SDN 3

Passerelles gérées par Omada 5

Commutateurs gérés d'Omada 5

Points d'accès Omada 7

Prise en main du contrôleur SDN d'Omada 8

2. 1 Configurer votre contrôleur logiciel 8

2. 1. 1 Déterminer la topologie réseau 9

2. 1. 2 Installer le contrôleur logiciel Omada 9

Installation sur Linux 10

Lancer le contrôleur logiciel Omada 12

Effectuer les configurations de base 13

Connectez-vous à l'interface de gestion 16

2. 2 Configurer votre contrôleur matériel 16

2. 2. 1 Déterminer la topologie réseau 17

2. 2. 2 Déployer le contrôleur matériel Omada 17

Connectez-vous à l'interface de gestion 17

Effectuer les configurations de base 18

Connectez-vous à l'interface de gestion 20

2. 3 Configurer votre contrôleur cloud 21

Gérer les périphériques et sites gérés par Omada 22

3. 1 Créer des sites 22

Aperçu 22

Configuration 23

3. 2 Adopter des appareils 26
Aperçu 26
Configuration 27
Configurer le réseau avec le contrôleur SDN Omada 38
4. 1 Naviguer dans l'interface utilisateur 39
4. 2 Modifier la configuration actuelle du site 42
Aperçu 42
Configuration 42
Aperçu 43
Configuration 43
Aperçu 45
Configuration 45
4. 3 Configurer les réseaux câblés 48
Configuration 49
Aperçu 66
Configuration 66
4. 4 Configurer les réseaux sans fil 77
Configuration 78
Configuration 88
Aperçu 89
Configuration 89
Configuration 91
4. 5 Sécurité réseau 92
Aperçu 92
Configuration 93
Aperçu 102
Configuration 102
Aperçu 105
Configuration 106
4. 6 Transmission 110
Aperçu 110
Configuration 110
Aperçu 113
Configuration 113

Configuration 116
Configuration 117
4. 7 Configuration VPN 120
Aperçu 120
Configuration 124
4. 8 Créer des profils 150
4. 8. 1 plage de temps 150
4. 8. 2 Groupes 152
4. 9 Authentification 156
Aperçu 156
Configuration 157
Aperçu 190
Configuration 191
Aperçu 193
Configuration 194
Aperçu 195
Configuration 195
4. 10 Services 197
Aperçu 197
Configuration 198
Aperçu 199
Configuration 200
Aperçu 201
Configuration 201
Aperçu 201
Configuration 202
Aperçu 202
Aperçu 204
Aperçu 205
Configurer le contrôleur SDN Omada 206
5. 1 Gérer le contrôleur 207
Configuration 207
Aperçu 208
Configuration 208
Configuration 210

Configuration 210
Aperçu 211
Configuration 211
Aperçu 212
Configuration 212
5. 2 Gérer votre contrôleur à distance via l'accès cloud 213
Aperçu 213
Configuration 213
5. 3 Maintenance 215
5. 3. 1 État du contrôleur 215
Configuration 215
Aperçu 217
Configuration 217
5. 4 Migration 218
Aperçu 218
Configuration 218
Aperçu 224
Configuration 224
5. 5 Auto Backup 229
Aperçu 229
Configuration 229
Configurer et surveiller les périphériques gérés par Omada 231
6. 1 Introduction à la page Périphériques 232
Aperçu 232
Configuration 233
6. 2 Configurer et surveiller la passerelle 235
6. 2. 1 Configurer la Gateway 236
6. 2. 2 Surveiller la passerelle 240
Panneau de moniteur 240
Détails 241
Network 242
Statistiques 242
6. 3 Configurer et surveiller les commutateurs 243
6. 3. 1 Configurer les commutateurs 243

Ports 244
Configuration 255
Panneau de moniteur 260
Détails 261
Clients 262
Statistiques 263
6. 4 Configurer et surveiller les EAP 264
6. 4. 1 Configurer les EAP's 265
6. 4. 2 Surveiller les EAP's 273
Panneau de moniteur 273
Détails 274
Clients 276
Maillage (uniquement pour les périphériques en attente/connectés/isolés prenant en charge Mesh) 277
Statistiques 279
Surveiller et gérer les clients 280
7. 1 Gérer les clients filaires et sans fil dans la page clients 281
7. 1. 1 Page Introduction aux clients 281
7. 1. 2 Utilisation de la Table clients pour surveiller et gérer les clients 281
7. 1. 3 Utilisation de la fenêtre Propriétés pour surveiller et gérer les clients 283
Surveiller et gérer un seul client 283
Surveiller et gérer plusieurs clients 286
7. 2 Gérer l'authentification du client dans le Gestionnaire de points d'accès 288
7. 2. 1 Clients autorisés 288
7. 2. 2 Vouchers 289
Créer vouchers 289
Créer des utilisateurs locaux 292
Créer des opérateurs 296
Surveillance du réseau 298
8. 1 Afficher l'état du réseau avec le tableau de bord 299
8. 1. 1 Disposition de page du tableau de bord 299
Vue d'ensemble de la topologie 299
Barre d'onglets 300
Système 302
Réseau 302
Client 306

8. 2 Voir les statistiques du réseau 308
8. 2. 1 Performance 308
Barre d'onglets 308
Graphiques statistiques 310
Barre d'onglets 313
Graphiques statistiques 315
Barre d'onglets 315
Graphiques statistiques 316
8. 3 Surveiller le réseau avec la carte 317
8. 4 Afficher les statistiques pendant la période spécifiée avec Insight 321
8. 5 Afficher et gérer les journaux 326
Gérer les comptes d'administrateur du contrôleur SDN Omada 336
9. 1 Introduction aux comptes d'utilisateurs 337
- Master Administrator 337
- Administrator 337
- Viewer 337

9. 2 Gérer et créer des comptes d'utilisateurs locaux 338
9. 2. 1 Modifier le compte d'administrateur principal 338
9. 2. 2 Créer et gérer l'administrateur et le visionneur 340
9. 3 Gérer et créer des comptes utilisateur cloud 342
9. 3. 1 Configurer l'administrateur maître cloud 342
9. 3. 2 Créer et gérer l'administrateur cloud et l'observateur de cloud 343
DROITS D'AUTEUR ET MARQUES DE COMMERCE 345

1

Vue d’ensemble de la solution de contrôleur Omada SDN

Omada SDN Controller Solution offre une gestion centralisée et efficace pour la configuration des réseaux d’entreprise composés de passerelles de sécurité, de commutateurs et de points d’accès sans fil.

Grâce à une plate-forme de gestion de réseau fiable alimentée par TP-Link Omada SDN Controller, vous pouvez développer un réseau complet et défini par logiciel dans des environnements exigeants et à fort trafic avec des solutions filaires et sans fil robustes.

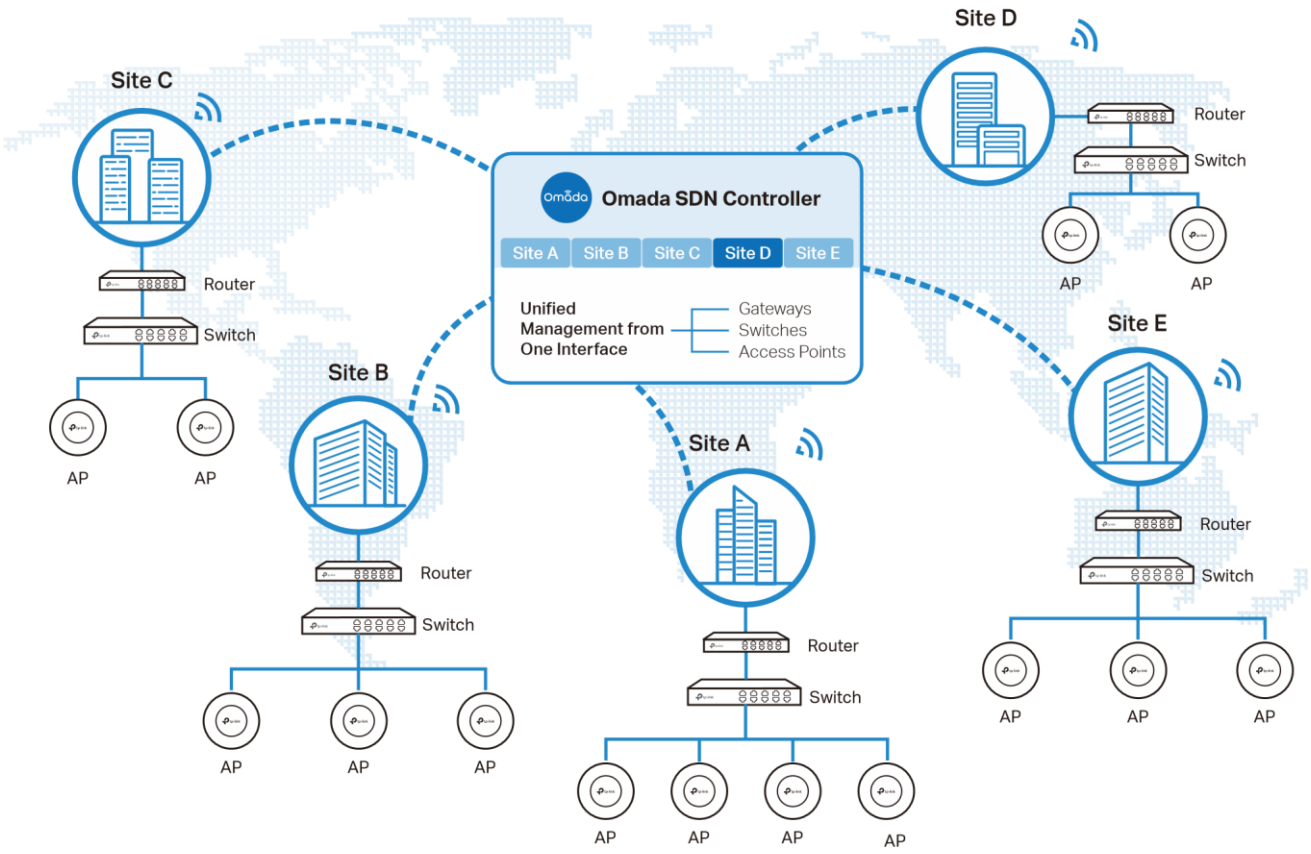
Le chapitre comprend les sections suivantes :

1. Vue d’ensemble de la solution de contrôleur SDN d’Omada
2. Composants de base

1. 1 Vue d'ensemble de la solution de contrôleur SDN d'Omada

Omada SDN Controller Solution est conçue pour fournir des solutions de réseautage de classe affaires pour des environnements exigeants et à fort trafic tels que les campus, les hôtels, les centres commerciaux et les bureaux. Omada SDN Controller Solution simplifie le déploiement et la gestion des réseaux d'entreprise à grande échelle et offre une maintenance facile, une surveillance continue et une évolutivité flexible.

Cette figure montre un exemple d'architecture d'un réseau d'entreprise Omada SDN :



Les éléments interconnectés qui travaillent ensemble pour fournir un réseau d'entreprise unifié incluent : Le contrôleur SDN d'Omada, les passerelles, les commutateurs, les points d'accès et les périphériques clients. En commençant par une base d'appareils clients, chaque élément ajoute fonctionnalité et complexité au fur et à mesure que le réseau se développe, s'interconnectant avec les éléments ci-dessus et en dessous pour créer une solution câblée et sans fil complète, sécurisée.

Omada SDN Controller est un centre de commandement et une plate-forme de gestion au cœur du réseau Omada. Avec une seule plate-forme, les administrateurs réseau configurent et gèrent les réseaux d'entreprise composés de routeurs, de commutateurs et de points d'accès sans fil par lots. Cela déclenche de nouveaux niveaux de gestion pour éviter une sur provision complexe et coûteuse.

1. 2 Composants de base

Un réseau Omada SDN se compose des composants de base suivants :

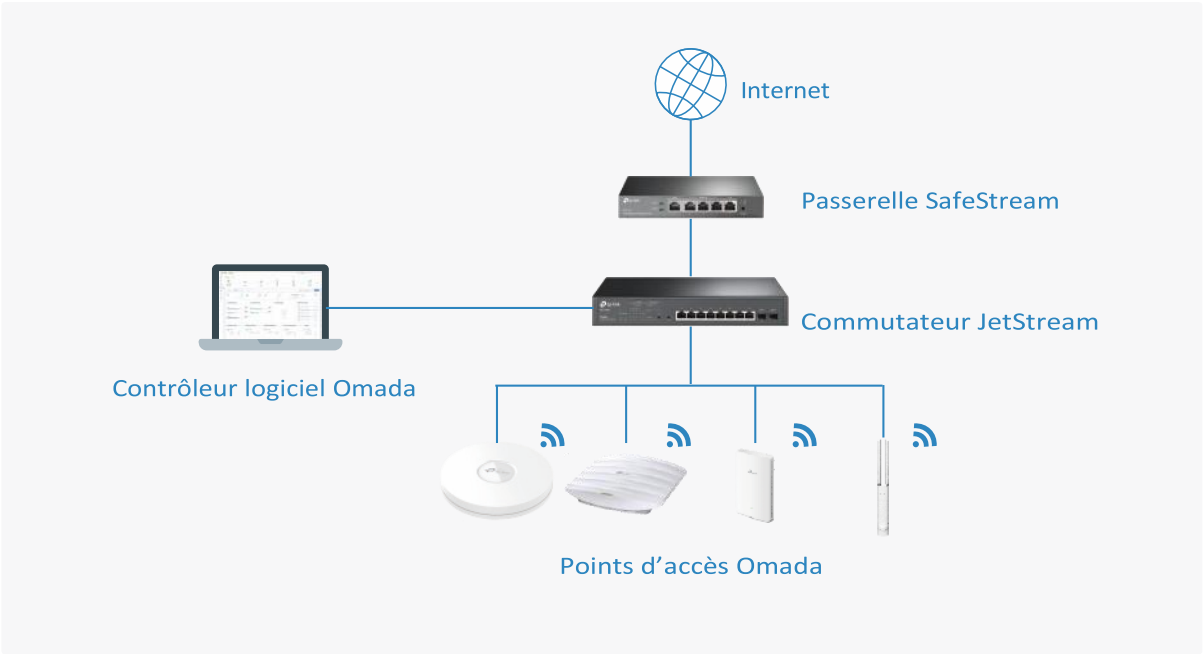
- **Omada SDN Controller** : un centre de commande et une plate-forme de gestion au cœur de la solution réseau Omada pour l’entreprise. Avec une seule plate-forme, les administrateurs réseau configurent et gèrent tous les produits Omada qui ont tous vos besoins couverts en termes de routage, de commutation et de Wi-Fi.
- **Passerelles** : disposent d’excellentes capacités de traitement des données et d’une gamme de fonctions puissantes, y compris le VPN IPsec/OpenVPN/PPTP/L2TP, le balancement de charge et le contrôle de bande passante, qui sont idéaux pour le réseau d’entreprise où un grand nombre d’utilisateurs ont besoin d’une connexion stable et sécurisée.
- **Commutateurs** : offrent une solution réseau flexible et rentable avec de puissantes fonctionnalités Layer 2 et des options PoE. Les fonctionnalités avancées telles que Access Control, QoS, LAG et Spanning Tree satisfont les réseaux d’affaires avancés.
- **Points d’accès** (EAP Omada) — répondez à la norme Wi-Fi grand public et répondez à vos besoins d’accès à la hauteur grâce à l’innovation de TP-Link pour vous aider à créer un réseau sans fil polyvalent et fiable pour toutes les applications professionnelles.

Contrôleur Omada SDN

Adapté aux différents besoins et budgets, Omada SDN Controller propose diverses solutions de déploiement. Le contrôleur logiciel Omada, le contrôleur matériel Omada et le contrôleur cloud d’Omada ont chacun leurs propres avantages et applications.

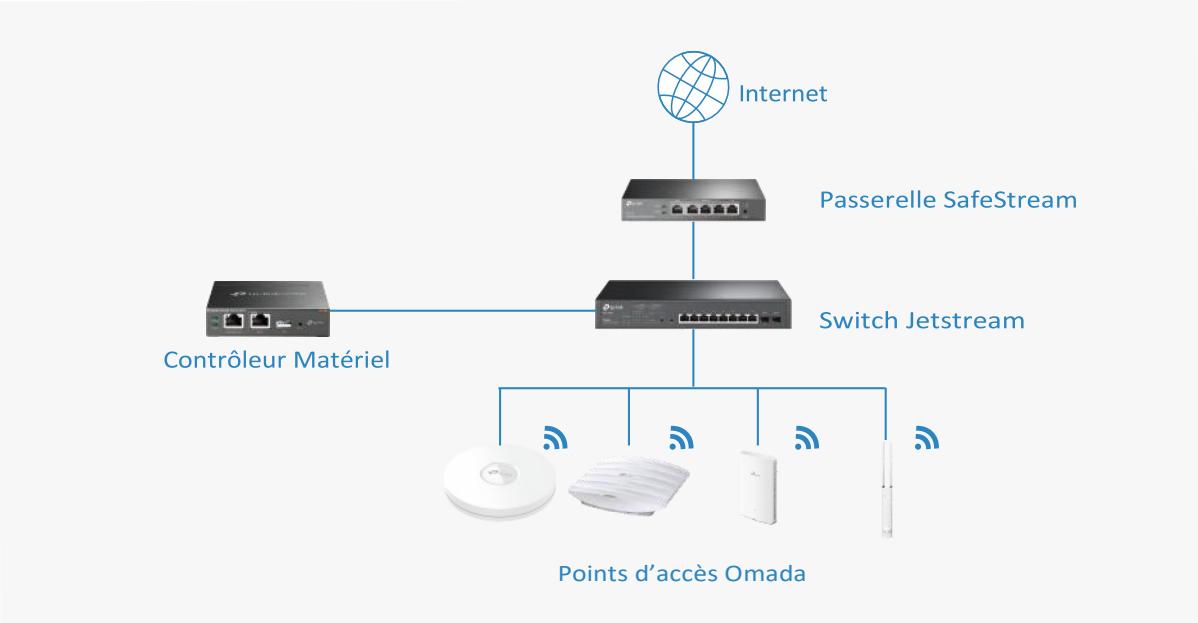
- **Contrôleur logiciel Omada**

  Omada Software Controller est totalement gratuit, ainsi que toutes les mises à niveau. Le contrôleur peut être hébergé sur n’importe quel ordinateur avec des systèmes Windows ou Linux sur votre réseau.



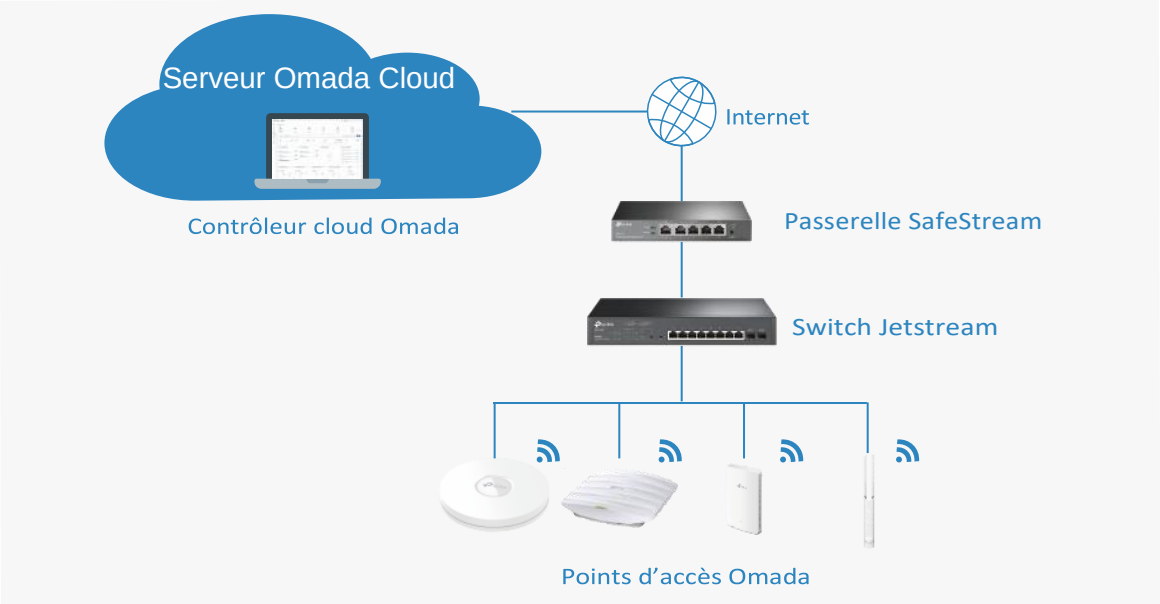
■ **Contrôleur matériel Omada**

Omada Hardware Controller est le périphérique de gestion qui est pré-installé avec Omada Software Controller. Vous avez juste besoin de payer pour l’appareil, puis le logiciel intégré Omada Controller est libre d’utiliser, pas de frais de licence ou de coûts supplémentaires requis. De la taille d’un téléphone mobile, l’appareil est facile à déployer et à installer sur votre réseau.



■ **Contrôleur cloud Omada**

Le contrôleur Cloud Omada est déployé sur le serveur Omada Cloud, fournissant un service payant avec des prix à plusieurs niveaux. Avec un abonnement payant au service Cloud Omada, vous n’avez pas besoin d’acheter un périphérique matériel supplémentaire ou d’installer le logiciel sur l’hôte.



Les contrôleurs diffèrent dans les formulaires, mais ils ont presque la même interface de gestion basée sur le navigateur et servent les mêmes fonctions de gestion du réseau. Dans ce guide, Omada Software Controller, Omada Hardware Controller et Omada Cloud-Based Controller sont appelés le contrôleur, sauf indication contraire.

Passerelles gérées par Omada

Le routeur VPN SafeStream de TP-Link prend en charge les connexions Gigabit Ethernet sur les ports WAN et LAN qui maintiennent les données en mouvement à la vitesse maximale. En incluant toutes les fonctions de routage et de segmentation réseau qu’un routeur d’entreprise doit avoir, le routeur VPN SafeStream sera l’épine dorsale du réseau Omada SDN. En outre, le routeur offre une approche à la fois sécurisée et facile pour déployer des tunnels VPN de site à site et d’accès pour les clients distants.

La gestion centralisée de la passerelle par l’intermédiaire du contrôleur SDN Omada est disponible uniquement sur certains modèles. Le tableau suivant fournit des informations spécifiques du routeur qui peuvent être gérées par le contrôleur.

Passerelles prises en charge par Omada	TL-R605(UN) V1 (version usine par défaut ou ou supérieure)
	TL-ER7206(UN) V1 (version usine par défaut ou ou supérieure)

Commutateurs gérés d’Omada

JetStream Switch de TP-Link offre des stratégies de sécurité de haute performance et de niveau d’entreprise et un engourdissement de fonctionnalités avancées, ce qui est idéal pour le réseau Omada SDN.

La gestion centralisée du commutateur via le contrôleur SDN Omada est disponible uniquement sur certains modèles. Le tableau suivant fournit des informations spécifiques sur le commutateur qui peuvent être gérées par le contrôleur.

Commutateurs pris en charge par Omada	TL-SG2210MP V1 (default factory version or above)
	TL-SG2428P V1 (default factory version ou supérieure)
	TL-SG2008P V1 (default factory version ou supérieure)
	TL-SG2008 V3 (version 3.0.0 ou supérieure)
	TL-SG2210P V3.20 (version 3.2.0 ou supérieure)
	TL-SG3428 V1 (default factory version ou supérieure)
	TL-SG3428MP V1 (default factory version ou supérieure)

TL-SG3452 V1 (default factory version ou supérieure)
TL-SG3452P V1 (default factory version ou supérieure)
TL-SG3428X V1 (default factory version ou supérieure)
TL-SG3428XMP V1 (default factory version ou supérieure)
TL-SG3210XHP-M2 V1 (default factory version ou supérieure)

Points d’accès Omada

Le point d’accès Omada de TP-Link offre une connexion Wi-Fi avec des performances et une autonomie supérieure qui garantissent une connectivité sans fil fiable pour le réseau Omada SDN.

La gestion centralisée des points d’accès par l’intermédiaire du contrôleur SDN Omada est disponible uniquement sur certains modèles. Le tableau suivant fournit des informations spécifiques sur les points d’accès qui peuvent être gérés par le contrôleur.

Points d’accès pris en charge par Omada	EAP660 HD V1 (default factory version ou supérieure)
	EAP620 HD V1 (default factory version ou supérieure)
	EAP265HD V1 (1.0.0 Build 20200424 ou supérieure)
	EAP245 V3 (2.20.0 Build 20200423 ou supérieure)
	EAP235-Wall (1.0.1 Build 20200618 ou supérieure)
	EAP230-Wall (1.0.0 Build 20200618 ou supérieure)
	EAP225 V3 (2.20.0 Build 20200630 ou supérieure)
	EAP225-Wall V2 (1.20.0 Build 20200422 ou supérieure)
	EAP225-Outdoor V1 (1.20.0 Build 20200422 ou supérieure)
	EAP115 V4 (3.20.0 Build 20200525 ou supérieure)
	EAP115-Wall V1 (1.20.0 Build 20200619 ou supérieure)
	EAP110 V4 (3.20.0 Build 20200525 ou supérieure)
	EAP110-Outdoor V3 (3.20.0 Build 20200511 ou supérieure)

2

Prise en main du contrôleur SDN d’Omada

Ce chapitre vous guide sur la façon de commencer avec omada contrôleur SDN pour configurer le réseau. Omada Software Controller, Omada Hardware Controller et Omada Cloud-Based Controller diffèrent dans les formulaires, mais ils ont presque la même interface de gestion basée sur le navigateur pour la gestion du réseau.
Par conséquent, ils ont presque les mêmes étapes initiales de configuration, y compris la construction de votre topologie réseau, le déploiement de votre contrôleur, et la connexion au contrôleur. Le chapitre comprend les sections suivantes :

- Configurer votre contrôleur logiciel
- Configurer votre contrôleur matériel
- Configurer votre contrôleur cloud

2. 1 Configurer votre contrôleur logiciel

La solution de contrôleur Omada SDN est conçue pour les réseaux évolutifs. Les déploiements et les configurations varient selon les situations réelles. Comprendre vos besoins réseau est la première étape lors de la planification de la fourniture d’un projet. Une fois que vous avez identifié ces exigences, suivez les étapes ci-dessous pour configurer initialement Omada Software Controller :

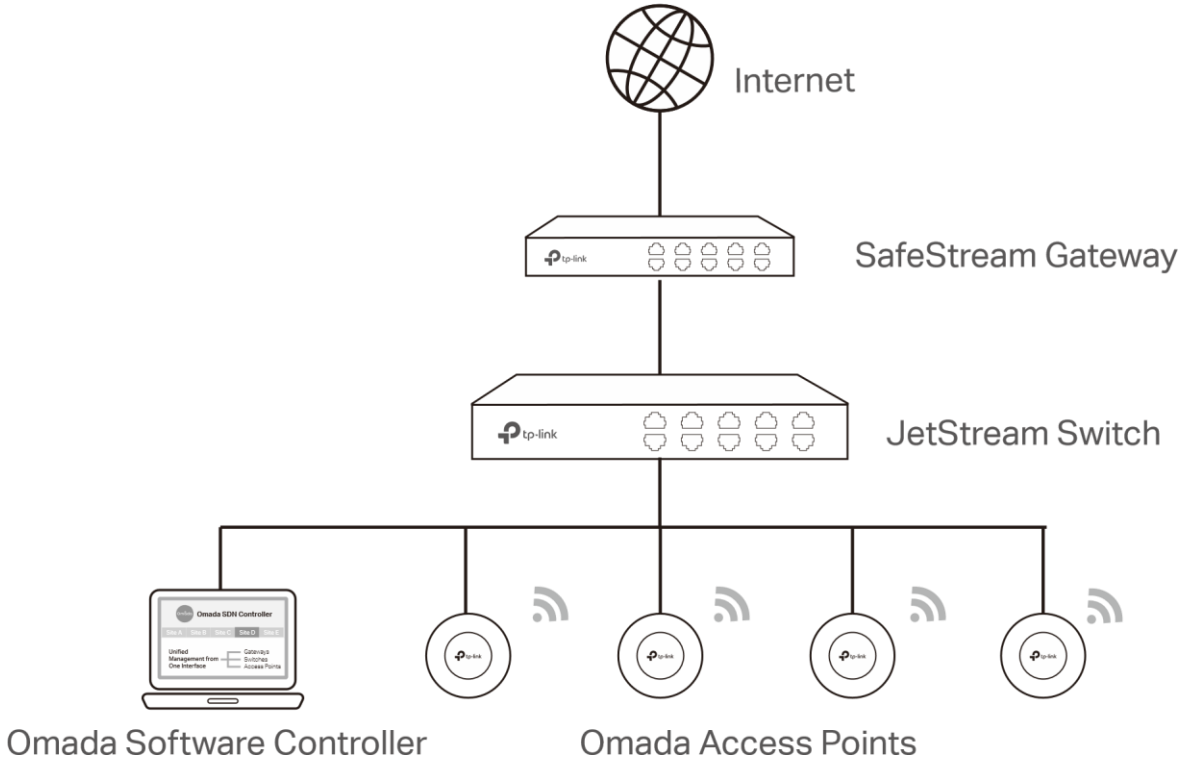
1) Déterminer la topologie du réseau.

2) Installer le contrôleur logiciel Omada.

3) Démarrer et se connecter au contrôleur.

2. 1. 1 Déterminer la topologie réseau

La topologie réseau que vous créez pour le contrôleur SDN Omada varie en fonction des besoins de votre entreprise. La figure suivante montre une topologie typique pour un cas d'utilisation à haute disponibilité.



Note:

Lorsque vous utilisez le contrôleur Omada SDN, nous vous recommandons de déployer la topologie Omada complète avec des périphériques TP-Link pris en charge. Si vous utilisez des appareils tiers, le contrôleur SDN Omada ne peut pas les découvrir et les gérer.

2. 1. 2 Installer le contrôleur logiciel Omada

Omada Software Controller est fourni pour les systèmes d'exploitation **Windows** et **Linux**.

Déterminez votre système d'exploitation et suivez les introductions ci-dessous pour installer Omada Software Controller.

Installation sur Windows

Omada Software Controller peut être hébergé sur n'importe quel ordinateur avec des systèmes Windows sur votre réseau. Assurez-vous que le matériel et le système de votre PC répondent aux exigences suivantes, puis installez correctement le contrôleur logiciel Omada.

- **Exigences matérielles**

  Le contrôleur logiciel Omada peut gérer jusqu'à 1500 EAP si l'hôte du contrôleur dispose de suffisamment de ressources matérielles. Pour garantir la stabilité opérationnelle de la gestion de 1500 PAE, nous vous recommandons d'utiliser le matériel qui répond ou dépasse les spécifications suivantes :

  Processeur : Intel Core i3-8100, i5-6500 ou i7-4700 avec 2 cœurs ou plus et 4 threads ou plus.

  Mémoire : 6 Go de RAM ou plus.

- **Exigences du système**

  Système d'exploitation : Microsoft Windows 7/8/10/Server. (Nous vous recommandons de déployer le contrôleur sur un système d'exploitation 64 bits pour garantir la stabilité du logiciel.)

  Navigateur Web : Mozilla Firefox 32 (ou supérieure), Google Chrome 37 (ou supérieure), Opera 24 (ou supérieure), ou Microsoft Internet Explorer 11 (ou supérieure).

- **Installer le contrôleur logiciel Omada**

  Téléchargez le fichier d'installation d'Omada Software Controller à partir du site Web. Suivez ensuite les instructions pour installer correctement le contrôleur logiciel Omada. Après une installation réussie, une icône de raccourci du contrôleur logiciel Omada sera créée sur votre bureau.

Installation sur Linux

Deux versions du package d'installation sont fournies : fichier.**tar.gz** et fichier **.deb.** Les deux peuvent être utilisés dans plusieurs versions du système d'exploitation Linux, y compris Ubuntu, CentOS, Fedora, et Debian.

Assurez-vous que le matériel et le système de votre PC répondent aux exigences suivantes, puis choisissez les fichiers d'installation appropriés pour installer le contrôleur logiciel Omada.

- **Exigences matérielles**

  Le contrôleur logiciel Omada peut gérer jusqu'à 1500 EAP si l'hôte du contrôleur dispose de suffisamment de ressources matérielles. Pour garantir la stabilité opérationnelle de la gestion de 1500 PAE, nous vous recommandons d'utiliser le matériel qui répond ou dépasse les spécifications suivantes :

  Processeur : Intel Core i3-8100, i5-6500 ou i7-4700 avec 2 cœurs ou plus et 4 threads ou plus.

  Mémoire : 6 Go de RAM ou plus.

- **Exigences du système**

  Système d'exploitation : système d'exploitation Linux 64 bits, y compris Ubuntu 14.04/16.04/17.04/18.04, CentOS 6.x/7.x, Fedora 20 (ou supérieure), et Debian 9.8.

  Navigateur Web : Mozilla Firefox 32 (ou supériorité), Google Chrome 37 (ou supériorité), Opera 24 (ou supérieure), ou Microsoft Internet Explorer 11 (ou supériorité).

■ **Installer le contrôleur logiciel Omada**

Téléchargez le fichier d'installation d'Omada Software Controller à partir du site Web. Vérifiez les conditions préalables et suivez les étapes en fonction de votre version de fichier pour installer le contrôleur.

• Conditions préalables à l'installation

Pour installer avec succès le contrôleur logiciel Omada, assurez-vous d'avoir effectué les tâches suivantes avant votre installation :

1. Assurez-vous que l'environnement Java Runtime (JRE) a été installé dans votre système. Le contrôleur exige que le système ait Java 8 installé. Téléchargez le fichier en fonction de votre système d'exploitation à partir du site web et suivez les conditions à l'installation

   Instructions pour installer le JRE.

   Pour Ubuntu16.04 ou supérieure, vous pouvez utiliser la commande : **apt-get installer openjdk-8-jre-headless** pour obtenir le Java 8 installé.
2. Assurez-vous que MongoDB a été installé dans votre système. Le contrôleur fonctionne lorsque le système exécute MongoDB 3.0.15–3.6.18. Téléchargez le fichier selon votre système d'exploitation à partir du site Web et suivez les instructions pour installer le MongoDB.
3. Assurez-vous que vous avez **jsvc** et **curl** installé dans votre système avant l'installation, ce qui est vital pour le bon fonctionnement du système. Si votre système n'a pas **jsvc** ou **curl** installé, vous pouvez l'installer manuellement avec la commande: **apt-get installer** ou **yum installer**. Par exemple, vous pouvez utiliser la commande : **apt-get installer jsvc** ou **yum installer jsvc** pour obtenir **jsvc** installé. Et si des dépendances sont manquantes, vous pouvez utiliser la commande : **apt-get -f installer** pour résoudre le problème.

• Installer le fichier.**tar.gz**

1. Assurez-vous que votre PC fonctionne en mode racine. Vous pouvez utiliser cette commande pour entrer en mode racine : **sudo**
2. Extraire le fichier tar.gz à l'aide de la commande :
   tar zxvf Omada_Controller_v4.1.5_linux_x64_targz.tar.gz
3. Installez le contrôleur Omada à l'aide de la commande :
   sudo bash ./install.sh

• **Installer le .deb file**

1. Assurez-vous que votre PC fonctionne en mode racine. Vous pouvez utiliser cette commande pour entrer en mode racine : **sudo**
2. Installer le fichier .**deb** à l'aide de la commande :
   dpkg -i Omada_Controller_v4.1.5_linux_x64.deb

   Si des dépendances sont manquantes pendant l'installation, vous pouvez utiliser la commande : **installation apt-fix-broken** pour résoudre le problème.

Après l'installation du contrôleur, utilisez les commandes suivantes pour vérifier et modifier l'état du contrôleur.

1. Pour démarrer le contrôleur, utiliser la commande. **tpeap start**
2. Pour démarrer le contrôleur, utiliser la commande. **tpeap**
3. Pour afficher l'état du contrôleur **stop tpeap status**

Note:

- Pour installer le.**tar.gz**, si vous souhaitez que le contrôleur Omada s'exécute en tant qu'utilisateur (il s'exécute comme racine par défaut), vous devez modifier OMADA_ valeur USER dans bin/control.sh.
- Pour désinstaller le contrôleur Omada, accédez au chemin d'installation : **/opt/tplink/EAPController**, puis exécutez la commande : **sudo bash ./désinstallez. Sh.**
- Lors de la désinstallation, vous pouvez choisir de sauvegarder ou non la base de données. Le dossier de sauvegarde est **/opt/tplink/eap_db_backup**.
  - Pendant l'installation, on vous demandera s'il faut restaurer la base de données s'il y a une base de données de sauvegarde dans le dossier **/opt/tplink/ eap_db_backup**

2. 1. 3 Démarrer et se connecter au contrôleur logiciel Omada

Lancez omada Software Controller et suivez les instructions pour compléter les configurations de base, puis vous pouvez vous connecter à l'interface de gestion.

Lancer le contrôleur logiciel Omada

Double-cliquez sur l'icône et la fenêtre suivante apparaîtra. Vous pouvez cliquer sur Masquer pour masquer ne le fermez pas. Après un certain temps, votre navigateur Web s'ouvre automatiquement.



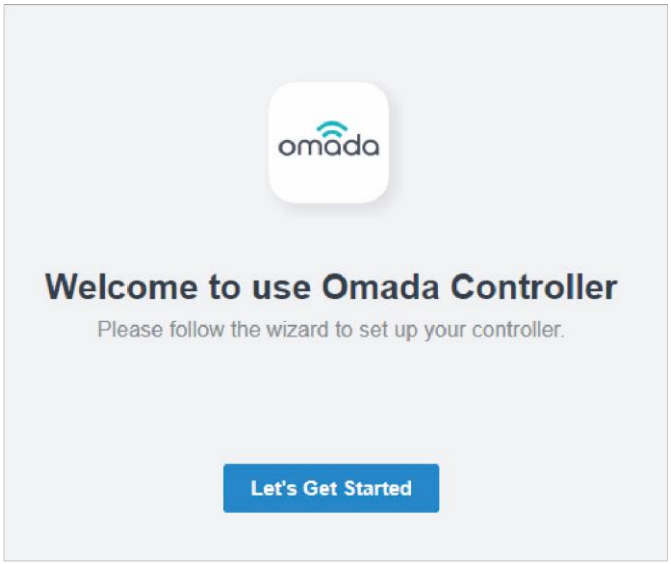
Note:

- Si votre navigateur ne s'ouvre pas automatiquement, cliquez sur Lancer un navigateur pour gérer le réseau. Vous pouvez également lancer un navigateur Web et entrer **http://127.0.0.1:8088** dans la barre d'adresses.
- Si votre navigateur Web s'ouvre mais provoque un problème avec le certificat de sécurité du site Web, cliquez sur Continuer.
- Un seul contrôleur Omada peut s'exécuter dans un réseau local. Si un contrôleur Omada s'exécute déjà sur un hôte qui se trouve dans votre réseau local, vous serez redirigé vers l'interface Du contrôleur Omada sur cet hôte.

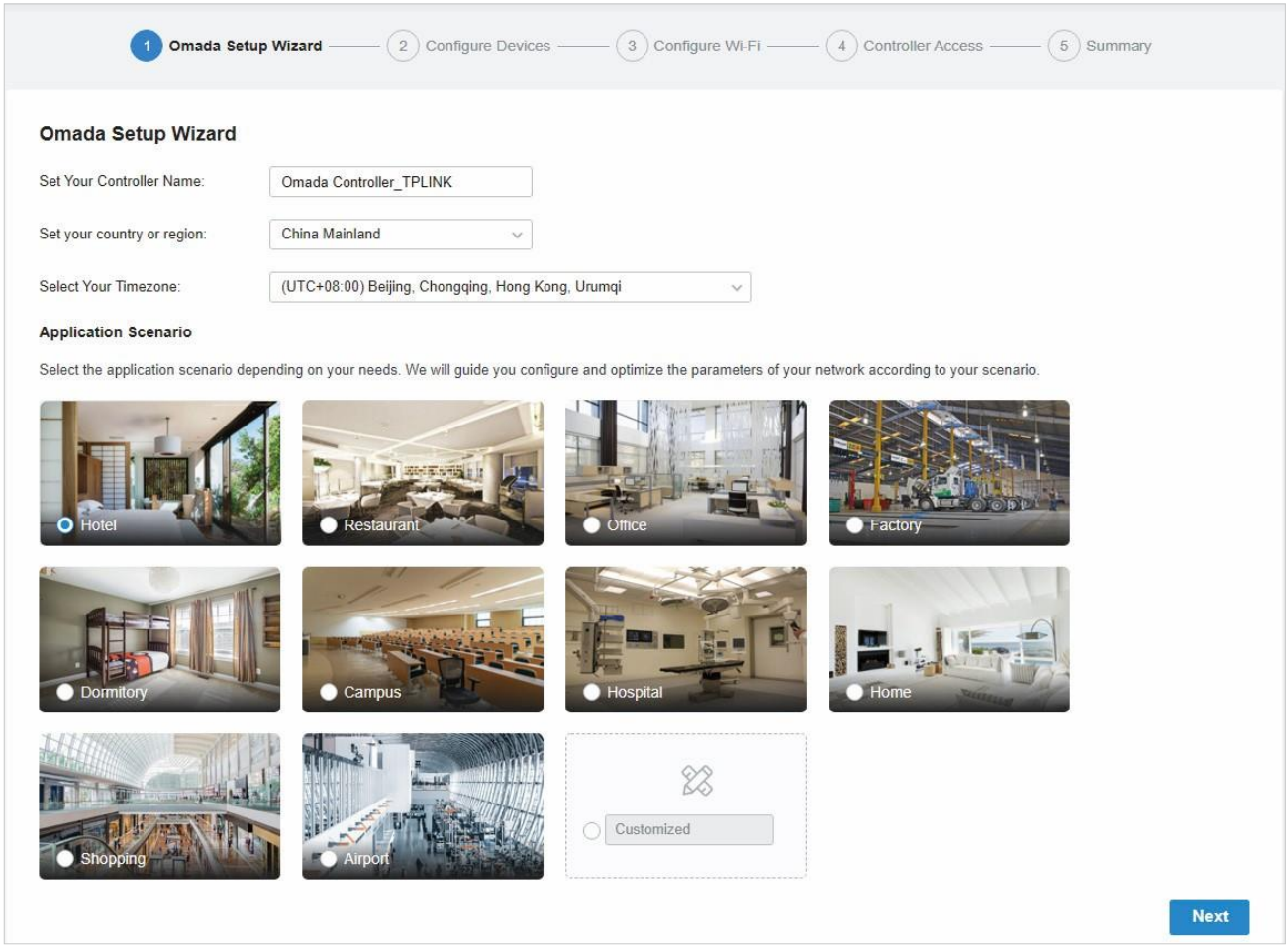
Effectuer les configurations de base

Dans le navigateur Web, vous pouvez voir la page de configuration. Suivez l'Assistant Configuration pour terminer les paramètres de base du contrôleur Omada.

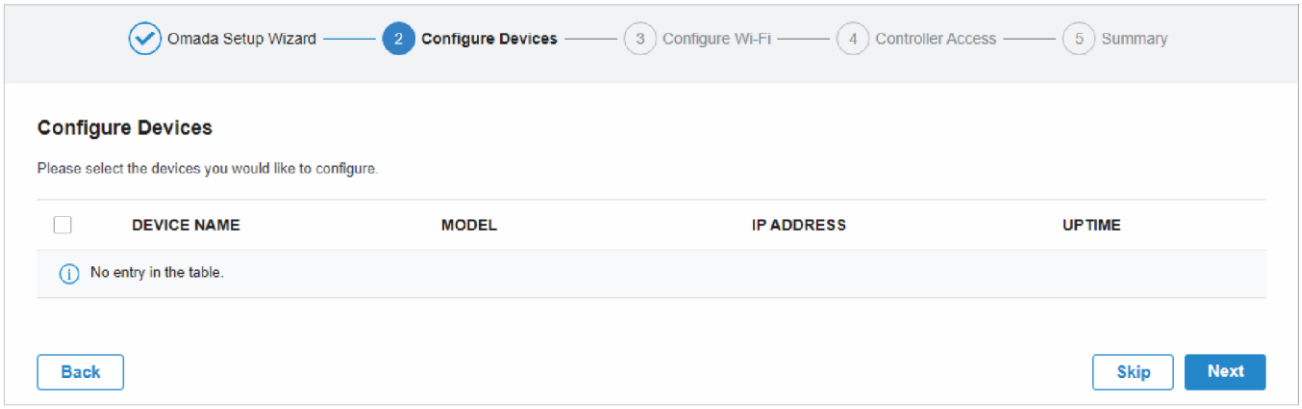
1. Cliquez sur Let's Get Started.



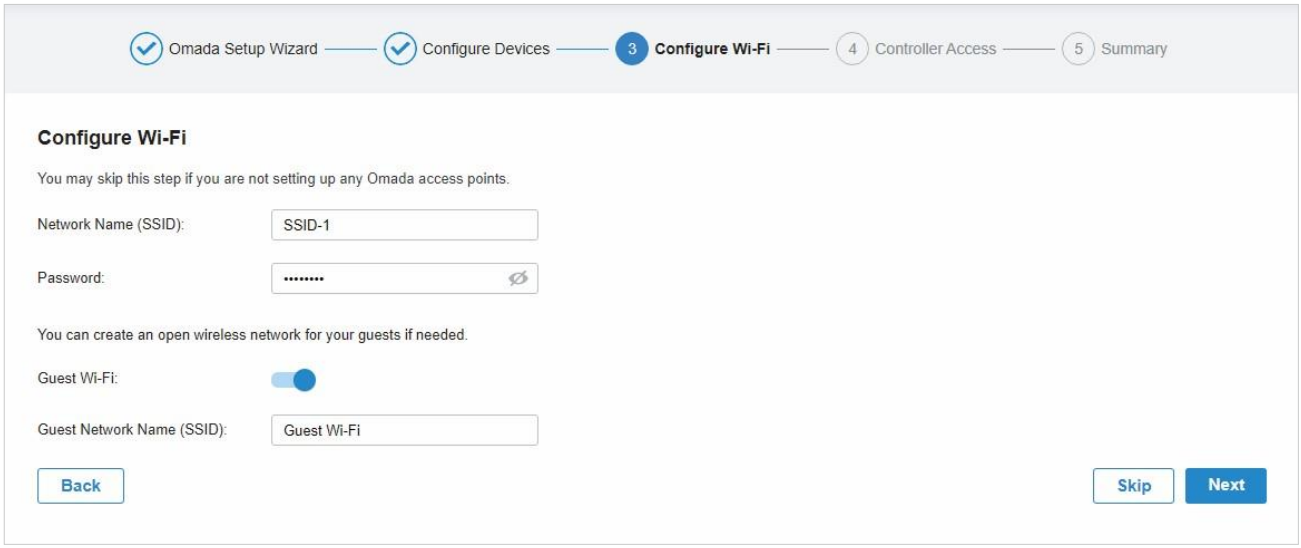
2. Spécifiez un nom pour Le contrôleur Omada et définissez votre région et votre fuseau horaire. Sélectionnez ensuite le scénario de l'application en fonction de vos besoins. Cliquez sur Next.



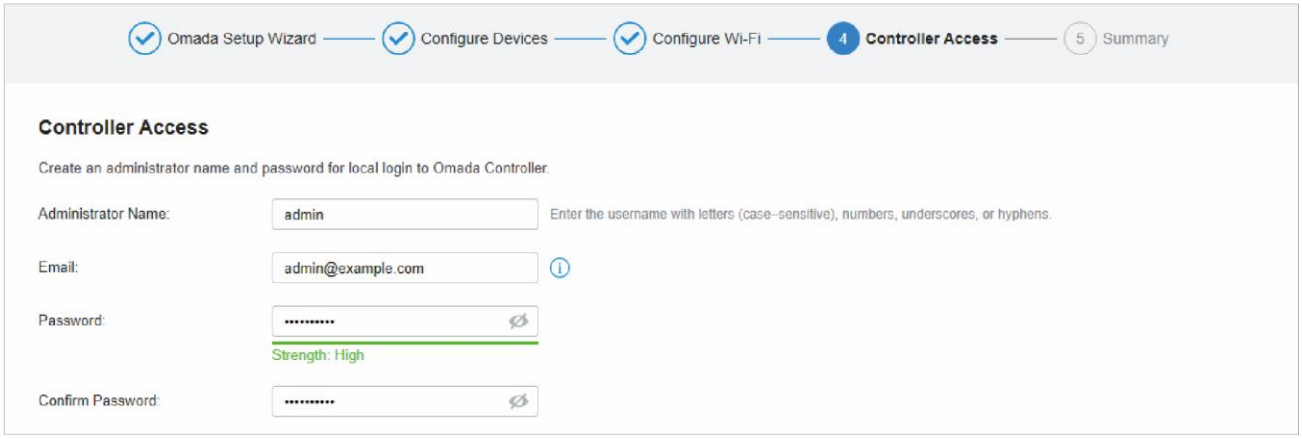
3. La page d'installation affiche tous les périphériques découverts dans le réseau. Sélectionner un ou plusieurs appareils à gérer et cliquer sur Next.



4. Définissez un nom de réseau sans fil (SSID) et un mot de passe pour que les EAP soient gérés. Omada Controller créera deux réseaux sans fil, un 2,4 GHz et un 5GHz, tous deux cryptés en mode WPA-Personal. Vous pouvez définir le Wi-Fi invité pour fournir un accès Wi-Fi ouvert aux clients sans divulguer votre réseau principal si nécessaire. Cliquez sur Next.

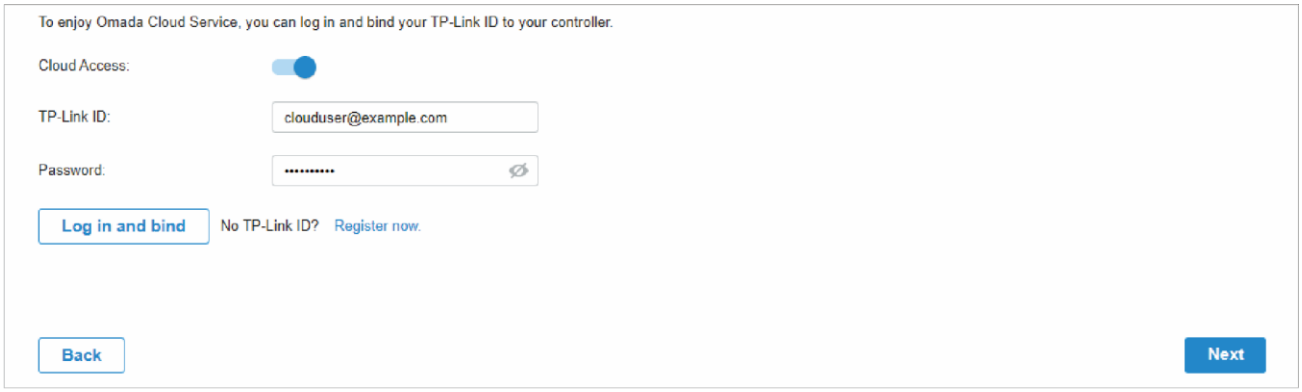


5. Définissez un nom d'utilisateur et un mot de passe pour le compte de connexion. Spécifiez l'adresse e-mail pour réinitialiser votre mot de passe au cas où vous oublieriez le mot de passe. Après vous être connecté à Omada Controller, définissez un serveur de messagerie pour que vous puissiez recevoir des e-mails et réinitialiser votre mot de passe. Pour définir un serveur de messagerie, reportez-vous à Notifications.

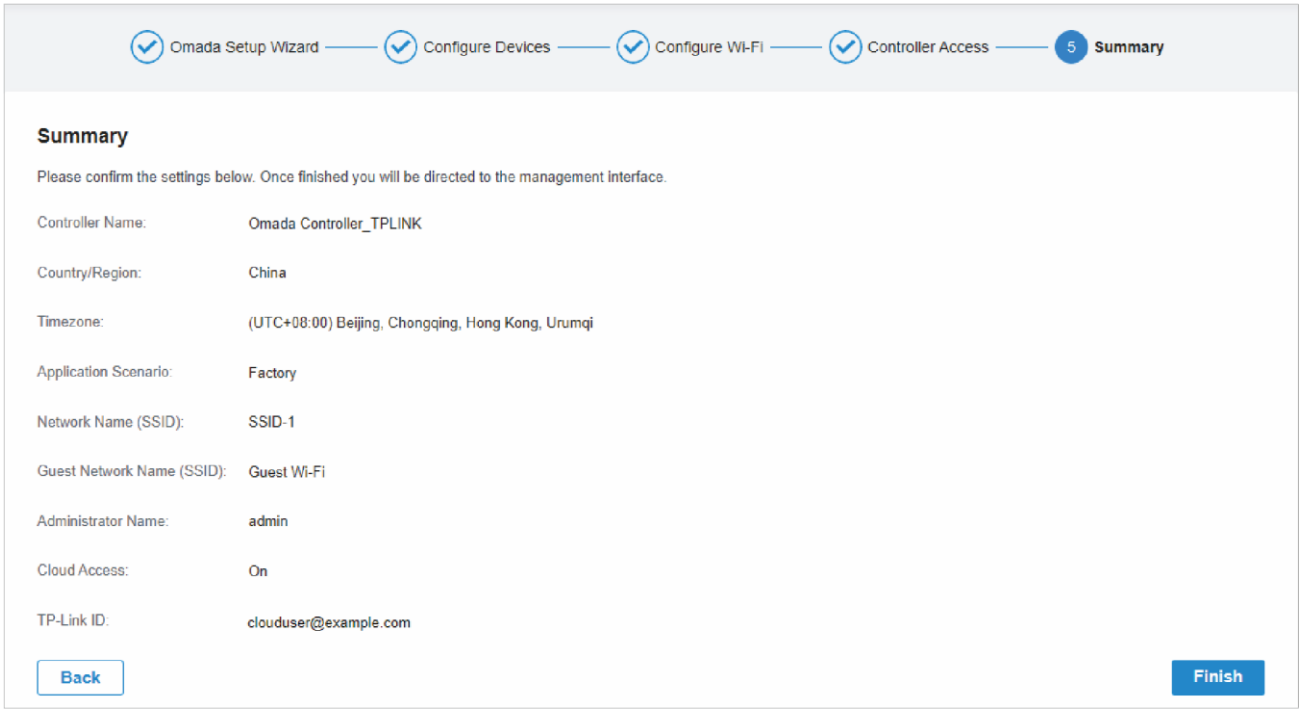


6. Si vous souhaitez accéder au contrôleur pour gérer les réseaux à distance, activer le bouton Cloud Access et lier votre ID TP-Link à votre contrôleur Omada, puis cliquez sur Next. Si ce n'est pas le cas, cliquez sur Next Directement.

   Pour plus de détails sur Omada Cloud, Omada Cloud Service.

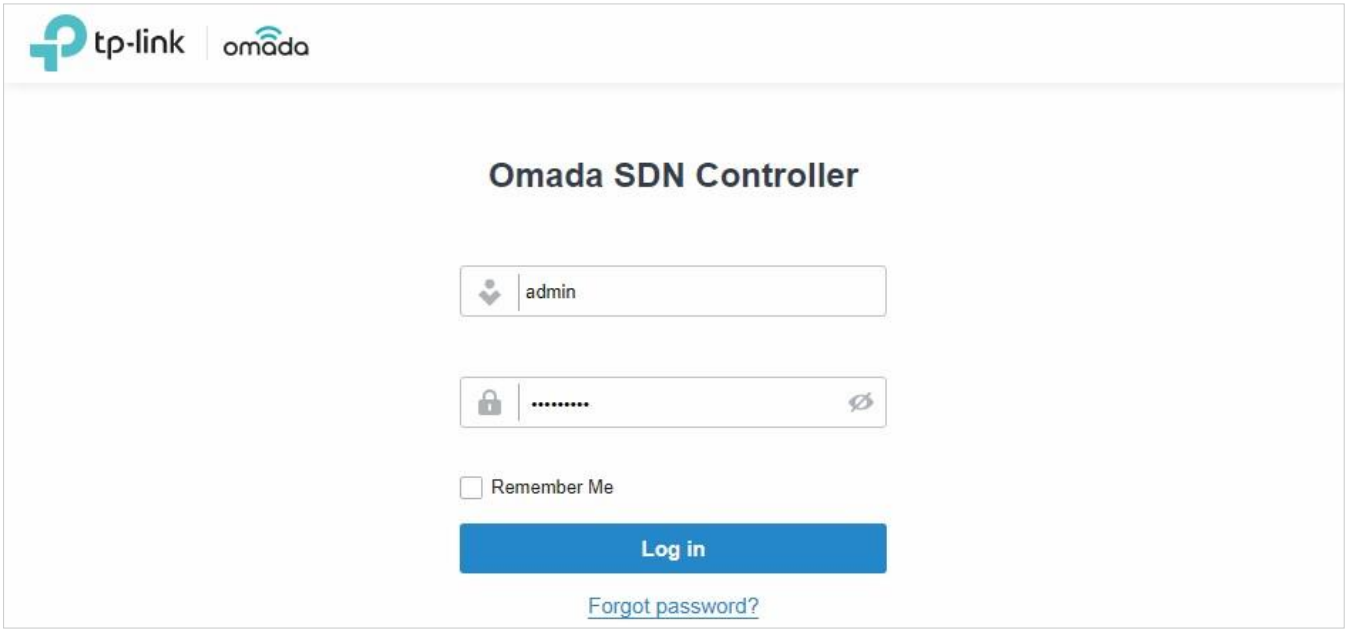


7. Examiner vos paramètres et cliquer sur Finish.



Connectez-vous à l'interface de gestion

Une fois les configurations de base terminées, le navigateur sera redirigé vers la page suivante. Connectez-vous à l'interface de gestion à l'aide du nom d'utilisateur et du mot de passe que vous avez défini dans les configurations de base.



Note:

En plus de l'hôte contrôleur, d'autres hôtes du même réseau local peuvent également gérer les EAP via un accès à distance à l'hôte du contrôleur. Par exemple, si l'adresse IP de l'hôte contrôleur est 192.168.0.100 et que le contrôleur Omada s'exécute normalement sur cet hôte, vous pouvez entrer https://192.168.0.100:8043 ou http://192.168.0.100:8088 dans le navigateur Web d'autres hôtes du même réseau local pour vous connecter au contrôleur Omada et gérer les EAP. Vous pouvez également vous connecter à Omada Controller à l'aide d'autres périphériques de gestion via le service Omada Cloud.

2. 2 Configurer votre contrôleur matériel

La solution de contrôleur Omada SDN est conçue pour les réseaux évolutifs. Les déploiements et les configurations varient selon les situations réelles. Comprendre vos besoins réseau est la première étape lors de la planification de la fourniture d'un projet. Une fois que vous avez identifié ces exigences, suivez les étapes ci-dessous pour configurer initialement Omada Hardware Controller :

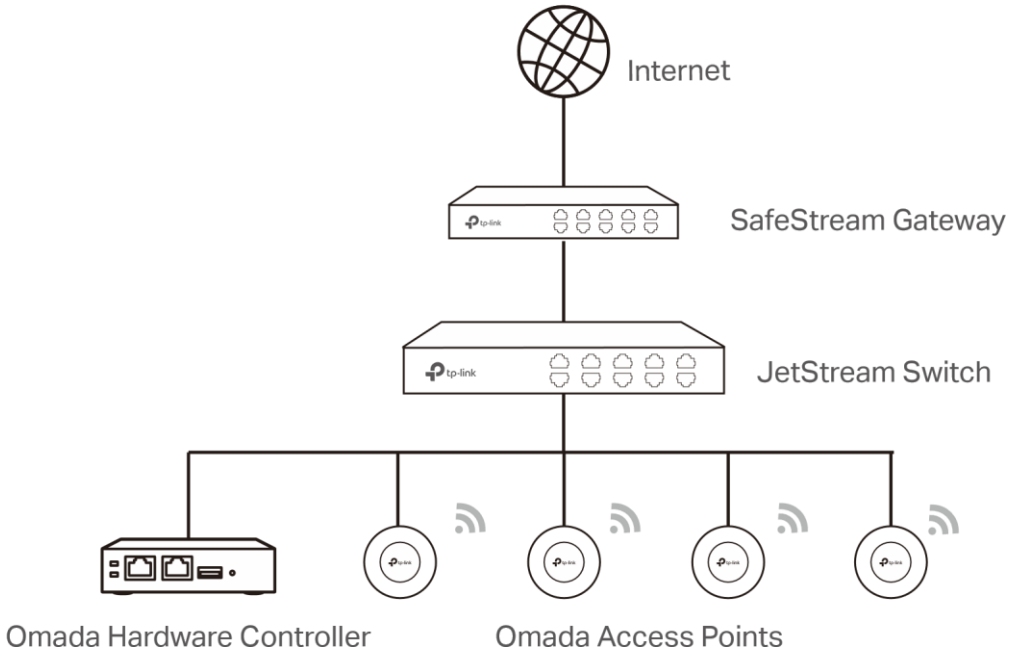
1) Déterminer la topologie du réseau.

2) Déployez le contrôleur matériel Omada.

3) Démarrer et connectez-vous au contrôleur.

2. 2. 1 Déterminer la topologie réseau

La topologie réseau que vous créez pour le contrôleur SDN Omada varie en fonction des besoins de votre entreprise. La figure suivante montre une topologie typique pour un cas d'utilisation à haute disponibilité.



Note:

Lorsque vous utilisez le contrôleur Omada SDN, nous vous recommandons de déployer la topologie Omada complète avec des périphériques TP-Link pris en charge. Si vous utilisez des appareils tiers, le contrôleur SDN Omada ne peut pas les découvrir et les gérer.

2. 2. 2 Déployer le contrôleur matériel Omada

Le Omada Hardware Controller est livré avec le logiciel de contrôleur pré-installé, de sorte que l'installation n'est pas nécessaire. Après avoir déployé omada Hardware Controller sur votre infrastructure réseau, procédez à la configuration du contrôleur.

2. 2. 3 Démarrer et se connecter au contrôleur

Connectez-vous à l'interface de gestion

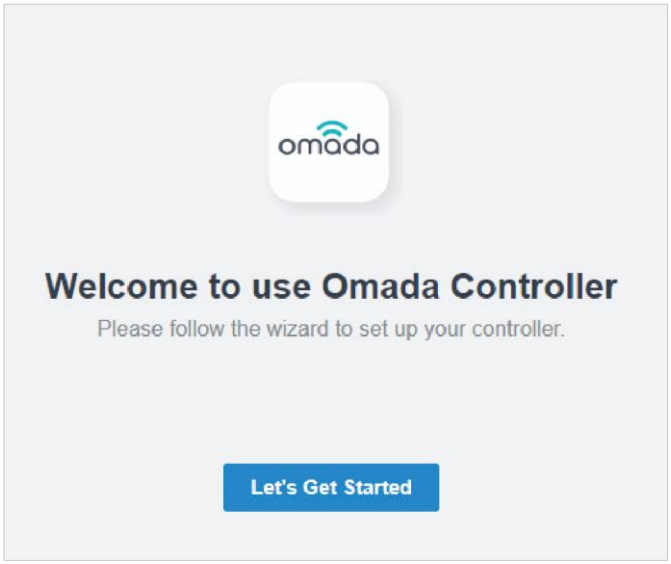
Suivez les étapes ci-dessous pour entrer dans l'interface de gestion d'Omada Hardware Controller :

1. Assurez-vous que votre périphérique de gestion dispose de l'itinéraire pour accéder au contrôleur.
2. Vérifiez le serveur DHCP (généralement un routeur) pour l'adresse IP du contrôleur. Si le contrôleur ne parvient pas à obtenir une adresse IP dynamique à partir du serveur DHCP, l'adresse IP de secours par défaut 192.168.0.253 est utilisée.
3. Lancez un navigateur Web et tapez l'adresse IP du contrôleur dans la barre d'adresses, puis appuyez sur **Entrée** (Windows) ou **Retour** (Mac).

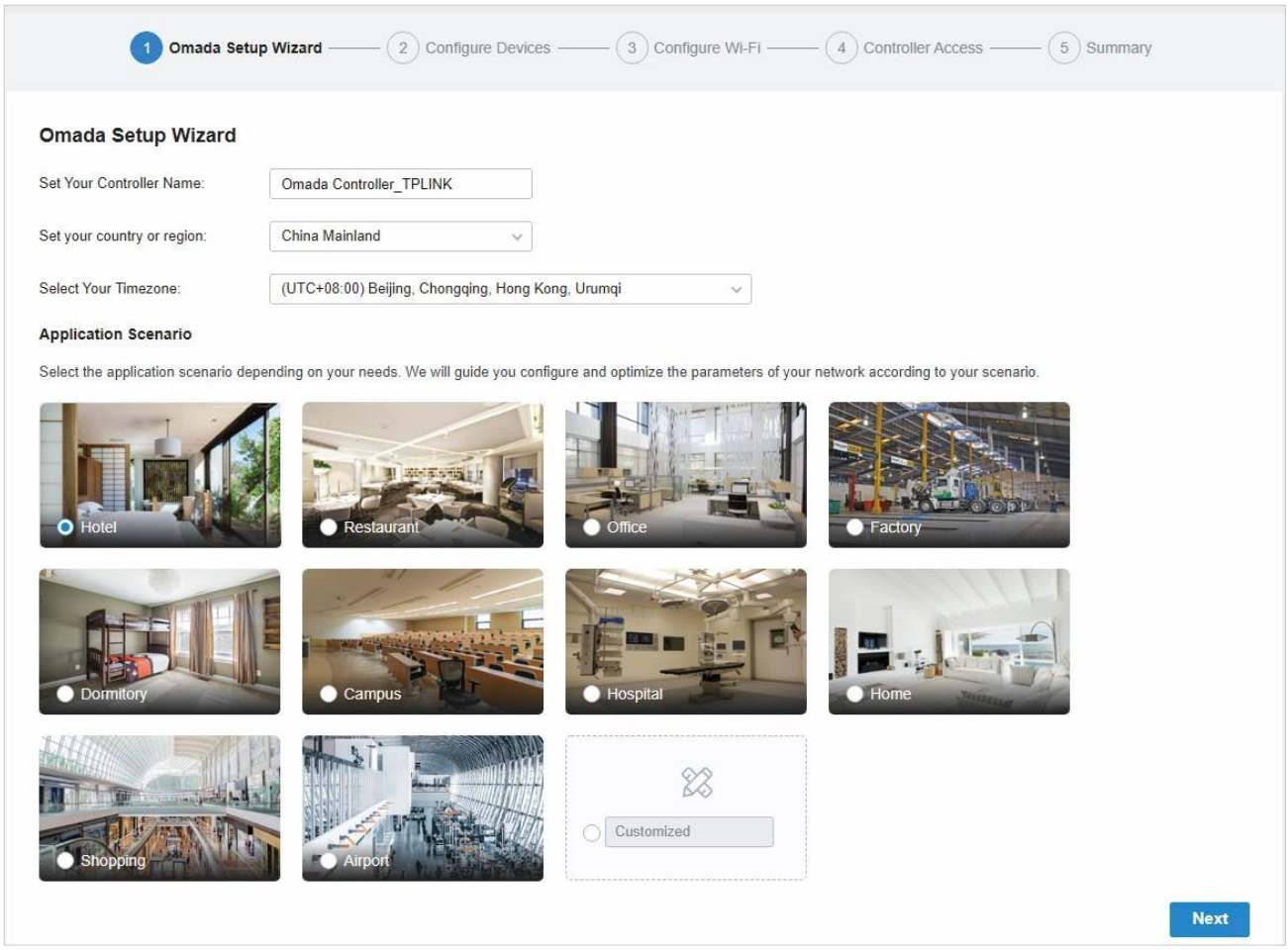
Effectuer les configurations de base

Dans le navigateur Web, vous pouvez voir la page de configuration. Suivez l'Assistant Configuration pour compléter les paramètres de base du contrôleur Omada.

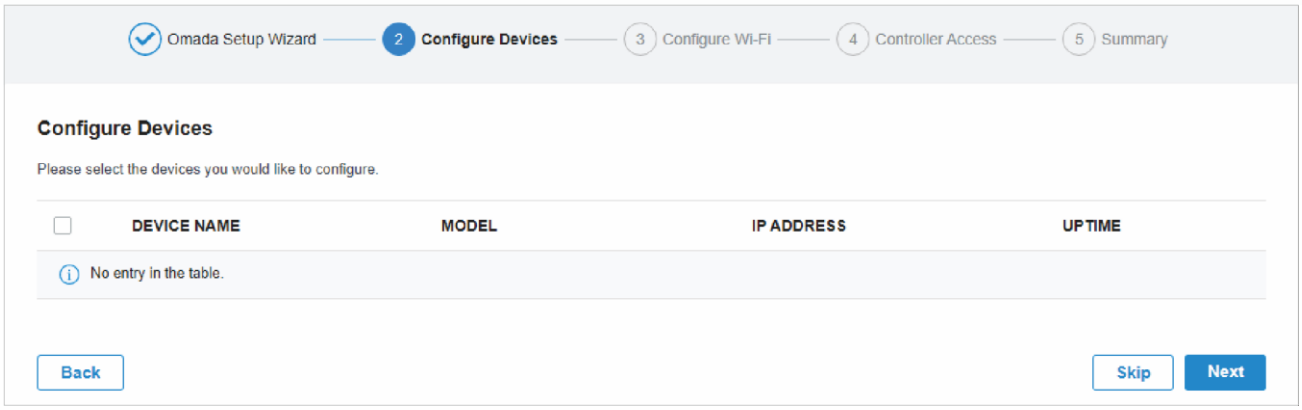
1. Cliquez sur Let's Get Started.



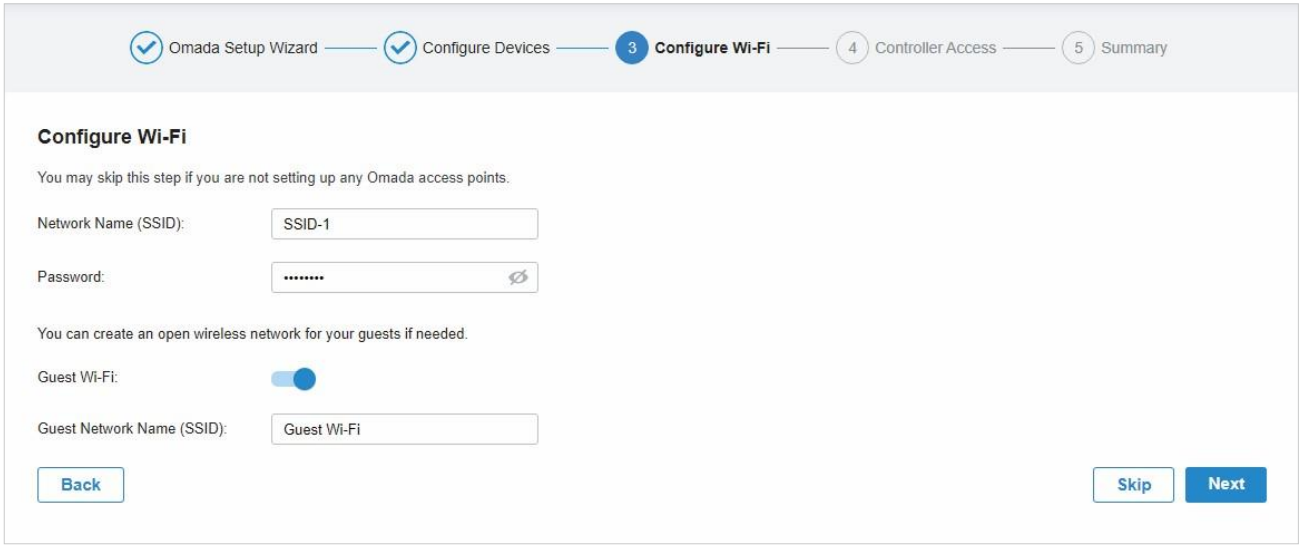
2. Spécifiez un nom pour Le contrôleur Omada et définissez votre région et votre fuseau horaire. Sélectionnez ensuite le scénario de l'application en fonction de vos besoins. Cliquez sur Next.



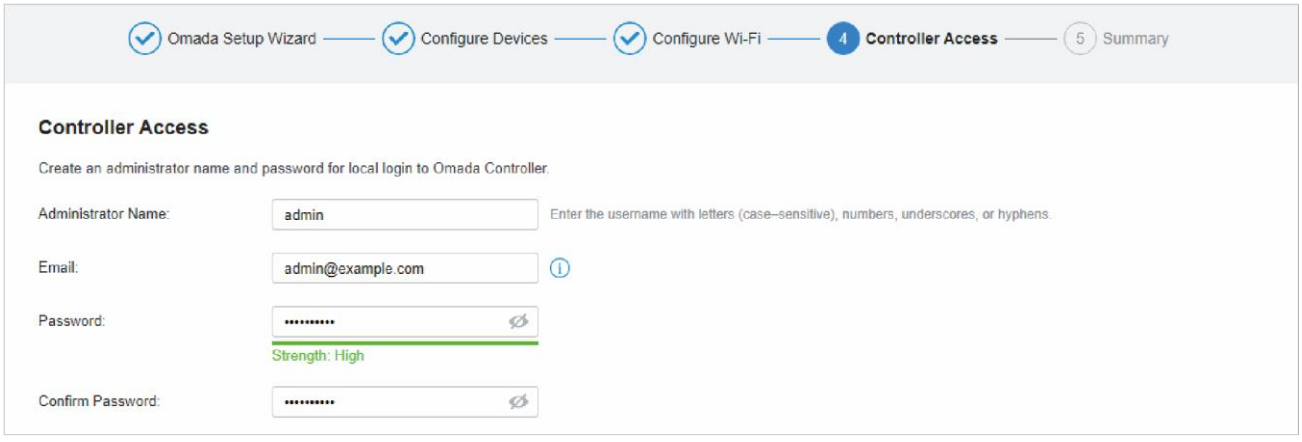
3. La page d'installation affiche tous les périphériques découverts dans le réseau. Sélectionner un ou plusieurs appareils à gérer et cliquer sur Next.



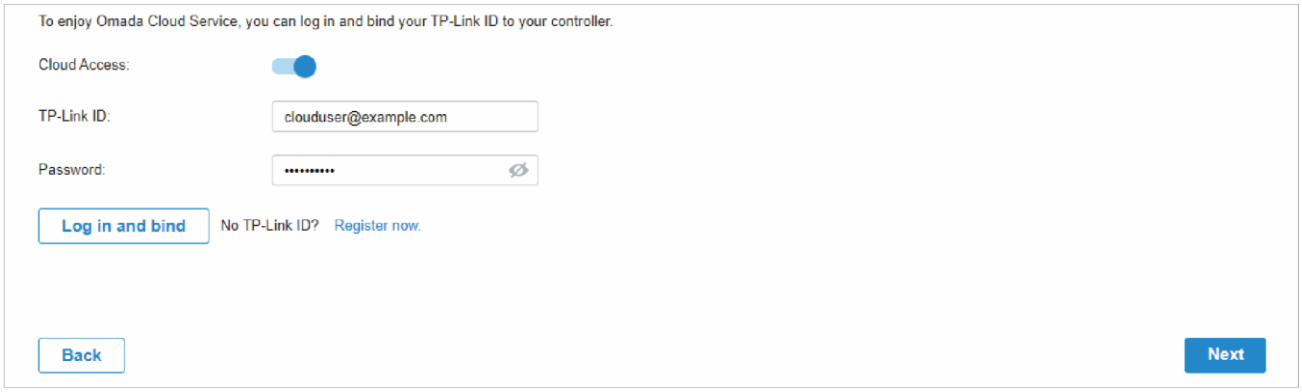
4. Définissez un nom de réseau sans fil (SSID) et un mot de passe pour que les EAP soient gérés. Omada Controller créera deux réseaux sans fil, un 2,4 GHz et un 5GHz, tous deux cryptés en mode WPA-Personal. Vous pouvez définir le Wi-Fi invité pour fournir un accès Wi-Fi ouvert aux clients sans divulguer votre réseau principal si nécessaire. Cliquez sur Next.



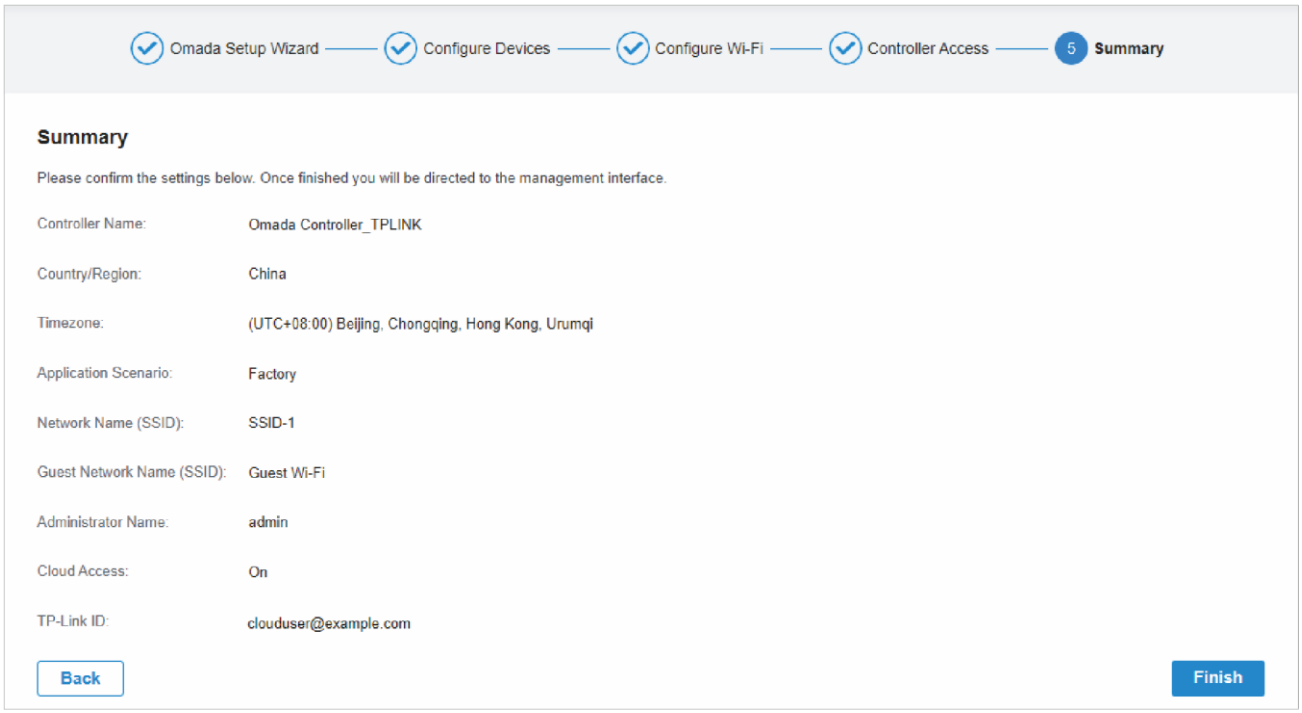
5. Définissez un nom d'utilisateur et un mot de passe pour le compte de connexion. Spécifiez l'adresse e-mail pour réinitialiser votre mot de passe au cas où vous oublieriez le mot de passe. Après vous être connecté à Omada Controller, définissez un serveur de messagerie pour que vous puissiez recevoir des e-mails et réinitialiser votre mot de passe. Pour définir un serveur de messagerie, reportez-vous à Notifications.



6. Si vous souhaitez accéder au contrôleur pour gérer les réseaux à distance, activez le bouton « Cloud Access » et lier (Log in and Bind) à votre ID TP-Link votre contrôleur Omada, puis cliquez sur Next.
Si ce n'est pas le cas, cliquez directement sur Suivant. Pour plus de détails sur Omada Cloud, veuillez consulter Omada Cloud Service.

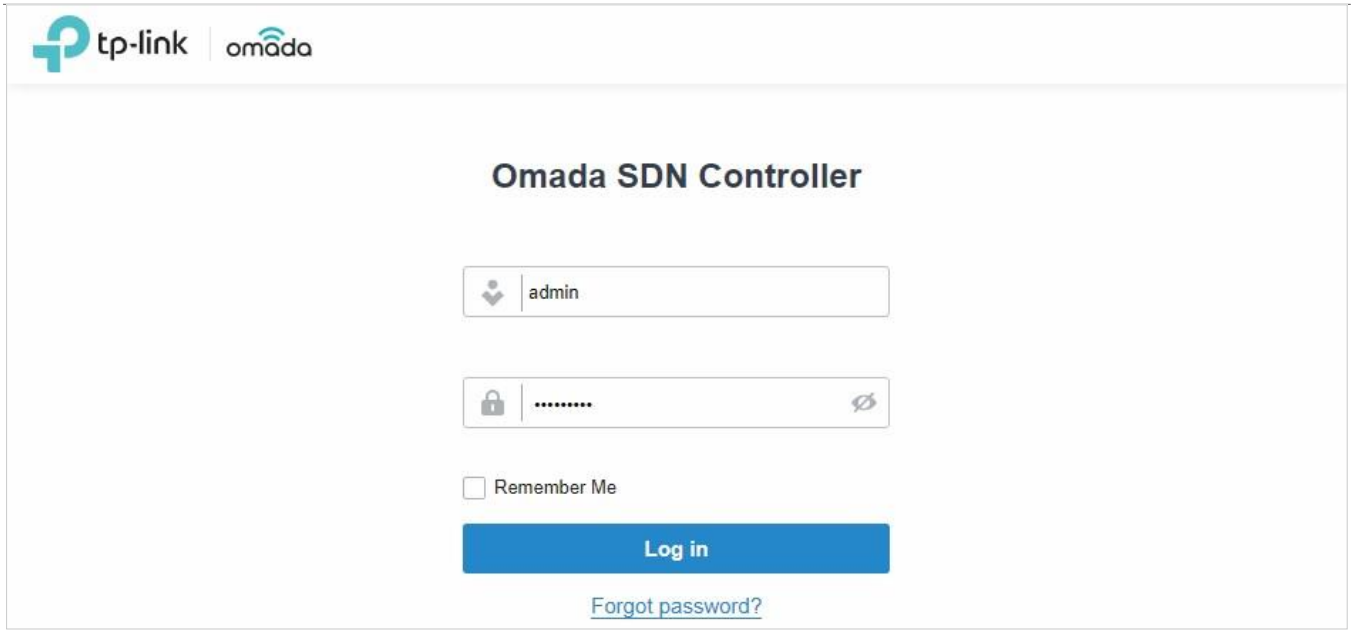


7. Examiner vos paramètres et cliquer sur Finish.



Connectez-vous à l'interface de gestion

Une fois les configurations de base terminées, le navigateur sera redirigé vers la page suivante. Connectez-vous à l'interface de gestion à l'aide du nom d'utilisateur et du mot de passe que vous avez défini dans les configurations de base.



Note:

En plus de l'hôte contrôleur, d'autres hôtes du même réseau local peuvent également gérer les EAP via un accès à distance à l'hôte du contrôleur. Par exemple, si l'adresse IP de l'hôte contrôleur est 192.168.0.100 et que le contrôleur Omada s'exécute normalement sur cet hôte, vous pouvez entrer https://192.168.0.100:8043 ou http://192.168.0.100:8088 dans le navigateur Web d'autres hôtes du même réseau local pour vous connecter au contrôleur Omada et gérer les EAP. Vous pouvez également vous connecter à Omada Controller à l'aide d'autres périphériques de gestion via le service Omada Cloud.

2. 3 Configurer votre contrôleur cloud

La solution de contrôleur Omada SDN est conçue pour les réseaux évolutifs. Les déploiements et les configurations varient selon les situations réelles. Comprendre vos besoins réseau est la première étape lors de la planification de la fourniture d'un projet. Une fois que vous avez identifié ces exigences, suivez les étapes ci-dessous pour configurer initialement le contrôleur cloud Omada :

1.) Créez un ID TP-Link.

2.) Abonnez-vous au service Cloud d'Omada.

1) Démarrer et se connecter au contrôleur.

Les étapes de configuration d'Omada Cloud sont similaires à Omada Software Controller, Start and Log In to the Omada Software Controller pour obtenir des informations détaillées.

3

Gérer les périphériques et sites gérés par Omada

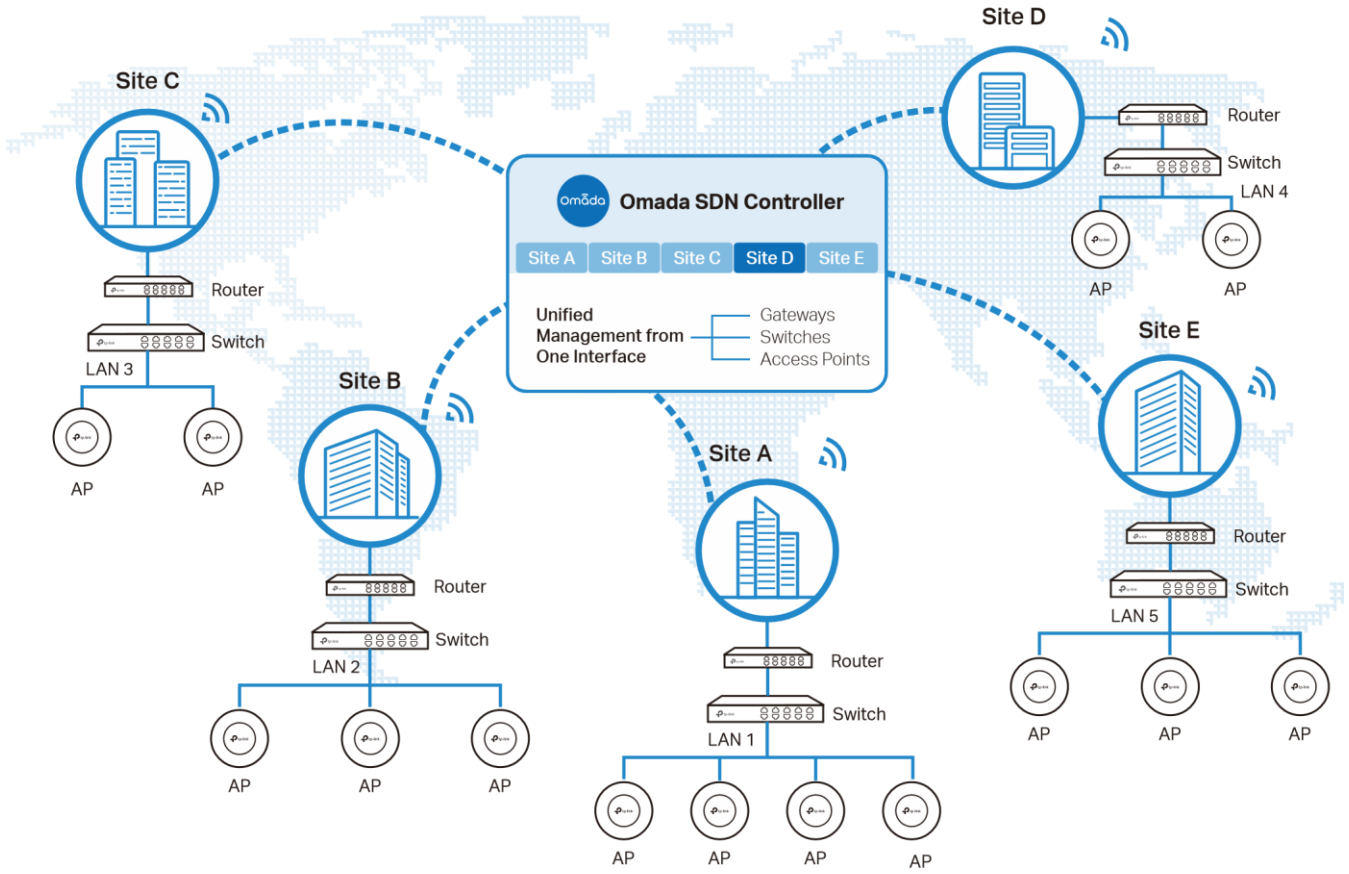
Commencez à gérer votre réseau en créant des sites et en adoptant des périphériques afin que vous puissiez configurer et surveiller vos appareils de manière centralisée tout en gardant les choses organisées. Le chapitre comprend les sections suivantes :

1. Créer des sites
2. Adopter des appareils

3. 1 Créer des sites

Aperçu

Différents sites sont logiquement séparés, comme différentes filiales ou départements. Il est de pratique de créer un site pour chaque réseau local (Local Area Network) et d'ajouter tous les périphériques du réseau au site, y compris le routeur, les commutateurs et les points d'accès.



Les périphériques d'un site ont besoin de configurations unifiées, tandis que celles de différents sites ne sont pas relatives. Pour tirer le meilleur parti d'un site, configurez simultanément des fonctionnalités pour plusieurs appareils sur le site, tels que la planification VLAN et PoE pour les commutateurs, et la planification SSID et WLAN pour les AP, plutôt que de les configurer un par un.

Configuration

Pour créer et gérer un site, procédez comme suit :

1.) Créer un site.

2.) Afficher et modifier le site.

3.) Allez sur le site.

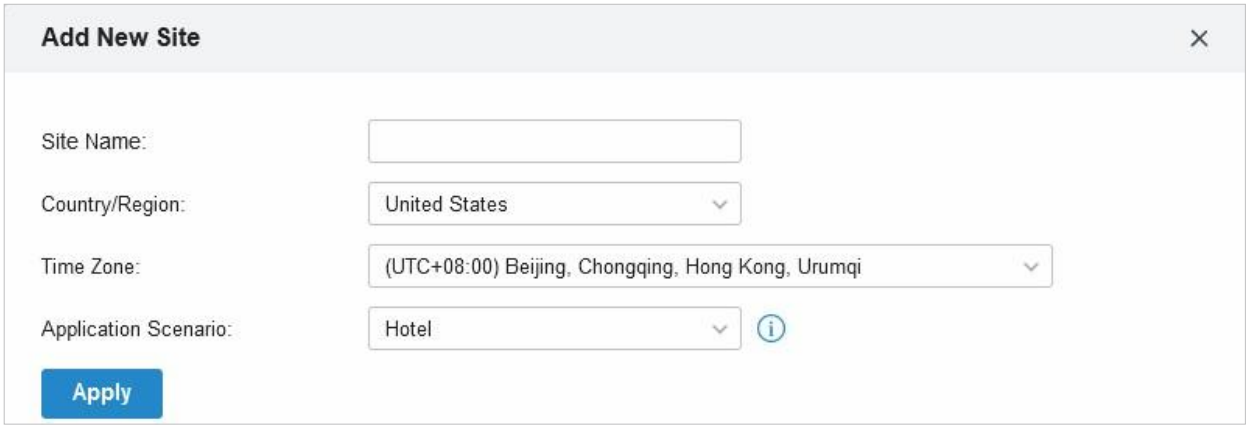


Pour créer un site, choisissez-en une parmi les méthodes suivantes en fonction de vos besoins.

- **Créer un site à partir de zéro**

  1. Cliquez sur + Add New Site dans la liste déroulante des Sites. Sinon, cliquez sur Site Manager dans la liste déroulante des Sites et cliquez sur ⊕ dans la page deSite Management

2. Entrez un Site Name pour identifier le site et configurer d'autres paramètres en fonction de l'emplacement du site. Cliquez ensuite sur Apply. Le nouveau site est ajouté à la liste déroulante des Sites, et la table dans la page de Site Management .



■ **Copier un site existant**

Vous pouvez rapidement créer un site basé sur un site existant en copiant sa configuration de site, sa configuration câblée et sa configuration sans fil, entre autres. Après cela, vous pouvez modifier avec souplesse la nouvelle configuration du site pour la rendre différente de l'ancienne.

1. Cliquez sur Site Manager dans la liste déroulante des Sites. dans la page de Site Management, Cliquez sur dans la colonne ACTION du site que vous souhaitez copier.

2. Entrez un Site Name pour identifier le nouveau site. Cliquez sur Apply. Le nouveau site est ajouté à la liste déroulante des Sites, et le tableau dans la page de Site Management.

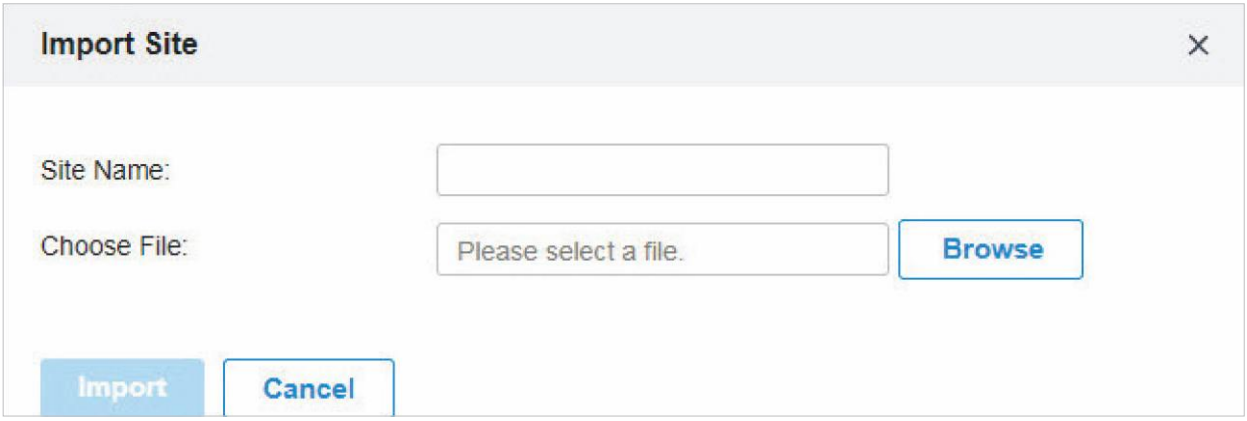


■ **Importer un site à partir d'un autre contrôleur**

Si vous souhaitez migrer en toute transparence d'un ancien contrôleur vers un nouveau contrôleur, importez le fichier de configuration de site de l'ancien contrôleur dans le nouveau. Avant cela, vous devez exporter le fichier de configuration du site à partir de l'ancien contrôleur, qui est couvert par Site Migration.

1. Cliquez sur Import Site dans la liste déroulante des Sites. Sinon, cliquez sur Site Manager dans la liste déroulante de Sites et cliquez sur dans la page de Site Management.

2. Entrez un Site Name pour identifier le site. Parcourez l'explorateur de fichiers et choisissez un fichier de configuration de site. Cliquez sur Import. Le nouveau site est ajouté à la liste déroulante des Sites, et le tableau dans la page de Site Management.



Créer un site → Afficher et modifier le site → Aller sur le site

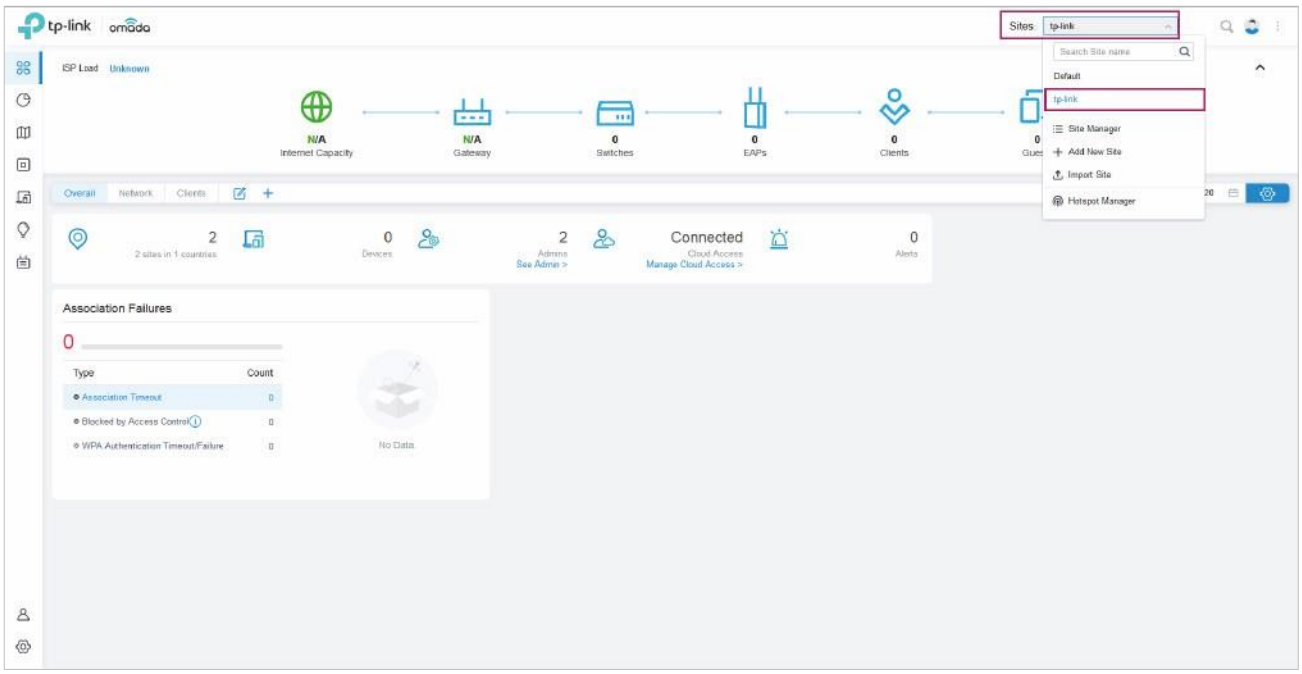
Après avoir créé le site, vous pouvez cliquer sur Site Manager, et afficher l'état du site dans la page de Site Management. vous pouvez cliquer sur dans la colonne ACTION pour modifier la configuration du site.
Vous pouvez cliquer sur dans la colonne ACTION pour supprimer le site.



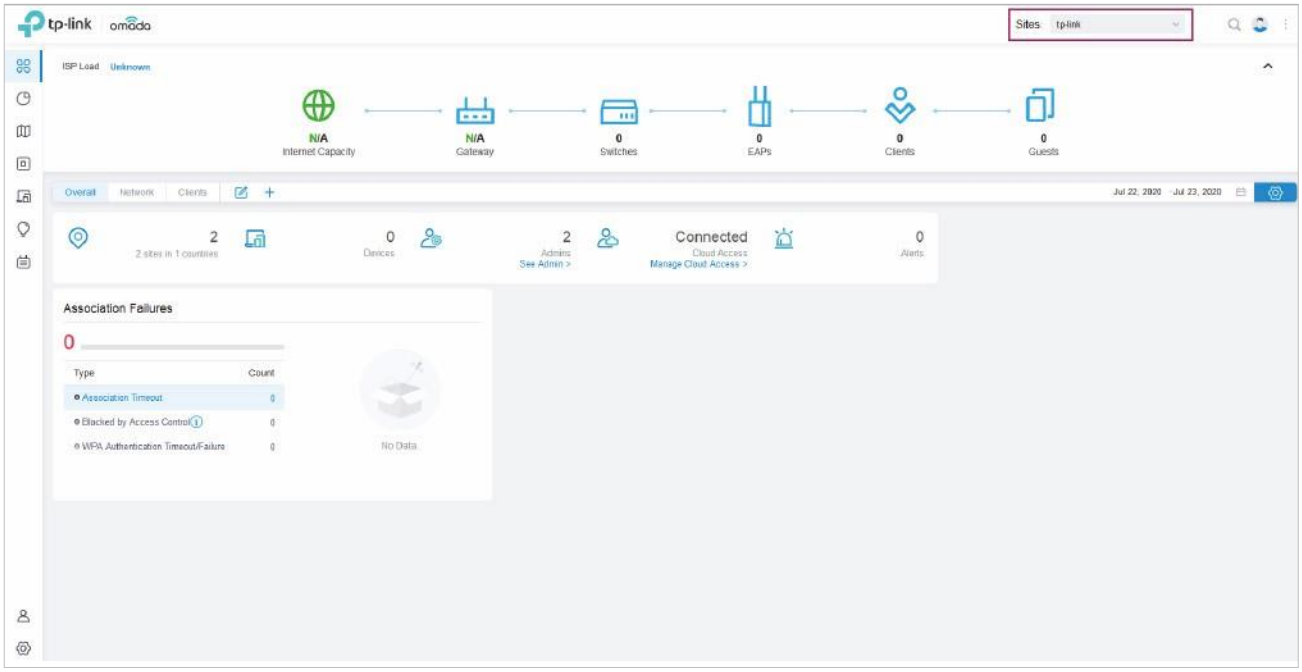
Créer un site → Afficher et modifier le site → Aller sur le site

Pour surveiller et configurer un site, vous devez d'abord aller dans le site.

1. Sélectionnez le site dans la liste déroulante de Sites pour aller sur le site.



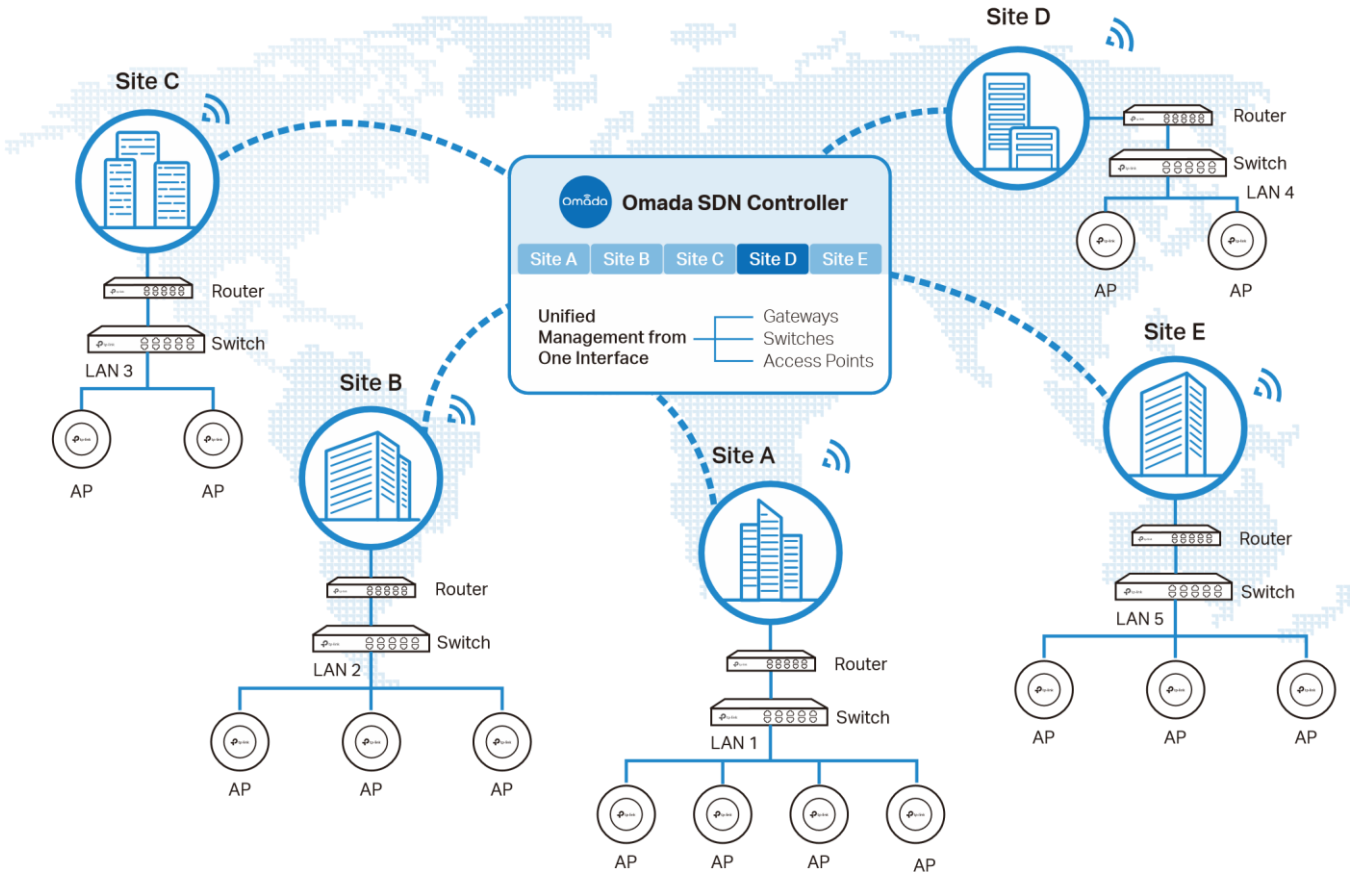
1. Le champ Site indique le site dans lequel vous vous trouvez actuellement. Certains éléments de configuration du menu sont appliqués au site dans lequel vous vous trouvez actuellement, tandis que d'autres sont appliqués à l'ensemble du contrôleur.



3. 2 Adopter des appareils

Aperçu

Après avoir créé un site, ajoutez vos appareils au site en faisant adopter le contrôleur. Assurez-vous que vos périphériques dans chaque réseau local sont ajoutés au site correspondant afin qu'ils puissent être gérés de manière centralisée.



Configuration

Choisissez une procédure selon le type de votre contrôleur :

- Pour Le contrôleur logiciel Omada / Contrôleur matériel Omada
- For Omada Cloud-Based Controller

3. 3. 1 Pour Le contrôleur logiciel Omada / Contrôleur matériel Omada

Pour adopter les périphériques du contrôleur, procédez comme suit :

1.) Préparez-vous à communiquer entre le contrôleur et les appareils.

2.) Préparez-vous à la découverte de l'appareil.

1) Adopter les appareils.



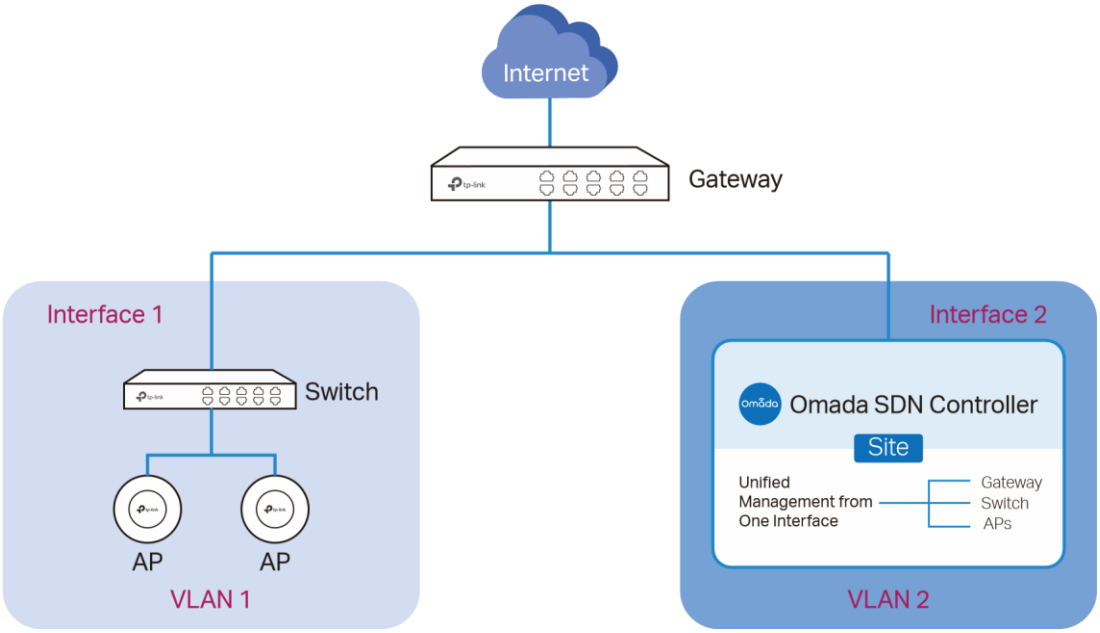
Note:

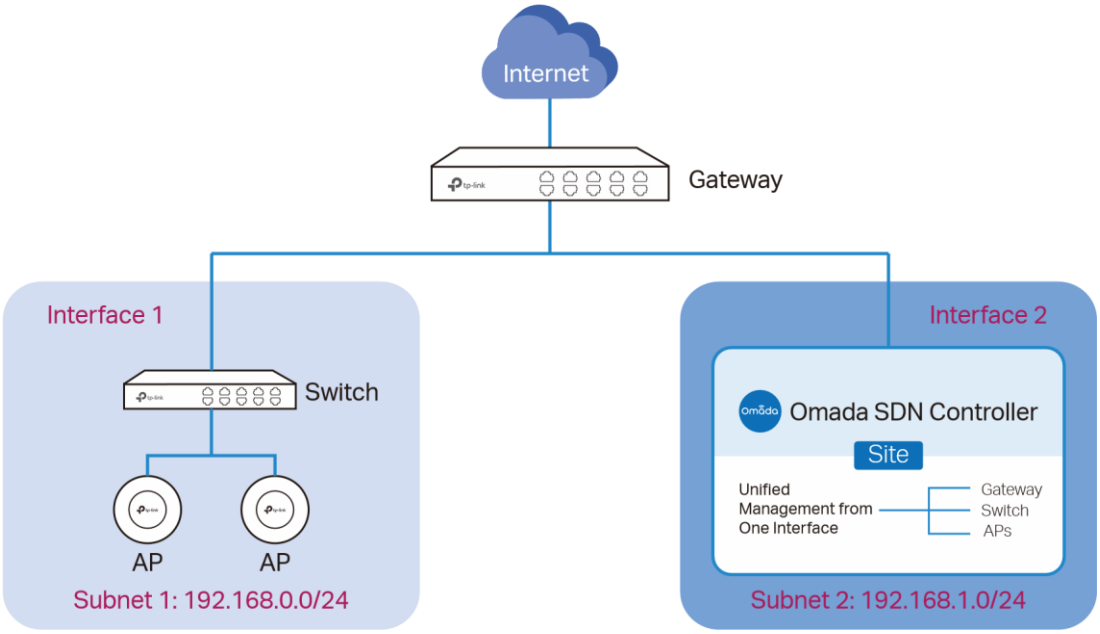
Si le contrôleur et les périphériques se trouvent dans le même réseau local, sous-réseau et VLAN,assurez-vous que le contrôleur peut communiquer avec les appareils. Dans le cas contraire, le contrôleur ne peut pas découvrir ou adopter les appareils par quelque moyen que ce soit. Si le contrôleur et les périphériques se trouvent dans différents LAN, sous-réseaux ou VLANs, utilisez les techniques suivantes pour créer la connexion en fonction de votre scénario.

1. Configurer le réseau

■ Scénario 1 : dans les VLANs ou les sous-réseaux

Comme indiqué dans les chiffres suivants, le contrôleur et les périphériques sont dans différents VLANs ou sous-réseaux. Vous devez configurer une interface IP pour chaque VLAN ou sous-réseau, et assurez-vous que les interfaces peuvent communiquer les unes avec les autres.





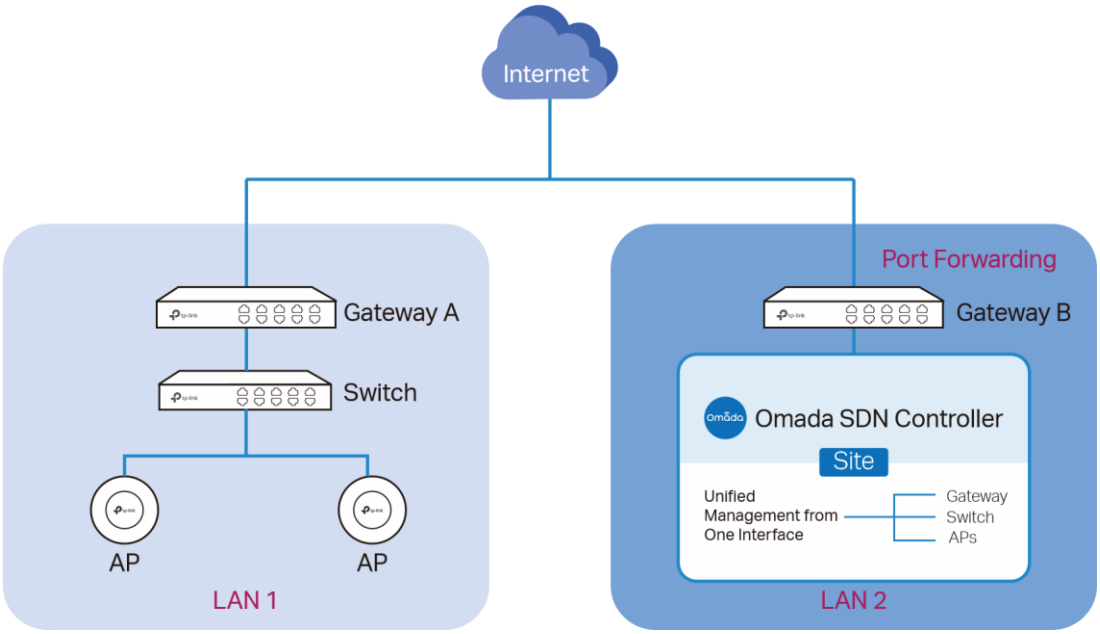
■ Scénario 2: Dans tous les LAN

Comme indiqué dans la figure suivante, le contrôleur et les périphériques sont dans différents LAN. Vous devez établir la communication à travers l'Internet et les passerelles.

Par défaut, les périphériques du RÉSEAU NATIONAL 1 ne peuvent pas communiquer avec le contrôleur dans LAN 2, car la passerelle B se trouve devant le contrôleur et bloque l'accès à celui-ci. Pour rendre le contrôleur accessible aux appareils, vous pouvez utiliser le port de transport ou le VPN.

1. Utiliser le port de forwarding

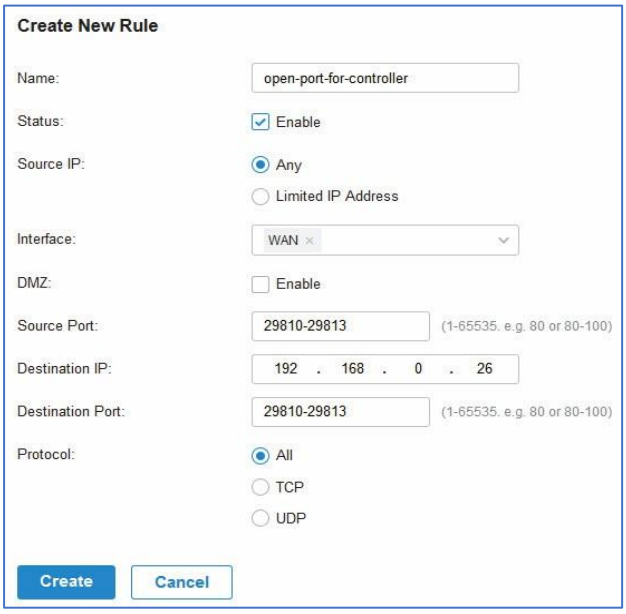
Configurez le port de transmettre sur la passerelle B et le port ouvert 29810-29813 pour le contrôleur, qui sont essentiels pour la découverte et l'adoption de périphériques. Si vous utilisez des pares-feux dans les réseaux, assurez-vous que les pares-feux ne bloquent pas ces ports.



Pour configurer le port de transmettre sur la passerelle B, vous devez d'abord adopter la passerelle B sur le contrôleur. Pour savoir comment adopter la passerelle B, reportez-vous à Adopt the Devices.

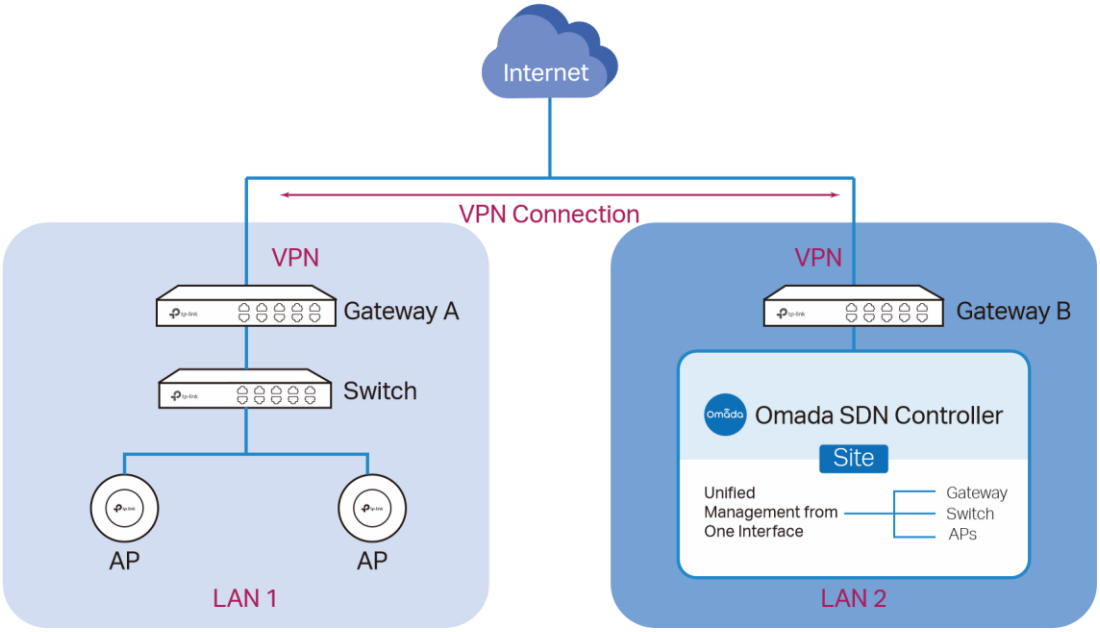
Allez dans Settings > Transmission > NAT > Port Forwarding.

Cliquez sur + Create New Rule pour charger la page suivante. Spécifiez un nom pour identifier la règle de transfert de port, cochez Activer l'état, sélectionnez N'importe quel ip de source, sélectionnez le port WAN souhaité comme interface, désactivez DMZ, spécifiez 29810-29813 en tant que port de port source et destination, spécifiez l'adresse IP du contrôleur en tant qu'ADRESSE IP de destination et sélectionnez Tout comme protocole. Cliquez ensuite sur Create.



1. Utiliser un VPN

Configurer une connexion VPN entre la passerelle A et la passerelle B en mode autonome. Pour plus d'informations sur la configuration VPN, reportez-vous au Guide utilisateur des passerelles.



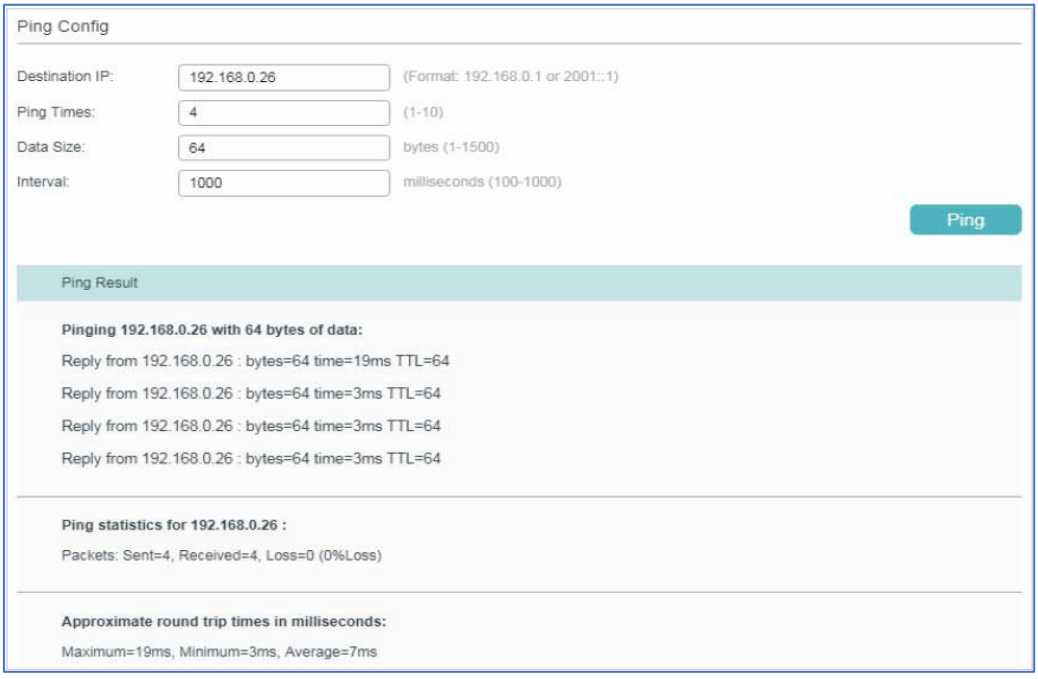
2. (Facultatif) Tester le réseau

Si vous n'êtes pas sûr si le contrôleur et les appareils peuvent établir la communication, il est recommandé de faire le test ping des appareils au contrôleur.

Prenons un switch par exemple.

Connectez-vous à la page Web du commutateur en mode autonome.

Puis allez à MAINTENANCE > Network Diagnostics > Ping pour charger la page suivante et spécifier l'adresse IP de destination comme adresse IP du contrôleur (si vous avez configuré le transfert de port du côté du contrôleur, utilisez plutôt l'adresse IP WAN publique de la passerelle). Cliquez ensuite sur Ping.



Si le résultat ping indique que les paquets sont reçus, cela implique que le contrôleur peut communiquer avec les appareils. Sinon, le contrôleur ne peut pas communiquer avec les appareils, alors vous devez vérifier votre réseau.



Note:

Si le contrôleur et les périphériques se trouvent dans le même réseau local, sous-réseau et VLAN, sautez cette étape. Dans ce scénario, le contrôleur peut découvrir les périphériques directement, et aucun réglage supplémentaire n'est requis.

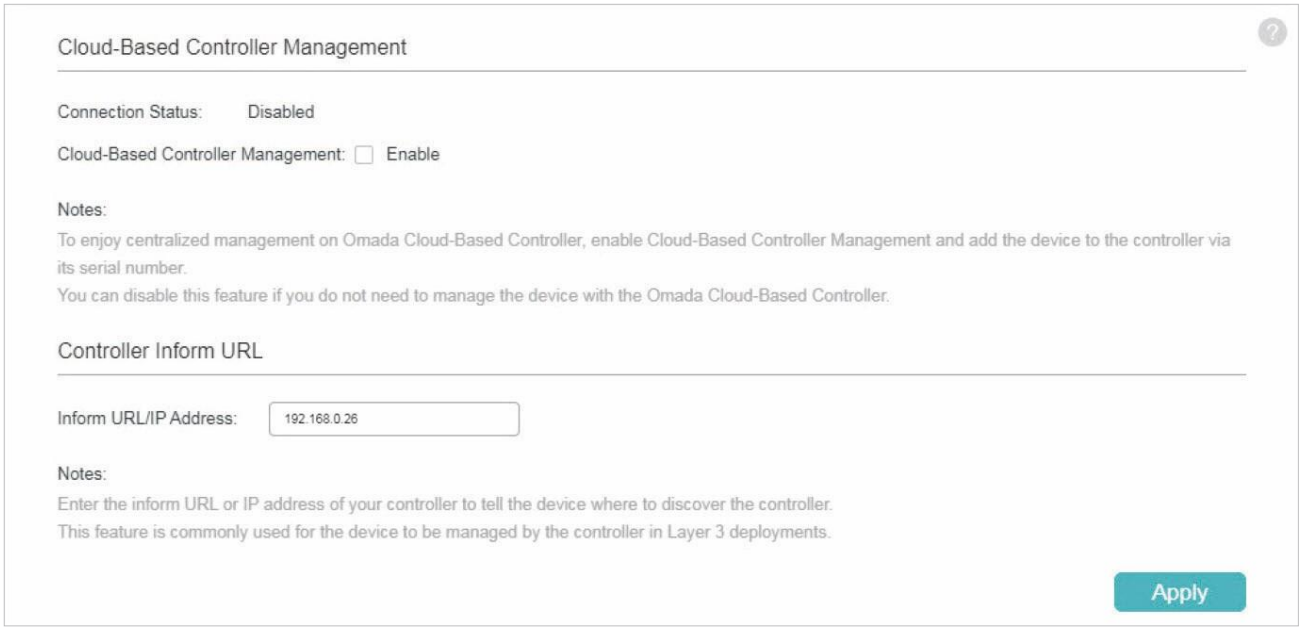
Assurez-vous que le contrôleur peut découvrir les périphériques.

Lorsque le contrôleur et les périphériques se trouvent dans différents LAN, sous-réseaux ou VLANs, le contrôleur ne peut pas découvrir directement les périphériques. Vous devez choisir Controller Inform URL, Discovery Utility, Ou DHCP Option 138 comme méthode pour aider le contrôleur à découvrir les appareils.

■ URL d'information du contrôleur

L'URL d'information du contrôleur informe les périphériques de l'URL ou de l'adresse IP du contrôleur. Ensuite, les appareils entrent en contact avec le contrôleur afin que le contrôleur puisse découvrir les appareils.

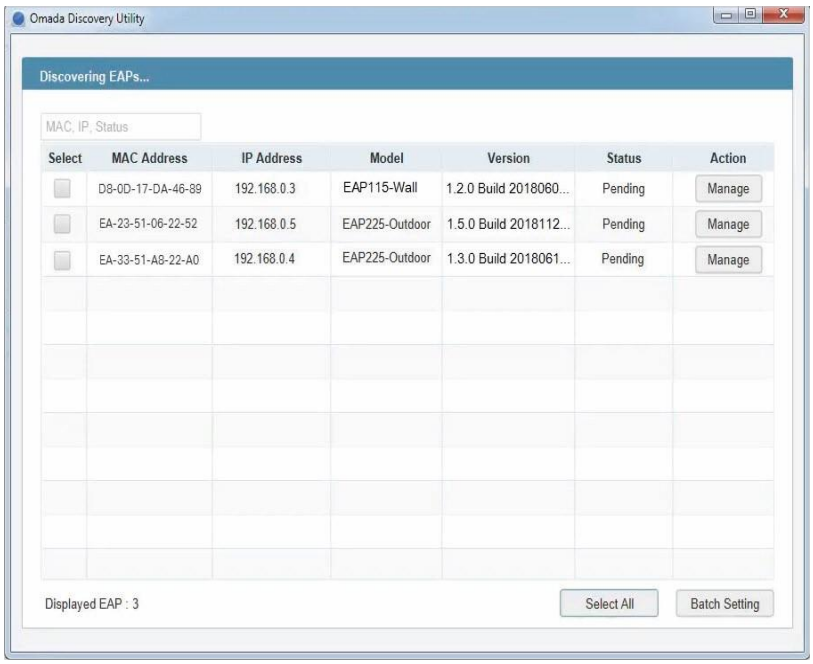
Vous pouvez configurer l'URL d'information du contrôleur pour les périphériques en mode autonome. Prenons un interrupteur par exemple. Connectez-vous à la page de gestion du commutateur en mode autonome et accédez à SYSTEM > Controller Settings pour charger la page suivante. Dans Controller Inform URL, Spécifiez Informer l'URL/l'adresse IP comme URL ou adresse IP du contrôleur (si vous avez configuré le transfert de port du côté du contrôleur, utilisez plutôt l'adresse IP WAN publique de la passerelle). Cliquez ensuite sur Apply.



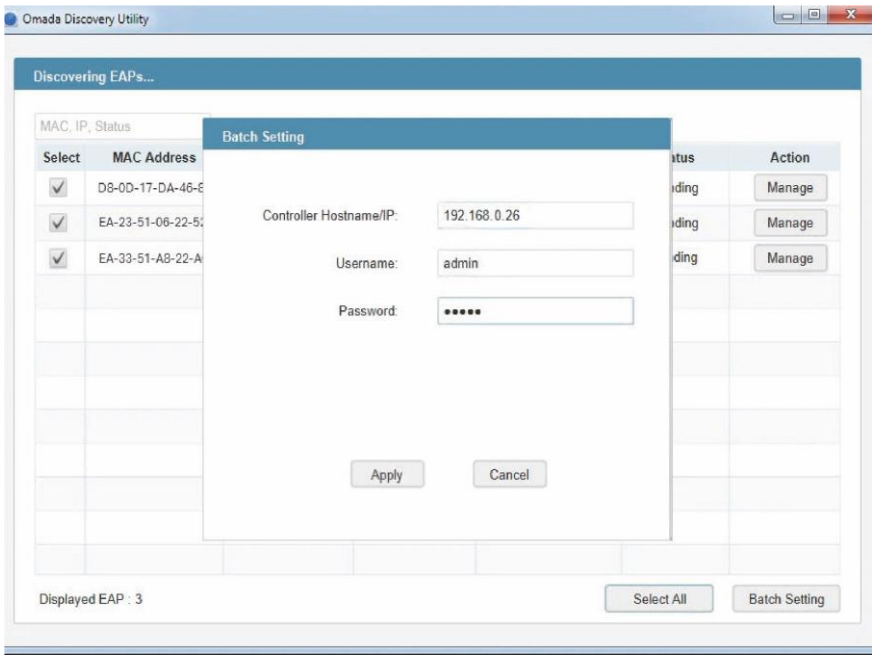
■ Utilitaire découverte

Discovery Utility peut découvrir les appareils dans le même réseau local, sous-réseau et VLAN, et informer les appareils de l'adresse IP du contrôleur. Ensuite, les appareils entrent en contact avec le contrôleur afin que le contrôleur puisse découvrir les appareils.

1. Télécharger **Discovery Utility** à partir de la website et puis installez-le sur votre PC qui doit être situé dans le même RÉSEAU, sous-réseau et VLAN que vos appareils.
1. Ouvrez **Discovery Utility** et vous pouvez voir une liste d'appareils. Sélectionnez les périphériques à adopter et cliquez sur Batch Setting.



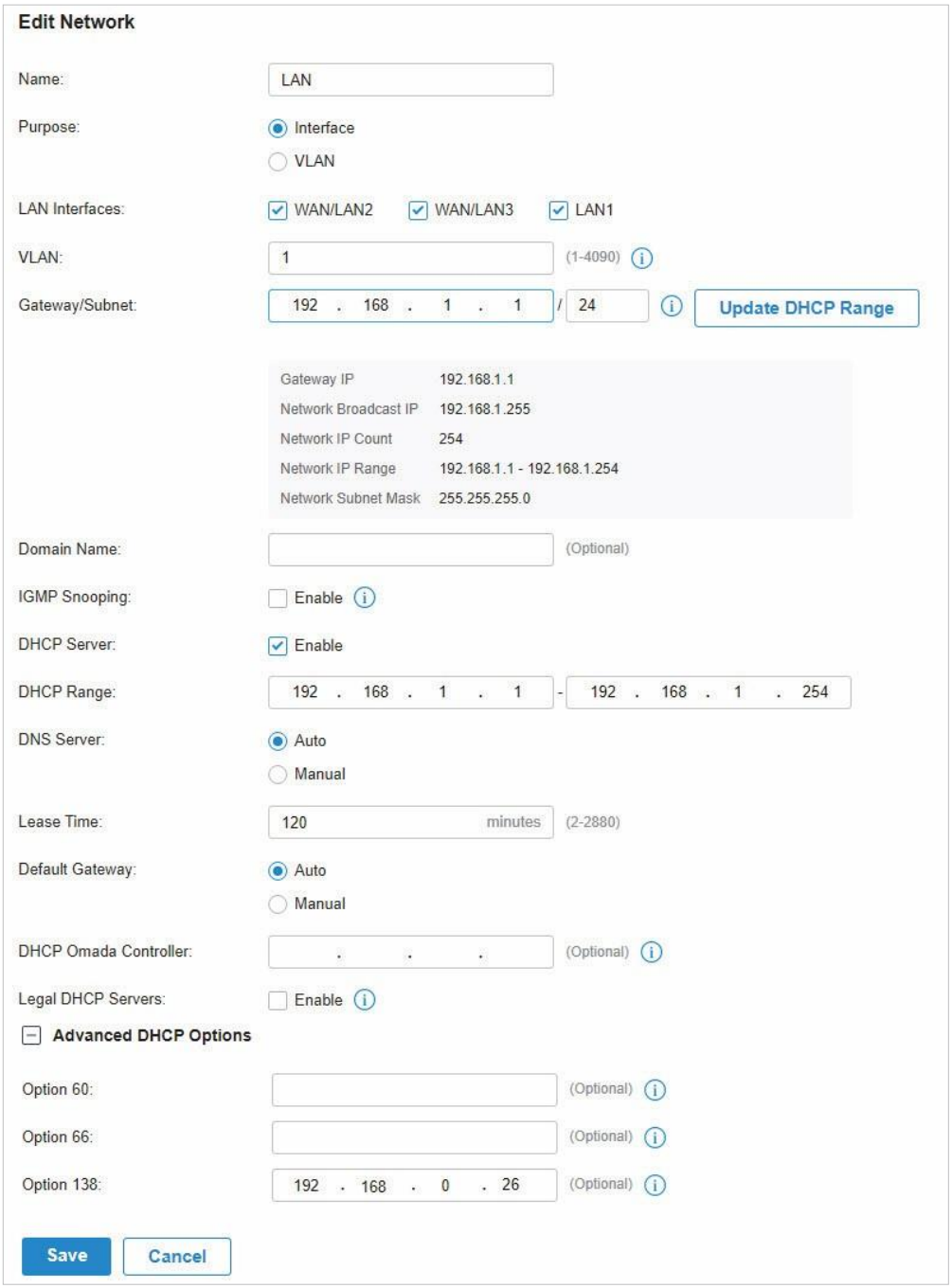
2. Spécifiez le nom d'hôte/IP du contrôleur comme adresse IP du contrôleur (si vous avez configuré le transfert de port du côté du contrôleur, utilisez plutôt l'adresse IP WAN publique de la passerelle) et entrez le nom d'utilisateur et le mot de passe des périphériques. Par défaut, le nom d'utilisateur et le mot de passe sont tous deux admin. Cliquez ensuite sur Apply. Attendez que le réglage réussisse.



■ DHCP Option 138

DHCP Option 138 informe un client DHCP, tel qu'un commutateur ou un EAP, de l'adresse IP du contrôleur lorsque le client DHCP envoie des demandes DHCP au serveur DHCP, qui est généralement une passerelle.

1. Pour utiliser d'abord l'option 138 DHCP, vous devez d'abord adopter la passerelle sur le contrôleur, ce qui peut nécessiter d'autres techniques telles que Controller Inform URL ou Discovery Utility si nécessaire.
2. Après l'adoption de la passerelle, Settings > Wired Networks > LAN > Networks, et cliquez sur dans la colonne ACTION du RÉSEAU LOCAL où se trouvent les clients DHCP. Activez DHCP Server et configurez les paramètres DHCP courants. Cliquez ensuite sur Advanced DHCP Options et spécifier Option 138 en tant qu'adresse IP du contrôleur (si vous avez configuré le transfert de port du côté du contrôleur, utilisez plutôt l'adresse IP WAN publique de la passerelle). Cliquez sur Save.

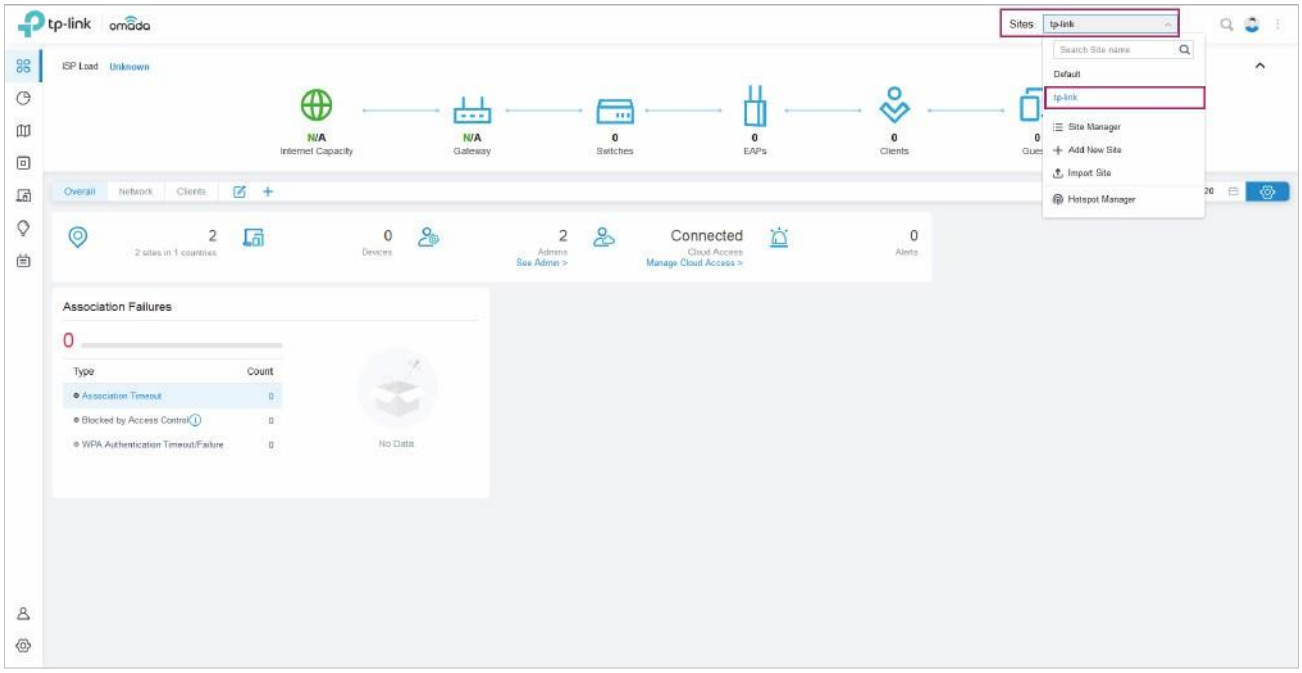


3. Pour que DHCP option 138 prenne effet, vous devez renouveler les paramètres DHCP pour les clients DHCP. Une façon possible est de déconnecter les clients DHCP, puis de les reconnecter.

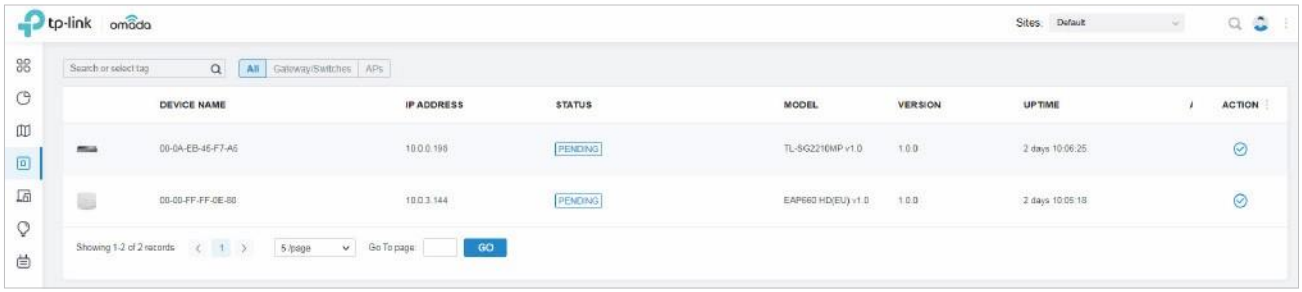
Se préparer à la communication > **Préparez-vous à la découverte des périphériques** > **Adopter les appareils**

1. Décidez à quel site vous souhaitez ajouter les périphériques. Dans la page configuration du contrôleur, sélectionnez le site dans la liste déroulante des Sites.

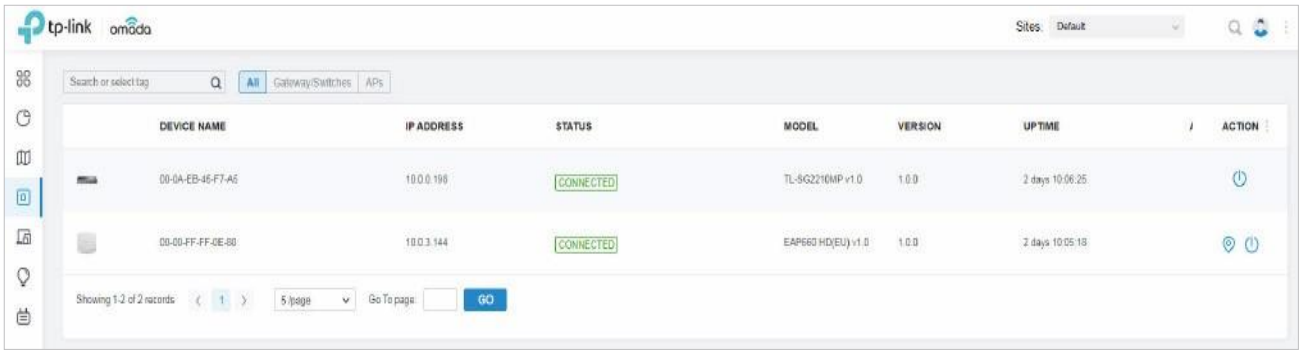
2.



Allez dansDevices, et les appareils qui ont été découverts par le contrôleur sont affichés. Cliquez sur dans la colonne ACTION des périphériques que vous souhaitez ajouter au site.



3. Attendez que le STATUS se transforme en Connected. Ensuite, les périphériques sont adoptés par le contrôleur et ajoutés au site actuel. Une fois les dispositifs adoptés, ils sont soumis à la gestion centrale du site.



3. 3. 2 Pour le contrôleur cloud d'Omada

Pour adopter les périphériques du contrôleur, procédez comme suit :

1.) Connectez-vous à Internet.

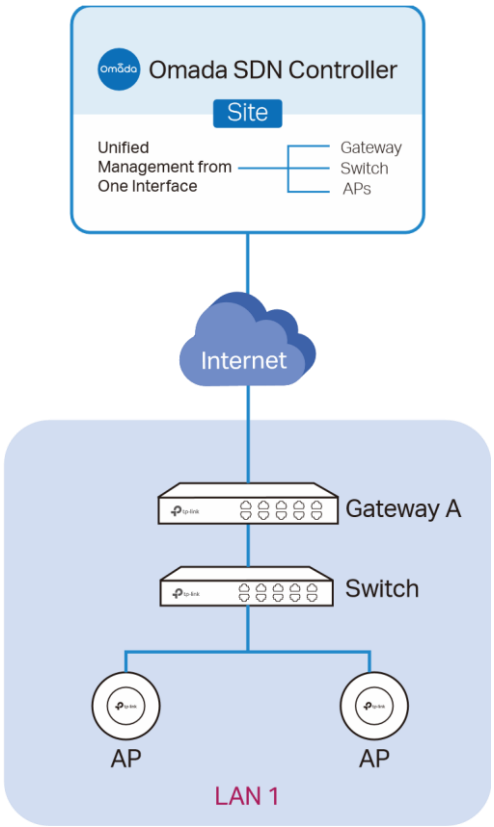
2.) Préparer la gestion du contrôleur.

3 .) Adopter les appareils.



1. Configurer le réseau.

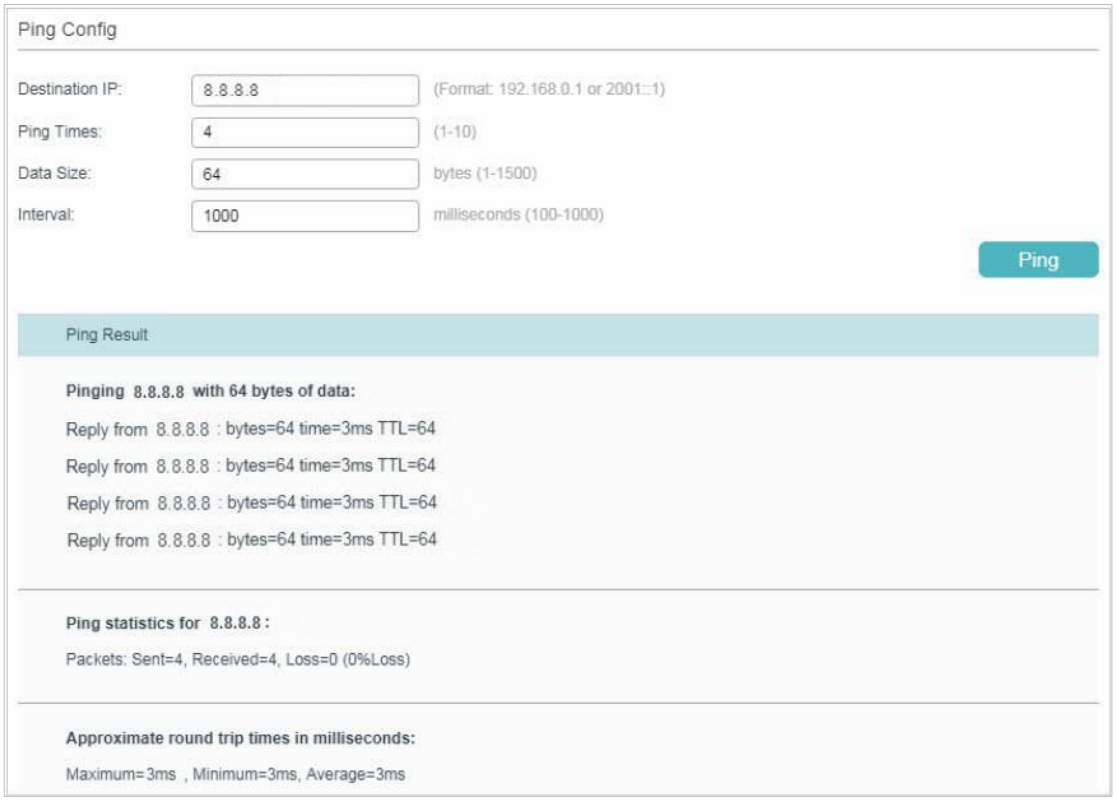
   Assurez-vous que vos appareils sont connectés à Internet.



   Si vous utilisez des pares-feux dans votre réseau, assurez-vous que le pare-feu ne bloque pas le trafic à partir du contrôleur. Pour configurer votre stratégie de pare-feu, vous pouvez connaître l'URL du contrôleur. Après avoir ouvert la page Web du contrôleur, vous pouvez obtenir l'URL à partir de la barre d'adresses du navigateur.

1. (Facultatif) Tester le réseau.

   Si vous n'êtes pas sûr si les appareils sont connectés à Internet, il est recommandé de faire le test ping des appareils à une adresse IP publique, comme 8.8.8.8.
   Prenons un interrupteur par exemple. Connectez-vous à la page Web du commutateur en mode autonome. selectionnez MAINTENANCE > Network Diagnostics > Ping pour charger la page suivante. Spécifiez l'adresse IP de destination en tant qu'adresse IP publique, telle que le 8.8.8.8. Cliquez ensuite sur Ping.



   Si le résultat ping indique que les paquets sont reçus, cela implique que les appareils sont connectés à Internet. Sinon, les appareils ne sont pas connectés à Internet, alors vous devez vérifier votre réseau.

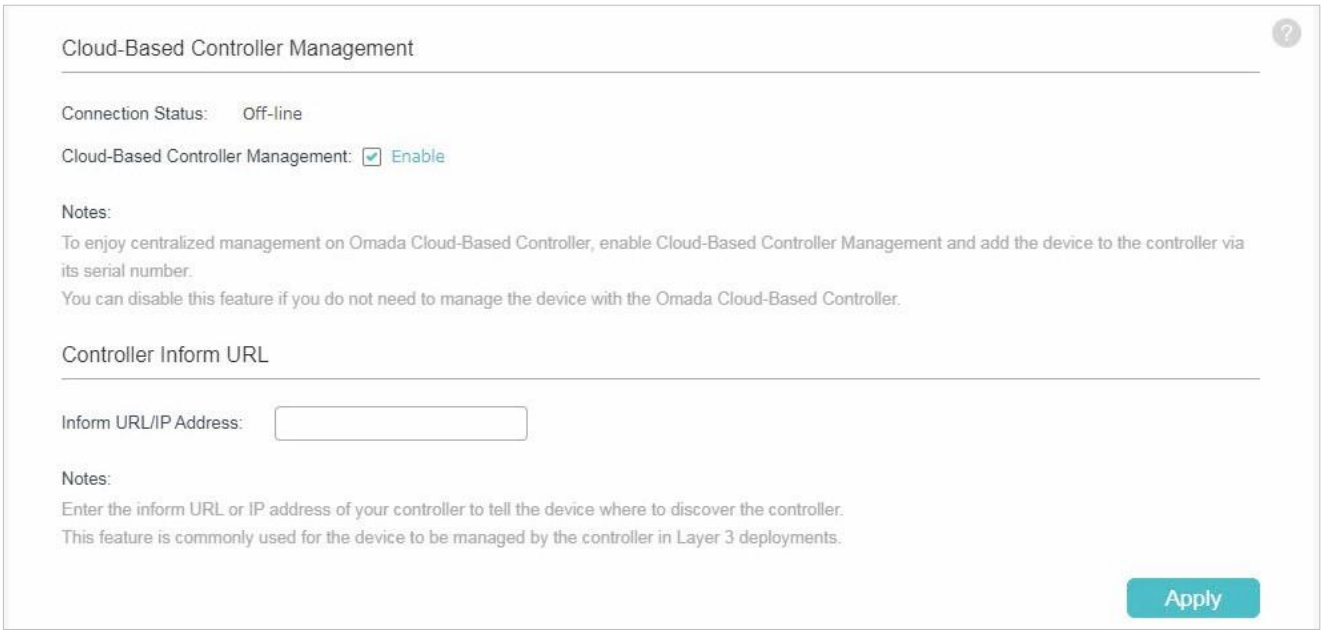


Note:

Si vos appareils sont dans le paramètre par défaut de l'usine, sautez cette étape.

La fonction Cloud-Based Controller Management permet aux périphériques d'être adoptés par Omada Cloud Based Controller. Assurez-vous que la gestion des contrôleurs basés sur le cloud est activée sur les périphériques. Pour plus d'informations, consultez le Guide de l'utilisateur de vos appareils, qui peut être téléchargé à partir de la TP-Link download center.

Prenons un interrupteur par exemple. Connectez-vous à la page Web du commutateur en mode autonome. Atteindre SYSTEM > Controller Settings pour charger la page suivante. Dans Cloud-Based Controller Management, activer cloud based Controller Management et cliquez sur Apply.





Dans la page de configuration du contrôleur, accédez au site où vous souhaitez ajouter les périphériques. Accédez à Devices, puis cliquez sur Ajouter des périphériques. Ajoutez ensuite vos appareils au contrôleur. Une fois les dispositifs adoptés, ils sont soumis à la gestion centrale du site.

4

Configurer le réseau avec le contrôleur SDN Omada

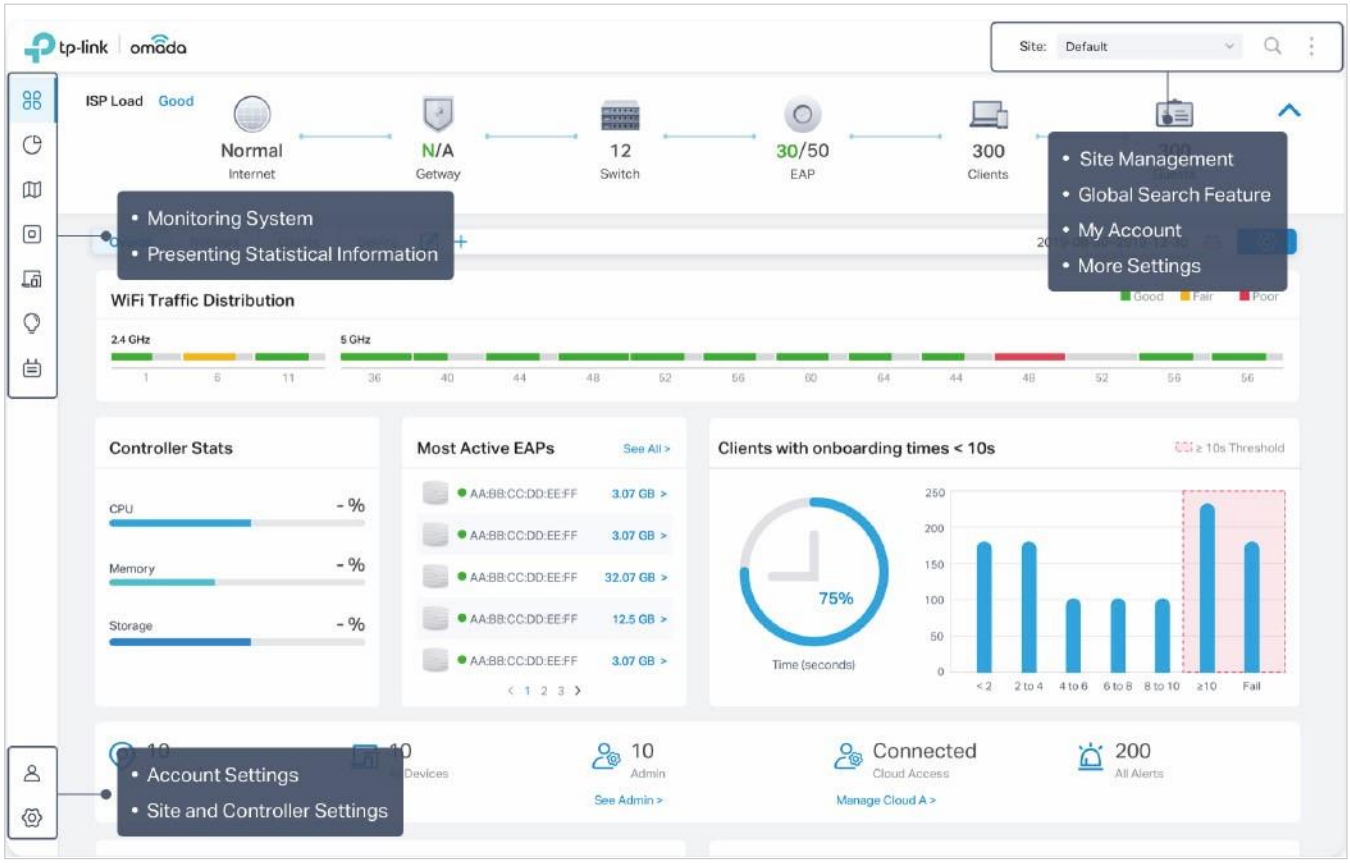
Ce chapitre vous guide sur la configuration du réseau avec le contrôleur SDN Omada. En tant que centre de commande et plate-forme de gestion au cœur du réseau Omada, Omada SDN Controller offre une approche unifiée pour configurer les réseaux d'entreprise composés de routeurs, commutateurs et points d'accès sans fil. Le chapitre comprend les sections suivantes :

1. Naviguer dans l'interface utilisateur
2. Modifier la configuration actuelle du site
3. Configurer les réseaux câblés
4. Configurer les réseaux sans fil
5. Sécurité réseau
6. Transmission
7. Configurer VPN
8. Créer des profils
9. Authentification
10. Services

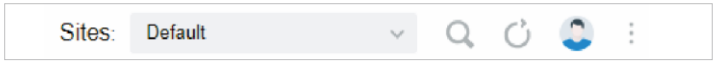
4. 1 Naviguer dans l'interface utilisateur

Lorsque vous commencez à utiliser l'interface de gestion du contrôleur (Interface utilisateur du contrôleur) pour configurer et surveiller votre réseau, il est utile de vous familiariser avec les éléments les plus couramment utilisés de l'interface utilisateur du contrôleur qui sont fréquemment référencés dans ce guide.

L'interface utilisateur du contrôleur est regroupée en menus orientés tâches, qui se trouvent dans le coin supérieur droit et la barre de navigation à gauche de la page. Notez que les paramètres et fonctionnalités qui apparaissent dans l'interface utilisateur dépendent des autorisations de votre compte d'utilisateur. L'image suivante représente les principaux éléments de l'interface utilisateur du contrôleur.



Les éléments dans le coin supérieur droit de l'écran donnent un accès rapide à:



Site Management

Site, qui signifie emplacement réseau logiquement séparé, est la plus grande unité pour la gestion des réseaux avec Omada SDN Controller. Vous pouvez simultanément configurer des fonctionnalités pour plusieurs périphériques sur un site. La gestion du site comprend :

Site Manager — avoir une vue d'ensemble rapide des sites, y compris le nom, l'emplacement, les périphériques gérés et les clients connectés.

Add New Site — ajouter un nouveau site, qui est l'emplacement du réseau logiquement séparé. Le site est la plus grande unité de gestion du réseau.

Import Site— importer le site, à partir d'un autre contrôleur.

Global Search Feature

Cliquez sur et entrez les mots clés pour rechercher rapidement les fonctions que vous souhaitez configurer.

My Account

Cliquez sur l'icône du compte pour afficher les informations du compte, paramètres du compte et déconnecter. Vous pouvez modifier votre mot de passe sur les paramètres du compte.

More Settings

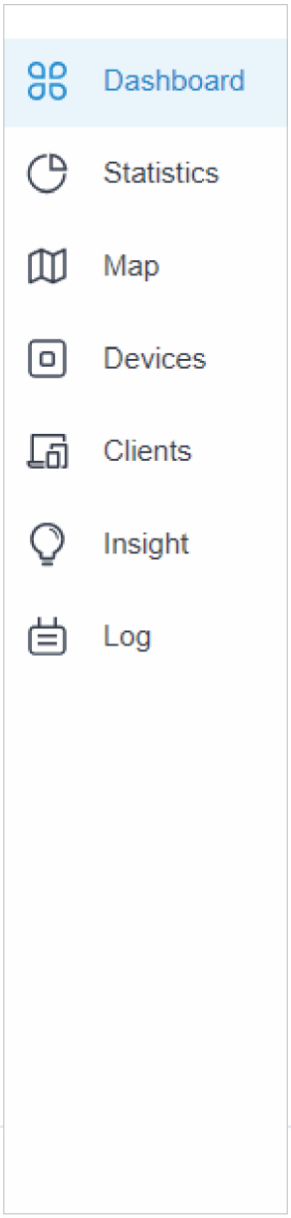
Cliquez sur pour afficher Préférences, À propos et Didacticiel.

Preferences: Cliquez pour passer à la maintenance et personnaliser l'interface utilisateur du contrôleur en fonction de vos besoins. Pour plus de détails, reportez-vous à Maintenance

About: Cliquez pour afficher la version du contrôleur.

Tutorial: Cliquez pour afficher le guide De démarrage rapide qui montre la navigation et les outils disponibles pour le contrôleur.

La barre de navigation à gauche donne accès à :



Dashboard affiche une vue résumée de l'état du réseau à travers différentes visualisations. Le tableau de bord basé sur les widgets est personnalisable en fonction de vos besoins.

Statistics fournit une représentation visuelle des clients et du réseau géré par le contrôleur. Les graphiques d'exécution montrent les changements dans les performances de l'appareil au fil du temps, y compris l'état des commutateurs et les résultats des tests de vitesse.

Map génère automatiquement la topologie du système et vous pouvez examiner l'état d'approvisionnement des appareils. En cliquant sur chaque nœud, vous pouvez afficher les informations détaillées de chaque appareil. Vous pouvez également télécharger des images de votre emplacement pour une représentation visuelle de votre réseau.

Devices affiche tous les appareils TP-Link découverts sur le site et leurs informations générales. Cette vue de liste peut changer en fonction de vos besoins de surveillance grâce à la personnalisation des colonnes. Vous pouvez cliquer sur n'importe quel périphérique de la liste pour révéler la fenêtre Propriétés pour obtenir des informations plus détaillées sur chaque appareil et fournir des configurations individuelles à l'appareil.

Clients affiche une vue de liste des clients câblés et sans fil connectés au réseau. Cette vue de liste peut changer en fonction de vos besoins de surveillance grâce à la personnalisation des colonnes. Vous pouvez cliquer sur tous les clients de la liste pour révéler la fenêtre Propriétés pour obtenir des informations plus détaillées sur chaque client et fournir des configurations individuelles au client.

Insight affiche une liste de statistiques de votre périphérique réseau, de vos clients et de vos services au cours d'une période spécifiée. Vous pouvez modifier la plage de date par incréments d'un jour.

Log affiche les journaux qui enregistrent les activités variées des utilisateurs, des périphériques et des événements des systèmes, tels que les actions administratives et les comportements anormaux des périphériques. Vous pouvez également configurer les notifications pour recevoir des e-mails d'alerte de certaines activités.

Admin vous permet de configurer des comptes administratifs à plusieurs niveaux avec une hiérarchie d'autorisations qui peuvent être configurées pour fournir des niveaux d'accès finement grains au contrôleur, comme l'exige votre entreprise.

Settings est divisé en deux parties : Paramètres du site et Paramètres du contrôleur. Dans Paramètres du site, vous pouvez fournir et configurer tous vos périphériques réseau sur le même site en quelques minutes. Dans les paramètres du contrôleur, vous pouvez maintenir le système de contrôleur pour les meilleures performances.

4. 2 Modifier la configuration actuelle du site

Vous pouvez afficher et modifier les configurations du site actuel dans le site, y compris les informations de base du site, les fonctionnalités du périphérique gérés de manière centralisée et le compte de périphérique. Les fonctionnalités et le compte de périphérique configurés ici sont appliqués à tous les appareils du site, de sorte que vous pouvez facilement gérer les périphériques de manière centralisée.

4. 2. 1 Site Configuration

Aperçu

Dans Configuration du site, vous pouvez afficher et modifier le nom du site, l'emplacement, le fuseau horaire et le scénario d'application du site actuel.

Configuration

Sélectionner un site dans la liste déroulante de Sites dans le coin supérieur droit, aller à Settings > Site, et configurer les informations suivantes du site dans Site Configuration. Cliquez sur Save.



Site Name	Spécifiez le nom du site actuel. Il ne devrait pas être plus de 64 caractères.
Country/Region	Sélectionner l'emplacement du site.
Time Zone	Sélectionner le fuseau horaire du site.
Application Scenario	Spécifiez le scénario d'application du site. Pour personnaliser votre scénario, cliquez sur Create New Scenario dans la liste déroulante.

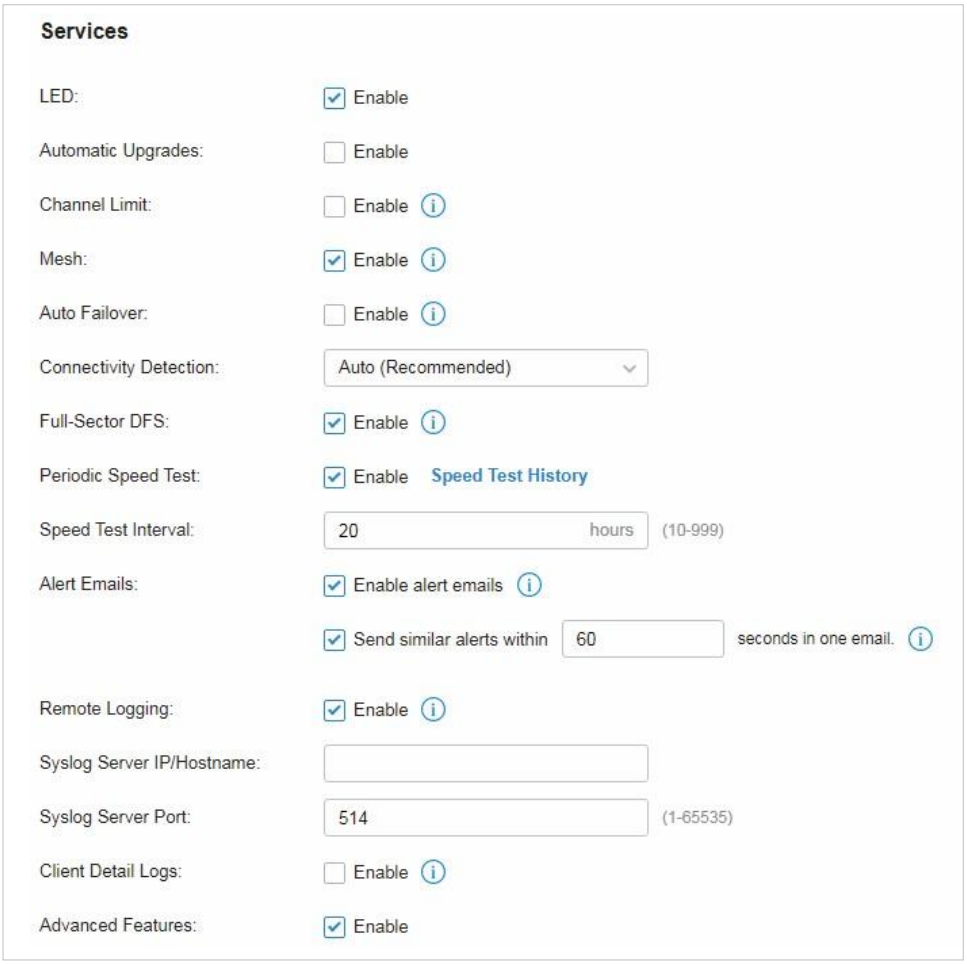
4. 2. 2 Services

Aperçu

Dans Services, vous pouvez afficher et modifier les fonctionnalités appliquées aux périphériques du site actuel. La plupart des fonctionnalités sont appliquées à tous les appareils, tels que le LED, les mises à niveau automatiques et les e-mails d'alerte, tandis que certaines sont appliquées uniquement aux FAI, tels que Channel Limit et Mesh.

Configuration

Sélectionner un site dans la liste déroulante de Sites dans le coin supérieur droit, aller à Settings > Site, et configurer les fonctionnalités suivantes pour le site actuel dans Services. Cliquez sur Save.Sélectionnez un site dans la liste déroulante des sites dans le coin supérieur droit, accédez à Paramètres > Site et configurez les fonctionnalités suivantes pour le site actuel dans Services. Cliquez sur Enregistrer



LED	Activer ou désactiver les LED de tous les appareils du site. Par défaut, l'appareil suit le paramètre LED du site auquel il appartient. Pour modifier le paramètre LED de certains appareils, reportez-vous à Configure and Monitor Omada Managed Devices.
Automatic Upgrades	Lorsqu'il est activé, le contrôleur mettra automatiquement à niveau les périphériques de ce site vers la dernière version.

Channel Limit	(Pour les AP extérieurs) Lorsqu'ils sont activés, les EAP extérieurs n'utilisent pas le canal avec une fréquence allant de 5150 MHz à 5350 MHz pour respecter la limite des lois et règlements locaux dans les pays de l'UE.
Mesh	(Pour EAP225/EAP245/EAP225-Outdoor) Lorsqu'il est activé, les EAP prenant en charge Mesh peuvent établir le réseau de maillage sur le site.
Auto Failover	(Pour les AP du réseau de maillage, le basculement automatique est utilisé pour maintenir automatiquement le réseau de maillage. Lorsqu'il est activé, le contrôleur sélectionne automatiquement un nouveau lien d'accès sans fil pour l'AP si le lien d'ouverture d'origine échoue. Pour activer cette fonctionnalité, activez Mesh.
Connectivity Detection	(Pour les AP du réseau de maillage) Spécifiez la méthode de détection de connexion lorsque le maillage est activé. Dans un réseau de maillage, les AP peuvent envoyer des paquets de demande ARP à une adresse IP fixe pour tester la connectivité. Si le lien échoue, l'état de ces AP passera à Isolé. Auto (Recommended): Sélectionnez cette méthode et les AP de maillage enverront des paquets de demande ARP à la passerelle par défaut pour la détection. Custom IP Address: Sélectionnez cette méthode et spécifiez une adresse IP souhaitée. Les AP en maille envoient des paquets de demande ARP à l'adresse IP personnalisée pour tester la connectivité. Si l'adresse IP de l'AP se trouve dans différents segments réseau de l'adresse IP personnalisée, l'AP utilisera l'adresse IP de passerelle par défaut pour la détection.
Full-Sector DFS	(Pour les AP du réseau de maillage) Avec cette fonctionnalité activée, lorsque les signaux radar sont détectés sur le canal actuel par un EAP, les autres EAP du réseau de maillage seront également informés. Ensuite, tous les EAP du réseau de maillage passeront à un autre canal. Pour activer cette fonctionnalité, activez Mesh.
Periodic Speed Test	Lorsqu'il est activé, le contrôleur teste et enregistre périodiquement la vitesse et la latence des ports WAN. Speed Test Interval: Lorsqu'il est activé, spécifiez l'intervalle pour décider à quelle fréquence tester la vitesse des appareils. Speed Test History: Click it to view the history statistics of speed test in Speed Test

	Alert Emails Enable alert emails: Lorsqu'il est activé, le contrôleur peut envoyer des e-mails pour informer les administrateurs et les téléspectateurs des journaux d'alerte du site une fois générés. Send similar alerts within seconds in one email: Lorsqu'elles sont activées, les alertes similaires générées à chaque période sont collectées et envoyées aux administrateurs et aux téléspectateurs dans un seul e-mail. To configure alert-level logs and enable email notifications on the controller, refer to Notifications.
Remote Logging	With this feature configured, the controller will send generated system logs to the log server. When enabled, the following items are required: Syslog Server IP/Hostname: Enter the IP address or hostname of the log server. Syslog Server Port: Enter the port of the server. Client Detail Logs: With this feature enabled, the logs of clients will be sent to the syslog server.
Advanced Features	(For APs) When enabled, you can configure more features for APs in Advanced Features. When disabled, these features keep the default settings. For detailed configuration, refer to Advanced Features.

4. 2. 3 Fonctionnalités avancées

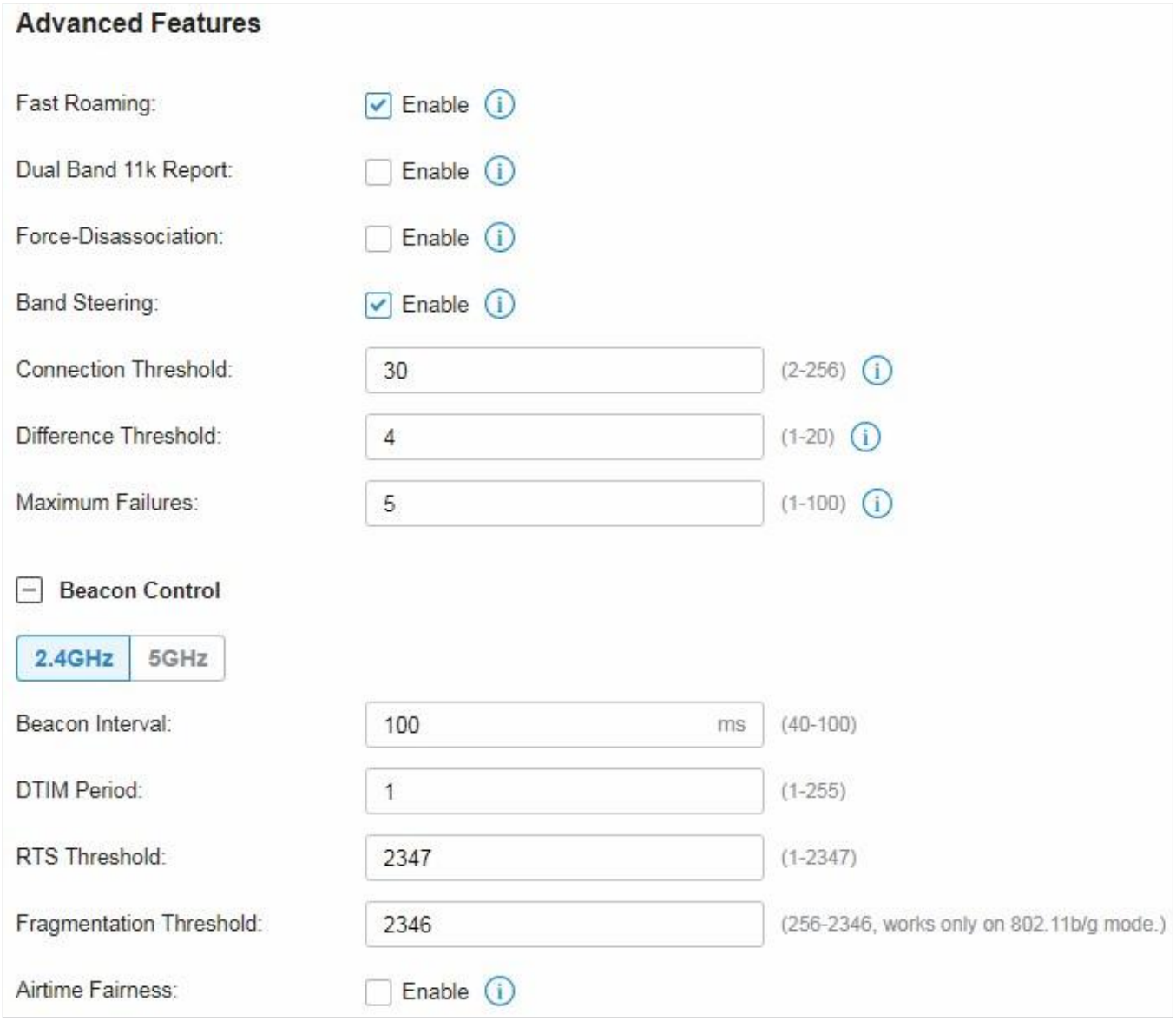
Aperçu

Les fonctionnalités avancées incluent l'itinérance rapide, la direction de bande et le contrôle de balise, qui sont applicables aux AP seulement. Grâce à ces fonctionnalités avancées configurées correctement, vous pouvez améliorer la stabilité, la fiabilité et l'efficacité de communication du réseau.

Les fonctionnalités avancées sont recommandées pour être configurées par les administrateurs réseau avec les connaissances WLAN. Si vous n'êtes pas sûr des conditions de votre réseau et de l'impact potentiel de tous les paramètres, Advanced Features désactivé dans Services pour utiliser leurs configurations par défaut.

Configuration

Sélectionnez un site dans la liste déroulante des sites dans le coin supérieur droit, accédez àSettings > Site, et activer Advanced Features dans Services tout d'abord. Ensuite, configurez les fonctionnalités suivantes dans Advanced Features. Cliquez sur Save.



Fast Roaming	Avec cette fonctionnalité activée, les clients qui 602.11k/v peuvent améliorer l'expérience d'itinérance rapide lors du déplacement entre différents AP. Par défaut, il est désactivé.
Dual Band 11k Report	Lorsqu'il est désactivé, le contrôleur fournit une liste de voisins qui ne contient que des AP voisins dans la même bande à laquelle le client est associé. Lorsqu'il est activé, le contrôleur fournit une liste de voisins qui contient des AP voisins dans les bandes de 2,4 GHz et de 5 GHz. Cette fonctionnalité n'est disponible que lorsque l'itinérance rapide est activée. Par défaut, il est désactivé.

Force-Disassociation	Avec cette fonctionnalité désactivée, l'AP émet uniquement une suggestion d'itinérance 802.11v lorsque la qualité du lien d'un client tombe en dessous du seuil prédéfini et qu'il existe une meilleure option d'AP, mais si vous devez errer ou non est déterminée par le client. Avec cette fonctionnalité activée, l'AP forcera le dissocier le client s'il ne se reconnectent pas à un autre AP. This feature is available only when Fast Roaming is enabled. By default, it is disabled.
Band Steering	La direction de bande peut ajuster le nombre de clients sur des bandes de 2,4 GHz et de 5 GHz pour offrir une meilleure expérience sans fil. Lorsqu'ils sont activés, les clients à double bande seront orientés vers la bande de 5 GHz selon les paramètres configurés. Avec les réglages appropriés, la direction de bande peut améliorer les performances du réseau parce que la bande de 5 GHz prend en charge un plus grand nombre de canaux non-se chevauchent et est moins bruyant. Par défaut, il est désactivé. Connection Threshold: Spécifiez le nombre maximal de clients connectés à la bande de 5 GHz. Par défaut, le seuil est de 30. Difference Threshold: Spécifiez la différence maximale entre le nombre de clients de la bande de 5 GHz et de la bande de 2,4 GHz. Par défaut, le seuil est de 4. Lorsque le numéro de connexion et la différence de nombre de clients dépassent à la fois leur seuil configuré, le PAE refuse la demande de connexion sur la bande de 5 GHz et ne dirige plus les autres clients vers la bande de 5 GHz. Maximum Failures: Spécifiez le nombre maximal de tentatives ratées lorsqu'un client tente à plusieurs reprises de s'associer à un EAP sur 5 GHz. Lorsque le nombre de rejets atteint le maximum d'échecs, le EAP accepte la demande de connexion du client. Par défaut, il est 4.
Beacon Control	Les balises sont transmises périodiquement par le PAE pour annoncer la présence d'un réseau sans fil pour les clients. Cliquez sur, ⊞ sélectionnez la bande et configurez les paramètres suivants de Beacon Control. Beacon Interval: Spécifiez la fréquence à laquelle les AP envoient une balise aux clients. Par défaut, il est de 100. DTIM Period: Spécifiez la fréquence à laquelle les clients vérifient les données tamponnées qui sont toujours sur le EAP en attente de ramassage. Par défaut, les clients vérifient pour eux à chaque balise. DTIM (Message d'indication de trafic de livraison) est contenu dans certains cadres de balise indiquant si le PAE a des données tamponnées pour les périphériques clients. Un intervalle DTIM excessif peut réduire les performances des applications multidiffusion, nous vous recommandons donc de conserver l'intervalle par défaut, 1. RTS Threshold: RTS (Demande d'envoi) peut assurer une transmission efficace des données en évitant le conflit de paquets. Si un client souhaite envoyer un paquet supérieur au seuil, le mécanisme RTS sera activé pour retarder les paquets d'autres clients dans le même réseau sans fil. Nous vous recommandons de maintenir le seuil par défaut, qui est de 2347. Si vous spécifiez une valeur seuil faible, le mécanisme RTS peut être activé plus fréquemment pour récupérer le réseau des interférences ou des collisions possibles. Toutefois, il consomme également plus de bande passante et réduit le débit du paquet. Fragmentation Threshold: La fragmentation peut limiter la taille des paquets transmis sur le réseau. Si un paquet à envoyer dépasse le seuil de fragmentation, la fonction Fragmentation sera activée et le paquet sera fragmenté en plusieurs paquets. Par défaut, le seuil est de 2346.

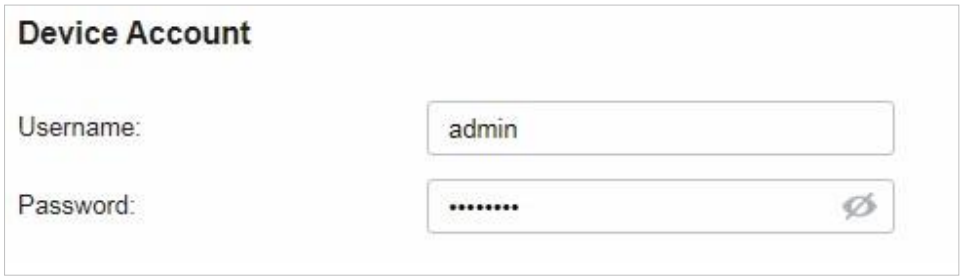
La fragmentation permet d'améliorer les performances du réseau si elles sont correctement configurées. Toutefois, un seuil de fragmentation trop bas peut entraîner de mauvaises performances sans fil en raison de l'augmentation du trafic des messages et du travail supplémentaire de division et de remontage des paquets de données.

Airtime Fairness: Avec cette option activée, chaque client se connectant au PAE peut obtenir le même temps pour transmettre des données afin que les clients à faible débit de données n'occupent pas trop de bande passante réseau et que les performances du réseau s'améliorent dans leur ensemble. Nous vous recommandons d'activer cette fonction sous des réseaux sans fil multi-taux.

4. 2. 4 Compte de périphérique

Vous pouvez spécifier un compte de périphérique pour tous les périphériques adoptés sur le site par lots. Une fois que les périphériques sont adoptés par le contrôleur, leur nom d'utilisateur et mot de passe deviennent les mêmes que les paramètres du compte de périphérique pour protéger la communication entre le contrôleur et les appareils. Par défaut, le nom d'utilisateur est admin et le mot de passe est généré au hasard.

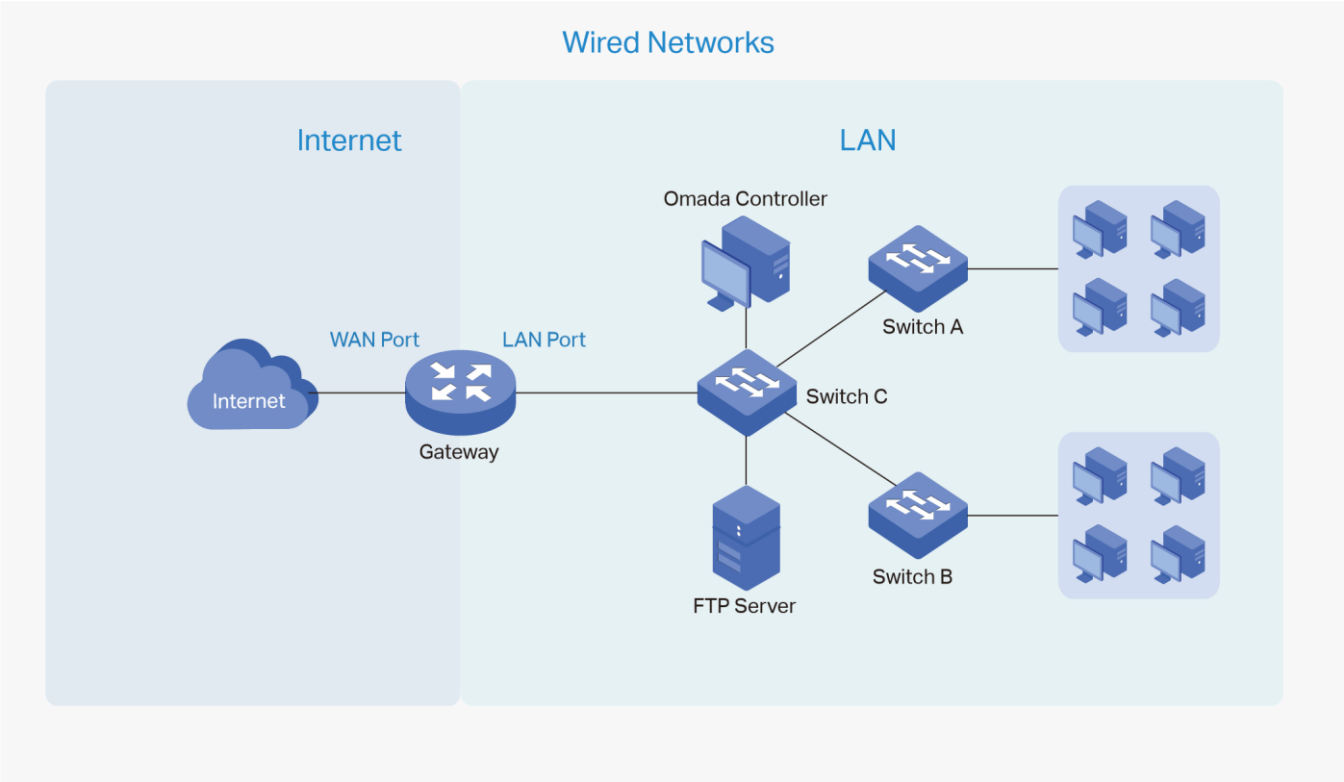
Atteindre Settings > Site et modifier le nom d'utilisateur et le mot de passe dans Device Account. Cliquez sur Save et le nouveau nom d'utilisateur et mot de passe sont appliqués à tous les appareils du site.



4. 3 Configurer les réseaux câblés

Les réseaux câblés permettent à vos périphériques et clients câblés, y compris la passerelle, les commutateurs, les EAP et les PC, de se connecter les uns aux autres et à Internet.

Comme indiqué dans la figure suivante, Réseaux câblés se compose de deux parties : Internet et LAN.



Pour Internet, vous déterminez le nombre de ports WAN déployés par la passerelle et la façon dont ils se connectent à Internet en fonction de vos besoins. Pour se connecter à Internet, la passerelle en choisit une parmi les types de connexion suivants : IP dynamique, IP statique, PPPoE, L2TP et PPTP.

Pour LAN, vous configurez le réseau interne câblé et la façon dont vos appareils se séparent logiquement ou se connectent les uns aux autres au moyen de VLANs et d'interfaces. Les fonctionnalités lan avancées incluent IGMP Snooping, DHCP Server et DHCP Options, PoE, Voice Network, 802.1X Control, Port Isolation, Spanning Tree, LLDP-MED et Contrôle de la bande passante.

4. 3. 1 Configurer une connexion Internet

Configuration

Pour configurer une connexion Internet, procédez comme suit :

1.) Sélectionnez le mode WAN.

2.) Configurer les connexions WAN.

3.) (Facultatif) Configurer l'équilibrage de la charge.

Sélectionner le mode WAN > Configurer les connexions WAN > (Facultatif) Configurer l'équilibrage de charge

Atteindre Settings > Wired Networks > Internet pour charger la page suivante. Dans WAN Mode, configurer le nombre de ports WAN déployés par la passerelle et d'autres paramètres. Cliquez ensuite sur Apply.



WAN Ports	Cliquez sur la case à cocher pour activer le port en tant que port WAN. Pour configurer plusieurs ports WAN, activez les ports un par un.
Online Detection Interval	Sélectionnez la fréquence à laquelle les ports WAN détectent l'état de connexion WAN. Si vous ne souhaitez pas activer la détection en ligne, sélectionnez Désactiver.



Note:

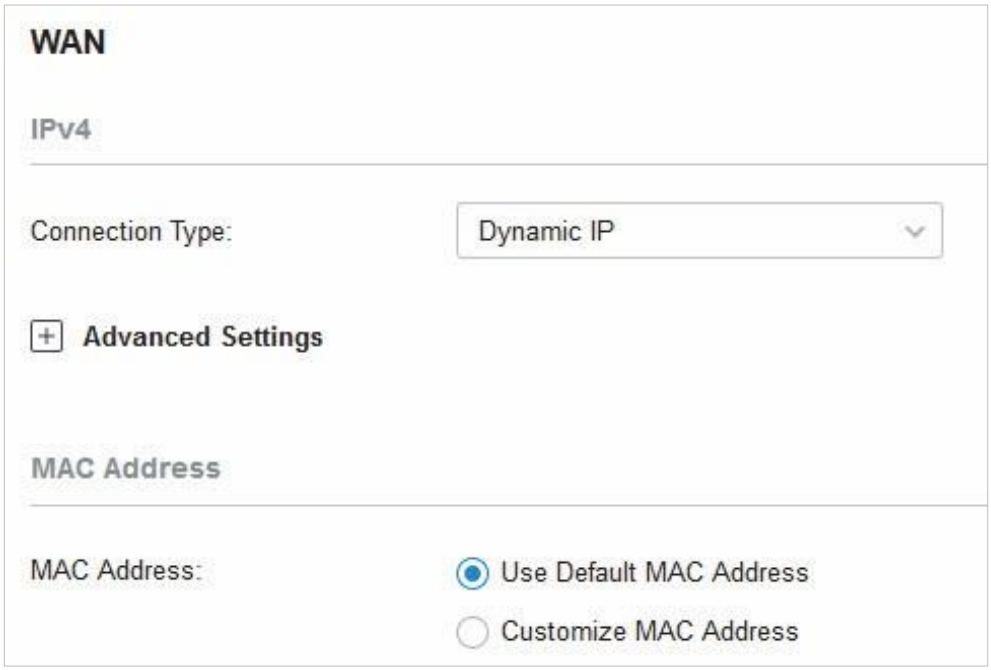
Le nombre de ports WAN configurables est déterminé par le mode WAN.

Allez dans Settings > Wired Networks > Internet. pour les connexions WAN, choisissez un type de connexion en fonction du service fourni par votre FAI.

Connection Type	Dynamic IP : Si votre FAI affecte automatiquement l'adresse IP et les paramètres correspondants, choisissez IP dynamique. Static IP : Si votre FAI vous fournit une adresse IP fixe et les paramètres correspondants, choisissez IP statique. PPPoE: Si votre FAI vous fournit un compte PPPoE, choisissez PPPoE. L2TP: Si votre FAI vous fournit un compte L2TP, choisissez L2TP. PPTP: Si votre FAI vous fournit un compte PPTP, choisissez PPTP.

IP dynamique

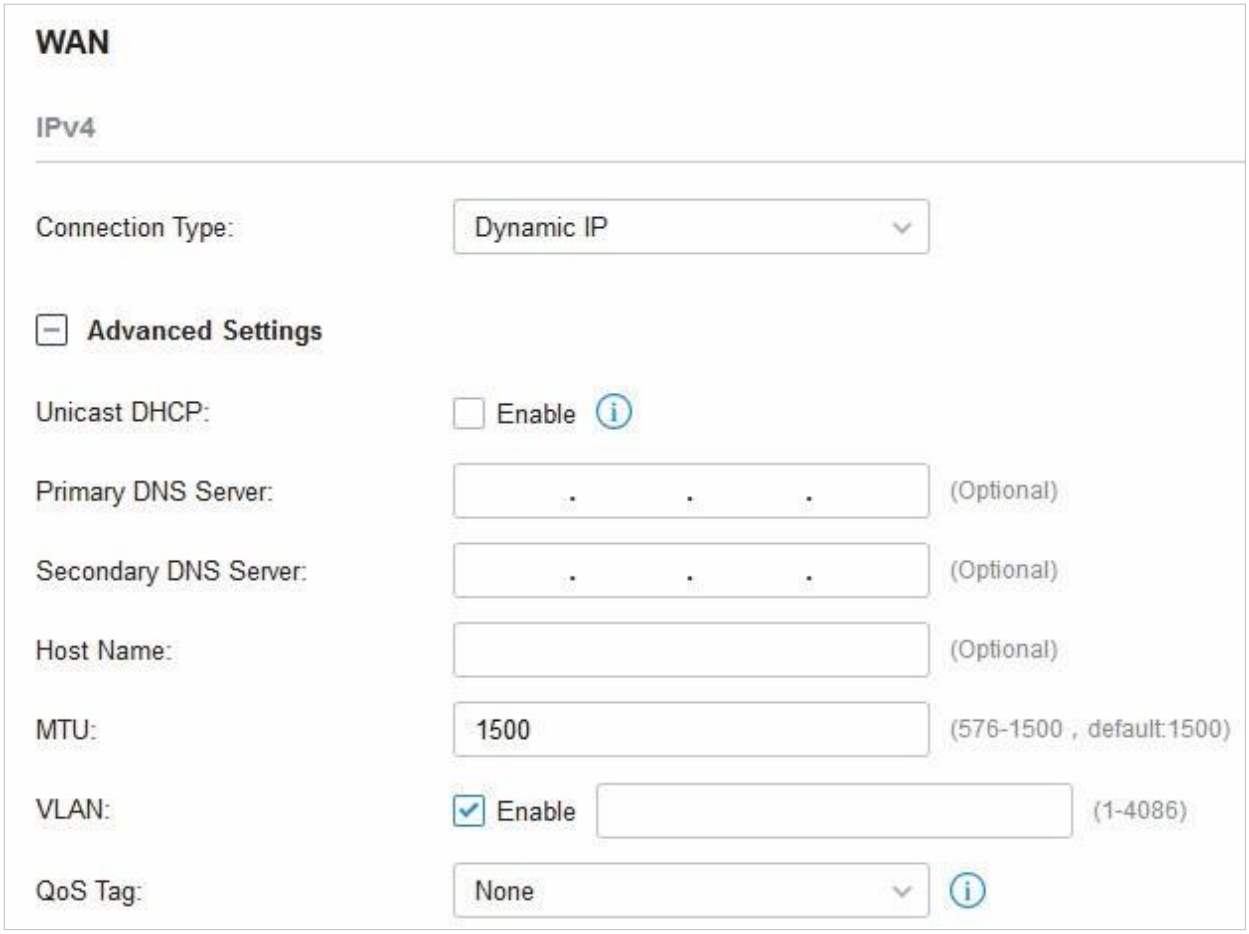
1. Choisissez Type de connexion en tant qu'IP dynamique et configurez les paramètres suivants.



MAC Address Use Default MAC Address: Le port WAN utilise l'adresse MAC par défaut pour configurer la connexion Internet. Il est recommandé d'utiliser l'adresse MAC par défaut, sauf si nécessaire.

Customize MAC Address: Le port WAN utilise une adresse MAC personnalisée pour configurer la connexion Internet et vous devez spécifier l'adresse MAC. En règle générale, cela est nécessaire lorsque votre FAI a lié l'adresse MAC avec votre compte ou votre adresse IP. Si vous n'êtes pas sûr, contactez le FAI.

2. Cliquez sur + Advanced Settings et configurer les paramètres suivants. Cliquez ensuite sur Apply.

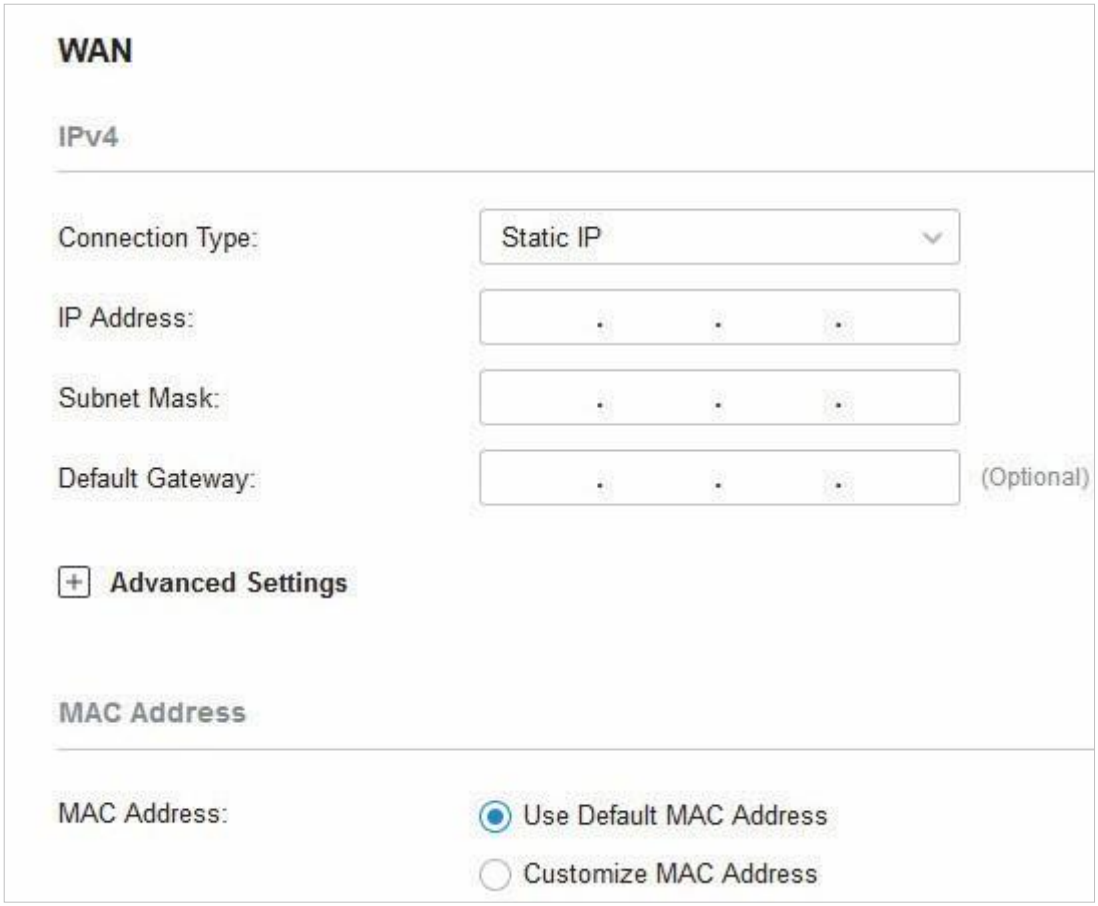


Unicast DHCP	Avec cette option activée, la passerelle exigera que le serveur DHCP affecte l'adresse IP en envoyant des paquets DHCP unicast. Habituellement, vous n'avez pas besoin d'activer l'option.
Primary DNS Server / Secondary DNS Server	Entrez l'adresse IP du serveur DNS fourni par votre FAI s'il y en a.
Host Name	Entrez un nom pour la passerelle.
MTU	Spécifier le MTU (Unité de transmission maximale) du port WAN. MTU est l'unité de données maximale transmise dans le réseau physique. Lorsque le type de connexion est IP dynamique, MTU peut être défini dans la plage de 576-1500 octets. La valeur par défaut est 1500.
VLAN	Ajoutez le port WAN à un VLAN et vous devez spécifier le VLAN. En règle générale, vous n'avez pas besoin de le configurer manuellement à moins que votre FAI ne l'exige.

QoS Tag	La fonction QoS (Qualité de service) permet de prioriser le trafic Internet en fonction de vos besoins. Vous pouvez déterminer le niveau de priorité du trafic en spécifiant la balise. L'étiquette varie de 1 à 7. Aucun ne signifie pas que le paquet sera transmis sans aucune opération. QoS Tag n'est disponible que lorsque VLAN est activé.

IP statique

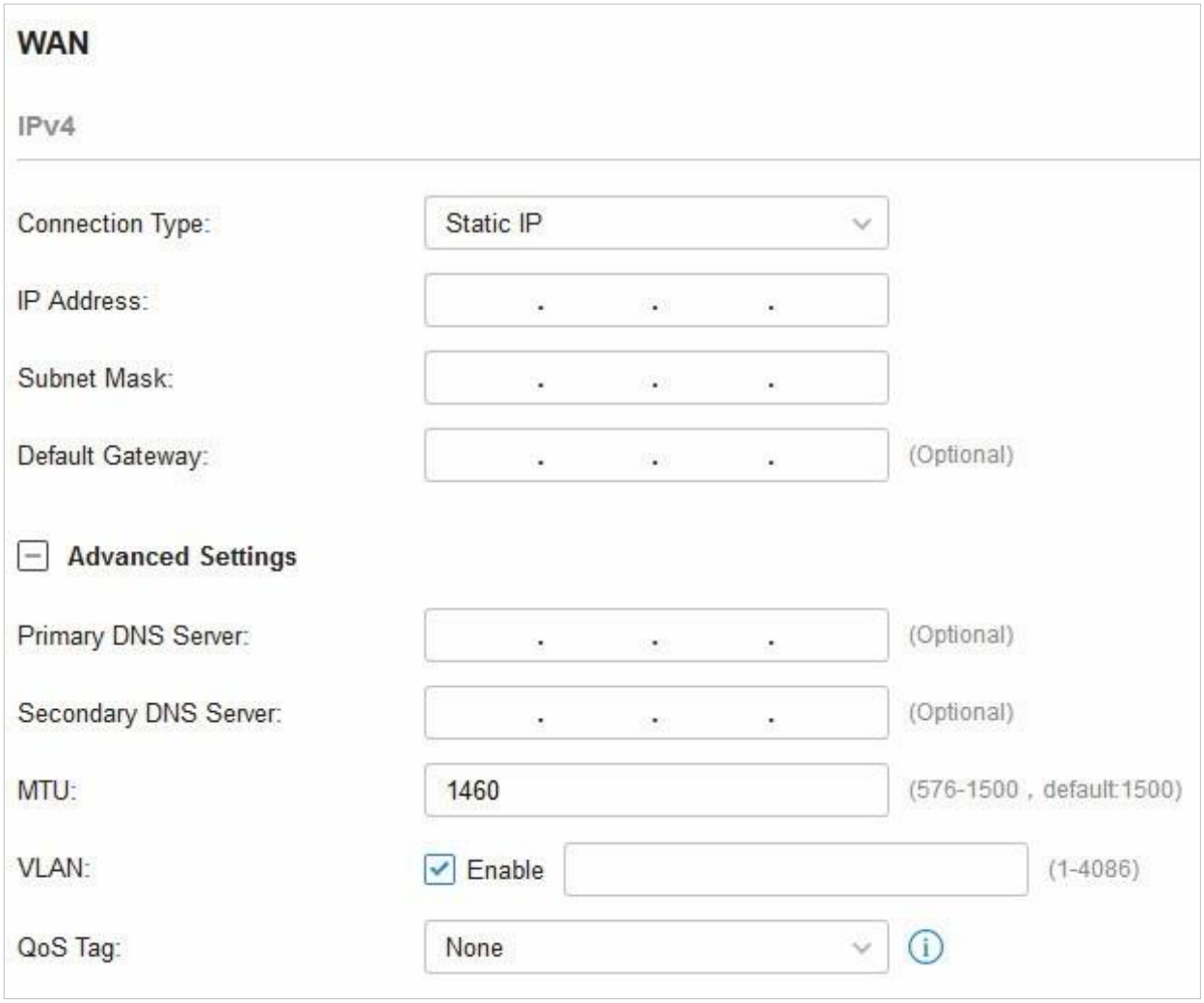
1. Choisissez Type de connexion en tant qu'IP statique et configurez les paramètres suivants.



IP Address	Entrez l'adresse IP fournie par votre FAI.
Subnet Mask	Entrez le masque de sous-réseau fourni par votre FAI.
Default Gateway	Entrez la passerelle par défaut fournie par votre FAI.

2. Cliquez sur + Advanced Settings et configurer les paramètres suivants. Cliquez ensuite sur Apply.

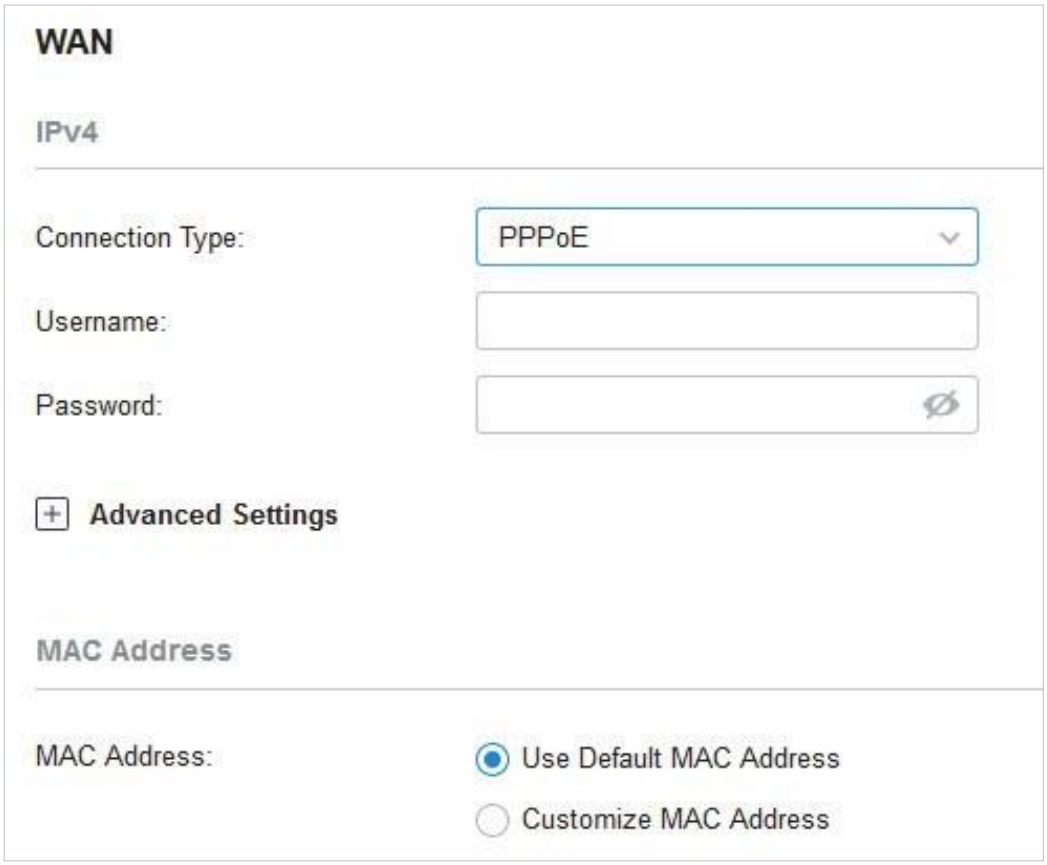
MAC Address	Use Default MAC Address: Le port WAN utilise l'adresse MAC par défaut pour configurer la connexion Internet. Il est recommandé d'utiliser l'adresse MAC par défaut, sauf si nécessaire. Customize MAC Address: Le port WAN utilise une adresse MAC personnalisée pour configurer la connexion Internet et vous devez spécifier l'adresse MAC. En règle générale, cela est nécessaire lorsque votre FAI a lié l'adresse MAC avec votre compte ou votre adresse IP. Si vous n'êtes pas sûr, contactez le FAI.
Primary DNS Server / Secondary DNS Server	Entrez l'adresse IP du serveur DNS fourni par votre FAI s'il y en a.
MTU	Spécifier le MTU (Unité de transmission maximale) du port WAN. MTU est l'unité de données maximale transmise dans le réseau physique. Lorsque le type de connexion est IP statique, MTU peut être défini dans la plage de 576-1500 octets. La valeur par défaut est 1500.
VLAN	Ajoutez le port WAN à un VLAN et vous devez spécifier le VLAN. En général, vous n'avez pas besoin de le configurer manuellement à moins que votre FAI ne l'exige.
QoS Tag	La fonction QoS (Qualité de service) permet de prioriser le trafic Internet en fonction de vos besoins. Vous pouvez déterminer le niveau de priorité du trafic en spécifiant la balise. L'étiquette varie de 1 à 7. Aucun ne signifie pas que le paquet sera transmis sans aucune opération. QoS Tag n'est disponible que lorsque VLAN est activé.


WAN
IPv4
Connection Type:
Static IP
IP Address:
Subnet Mask:
Default Gateway:
(Optional)
Advanced Settings
Primary DNS Server:
(Optional)
Secondary DNS Server:
(Optional)
MTU:
1460
(576-1500 , default:1500)
VLAN:
Enable
(1-4086)
QoS Tag:
None

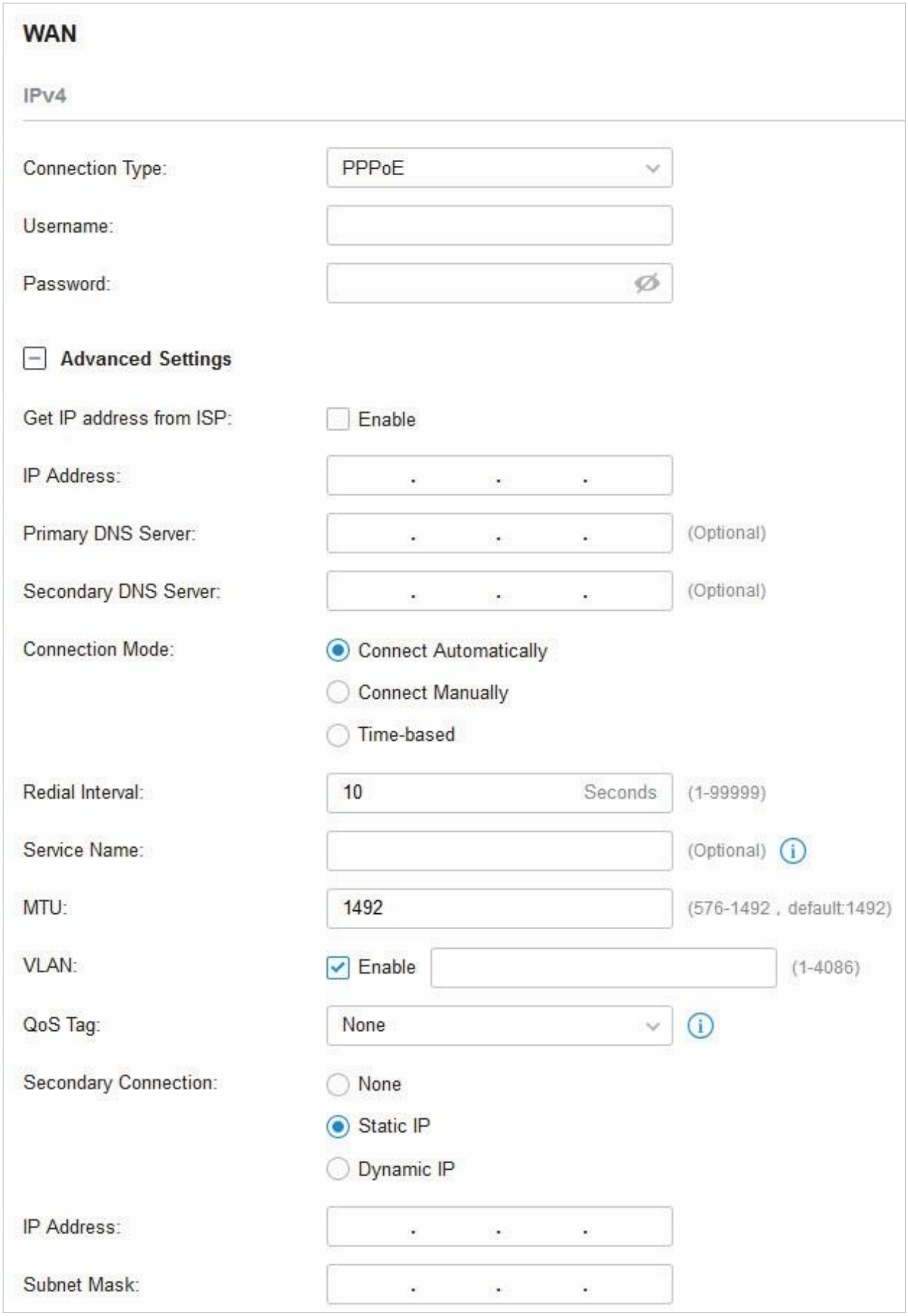
2. Cliquez sur + Advanced Settings et configurer les paramètres suivants. Cliquez ensuite sur Apply.

PPPoE

1. Choisissez Type de connexion en tant qu'IP statique et configurez les paramètres suivants.



Username	Entrez le nom d'utilisateur PPPoE fourni par votre FAI.
Password	Entrez le mot de passe PPPoE fourni par votre FAI.
MAC Address	Use Default MAC Address: Le port WAN utilise l'adresse MAC par défaut pour configurer la connexion Internet. Il est recommandé d'utiliser l'adresse MAC par défaut, sauf si nécessaire. Customize MAC Address: Le port WAN utilise une adresse MAC personnalisée pour configurer la connexion Internet et vous devez spécifier l'adresse MAC. En règle générale, cela est nécessaire lorsque votre FAI a lié l'adresse MAC avec votre compte ou votre adresse IP. Si vous n'êtes pas sûr, contactez le FAI.

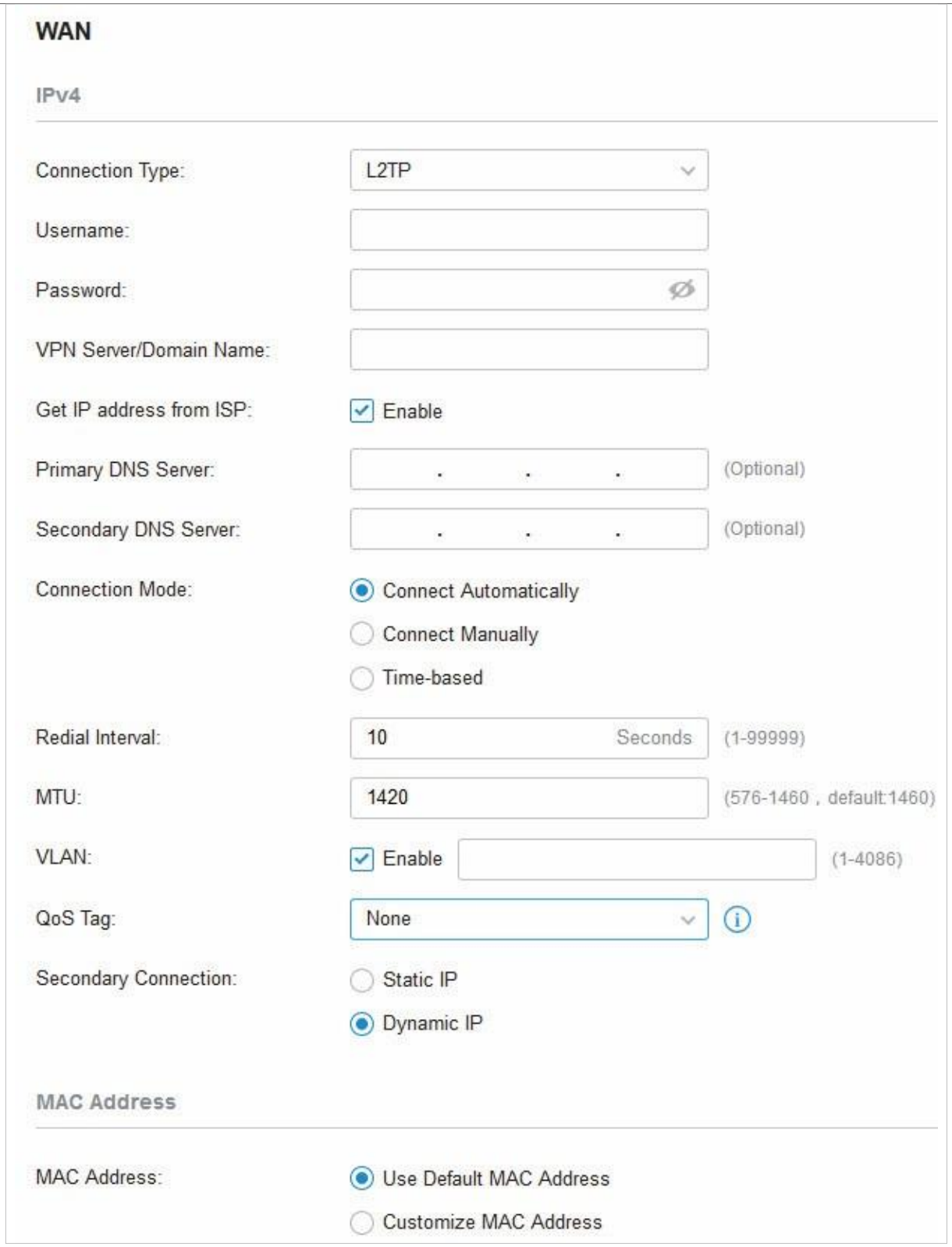

WAN
IPv4
Connection Type:
PPPoE
Username:
Password:
Advanced Settings
Get IP address from ISP:
Enable
IP Address:
Primary DNS Server:
(Optional)
Secondary DNS Server:
(Optional)
Connection Mode:
Connect Automatically
Connect Manually
Time-based
Redial Interval:
10
Seconds
(1-99999)
Service Name:
(Optional)
MTU:
1492
(576-1492 , default:1492)
VLAN:
Enable
(1-4086)
QoS Tag:
None
Secondary Connection:
None
Static IP
Dynamic IP
IP Address:
Subnet Mask:

Get IP address from ISP	Avec cette option activée, la passerelle obtient l'adresse IP du FAI lors de la configuration de la connexion WAN. Avec cette option désactivée, vous devez spécifier l'adresse IP fournie par votre FAI.
Primary DNS Server / Secondary DNS Server	Entrez l'adresse IP du serveur DNS fourni par votre FAI s'il y a.
Connection Mode	Connect Automatically: La passerelle active automatiquement la connexion lorsque la connexion est en panne. Vous devez specifier dans le Redial Interval, qui décide de la fréquence à laquelle la passerelle tente de refaire après la connexion est en panne. Connect Manually: Vous pouvez activer ou terminer manuellement la connexion. Time-Based: Pendant la période spécifiée, la passerelle active automatiquement la connexion. Vous devez spécifier le Time Range lorsque la connexion est en place.
Service Name	Gardez-le vide à moins que votre FAI ne vous oblige à le configurer.
MTU	Spécifier le MTU (Unité de transmission maximale) du port WAN. MTU est l'unité de données maximale transmise dans le réseau physique. Lorsque le type de connexion est PPPoE, MTU peut être défini dans la plage de 576-1492 octets. La valeur par défaut est 1492.
VLAN	Ajoutez le port WAN à un VLAN et vous devez spécifier le VLAN. En règle générale, vous n'avez pas besoin de le configurer manuellement à moins que votre FAI ne l'exige.
QoS Tag	La fonction QoS (Qualité de service) permet de prioriser le trafic Internet en fonction de vos besoins. Vous pouvez déterminer le niveau de priorité du trafic en spécifiant la balise. L'étiquette varie de 1 à 7. Aucun ne signifie pas que le paquet ne pas sera transmis sans aucune opération. QoS Tag n'est disponible que lorsque VLAN est activé.

Secondary Connection	Secondary connection is required by some ISPs. Select the connection type required by your ISP. None: Select this if the secondary connection is not required by your ISP. Static IP: Select this if your ISP provides you with a fixed IP address and subnet mask for the secondary connection. You need to specify the IP Address and Subnet Mask provided by your ISP. Dynamic IP: Select this if your ISP automatically assigns the IP address and subnet mask for the secondary connection.

- **L2TP**

  Choose Connection Type as L2TP and configure the following parameters. Then click Apply.

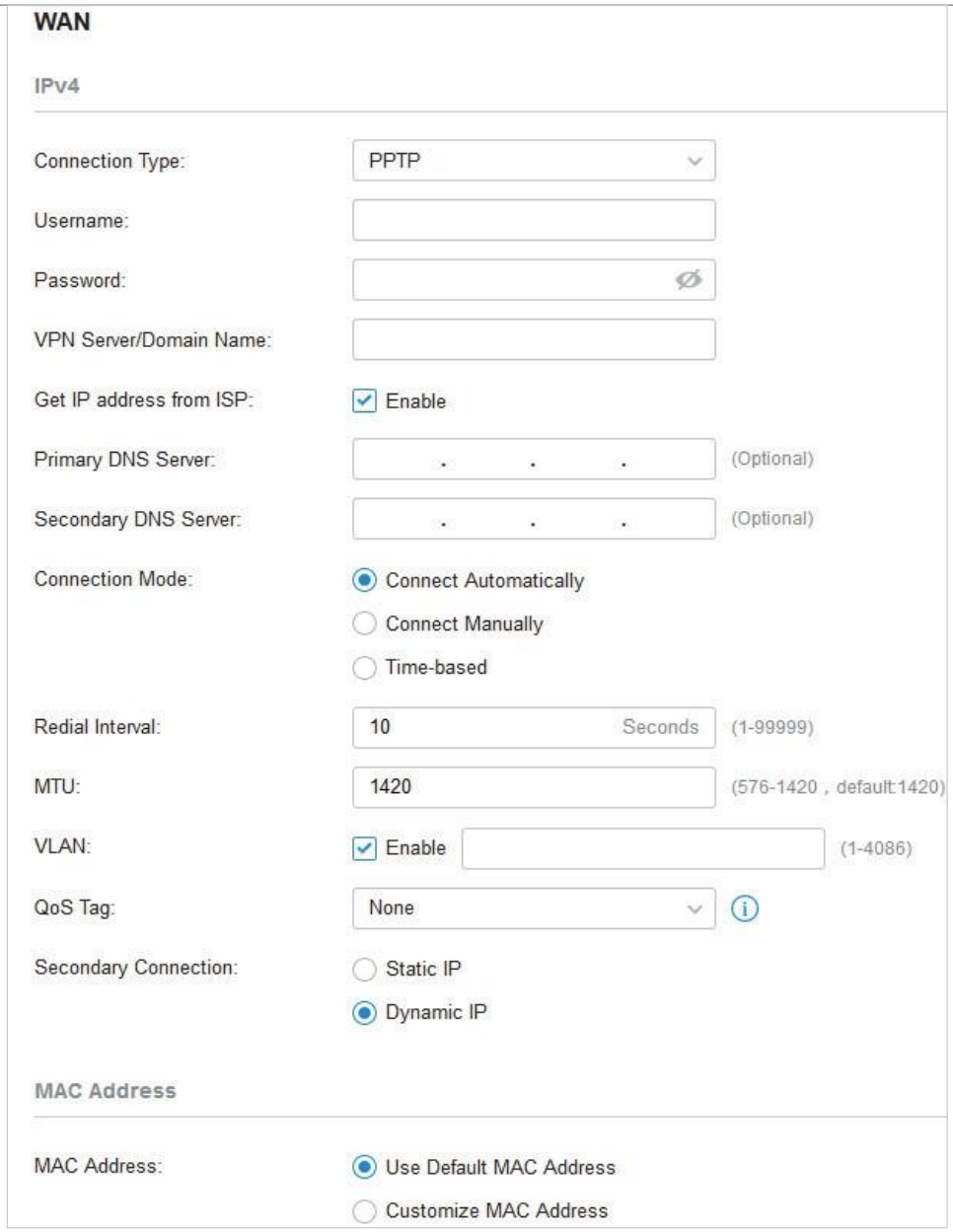

WAN
IPv4
Connection Type:
L2TP
Username:
Password:
VPN Server/Domain Name:
Get IP address from ISP:
Enable
Primary DNS Server:
(Optional)
Secondary DNS Server:
(Optional)
Connection Mode:
Connect Automatically
Connect Manually
Time-based
Redial Interval:
10
Seconds
(1-99999)
MTU:
1420
(576-1460 , default:1460)
VLAN:
Enable
(1-4086)
QoS Tag:
None
Secondary Connection:
Static IP
Dynamic IP
MAC Address
MAC Address:
Use Default MAC Address
Customize MAC Address

Username	Enter the L2TP username provided by your ISP.
Password	Entrez le mot de passe L2TP fourni par votre FAI.
VPN Server / Domain Name	Entrez le serveur VPN/nom de domaine fourni par votre FAI.
Get IP address from ISP	Avec cette option activée, la passerelle obtient l'adresse IP du FAI lors de la configuration de la connexion WAN. Cette option ayant été désactivée, vous devez spécifier l'adresse IP fournie par votre FAI.
Primary DNS Server / Secondary DNS Server	Entrez l'adresse IP du serveur DNS fourni par votre FAI s'il y a.
Connection Mode	Connect Automatically: La passerelle active automatiquement la connexion lorsque la connexion est en panne. Vous devez spécifier le Redial Interval, qui décide de la fréquence à laquelle la passerelle tente de refaire après la connexion est en panne. Connect Manually : Vous pouvez activer ou terminer manuellement la connexion. Time-Based: Pendant la période spécifiée, la passerelle active automatiquement la connexion. Vous devez spécifier leTime Range lorsque la connexion est en place.
MTU	Spécifier le MTU (Unité de transmission maximale) du port WAN. MTU est l'unité de données maximale transmise dans le réseau physique. Lorsque le type de connexion est L2TP, MTU peut être défini dans la plage de 576-1460 octets. La valeur par défaut est 1460.
VLAN	Ajoutez le port WAN à un VLAN et vous devez spécifier le VLAN. En général, vous n'avez pas besoin de le configurer manuellement à moins que votre FAI ne l'exige.
QoS Tag	La fonction QoS (Qualité de service) permet de prioriser le trafic Internet en fonction de vos besoins. Vous pouvez déterminer le niveau de priorité du trafic en spécifiant la balise. L'étiquette varie de 1 à 7. Aucun ne signifie pas que le paquet ne sera pas transmis sans aucune opération. QoS La balise n'est disponible que lorsque VLAN est activé.

Secondary Connection	Select the connection type required by your ISP. Static IP: Select this if your ISP provides you with a fixed IP address and subnet mask for the secondary connection. You need to specify the IP Address, Subnet Mask, Default Gateway (Optional), Primary DNS Server (Optional), and Secondary DNS Server (Optional) provided by your ISP. Dynamic IP: Select this if your ISP automatically assigns the IP address and subnet mask for the secondary connection.
MAC Address	Use Default MAC Address: The WAN port uses the default MAC address to set up the internet connection. It's recommended to use the default MAC address unless required otherwise. Customize MAC Address: The WAN port uses a customized MAC address to set up the internet connection and you need to specify the MAC address. Typically, this is required when your ISP bound the MAC address with your account or IP address. If you are not sure, contact the ISP.

- **PPTP**

  Choose Connection Type as PPTP and configure the following parameters. Then click Apply.



Username	Entrez le nom d'utilisateur PPTP fourni par votre FAI.
Password	Entrez le mot de passe PPTP fourni par votre FAI.
VPN Server / Domain Name	Enter the VPN Server/Domain Name provided by your ISP.

Get IP address from ISP	Avec cette option activée, la passerelle obtient l'adresse IP du FAI lors de la configuration de la connexion WAN. Cette option désactivée, vous devez spécifier l' adresse IP fournie par votre FAI.
Primary DNS Server / Secondary DNS Server	Entrez l'adresse IP du serveur DNS fourni par votre FAI s'il y a.
Connection Mode	Connect Automatically: La passerelle active automatiquement la connexion lorsque la connexion est en panne. Vous devez spécifier le Redial Interval, qui décide de la fréquence à laquelle la passerelle tente de refaire après la connexion est en panne. Connect Manually: Vous pouvez activer ou terminer manuellement la connexion. Time-Based: Pendant la période spécifiée, la passerelle active automatiquement la connexion. Vous devez spécifier leTime Range lorsque la connexion est en place.
MTU	Spécifier le MTU (Unité de transmission maximale) du port WAN. MTU est l'unité de données maximale transmise dans le réseau physique. Lorsque le type de connexion est PPTP, MTU peut être défini dans la plage de 576-1420 octets. La valeur par défaut est 1420.
VLAN	Ajoutez le port WAN à un VLAN et vous devez spécifier le VLAN. En général, vous n'avez pas besoin de le configurer manuellement à moins que votre FAI ne l'exige.
QoS Tag	La fonction QoS (Qualité de service) permet de prioriser le trafic Internet en fonction de vos besoins. Vous pouvez déterminer le niveau de priorité du trafic en spécifiant la balise. L'étiquette varie de 1 à 7. Aucun signifie que le paquet sera transmis sans aucune opération. QoS Tag n'est disponible que lorsque VLAN est activé.
Secondary Connection	Sélectionnez le type de connexion requis par votre FAI. Static IP: Sélectionnez ceci si votre FAI vous fournit une adresse IP fixe et un masque de sous-réseau pour la connexion secondaire. Vous devez spécifier l'adresse IP, Subnet Mask, Default Gateway (Optionelle), Primary DNS Server (Optionelle), et la Secondary DNS Server (Optionelle) fourni par votre FAI. Dynamic IP: Sélectionnez ceci si votre FAI affecte automatiquement l'adresse IP et le masque de sous-réseau pour la connexion secondaire.

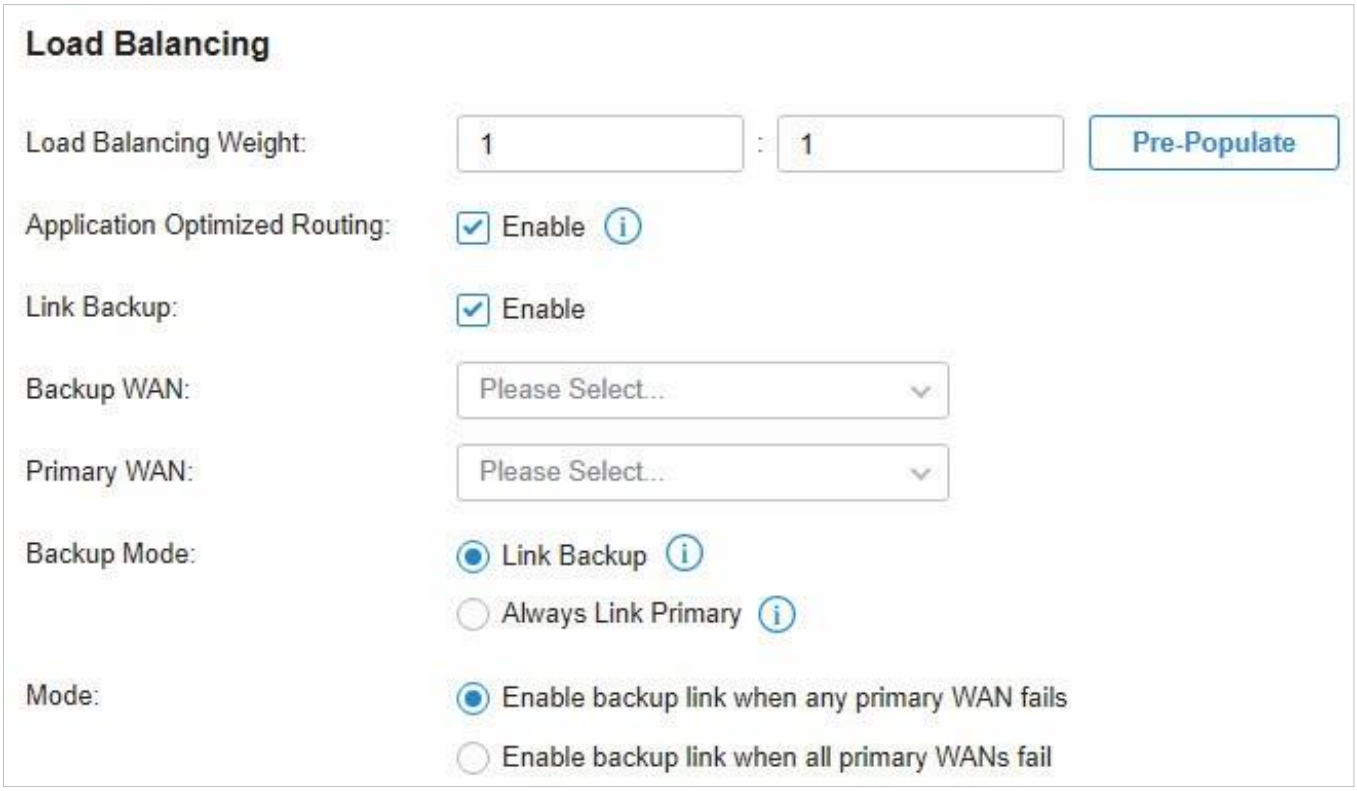
MAC Address	Use Default MAC Address: Le port WAN utilise l'adresse MAC par défaut pour configurer la connexion Internet. Il est recommandé d'utiliser l'adresse MAC par défaut, sauf si nécessaire. Customize MAC Address: Le port WAN utilise une adresse MAC personnalisée pour configurer la connexion Internet et vous devez spécifier l'adresse MAC. En règle générale, cela est nécessaire lorsque votre FAI a lié l'adresse MAC avec votre compte ou votre adresse IP. Si vous n'êtes pas sûr, contactez le FAI.

Sélectionner le mode WAN > Configurer les connexions WAN > (Facultatif) Configurer l'équilibrage de charge

Note:

L'équilibrage de chargement n'est disponible que lorsque vous configurez plusieurs ports WAN.

Allez dans Settings > Wired Networks > Internet pour charger la page suivante. Dans Load Balancing, configurer les paramètres suivants et cliquer sur Apply.



Load Balancing Weight	Spécifiez le ratio de trafic réseau que chaque port WAN transporte. Vous pouvez également cliquer sur Pre-Populate pour tester la vitesse des ports WAN et remplir automatiquement le ratio approprié en fonction du résultat de l'essai.
Application Optimized Routing	Avec l'activation du routage optimisé pour l'application, le routeur tiendra compte de l'adresse IP source et de l'adresse IP de destination (ou du port de destination) des paquets dans son ensemble et enregistrera le port WAN qu'ils traversent. Ensuite, les paquets ayant la même adresse IP source et l'adresse IP de destination (ou port de destination) seront transmis au port WAN enregistré. Cette fonctionnalité garantit que les applications multi-connectées fonctionnent correctement.
Link Backup	Avec Link Backup activé, le routeur commute automatiquement toutes les nouvelles sessions des lignes abandonnées vers une autre pour conserver un réseau toujours en ligne.
Backup WAN / Primary WAN	Le port WAN de sauvegarde, sauvegarde le trafic des ports WAN primaires dans les conditions spécifiées.
Backup Mode	Link Backup : Le système commute automatiquement toutes les nouvelles sessions de la ligne abandonnée à une autre pour conserver un réseau toujours en liaison. Always Link Primary: Le trafic est toujours acheminé par le port WAN principal à moins qu'il ne tombe en panne. Le système va essayer de transférer le trafic via le port wan de sauvegarde quand il échoue, et revenir en arrière quand il récupère.
Mode	Sélectionnez si l'activation d'un lien de sauvegarde en cas d'échec d'un WAN primaire ou d'échec de tous les WAN primaires.

4. 3. 2 Configurer les réseaux LAN

Aperçu

La fonction **LAN** vous permet de configurer le réseau interne câblé. Basé sur 802.1Q VLAN, Omada Controller offre un moyen pratique et flexible de séparer et de déployer le réseau. Le réseau peut être logiquement segmenté par les départements, les applications ou les types d'utilisateurs, sans égard aux emplacements géographiques.

Configuration

Pour créer un réseau local, suivez les lignes directrices :

1.) Créer un réseau avec un but spécifique. Pour l'isolement de la couche 2, créez un réseau en VLAN.

Pour réaliser le routage inter-VLAN, créez un réseau en tant qu'interface IP, qui est configuré avec une interface VLAN.

2.) Créez un profil de port pour le réseau. Le profil définit la façon dont les paquets dans les deux instructions d'entrée et d'évacuation sont manipulés.

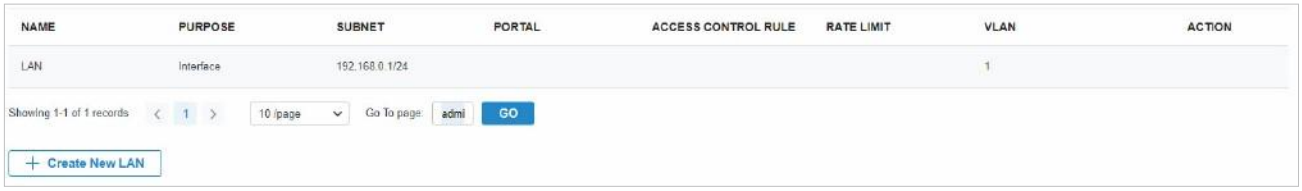
3.) Affectez le profil de port aux ports souhaités du commutateur pour activer le réseau de réseau local.



Note:

Un réseau par défaut (VLAN par défaut) nommé LAN est préconfiguré en tant qu'interface et est associé à tous les ports LAN de la passerelle Omada et de tous les ports de commutateur. L'ID VLAN du réseau par défaut est 1. Le réseau par défaut peut être modifié, mais non supprimé.

1. Allez dans Settings > Wired Networks > LAN > Networks pour charger la page suivante.



1. Cliquez sur + Create New LAN Pour charger la page suivante, entrez un nom pour identifier le réseau et sélectionnez l'objet du réseau.

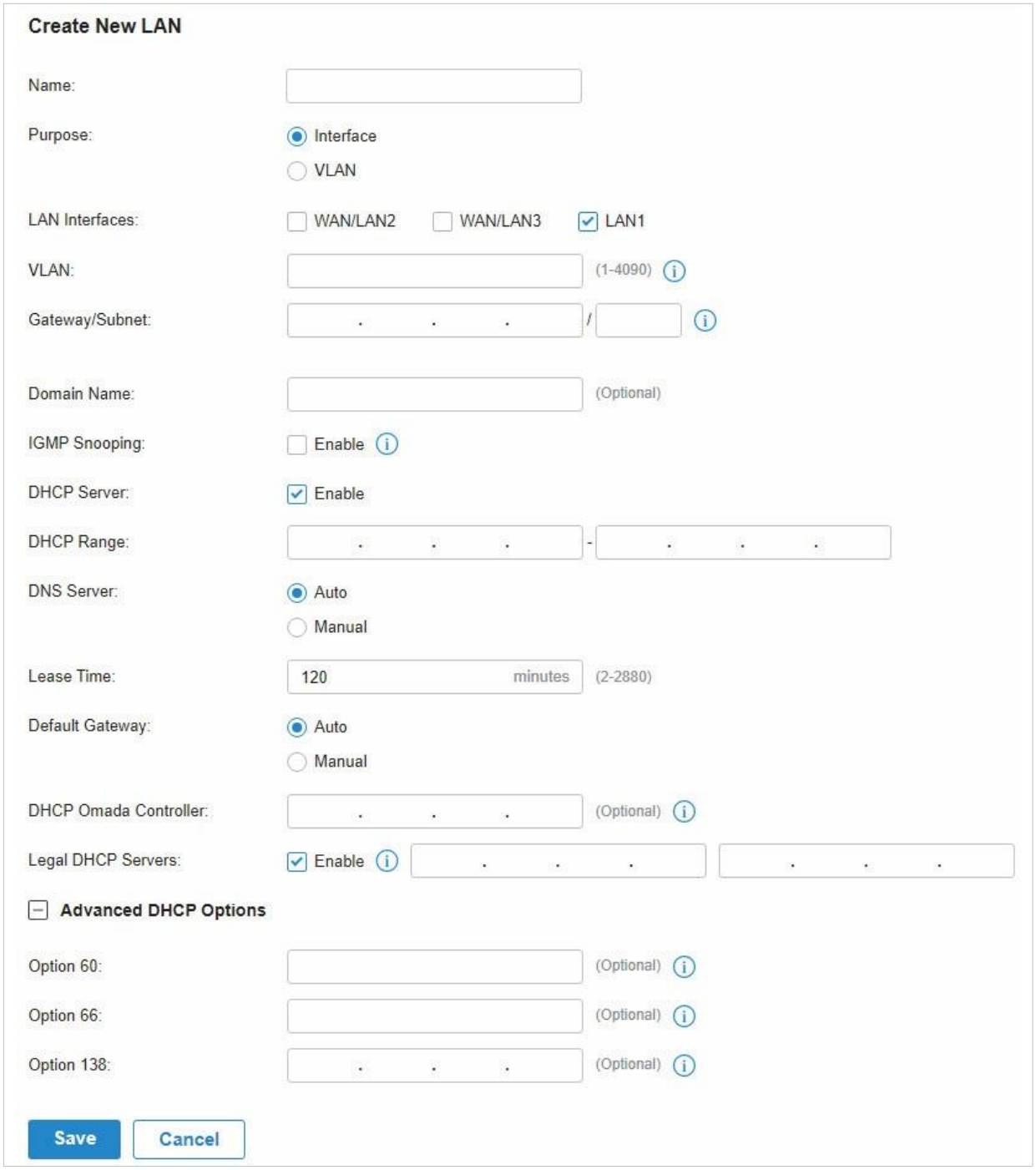


Purpose — Interface: Créer le réseau avec une interface IP de niveau 3, requise pour le routage inter-VLAN.

VLAN: Créer le réseau en tant que VLAN de niveau, par port Ethernet.

2. Configurer les paramètres en fonction de l'objectif du réseau.

■ Interface

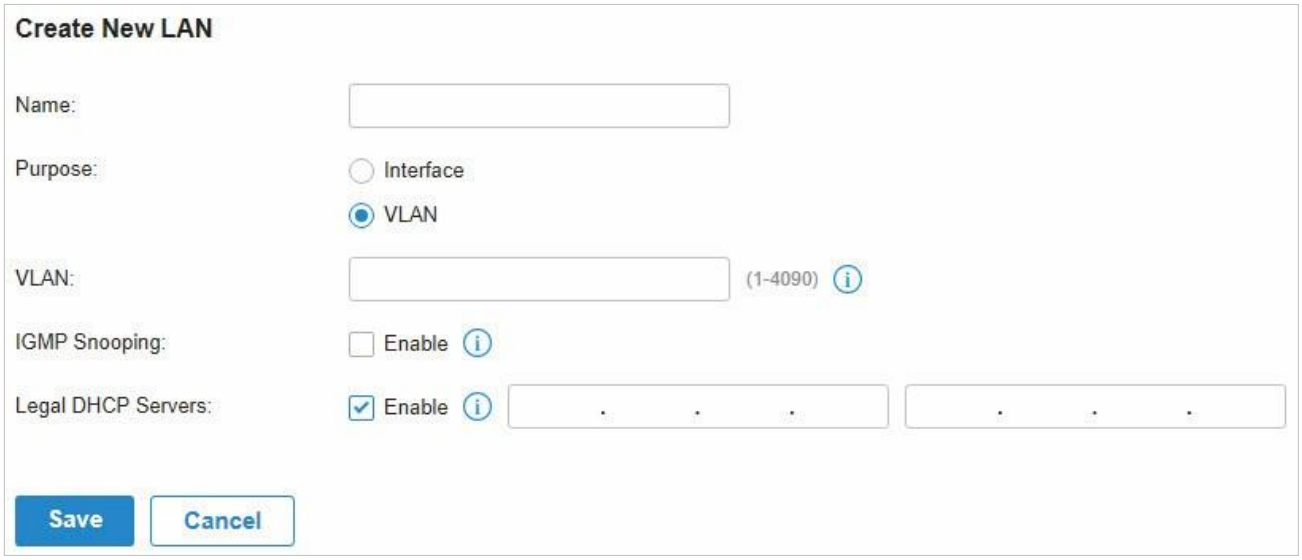


LAN Interface	Sélectionnez les interfaces physiques de la passerelle Omada auxquelles ce réseau sera associé.

VLAN	Entrez un ID VLAN avec les valeurs comprises entre 1 et 4090. Chaque VLAN peut être identifié de façon unique par vlan ID, qui est transmis et reçu sous la forme d'une balise IEEE 802.1Q dans une trame Ethernet.
Gateway/Subnet	Entrez l'adresse IP et le masque de sous-réseau au format CIDR. La notation CIDR inclut ici l'adresse IP et le masque de sous-réseau de la passerelle par défaut. Le résumé des informations que vous avez saisies s'affichera ci-dessous en temps réel.
Domain Name	Entrez le nom de domaine.
IGMP Snooping	Cliquez sur la case à cocher pour surveiller le trafic IGMP (Internet Group Management Protocol) et gérer ainsi le trafic multidiffusion.
DHCP Server	Cliquez sur la case à cocher pour permettre à la passerelle Omada de servir de serveur DHCP pour ce réseau. Un serveur DHCP attribue des adresses IP, un serveur DNS, une passerelle par défaut et d'autres paramètres à tous les périphériques du réseau. Décochez la case s'il existe déjà un serveur DHCP dans le réseau.
DHCP Range	Entrez les adresses IP de départ et de fin du pool d'adresses DHCP dans les champs fournis. Pour une opération rapide, cliquez sur le Update DHCP Range à côté de la Gateway/ Subnet pour obtenir la plage d'adresses IP remplie automatiquement, et modifier la plage en fonction de vos besoins.
DNS Server	Sélectionnez une méthode pour configurer le serveur DNS pour le réseau. Auto: Le serveur DHCP affecte automatiquement le serveur DNS pour les périphériques du réseau. Il utilise l'adresse IP spécifiée dans le Gateway/Subnet entrée en tant qu'adresse serveur DNS. Manual: Spécifiez manuellement les serveurs DNS. Entrez l'adresse IP d'un serveur dans chaque champ serveur DNS.
Lease TIme	Spécifier la durée pendant laquelle un client peut utiliser l'adresse IP affectée à partir de ce pool d'adresses.
Default Gateway	Entrez l'adresse IP de la passerelle par défaut. Auto: Le serveur DHCP affecte automatiquement la passerelle par défaut pour les périphériques du réseau. Il utilise l'adresse IP spécifiée dans l'entrée Gateway/Subnet comme adresse de passerelle par défaut. Manual: Spécifiez manuellement la passerelle par défaut. Entrez l'adresse IP de la passerelle par défaut dans le champ.

DHCP Omada Controller	Entrez l'adresse IP du contrôleur Omada. Le serveur DHCP utilise cette adresse IP comme option 138 dans les paquets DHCP pour indiquer aux clients où se trouve le contrôleur.
Legal DHCP Servers	Cliquez sur la case à cocher pour spécifier les serveurs DHCP légaux pour le réseau. Grâce à la configuration légale des serveurs DHCP, les passerelles et commutateurs Omada garantissent que les clients obtiennent des adresses IP uniquement à partir des serveurs DHCP spécifiés ici.
Option 60	Entrez la valeur de l'option 60 DHCP. Les clients DHCP utilisent ce champ pour identifier éventuellement le type de fournisseur et la configuration d'un client DHCP. La plupart du temps, il est utilisé dans le scénario où les AP s'appliquent pour différentes adresses IP à partir de différents serveurs en fonction des besoins.
Option 66	Entrez la valeur de l'option DHCP 66. Il spécifie les informations du serveur TFTP et prend en charge une seule adresse IP du serveur TFTP.
Option 138	Entrez la valeur de l'option DHCP 138. Il est utilisé pour découvrir les appareils par le contrôleur Omada.

■ VLAN



VLAN	Entrez un ID VLAN avec les valeurs comprises entre 1 et 4090. Chaque VLAN peut être identifié de façon unique par vlan ID, qui est transmis et reçu sous la forme d'une balise IEEE 802.1Q dans un cadre Ethernet.

IGMP Snooping	Cliquez sur la case à cocher pour surveiller le trafic IGMP (Internet Group Management Protocol) et gérer ainsi le trafic multidiffusion.
Legal DHCP Servers	Cliquez sur la case à cocher pour spécifier les serveurs DHCP légaux pour le réseau. Grâce à la configuration légale des serveurs DHCP, les passerelles et commutateurs Omada garantissent que les clients obtiennent des adresses IP uniquement à partir des serveurs DHCP spécifiés ici.

4. Cliquez sur Save

Le nouveau RÉSEAU EST AJOUTÉ à la liste LAN. Vous pouvez cliquer sur dans la colonne ACTION Pour modifier ou supprimer le RÉSEAU LOCAL. Vous pouvez cliquer sur



Créer un réseau → **Créer un profil de port** → Affecter le profil de port aux ports

Note:

1. Trois profils de port par défaut sont préconfigurés sur le contrôleur. Ils peuvent être consultés, mais pas modifiés ou supprimés.

   All: Dans le profil Tout, tous les réseaux, à l'exception du réseau par défaut (LAN), sont configurés en tant que réseau marqué, et le réseau natif est le réseau par défaut (LAN). Ce profil est attribué à tous les ports de commutateur par défaut.

   Disable: Dans le profil Désactiver, aucun réseau n'est configuré en tant que réseau natif, réseaux marqués et réseaux non marqués. Avec ce profil attribué à un port, le port n'appartient à aucun VLAN.

   LAN: Dans le profil LAN, le réseau natif est le réseau par défaut (LAN) et aucun réseau n'est configuré en tant que réseaux marqués et réseaux non marqués.

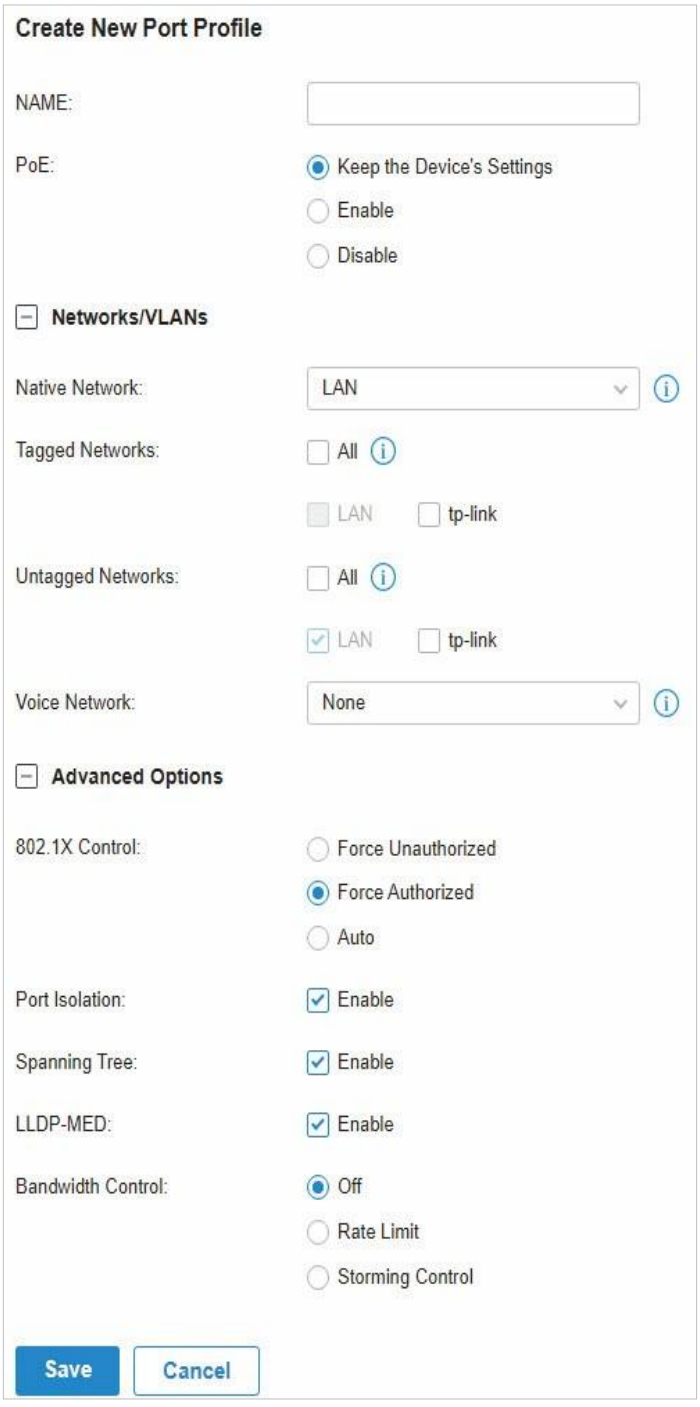
- Lorsqu'un réseau est créé, le système crée automatiquement un profil du même nom et configure le réseau comme réseau natif du profil. Dans ce profil, aucun réseau n'est configuré en tant que réseaux marqués et réseaux non marqués. Le profil peut être consulté, mais non modifié ou supprimé.

1. Atteindre Wired Networks > LAN > Profiles pour charger la page suivante.



2. Cliquez sur + Create New Port Profile pour charger la page suivante et configurer les paramètres suivants pour charger la page suivante et configurer les paramètres suivants.

3.



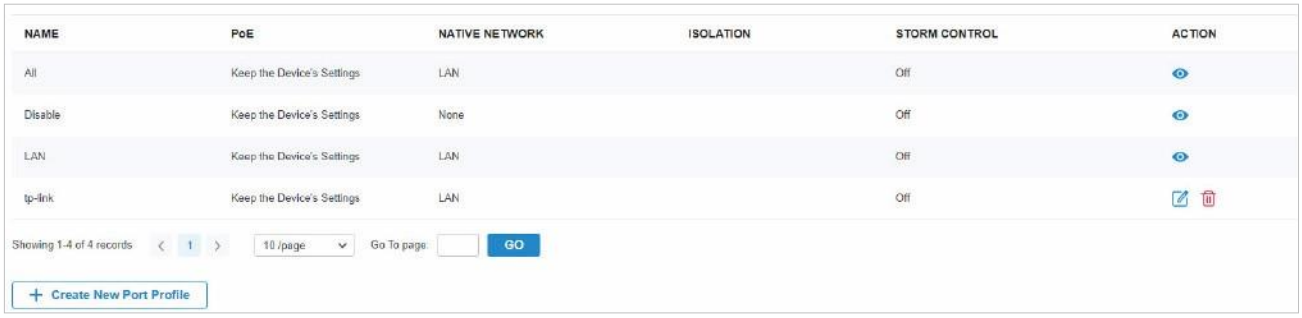
4.

Name	Entrez un nom pour identifier le profil de port.
PoE	Sélectionnez le mode PoE pour les ports. Keep the Device's Settings: PoE garder activé ou désactivé en fonction des paramètres des commutateurs. Par défaut, les commutateurs permettent PoE sur tous les ports PoE. Enable: Activer le PoE sur les ports PoE. Disable: Désactiver le PoE sur les ports PoE.
Native Network	Sélectionnez le réseau natif de tous les réseaux. Le réseau natif détermine l'identificateur VLAN de port (PVID) pour les ports de commutateur. Lorsqu'un port reçoit un cadre non marqué, le commutateur insère une balise VLAN dans le cadre en fonction du PVID et transmet le cadre dans le réseau natif. Chaque port de commutateur physique peut avoir plusieurs réseaux attachés, mais un seul d'entre eux peut être natif.
Tagged Networks	Sélectionnez les réseaux marqués. Les images envoyées à partir d'un réseau marqué sont conservées avec des balises VLAN. Habituellement, les réseaux qui connectent le commutateur à des périphériques réseau comme les routeurs et autres switches, ou les appareils VoIP comme les téléphones IP doivent être configurés comme réseaux marqués.
Untagged Networks	Sélectionnez les réseaux non marqués. Les images envoyées d'un réseau non étiqueté sont dépouillées des balises VLAN. Habituellement, les réseaux qui connectent le commutateur aux périphériques de point de terminaison comme les ordinateurs doivent être configurés en tant que réseaux non marqués. Notez que le réseau natif n'est pas marqué.
Voice Network	Sélectionnez le réseau qui connecte les périphériques VoIP comme les téléphones IP comme réseau vocal. Omada Switches priorisera le trafic vocal en modifiant sa priorité 802.1p. Pour configurer un réseau en tant que réseau vocal, configurez-le d'abord en tant que réseau marqué, puis activez LLDP-MED. Seuls les réseaux marqués peuvent être configurés en tant que réseau vocal, et Voice network entrera en vigueur avec LLDP-MED activé.

802.1X Control	Sélectionnez le mode de contrôle 802.1X pour les ports. Pour configurer l'authentification 802.1X, accédez à **Settings** > **Authentication** > **802.1X**. Auto: Le port n'est pas autorisé jusqu'à ce que le client soit authentifié par le serveur d'authentification avec succès. Force Authorized: Le port reste dans l'état autorisé, envoie et reçoit le trafic normal sans 802.1X authentification du client. Force Unauthorized: Le port reste dans l'état non autorisé, ignorant toutes les tentatives du client pour s'authentifier. Le commutateur ne peut pas fournir des services d'authentification au client via le port.
Port Isolation	Cliquez sur la case à cocher pour activer l'isolement des ports. Un port isolé ne peut pas communiquer directement avec d'autres ports isolés, tandis que le port isolé peut envoyer et recevoir du trafic vers des ports non isolés.
Spanning Tree	Cliquez sur la case à cocher pour activer l'arborescence enjambant. Il permet de s'assurer que vous ne créez pas de boucles lorsque vous avez des chemins redondants dans le réseau. Si vous souhaitez activer l'arborescence enjambant pour le commutateur, vous devez également sélectionner le protocole Spanning Tree dans la page Configuration de périphérique. Pour plus de détails, reportez-vous à Configure and Monitor Switches.
LLDP-MED	Cliquez sur la case à cocher pour activer LLDP-MED (Link Layer Discovery Protocol-Media Endpoint Discovery) pour la découverte de périphériques et la configuration automatique des périphériques VoIP.
Bandwidth Control	Sélectionnez le type de fonctions de contrôle de bande passante pour contrôler le taux de trafic et le seuil de trafic sur chaque port afin d'assurer les performances du réseau. Off: Désactiver le contrôle de bande passante pour le port. Rate Limit: Sélectionnez limite tarifaire pour limiter le taux de trafic d'entrée/sortie sur chaque port. Avec cette fonction, la bande passante réseau peut être raisonnablement distribuée et utilisée. Storm Control: Sélectionnez Storm Control pour permettre au commutateur de surveiller les images de diffusion, les images multidiffusions et les cadres UL (cadres unicast inconnus) dans le réseau. Si le taux de transmission des images dépasse le taux fixé, les images seront automatiquement écartées pour éviter la tempête de diffusion réseau.
Ingress Rate Limit	Quand Rate Limit est sélectionné, cliquez sur la case à cocher et spécifiez la limite de taux supérieure pour recevoir les paquets sur le port.

Egress Rate Limit	Quand Rate Limit est sélectionné, cliquez sur la case à cocher et spécifiez la limite de taux supérieure pour l'envoi de paquets sur le port.
Broadcast Threshold	Quand Storm Control est sélectionné, cliquez sur la case à cocher et spécifiez la limite de taux supérieure pour recevoir des images de diffusion. Le trafic de diffusion dépassant la limite sera traité selon les configurations Action.
Multicast Threshold	Quand Storm Control est sélectionné, cliquez sur la case à cocher et spécifiez la limite de taux supérieure pour recevoir des images multidiffusion. Le trafic multidiffusion dépassant la limite sera traité selon les configurations Action.
UL-Frame Threshold	Quand Storm Control est sélectionné, cliquez sur la case à cocher et spécifiez la limite de taux supérieure pour recevoir des images unicast inconnues. Le trafic dépassant la limite sera traité en fonction des configurations Action.
Action	Quand Storm Control est sélectionné, sélectionnez l'action que le commutateur prendra lorsque le trafic dépasse sa limite correspondante. Avec Drop sélectionné, le port baisse les images suivantes lorsque le trafic dépasse la limite. Avec shutdown sélectionné, le port sera arrêté lorsque le trafic dépasse la limite.

1. Cliquez sur Save. Le nouveau profil de port est ajouté à la liste de profils. Vous pouvez cliquer sur dans la colonne ACTION pour modifier le profil de port.
   Vous pouvez cliquer sur dans la colonne ACTION pour supprimer le profil de port.

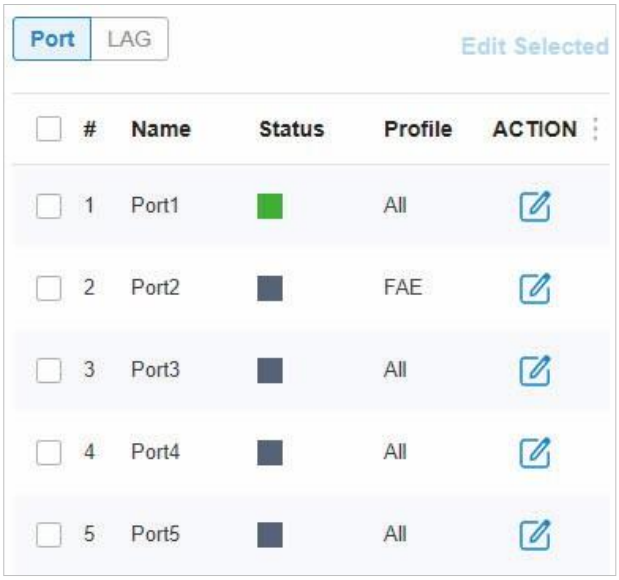


Créer un réseau > Créer un profil de port > Affecter le profil de port aux ports

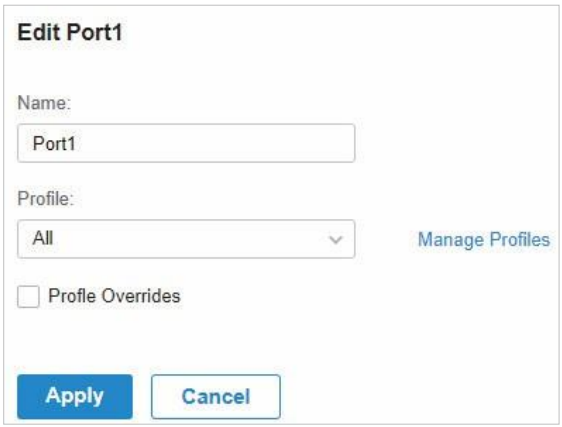
Note:

Par défaut, il existe un profil de port nommé All, qui est attribué à tous les ports de commutateur par défaut. Dans le profil Tout, tous les réseaux, à l'exception du réseau par défaut (LAN), sont configurés en tant que réseau marqué, et le réseau natif est le réseau par défaut (LAN).

1. Dans Settings > Wired Networks > LAN > Networks, et cliquez sur à côté du commutateur dans la liste des périphériques pour révéler la fenêtre Propriétés. Accédez à Ports, vous pouvez cliquer dans la colonne Action pour affecter le profil de port à un seul port, soit sélectionner les ports souhaités et cliquer sur Edit Selected en haut pour affecter le profil de port à plusieurs ports par lots.



2. Sélectionnez le profil dans la liste déroulante pour affecter le profil de port aux ports souhaités du commutateur. Vous pouvez activer les substitutions de profil pour personnaliser les paramètres des ports, et toute la configuration remplace ici le profil de port. Pour plus de détails, reportez-vous à Configure and Monitor Omada Managed Devices.



4. 4 Configurer les réseaux sans fil

Les réseaux sans fil permettent à vos clients sans fil d'accéder à Internet. Une fois que vous avez configuré un réseau sans fil, vos EAP diffusent généralement le nom du réseau (SSID) dans les airs, grâce auxquels vos clients sans fil se connectent au réseau sans fil et accèdent à Internet.

Un groupe WLAN est une combinaison de réseaux sans fil. Configurez chaque groupe afin que vous puissiez appliquer de manière flexible ces groupes de réseaux sans fil à différents EAP en fonction de vos besoins.

Après avoir configuré les réseaux sans fil de base, vous pouvez configurer davantage WLAN Schedule, 802.11 Rate Control et MAC Filter parmi d'autres paramètres avancés.

4. 4. 1 Configurer les réseaux sans fil de base

Configuration

Pour créer, configurer et appliquer des réseaux sans fil, procédez comme suit :

1.) Créez un groupe WLAN.

2.) Créer des réseaux sans fil

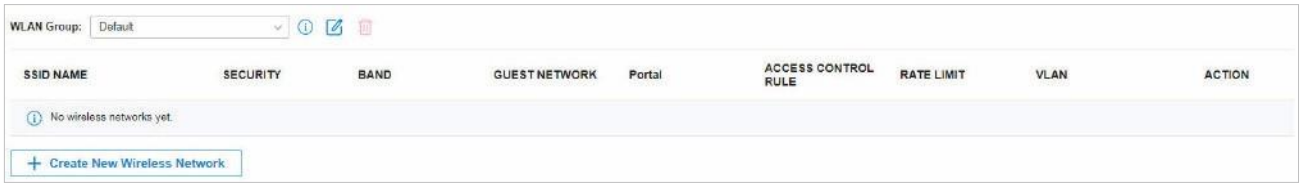
3) Appliquer le groupe WLAN à vos EAP



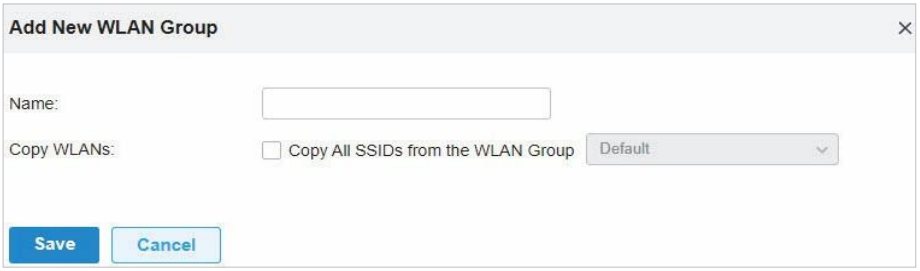
Note:

Par défaut, il existe un groupe WLAN nommé Default, qui est appliqué à tous les EAP. Si vous souhaitez simplement configurer des réseaux sans fil pour le groupe WLAN par défaut et l'appliquer à tous vos EAP, sautez cette étape.

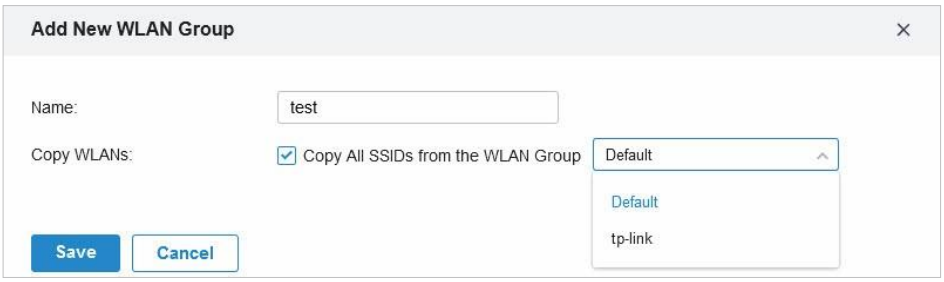
1. Atteindre Settings > Wireless Networks pour charger la page suivante.



1. Sélectionnez + Create New Group à partir de la liste déroulante de WLAN Group pour charger la page suivante. Entrez un nom pour identifier le groupe WLAN.



2. (Facultatif) Si vous souhaitez créer un nouveau groupe WLAN basé sur un groupe existant, Copy All SSIDs from the WLAN Group et sélectionnez le groupe WLAN souhaité. Ensuite, vous pouvez configurer davantage les réseaux sans fil en fonction des paramètres actuels.



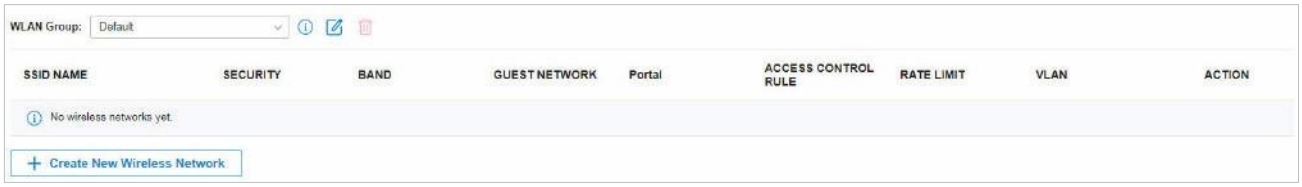
3. Cliquez sur Save. Le nouveau groupe WLAN est ajouté à la liste WLAN Group. Vous pouvez sélectionner un groupe WLAN

Pour modifier le nom of the WLAN Group. Vous pouvez cliquer pour supprimer le groupe WLAN.

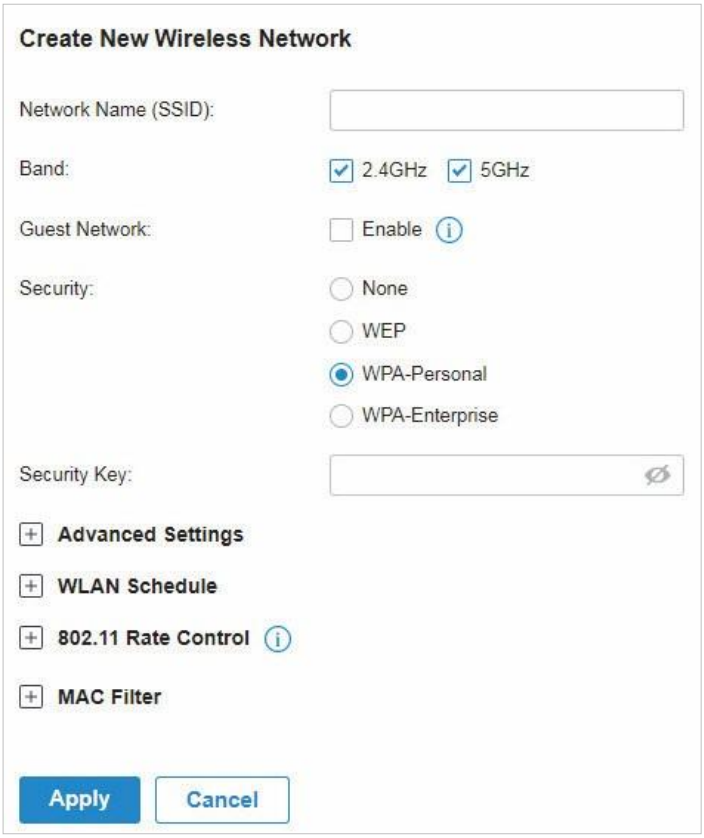


Créer un groupe WLAN | Créer des réseaux sans fil | Appliquer le groupe WLAN

1. Sélectionnez le groupe WLAN pour lequel vous souhaitez configurer les réseaux sans fil à partir de la liste déroulante du Groupe WLAN.



2. Cliquez sur + Create New Wireless Network pour charger la page suivante. Configurez les paramètres de base du réseau.



Network Name (SSID)	Entrez le nom du réseau (SSID) pour identifier le réseau sans fil. Les utilisateurs de clients sans fil choisissent de se connecter au réseau sans fil selon le SSID, qui apparaît sur la page de paramètres WLAN des clients sans fil.
Band	Activez la bande radio de 2,4 GHz et/ou 5 GHz pour le réseau sans fil.
Guest Network	Avec guest network activé, tous les clients se connectant au SSID sont bloqués pour atteindre n'importe quel sous-réseau IP privé.

1. Sélectionnez la stratégie de sécurité pour le réseau sans fil.

- **None**

  Avec Aucun sélectionné, les hôtes peuvent accéder au réseau sans fil sans authentification, ce qui est applicable à des exigences de sécurité inférieures.

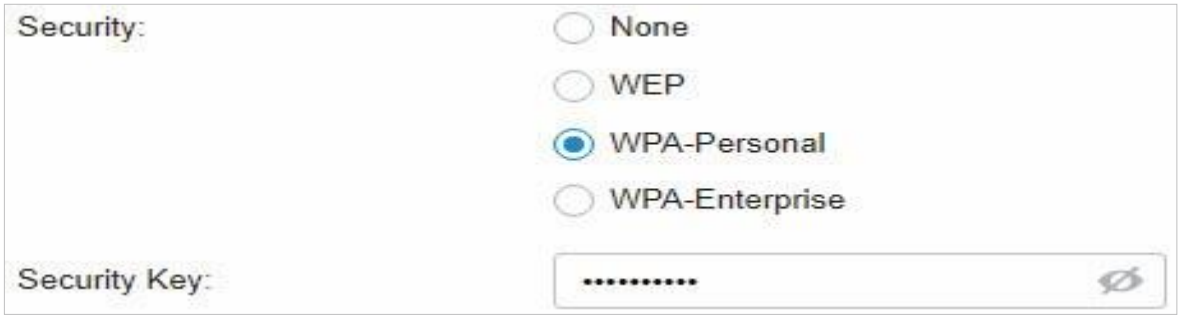
- **WEP**

  Le trafic est crypté avec une clé WEP, que vous devez spécifier. WEP n'est pas recommandé parce qu'il est précaire.



- **WPA-Personal**

Le trafic est crypté avec une clé de sécurité, que vous devez spécifier. WPA-Personal est plus sûr que WEP.

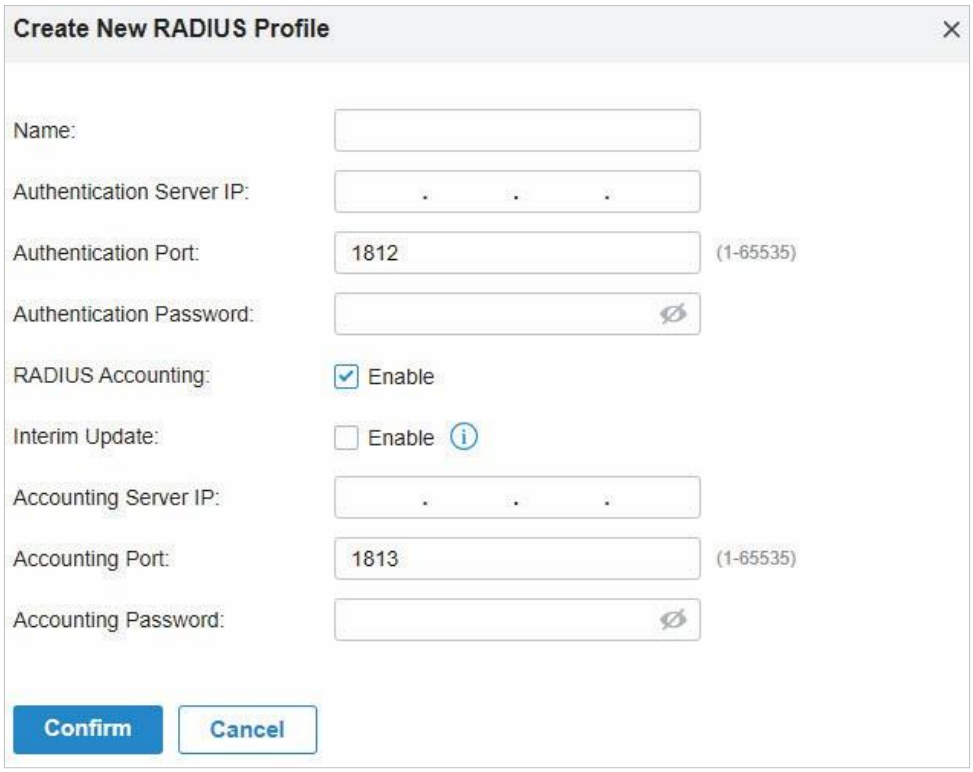


- **WPA-Enterprise**

WPA-Enterprise nécessite un serveur d'authentification pour authentifier les clients sans fil, et probablement un serveur comptable pour enregistrer les statistiques de trafic.



Sélectionnez un profil RADIUS, qui enregistre les paramètres du serveur d'authentification et du serveur comptable. Vous pouvez créer un profil RADIUS en cliquant sur + Create New Radius Profile à partir de la liste déroulante du profil RADIUS. Pour plus de détails, reportez-vous à Authentication.



4. (Facultatif) Vous pouvez également configurer Advanced Settings, WLAN Schedule, 802.11 Rate Control, Et MAC Filter selon vos besoins. Les sujets connexes sont abordés plus loin dans ce chapitre.

1. Cliquez sur Apply. Le nouveau réseau sans fil est ajouté à la liste des réseaux sans fil sous le groupe WLAN. Vous pouvez cliquer sur dans la colonne ACTION



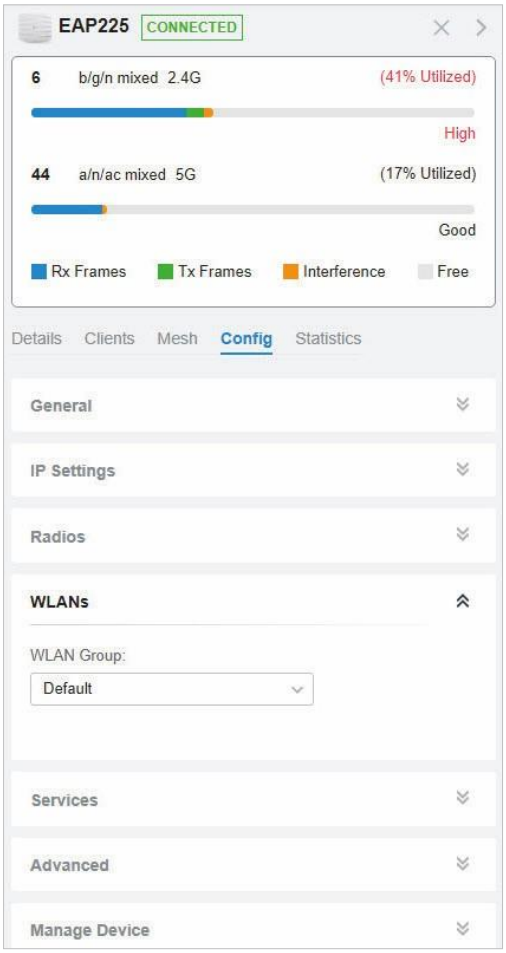


Note:

La colonne ACTION permet de modifier le réseau sans fil. Vous pouvez cliquer sur colonne pour supprimer le réseau sans fil. Par défaut, il existe un groupe WLAN nommé Default, qui est appliqué à tous les EAP. Si vous souhaitez simplement configurer des réseaux sans fil pour le groupe WLAN par défaut et l'appliquer à tous vos EAP, sautez cette étape.

■ **Appliquer à un EAP unique**

Accédez à Périphériques, sélectionnez l'EAP auquel vous souhaitez appliquer le groupe WLAN. Dans la fenêtre Propriétés, accédez à Config > WLANs, sélectionnez le groupe WLAN que vous souhaitez appliquer au EAP.

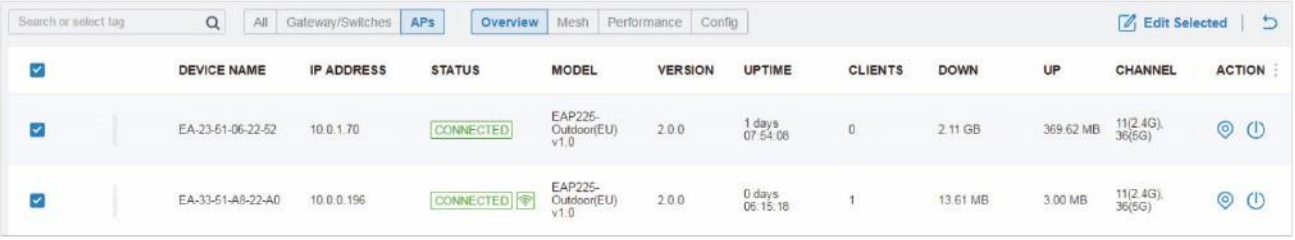


■ **Appliquer aux EAP dans le lot**

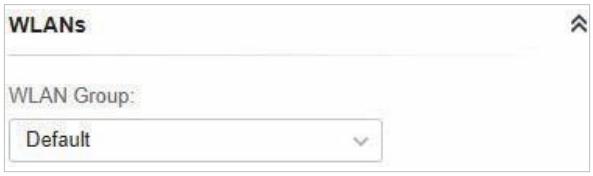
1.Allez dans Devices, Sélectionnez APs

Cliquez sur , Sélectionnez Batch Config .

Cochez les cases des EAP auxquels vous souhaitez appliquer le groupe WLAN, puis cliquez sur Edit Selected

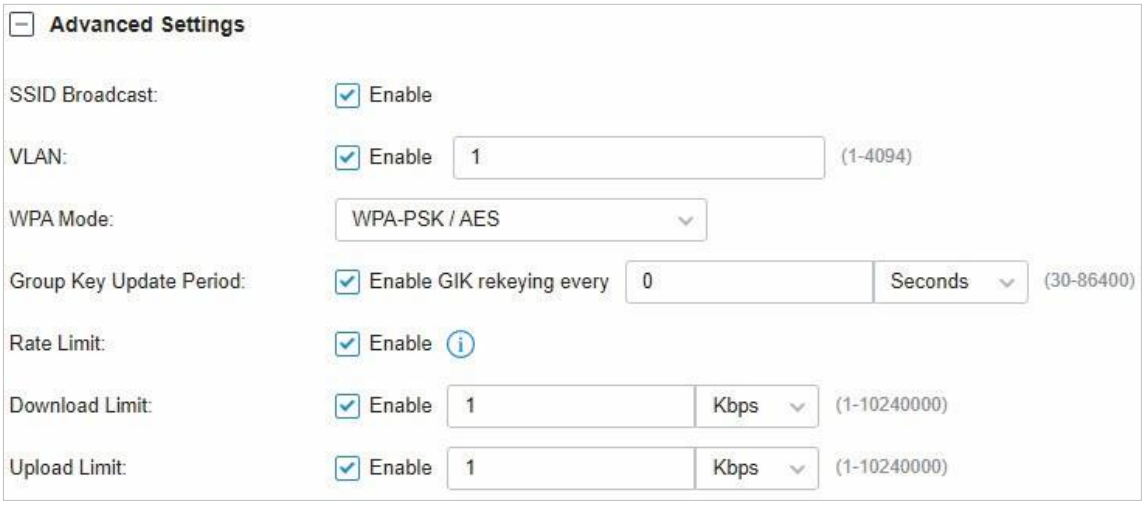


2. Dans la fenêtre Propriétés, accédez à Config > WLANs, sélectionnez le groupe WLAN que vous souhaitez appliquer aux EAP.



4. 4. 2 Paramètres avancés

Atteindre Settings > Wireless Networks, Cliquez sur dans la colonne ACTION du réseau sans fil que vous souhaitez configurer, puis cliquez sur + Advanced Settings pour charger la page suivante. Configurer les paramètres et cliquer sur Apply.



SSID Broadcast	Grâce à la diffusion SSID activée, les EAP diffusent le SSID (nom du réseau) en l'air afin que les clients sans fil puissent se connecter au réseau sans fil, ce qui est identifié par le SSID. Avec la diffusion SSID désactivée, les utilisateurs de clients sans fil doivent entrer le SSID manuellement pour se connecter au réseau sans fil.
VLAN	Pour définir un VLAN sans fil pour le réseau sans fil, activez cette option et définissez un ID VLAN de 1 à 4094. Avec cette option activée, le trafic dans différents réseaux sans fil est marqué par différentes balises VLAN selon le ID VLAN configurés. Ensuite, les EAP travaillent en collaboration avec les commutateurs qui supportent également le 802.1Q VLAN, pour distribuer le trafic à différents VLAN selon les balises VLAN. Par conséquent, les clients sans fil de différents VLAN ne peuvent pas communiquer directement les uns avec les autres.
WEP Mode	Si vous sélectionnez WEP comme stratégie de sécurité, vous pouvez sélectionner le mode WEP, y compris le type d'authentification WEP, le format de clé WEP et la longueur de la clé WEP. Sélectionner le type d'authentification WEP. Open System: Les clients sans fil peuvent passer l'authentification et se connecter au réseau sans fil sans mot de passe. Toutefois, le mot de passe correct est requis pour la transmission de données. Shared Key: Le mot de passe correct est nécessaire pour que les clients sans fil passent l'authentification, se connectent au réseau sans fil et transmettent des données. Auto: Les EAP décident automatiquement d'utiliser le système ouvert ou la clé partagée dans le processus d'authentification. Sélectionner le format de clé WEP. ASCII: Le format ASCII représente toute combinaison de caractères clavier de la longueur spécifiée. Hexadecimal: Le format hexadécimal signifie n'importe quelle combinaison de chiffres hexadécimals (0-9, A-F) avec la longueur spécifiée. Sélectionnez la longueur de la clé WEP. 64Bit: La clé WEP est de 10 chiffres hexadécimals ou 5 caractères ASCII. 128Bit: La clé WEP est de 26 chiffres hexadécimal ou 13 caractères ASCII. 152Bit: La clé WEP est de 32 chiffres hexadécimal ou 16 caractères ASCII.

WPA Mode	Si vous sélectionnez WPA-Personal ou WPA-Enterprise comme stratégie de sécurité, vous pouvez sélectionner le mode WPA comprenant la version WPA et le type de chiffrement. Sélectionnez la version WPA en fonction de vos besoins. Sélectionnez le type de chiffrement. Un type de chiffrement n'est disponible que dans certaines circonstances. TKIP: TKIP signifie Protocole d'intégrité des clés temporelles. AES: AES signifie Advanced Encryption Standard. Nous vous recommandons de sélectionner AES comme type de chiffrement pour qu'il soit plus sécurisé que TKIP. Auto: Les PAE décident automatiquement d'utiliser le TKIP ou l'AES dans le processus d'authentification.
Group Key Update Period	Si vous sélectionnez WPA-Personal ou WPA-Enterprise comme stratégie de sécurité, vous pouvez spécifier si et à quelle fréquence la clé de sécurité change. Si vous souhaitez que la clé de sécurité change périodiquement, activez le rekeying GIK et spécifiez la période de temps.
Rate Limit	Vous pouvez limiter le taux de téléchargement et de téléchargement de chaque client pour équilibrer l'utilisation de la bande passante. Download Limit: Définir le taux de téléchargement pour chaque client pour recevoir le trafic. Upload Limit: Définir le taux de téléchargement pour chaque client afin de transmettre le trafic.

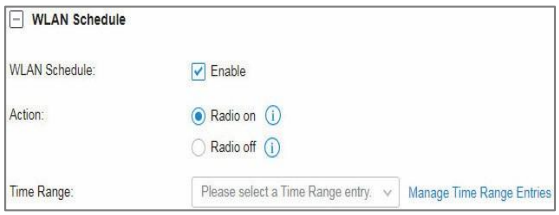
4. 4. 3 Paramétrage Horaire WLAN (schedule)

Aperçu

WLAN Schedule peut activer ou désactiver votre réseau sans fil dans la période de temps spécifique que vous le souhaitez.

Configuration

Accéder à Paramètres >Réseaux sans fil, cliquez dans la colonne ACTION du réseau sans fil que vous souhaitez configurer, puis cliquez sur + WLAN Schedule pour charger la page suivante. Activer la planification WLAN et configurer les paramètres. Cliquez ensuite surApply.



Action	Radio On: Activez votre réseau sans fil dans la plage de temps que vous définissez et désactivez-le au-delà de la plage de temps. Radio Off: Désactivez votre réseau sans fil dans la plage de temps que vous définissez et activez-le au-delà de la plage de temps.
Time Range	Sélectionnez la plage de temps pour que l'action prenne effet. Vous pouvez créer une entrée de plage de temps en cliquant sur + Create New Time Range Entry à partir de la liste déroulante de Time Range. Pour plus de détails, reportez-vous à Create Profiles.

4. 4. 4 802.11 Contrôle des seuils

Aperçu

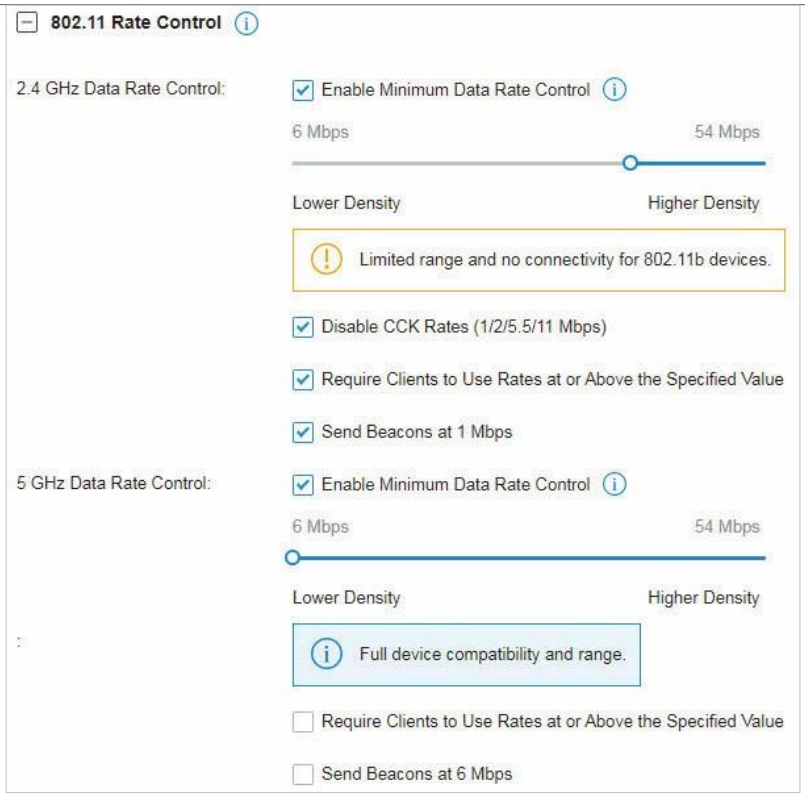
Note:

802.11 Le contrôle des seuils n'est disponible que pour certains appareils.

802.11 Rate Control peut améliorer les performances des réseaux à densité plus élevée en désactivant des débits de bits plus faibles et en ne permettant que les plus élevés. Toutefois, le contrôle des tarifs 802.11 peut rendre certains périphériques hérités incompatibles avec vos réseaux et limiter la portée de vos réseaux sans fil..

Configuration

Atteindre Settings > Wireless Networks, cliquez dans la colonne ACTION du réseau sans fil que vous souhaitez configurer, puis cliquez sur + 802.11 Rate Control pour charger la page suivante. Sélectionnez la bande de 2,4 GHz et/ou 5 GHz pour permettre un contrôle minimal du débit de données en fonction de vos besoins, déplacez le curseur pour déterminer les taux de bits autorisés par votre réseau sans fil et configurez les paramètres. Cliquez ensuite surApply.



Disable CCK Rates (1/2/5.5/11 Mbps)	Sélectionnez désactiver le CCK (Complementary Code Keying), le schéma de modulation qui fonctionne avec les périphériques 802.11b. Disable CCK Rates (1/2/5.5/11 Mbps) n'est disponible que pour la bande de 2,4 GHz.
Require Clients to Use Rates at or Above the Specified Value	Sélectionnez, s'il faut ou non exiger des clients qu'ils utilisent des taux à ou supérieure à la valeur que le curseur indique.
Send Beacons at 1 Mbps/6 Mbps	Sélectionnez d'envoyer ou non des balises au taux minimum de 1 Mbps pour la bande de 2,4 GHz ou de 6 Mbps pour la bande de 5 GHz.

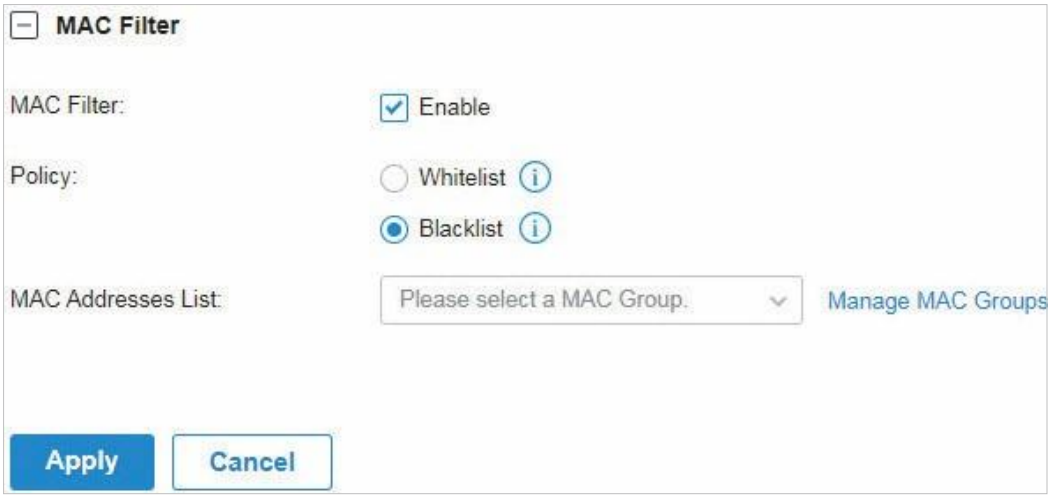
4. 4. 5 Filtrage MAC

Aperçu

MAC Filter permet ou bloque les connexions à partir de clients sans fil d'adresses MAC spécifiques.

Configuration

Allez dans Settings > Wireless Networks, cliquez dans la colonne ACTION du réseau sans fil que vous souhaitez configurer, puis cliquez sur + Filtre MAC pour charger la page suivante. Activer mac filtre et configurer les paramètres. Cliquez ensuite sur Apply.



Policy	Whitelist: Autoriser la connexion des clients dont les adresses MAC se trouvent dans le MAC spécifié Liste d'adresses, tout en bloquant d'autres. Blacklist: Bloquer la connexion des clients dont l'adresse MAC se trouve dans la liste d'adresses MAC spécifiée, tout en permettant à d'autres.
MAC Address List	Sélectionnez le groupe MAC que vous souhaitez autoriser ou bloquer en fonction de la stratégie. Vous pouvez créer un nouveau groupe MAC en cliquant sur + Create New MAC Group à partir de la liste déroulante de la liste d'adresses MAC. Pour plus de détails, reportez-vous à Create Profiles.

4. 5 Sécurité réseau

Network Security est un portefeuille de fonctionnalités conçues pour améliorer la facilité d'utilisation et assurer la sécurité de votre réseau et de vos données. Les services de sécurité réseau incluent ACL, LE Filtrage d'URL et Attack Defense, qui implémentent des stratégies et des contrôles sur plusieurs couches de défenses dans le réseau.

4. 5. 1 ACL

Aperçu

ACL (Liste de contrôle d'accès) permet à un administrateur réseau de créer des règles pour restreindre l'accès aux ressources réseau. Les règles ACL filtrent le trafic en fonction de critères spécifiés tels que les adresses IP source, les adresses IP de destination et les numéros de port, et déterminent s'il convient de transférer les paquets correspondants. Ces règles peuvent être appliquées à des clients ou des groupes spécifiques dont le trafic passe par la passerelle, les commutateurs et les EAP.

Le système filtre le trafic par rapport aux règles de la liste séquentiellement.

La première correspondance détermine si le paquet est accepté ou abandonné, et d'autres règles ne sont pas vérifiées après le premier match. Par conséquent, l'ordre des règles est critique. Par défaut, les règles sont classées par ordre de priorité par leur temps créé.

La règle créée précédemment est vérifiée pour une correspondance avec une priorité plus élevée. Pour réorganiser les règles, sélectionnez une règle et faites-la glisser vers une nouvelle position. Si aucune règle ne correspond, l'appareil transmet le paquet en raison **d'une clause implicite autorise Tout**.

Le système fournit trois types d'ACL :

■	**Gateway ACL** Une fois que les ACL de Passerelle sont configurées sur le contrôleur, ils peuvent être appliqués à la passerelle pour contrôler le trafic qui provient des ports LAN et transmis aux ports WAN. Vous pouvez définir le réseau, l'adresse IP, le numéro de port d'un paquet comme critères de filtrage de paquets dans la règle.
■	**Switches ACL** Une fois que les ACL de commutateur sont configurées sur le contrôleur, ils peuvent être appliqués au commutateur pour contrôler le trafic entrant et sortant via les ports de commutateur. Vous pouvez définir l'adresse Réseau, adresse IP, numéro de port et MAC d'un paquet en tant que critères de filtrage de paquets dans la règle.
■	**EAP ACL** . Une fois que les ACL de l'EAP sont configurées sur le contrôleur, ils peuvent être appliqués aux EAP pour contrôler le trafic dans les réseaux sans fil. Vous avez défini le réseau, l'adresse IP, le numéro de port et le SSID d'un paquet comme critère de paquets dans la règle

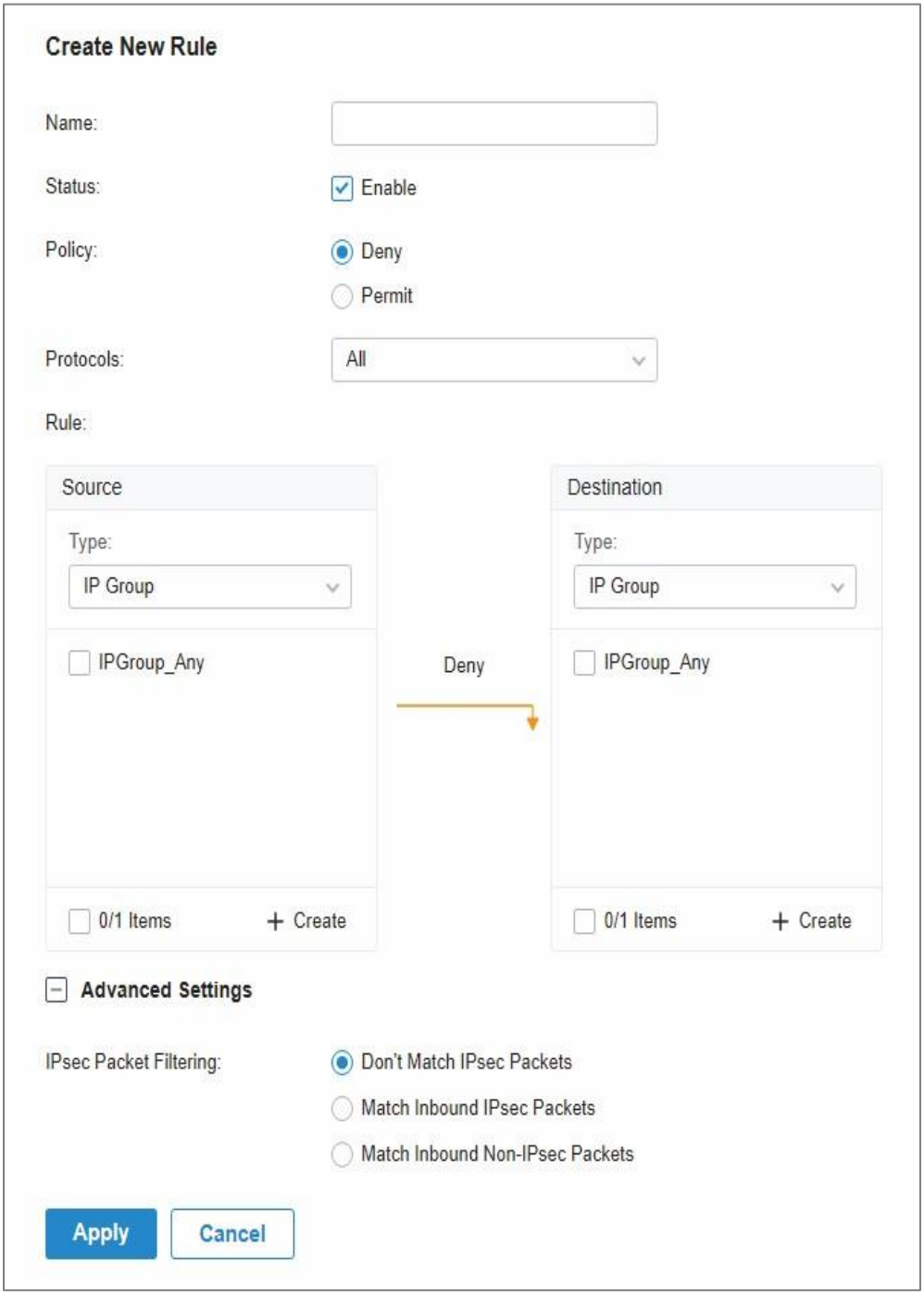
Configuration

Pour terminer la configuration ACL, procédez comme suit :

1. **)** Créez une ACL avec le type spécifié.
2. **)** Définissez les critères de filtrage des paquets de la règle, y compris les protocoles, la source et la destination, et déterminez s'il convient de transférer les paquets correspondants.

- **Configuration des ACL de la passerelle**

1 Allez dans Settings> Network>Security>ACLSous l'onglet ACL de la passerelle, cliquez sur + Create New Rule pour charger la page suivante



2. Définissez les critères de filtrage des paquets de la règle, y compris les protocoles, la source et la destination, et déterminez s'il convient de transférer les paquets correspondants. Reportez-vous au tableau suivant pour configurer les paramètres requis, puis cliquez sur Apply.

Name	Entrez un nom pour identifier l'ACL.
Status	Cliquez sur la case à cocher pour activer l'ACL.
Policy	Sélectionnez l'action à prendre lorsqu'un paquet correspond à la règle. Permit: Transférer le paquet correspondant. Deny: Jeter le paquet correspondant.
Protocols	Sélectionnez un ou plusieurs types de protocole auxquels la règle s'applique dans la liste déroulante. La valeur par défaut est Tout, indiquant que les paquets de tous les protocoles seront appariés. Lorsque vous sélectionnez l'un des TCP et UDP ou les deux, vous pouvez définir l'adresse IP et le numéro de port d'un paquet comme critères de filtrage de paquets dans la règle.

Dans la liste déroulante Source, choisissez l'une de ces options pour spécifier la source des paquets auxquels ACL s'applique :

Network	Sélectionnez le réseau que vous avez créé. Si aucun réseau n'a été créé, vous pouvez sélectionner le réseau par défaut (LAN) ou Settings > Wired Networks > LAN pour en créer un. La passerelle examinera si les paquets proviennent du réseau sélectionné.
IP Group	Sélectionnez le groupe IP que vous avez créé. Si aucun groupe IP n'a été créé, cliquez sur +Create sur cette page ou aller à Settings > Profiles > Groups pour en créer un. La passerelle examinera si l'adresse IP source du paquet se trouve dans le groupe IP.
IP-Port Group	Sélectionnez le groupe IP-Port que vous avez créé. Si aucun groupe IP-Port n'a été créé, cliquez sur +Create sur cette page ou aller à Settings > Profiles > Groups pour en créer un. La passerelle examinera si l'adresse IP source et le numéro de port du paquet se trouvent dans le groupe IP-Port.

Dans la liste déroulante Destination, choisissez l'une de ces options pour spécifier la destination des paquets auxquels l'ACL s'applique :

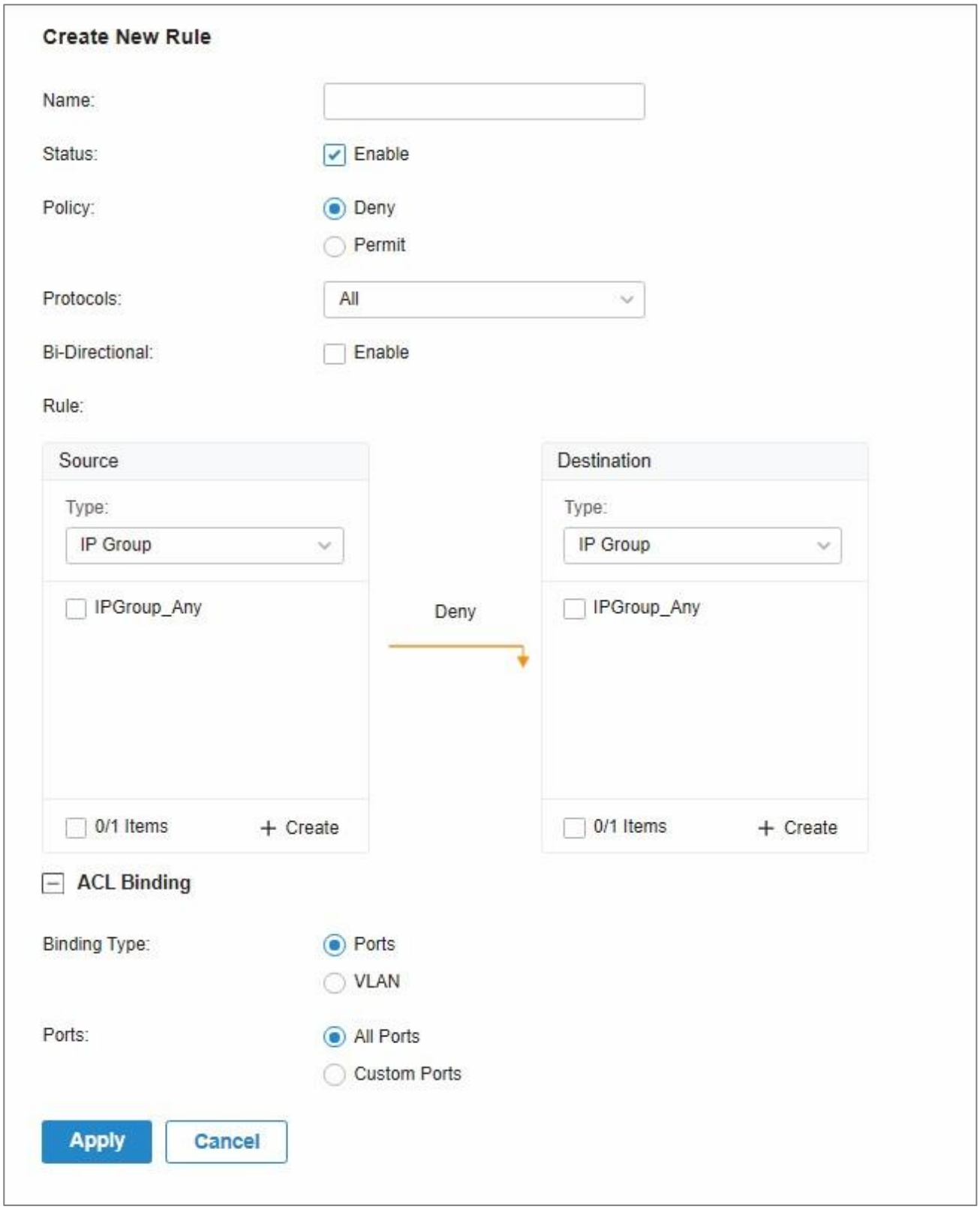
IP Group	Sélectionnez le groupe IP que vous avez créé. Si aucun groupe IP n'a été créé, cliquez sur +Create sur cette page ou aller à Settings > Profiles > Groups pour en créer un. La passerelle examinera si l'adresse IP de destination du paquet se trouve dans le groupe IP.
IP-Port Group	Sélectionnez le groupe IP-Port que vous avez créé. Si aucun groupe IP-Port n'a été créé, cliquez sur +Create sur cette page ou aller à Settings > Profiles > Groups pour en créer un. La passerelle examinera si l'adresse IP de destination et le numéro de port du paquet se trouvent dans le groupe IP-Port.

Vous pouvez déterminer si l'ACL est appliquée aux paquets chiffrés avec des protocoles IPsec dans les paramètres avancés.

IPsec packet filtering	Sélectionnez s'il faut faire correspondre les paquets IPsec. Trois options sont disponibles : Ne pas correspondre aux paquets IPsec, Match Inbound IPsec Packets, Match Inbound Non-IPsec Packets.

■ Configuration des ACL sur commutateur

1. Allez dans Settings> Network>Security>ACL. Sous l'onglet Basculer ACL, cliquez sur + Create New Rule pour charger page et les éléments suivants.



2. Paramètres requis. Définissez les critères de filtrage des paquets de la règle, y compris les protocoles, la source et la destination, et déterminez s'il convient de transférer les paquets correspondants.
Reportez-vous au tableau suivant pour configurer le :

Name	Entrez un nom pour identifier l'ACL.
Status	Cliquez sur la case à cocher pour activer l'ACL.
Policy	Sélectionnez l'action à prendre lorsqu'un paquet correspond à la règle. Permit: Transférer le paquet correspondant. Deny: Jeter le paquet correspondant.
Protocols	Sélectionnez un ou plusieurs types de protocole auxquels la règle s'applique dans la liste déroulante. La valeur par défaut est Tout, indiquant que les paquets de tous les protocoles seront appariés. Lorsque vous sélectionnez l'un des TCP et UDP ou les deux, vous pouvez définir l'adresse IP et le numéro de port d'un paquet comme critères de filtrage de paquets dans la règle.
Bi-Directional	Cliquez sur la case à cocher pour activer le commutateur pour créer une autre ACL symétrique avec le nom « xxx_reverse », où « i » est le nom de l'ACL actuel. Les deux ACL ciblent les paquets dans la direction opposée l'une de l'autre.

Dans la liste déroulante Source, choisissez l'une de ces options pour spécifier la source des paquets auxquels l'ACL s'applique :

Network	Sélectionnez le réseau que vous avez créé. Si aucun réseau n'a été créé, vous pouvez sélectionner le réseau par défaut (LAN) ou Settings > Wired Networks > LAN pour en créer un. Le commutateur examinera si les paquets proviennent du réseau sélectionné.
IP Group	Sélectionnez le groupe IP que vous avez créé. Si aucun groupe IP n'a été créé, cliquez sur +Create sur cette page ou aller à Settings > Profiles > Groups pour en créer un. Le commutateur examinera si l'adresse IP source du paquet se trouve dans le groupe IP.
IP-Port Group	Sélectionnez le groupe IP-Port que vous avez créé. Si aucun groupe IP-Port n'a été créé, cliquez sur +Create sur cette page ou aller à Settings > Profiles > Groups pour en créer un. Le commutateur examinera si l'adresse IP source et le numéro de port du paquet se trouvent dans le groupe IP-Port.
MAC Group	Sélectionnez le groupe MAC que vous avez créé. Si aucun groupe MAC n'a été créé, cliquez sur +Create sur cette page ou aller à Settings > Profiles > Groups pour en créer un. Le commutateur examinera si l'adresse MAC source du paquet se trouve dans le Groupe MAC.

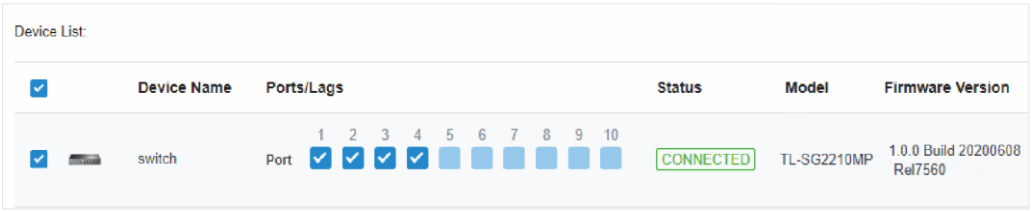
Dans la liste déroulante Destination, choisissez l'une de ces options pour spécifier la destination de l'ACL pour qu'elle s'applique :

Network	Sélectionnez le réseau que vous avez créé. Si aucun réseau n'a été créé, vous pouvez sélectionner le réseau par défaut (LAN) ou Settings > Wired Networks > LAN pour en créer un. Le commutateur examinera si les paquets sont transmis au réseau sélectionné.
IP Group	Sélectionnez le groupe IP que vous avez créé. Si aucun groupe IP n'a été créé, cliquez sur +Create sur cette page ou aller à Settings > Profiles > Groups pour en créer un. Le commutateur examinera si l'adresse IP de destination du paquet se trouve dans le groupe IP.
IP-Port Group	Sélectionnez le groupe IP-Port que vous avez créé. Si aucun groupe IP-Port n'a été créé, cliquez sur +Create sur cette page ou aller à Settings > Profiles > Groups pour en créer un. Le commutateur examinera si l'adresse IP de destination et le numéro de port du paquet se trouvent dans le groupe IP-Port.
MAC Group	Sélectionnez le groupe MAC que vous avez créé. Si aucun groupe MAC n'a été créé, cliquez sur +Create sur cette page ou aller à Settings > Profiles > Groups pour en créer un. Le commutateur examinera si l'adresse MAC de destination du paquet se trouve dans le Groupe MAC.

1. Lier le commutateur ACL à un port de commutateur ou à un VLAN, puis cliquez sur Bind. Notez qu'un commutateur ACL prend effet seulement après qu'il est lié à un port ou VLAN.

Binding Type Spécifiez si vous devez lier l'ACL aux ports ou à un VLAN.

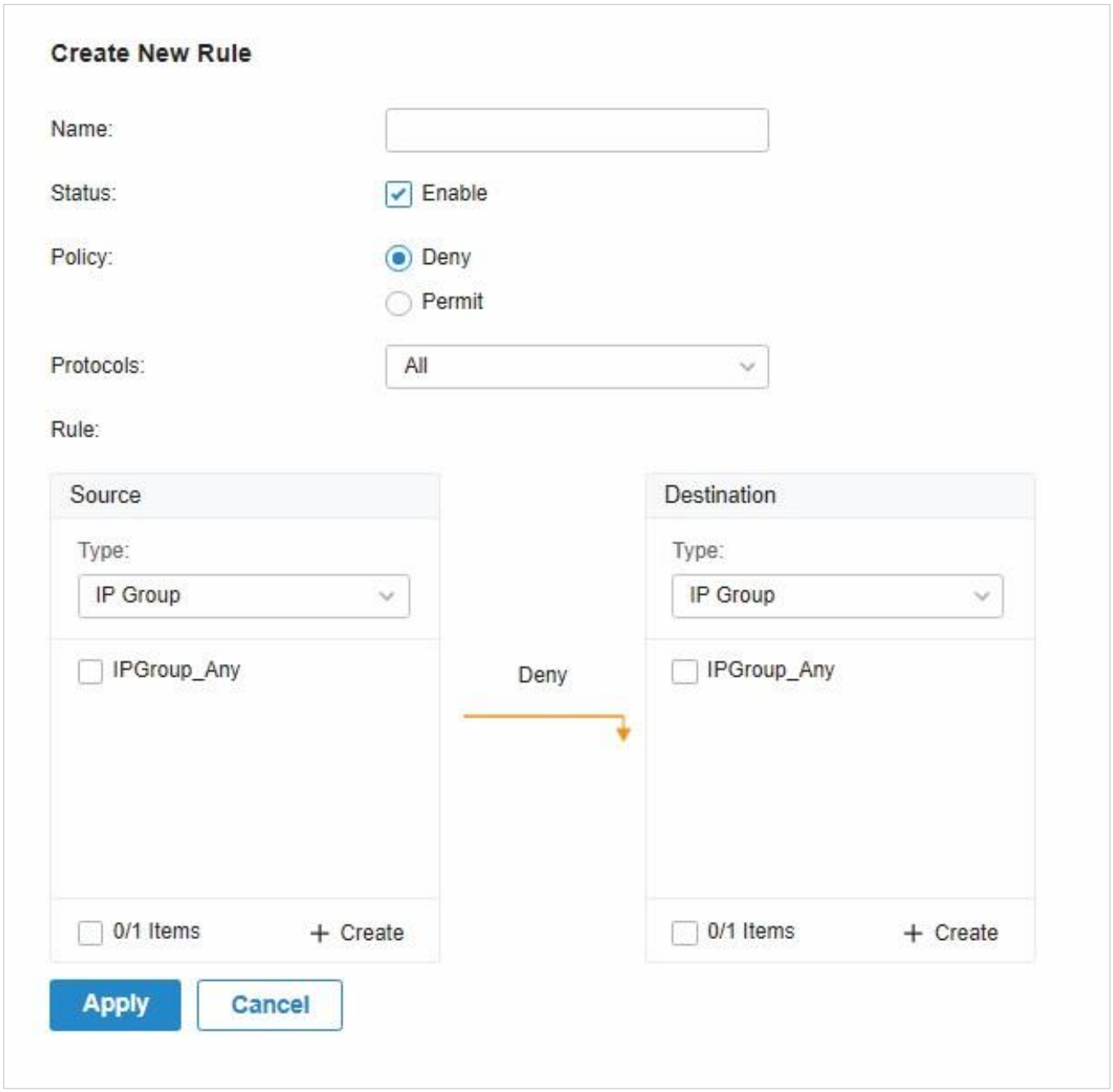
Ports: Sélectionnez Tous les ports ou ports personnalisés comme interfaces à lier à l'ACL. Avec tous les ports sélectionnés, la règle est appliquée à tous les ports du commutateur. Avec les ports personnalisés sélectionnés, la règle est appliquée aux ports sélectionnés du commutateur. Cliquez sur les ports de la liste des périphériques pour sélectionner les ports de liaison.



VLAN: Sélectionnez un VLAN dans la liste déroulante comme interface à lier à l'ACL. Si aucun VLAN n'a été créé, vous pouvez sélectionner le VLAN 1 (LAN) par défaut ou Settings > Wired Networks > LAN pour en créer un.

■ Configuration de l’ACL sur un EAP

1. Allez dans Settings> Network>Security>ACL Sous l’onglet ACL du EAP, cliquez sur + Create New Rule pour charger la page suivante.



2. Définissez les critères de filtrage des paquets de la règle, y compris les protocoles, la source et la destination, et déterminez s’il convient de transférer les paquets correspondants. Reportez-vous au tableau suivant pour configurer les paramètres requis, puis cliquez sur Apply.

Name	Entrez un nom pour identifier l’ACL.
Status	Cliquez sur la case à cocher pour activer l’ACL.

Policy	Sélectionnez l'action à prendre lorsqu'un paquet correspond à la règle. Permit: Transférer le paquet correspondant. Deny: Jeter le paquet correspondant.
Protocols	Sélectionnez un ou plusieurs types de protocole auxquels la règle s'applique dans la liste déroulante. La valeur par défaut est Tout, indiquant que les paquets de tous les protocoles seront appariés. Lorsque vous sélectionnez l'un des critères de filtrage de TCP et d'UDP ou les deux, vous pouvez définir l'adresse IP et le numéro de port d'un paquet comme critères de filtrage de paquets dans la règle.

Dans la liste déroulante Source, choisissez l'une de ces options pour spécifier la source des paquets auxquels l' ACL s'applique:

Network	Sélectionnez le réseau que vous avez créé. Si aucun réseau n'a été créé, vous pouvez sélectionner le réseau par défaut (LAN) ou Settings > Wired Networks > LAN pour en créer un. L'EAP examinera si les paquets proviennent du réseau sélectionné.
IP Group	Sélectionnez le groupe IP que vous avez créé. Si aucun groupe IP n'a été créé, cliquez sur +Create sur cette page ou aller à Settings > Profiles > Groups pour en créer un. L'EAP examinera si l'adresse IP source du paquet se trouve dans le groupe IP.
IP-Port Group	Sélectionnez le groupe IP-Port que vous avez créé. Si aucun groupe IP-Port n'a été créé, cliquez sur +Create sur cette page ou aller à Settings > Profiles > Groups pour en créer un. Le PAE examinera si l'adresse IP source et le numéro de port du paquet se trouvent dans le groupe IP-Port.
SSID	Sélectionnez le SSID que vous avez créé. Si aucun SSID n'a été créé, Settings > Wireless Networks pour en créer un. Le EAP examinera si le SSID du paquet est le SSID sélectionné ici.

Dans la liste déroulante Destination, choisissez l'une de ces options pour spécifier la destination des paquets auxquels l'ACL s'applique :

Network	Sélectionnez le réseau que vous avez créé. Si aucun réseau n'a été créé, vous pouvez sélectionner le réseau par défaut (LAN) ou Settings > Wired Networks > LAN pour en créer un. L'EAP examinera si les paquets sont transmis au réseau sélectionné.
IP Group	Sélectionnez le groupe IP que vous avez créé. Si aucun groupe IP n'a été créé, cliquez sur +Create sur cette page ou aller à Settings > Profiles > Groups pour en créer un. L'EAP examinera si l'adresse IP de destination du paquet se trouve dans le groupe IP.
IP-Port Group	Sélectionnez le groupe IP-Port que vous avez créé. Si aucun groupe IP-Port n'a été créé, cliquez sur +Create sur cette page ou aller à Settings > Profiles > Groups pour en créer un. L'EAP examinera si l'adresse IP de destination et le numéro de port du paquet se trouvent dans le groupe IP-Port.

4. 5. 2 Filtrage d’URL

Aperçu

Le filtrage d’URL permet à un administrateur réseau de créer des règles pour bloquer ou autoriser certains sites Web, ce qui le protège contre les menaces basées sur le Web, et refuser l’accès à des sites Web malveillants.

Dans le filtrage d’URL, le système compare les URL dans les demandes HTTP, HTTPS et DNS aux listes d’URL définies dans les règles de filtrage d’URL et intercepte les demandes dirigées vers une URL bloquée. Ces règles peuvent être appliquées à des clients ou des groupes spécifiques dont le trafic passe par la passerelle et les PAE.

Le système filtre le trafic par rapport aux règles de la liste séquentiellement. La première correspondance détermine si le paquet est accepté ou abandonné, et d’autres règles ne sont pas vérifiées après le premier match. Par conséquent, l’ordre des règles est critique. Par défaut, les règles sont classées par ordre de priorité en fonction de la séquence qu’elles sont créées. La règle créée précédemment est vérifiée pour une correspondance avec une priorité supérieure. Pour réorganiser les règles, sélectionnez une règle et faites-la glisser vers une nouvelle position. Si aucune règle ne correspond, l’appareil transmet le paquet en raison d’une clause implicite De permis Tous.

Notez que les règles de filtrage d’URL prennent des effets avec une priorité plus élevée sur les règles ACL. Autrement dit, le système traitera d’abord la règle de filtrage d’URL lorsque la règle de filtrage d’URL et les règles ACL sont configurées en même temps.

Configuration

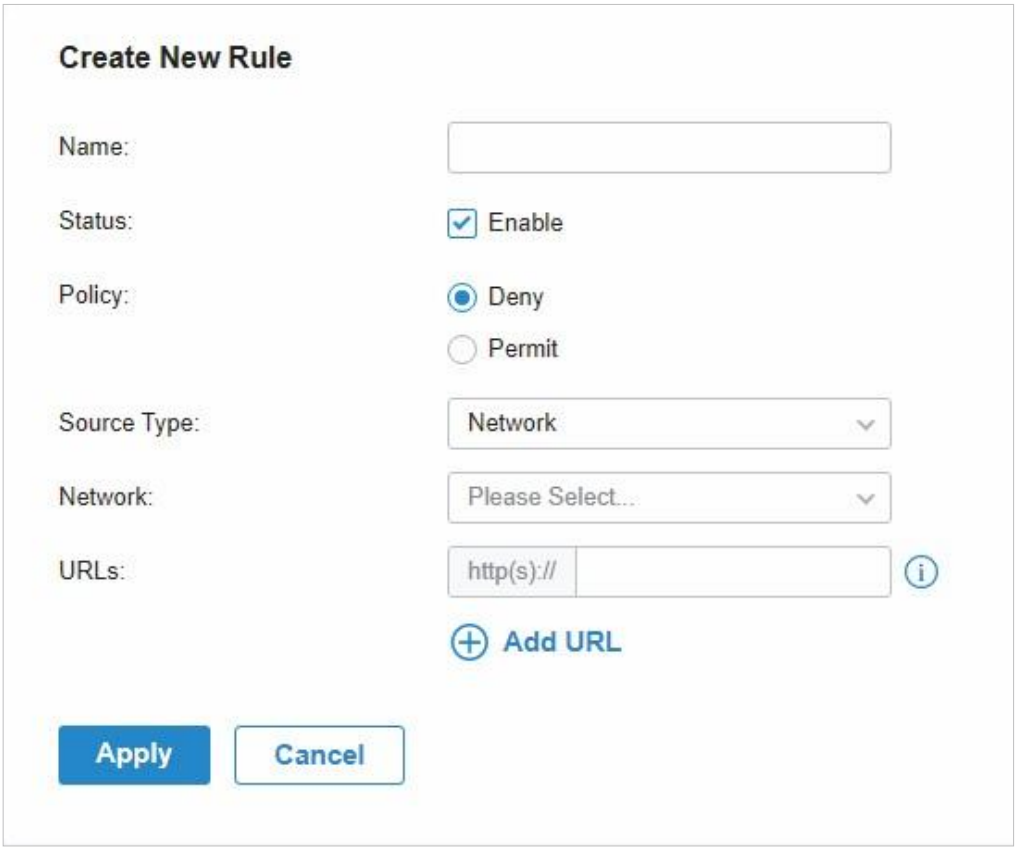
Pour terminer la configuration de filtrage d’URL, procédez comme suit :

1.) Créez une nouvelle règle de filtrage d’URL avec le type spécifié.

2.) Définissez les critères de filtrage de la règle, y compris la source, et les URL, et déterminez s’il convient de transférer les paquets correspondants.

■ Configuring Gateway Rules

1. Atteindre Settings > Network Security > URL Filtering. Sous l'onglet Règles de passerelle, cliquez + Create New Rule pour charger la page suivante.



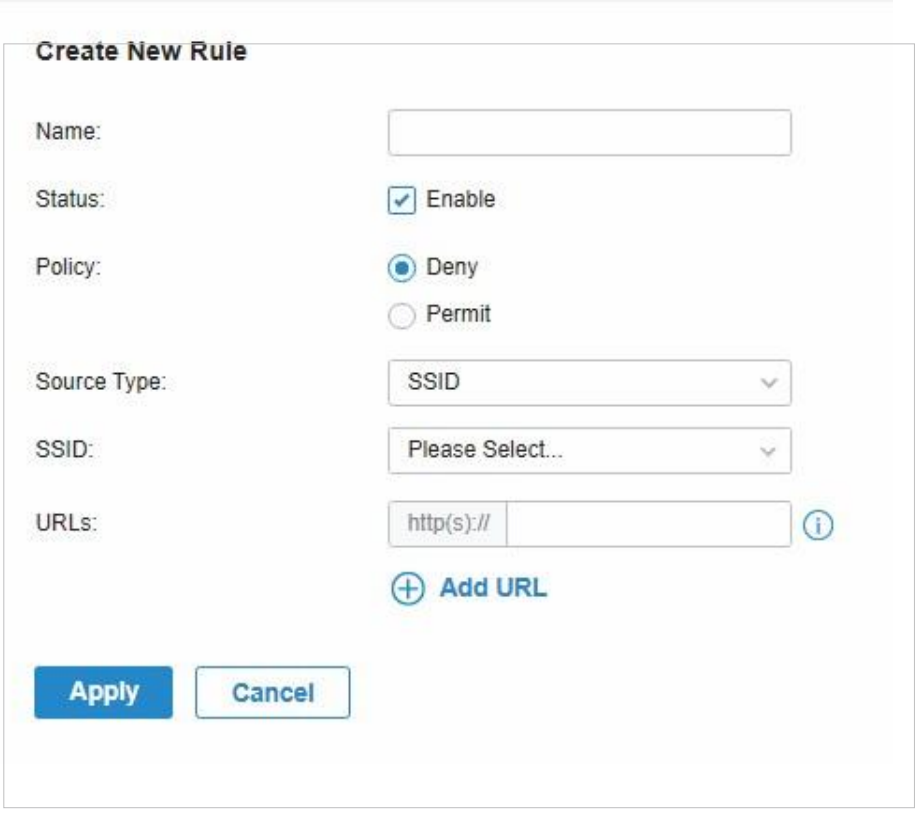
1. Définissez les critères de filtrage de la règle, y compris les URL source et les URL, et déterminez s'il convient de transférer les paquets correspondants. Reportez-vous au tableau suivant pour configurer les paramètres requis, puis cliquez sur Apply.

Name	Entrez un nom pour identifier la règle de filtrage d'URL.
Status	Cliquez sur la case à cocher pour activer la règle de filtrage d'URL.
Policy	Sélectionnez l'action à prendre lorsqu'un paquet correspond à la règle. Deny: Supprimer le paquet correspondant et les clients ne peuvent pas accéder aux URL. Permit: Transférer le paquet correspondant et les clients peuvent accéder aux URL.

Source Type	Sélectionnez la source des paquets auxquels cette règle s'applique. Network: Avec Réseau sélectionné, sélectionnez le réseau que vous avez créé à partir de la liste déroulante Réseau. Si aucun réseau n'a été créé, vous pouvez sélectionner le réseau par défaut (LAN) ou Settings > Wired Networks > LAN pour en créer un. La passerelle filtrera les paquets provenant du réseau sélectionné. IP Group: Avec la sélection du groupe IP, sélectionnez le groupe IP que vous avez créé dans la liste déroulante Groupe IP. Si aucun groupe IP n'a été créé, cliquez sur +Create Nouveau groupe IP sur cette page ou accédez à Settings > Profiles > Groups pour en créer un. La passerelle examinera si l'adresse IP source du paquet se trouve dans le groupe IP.
URLs	Entrez l'adresse URL à l'aide de 128 caractères. L'adresse URL doit être donnée dans un format valide. L'URL qui contient un caractère générique (*) est prise en charge. Une URL avec une wildcard(*) peut correspondre aux sous-domaines multiple. Par exemple, avec *.tp-link.com spécifié, community.tp-link.com seront appariés.

■ Configuration des règles aux EAP's

1. Atteindre Settings > Network Security > URL Filtering. Sous l'onglet Règles de passerelle, cliquez + Create New Rule pour charger la page suivante



2. Définissez les critères de filtrage de la règle, y compris les URL source et les URL, et déterminez s'il convient de transférer les paquets correspondants. Reportez-vous au tableau suivant pour configurer les paramètres requis, puis cliquez sur Apply.

Name	Entrez un nom pour identifier la règle de filtrage d'URL.
Status	Cliquez sur la case à cocher pour activer la règle de filtrage d'URL.
Policy	Sélectionnez l'action à prendre lorsqu'un paquet correspond à la règle. Deny: Supprimer le paquet correspondant et les clients ne peuvent pas accéder aux URL. Permit: Transférer le paquet correspondant et les clients peuvent accéder aux URL.
Source Type	Sélectionnez le SSID des paquets auxquels cette règle s'applique.
URLs	Entrez l'adresse URL à l'aide de 128 caractères. L'adresse URL doit être donnée dans un format valide. L'URL qui contient un caractère générique (*) est prise en charge. Une URL avec une wildcard (*) peut correspondre aux sous-domaines multiples. Par exemple, avec *.tp-link.com spécifié, community.tp-link.com seront appariés

4. 5. 3 Attack Defense

Aperçu

Les attaques lancées par l'utilisation de bogues inhérents aux protocoles de communication ou le déploiement inapproprié du réseau ont des impacts négatifs sur les réseaux. En particulier, les attaques sur un périphérique réseau peuvent provoquer la paralysie de l'appareil ou du réseau.

Avec la fonctionnalité Défense d'attaque, la passerelle peut identifier et jeter divers paquets d'attaque dans le réseau, et limiter le taux de réception des paquets. De cette façon, la passerelle peut se protéger elle-même et le réseau connecté contre les attaques malveillantes.

The gateway provides two types of Attack Defense:

- **Flood Defense**

Si un attaquant envoie un grand nombre de faux paquets à un appareil cible, le périphérique cible est occupé avec ces faux paquets et ne peut pas traiter les services normaux. Flood Defense détecte les paquets d'inondation en temps réel et limite le taux de réception des paquets pour protéger l'appareil.

Les attaques d'inondation incluent les attaques d'inondation syn TCP, les attaques d'inondation udp et les attaques d'inondation icmp.

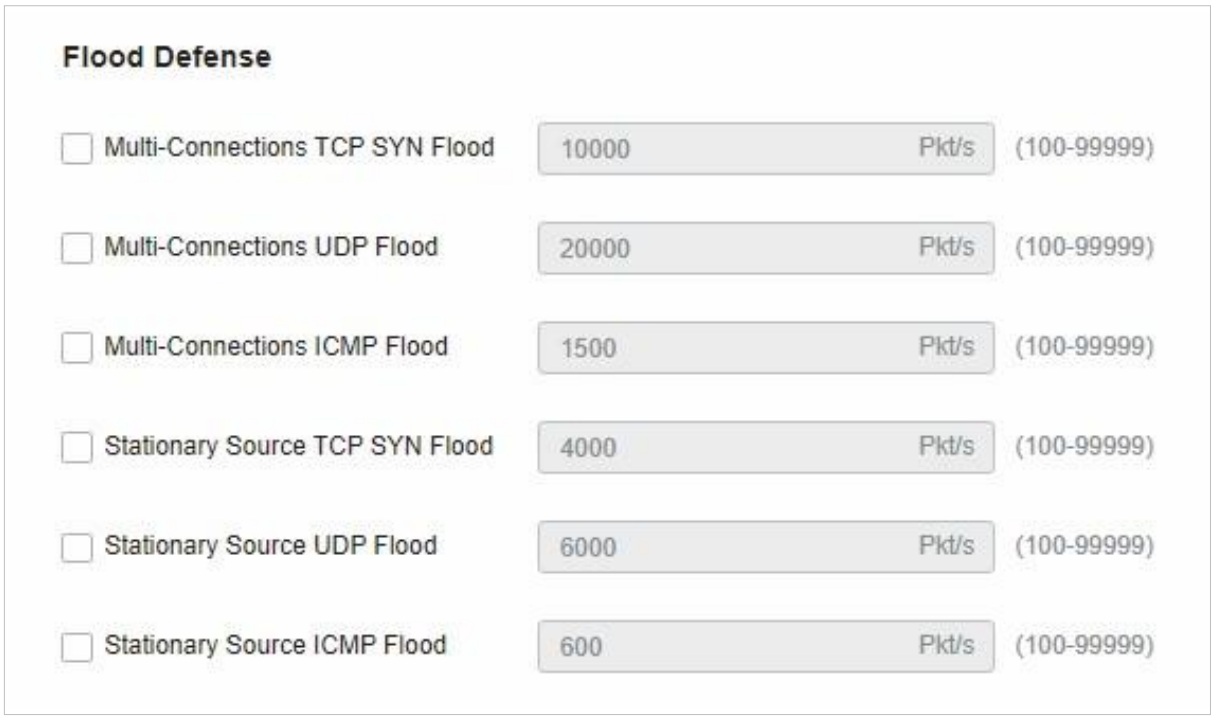
- **Packet Anomaly Defense**

Les paquets anormaux sont des paquets qui ne sont pas conformes aux normes ou contiennent des erreurs qui les rendent impropres au traitement. Packet Anomaly Defense rejette directement les paquets illégaux.

Configuration

■ Configuration Flood Defense

Allez sur Settings > Network Security > Attack Defense. Dans la défense contre les inondations, cliquez sur la case à cocher et définissez la limite correspondante de la vitesse à laquelle des paquets spécifiques sont reçus.

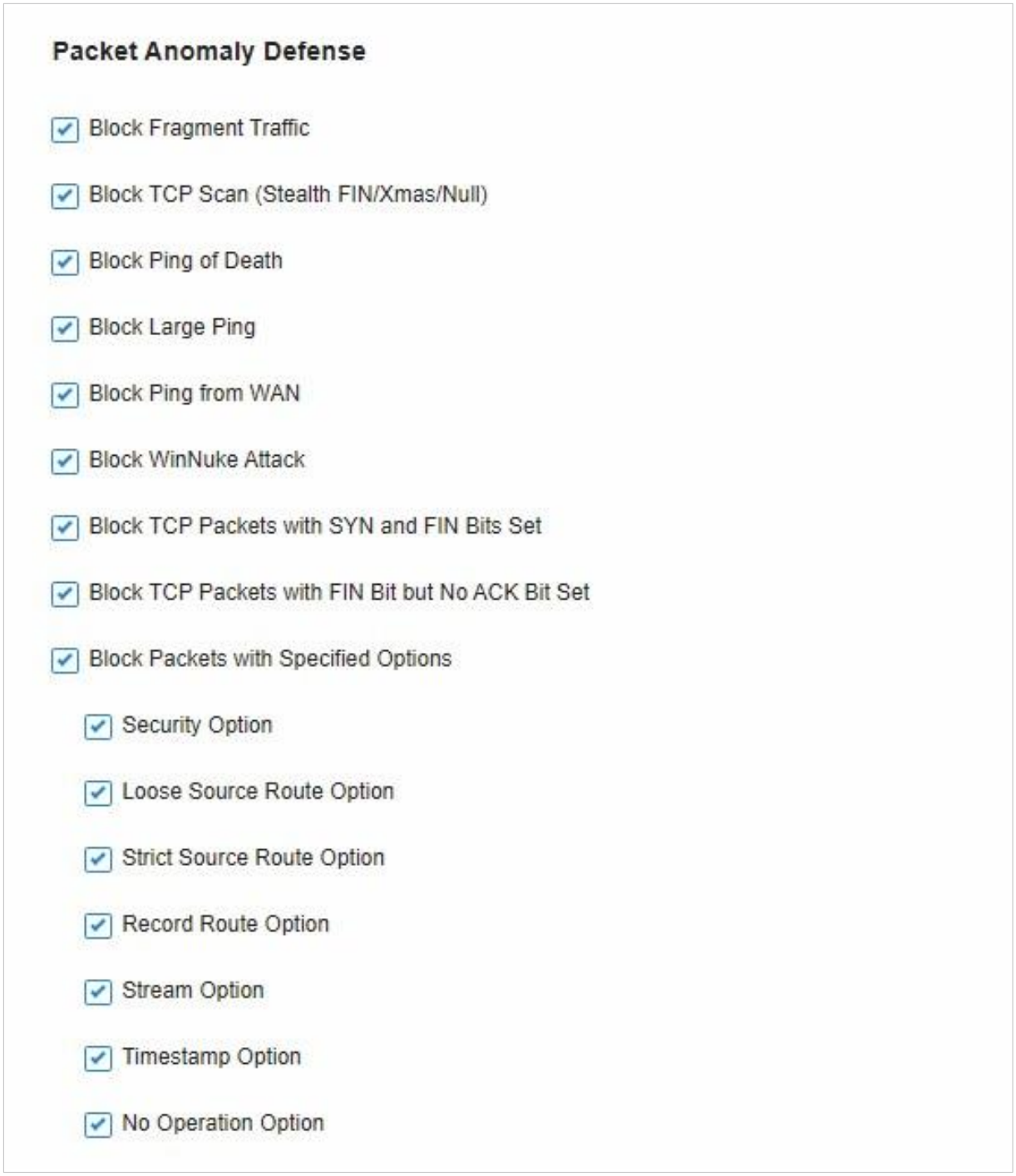


Multi-Connections TCP SYN Flood	Une attaque d'inondation SYN TCP se produit lorsque l'attaquant envoie le système cible avec une succession de demandes SYN (synchroniser). Lorsque le système répond, l'attaquant ne complète pas les connexions, laissant ainsi la connexion à moitié ouverte et inondant le système de messages SYN. Aucune connexion légitime ne peut alors être faite. Avec cette fonctionnalité activée, la passerelle limite le taux de réception des paquets TCP SYN de tous les clients au taux spécifié.
Multi-Connections UDP Flood	Une attaque d'inondation UDP se produit lorsque l'attaquant envoie un grand nombre de paquets UDP à un hôte cible dans un court laps de temps, l'hôte cible est occupé avec ces paquets UDP et ne peut pas traiter les services normaux. Avec cette fonctionnalité activée, la passerelle limite le taux de réception des paquets UDP de tous les clients au taux spécifié.
Multi-Connections ICMP Flood	Si un attaquant envoie de nombreux messages ICMP Echo au périphérique cible, le périphérique cible est occupé avec ces messages Echo et ne peut pas traiter d'autres paquets de données. Par conséquent, les services normaux sont affectés. Avec cette fonctionnalité activée, le système limite le taux de réception des paquets ICMP de tous les clients au taux spécifié.

Stationary Source TCP SYN Flood	Une attaque d'inondation SYN TCP se produit lorsque l'attaquant envoie le système cible avec une succession de demandes SYN (synchroniser). Lorsque le système répond, l'attaquant ne complète pas les connexions, laissant ainsi la connexion à moitié ouverte et inondant le système de messages SYN. Aucune connexion légitime ne peut alors être faite. Avec cette fonctionnalité activée, la passerelle limite le taux de réception des paquets SYN TCP d'un seul client au taux spécifié.
Stationary Source UDP Flood	Une attaque d'inondation UDP se produit lorsque l'attaquant envoie un grand nombre de paquets UDP à un hôte cible dans un court laps de temps, l'hôte cible est occupé avec ces paquets UDP et ne peut pas traiter les services normaux. Avec cette fonctionnalité activée, la passerelle limite le taux de réception des paquets UDP d'un seul client au taux spécifié.
Stationary Source ICMP Flood	Si un attaquant envoie de nombreux messages ICMP Echo au périphérique cible, le périphérique cible est occupé avec ces messages Echo et ne peut pas traiter d'autres paquets de données. Par conséquent, les services normaux sont affectés. Avec cette fonctionnalité activée, le système limite le taux de réception des paquets ICMP d'un seul client au taux spécifié.

■ **Configuration Packet Anomaly Defense**

Allez dans Settings > Network Security > Attack Defense. Dans la défense anomalie du paquet, cliquez sur la case à cocher et définissez la limite correspondante de la vitesse à laquelle des paquets spécifiques sont reçus.



Block Fragment Traffic	Avec cette option activée, les paquets fragmentés sans la première partie du paquet seront jetés.

Block TCP Scan (Stealth FIN/Xmas/Null)	Avec cette option activée, la passerelle bloquera les paquets anormaux dans les scénarios d'attaque suivants : Stealth FIN Scan : l'attaquant envoie le paquet avec son champ SYN et le champ FIN défini sur 1. Le champ SYN est utilisé pour demander la connexion initiale tandis que le champ FIN est utilisé pour demander la déconnexion. Par conséquent, le paquet de ce type est illégal. Analyse de Noël : l'attaquant envoie le paquet illégal avec son index TCP, fin, urg et champ PSH défini sur 1. Null Scan : l'attaquant envoie le paquet illégal avec son index TCP et tous les champs de contrôle réglés sur 0. Au cours de la connexion TCP et de la transmission de données, les paquets avec tous les champs de contrôle réglés sur 0 sont considérés comme illégaux.
Block Ping of Death	Avec cette option activée, la passerelle bloquera l'attaque ping de la mort. Ping of Death attack signifie que l'attaquant envoie des paquets ping anormaux qui sont inférieurs à 64 octets ou plus de 65535 octets pour provoquer un crash du système sur l'ordinateur cible.
Block Large Ping	Avec cette option activée, le routeur bloquera les paquets ping qui sont plus grands que 1024 paquets pour protéger le système contre l'attaque de Gros Ping.
Block Ping from WAN	Avec cette option activée, le routeur bloquera la demande ICMP de WAN.
Block WinNuke Attack	Avec cette option activée, le routeur bloquera les attaques WinNuke. L'attaque WinNuke fait référence à une attaque DoS (déni de service) distante qui affecte certains systèmes d'exploitation Windows, tels que Windows 95. L'attaquant envoie une chaîne de données OOB (Out of Band) à l'ordinateur cible sur le port TCP 137, 138 ou 139, causant un crash du système ou un écran bleu de la mort.
Block TCP Packets with SYN and FIN Bits Set	Avec cette option activée, le routeur filtrera les paquets TCP avec le jeu de bits SYN et FIN.
Block TCP Packets with FIN Bit but No ACK Bit Set	Avec cette option activée, le routeur filtrera les paquets TCP avec l'ensemble FIN Bit mais sans jeu de bits ACK.
Block Packets with Specified Options	Avec cette option activée, le routeur filtrera les paquets avec des options IP spécifiées, y compris l'option de sécurité, l'option d'itinéraire source lâche, l'option d'itinéraire de source stricte, l'option d'itinéraire d'enregistrement, l'option de flux, l'option d'horodatage et aucune option d'opération. Vous pouvez choisir les options en fonction de vos besoins.

4. 6 Transmission

La transmission vous aide à contrôler le trafic réseau de plusieurs façons. Vous pouvez ajouter des stratégies et des règles pour contrôler les itinéraires de transmission et limiter la session et la bande passante.

4. 6. 1 Routing

Aperçu

- **Static Route**

  Le trafic réseau est orienté vers une destination spécifique, et Static Route désigne le saut ou l'interface suivant où transférer le trafic.

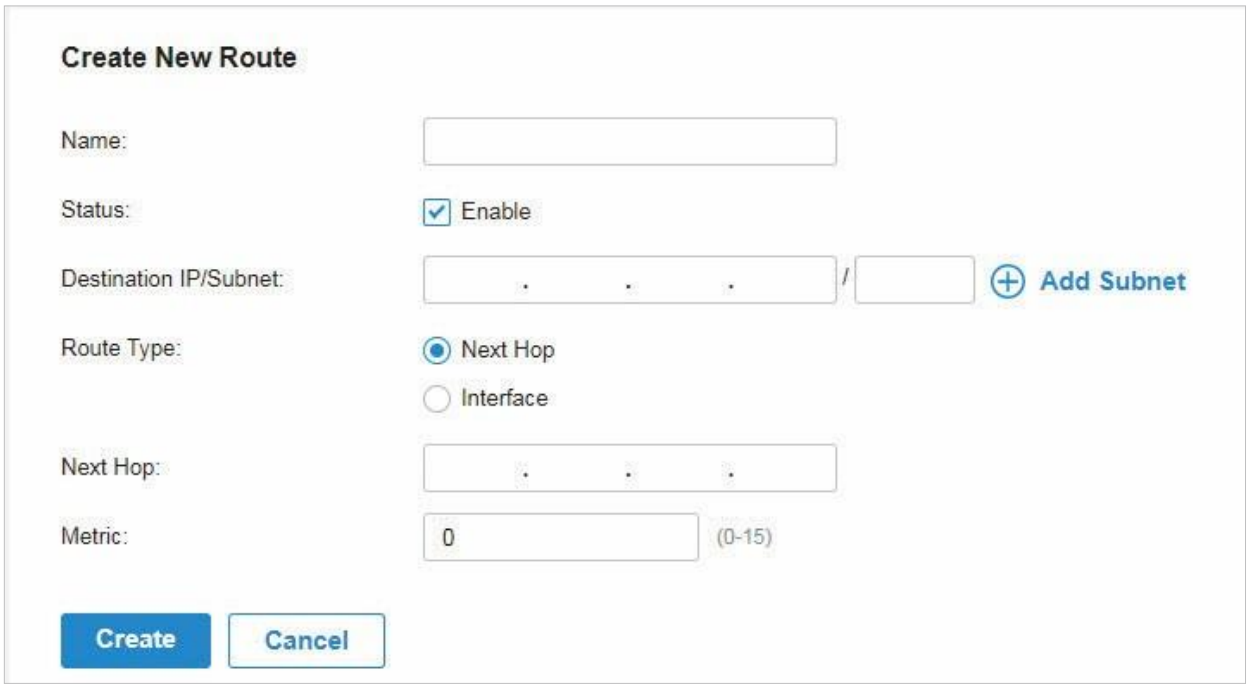
- **Policy Routing**

  Routage de stratégie désigne le port WAN utilisé par le routeur pour transférer le trafic en fonction de la source, de la destination et du protocole du trafic.

Configuration

- **Static Route**

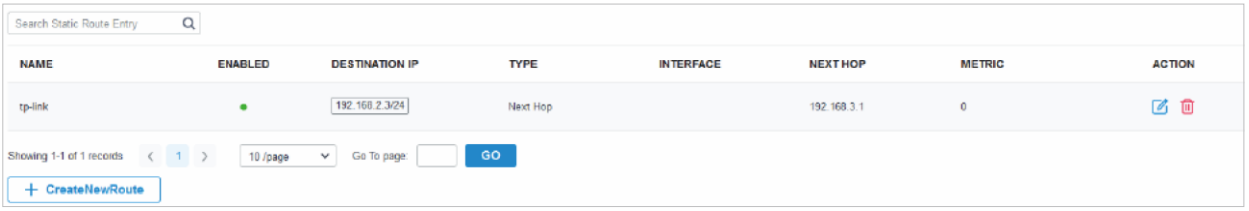
1. Allez dans Setting > Transmission > Routing > Static Route. Cliquez sur + Create New Route pour charger la page suivante et configurer les paramètres.



Name	Entrez le nom pour identifier l'entrée Itinéraire statique.
Status	Activer ou désactiver l'entrée Itinéraire statique.

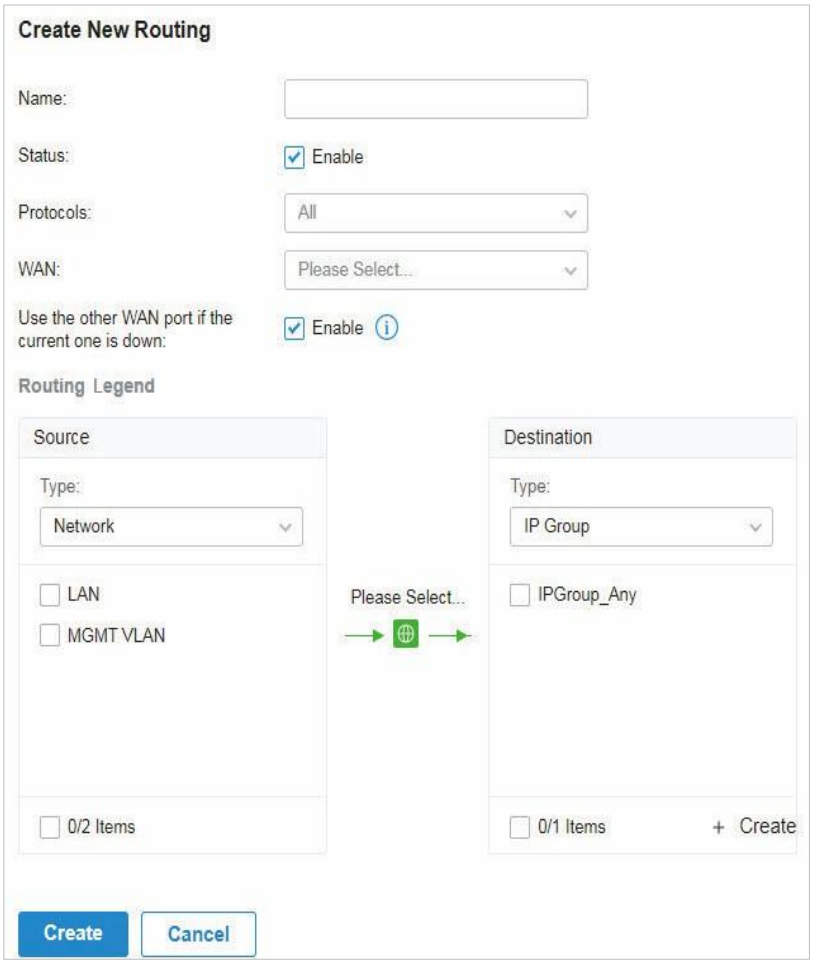
Destination IP/Subnet	Destination IP/Subnet identifier le trafic réseau que l'entrée de l'itinéraire statique contrôle. Spécialiste de la destination du trafic réseau au format de 192.168.0.1/24. Vous avez besoin de savoir + Ajouter un sous-réseau pour spécifier plusieurs sous-réseaux IP/Subnets de destination et cliquez pour les supprimer.
Route Type	Next Hop: Avec Next Hop sélectionné, vos appareils reportent le trafic réseau correspondant vers une adresse IP spécifique. Vous devez spécifier l'adresse IP en tant que prochain saut. Interface: Avec interface sélectionnée, vos appareils avancent le trafic réseau correspondant via une interface spécifique. Vous devez spécifier l'interface en fonction de vos besoins.
Metric	Définissez la priorité de l'entrée Itinéraire statique. Une valeur plus petite signifie une priorité plus élevée. Si plusieurs entrées correspondent au sous-réseau IP/Subnet de destination du trafic, l'entrée d'une priorité supérieure a préséance. En général, vous pouvez simplement conserver la valeur par défaut.

2.Cliquez sur Create .pour charger la page suivante et configurer les paramètres. pour modifier ou pour supprimer l'entrée Vous pouvez cliquer sur



■ **Policy Routing**

1. Allez dans Setting > Transmission > Routing > Policy Routing. Cliquez sur + Create New Routing pour charger la page suivante et configurer les paramètres.



Name	Entrez le nom pour identifier l'entrée Routage de stratégie.
Status	Activer ou désactiver l'entrée Routage de stratégie.
Protocols	Sélectionnez les protocoles du trafic que contrôle l'entrée de routage de stratégie. L'entrée Routage de stratégie prend effet uniquement lorsque le trafic correspond aux critères de l'entrée, y compris les protocoles.
WAN	Sélectionnez le port WAN pour transférer le trafic. Si vous souhaitez transférer le trafic à travers l'autre port WAN lorsque le WAN actuel est en panne, Use the other WAN port if the current WAN is down.
Routing Legend	L'entrée Routage de stratégie prend effet uniquement lorsque le trafic à l'aide de protocoles spécifiés correspond à la source et à la destination spécifiés dans la légende du routage.Sélectionnez le type de source de trafic et de destination. Network: Sélectionnez les interfaces LAN pour la source de trafic ou la destination IP Group: Sélectionnez le groupe IP pour la source de trafic ou la destination. Vous pouvez cliquer sur + Créer pour créer un nouveau groupe IP.

4. 6. 2 NAT

Aperçu

- **Port Forwarding**

  Vous pouvez configurer le transport de ports pour permettre aux internautes d'accéder aux hôtes locaux ou d'utiliser les services réseau qui sont déployés dans le réseau local.

  Port Forwarding permet d'établir des connexions réseau entre un hôte sur Internet et l'autre dans le réseau local en laissant le trafic passer par le port spécifique de la passerelle. Sans port forwarding, les hôtes dans le LAN sont généralement inaccessibles à partir d'Internet pour des raisons de sécurité.

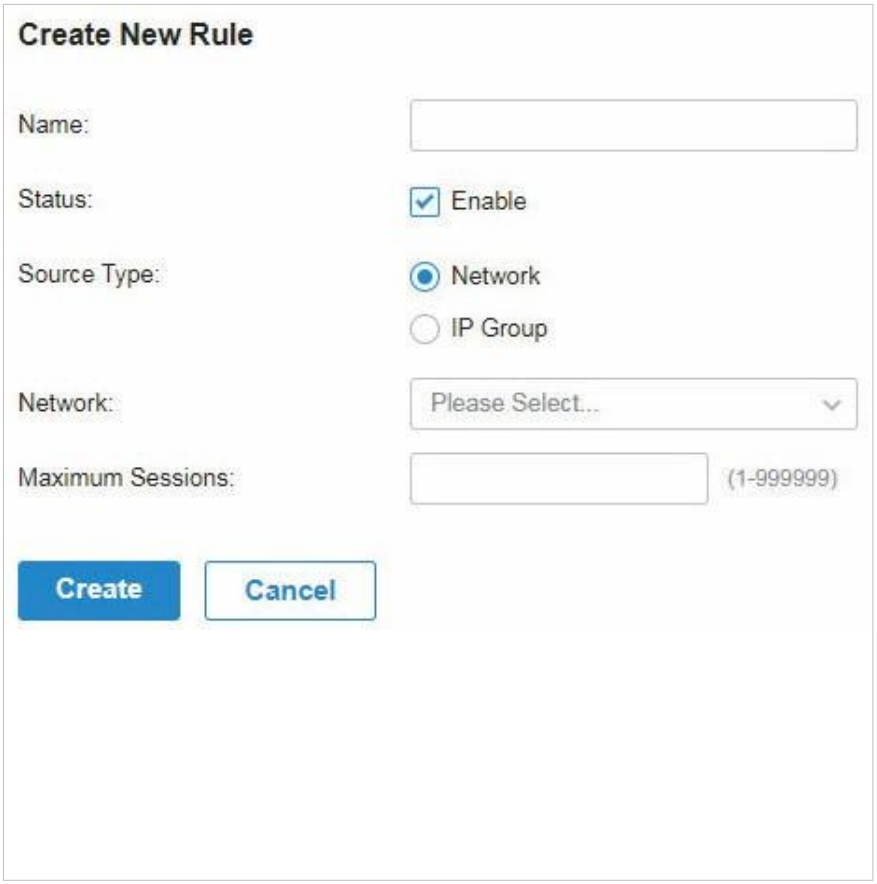
- **ALG**

  ALG veille à ce que certains protocoles au niveau de l'application fonctionnent de manière appropriée à travers votre passerelle.

Configuration

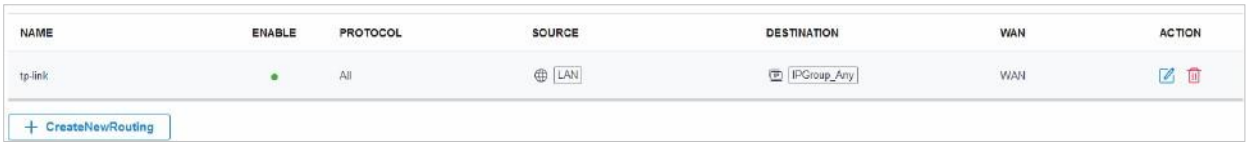
- **Port Forwarding**

1. Dans Setting > Transmission > NAT > Port Forwarding. Cliquez sur + Create New Rule pour charger la page suivante et configurer les paramètres.



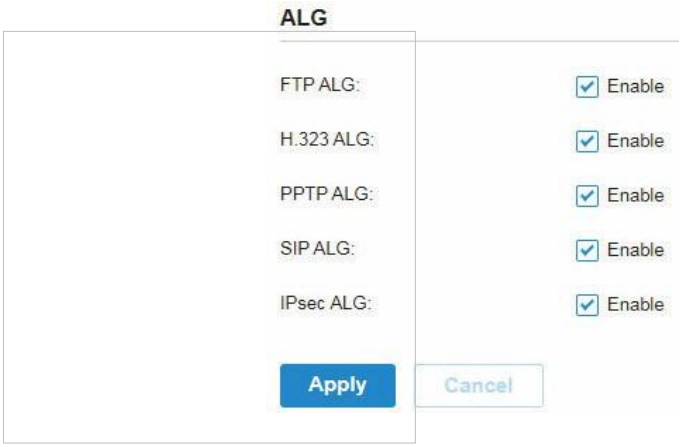
Name	Entrez le nom pour identifier la règle de mise en avant du port.
Status	Activer ou désactiver la règle de mise en avant du port.
Source IP	Any: La règle s'applique au trafic à partir de n'importe quelle adresse IP source. Limited IP Address: La règle ne s'applique qu'au trafic à partir d'adresses IP spécifiques. Avec cette option sélectionnée, spécifiez les adresses IP et les sous-réseaux en fonction de vos besoins.
Interface	Sélectionnez l'interface à laquelle la règle s'applique. Le trafic reçu par l'interface est transmis conformément à la règle.
DMZ	Avec DMZ activé, tout le trafic est transmis à la Destination IP dans le LAN, du port au port. Vous avez spécifique la Destination IP. Avec DMZ, seul le trafic qui correspond à la Source Port et le Protocole est transmis. Le trafic est transmis au Port de destination de la Destination IP dans la LAN. Vous devez spécifique le Port Source, Destination IP, Port de destination, et Protocole.
Source Port	La passerelle utilise la Source Port pour recevoir le trafic de l'Internet. Seul le trafic qui correspond au port Source et le Protocole est transmis.
Destination IP	Le trafic est transmis à l'hôte de la destination IP dans le LAN.
Destination Port	Le trafic est transmis au port de destination de l'hôte dans le réseau local.
Protocol	Le trafic réseau est transmis à l'aide du protocole TCP ou UDP. Seul le trafic correspondant au port source et au protocole est transmis. Si vous souhaitez transférer le trafic TCP et le trafic UDP, sélectionnez All.

1. Cliquez sur Create. La nouvelle entrée de mise en avant du port est ajoutée à la table. Vous pouvez cliquer sur pour modifier l'entrée



■ ALG

Dans Setting > Transmission > NAT > ALG. Activer ou désactiver certains types d'ALG en fonction de vos besoins et cliquez sur Apply.



H.323 ALG	H.323 ALG permet aux téléphones IP et aux appareils multimédias de configurer des connexions à l'aide du protocole H.323 dans l'un des scénarios suivants : • L'un des points de terminaison est dans le LAN, tandis que l'autre est sur Internet. • Les points de terminaison sont dans différents LAN.
PPTP ALG	PPTP ALG permet au serveur et au client PPTP de configurer un VPN PPTP dans l'un des scénarios suivants : • Le serveur PPTP se trouve dans le réseau local, tandis que le client PPTP se trouve sur Internet. • Le serveur PPTP se trouve sur Internet, tandis que le client PPTP se trouve dans le réseau local. • Le serveur PPTP et le client PPTP sont dans différents LAN.
SIP ALG	SIP ALG permet aux téléphones IP et aux appareils multimédias de configurer des connexions à l'aide du protocole SIP dans l'un des scénarios suivants : • L'un des points de terminaison est dans le LAN, tandis que l'autre est sur Internet. • Les points de terminaison sont dans différents LAN.
IPsec ALG	IPsec ALG permet aux points de terminaison IPsec de configurer un VPN IPsec dans l'un des scénarios suivants : • L'un des points de terminaison est dans le LAN, tandis que l'autre est sur Internet. • Les points de terminaison sont dans différents LAN.
FTP ALG	FTP ALG permet au serveur FTP et au client de transférer des données à l'aide du protocole FTP dans l'un des scénarios suivants :• Le serveur FTP se trouve dans le réseau local, tandis que le client FTP se trouve sur Internet. • Le serveur FTP est sur Internet, tandis que le client FTP se trouve dans la zone de réseau.

	• Le serveur FTP et le client FTP sont dans différents LAN.

4. 6. 3 Session Limit

Aperçu

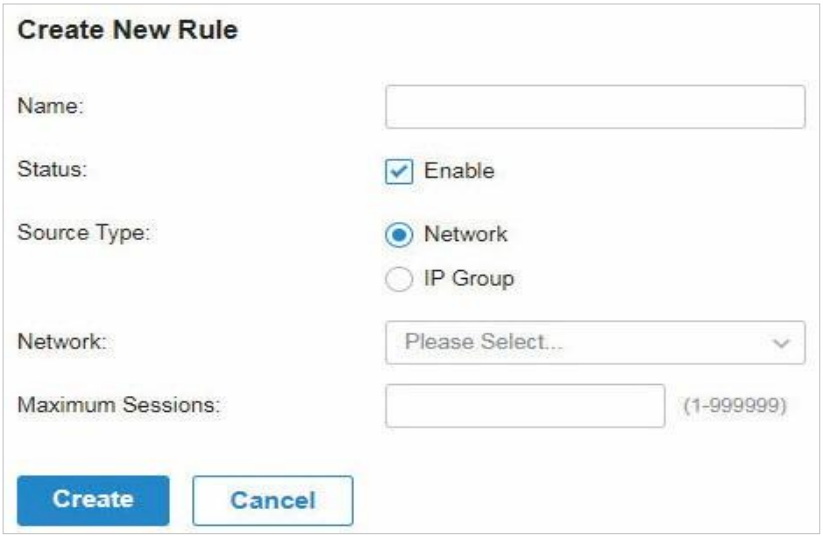
Session Limit optimise les performances du réseau en limitant le maximum de sessions de sources spécifiques.

Configuration

1. Allez dans Setting > Transmission > Session Limit. et dans Session Limit, activer la limite de session globalement et cliquer Apply.



1. Dans Session Limit Rule List, Cliquez sur + Create New Rule pour charger la page suivante et configurer les paramètres.



Name	Entrez le nom pour identifier la règle Limite de session.
Status	Activer ou désactiver la règle Limite de session.
Source Type	Network: Limitez les sessions maximales de réseaux LAN spécifiques. Avec cette option sélectionnée, sélectionnez les réseaux, que vous pouvez personnaliser dans Wired Networks >

	LAN Networks. Pour une configuration détaillée des réseaux, reportez-vous à Configure LAN Networks. IP Group: Limitez les sessions maximales de groupes IP spécifiques. Avec cette option sélectionnée, sélectionnez les groupes IP, que vous pouvez personnaliser dans Profiles > Groups. Pour la configuration détaillée des groupes IP, reportez-vous à Create Profiles.
Maximum Sessions	Entrez les sessions maximales des sources spécifiques.

3. CliqueCreate . La nouvelle règle Limite de session est ajoutée à la liste. Vous pouvez cliquer sur



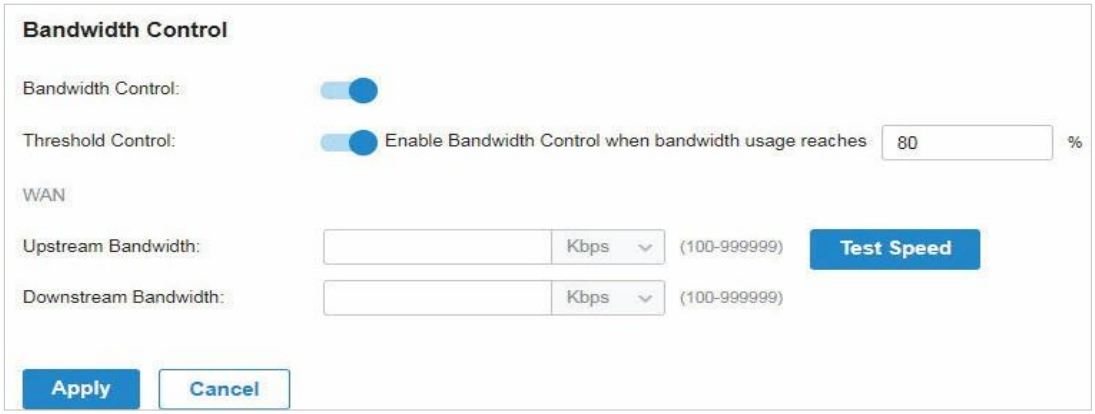
4. 6. 4 Bandwidth Control

Aperçu

Bande passante Control optimise les performances du réseau en limitant la bande passante de sources spécifiques.

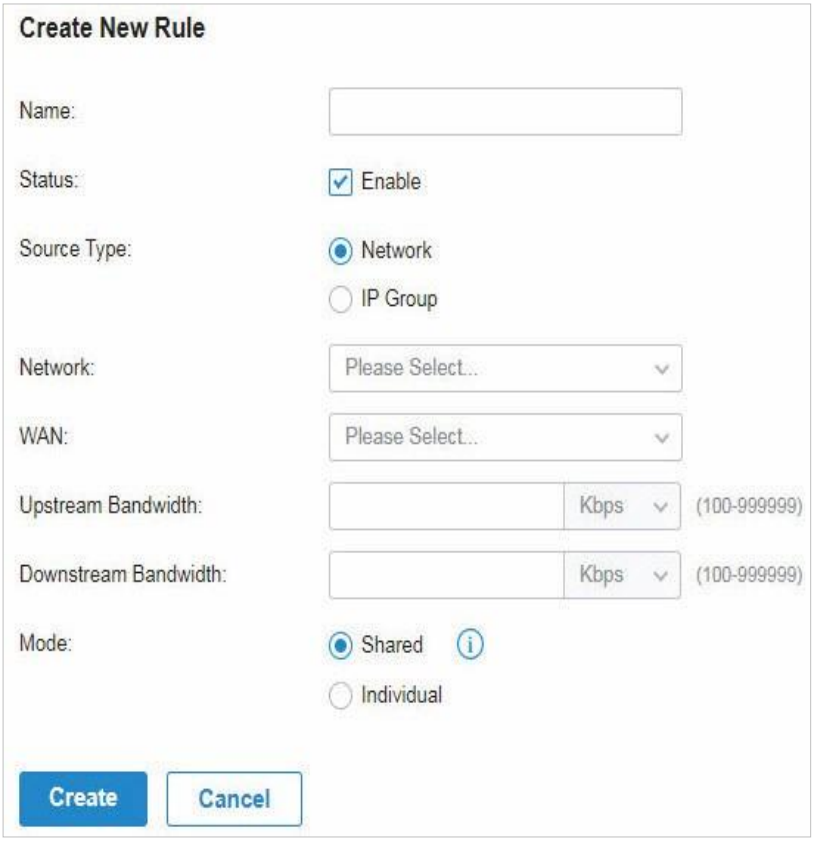
Configuration

1. Allez dans Setting > Transmission > Bandwidth Control.et dans Bandwidth Control, activer le contrôle de bande passante globalement et configurer les paramètres. Cliquez ensuite sur Apply.



Threshold Control	Avec le contrôle de seuil activé, le contrôle de bande passante prend effet uniquement lorsque l'utilisation totale de la bande passante atteint le pourcentage spécifié. Vous devez spécifier la bande passante en amont totale et la bande passante en aval des ports WAN. Il est recommandé d'utiliser l'outil Vitesse de test pour décider de la bande passante en amont réelle et de la bande passante en aval.

1. Dans Bandwidth Control Rule List, Cliquez sur + Create New Rule pour charger la page suivante et configurer les paramètres.



Name	Entrez le nom pour identifier la règle De contrôle de bande passante.
Status	Activer ou désactiver la règle De contrôle de bande passante.
Source Type Network:	Limitez la bande passante maximale des réseaux LAN spécifiques. Avec cette option sélectionnée, sélectionnez les réseaux, que vous pouvez personnaliser dans Wired Networks > LAN Networks. Pour une configuration détaillée des réseaux, reportez-vous à Configure LAN Networks.
IP Group:	Limitez la bande passante maximale de groupes IP spécifiques. Avec cette option sélectionnée, sélectionnez les groupes IP, que vous pouvez personnaliser dans Profiles > Groups. Pour la configuration détaillée des groupes IP, reportez-vous à Create Profiles.
WAN	Sélectionnez le port WAN auquel la règle s'applique.
Upstream Bandwidth	Spécifier la limite de bande passante en amont, que les hôtes locaux spécifiques utilisent pour transmettre du trafic à Internet via la passerelle.
Downstream Bandwidth	Specify the limit of Downstream Bandwidth, which the specific local hosts use to receive traffic from the internet through the gateway.
Mode	Spécifier le mode de contrôle de bande passante pour les hôtes locaux spécifiques. Shared: La bande passante totale de tous les hôtes locaux est égale aux valeurs spécifiées Individual: La bande passante de chaque hôte local est égale aux valeurs spécifiées.

3. Cliquez sur Create. La nouvelle règle de contrôle de bande passante est ajoutée à la liste. Vous pouvez cliquez sur pour éditer la règle.



4. 7 Configuration VPN

Aperçu

VPN (Virtual Private Network) permet aux utilisateurs distants d'accéder à des ressources LAN sécurisées via un réseau public tel qu'Internet. Virtual indique que la connexion VPN est basée sur la connexion logique de bout en bout au lieu de la connexion physique de bout en bout. Private indique que les utilisateurs peuvent établir la connexion VPN en fonction de leurs besoins et que seuls les utilisateurs spécifiques sont autorisés à utiliser la connexion VPN.

Le noyau de la connexion VPN est de réaliser la communication en tunnel, qui remplit la tâche de l'encapsulation des données, la transmission de données et la décompression des données via le protocole de tunnelage. La passerelle prend en charge les protocoles de tunnelage communs qu'un VPN utilise pour sécuriser les données :

- **IPsec**

IPsec (IP Security) peut fournir des services de sécurité tels que la confidentialité des données, l'intégrité des données et l'authentification des données à la couche IP. IPsec utilise IKE (Internet Key Exchange) pour gérer la négociation de protocoles et d'algorithmes basés sur la stratégie spécifiée par l'utilisateur et pour générer les clés de chiffrement et d'authentification à utiliser par IPsec. IPsec peut être utilisé pour protéger un ou plusieurs chemins entre une paire d'hôtes, entre une paire de passerelles de sécurité ou entre une passerelle de sécurité et un hôte.

- **PPTP**

PPTP (Point-to-Point Tunneling Protocol) est un protocole réseau qui permet le transfert sécurisé de données d'un client distant vers un serveur d'entreprise privé en créant un VPN sur les réseaux de données TCP/IP. PPTP utilise le nom d'utilisateur et le mot de passe pour valider les utilisateurs.

- **L2TP**

L2TP (Layer 2 Tunneling Protocol) fournit un moyen pour un utilisateur de dialup de créer une connexion virtuelle point-à-point protocol (PPP) à un serveur réseau L2TP (LNS), qui peut être une passerelle de sécurité. L2TP envoie des cadres PPP à travers un tunnel entre un concentrateur d'accès L2TP (BAC) et le LNS. En raison du manque de confidentialité inhérent au protocole L2TP, il est souvent mis en œuvre avec IPsec. L2TP utilise le nom d'utilisateur et le mot de passe pour valider les utilisateurs.

- **OpenVPN**

OpenVPN utilise OpenSSL pour le chiffrement d'UDP et de TCP pour la transmission du trafic. OpenVPN utilise une connexion client-serveur pour fournir des communications sécurisées entre un serveur et un client distant via Internet. L'une des étapes les plus importantes dans la configuration d'OpenVPN est l'obtention d'un certificat utilisé pour l'authentification. Le contrôleur Omada SDN prend en charge la génération du certificat qui peut être téléchargé sous forme de fichier sur votre ordinateur. Avec le certificat importé, les clients distants sont vérifiés par le certificat et ont accès aux ressources LAN.

Il existe de nombreuses variantes de réseaux privés virtuels, la majorité étant basée sur deux modèles principaux :

■ **Site-to-Site VPN**

Un VPN de site à site crée une connexion entre deux réseaux à des emplacements géographiques différents. En règle générale, le siège social a mis en place le VPN du site au site avec la filiale pour fournir à la succursale un accès au réseau du siège social.



La passerelle gérée par Omada prend en charge deux types de VPN de site à site:

- Auto IPsec

  Le contrôleur crée automatiquement un tunnel VPN IPsec entre deux sites sur le même contrôleur. La connexion VPN est bidirectionnelle. Autrement dit, la création d'un VPN Auto Ipsecc du site A au site B fournit également la connectivité du site B au site A, et rien n'est nécessaire pour être configuré sur le site B.

- Manual IPsec

  Vous créez manuellement un tunnel VPN IPsec entre deux routeurs homologues via Internet, d'un routeur local à un routeur distant qui prend en charge IPsec. Omada géré passerelle sur ce site est le routeur homologue local.

■ **Client-to-Site VPN**

Un VPN client à site crée une connexion au réseau local à partir d'un hôte distant. Il est utile pour les télétravailleurs et les voyageurs d'affaires d'accéder à leur réseau local central à partir d'un endroit éloigné sans compromettre la vie privée et la sécurité.

La première étape pour créer une connexion VPN client à site consiste à déterminer le rôle des passerelles et le protocole de tunnelage VPN à utiliser :

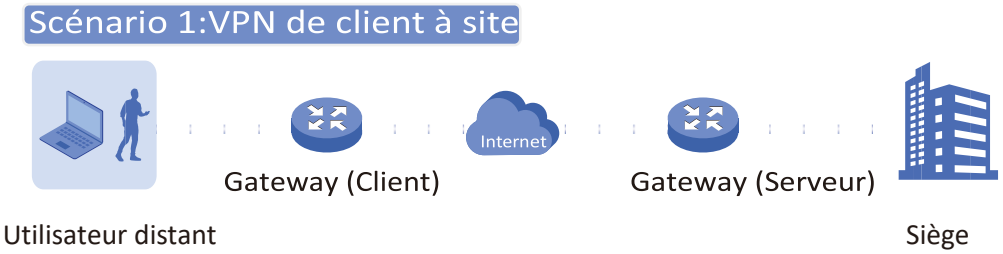
1. Serveur VPN

   La passerelle sur le réseau local fonctionne comme un serveur VPN pour fournir à un hôte distant un accès au réseau local. La passerelle qui fonctionne en tant que serveur VPN peut utiliser L2TP, PPTP, IPsec ou OpenVPN comme protocole de tunnelage.

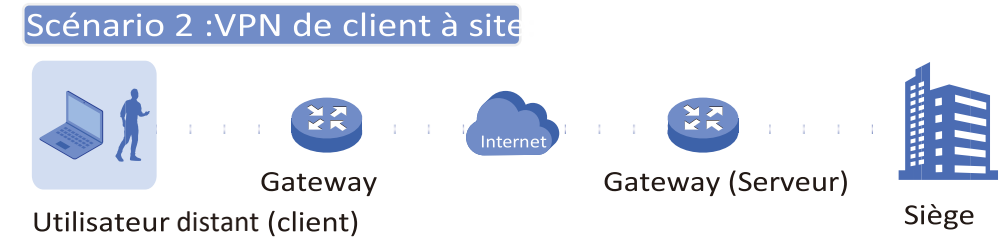
2. VPN Client

   Soit la passerelle de l'utilisateur distant, soit l'ordinateur portable ou le PC de l'utilisateur distant fonctionne comme client VPN.

Lorsque la passerelle de l'utilisateur distant fonctionne en tant que client VPN, la passerelle permet de créer des tunnels VPN entre ses hôtes connectés et le serveur VPN. La passerelle qui fonctionne en tant que client VPN peut utiliser L2TP, PPTP ou OpenVPN comme protocole de tunnelage.



Lorsque l'ordinateur portable ou le PC de l'utilisateur distant fonctionne comme le client VPN, l'ordinateur portable ou le PC utilise un logiciel client VPN pour créer des tunnels VPN entre lui-même et le serveur VPN. Le logiciel client VPN peut utiliser L2TP, PPTP, IPsec ou OpenVPN comme protocole de tunnelage.

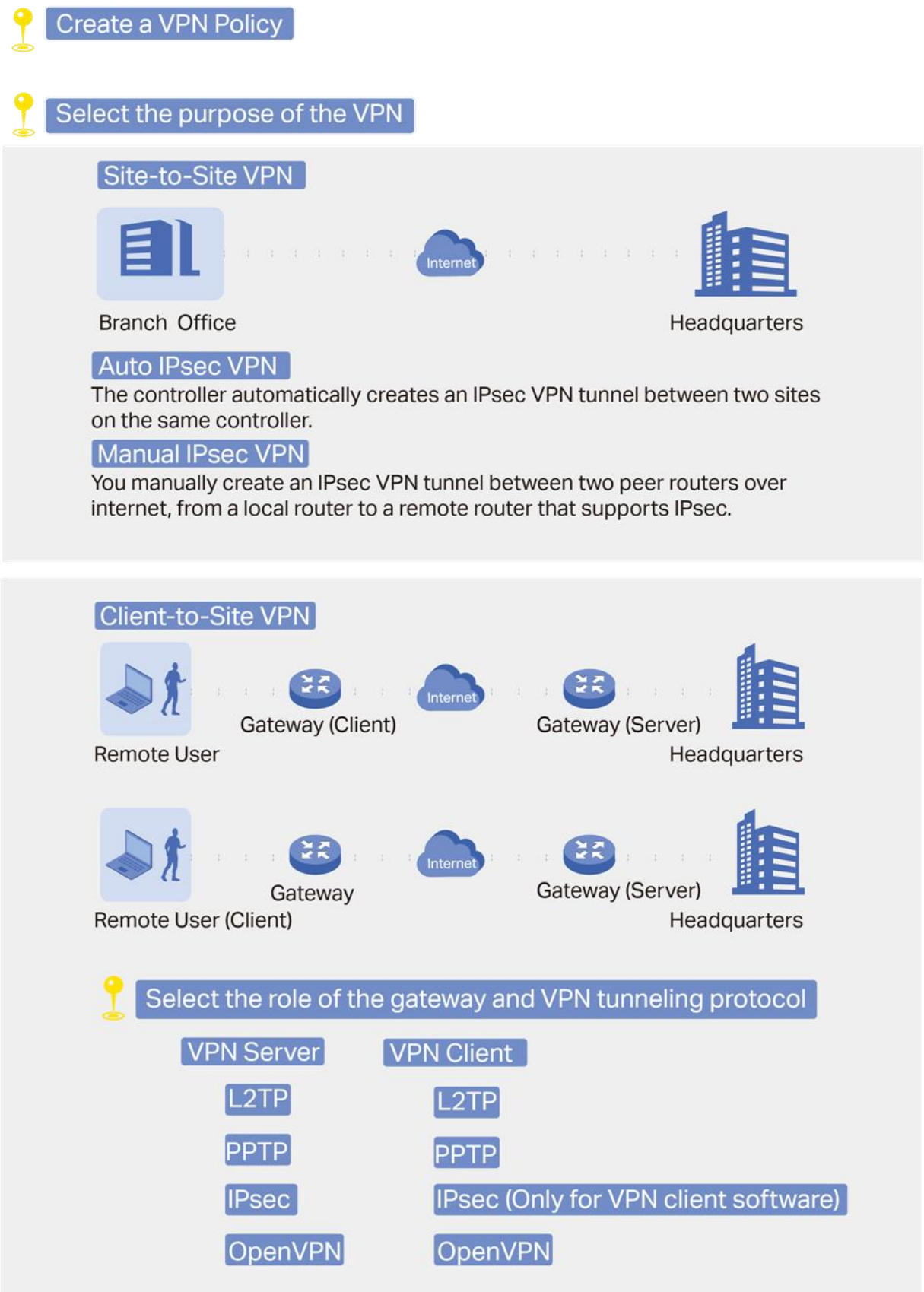


Note:

Dans le scénario 1, vous devez configurer le client VPN et le serveur VPN séparément sur les passerelles, tandis que les hôtes distants peuvent accéder aux réseaux locaux sans exécuter le logiciel client VPN.

Dans le scénario 2, vous devez configurer le serveur VPN sur la passerelle, puis configurer le logiciel client VPN sur l'ordinateur portable ou le PC de l'utilisateur distant, tandis que la passerelle de l'utilisateur distant n'a pas besoin de configuration VPN.

Voici l'infographie pour fournir un aperçu rapide des solutions VPN.



Configuration

Pour compléter la configuration VPN, procédez comme suit :

1.) Créez une nouvelle stratégie VPN et sélectionnez l'objet du VPN en fonction de vos besoins. Sélectionnez Site to-Site si vous souhaitez que le réseau soit connecté à un autre. Sélectionnez Client-à-Site si vous souhaitez que certains hôtes se connectent au réseau.

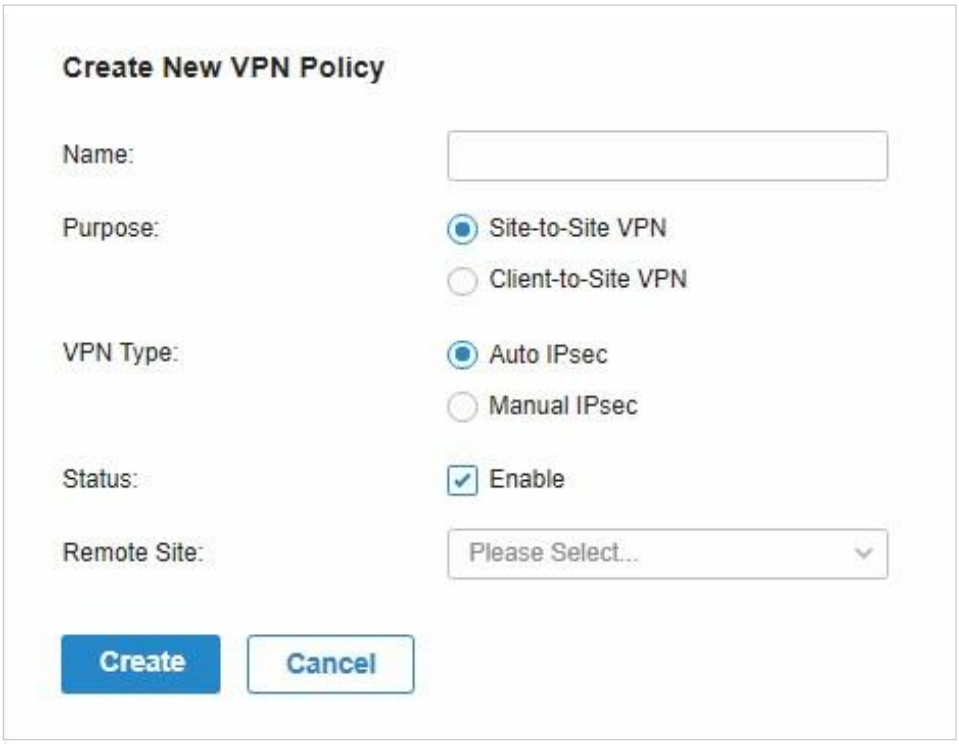
1) Sélectionnez le protocole de tunnel VPN et configurez la stratégie VPN en fonction du protocole.

■ **Configuration du VPN de site à site**

La passerelle gérée par Omada prend en charge deux types de VPN de site à site : Auto IPsec et Manual IPsec.

- Configuration du VPN d'Auto-IPsec

1. Allez dans Settings>VPN et cliquez sur + Create New VPN Policy pour charger la page suivante.



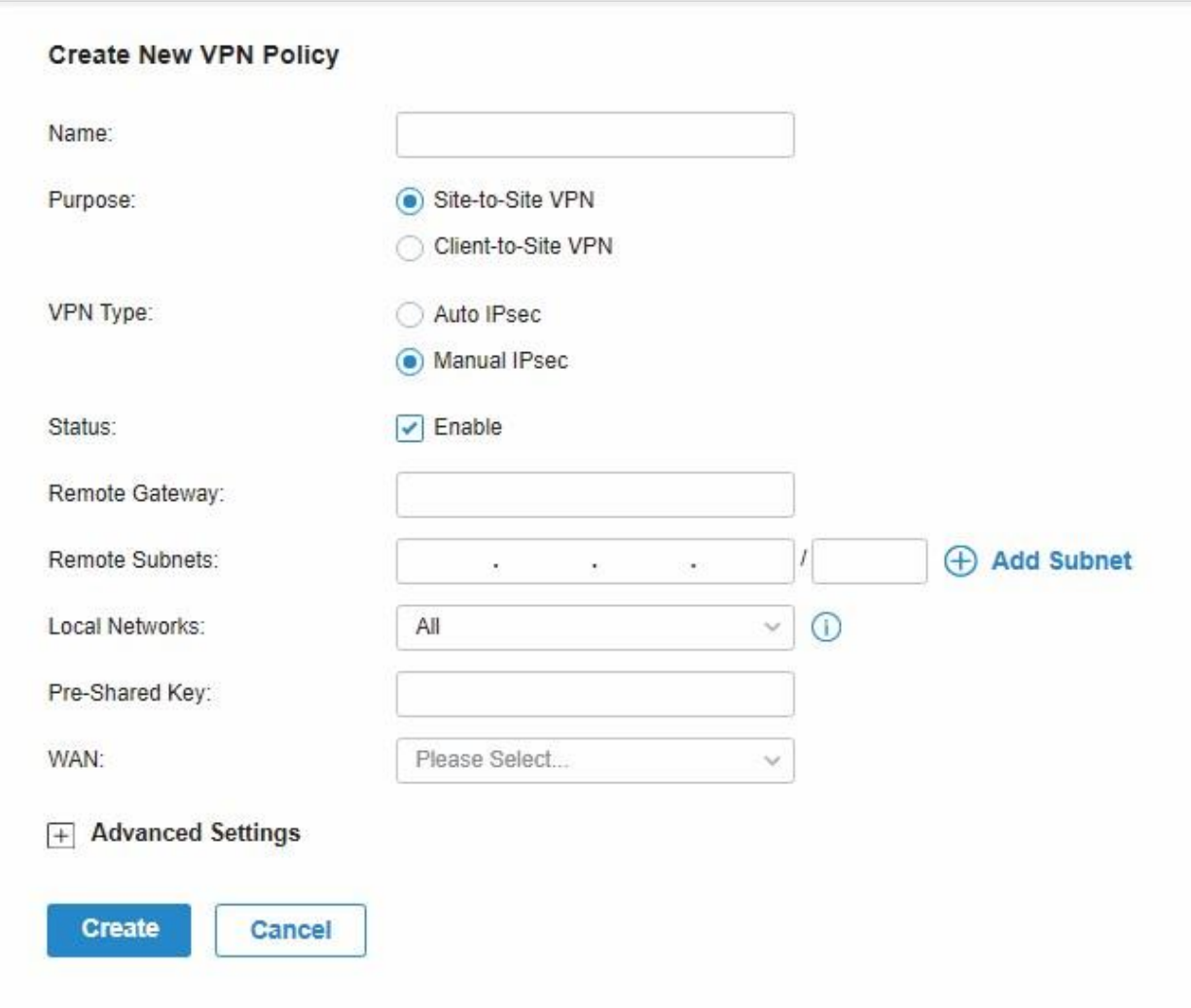
2. Entrez un nom pour identifier la stratégie VPN et sélectionnez l'objet en tant que VPN de site à site. Reportez-vous au tableau suivant pour configurer les paramètres requis, puis cliquez sur Create.

Name	Entrez un nom pour identifier la stratégie VPN.
Purpose	Sélectionnez l'objet du VPN Site-to-Site VPN.
VPN Type	Sélectionnez le type VPN comme Auto IPsec.

Status	Cliquez sur la case à cocher pour activer la stratégie VPN.
Remote Site	Sélectionnez le site à l'autre extrémité du tunnel VPN Auto IPsec. Assurez-vous que le site distant sélectionné dispose d'une passerelle gérée par Omada en ligne au sein du même contrôleur.

- Configuration du VPN manuel IPsec

1. Allez dans Settings>VPN Cliquez sur + Create New VPN Policy pour charger la page suivante.

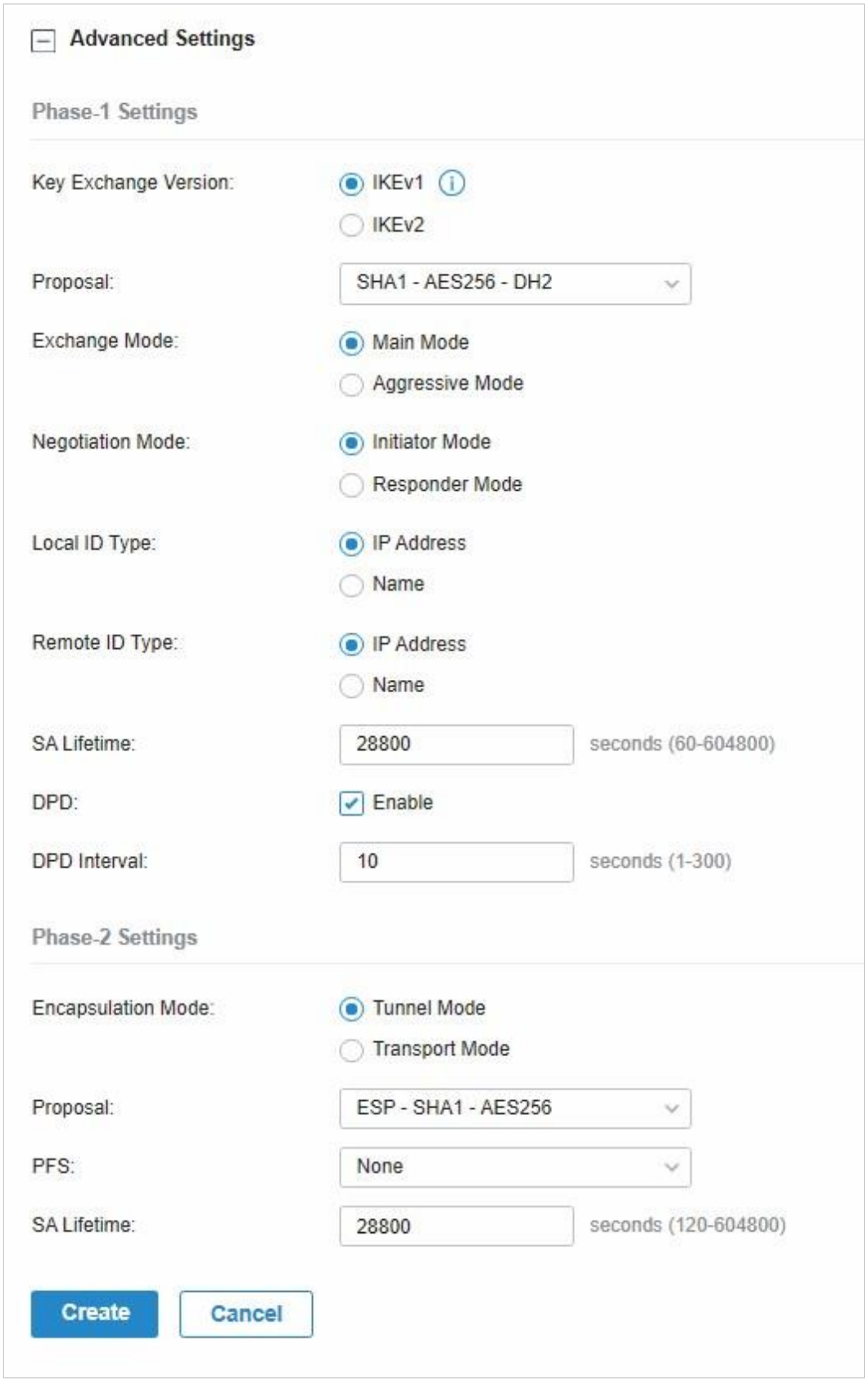


2. Entrez un nom pour identifier la stratégie VPN et sélectionnez l'objet en tant que VPN de site à site. Reportez-vous au tableau suivant pour configurer les paramètres de base et cliquez sur Create.

Name	Entrez un nom pour identifier la stratégie VPN.
Purpose	Sélectionnez l'objet du VPN Site-to-Site VPN.
VPN Type	Sélectionnez le type VPN comme Manual IPsec.

Status	Cliquez sur la case à cocher pour activer la stratégie VPN.
Remote Gateway	Entrez une adresse IP ou un nom de domaine comme passerelle sur l'homologue distant du tunnel VPN.
Remote Subnets	Entrez la plage d'adresses IP de LAN sur le pair distant du tunnel VPN.
Local Networks	Sélectionnez les réseaux du côté local du tunnel VPN. La stratégie VPN ne s'appliquera qu'aux réseaux locaux sélectionnés.
Pre-Shared Key	Entrez la clé pré-partagée (PSK). Les deux passerelles homologues doivent utiliser la même clé secrète pré-partagée pour l'authentification. Une clé pré-partagée est une chaîne de caractères qui est utilisée comme clé d'authentification. Les deux passerelles par les pairs créent une valeur de hachage basée sur la même clé pré-partagée et d'autres informations. Les valeurs de hachage sont ensuite échangées et vérifiées pour authentifier l'autre partie. Les clés pré-partagées doivent être longues et aléatoires pour la sécurité. Les touches courtes ou prévisibles pré-partagées peuvent être facilement brisées dans des attaques de force brute. Pour maintenir un niveau élevé de sécurité, il est recommandé aux administrateurs de mettre à jour périodiquement la clé pré-partagée.
WAN	Sélectionnez le port WAN sur lequel le tunnel VPN IPsec est établi.

1. Cliquez sur Paramètres avancés pour charger la page suivante.



Les paramètres avancés incluent les paramètres de phase 1 et les paramètres de phase 2. Phase-1 est utilisée pour configurer un canal crypté sécurisé que les deux pairs peuvent négocier phase-2, puis établir

les associations de sécurité IKE (IKE SA). Phase-2 est utilisé pour négocier un ensemble de paramètres qui définissent ce que le trafic peut passer par le VPN, et comment chiffrer et authentifier le trafic, puis établir les associations de sécurité IPsec (IPsec SA).

Reportez-vous au tableau suivant pour compléter les configurations en fonction de vos besoins réels, puis cliquez sur Créer.

Pour les paramètres de phase 1 :

Phase-1 Settings	La version IKE que vous sélectionnez détermine les paramètres de phase 1 disponibles et définit le processus de négociation. Les deux passerelles VPN doivent être configurées pour utiliser les mêmes paramètres de version IKE et de phase 1.
Internet Key Exchange Version	Sélectionnez la version du protocole IKE (Internet Key Exchange) qui est utilisé pour configurer des associations de sécurité pour IPsec. IKEv1 et IKEv2 sont pris en charge par des passerelles gérées par Omada, mais IKEv1 n'est disponible que lorsque la stratégie VPN est appliquée à un seul sous-réseau distant et à un seul réseau local. Notez que les deux passerelles homologues doivent être configurées pour utiliser la même version IKE.
Proposal	Préciser la proposition de phase de négociation IKE phase-1. Une proposition IKE répertorie l'algorithme de chiffrement, l'algorithme d'authentification et les groupes Diffie-Hellman (DH) à négocier avec l'homologue IPsec distant— Les algorithmes d'authentification vérifient l'intégrité et l'authenticité d'un message. Les types d'authentification incluent MD5 et SHA1. Les algorithmes de chiffrement protègent les données contre la lecture par un tiers. Les types d'algorithme de chiffrement incluent DES, 3DES, AES128, AES192 et AES256. Les groupes Diffie-Hellman (DH) déterminent la force de la clé utilisée dans le processus d'échange de clés. Le groupe DH comprend DH1, DH2, DH5, DH14, DH15, DH16, DH19, DH20, DH21, DH25 et DH26. Notez que les deux passerelles homologues doivent être configurées pour utiliser la même proposition.
Exchange Mode	Spécifier le mode Exchange IKE lorsque IKEv1 est sélectionné. Main Mode: Ce mode offre une protection de l'identité et échange plus d'informations, ce qui s'applique aux scénarios ayant des exigences plus élevées en matière de protection de l'identité. Aggressive Mode: Ce mode établit une connexion plus rapide mais avec une sécurité plus faible, qui s'applique aux scénarios ayant des exigences inférieures pour la protection de l'identité.

Negotiation Mode	Spécifier le mode de négociation IKE en tant que mode initiateur ou mode de répondeur. Initiator Mode: Ce mode signifie que le périphérique local initie une connexion au. Responder Mode: Ce mode signifie que le périphérique local attend la demande de connexion initiée par le pair.

Local ID Type	Spécifier le type d'ID local qui indique l'identificateur d'authentification envoyé au pair pour la négociation IKE. IP Address: Sélectionner l'adresse IP pour utiliser l'adresse IP pour l'authentification. Name: Sélectionnez Nom, puis entrez le nom dans le champ ID local pour utiliser le nom comme ID pour l'authentification. Notez que le type et la valeur de l'ID local doivent être les mêmes que l'ID distant donné pour l'homologue distant du tunnel VPN.
Local ID	Lorsque le type d'ID local est configuré en tant que nom, entrez un nom pour le périphérique local en tant qu'ID dans la négociation IKE. Le nom doit être dans le format de FQDN (Nom de domaine entièrement qualifié).
Remote ID Type	Spécifier le type d'ID distant qui indique l'identificateur d'authentification reçu de l'homologue pour la négociation IKE. IP Address: Sélectionner l'adresse IP pour utiliser l'adresse IP pour l'authentification. Name: Sélectionnez Nom, puis entrez le nom dans le champ ID distant pour utiliser le nom comme ID pour l'authentification. Notez que le type et la valeur de l'ID distant doivent être les mêmes que l'ID local donné pour l'homologue distant du tunnel VPN.
Remote ID	Lorsque le type d'ID distant est configuré en tant que nom, entrez un nom de l'homologue distant en tant qu'ID dans la négociation IKE. Le nom doit être dans le format de FQDN (Nom de domaine entièrement qualifié).
SA Lifetime	Spécifiez ISAKMP SA (Security Association) Lifetime dans la négociation IKE. Si la durée de vie de l'AS a expiré, l'ISAKMP SA associée sera supprimée.
DPD	Cochez la case pour activer la fonction DPD (Dead Peer Detect). S'il est activé, le point de terminaison IKE peut envoyer une demande DPD au pair pour vérifier si le pair IKE est vivant.

DPD Interval	Spécifiez l'intervalle entre l'envoi de demandes DPD avec DPD activé. Si le point de terminaison IKE reçoit une réponse de l'homologue pendant cet intervalle, il considère le pair vivant. Si le point de terminaison IKE ne reçoit pas de réponse pendant l'intervalle, il considère le pair mort et supprime l'AS.
Pour les paramètres de phase 2:	
Phase-2 Settings	Le but des négociations de la phase 2 est d'établir la phase 2 sa (également appelée IPsec SA). L'IPsec SA est un ensemble de spécifications de trafic qui indiquent à l'appareil quel trafic envoyer sur le VPN, et comment chiffrer et authentifier ce trafic.
Encapsulation Mode	Spécifiez le mode encapsulation en mode tunnel ou mode de transport. Lorsque les deux extrémités du tunnel sont hôtes, l'un ou l'autre mode peut être choisi. Lorsqu'au moins l'un des points de terminaison d'un tunnel est une passerelle de sécurité, comme un routeur ou un pare-feu, le mode tunnel est recommandé pour assurer la sécurité.
Proposal	Spécifiez la proposition de phase de négociation ike phase-2. Une proposition IPsec répertorie l'algorithme de chiffrement, l'algorithme d'authentification et le protocole à négocier avec le pair IPsec distant. Notez que les deux passerelles homologues doivent être configurées pour utiliser la même proposition.
PFS	Sélectionnez le groupe DH pour activer **pfs** (Perfect Forward Security) pour le mode IKE, puis la clé générée dans la phase-2 ne sera pas pertinente avec la clé dans la phase-1, qui améliorent la sécurité du réseau. Avec Aucun sélectionné, cela signifie que le SFP est désactivé et que la clé de la phase 2 sera générée en fonction de la clé de phase 1.
SA Lifetime	Spécifiez IPsec SA (Security Association) **Lifetime** dans la négociation IKE. Si la durée de vie de sa a expiré, l'IPsec SA connexe sera supprimé.

■ Configuration du VPN client-site

La passerelle gérée par Omada prend en charge sept types de VPN de client à site en fonction du rôle de votre passerelle gérée par Omada et du protocole que vous avez utilisé :

Configuration de la passerelle en tant que serveur VPN à l'aide de L2TP

Configuration de la passerelle en tant que serveur VPN à l'aide de PPTP

Configuration de la passerelle en tant que serveur VPN à l'aide d'IPsec

Configuration de la passerelle en tant que serveur VPN à l'aide d'OpenVPN

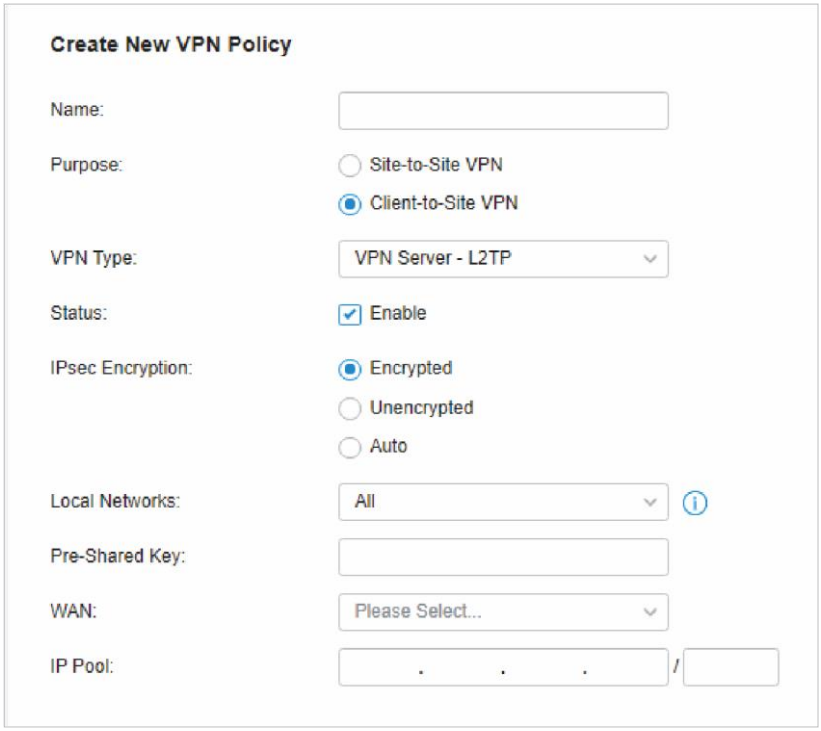
Configuration de la passerelle en tant que client VPN à l'aide de L2TP

Configuration de la passerelle en tant que client VPN à l'aide de PPTP

Configuration de la passerelle en tant que client VPN à l'aide d'OpenVPN

• Configuration de la passerelle en tant que serveur VPN à l'aide de L2TP

1. Allez dans Settings>VPN et cliquez sur + Create New VPN Policy pour charger la page suivante.

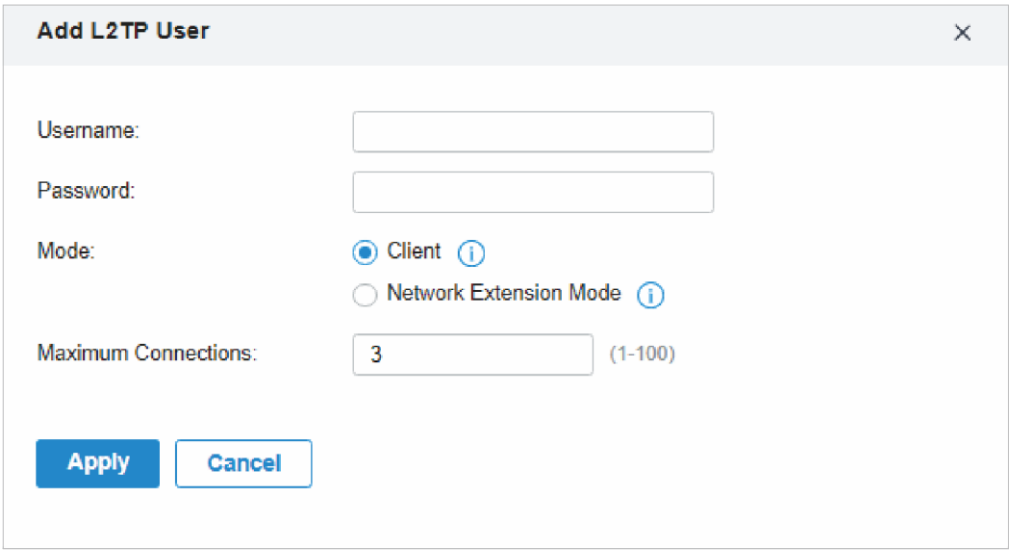


2. Entrez un nom pour identifier la stratégie VPN et sélectionnez l'objet en tant que VPN de client à site. Reportez-vous au tableau suivant pour configurer les paramètres requis, puis cliquez sur Create.

Name	Entrez un nom pour identifier la stratégie VPN.
Purpose	Sélectionnez l'objet du VPN Client-to-Site VPN.
VPN Type	Sélectionnez le type VPN comme VPN Server - L2TP.
Status	Cliquez sur la case à cocher pour activer la stratégie VPN.

IPsec Encryption	Spécifier s'il faut activer le chiffrement du tunnel. Encrypted: Sélectionnez Crypté pour chiffrer le tunnel L2TP par IPsec (L2TP sur IPsec). Avec crypté sélectionné, entrez la clé pré-partagée pour l'authentification IKE. Le serveur VPN et le client VPN doivent utiliser la même clé secrète pré-partagée pour l'authentification. Unencrypted: Avec un non chiffré sélectionné, le tunnel L2TP ne sera pas crypté par IPsec. Auto: Avec la sélection automatique, le serveur L2TP déterminera s'il faut chiffrer le tunnel en fonction des paramètres de chiffrement du client. Et entrez la clé pré-partagée pour l'authentification IKE. Le serveur VPN et le client VPN doivent utiliser la même clé secrète pré-partagée pour l'authentification.
Local Networks	Sélectionnez les réseaux du côté local du tunnel VPN. La stratégie VPN ne s'appliquera qu'aux réseaux locaux sélectionnés.
Pre-shared Key	Entrez la clé secrète pré-partagée lorsque iPsec Encryption est sélectionné comme crypté et automatique. Les deux routeurs homologues doivent utiliser la même clé secrète pré-partagée pour l'authentification.
WAN	Sélectionnez le port WAN sur lequel le tunnel VPN L2TP est établi. Chaque port WAN prend en charge un seul tunnel VPN L2TP lorsque la passerelle fonctionne en tant que serveur L2TP.
IP Pool	Entrez l'adresse IP et le masque de sous-réseau pour décider de la plage du pool IP VPN. Le serveur VPN affecte l'adresse IP à l'hôte distant lorsque le tunnel est établi. Vous pouvez spécifier toute adresse IP raisonnable qui ne provoquera pas de chevauchement avec l'adresse IP du RÉSEAU LOCAL sur le routeur homologue local.

3. Créez les comptes d'utilisateurs VPN pour valider les hôtes distants dans la liste utilisateur L2TP. Cliquez ⊕ Add User pour charger la page suivante.



Username	Entrez le nom d'utilisateur utilisé pour le tunnel VPN. Le client L2TP utilise le nom d'utilisateur pour la validation avant d'accéder au réseau.
Password	Entrez le mot de passe de l'utilisateur. Le client L2TP utilise le mot de passe pour la validation avant d'accéder au réseau.
Mode	Spécialiste le mode de connexion pour les utilisateurs L2TP. Client: Ce mode permet au client de demander une adresse IP et le serveur fournit les adresses IP à partir du pool IP VPN. Avec ce mode sélectionné, définissez le nombre maximal de connexions VPN simultanées avec le même compte dans Connexions maximales. Network Extension Mode: Ce mode permet uniquement aux clients du sous-réseau configuré de se connecter au serveur et d'obtenir des services VPN. Avec ce mode sélectionné, spécifiez le sous-réseau dans les sous-réseaux distants.
Maximum Connections	Avec le mode Client sélectionné, définissez le nombre maximum de connexions VPN simultanées avec le même compte.
Remote Subnets	Avec le mode extension réseau sélectionné, seuls les clients du sous-réseau configuré sont autorisés à se connecter au serveur et à obtenir des services VPN. Cliquez pour spécifier le sous-réseau.

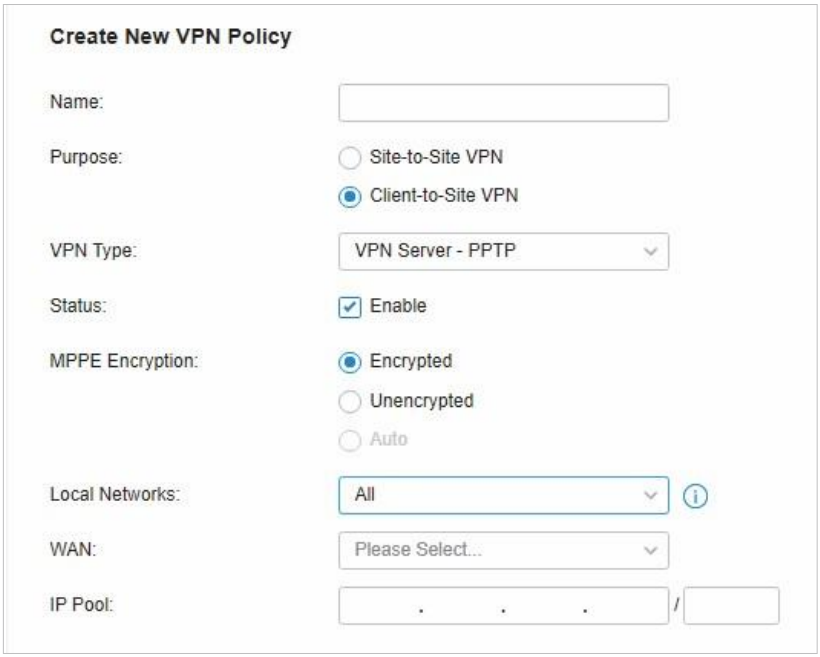
Pour modifier ou supprimer les utilisateurs L2TP, cliquez sur l'icône de la colonne Action.



	Afficher et modifier les informations de compte des
	Supprimer l'utilisateur L2TP .

• Configuration de la passerelle en tant que serveur VPN à l'aide de PPTP

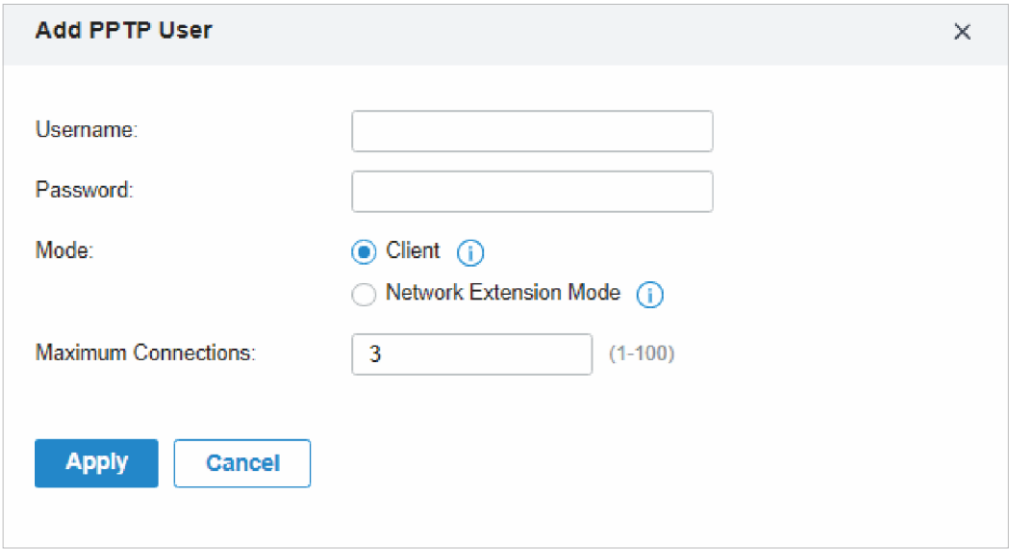
1. Allez dans Settings>VPN et cliquez + Create New VPN Policy pour charger la page suivante.



2. Entrez un nom pour identifier la stratégie VPN et sélectionnez l'objet en tant que VPN de client à site. Reportez-vous au tableau suivant pour configurer les paramètres requis, puis cliquez sur Create.

Name	Entrez un nom pour identifier la stratégie VPN.
Purpose	Sélectionnez l'objet du VPN Client-to-Site VPN.
VPN Type	Sélectionnez le type VPN comme VPN Server - PPTP.
Status	Cliquez sur la case à cocher pour activer la stratégie VPN.
MPPE Encryption	Spécifier s'il faut activer MPPE (Microsoft Point-to-Point Encryption) pour le tunnel. Encrypted: Avec crypté sélectionné, le tunnel PPTP sera crypté par MPPE. Unencrypted: Avec un non chiffré sélectionné, le tunnel PPTP ne sera pas crypté par MPPE.
Local Networks	Sélectionnez les réseaux du côté local du tunnel VPN. La stratégie VPN ne s'appliquera qu'aux réseaux locaux sélectionnés.
WAN	Sélectionnez le port WAN sur lequel le tunnel VPN PPTP est établi. Chaque port WAN prend en charge un seul tunnel VPN PPTP lorsque la passerelle fonctionne comme un serveur PPTP.
IP Pool	Entrez l'adresse IP et le masque de sous-réseau pour décider de la plage du pool IP VPN. Le serveur VPN affecte l'adresse IP à l'hôte distant lorsque le tunnel est établi. Vous pouvez spécifier toute adresse IP raisonnable qui ne provoquera pas de chevauchement avec l'adresse IP du RÉSEAU LOCAL sur le routeur homologue local.

1. Créez les comptes d'utilisateurs VPN pour valider les hôtes distants dans la liste d'utilisateurs PPTP. Cliquez sur ⊕ Add User pour charger la page suivante.



Username	Entrez le nom d'utilisateur utilisé pour le tunnel VPN. Le client PPTP utilise le nom d'utilisateur pour la validation avant d'accéder au réseau.
Password	Entrez le mot de passe de l'utilisateur. Le client PPTP utilise le mot de passe de la validation avant d'accéder au réseau.
Mode	Spécifier le mode de connexion pour les utilisateurs PPTP. Client: Ce mode permet au client de demander une adresse IP et le serveur fournit les adresses IP à partir du pool IP VPN. Avec ce mode sélectionné, définissez le nombre maximal de connexions VPN simultanées avec le même compte dans Maximum Connections. Network Extension Mode: Ce mode permet uniquement aux clients du sous-réseau configuré de se connecter au serveur et d'obtenir des services VPN. Avec ce mode sélectionné, spécifiez le sous-réseau dans les sous-réseaux distants.
Maximum Connections	Avec le mode Client sélectionné, définissez le nombre maximum de connexions VPN simultanées avec le même compte.
Remote Subnets	Avec le mode extension réseau sélectionné, seuls les clients du sous-réseau configuré sont autorisés à se connecter au serveur et à obtenir des services VPN. Cliquez pour spécifier le sous-réseau.

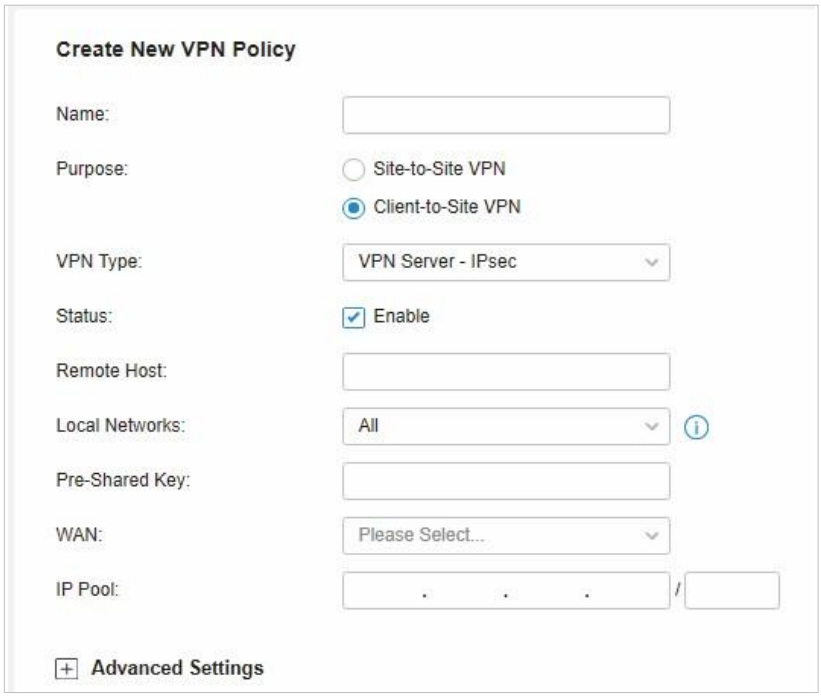
Pour modifier ou supprimer les utilisateurs PPTP, cliquez sur l'icône de la colonne Action.



	View and edit the account information of users.
	Delete the PPTP user.

• Configuration de la passerelle en tant que serveur VPN à l'aide d'IPsec

1 Allez dans Settings>VPN et cliquez sur + Create New VPN Policy pour charger la page suivante.



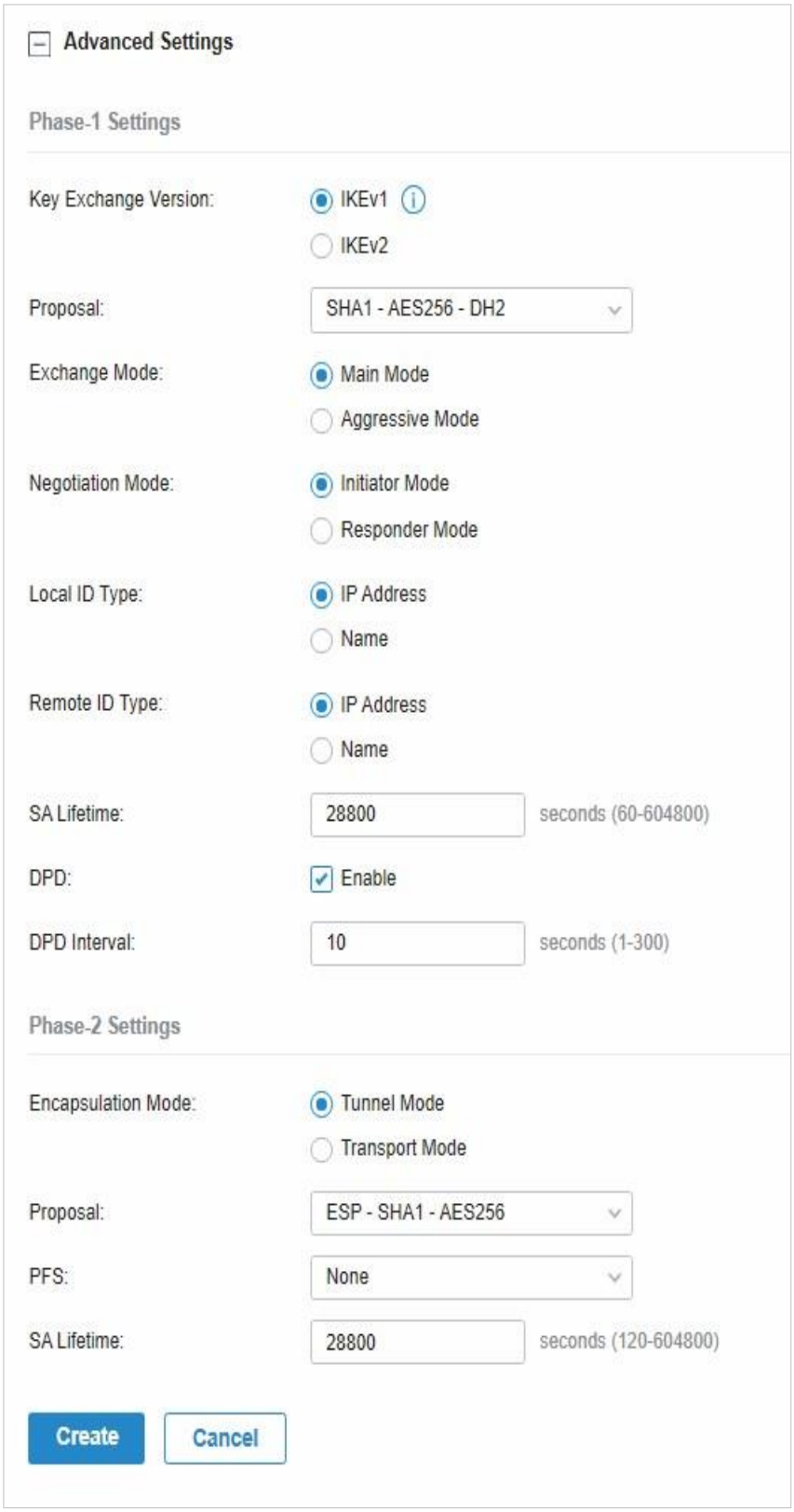
2. Entrez un nom pour identifier la stratégie VPN et sélectionnez l'objet en tant que VPN de client à site. Reportez-vous au tableau suivant pour configurer les paramètres de base et cliquez sur Create.

Name	Entrez un nom pour identifier la stratégie VPN.
Purpose	Sélectionnez l'objet du VPN Client-to-Site VPN.

VPN Type	Sélectionnez le type VPN comme VPN Server - IPsec.
Status	Cliquez sur la case à cocher pour activer la stratégie VPN.

Remote Host	Entrez une adresse IP ou un nom de domaine de l'hôte sur le pair distant du tunnel VPN. 0.0.0.0 représente toute adresse IP.
Local Networks	Sélectionnez les réseaux du côté local du tunnel VPN. La stratégie VPN ne s'appliquera qu'aux réseaux locaux sélectionnés.
Pre-Shared Key	Entrez la clé pré-partagée (PSK). Les deux passerelles homologues doivent utiliser la même clé secrète pré-partagée pour l'authentification. Une clé pré-partagée est une chaîne de caractères qui est utilisée comme clé d'authentification. Les deux pairs VPN créent une valeur de hachage basée sur la même clé pré-partagée et d'autres informations. Les valeurs de hachage sont ensuite échangées et vérifiées pour authentifier l'autre partie. Les clés pré-partagées doivent être longues et aléatoires pour la sécurité. Les touches courtes ou prévisibles pré-partagées peuvent être facilement brisées dans des attaques de force brute. Pour maintenir un niveau élevé de sécurité, il est recommandé aux administrateurs de mettre à jour périodiquement la clé pré-partagée.
WAN	Sélectionnez le port WAN sur lequel le tunnel VPN IPsec est établi.
IP Pool	Entrez l'adresse IP et le masque de sous-réseau pour décider de la plage du pool IP VPN. Le serveur VPN affecte l'adresse IP à l'hôte distant lorsque le tunnel est établi. Vous pouvez spécifier toute adresse IP raisonnable qui ne provoquera pas de chevauchement avec l'adresse IP du RÉSEAU LOCAL sur le routeur homologue local.

3. Cliquez sur Paramètres avancés pour charger la page suivante.



Les paramètres avancés incluent les paramètres de phase 1 et les paramètres de phase 2. Phase-1 est utilisée pour configurer un canal crypté sécurisé que les deux pairs peuvent négocier phase-2, puis établir les associations de sécurité IKE (IKE SA). Phase-2 est utilisé pour négocier un ensemble de paramètres qui définissent ce que le trafic peut passer par le VPN, et comment chiffrer et authentifier le trafic, puis établir les associations de sécurité IPsec (IPsec SA).

Reportez-vous au tableau suivant pour compléter les configurations en fonction de vos besoins réels et cliquez sur Create.

Pour les paramètres de phase 1:

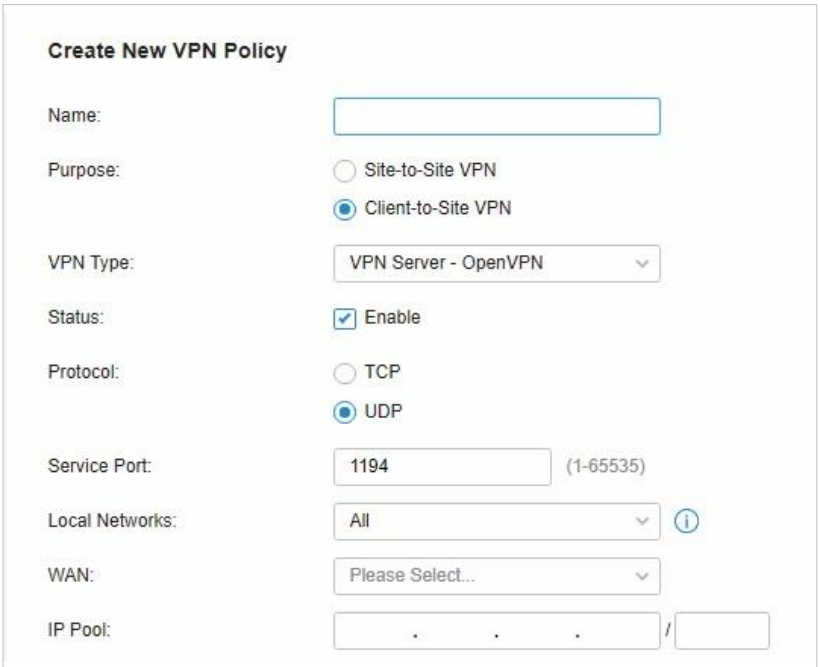
Phase-1 Settings	La version IKE que vous sélectionnez détermine les paramètres de phase 1 disponibles et définit le processus de négociation. Les deux passerelles VPN doivent être configurées pour utiliser les mêmes paramètres de version IKE et de phase 1.
Internet Key Exchange Version	Sélectionnez la version du protocole IKE (Internet Key Exchange) qui est utilisé pour configurer des associations de sécurité pour IPsec. IKEv1 et IKEv2 sont pris en charge par des passerelles gérées par Omada, mais IKEv1 n'est disponible que lorsque la stratégie VPN est appliquée à un seul sous-réseau distant et à un seul réseau local. Notez que les deux pairs VPN doivent être configurés pour utiliser la même version IKE.
Proposal	Préciser la proposition de phase de négociation IKE phase-1. Une proposition IKE répertorie l'algorithme de chiffrement, l'algorithme d'authentification et les groupes Diffie-Hellman (DH) à négocier avec l'homologue IPsec distant— Les algorithmes d'authentification vérifient l'intégrité et l'authenticité d'un message. Les types d'authentification incluent MD5 et SHA1. Les algorithmes de chiffrement protègent les données contre la lecture par un tiers. Les types d'algorithme de chiffrement incluent DES, 3DES, AES128, AES192 et AES256. Les groupes Diffie-Hellman (DH) déterminent la force de la clé utilisée dans le processus d'échange de clés. Le groupe DH comprend DH1, DH2, DH5, DH14, DH15, DH16, DH19, DH20, DH21, DH25 et DH26. Notez que les deux pairs VPN doivent être configurés pour utiliser la même proposition.
Exchange Mode	Spécifiez le mode Exchange IKE lorsque IKEv1 est sélectionné. Mode principal : ce mode offre une protection d'identité et échange plus d'informations, ce qui s'applique aux scénarios ayant des exigences plus élevées en matière de protection de l'identité. Mode agressif : ce mode établit une connexion plus rapide mais avec une sécurité inférieure, qui s'applique aux scénarios ayant des exigences inférieures pour la protection de l'identité.

Negotiation Mode	Spécifiez le mode de négociation IKE en mode initiateur ou en mode répondeur. Mode initiateur : ce mode signifie que le périphérique local initie une connexion au pair. Mode répondeur : ce mode signifie que l'appareil local attend la demande de connexion initiée par le pair.
Local ID Type	Spécifier le type d'ID local qui indique l'identificateur d'authentification envoyé au pair pour la négociation IKE. IP Address: Sélectionner l'adresse IP pour utiliser l'adresse IP pour l'authentification. Name: Sélectionnez Nom, puis entrez le nom dans le champ ID local pour utiliser le nom comme ID pour l'authentification. Notez que le type et la valeur de l'ID local doivent être les mêmes que l'ID distant donné pour l'homologue distant du tunnel VPN.
Local ID	Lorsque le type d'ID local est configuré en tant que nom, entrez un nom pour le périphérique local en tant qu'ID dans la négociation IKE. Le nom doit être au format de nom complet (nom de domaine entièrement qualifié).
Remote ID Type	Spécifier le type d'ID distant qui indique l'identificateur d'authentification reçu de l'homologue pour la négociation IKE. IP Address: Sélectionner l'adresse IP pour utiliser l'adresse IP pour l'authentification. Name: Sélectionnez Nom, puis entrez le nom dans le champ ID distant pour utiliser le nom comme ID pour l'authentification. Notez que le type et la valeur de l'ID distant doivent être les mêmes que l'ID local donné pour l'homologue distant du tunnel VPN.
Remote ID	Lorsque le type d'ID distant est configuré en tant que nom, entrez un nom de l'homologue distant en tant qu'ID dans la négociation IKE. Le nom doit être au format de nom complet (nom de domaine entièrement qualifié).
SA Lifetime	Spécifiez ISAKMP SA (Security Association) Lifetime dans la négociation IKE. Si la durée de vie de l'AS expire, l'ISAKMP SA associée sera supprimée.
DPD	Cochez la case pour activer la fonction DPD (Dead Peer Detect). S'il est activé, le point de terminaison IKE peut envoyer une demande DPD au pair pour vérifier si l'homologue IKE est vivant.

DPD Interval	Spécifiez l'intervalle entre l'envoi de demandes DPD avec DPD activé. Si le point de terminaison IKE reçoit une réponse de l'homologue pendant cet intervalle, il considère le pair vivant. Si le point de terminaison IKE ne reçoit pas de réponse pendant l'intervalle, il considère le pair mort et supprime l'AS.
Pour les paramètres de phase 2:	
Phase-2 Settings	Le but des négociations de la phase 2 est d'établir la phase 2 sa (également appelée IPsec SA). L'IPsec SA est un ensemble de spécifications de trafic qui indiquent à l'appareil quel trafic envoyer sur le VPN, et comment chiffrer et authentifier ce trafic.
Encapsulation Mode	Spécifiez le mode encapsulation en mode tunnel ou mode de transport. Lorsque les deux extrémités du tunnel sont hôtes, l'un ou l'autre mode peut être choisi. Lorsqu'au moins l'un des points de terminaison d'un tunnel est une passerelle de sécurité, comme un routeur ou un pare-feu, le mode tunnel est recommandé pour assurer la sécurité.
Proposal	Spécifiez la proposition de phase de négociation ike phase-2. Une proposition IPsec répertorie l'algorithme de chiffrement, l'algorithme d'authentification et le protocole à négocier avec le pair IPsec distant. Notez que les deux passerelles homologues doivent être configurées pour utiliser la même proposition.
PFS	Sélectionnez le groupe DH pour activer PFS (Perfect Forward Security) pour le mode IKE, puis la clé générée dans la phase-2 ne sera pas pertinente avec la clé dans la phase-1, qui améliorent la sécurité du réseau. Avec Aucun sélectionné, cela signifie que le SFP est désactivé et que la clé de la phase 2 sera générée en fonction de la clé de phase 1.
SA Lifetime	Spécifiez IPsec SA (Security Association) Lifetime dans la négociation IKE. Si la durée de vie de l'AS expire, l'IPsec SA associée sera supprimée.

• Configuration de la passerelle en tant que serveur VPN à l'aide d'OpenVPN

1. Allez dans Settings>VPN et cliquez sur + Create New VPN Policy pour charger la page suivante.

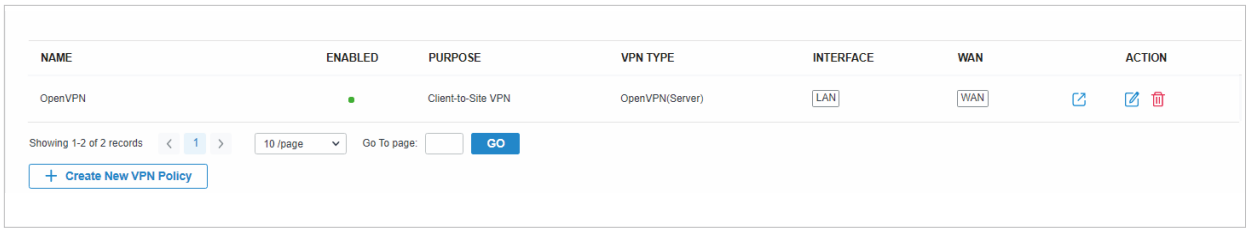


2. Entrez un nom pour identifier la stratégie VPN et sélectionnez l'objet en tant que VPN de client à site. Reportez-vous au tableau suivant pour configurer les paramètres requis, puis cliquez sur Create.

Name	Entrez un nom pour identifier la stratégie VPN.
Purpose	Sélectionnez l'objet du VPN Client-to-Site VPN.
VPN Type	Sélectionnez le type VPN comme VPN Server - OpenVPN.
Status	Cliquez sur la case à cocher pour activer la stratégie VPN.
Protocol	Sélectionnez le protocole de communication pour la passerelle qui fonctionne comme un serveur OpenVPN. Deux protocoles de communication sont disponibles : TCP et UDP.
Service Port	Entrez un port de service VPN auquel un périphérique VPN se connecte.
Local Networks	Sélectionnez les réseaux du côté local du tunnel VPN. La stratégie VPN ne s'appliquera qu'aux réseaux locaux sélectionnés.
WAN	Sélectionnez le port WAN sur lequel le tunnel VPN est établi. Chaque port WAN ne prend en charge qu'un seul tunnel OpenVPN lorsque la passerelle fonctionne comme serveur OpenVPN.

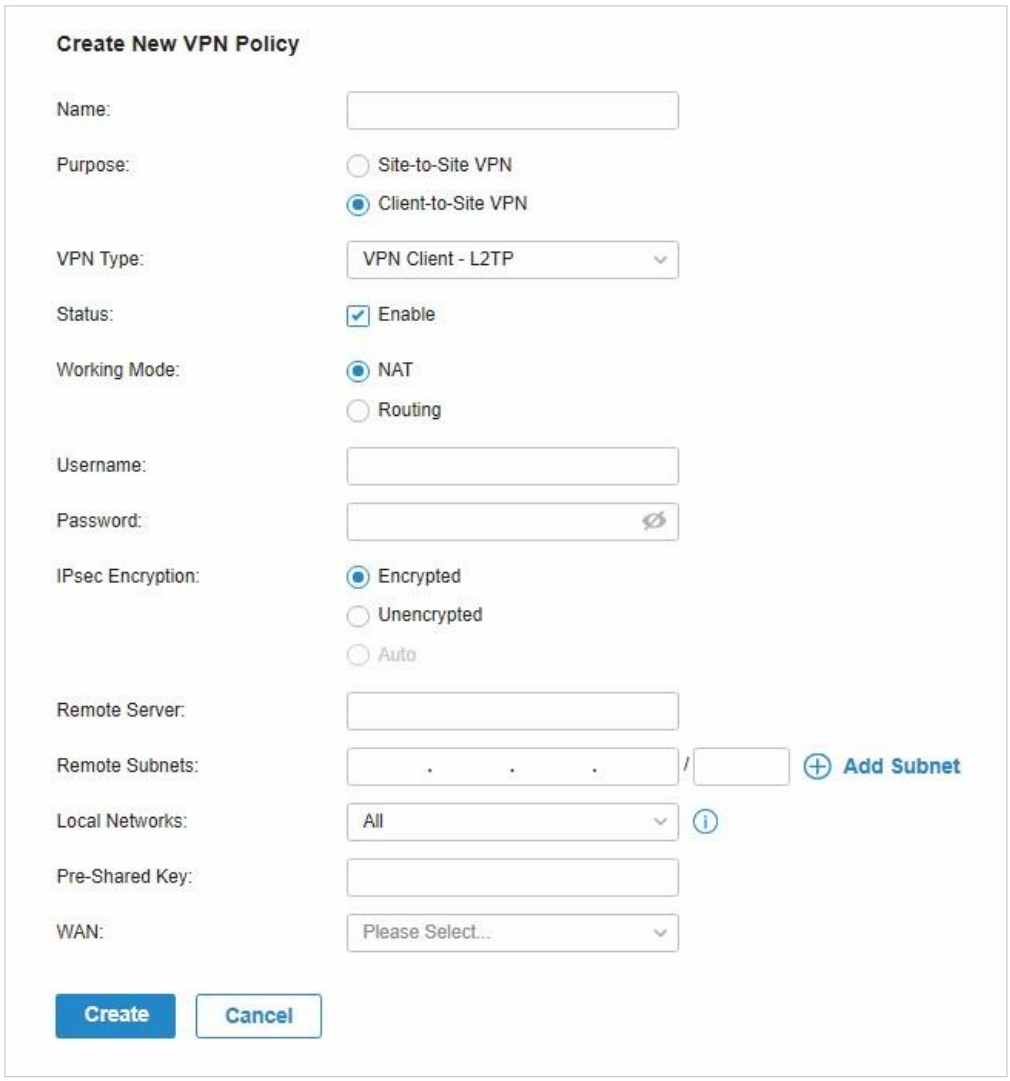
IP Pool	Entrez l'adresse IP et le masque de sous-réseau pour décider de la plage du pool IP VPN. Le serveur VPN affecte l'adresse IP à l'hôte distant lorsque le tunnel est établi. Vous pouvez spécifier toute adresse IP raisonnable qui ne provoquera pas de chevauchement avec l'adresse IP du RÉSEAU LOCAL sur le routeur homologue local.

1. Après avoir cliqué sur Créer pour enregistrer la stratégie VPN, accédez à la liste de stratégie VPN, puis cliquez dans la colonne Action pour exporter le fichier OpenVPN qui se termine par. ovpn qui doit être utilisé par le client distant.
2. Le fichier OpenVPN exporté contient les informations de certificat et de configuration.



• Configuration de la passerelle en tant que client VPN à l'aide de L2TP

1. Allez dans Settings>VPN et cliquez sur + Create New VPN Policy pour charger la page suivante.



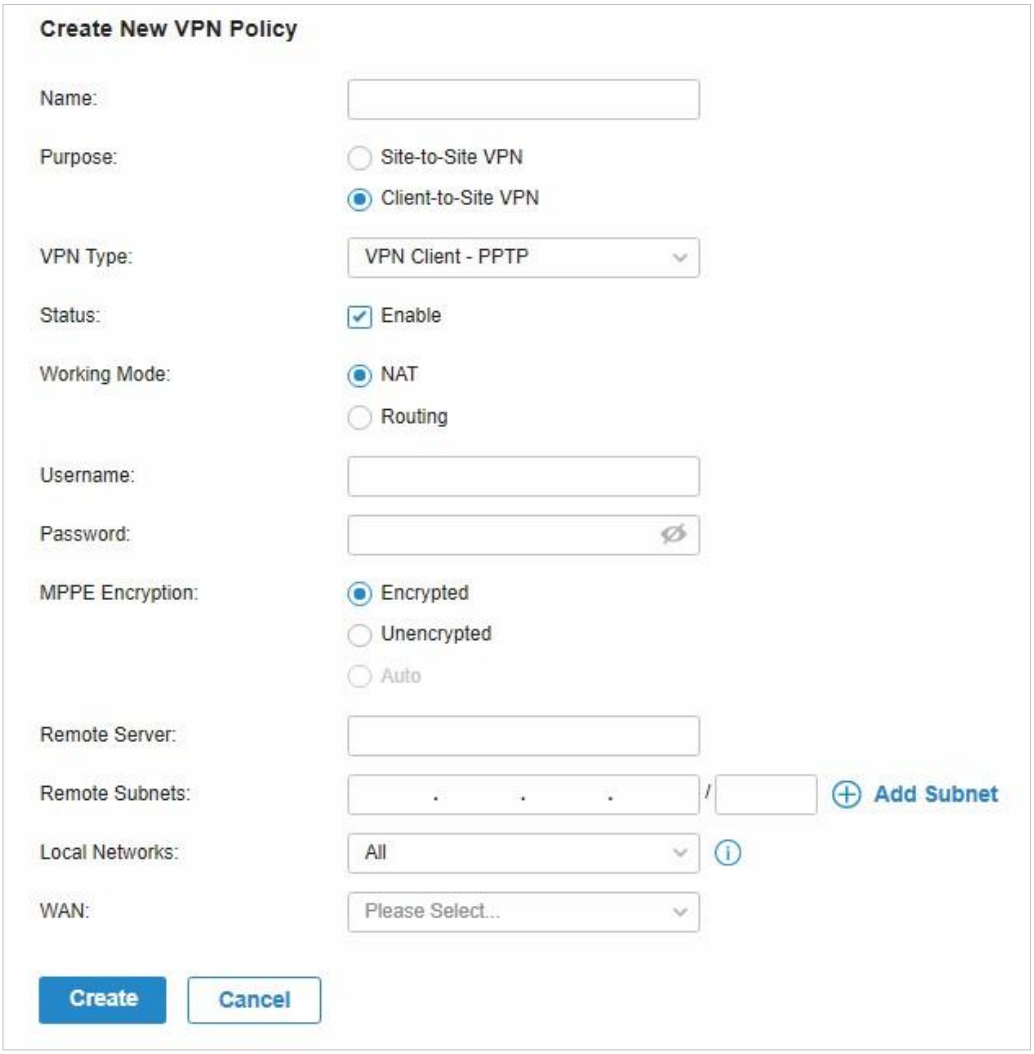
2. Entrez un nom pour identifier la stratégie VPN et sélectionnez l'objet en tant que VPN de client à site. Reportez-vous au tableau suivant pour configurer les paramètres requis, puis cliquez sur Create.

Name	Entrez un nom pour identifier la stratégie VPN.
Purpose	Sélectionnez l'objet du VPN Client-to-Site VPN.
VPN Type	Sélectionnez le type VPN comme VPN Client - L2TP.
Status	Cliquez sur la case à cocher pour activer la stratégie VPN.

Working Mode	Spécifiez le mode de travail en tant que NAT ou Routage. NAT : avec le mode NAT (Traduction d'adresses réseau) sélectionné, le client L2TP utilise l'adresse IP assignée comme adresses source de l'en-tête IP d'origine lors de l'transfert des paquets L2TP. Routage : avec routage sélectionné, le client L2TP utilise sa propre adresse IP comme adresses source de l'en-tête IP d'origine du transfert des paquets L2TP.
Username	Entrez le nom d'utilisateur utilisé pour le tunnel VPN. Ce nom d'utilisateur doit être le même que celui du serveur L2TP.
Password	Entrez le mot de passe de l'utilisateur. Ce mot de passe doit être le même que celui du serveur L2TP.
IPsec Encryption	Spécifiez-s'il faut activer le chiffrement du tunnel. Encrypted: Sélectionnez Crypté pour chiffrer le tunnel L2TP par IPsec (L2TP sur IPsec). Avec crypté sélectionné, entrez la clé pré-partagée pour l'authentification IKE. Le serveur VPN et le client VPN doivent utiliser la même clé secrète pré-partagée pour l'authentification. Unencrypted: Avec non chiffré sélectionné, le tunnel L2TP ne sera pas crypté par IPsec.
Remote Server	Entrez l'adresse IP ou le nom de domaine du serveur L2TP.
Remote Subnets	Entrez l'adresse IP et le masque de sous-réseau pour spécifier le réseau distant. C'est toujours la plage d'adresses IP de LAN sur le pair distant du tunnel VPN.
Local Networks	Sélectionnez les réseaux du côté local du tunnel VPN. La stratégie VPN ne s'appliquera qu'aux réseaux locaux sélectionnés.
Pre-shared Key	Entrez la clé secrète pré-partagée lorsque le tunnel L2TP est crypté par IPsec. Les deux passerelles homologues doivent utiliser la même clé secrète pré-partagée pour l'authentification.
WAN	Sélectionnez le port WAN sur lequel le tunnel VPN est établi.

• Configuration de la passerelle en tant que client VPN à l'aide de PPTP

. 1. Allez dans Settings>VPN et cliquez sur + Create New VPN Policy pour charger la page suivante.



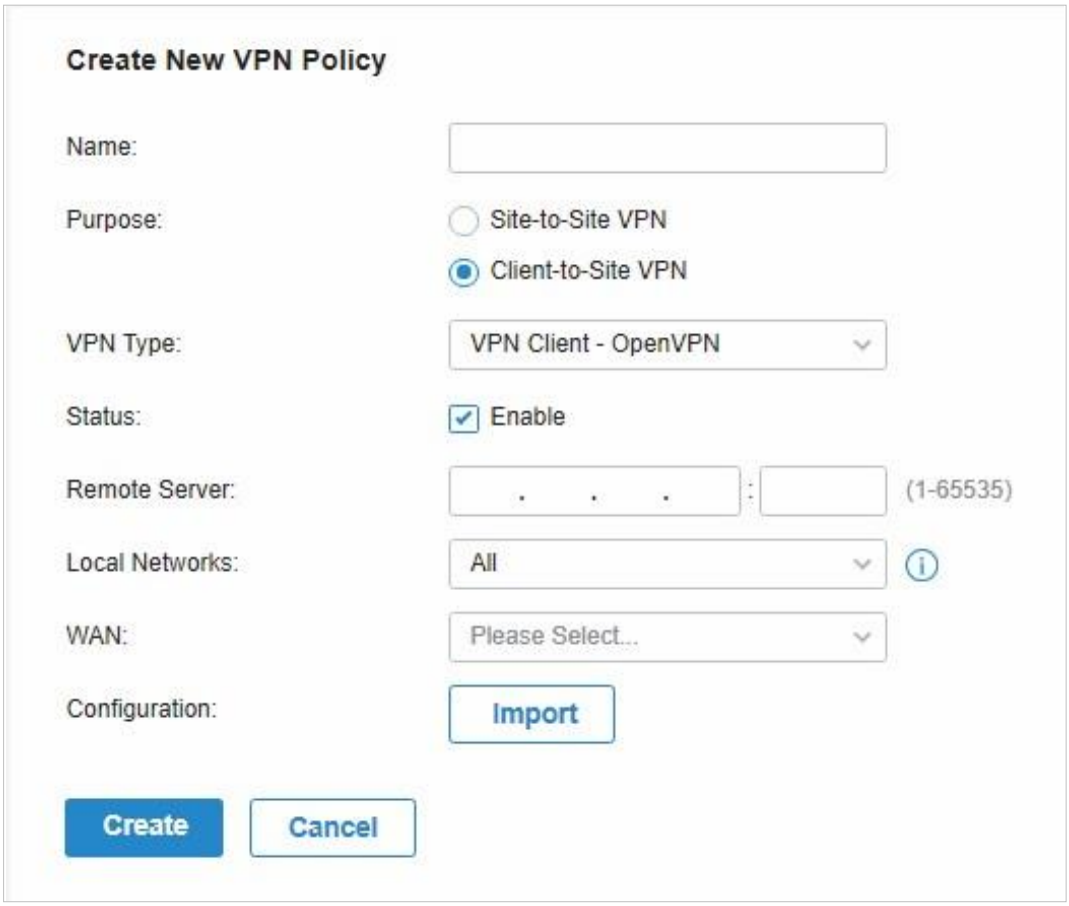
2. Entrez un nom pour identifier la stratégie VPN et sélectionnez l'objet en tant que VPN de client à site. Reportez-vous au tableau suivant pour configurer les paramètres requis, puis cliquez sur Create.

Name	Entrez un nom pour identifier la stratégie VPN.
Purpose	Sélectionnez l'objet du VPN Client-to-Site VPN.
VPN Type	Sélectionnez le type VPN comme VPN Client - PPTP.
Status	Cliquez sur la case à cocher pour activer la stratégie VPN.

Working Mode	Spécifier le mode de travail en tant que NAT ou Routage. NAT: Avec le mode NAT (Traduction d'adresses réseau) sélectionné, le client PPTP utilise l'adresse IP assignée comme adresses source de l'en-tête IP d'origine lors de l'transfert des paquets PPTP. Routing: Avec routage sélectionné, le client PPTP utilise sa propre adresse IP comme adresses sources de l'en-tête IP d'origine lors de la transfert de paquets PPTP.
Username	Entrez le nom d'utilisateur utilisé pour le tunnel VPN. Ce nom d'utilisateur doit être le même que celui du serveur PPTP.
Password	Entrez le mot de passe de l'utilisateur. Ce mot de passe doit être le même que celui du serveur PPTP.
MPPE Encryption	Spécifier s'il faut activer le chiffrement du tunnel. Encrypted: Sélectionnez Crypté pour chiffrer le tunnel PPTP par MPPE. Unencrypted: Avec un non chiffré sélectionné, le tunnel PPTP ne sera pas crypté par MPPE.
Remote Server	Entrez l'adresse IP ou le nom de domaine du serveur PPTP.
Remote Subnets	Entrez l'adresse IP et le masque de sous-réseau pour spécifier le réseau distant. C'est toujours la plage d'adresses IP de LAN sur le pair distant du tunnel VPN.
Local Networks	Sélectionnez les réseaux du côté local du tunnel VPN. La stratégie VPN ne s'appliquera qu'aux réseaux locaux sélectionnés.
WAN	Sélectionnez le port WAN sur lequel le tunnel VPN est établi.

• Configuration de la passerelle en tant que client VPN à l'aide d'OpenVPN

1. Allez dans Settings>VPN et cliquez sur + Create New VPN Policy pour charger la page suivante.



2. Entrez un nom pour identifier la stratégie VPN et sélectionnez l'objet en tant que VPN de client à site. Reportez-vous au tableau suivant pour configurer les paramètres requis, puis cliquez sur Create.

Name	Entrez un nom pour identifier la stratégie VPN.
Purpose	Sélectionnez l'objet du VPN Client-to-Site VPN.
VPN Type	Sélectionnez le type VPN comme VPN Client - OpenVPN.
Status	Cliquez sur la case à cocher pour activer la stratégie VPN.
Remote Server	Entrez l'adresse IP ou le nom de domaine du serveur OpenVPN.
Local Networks	Sélectionnez les réseaux du côté local du tunnel VPN. La stratégie VPN ne s'appliquera qu'aux réseaux locaux sélectionnés.
WAN	Sélectionnez le port WAN sur lequel le tunnel VPN est établi.

Configuration	Cliquez sur Import pour importer le fichier OpenVPN qui se termine dans .ovpn généré par le serveur OpenVPN. Un seul fichier peut être importé. Si le fichier de certificat et le fichier de configuration sont générés serveur OpenVPN, combinez deux fichiers et importez l'ensemble du fichier.

4. 8 Créer des profils

La section Profils est utilisée pour configurer et enregistrer vos paramètres personnalisés pour les configurations de site. Il inclut les profils Time Range et Groups. Dans la section Plage de temps, vous pouvez configurer des modèles de temps pour la planification sans fil, la planification poE, etc. Dans la section Groupes, vous pouvez configurer des groupes en fonction d'adresses IP, IP-Port et MAC pour ACL, Routage, NAT, etc. Après avoir créé les profils, vous pouvez les appliquer pour multiplier les configurations pour différents sites, vous permettant de vous empêcher de configurer à plusieurs reprises les mêmes informations.

4. 8. 1 plage de temps

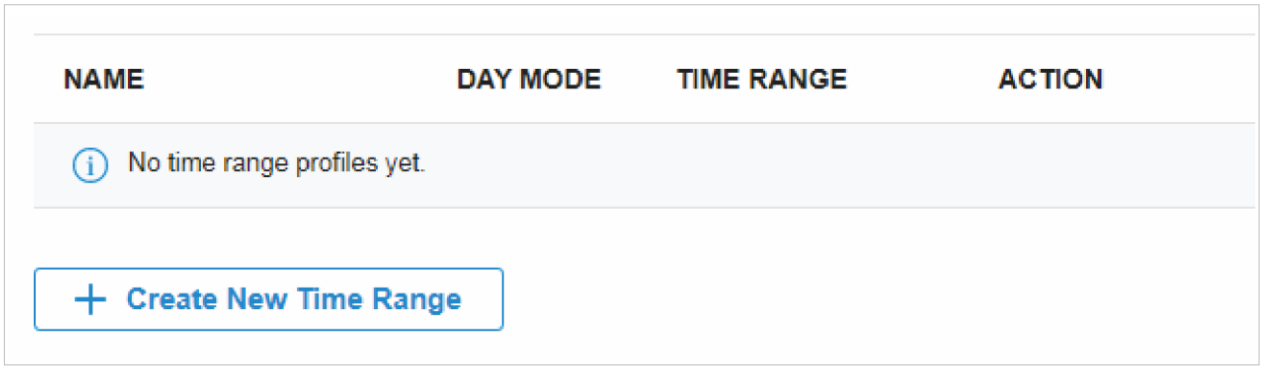
Aperçu

La section Plage de temps vous permet de personnaliser les configurations liées au temps. Vous pouvez définir différents modèles de plage de temps qui peuvent être partagés et appliqués à la planification sans fil, à la planification PoE, etc. dans la configuration du site.

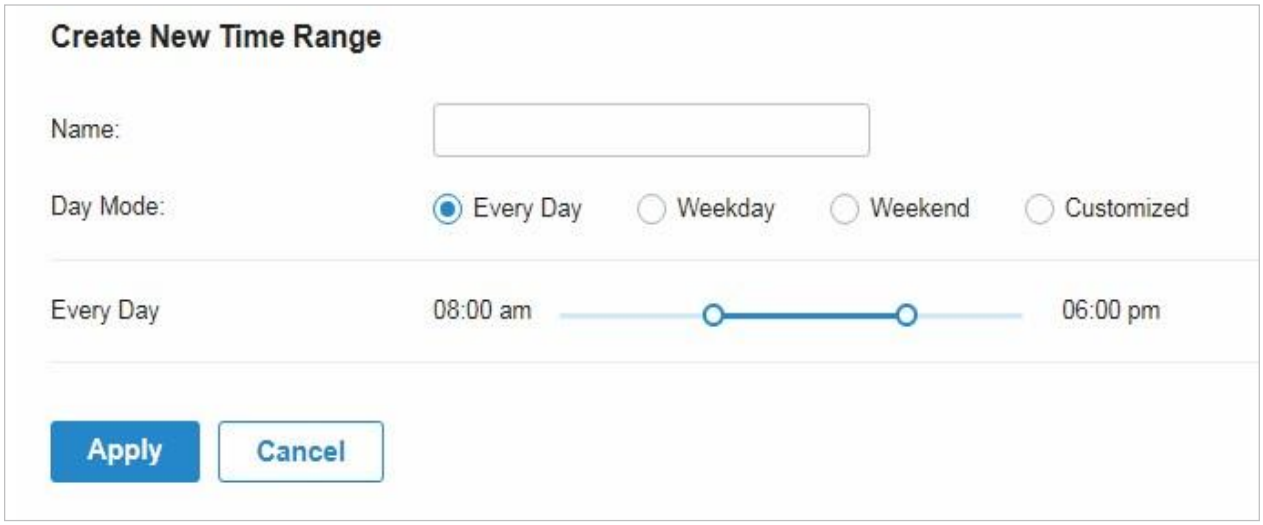
Configuration

Pour configurer les profils de plage de temps, procédez comme suit:

1. Allez dans Settings > Profiles >Time Range. Cliquez sur +Create New Time Range pour ajouter une nouvelle entrée de plage de temps. Par défaut, il n'y a pas d'entrée dans la liste.

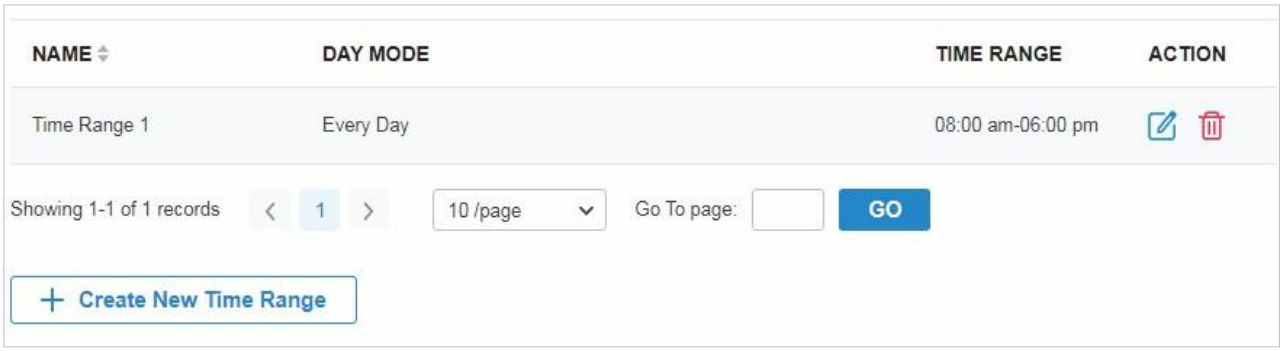


1. Entrez un nom pour la nouvelle entrée, sélectionnez le mode jour et spécifiez la plage d'heure. Cliquez sur Appliquer pour enregistrer l'entrée. Après avoir enregistré l'entrée nouvellement ajoutée, vous pouvez les appliquer à la configuration du site. Pour appliquer les profils de plage de temps personnalisés en configuration, WLAN Schedule, et PoE Schedule.



Name	Entrez un nom pour la nouvelle entrée, et il s'agit d'une chaîne avec 1 à 64 symboles ASCII.
Day Mode	Sélectionnez Every Day, Weekday, Weekend, ou Customized d'abord avant de spécifier la plage d'heure pour chaque jour. Every Day: Vous n'avez besoin de définir la plage de temps qu'une seule fois, et il se répétera tous les jours. Weekday: Vous n'avez besoin de définir la plage d'heure qu'une seule fois, et il se répétera tous les jours de la semaine du lundi au vendredi. Weekend: Vous n'avez besoin de définir la plage d'heure qu'une seule fois, et il se répétera tous les samedis et dimanches. Customized: Vous êtes en mesure de définir une plage d'horaires différente pour le(s) jour(s) choisi(s) en fonction de vos besoins. Lorsqu'un jour n'est pas choisi, le Wi-Fi est ouvert toute la journée par défaut.

Vous pouvez afficher le nom, le mode de jour et la plage d'heure dans la liste.



Pour modifier ou supprimer l'entrée de plage d'heure, cliquez sur l'icône de la colonne Action.

	Modifiez les paramètres de l'entrée.
	Supprimer l'entrée .

4. 8. 2 Groupes

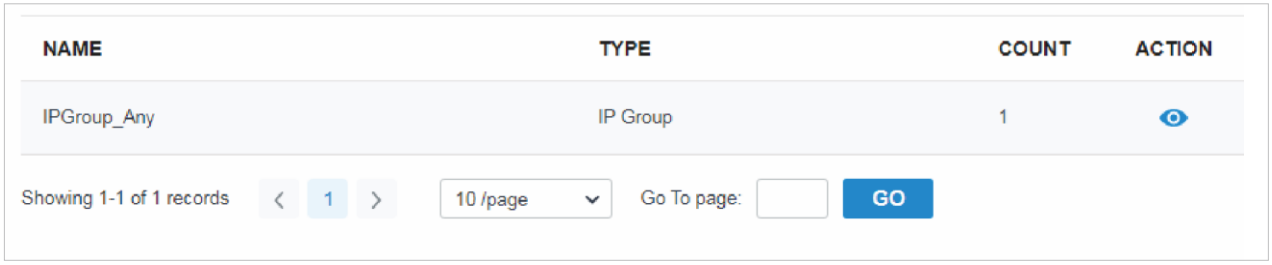
Aperçu

La section Groupes vous permet de personnaliser les groupes de clients en fonction de l'adresse IP, IP-Port ou MAC. Vous pouvez définir différentes règles pour les profils de groupes qui peuvent être partagés et appliqués à ACL, Routage, NAT, etc. dans la configuration du site.

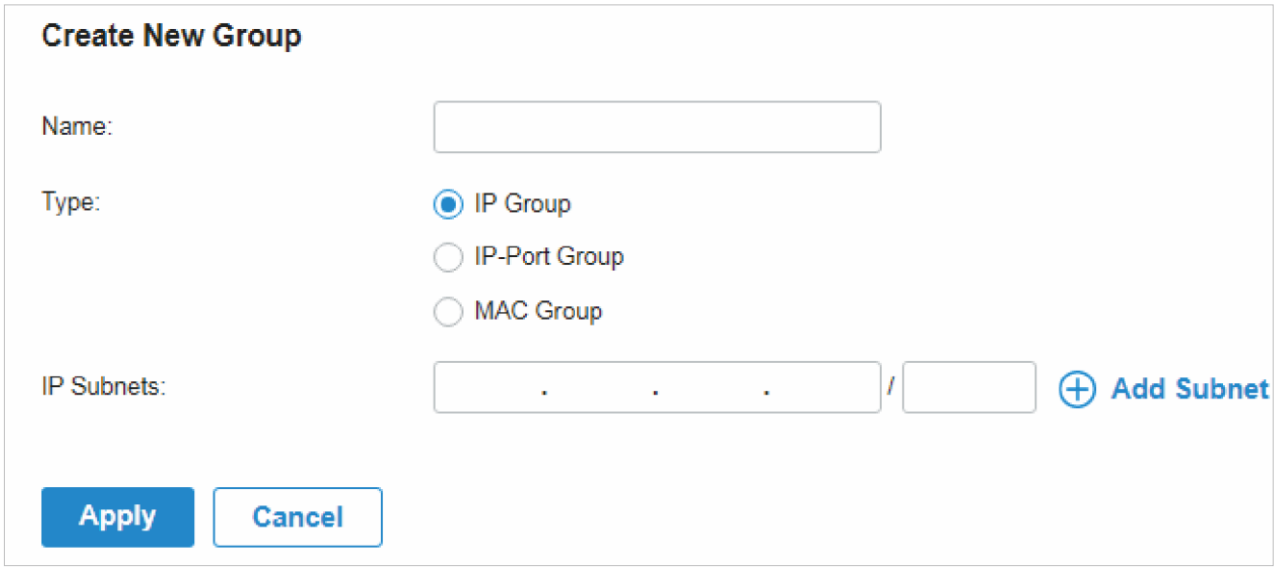
Configuration

Pour configurer les profils de groupe, procédez comme suit :

1. Allez dans Settings > Profiles > Groups. Par défaut, il y a une entrée couvrant tous les IP, et elle n'est pas modifiable. Cliquez sur +Add Subnet pour ajouter une nouvelle entrée de groupe.



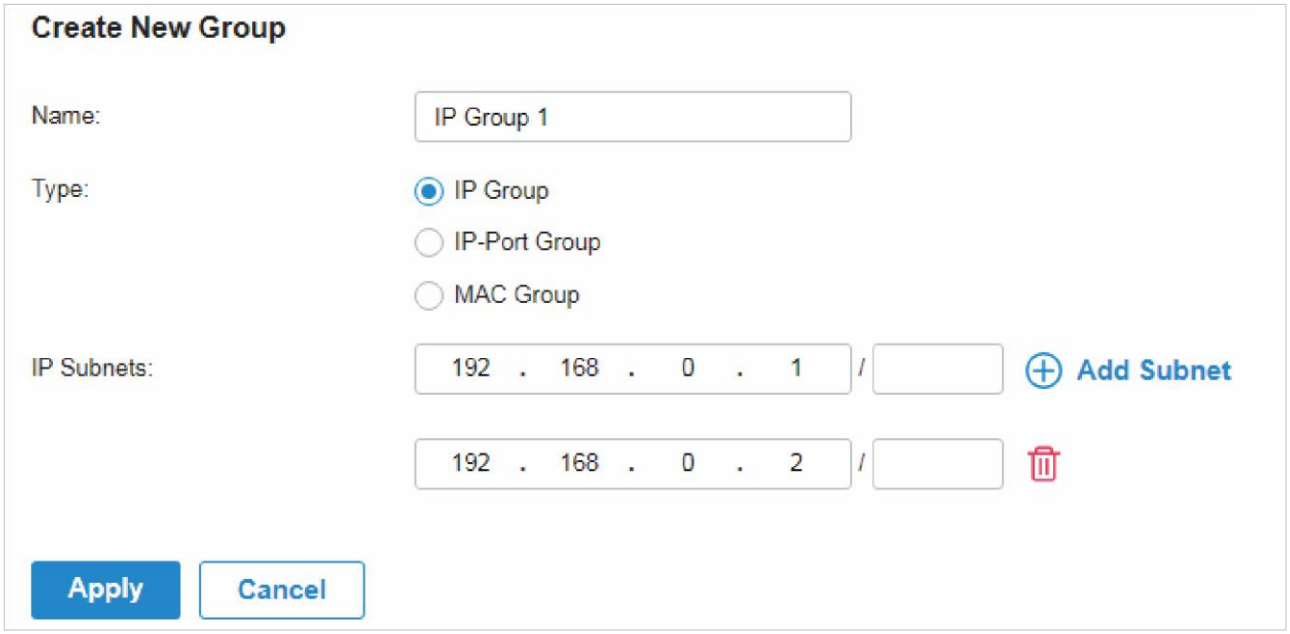
2. Entrez un nom pour la nouvelle entrée de profil de groupe, puis sélectionnez le type de la nouvelle entrée.



- **Based on IP Group**

  Pour configurer un profil de groupe basé sur IP Group, vous devez spécifier les sous-réseaux IP, masque de sous-réseau est facultatif. Vous pouvez cliquer sur +Ajouter un sous-réseau pour ajouter de nouveaux sous-réseaux, puis cliquez sur

pour les supprimer

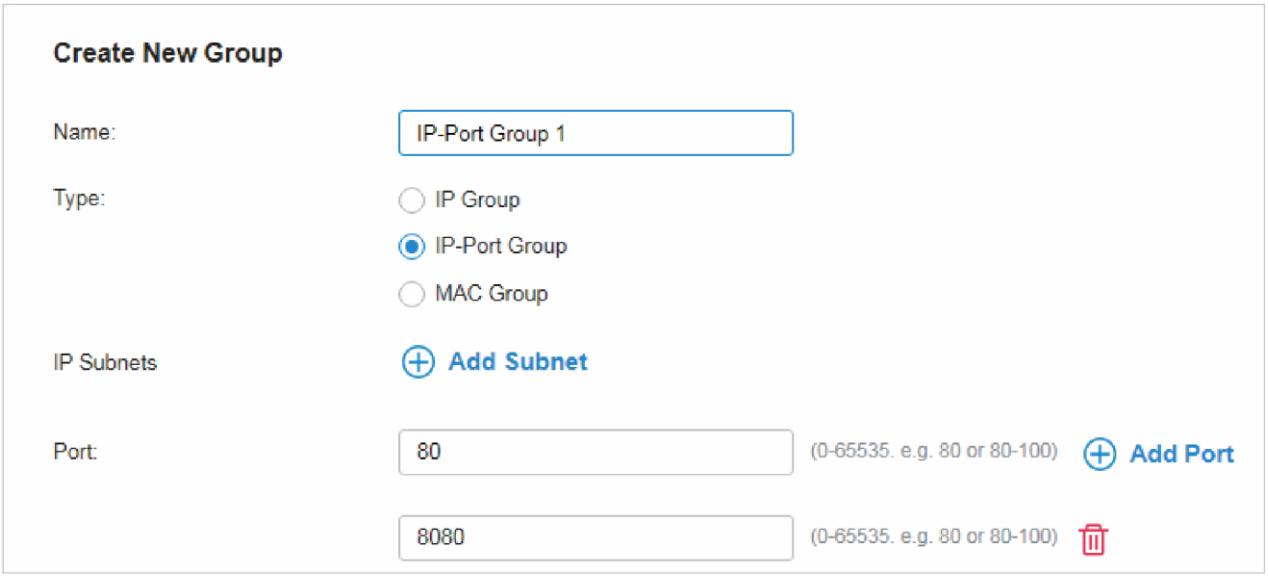


- **Based on IP-Port Group**

Pour configurer un profil de groupe basé sur ip-port Group, vous devez spécifier le ou les ports pour l'entrée, alors qu'il est facultatif de spécifier le sous-réseau IP.s. Si vous spécifiez uniquement le ou les ports sans entrer de sous-réseau IP, cela signifie que le groupe contient les ports spécifiés pour tous les adresses IP. Vous pouvez cliquer sur +Add

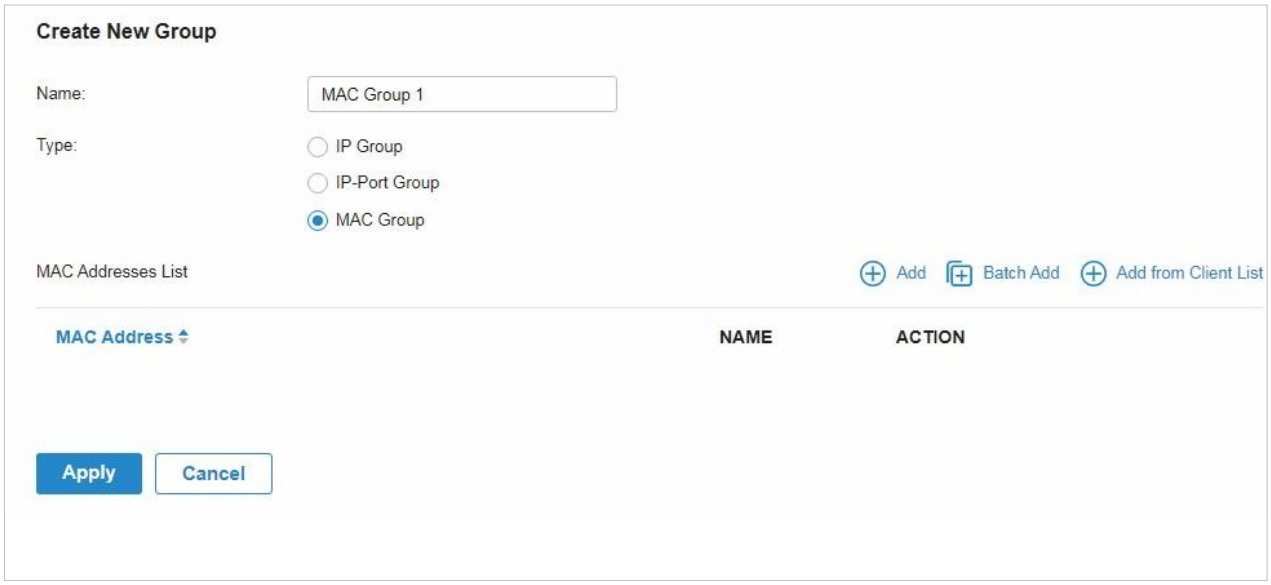
Pour ajouter de nouveaux sous-réseau IP cliquez sur Subnet

et pour ajouter des ports, puis cliquez sur + Add Port pour les supprimer.



- **Based on MAC Group**

Pour configurer un profil de groupe basé sur MAC Group, vous devez entrer les adresses MAC(es) dans la liste des adresses MAC. Il existe trois façons d'ajouter l'adresse(es) mac à la liste des adresses MAC.



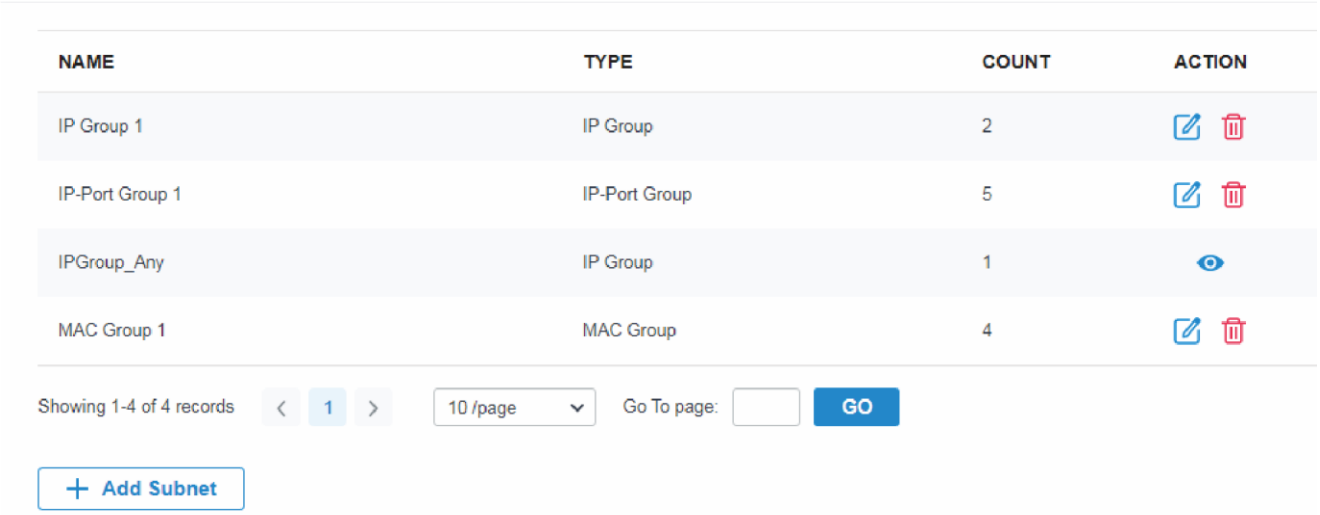
Add	Ajouter l'adresse Mac
Batch Add	Ajoutez des adresses MAC par lots. Vous pouvez entrer les adresses et les noms MAC dans la zone d'entrée ou les importer avec des fichiers au format Excel, txt et texte. Si vous souhaitez utiliser les adresses MAC(es) nouvellement ajoutées et les noms lorsqu'ils entrent en conflit avec les adresses existantes, cliquez sur site pour lui permettre de remplacer la liste de contrôle d'accès MAC curant.
Add from Client List	Ajouter des adresses MAC des clients connectés aux périphériques contrôlés par le Contrôleur Omada SDN.

Note:

1. Chaque adresse et nom MAC doivent être entrés sur une nouvelle ligne. L'adresse et le nom mac doivent être séparés par un espace.
2. Les octets d'une adresse MAC doivent être séparés par un trait d'union. Par exemple, AA-BB-CC-DDEE-FF.

1.Cliquez sur Appliquer pour enregistrer l'entrée.

Après avoir enregistré l'entrée nouvellement ajoutée, vous pouvez les appliquer à la configuration du site. Pour appliquer les profils personnalisés en configuration, reportez-vous à ACL, Routing, NAT.
Vous pouvez afficher le nom, le type et le compte dans la liste.



Pour afficher, modifier ou supprimer l'entrée de groupe, cliquez sur l'icône de la colonne Action.

	Afficher et modifier les paramètres de l'entrée. Vous ne pouvez pas modifier le type lors de l'édition de l'entrée.
	Supprimez l'entrée.

4. 9 Authentification

L'authentification est un portefeuille de fonctionnalités conçues pour autoriser l'accès réseau aux clients, ce qui améliore la sécurité du réseau. Les services d'authentification incluent Portal, 802.1X et MAC-Based Authentication, couvrant tous les besoins pour authentifier les clients filaires et sans fil.

4. 9. 1 Portail

Aperçu

L'authentification du portail fournit des services d'authentification pratiques aux clients qui n'ont besoin que d'un accès temporaire au réseau, tels que les clients dans un restaurant ou dans un supermarché. Pour accéder au réseau, ces clients doivent entrer la page de connexion d'authentification et utiliser les informations de connexion correctes pour passer l'authentification. En outre, vous pouvez personnaliser la page de connexion d'authentification et spécifier une URL vers laquelle les clients authentifiés seront redirigés.

L'authentification du portail peut fonctionner avec la stratégie de pré authentification et d'authentification, qui accorde un accès réseau spécifique aux utilisateurs ayant des identités valides. Les stratégies de pré-authentification permettent aux clients non authentifiés d'accéder aux ressources réseau spécifiques. Les stratégies sans authentification permettent aux clients spécifiques d'accéder aux ressources réseau spécifiques sans authentification.

L'authentification de portail prend effet sur les SSID et les réseaux LAN. Les EAP authentifient les clients sans fil qui se connectent au SSID avec le portail configuré, et la passerelle authentifie les clients câblés qui se connectent au réseau avec portal configuré. Pour rendre l'authentification portal disponible pour les clients câblés et sans fil, assurez-vous que la passerelle et les EAPs sont connectés et fonctionnent correctement.

Le contrôleur fournit six types d'authentification pour le Portail:

- **No Authentication**

  Avec ce type d'authentification configuré, les clients peuvent passer l'authentification et accéder au réseau sans fournir d'informations de connexion. Les clients n'ont qu'à accepter les conditions (si elles sont configurées) et cliquez sur le bouton Connexion.

- **Simple Password**

  Avec ce type d'authentification configuré, les clients sont tenus d'entrer le mot de passe correct pour passer l'authentification. Tous les clients utilisent le même mot de passe configuré dans le contrôleur.

- **Hotspot**

  Avec ce type d'authentification configuré, les clients peuvent accéder au réseau après avoir passé n'importe quel type de l'authentification :

  - **Voucher**

  Les clients peuvent utiliser les codes de bons uniques générés par le contrôleur dans un délai prédéfini. Les codes de bons peuvent être imprimés à partir du contrôleur, de sorte que vous pouvez imprimer les codes et les distribuer à vos clients pour lier l'accès du réseau à la consommation.

- **Local User**

  Les clients sont tenus d'entrer le nom d'utilisateur et le mot de passe corrects du compte de connexion pour passer l'authentification.

- **SMS**

  Les clients peuvent obtenir des codes de vérification à l'aide de leurs téléphones mobiles et entrer les codes reçus pour passer l'authentification.

- **RADIUS**

  Les clients sont tenus d'entrer le nom d'utilisateur et le mot de passe corrects qui sont stockés dans le serveur RADIUS pour passer l'authentification.

■ **External RADIUS Server**

Les clients sont tenus d'entrer le nom d'utilisateur et le mot de passe corrects créés sur le serveur RADIUS pour passer l'authentification.

■ **External Portal Server**

L'option External Portal Server est conçue pour les développeurs. Ils peuvent personnaliser leur propre type d'authentification comme l'authentification de compte Google en fonction de l'interface fournie par Omada Controller.

■ **Facebook**

Avec facebook portal configuré, lorsque les clients se connectent à votre Wi-Fi, ils seront redirigés vers votre page Facebook. Pour accéder à Internet, les clients doivent se connecter à leur compte ou entrer le code de mot de passe dans la page Facebook.

Configuration

Pour terminer la configuration du portail, procédez comme suit :

1.) Cliquez pour activer Portal.

2.) Sélectionnez les SSID et les réseaux LAN pour que le portail prenne effet et configure les paramètres de base, y compris le type d'authentification, le délai d'expiration d'authentification, et ainsi de suite.

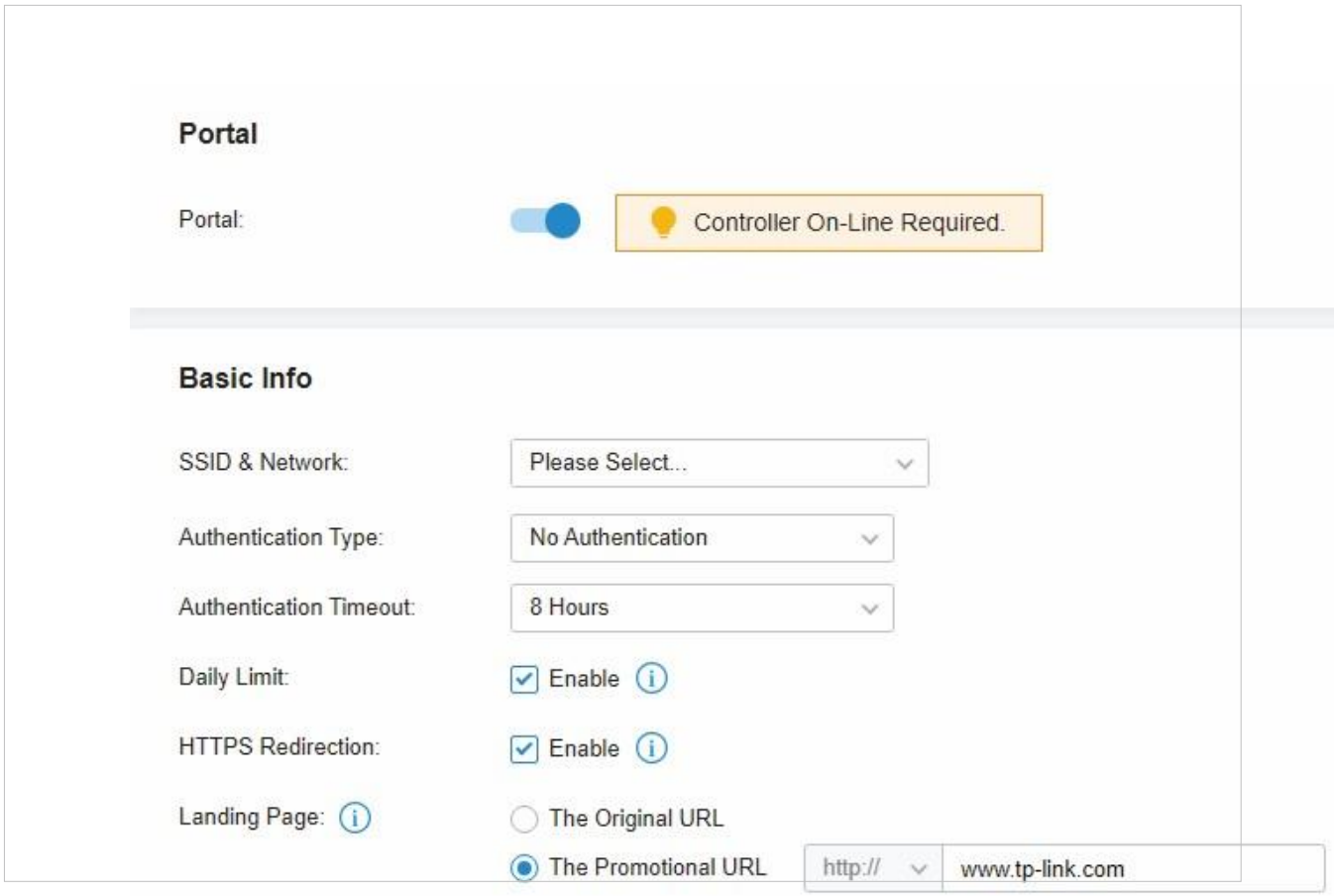
3.) Personnaliser la page Portail, y compris l'image d'arrière-plan, l'image du logo et ainsi de suite.

4.) Configurez les règles de contrôle d'accès, y compris l'accès pré-authentification et la stratégie sans authentification si nécessaire.

La partie suivante présente comment configurer chaque type d'authentification portal: No Authentication, Simple Password, Hotspot (Voucher, Local User, SMS, RADIUS), External RADIUS Server, External Portal Server et Facebook.

■ Configuration du portail sans authentification

1. Allez dans Settings > Authentication > Portal . Cliquez sur pour activer portal et. charger la page suivante

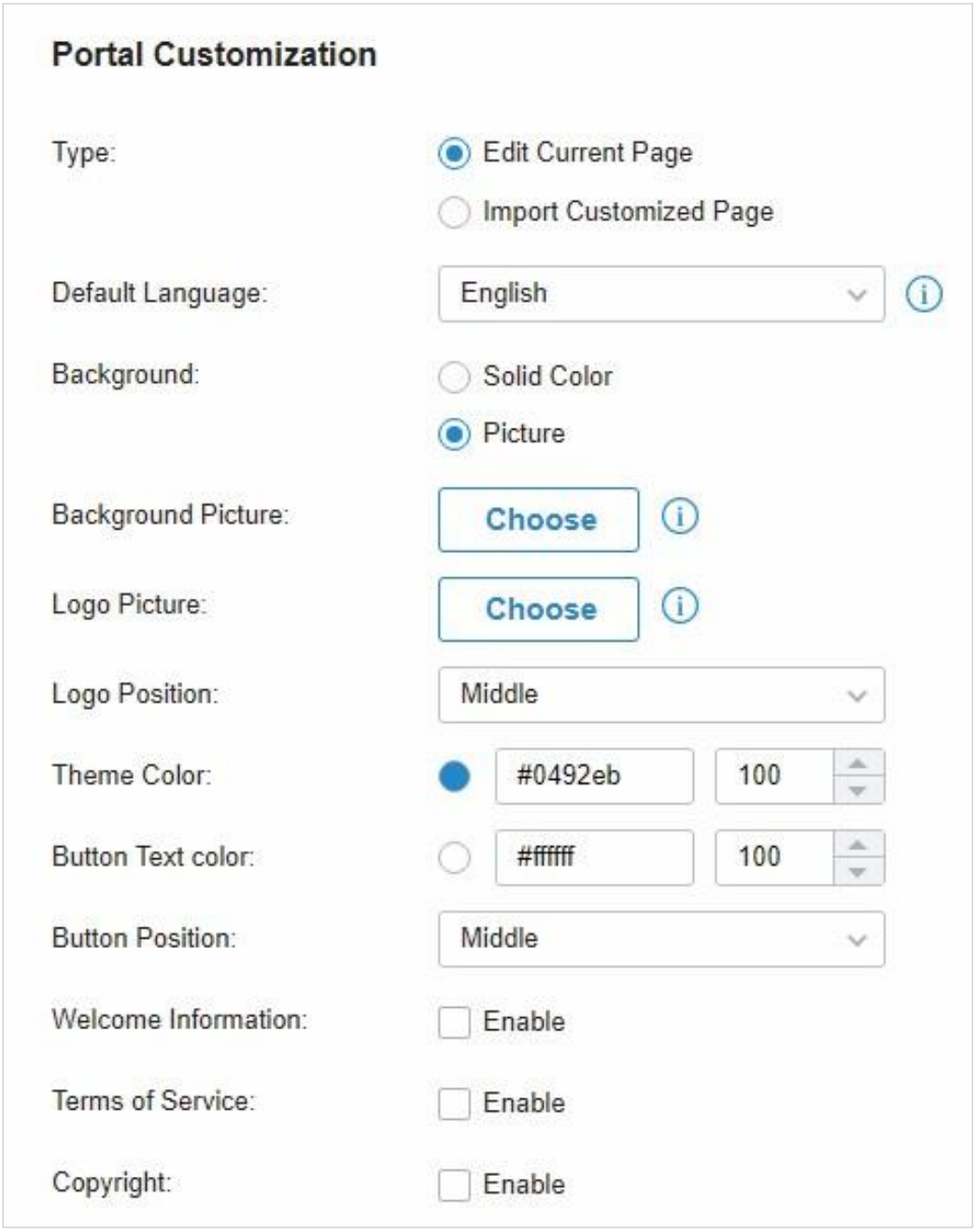


2. Sélectionnez les SSID et les réseaux LAN pour que le portail prenne effet et configure les paramètres de base, y compris le type d'authentification, le délai d'expiration d'authentification, et ainsi de suite.

SSID & LAN Network	Sélectionnez un ou plusieurs SSID ou réseaux LAN pour le portail. Les clients connectés aux SSID sélectionnés ou aux réseaux LAN doivent se connecter à une page Web pour établir la vérification avant d'accéder au réseau.
Authentication Type	Sélectionnez le type d'authentification portal comme aucune authentification.
Authentication Timeout	Sélectionnez la durée de connexion. Les clients seront hors ligne après le délai d'expiration d'authentification.

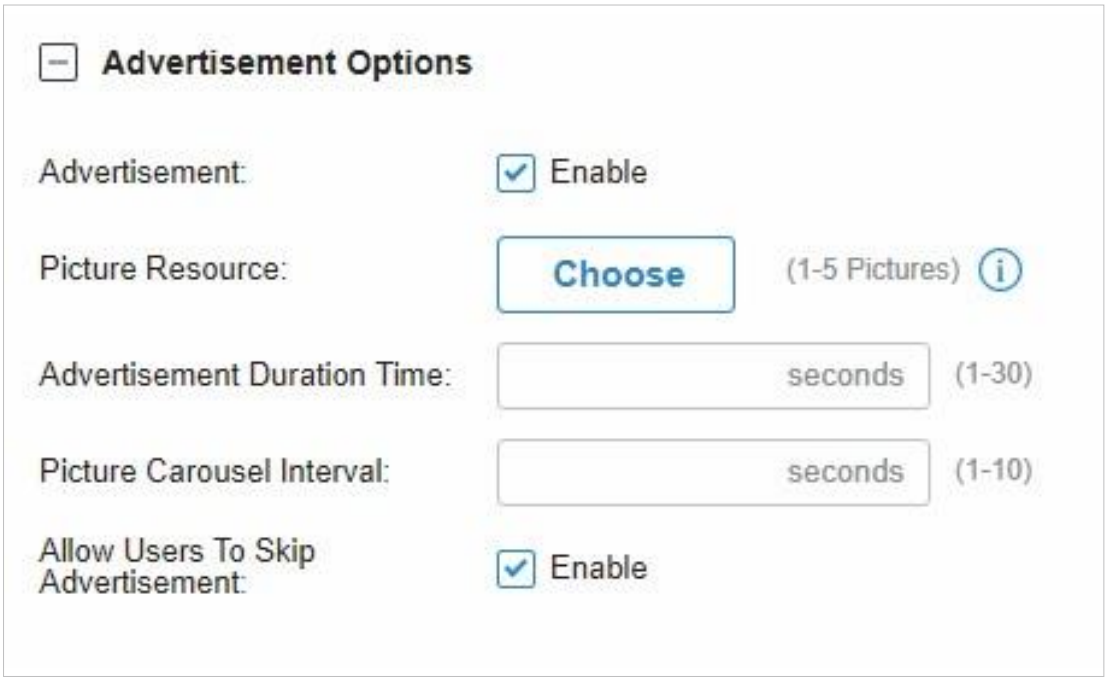
Daily Limit	Cliquez sur la case à cocher pour activer la limite quotidienne. Avec cette fonctionnalité activée, après la sortie de l'authentification, les clients ne peuvent pas s'authentifiés à nouveau avant le lendemain. Avec cette fonctionnalité désactivée, après la sortie de l'authentification, les clients peuvent se faire authentifier à nouveau sans limite.
HTTPS Redirection	Cliquez sur la case à cocher pour activer la redirection HTTPS. Avec cette fonctionnalité activée, les clients non autorisés seront redirigés vers la page Portail lorsqu'ils tentent de parcourir les sites Web HTTPS. Cette fonctionnalité ayant été désactivée, les clients non autorisés ne peuvent pas parcourir les sites Web HTTPS et ne sont pas redirigés vers la page Portail.
Landing Page	Sélectionnez la page vers laquelle le client sera redirigé après une authentification réussie. Avoir passé l'authentification portal. The Promotional URL: Les clients sont dirigés vers l'URL spécifiée après avoir passé l'authentification portal. The Original URL: Les clients sont dirigés vers l'URL qu'ils demandent après

3. Dans la section Personnalisation du portail, personnaliser la page Portail comprenant l'image d'arrière-plan, l'image du logo et ainsi de suite.



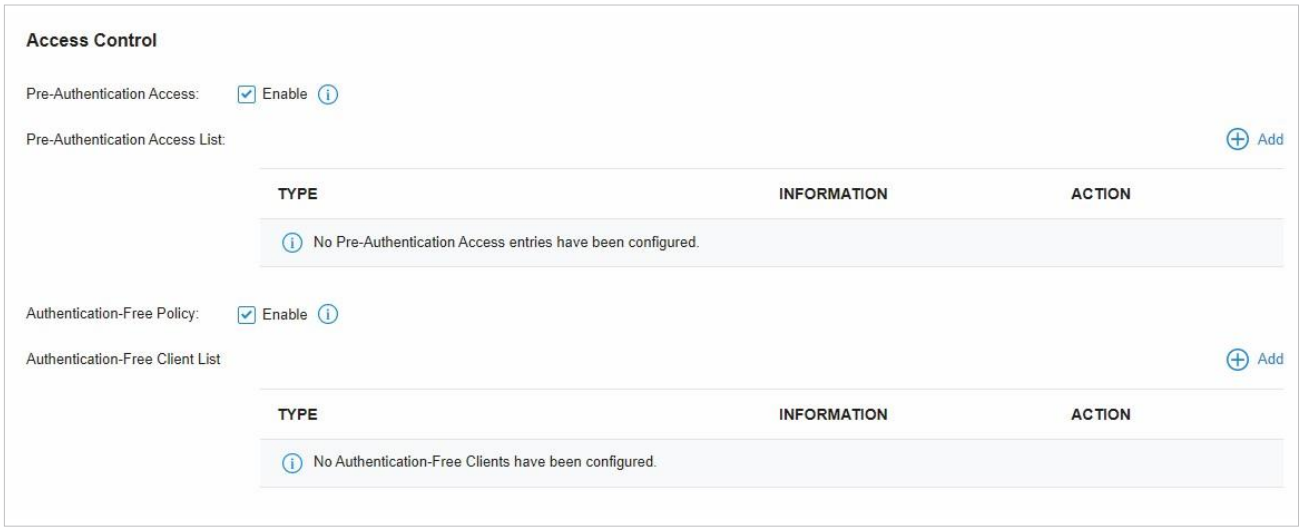
Type	Sélectionnez le type de la page Portail. Edit Current Page: Modifiez les paramètres connexes pour personnaliser la page Portail en fonction de la page fournie. Import Customized Page: Cliquez sur Import pour importer votre page portail unique pour la marquer selon votre entreprise.
Default Language	Sélectionnez la langue par défaut affichée dans la page Portail. Le contrôleur ajuste automatiquement la langue affichée sur la page Portail en fonction de la langue système des clients. Si la langue n'est pas prise en charge, le contrôleur utilisera la langue par défaut spécifiée ici.
Background	Select the background type. Solid Color: Configurez la couleur d'arrière-plan souhaitée en entrant manuellement le code de couleur HTML hexadécimal ou par l'intermédiaire du sélecteur de couleurs. Picture: Cliquez sur Choose et sélectionnez une image de votre PC en arrière-plan.
Logo Picture	Cliquez sur Choose et sélectionnez une image de votre PC comme logo.
Logo Position	Sélectionnez la position du logo dans la page Portail.
Theme Color	Configurez la couleur d'arrière-plan souhaitée pour le bouton en entrant manuellement le code de couleur HTML hexadécimal ou par l'intermédiaire du sélecteur de couleurs.
Button Text Color	Configurez la couleur de texte souhaitée pour le bouton en entrant manuellement le code de couleur HTML hexadécimal ou par l'intermédiaire du sélecteur de couleurs.
Button Position	Sélectionnez la position du bouton dans la page Portail.
Welcome Information	Cliquez sur la case à cocher et entrez le texte comme informations de bienvenue. Et vous pouvez configurer la couleur de texte souhaitée pour les informations de bienvenue en entrant manuellement le code de couleur HTML hexadécimal ou par l'intermédiaire du sélecteur de couleurs.
Terms of Service	Cliquez sur la case à cocher et entrez le texte comme conditions de service dans la zone suivante.
Copyright	Cliquez sur la case à cocher et entrez le texte comme droit d'auteur dans la zone suivante.

Cliquez sur Options de publicité et personnaliser les images publicitaires sur la page d'authentification.



Advertisement	Cliquez sur la case à cocher pour activer la fonctionnalité Publicité. Avec cette fonctionnalité activée, vous pouvez ajouter des images publicitaires sur la page d'authentification. Ces photos publicitaires s'afficheront avant l'apparition de la page de connexion.
Picture Resource	Cliquez sur Choose et sélectionnez des photos de votre PC comme images publicitaires. Lorsque plusieurs images sont ajoutées, elles seront jouées en boucle.
Advertisement Duration Time	Entrez l'heure de durée pour les images publicitaires. Pour cette durée, les images seront jouées en boucle. Si le temps de durée n'est pas suffisant pour toutes les photos, le reste ne sera pas affiché.
Picture Carousel Interval	Entrez l'intervalle carrousel d'images. Par exemple, si cette valeur est définie comme 5 secondes, la première image s'affiche pendant 5 secondes, suivie de la deuxième image pendant 5 secondes, et ainsi de suite.
Allow Users To Skip Advertisement	Cliquez sur la case à cocher pour permettre aux utilisateurs d'ignorer la publicité.

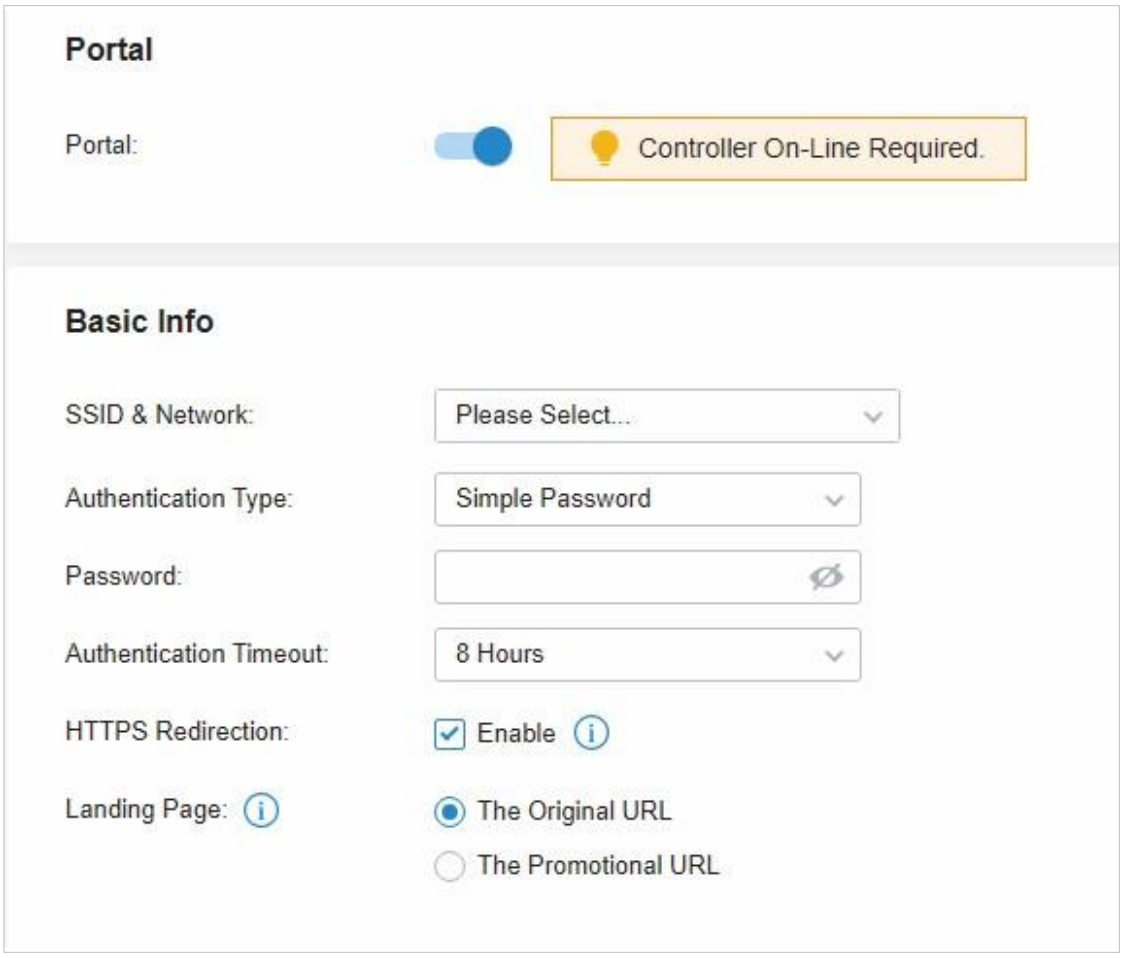
4. Dans la section Contrôle d'accès, configurez les règles de contrôle d'accès, y compris l'accès pré-authentification et la stratégie sans authentification si nécessaire.



Pre-Authentication Access	Cliquez sur la case à cocher pour activer l'accès pré-authentification. Grâce à cette fonctionnalité activée, les clients non authentifiés sont autorisés à accéder aux sous-réseaux et aux ressources Web spécifiés dans la liste d'accès pré-authentification ci-dessous.
Pre-Authentication Access List	Cliquez sur Add pour configurer la plage IP ou l'URL à laquelle les clients non authentifiés sont autorisés à accéder.
Authentication-Free Policy	Cliquez sur la case à cocher pour activer la stratégie sans authentification. Avec cette fonctionnalité activée, vous pouvez permettre à certains clients d'accéder à Internet sans authentification Portal.
Authentication-Free Client List	Cliquez sur Add et entrez l'adresse IP ou l'adresse MAC des clients sans authentification.

■ Configuration du portail avec mot de passe simple

1. Allez dans Settings > Authentication > Portal. cliquez sur pour activer portal et charger la page su

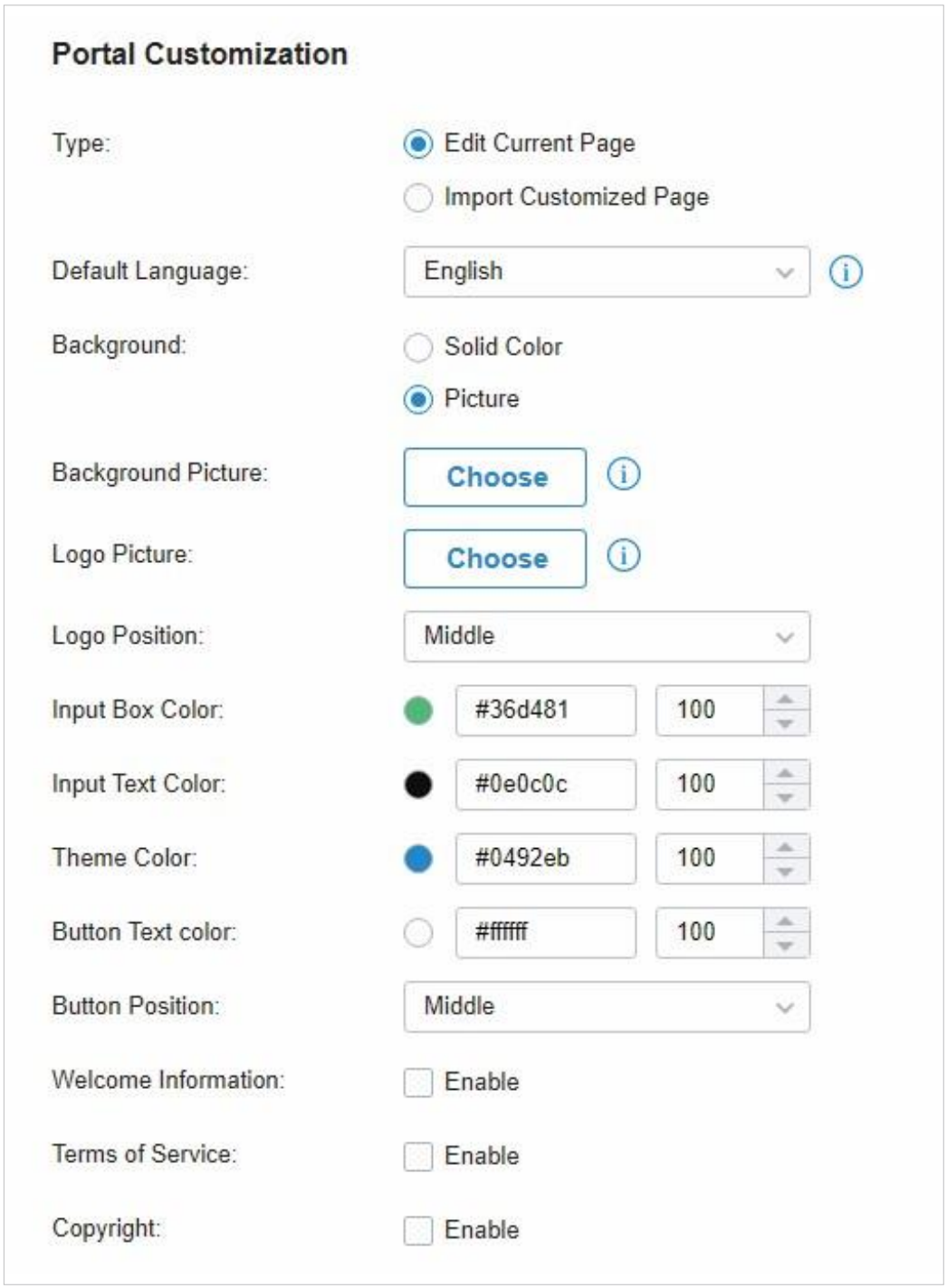


2. Sélectionnez les SSID et les réseaux LAN pour que le portail prenne effet et configure les paramètres de base, y compris le type d'authentification, le délai d'expiration d'authentification, et ainsi de suite.

SSID & LAN Network	Sélectionnez un ou plusieurs SSID ou réseaux LAN pour le portail. Les clients connectés aux SSID sélectionnés ou aux réseaux LAN doivent se connecter à une page Web pour établir la vérification avant d'accéder au réseau.
Authentication Type	Sélectionnez le type d'authentification portal comme mot de passe simple.
Authentication Timeout	Sélectionnez la durée de connexion. Les clients seront hors ligne après le délai d'expiration d'authentification.
HTTPS Redirection	Cliquez sur la case à cocher pour activer la redirection HTTPS. Avec cette fonctionnalité activée, les clients non autorisés seront redirigés vers la page Portail lorsqu'ils tentent de parcourir les sites Web HTTPS. Cette fonctionnalité ayant été désactivée, les clients non autorisés ne peuvent pas parcourir les sites Web HTTPS et ne sont pas redirigés vers la page Portail.

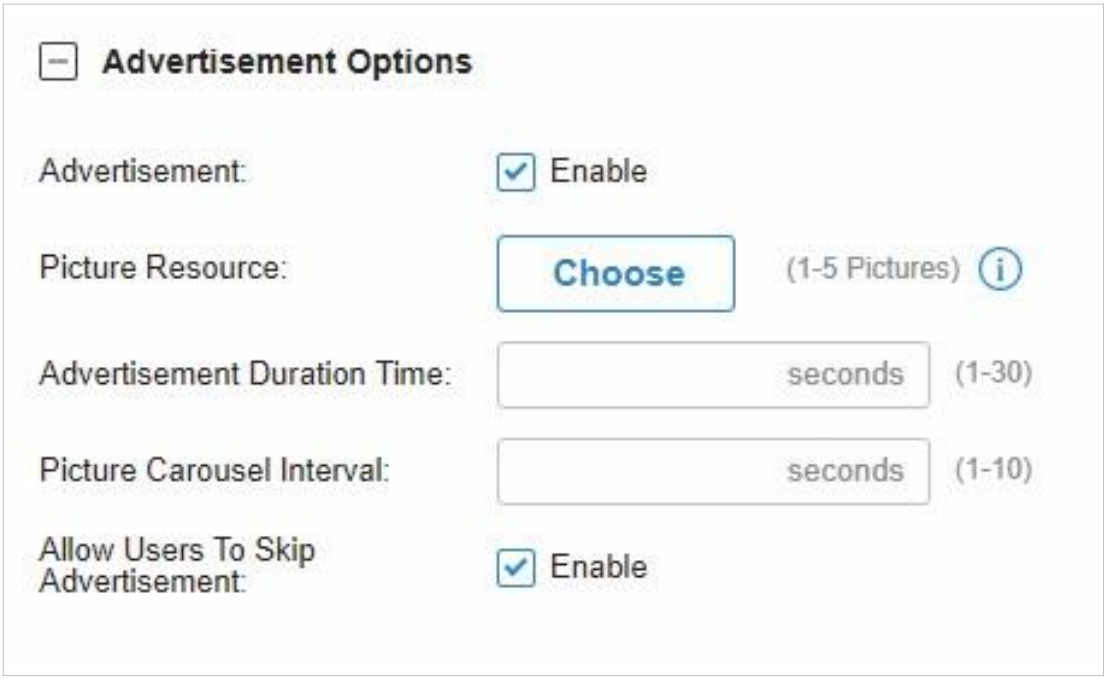
Landing Page	Sélectionnez la page vers laquelle le client sera redirigé après une authentification réussie. The Original URL: Les clients sont dirigés vers l'URL qu'ils demandent après avoir passé l'authentification portal. The Promotional URL: Les clients sont dirigés vers l'URL spécifiée ici après avoir passé l'authentification portal.

1. Dans la section Personnalisation du portail, personnalisez la page Portail comprenant l'image d'arrière-plan, l'image du logo et ainsi de suite.



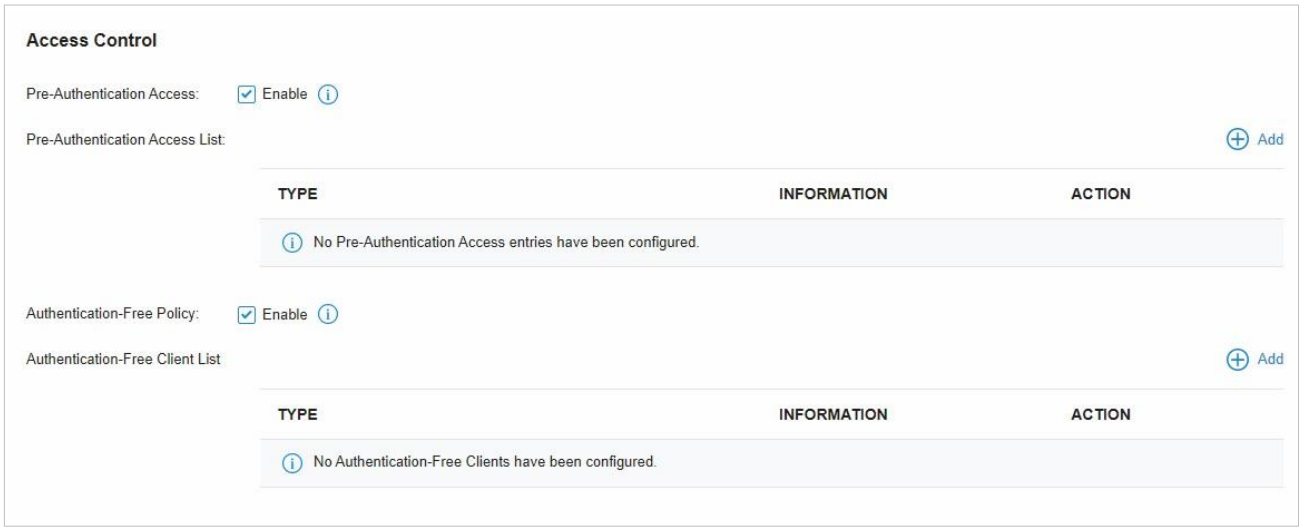
Default Language	Sélectionnez la langue par défaut affichée dans la page Portail. Le contrôleur ajuste automatiquement la langue affichée sur la page Portail en fonction de la langue système des clients. Si la langue n'est pas prise en charge, le contrôleur utilisera la langue par défaut spécifiée ici.
Type	Sélectionnez le type de la page Portail Edit Current Page: Modifiez les paramètres connexes pour personnaliser la page du portail en fonction de la page fournie Import Customized Page: cliquez sur Import pour importer votre page portail unique pour l'image de marque selon votre entreprise
Background	Sélectionner le type d'arrière-plan. Solid Color: Configurez la couleur d'arrière-plan souhaitée en entrant manuellement le code de couleur HTML hexadécimal ou par l'intermédiaire du sélecteur de couleurs. Picture : Cliquez Choose et sélectionnez une image de votre PC en arrière-plan .
Logo Picture	Cliquez Choose et sélectionnez une image de votre PC comme logo.
Logo Position	Sélectionnez la position du logo dans la page Portail.
Input Box Color	Configurez la couleur souhaitée de la zone d'entrée pour le mot de passe en entrant manuellement le code de couleur HTML hexadécimal ou par l'intermédiaire du sélecteur de couleurs.
Input Text Color	Configurez la couleur souhaitée du texte d'entrée pour le mot de passe en entrant manuellement le code de couleur HTML hexadécimal ou par l'intermédiaire du sélecteur de couleurs.
Theme Color	Configurez la couleur d'arrière-plan souhaitée pour le bouton en entrant manuellement le code de couleur HTML hexadécimal ou par l'intermédiaire du sélecteur de couleurs.
Button Text Color	Configurez la couleur de texte souhaitée pour le bouton en entrant manuellement le code de couleur HTML hexadécimal ou par l'intermédiaire du sélecteur de couleurs.
Button Position	Sélectionnez la position du bouton dans la page Portail.
Welcome Information	Cliquez sur la case à cocher et entrez le texte comme informations de bienvenue. Et vous pouvez configurer la couleur de texte souhaitée pour les informations de bienvenue en entrant le code de couleur HTML hexadécimal manuellement ou par l'intermédiaire du sélecteur de couleurs.
Terms of Service	Cliquez sur la case à cocher et entrez le texte comme conditions de service dans la zone suivante.
Copyright	Cliquez sur la case à cocher et entrez le texte comme droit d'auteur dans la zone suivante.

Cliquez sur Options de publicité et personnaliser les images publicitaires sur l'authentification page.



Advertisement	Cliquez sur la case à cocher pour activer la fonctionnalité Publicité. Avec cette fonctionnalité activée, vous pouvez ajouter des images publicitaires sur la page d'authentification. Ces photos publicitaires s'afficheront avant l'apparition de la page de connexion.
Picture Resource	Cliquez Choose et sélectionnez des photos de votre PC comme images publicitaires. Lorsque plusieurs images sont ajoutées, elles seront jouées en boucle.
Advertisement Duration Time	Entrez l'heure de durée pour les images publicitaires. Pour cette durée, les images seront jouées en boucle. Si le temps de durée n'est pas suffisant pour toutes les images, le reste ne sera pas affiché.
Picture Carousel Interval	Entrez l'intervalle carrousel d'images. Par exemple, si cette valeur est définie en 5 secondes, la première image s'affiche pendant 5 secondes, suivie de la deuxième image pendant 5 secondes, et ainsi de suite.
Allow Users To Skip Advertisement	Cliquez sur la case à cocher pour permettre aux utilisateurs d'ignorer la publicité.

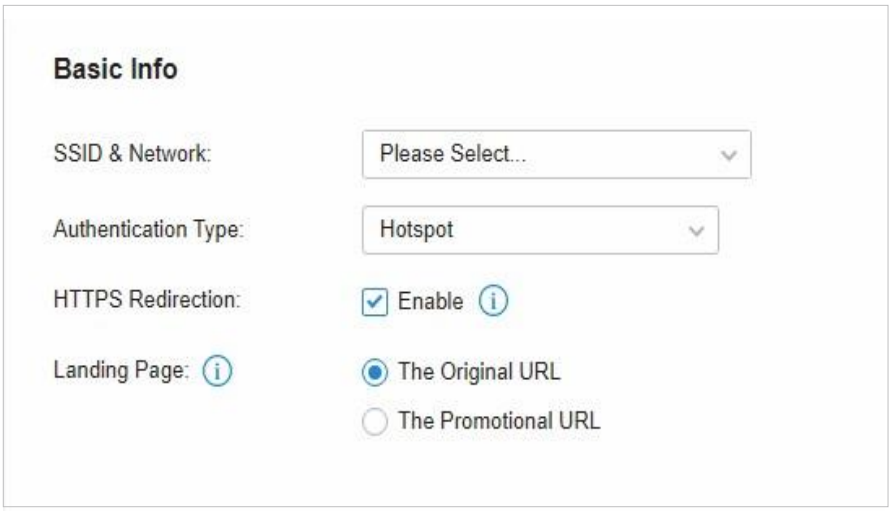
3. Dans la section Contrôle d'accès, configurez les règles de contrôle d'accès, y compris l'accès pré-authentification et la stratégie sans authentification si nécessaire.



Pre-Authentication Access	Cliquez sur la case à cocher pour activer l'accès pré-authentification. Grâce à cette fonctionnalité activée, les clients non authentifiés sont autorisés à accéder aux sous-réseaux et aux ressources Web spécifiés dans la liste d'accès pré-authentification ci-dessous.
Pre-Authentication Access List	Cliquez Add pour configurer la plage IP ou l'URL à laquelle les clients non authentifiés sont autorisés à accéder.
Authentication-Free Policy	Cliquez sur la case à cocher pour activer la stratégie sans authentification. Avec cette fonctionnalité activée, vous pouvez permettre à certains clients d'accéder à Internet sans authentification Portal.
Authentication-Free Client List	Cliquez sur Add et entrez l'adresse IP ou l'adresse MAC des clients sans authentification.

■ Configuration du portail avec hotspot

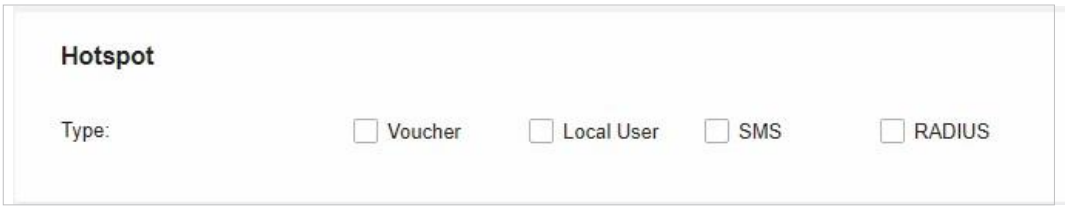
1. Allez dans Settings > Authentication > Portal Cliquez pour activer portal et charger la page suivante.



2. Sélectionnez les SSID et les réseaux LAN pour que le portail prenne effet et configure les réseaux de base parameters.

SSID & LAN Network	Sélectionnez un ou plusieurs SSID ou réseaux LAN pour le portail. Les clients connectés aux SSID sélectionnés ou aux réseaux LAN doivent se connecter à une page Web pour établir la vérification avant d'accéder au réseau.
Authentication Type	Sélectionnez le type d'authentification portal comme hotspot.
HTTPS Redirection	Cliquez sur la case à cocher pour activer la redirection HTTPS. Avec cette fonctionnalité activée, les clients non autorisés seront redirigés vers la page Portail lorsqu'ils tentent de parcourir les sites Web HTTPS. Cette fonctionnalité ayant été désactivée, les clients non autorisés ne peuvent pas parcourir les sites Web HTTPS et ne sont pas redirigés vers la page Portail.
Landing Page	Sélectionnez la page vers laquelle le client sera redirigé après une authentification réussie. The Original URL: Les clients sont dirigés vers l'URL qu'ils demandent après avoir passé l'authentification portal. The Promotional URL: Les clients sont dirigés vers l'URL spécifiée après avoir passé l'authentification du portail.

3. Dans la section Hotspot, sélectionnez un ou plusieurs types de hotspot pour authentifier les clients.



- **Configuration du portail des bons Voucher**

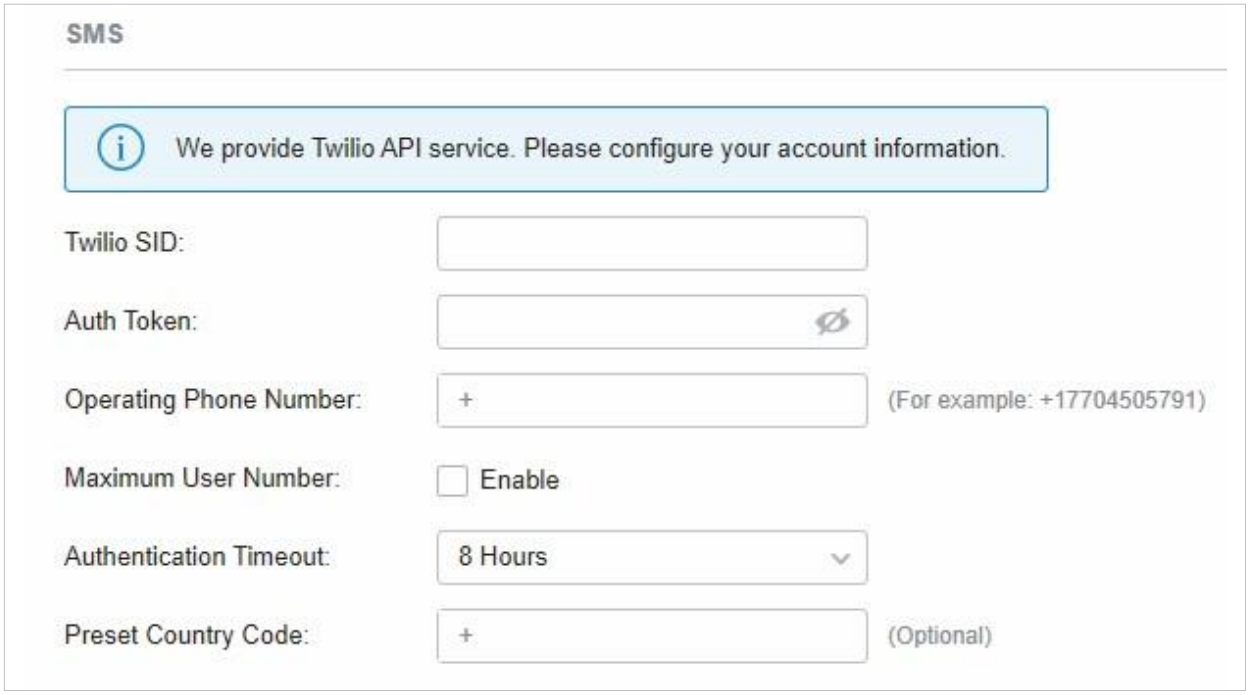
Voucher	SélectionnezVoucher et cliquez sur Voucher Manager pour gérer les codes de bons.
	Se référerVouchers pour des informations détaillées sur la façon de créer vouchers.

- **Configuring Local Portal**

Local User	Pour gérer les informations de l'utilisateur local Sélectionner et cliquez sur User Management Connexion accounts .
	Se référer à Utilisateurs locaux pour des informations détaillées sur la façon de créer des utilisateurs locaux.

- **Configuration du portail SMS**

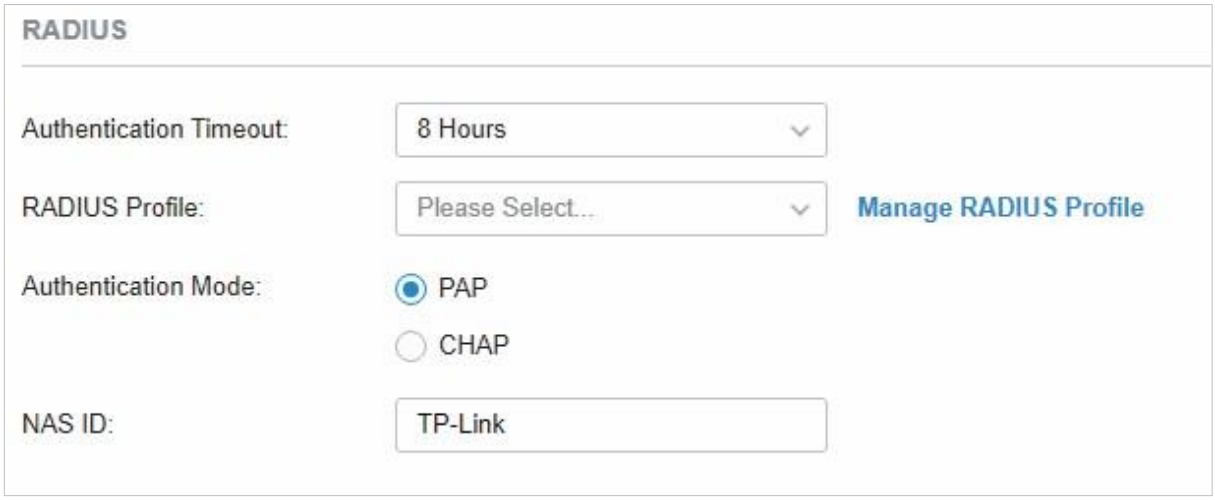
Sélectionnez SMS et configurez les paramètres requis dans la section SMS.



SMS	Les clients peuvent obtenir des codes de vérification à l'aide de leurs téléphones mobiles et entrer les codes reçus pour passer l'authentification.
Twilio SID	Entrez le SID de compte pour les informations d'identification de l'API Twilio.
Auth Token	Entrez le jeton d'authentification pour les informations d'identification de l'API Twilio.
Operating Phone Number	Entrez le numéro de téléphone utilisé pour envoyer des messages de vérification aux clients.
Maximum User Numbers	Cliquez sur la case à cocher et entrez le nombre maximal d'utilisateurs autorisés à être authentifiés à l'aide du même numéro de téléphone en même temps.
Authentication Timeout	Sélectionnez la durée de connexion. Le client doit se connecter à nouveau sur la page d'authentification Web pour accéder au réseau.
Preset Country Code	Entrez le code de pays par défaut qui sera rempli automatiquement sur la page d'authentification.

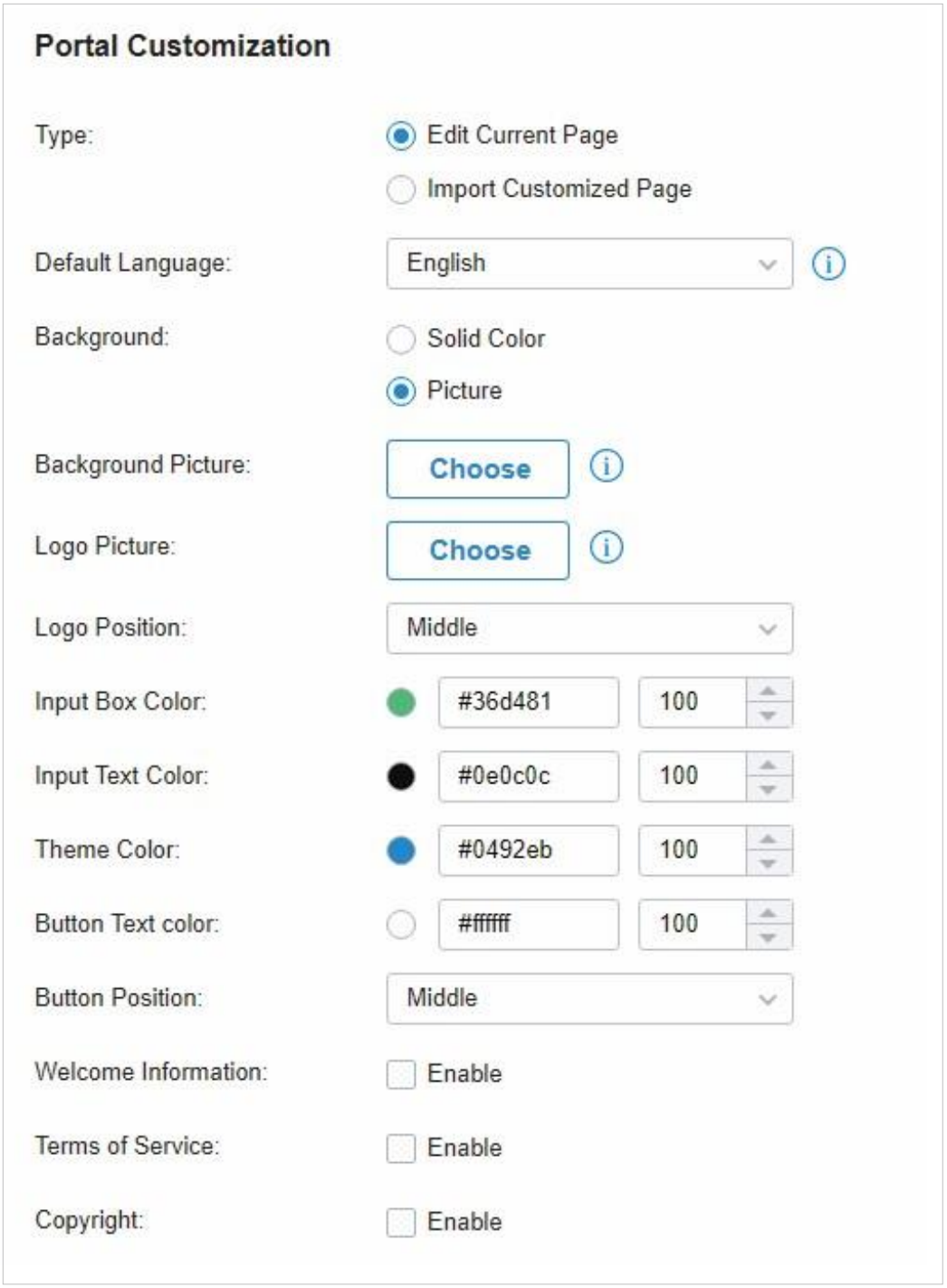
Configuration du portail RADIUS

Sélectionnez RADIUS et configurez les paramètres requis dans la section RADIUS.



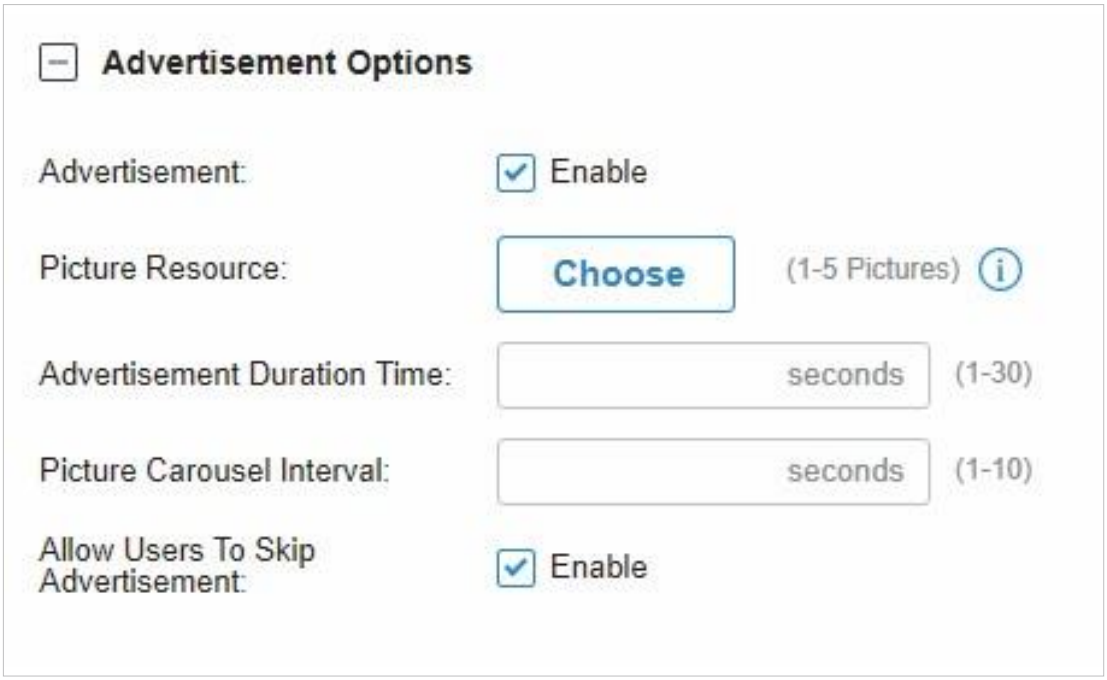
RADIUS	Les clients sont tenus d'entrer le nom d'utilisateur et le mot de passe corrects qui sont stockés dans le serveur RADIUS pour passer l'authentification.
RADIUS Profile	Sélectionnez le profil RADIUS que vous avez créé. Si aucun profil RADIUS n'a été créé, cliquez sur + Create New RADIUS Profile à partir de la liste déroulante ou Manage RADIUS Profile pour en créer un. Le profil RADIUS enregistre les informations du serveur RADIUS qui fournit une méthode de stockage central des informations d'authentification.
Authentication Mode	Sélectionnez le protocole d'authentification pour le serveur RADIUS. Deux protocoles d'authentification sont disponibles : PAP et CHAP.
NAS ID	Configurez un identificateur de serveur d'accès réseau (ID NAS) sur le portail. Les paquets de demande d'authentification du contrôleur vers le serveur RADIUS portent l'ID NAS. Le serveur RADIUS peut classer les utilisateurs en différents groupes en fonction de l'ID NAS, puis choisir des stratégies différentes pour différents groupes.

4. Dans la section Personnalisation du portail, personnaliser la page Portail comprenant l'image d'arrière-plan, l'image du logo et ainsi de suite.



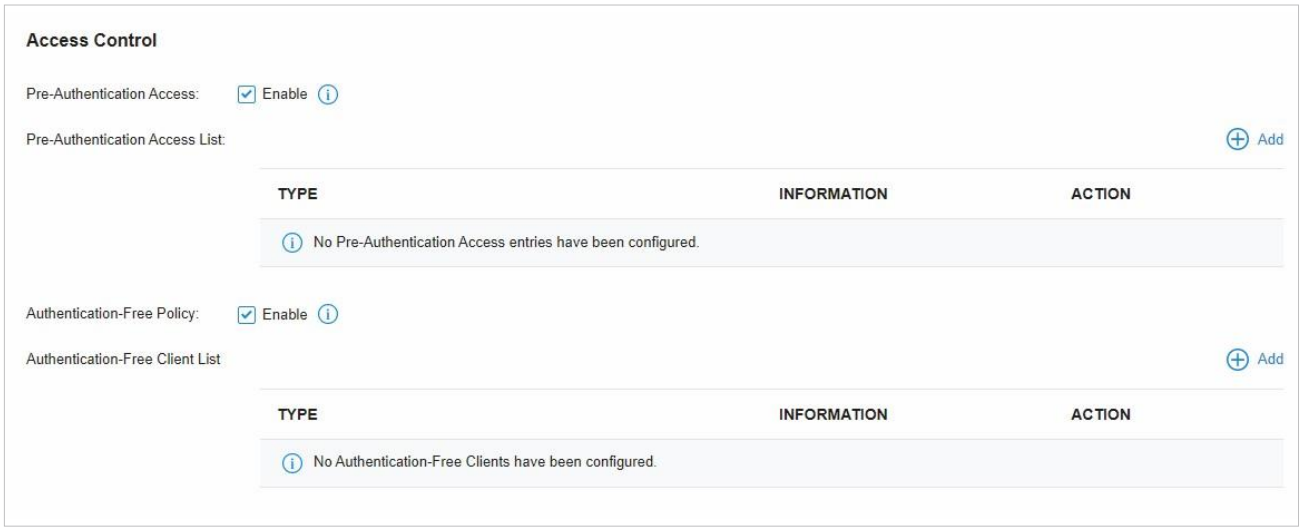
Default Language	Sélectionnez la langue par défaut affichée dans la page Portail. Le contrôleur ajuste automatiquement la langue affichée sur la page Portail en fonction de la langue système des clients. Si la langue n'est pas prise en charge, le contrôleur utilisera la langue par défaut spécifiée ici.
Type	Sélectionnez le type de la page Portail. Edit Current Page: Modifiez les paramètres connexes pour personnaliser la page du portail en fonction de la page fournie. Import Customized Page cliquez Import pour importer votre page Portail unique pour la marquer selon votre entreprise.
Background	Sélectionner le type d'arrière-plan. Solid Color: Configurez la couleur d'arrière-plan souhaitée en entrant manuellement le code de couleur HTML hexadécimal ou par l'intermédiaire du sélecteur de couleurs. Picture: Cliquez et sélectionnez une image de votre PC en arrière-plan. Choose
Logo Picture	Cliquez Choose et sélectionnez une image de votre PC comme logo.
Logo Position	Sélectionnez la position du logo dans la page Portail.
Input Box Color	Configurez la couleur souhaitée de la zone d'entrée pour le mot de passe en entrant manuellement le code de couleur HTML hexadécimal ou par l'intermédiaire du sélecteur de couleurs.
Input Text Color	Configurez la couleur souhaitée du texte d'entrée pour le mot de passe en entrant manuellement le code de couleur HTML hexadécimal ou par l'intermédiaire du sélecteur de couleurs.
Theme Color	Configurez la couleur d'arrière-plan souhaitée pour le bouton en entrant manuellement le code de couleur HTML hexadécimal ou par l'intermédiaire du sélecteur de couleurs.
Button Text Color	Configurez la couleur de texte souhaitée pour le bouton en entrant manuellement le code de couleur HTML hexadécimal ou par l'intermédiaire du sélecteur de couleurs.
Button Position	Sélectionnez la position du bouton dans la page Portail.
Welcome Information	Cliquez sur la case à cocher et entrez le texte comme informations de bienvenue. Et vous pouvez configurer la couleur de texte souhaitée pour les informations de bienvenue en entrant le code de couleur HTML hexadécimal manuellement ou par l'intermédiaire du sélecteur de couleurs.
Terms of Service	Cliquez sur la case à cocher et entrez le texte comme conditions de service dans la zone suivante.
Copyright	Cliquez sur la case à cocher et entrez le texte comme droit d'auteur dans la zone suivante.

Cliquez sur Options de publicité et personnaliser les images publicitaires sur la page d'authentification.



Advertisement	Cliquez sur la case à cocher pour activer la fonctionnalité Publicité. Avec cette fonctionnalité activée, vous pouvez ajouter des images publicitaires sur la page d'authentification. Ces photos publicitaires s'afficheront avant l'apparition de la page de connexion.
Picture Resource	Cliquez et sélectionnez des photos de votre PC comme images publicitaires. Lorsque plusieurs images sont ajoutées, elles seront jouées en boucle. Choose
Advertisement Duration Time	Entrez l'heure de durée pour les images publicitaires. Pour cette durée, les images seront jouées en boucle. Si le temps de durée n'est pas suffisant pour toutes les photos, le reste ne sera pas affiché.
Picture Carousel Interval	Enter the picture carousel interval. For example, if this value is set as 5 seconds, the first picture will be displayed for 5 seconds, followed by the second picture for 5 seconds, and so on.
Allow Users To Skip Advertisement	Cliquez sur la case à cocher pour permettre aux utilisateurs d'ignorer la publicité.

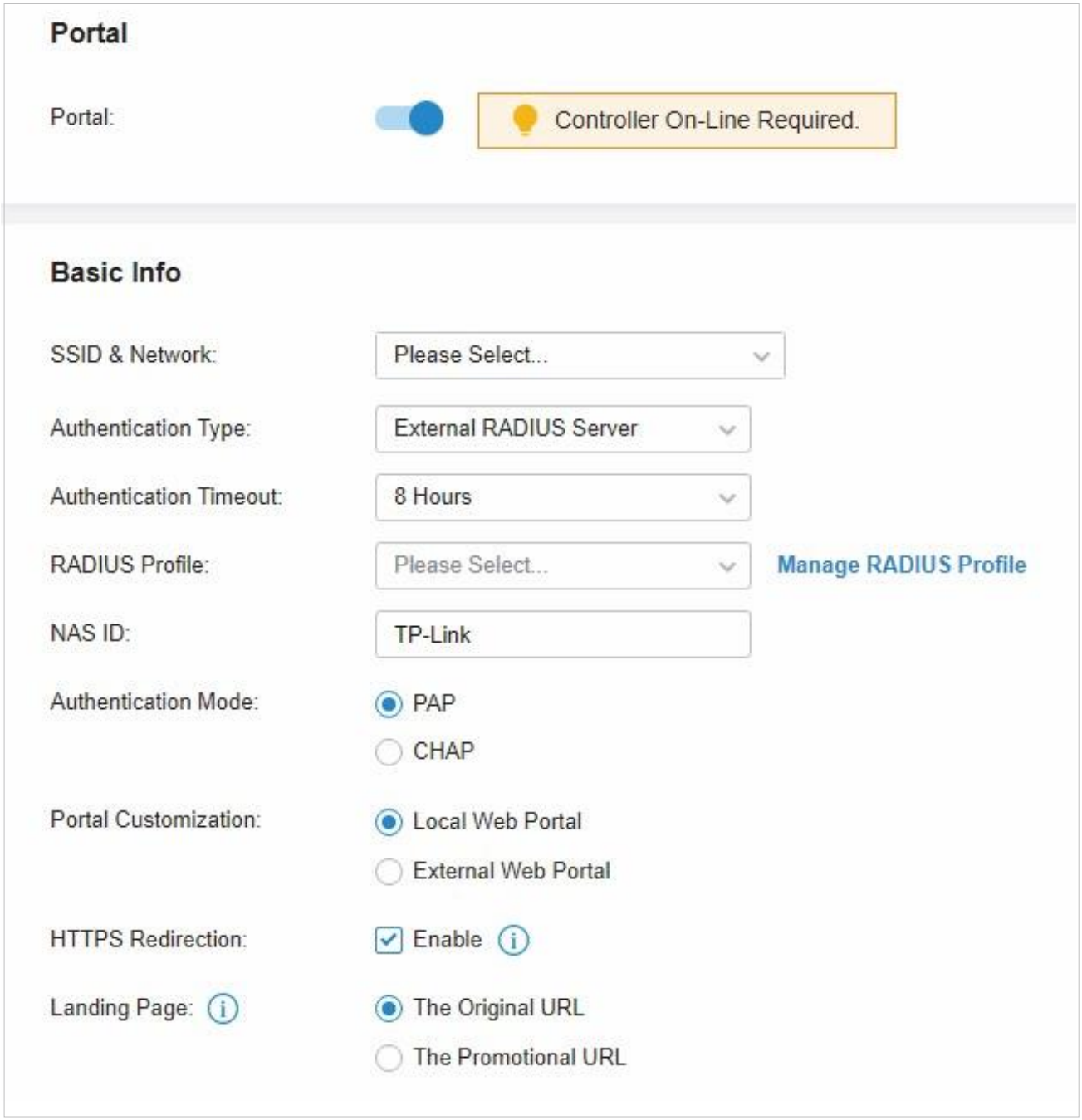
5. Dans la section Contrôle d'accès, configurez les règles de contrôle d'accès, y compris l'accès pré-authentification et la stratégie sans authentification si nécessaire.



Pre-Authentication Access	Cliquez sur la case à cocher pour activer l'accès pré-authentification. Grâce à cette fonctionnalité activée, les clients non authentifiés sont autorisés à accéder aux sous-réseaux et aux ressources Web spécifiés dans la liste d'accès pré-authentification ci-dessous.
Pre-Authentication Access List	Cliquez Add pour configurer la plage IP ou l'URL à laquelle les clients non authentifiés sont autorisés à accéder.
Authentication-Free Policy	Cliquez sur la case à cocher pour activer la stratégie sans authentification. Avec cette fonctionnalité activée, vous pouvez autoriser certains clients à accéder à Internet sans authentification Portal.
Authentication-Free Client List	Cliquez Add et entrez l'adresse IP ou l'adresse MAC des clients sans authentification.

■ **Configuration du portail avec le serveur RADIUS externe**

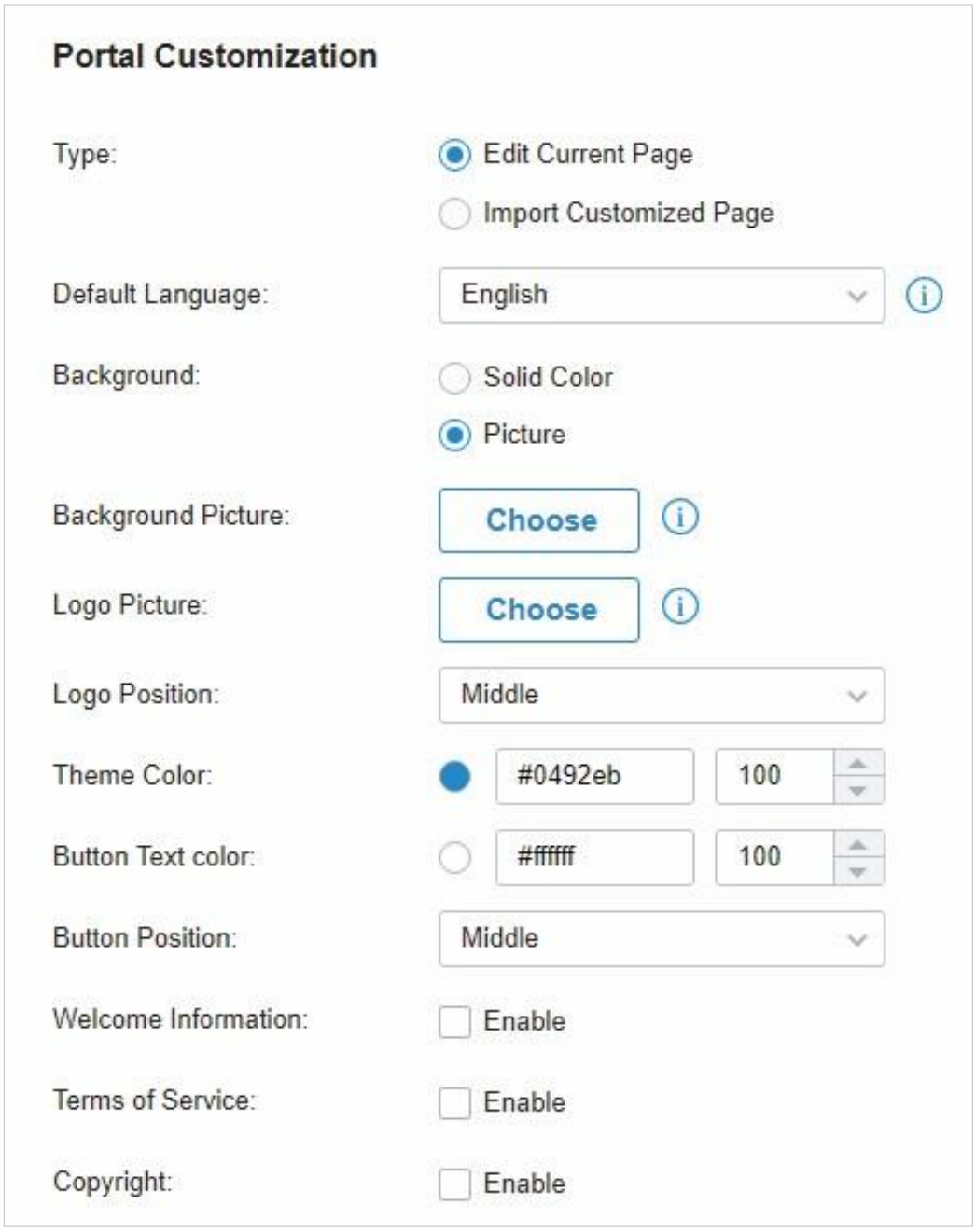
Allez dans Settings > Authentication > Portal. Cliquez sur pour activer portal et charger la page suivante.



2. Sélectionnez les SSID et les réseaux LAN pour que le portail prenne effet et configure les paramètres de base, y compris le type d'authentification, le délai d'expiration d'authentification, et ainsi de suite.

SSID & LAN Network	Sélectionnez un ou plusieurs SSID ou réseaux LAN pour le portail. Les clients connectés aux SSID sélectionnés ou aux réseaux LAN doivent se connecter à une page Web pour établir la vérification avant d'accéder au réseau.
Authentication Type	Sélectionnez le type d'authentification portal en tant que serveur RADIUS externe.
Authentication Timeout	Sélectionnez la durée de connexion. Les clients seront hors ligne après le délai d'expiration d'authentification.
RADIUS Profile	Sélectionnez le profil RADIUS que vous avez créé. Si aucun profil RADIUS n'a été créé, cliquez à partir de la liste déroulante ou Manage RADIUS Profile pour en créer un. Le profil RADIUS enregistre les informations du serveur RADIUS, y compris l'adresse IP, le port et ainsi de suite.
NAS ID	Configurez un identificateur de serveur d'accès réseau (ID NAS) sur le portail. Les paquets de demande d'authentification du contrôleur vers le serveur RADIUS portent l'ID NAS. Le serveur RADIUS peut classer les utilisateurs en différents groupes en fonction de l'ID NAS, puis choisir des stratégies différentes pour différents groupes.
Authentication Mode	Sélectionnez le protocole d'authentification pour le serveur RADIUS.
Portal Customization	Select Local Web Portal or External Web Portal. The authentication login page of Local Web Portal is provided by the built-in portal server of the controller. The External Web Portal is provided by external portal server. Enter the authentication login page's URL provided by the external portal server in the External Web Portal URL field.
HTTPS Redirection	Cliquez sur la case à cocher pour activer la redirection HTTPS. Avec cette fonctionnalité activée, les clients non autorisés seront redirigés vers la page Portail lorsqu'ils tentent de parcourir les sites Web HTTPS. Avec cette fonctionnalité désactivée, les clients non autorisés ne peuvent pas parcourir les sites Web HTTPS et ne sont pas redirigés vers la page Portail.
Landing Page	Sélectionnez la page vers laquelle le client sera redirigé après une authentification réussie. The Original URL: Les clients sont dirigés vers l'URL qu'ils demandent après avoir passé l'authentification portal. The Promotional URL: Les clients sont dirigés vers l'URL spécifiée ici après avoir passé l'authentification portal.

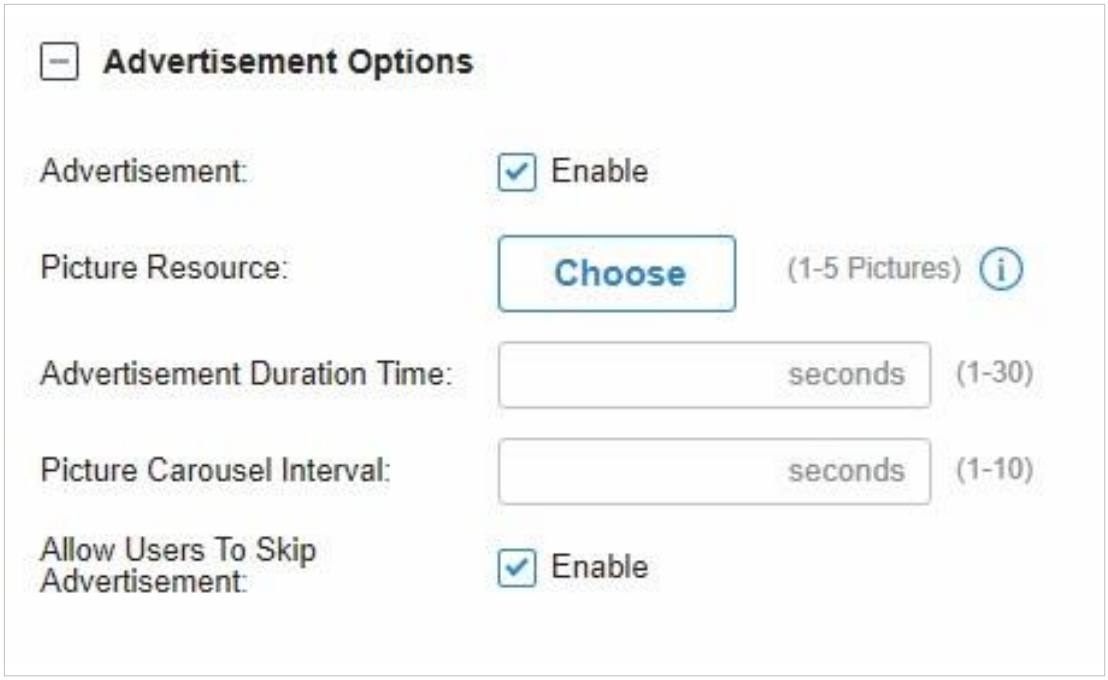
3. Si vous choisissez Portail Web local fourni par le serveur de portail intégré du contrôleur, personnalisez la page Portail dans la section Personnalisation du portail, y compris l'image d'arrière-plan, l'image du logo, et ainsi de suite.



Type	Sélectionnez le type de la page Portail. Edit Current Page: Modifiez les paramètres connexes pour personnaliser la page du portail en fonction de la page fournie. Customized Page: Import pour importer votre page portail unique pour l'image de marque selon votre entreprise

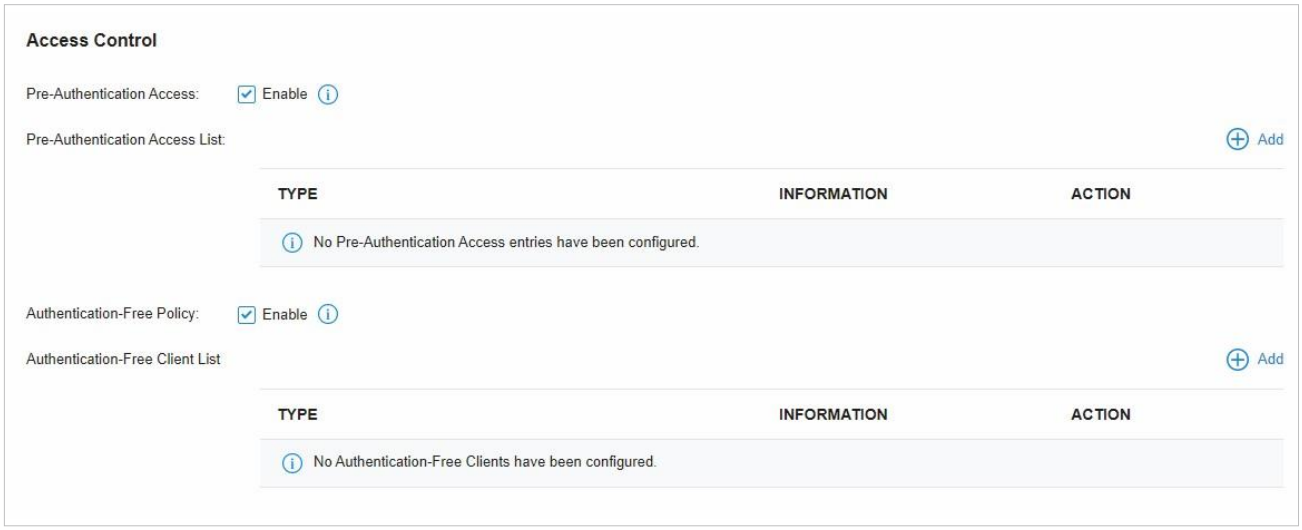
Default Language	Sélectionnez la langue par défaut affichée dans la page Portail. Le contrôleur ajuste automatiquement la langue affichée sur la page Portail en fonction de la langue système des clients. Si la langue n'est pas prise en charge, le contrôleur utilisera la langue par défaut spécifiée ici.
Background	Sélectionner le type d'arrière-plan. Solid Color: Configurez la couleur d'arrière-plan souhaitée en entrant manuellement le code de couleur HTML hexadécimal ou par l'intermédiaire du sélecteur de couleurs. Picture: Cliquez sur Choose et sélectionnez une image de votre PC en arrière-plan.
Logo Picture	Cliquez sur Choose et sélectionnez une image de votre PC comme logo.
Logo Position	Sélectionnez la position du logo dans la page Portail.
Theme Color	Configurez la couleur d'arrière-plan souhaitée pour le bouton en entrant manuellement le code de couleur HTML hexadécimal ou par l'intermédiaire du sélecteur de couleurs.
Button Text Color	Configurez la couleur de texte souhaitée pour le bouton en entrant manuellement le code de couleur HTML hexadécimal ou par l'intermédiaire du sélecteur de couleurs.
Button Position	Sélectionnez la position du bouton dans la page Portail.
Welcome Information	Cliquez sur la case à cocher et entrez le texte comme informations de bienvenue. Et vous pouvez configurer la couleur de texte souhaitée pour les informations de bienvenue en entrant le code de couleur HTML hexadécimal manuellement ou par l'intermédiaire du sélecteur de couleurs.
Terms of Service	Cliquez sur la case à cocher et entrez le texte comme conditions de service dans la zone suivante.
Copyright	Cliquez sur la case à cocher et entrez le texte comme droit d'auteur dans la zone suivante.

Cliquez sur Options de publicité et personnalisez les images publicitaires sur la page d'authentification.



Advertisement	Cliquez sur la case à cocher pour activer la fonctionnalité Publicité. Avec cette fonctionnalité activée, vous pouvez ajouter des images publicitaires sur la page d'authentification. Ces photos publicitaires seront affichées avant l'apparition de la page de connexion.
Picture Resource	Cliquez Choose et sélectionnez des photos de votre PC comme images publicitaires. Lorsque plusieurs images sont ajoutées, elles seront jouées en boucle.
Advertisement Duration Time	Entrez l'heure de durée pour les images publicitaires. Pour cette durée, les images seront jouées en boucle. Si le temps de durée n'est pas suffisant pour toutes les images, le reste ne sera pas affiché.
Picture Carousel Interval	Entrez l'intervalle carrousel d'images. Par exemple, si cette valeur est définie en 5 secondes, la première image s'affiche pendant 5 secondes, suivie de la deuxième image pendant 5 secondes, et ainsi de suite.
Allow Users To Skip Advertisement	Cliquez sur la case à cocher pour permettre aux utilisateurs d'ignorer la publicité.

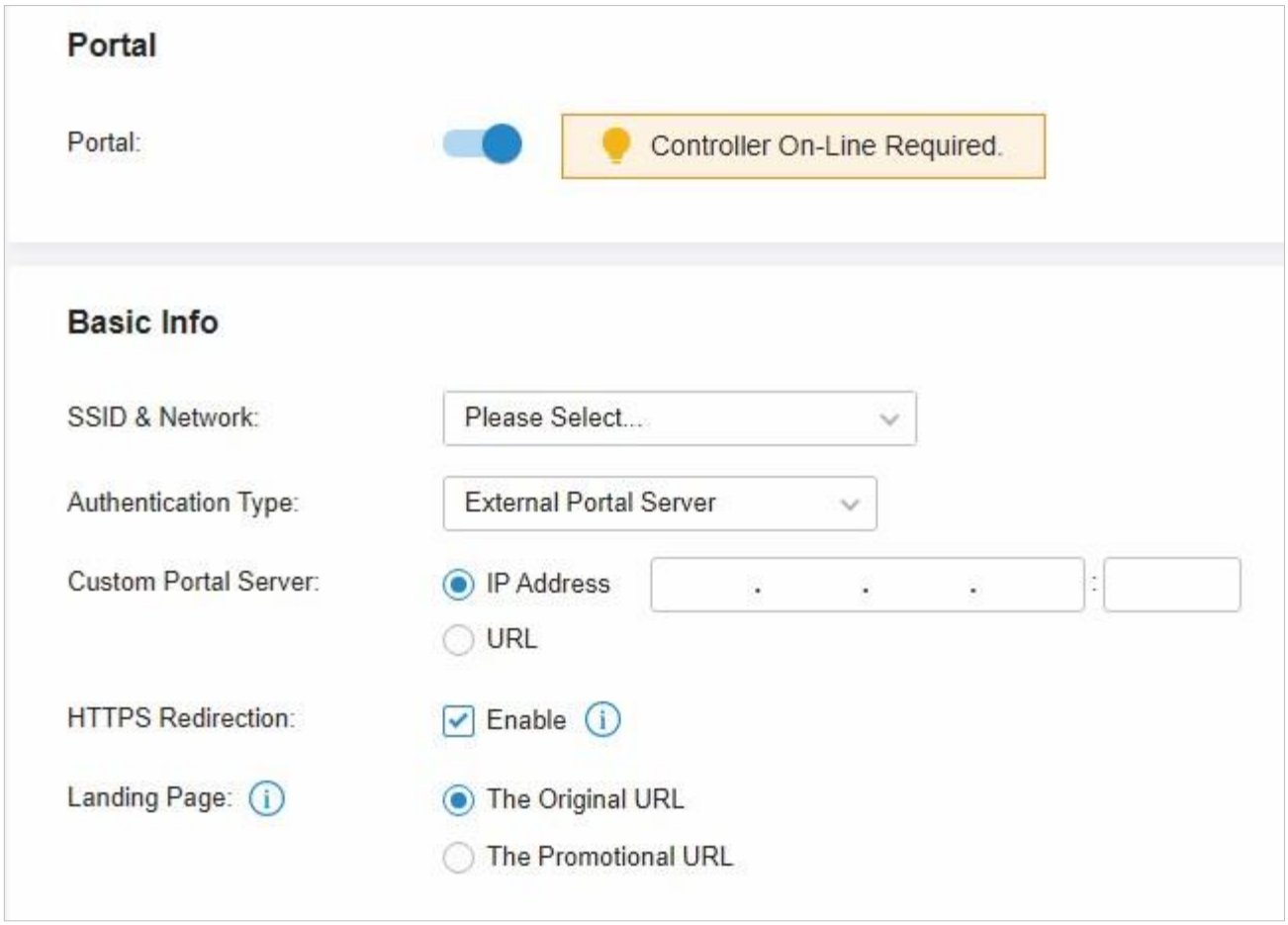
1. **Dans la section Contrôle d'accès, configurez les règles de contrôle d'accès, y compris l'accès pré-authentification et la stratégie sans authentification si nécessaire.**



Pre-Authentication Access	Cliquez sur la case à cocher pour activer l'accès pré-authentification. Grâce à cette fonctionnalité activée, les clients non authentifiés sont autorisés à accéder aux sous-réseaux et aux ressources Web spécifiés dans la liste d'accès pré-authentification ci-dessous.
Pre-Authentication Access List	Cliquez ⊕ Add pour configurer la plage IP ou l'URL à laquelle les clients non authentifiés sont autorisés à accéder.
Authentication-Free Policy	Cliquez sur la case à cocher pour activer la stratégie sans authentification. Avec cette fonctionnalité activée, vous pouvez autoriser certains clients à accéder à Internet sans authentification Portal.
Authentication-Free Client List	Cliquez ⊕ Add et entrez l'adresse IP ou l'adresse MAC des clients sans authentification.

■ Configuration du portail avec le serveur portail externe

1. Dans Settings > Authentication > Portal Cliquez pour activer portal et charger la page suivante.

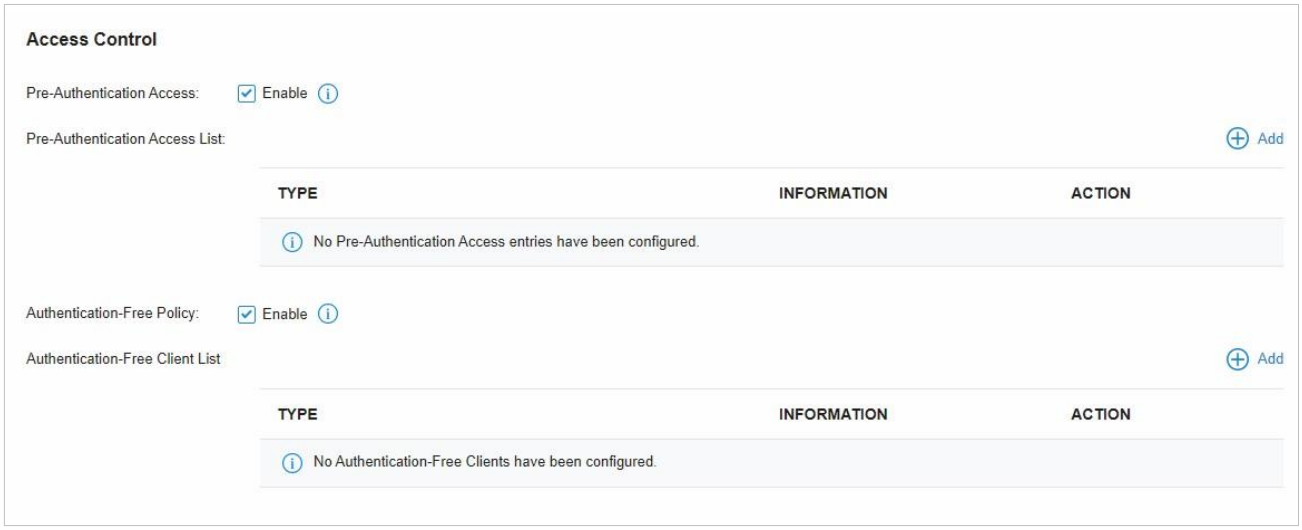


2. Sélectionnez les SSID et les réseaux LAN pour que le portail prenne effet et configure les paramètres de base, y compris le type d'authentification, le serveur de portail personnalisé, et ainsi de suite.

SSID & LAN Network	Sélectionnez un ou plusieurs SSID ou réseaux LAN pour le portail. Les clients connectés aux SSID sélectionnés ou aux réseaux LAN doivent se connecter à une page Web pour établir la vérification avant d'accéder au réseau.
Authentication Type	Sélectionnez le type d'authentification portal en tant que serveur portail externe.
Custom Portal Server	Spécifiez l'adresse IP ou l'URL qui redirige vers un serveur portail externe.
HTTPS Redirection	Cliquez sur la case à cocher pour activer la redirection HTTPS. Avec cette fonctionnalité activée, les clients non autorisés seront redirigés vers la page Portail lorsqu'ils tentent de parcourir les sites Web HTTPS. Cette fonctionnalité ayant été désactivée, les clients non autorisés ne peuvent pas parcourir les sites Web HTTPS et ne sont pas redirigés vers la page Portail.

Landing Page	Sélectionnez la page vers laquelle le client sera redirigé après une authentification réussie. The Original URL: Les clients sont dirigés vers l'URL qu'ils demandent après avoir passé l'authentification portal. The Promotional URL: Les clients sont dirigés vers l'URL spécifiée ici après avoir passé l'authentification portal.

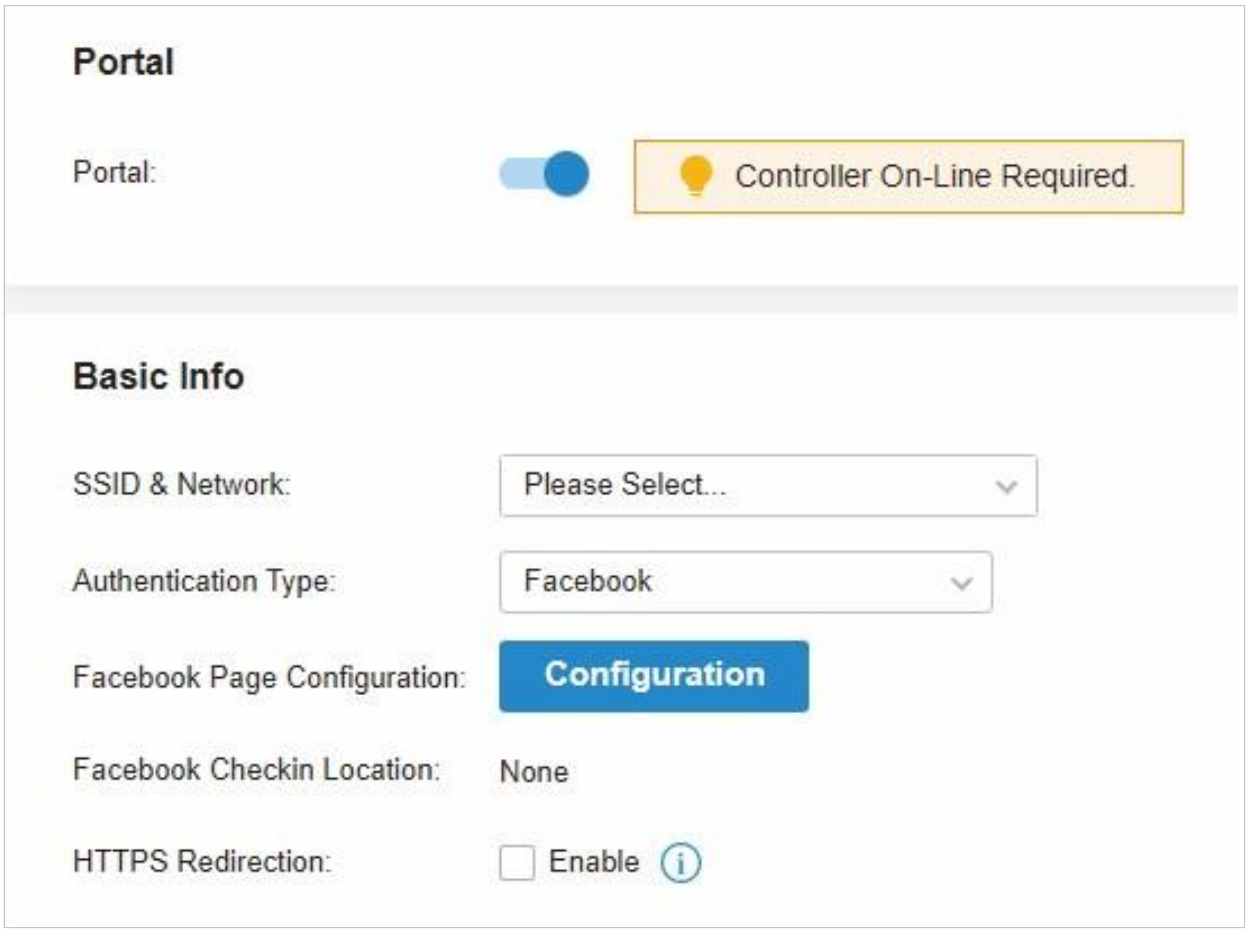
1. **Dans la section Contrôle d'accès, configurez les règles de contrôle d'accès, y compris l'accès pré-authentification et la stratégie sans authentification si nécessaire.**



Pre-Authentication Access	Cliquez sur la case à cocher pour activer l'accès pré-authentification. Grâce à cette fonctionnalité activée, les clients non authentifiés sont autorisés à accéder aux sous-réseaux et aux ressources Web spécifiés dans la liste d'accès pré-authentification ci-dessous.
Pre-Authentication Access List	Cliquez Add pour configurer la plage IP ou l'URL à laquelle les clients non authentifiés sont autorisés à accéder.
Authentication-Free Policy	Cliquez sur la case à cocher pour activer la stratégie sans authentification. Avec cette fonctionnalité activée, vous pouvez permettre à certains clients d'accéder à Internet sans authentification Portal.
Authentication-Free Client List	Cliquez Add et entrez l'adresse IP ou l'adresse MAC des clients sans authentification.

■ Configuration du portail avec Facebook

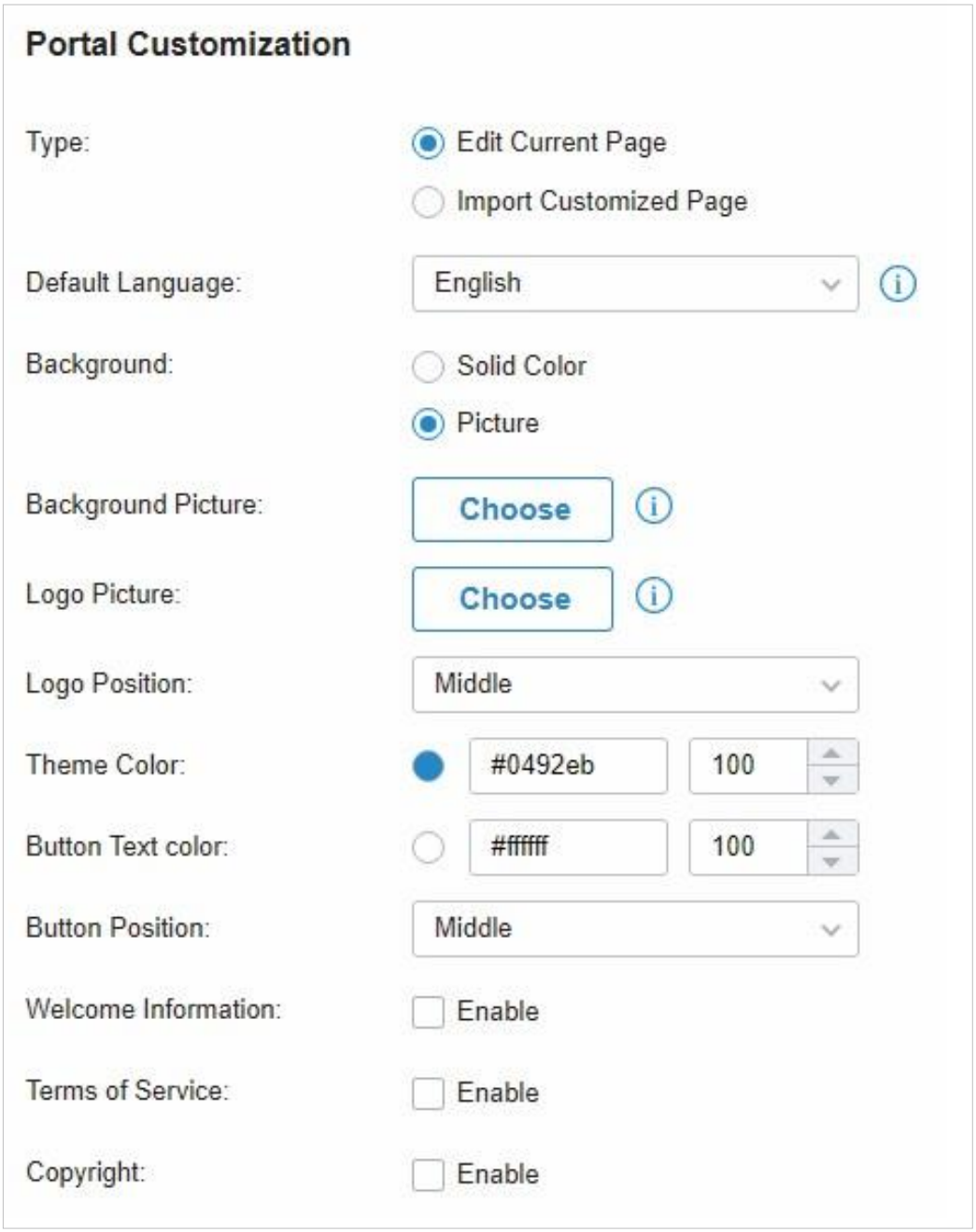
1. Dans Settings > Authentication > Portal. Click pour activer le portail et charger la page suivante.



1. Sélectionnez les SSID et les réseaux LAN pour que le portail prenne effet et configure les paramètres de base.

SSID & LAN Network	Sélectionnez un ou plusieurs SSID ou réseaux LAN pour le portail. Les clients connectés aux SSID sélectionnés ou aux réseaux LAN doivent se connecter à une page Web pour établir la vérification avant d'accéder au réseau.
Authentication Type	Sélectionnez le type d'authentification portal comme Facebook.
Facebook Page Configuration:	Cliquez Configuration pour spécifier la page Facebook.
Facebook Checkin Location	Lorsque le contrôleur Omada obtient avec succès la page Facebook, il affiche le nom de la page Facebook ici.
HTTPS Redirection	Cliquez sur la case à cocher pour activer la redirection HTTPS. Avec cette fonctionnalité activée, les clients non autorisés seront redirigés vers la page Portail lorsqu'ils tentent de parcourir les sites Web HTTPS. Cette fonctionnalité ayant été désactivée, les clients non autorisés ne peuvent pas parcourir les sites Web HTTPS et ne sont pas redirigés vers la page Portail.

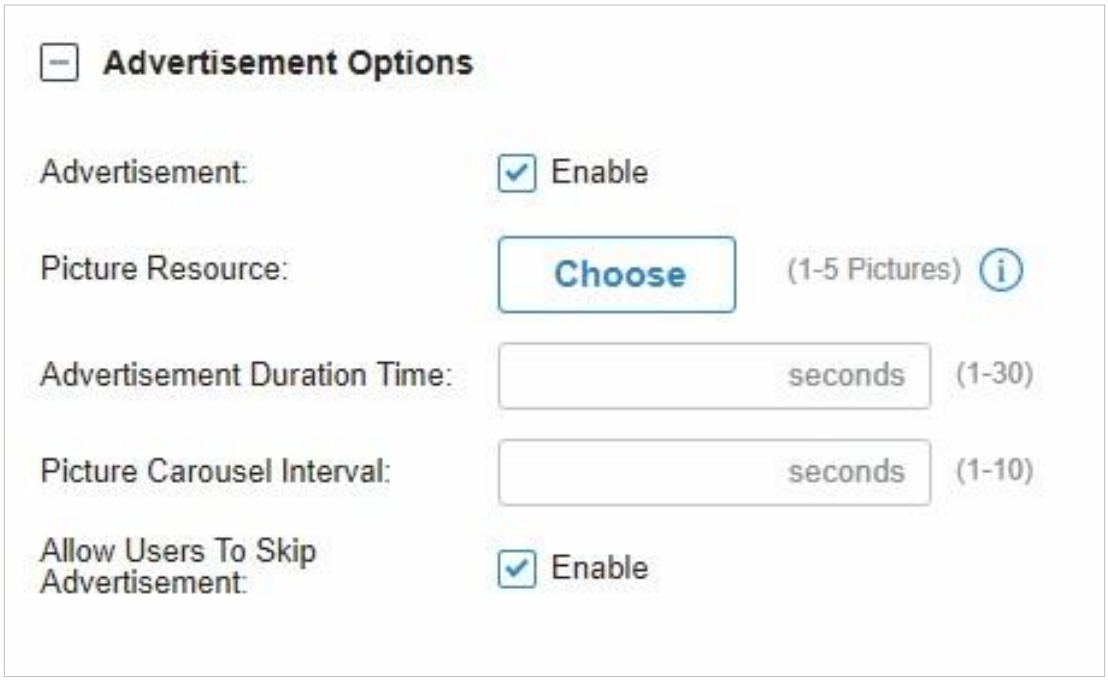
2. Dans la section Personnalisation du portail, personnaliser la page Portail comprenant l'image d'arrière-plan, l'image du logo et ainsi de suite.



Type	Sélectionnez le type de la page Portail. Edit Current Page: Modifiez les paramètres connexes pour personnaliser la page du portail en fonction de la page fournie. Import Customized Page: Cliquez pour importer votre page portail unique pour la marquer selon votre entreprise. Import

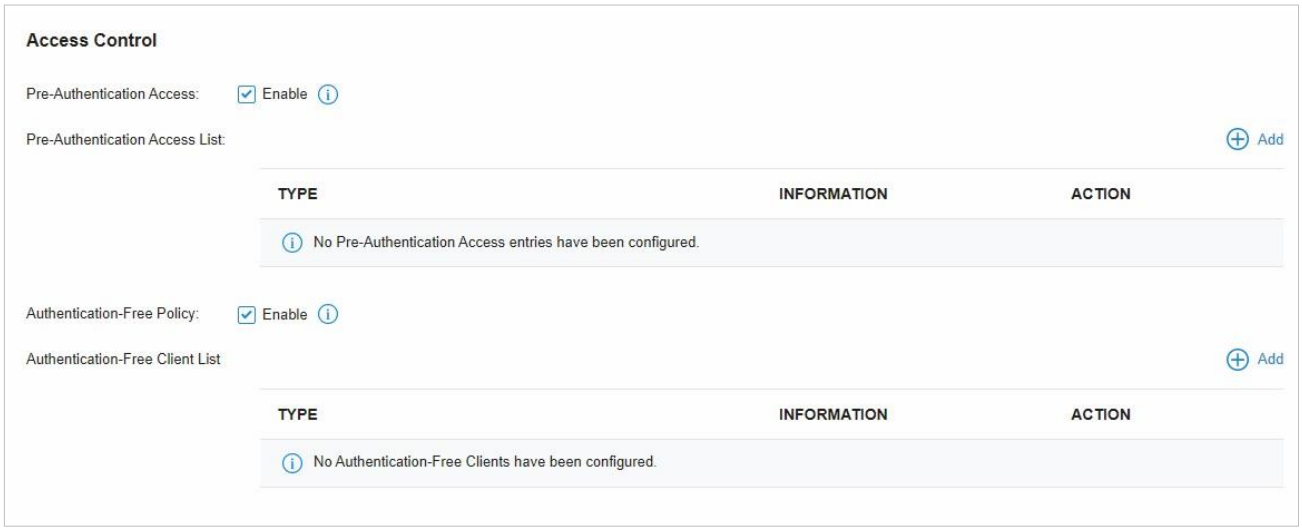
Default Language	Sélectionnez la langue par défaut affichée dans la page Portail. Le contrôleur ajuste automatiquement la langue affichée sur la page Portail en fonction de la langue système des clients. Si la langue n'est pas prise en charge, le contrôleur utilisera la langue par défaut spécifiée ici.
Background	Sélectionnez le type d'arrière-plan. Solid Color: Configurez la couleur d'arrière-plan souhaitée en entrant manuellement le code de couleur HTML hexadécimal ou par l'intermédiaire du sélecteur de couleurs. Picture: Cliquez Choose et sélectionnez une image de votre PC en arrière-plan.
Logo Picture	Cliquez Choose et sélectionnez une image de votre PC comme logo.
Logo Position	Sélectionnez la position du logo dans la page Portail.
Theme Color	Configurez la couleur d'arrière-plan souhaitée pour le bouton en entrant manuellement le code de couleur HTML hexadécimal ou par l'intermédiaire du sélecteur de couleurs.
Button Text Color	Configurez la couleur de texte souhaitée pour le bouton en entrant manuellement le code de couleur HTML hexadécimal ou par l'intermédiaire du sélecteur de couleurs.
Button Position	Sélectionnez la position du bouton dans la page Portail.
Welcome Information	Cliquez sur la case à cocher et entrez le texte comme informations de bienvenue. Et vous pouvez configurer la couleur de texte souhaitée pour les informations de bienvenue en entrant le code de couleur HTML hexadécimal manuellement ou par l'intermédiaire du sélecteur de couleurs.
Terms of Service	Cliquez sur la case à cocher et entrez le texte comme conditions de service dans la zone suivante.
Copyright	Cliquez sur la case à cocher et entrez le texte comme droit d'auteur dans la zone suivante.

Click Advertisement Options et personnaliser les images publicitaires sur la page d'authentification.



Picture Resource	Cliquez Choose et sélectionnez des photos de votre PC comme images publicitaires. Lorsque plusieurs images sont ajoutées, elles seront jouées en boucle.
Advertisement	Cliquez sur la case à cocher pour activer la fonctionnalité Publicité. Avec cette fonctionnalité activée, vous pouvez ajouter des images publicitaires sur la page d'authentification. Ces photos publicitaires seront affichées avant l'apparition de la page de connexion
Advertisement Duration Time	Entrez l'heure de durée pour les images publicitaires. Pour cette durée, les images seront jouées en boucle. Si le temps de durée n'est pas suffisant pour toutes les photos, le reste ne sera pas affiché.
Picture Carousel Interval	Entrez l'intervalle carrousel d'images. Par exemple, si cette valeur est définie en 5 secondes, la première image s'affiche pendant 5 secondes, suivie de la deuxième image pendant 5 secondes, et ainsi de suite.
Allow Users To Skip Advertisement	Cliquez sur la case à cocher pour permettre aux utilisateurs d'ignorer la publicité.

3. Dans le contrôle d'accès, configurez les règles de contrôle d'accès, y compris l'accès pré-authentification et la stratégie sans authentification si nécessaire.



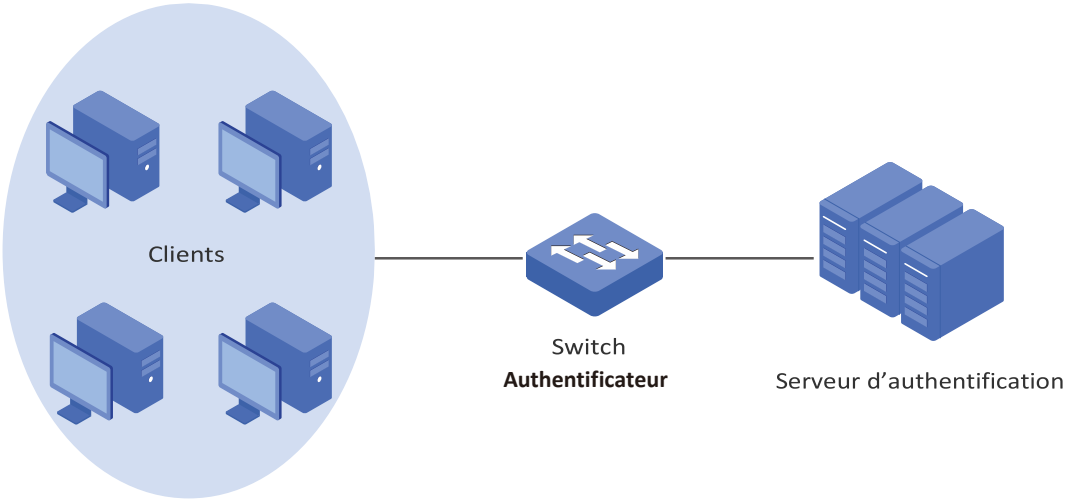
Pre-Authentication Access	Cliquez sur la case à cocher pour activer l'accès pré-authentification. Grâce à cette fonctionnalité activée, les clients non authentifiés sont autorisés à accéder aux sous-réseaux et aux ressources Web spécifiés dans la liste d'accès pré-authentification ci-dessous.
Pre-Authentication Access List	Cliquez Add pour configurer la plage IP ou l'URL à laquelle les clients non authentifiés sont autorisés à accéder.
Authentication-Free Policy	Cliquez sur la case à cocher pour activer la stratégie sans authentification. Avec cette fonctionnalité activée, vous pouvez autoriser certains clients à accéder à Internet sans authentification Portal.
Authentication-Free Client List	Cliquez Add et entrez l'adresse IP ou l'adresse MAC des clients sans authentification.

4. 9. 2 802.1X

Aperçu

802.1X fournit un service d'authentification basé sur le port pour empêcher les clients non autorisés d'accéder au réseau par l'intermédiaire de ports de commutateur accessibles au public. Un port compatible 802.1X permet uniquement les messages d'authentification et interdit le trafic normal jusqu'à ce que le client passe l'authentification.

L'authentification 802.1X utilise le modèle client-serveur qui contient trois rôles de périphérique : client/suppliant, authentificateur et serveur d'authentification. Ceci est décrit dans la figure ci-dessous:



- **Client**

  Un client, généralement un ordinateur, est connecté à l'authentificateur via un port physique. Nous vous recommandons d'installer le logiciel client d'authentification TP-Link 802.1X sur les hôtes clients, leur permettant de demander l'authentification 802.1X pour accéder au réseau local.

- **Authentificateur**

  Un authentificateur est généralement un périphérique réseau qui prend en charge le protocole 802.1X. Comme le montre la figure ci-dessus, le commutateur est un authentificateur.

  L'authentificateur agit comme un proxy intermédiaire entre le client et le serveur d'authentification. L'authentificateur demande des informations utilisateur du client et les envoie au serveur d'authentification ; En outre, l'authentificateur obtient des réponses à partir du serveur d'authentification et les envoie au client. L'authentificateur permet aux clients authentifiés d'accéder au RÉSEAU local via les ports connectés, mais nie les clients non authentifiés.

- **Serveur d'authentification**

  Le serveur d'authentification est généralement l'hôte exécutant le programme de serveur RADIUS. Il stocke les informations des clients, confirme si un client est légal et informe l'authentificateur si un client est authentifié.

  Basé sur l'identité authentifiée, 802.1X peut également fournir des services personnalisés. Par exemple, 802.1X et VLAN Assignment permettent d'affecter automatiquement différents utilisateurs authentifiés à différents VLAN.

Configuration

Pour compléter la configuration 802.1X, procédez comme suit :

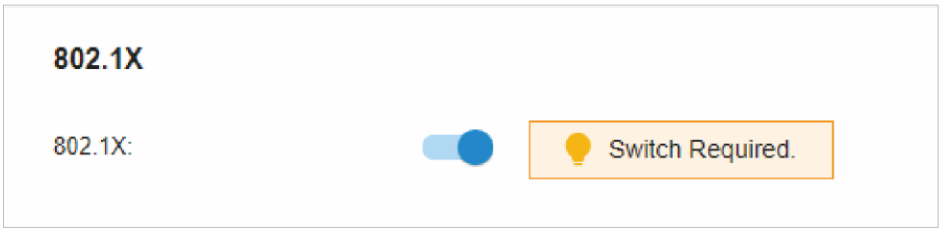
1.) Cliquez pour activer 802.1X.

2.) Sélectionnez le profil RADIUS que vous avez créé et configurez d'autres paramètres.

1) Sélectionnez les ports sur lesquels l'authentification 802.1X entrera en vigueur.

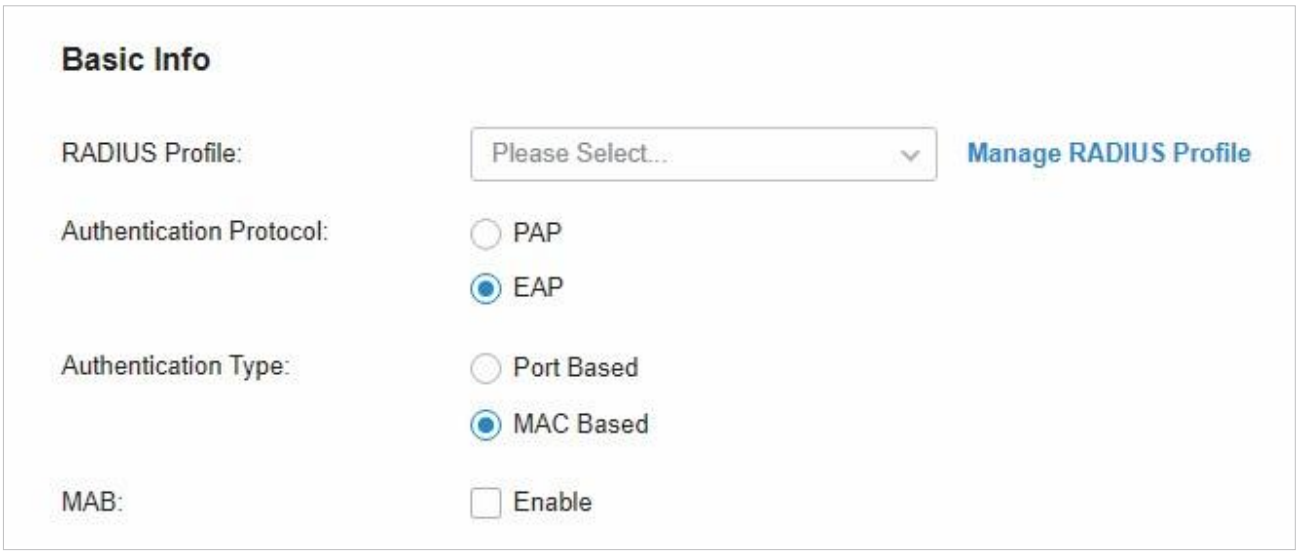


Dans Settings > Authentication > 802.1X. Cliquez pour activer 802.1X.





Sélectionnez le profil RADIUS que vous avez créé. Si aucun profil RADIUS n'a été créé, cliquez sur + Create New RADIUS Profile à partir de la liste déroulante ou Manage RADIUS Profile pour en créer un. Le profil RADIUS enregistre les informations du serveur RADIUS qui agit comme serveur d'authentification pendant l'authentification 802.1X.

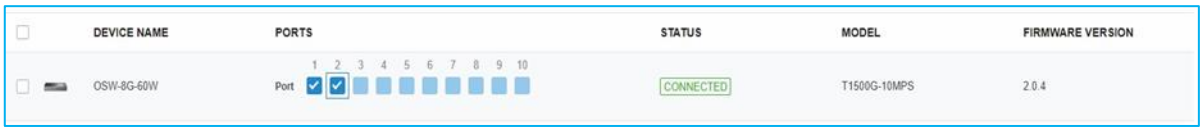


Authentication Protocol	Sélectionnez le protocole d'authentification pour l'échange de messages entre le commutateur et le serveur RADIUS. En tant que pont entre le client et le serveur RADIUS, le commutateur transmet les messages pour eux. Il utilise des paquets EAP pour échanger des messages avec le client et traite les messages selon le protocole d'authentification spécifié avant de les transférer au serveur RADIUS. PAP : les paquets EAP sont convertis en d'autres paquets de protocole (tels que RADIUS) et transmis au serveur RADIUS. EAP : les paquets EAP sont encapsulés dans d'autres paquets de protocole (tels que RADIUS) et transmis au serveur d'authentification. Pour utiliser ce mécanisme d'authentification, le serveur RADIUS doit prendre en charge les attributs EAP.
Authentication Type	Sélectionnez le type d'authentification 802.1X. Port basé : une fois qu'un client connecté au port est authentifié avec succès, d'autres clients peuvent accéder au réseau via le port sans authentification. MAC : les clients connectés au port doivent être authentifiés individuellement. Le serveur RADIUS distingue les clients par leurs adresses MAC.
VLAN Assignment	Cette fonctionnalité permet au serveur RADIUS d'envoyer dynamiquement les configurations VLAN au port. Une fois le port authentifié, le serveur RADIUS assigne le VLAN en fonction du nom d'utilisateur du client se connectant au port. Les mappages nom d'utilisateur à VLAN doivent déjà être stockés dans la base de données du serveur RADIUS. Cette fonctionnalité n'est disponible que lorsque le type d'authentification 802.1X est basé sur le port.
MAB	MAB (MAC Authentication Bypass) permet aux clients d'être authentifiés sans aucun logiciel client installé. MAB est utile pour authentifier les appareils sans capacité 802.1X comme les téléphones IP. Lorsque MAB est activé sur un port, le commutateur apprend automatiquement l'adresse MAC du client et envoie au serveur d'authentification un cadre de demande d'accès RADIUS avec l'adresse MAC du client comme nom d'utilisateur et mot de passe. Mab prend effet uniquement lorsque l'authentification 802.1X est activée sur le port.



Sélectionnez les ports pour activer l'authentification 802.1X ou MAB pour eux. Pour activer l'authentification 802.1X, cliquez sur les ports non sélectionnés. Les ports compatibles 802.1X seront marqués.

Pour activer MAB, cliquez sur les ports marqués avec ☑



Note

- Il n'est pas recommandé d'activer l'authentification 802.1X sur les ports de commutateur qui se connectent aux périphériques réseau sans capacité 802.1X comme le routeur et les AP.
- Le commutateur authentifie les clients câblés qui se connectent au port avec 802.1X activé. Et la passerelle authentifie les clients câblés qui se connectent au réseau avec Portal configuré. Les clients câblés doivent passer l'authentification Portal et 802.1X pour accéder à Internet lorsque les deux sont configurés.

4. 9. 3 MAC-Based Authentication

Aperçu

L'authentification mac permet ou interdit aux clients d'accéder aux réseaux sans fil en fonction des adresses MAC des clients. Dans cette méthode d'authentification, le contrôleur prend les adresses MAC des clients sans fil comme noms d'utilisateur et mots de passe pour l'authentification. Le serveur RADIUS authentifie les adresses MAC par rapport à sa base de données qui stocke les adresses MAC autorisées. Les clients peuvent accéder aux réseaux sans fil configurés avec l'authentification mac après avoir réussi l'authentification.

Note:

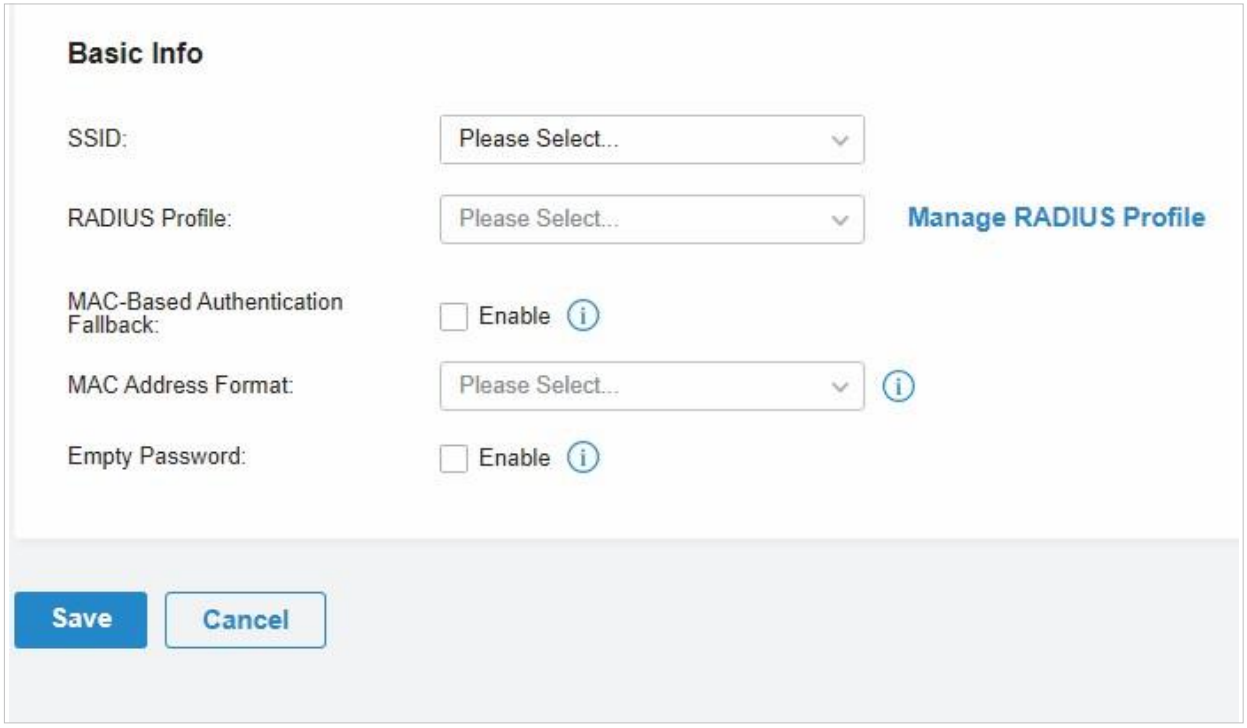
L'authentification mac et l'authentification portal peuvent authentifier les clients sans fil. Si les deux sont configurés sur un réseau sans fil, un client sans fil doit passer l'authentification mac d'abord, puis l'authentification du portail pour l'accès à Internet. Vous pouvez activer mac based authentication de secours pour permettre aux clients de contourner l'authentification mac, ce qui signifie que le client doit passer l'une ou l'autre des deux authentifications. Le client essaie d'abord l'authentification mac et est autorisé à essayer l'authentification du portail s'il échoue à l'authentification mac.

Configuration

1. Dans Settings > Authentication > MAC-Based Authentication. Cliquez pour activer l'authentification mac.



2. Dans les informations de base, sélectionnez les SSID, le profil RADIUS et d'autres paramètres requis. Reportez-vous au tableau suivant pour configurer les paramètres requis, puis cliquez sur Save.



SSID	Sélectionnez un ou plusieurs SSID pour que l'authentification mac prenne effet.
RADIUS Profile	Sélectionnez le profil RADIUS que vous avez créé. Si aucun profil RADIUS n'a été créé, cliquez à partir de la liste déroulante ou Manage RADIUS Profile pour en créer un. Le profil RADIUS enregistre les informations du serveur RADIUS qui agit comme serveur d'authentification pendant l'authentification mac.
MAC-Based Authentication Fallback	Pour le réseau sans fil configuré avec l'authentification mac et le portail, si vous activez cette fonctionnalité, un client sans fil doit passer une seule authentification. Le client essaie d'abord l'authentification mac et est autorisé à essayer l'authentification portal si elle échoue à l'authentification mac. Si vous désactivez cette fonctionnalité par défaut, un client sans fil doit passer à la fois l'authentification MAC et l'authentification du portail pour l'accès à Internet, et sera refusé en cas d'échec de l'une ou l'autre des authentifications.

MAC Address Format	Sélectionnez le format d'adresse MAC des clients que le contrôleur utilise pour l'authentification. Configurez ensuite les adresses MAC dans le format spécifié en tant que noms d'utilisateur pour les clients sur le serveur RADIUS.
Empty Password	Cliquez pour autoriser un mot de passe vide pour l'authentification mac. Avec cette option désactivée, le mot de passe sera le même que le nom d'utilisateur.

4. 9. 4 Profil RADIUS

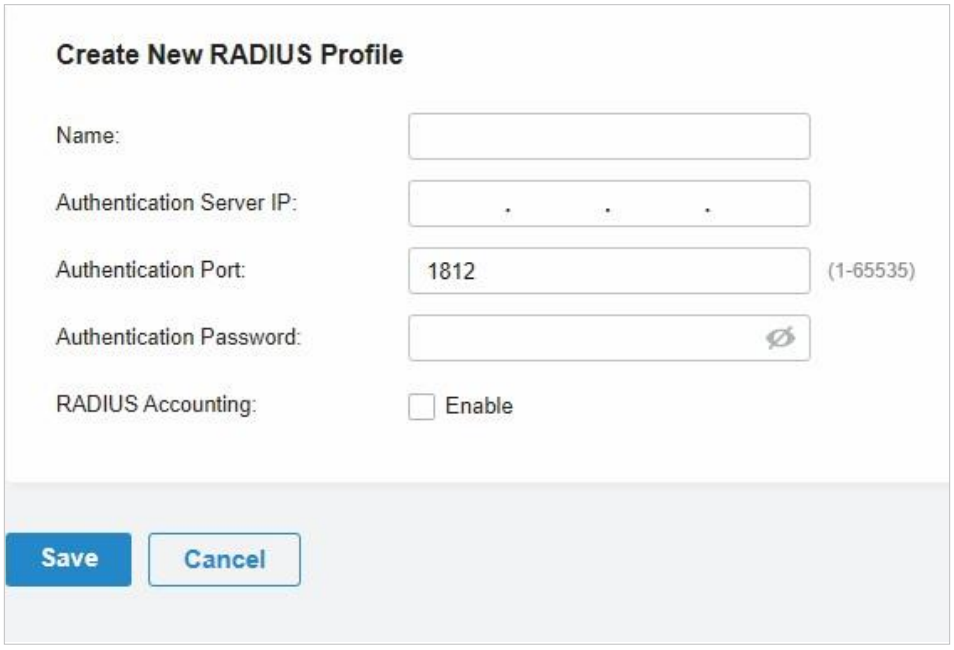
Aperçu

RADIUS (Remote Authentication Dial In User Service) est un protocole client/serveur qui répond aux besoins AAA (Authentification, autorisation et comptabilité) dans les environnements informatiques modernes.
Dans les services d'authentification tels que 802.1X, Portal et MAC,les appareils Omada fonctionnent en tant que clients de RADIUS pour transmettre les informations utilisateur aux serveurs RADIUS désignés. Un serveur RADIUS gère une base de données qui stocke les informations d'identité des utilisateurs légaux. Il authentifie les utilisateurs par rapport à la base de données lorsque les utilisateurs demandent d'accéder au réseau et leur fournit des services d'autorisation et de comptabilité.

Un profil RADIUS enregistre vos paramètres personnalisés d'un serveur RADIUS. Après avoir créé un profil RADIUS, vous pouvez l'appliquer à plusieurs stratégies d'authentification comme Portal et 802.1X, vous permettant d'économiser la saisie répétée des mêmes informations.

Configuration

1. Dans Settings > Authentication > RADIUS Profile. Cliquez sur + Create New RADIUS Profile



3. Entrez les informations des serveurs RADIUS. Reportez-vous au tableau suivant pour configurer les paramètres requis, puis cliquez sur Save.

Name	Entrez un nom pour identifier le profil RADIUS.
Authentication Server IP	Entrez l'adresse IP du serveur d'authentification.
Authentication Port	Entrez le port de destination UDP sur le serveur d'authentification pour les demandes d'authentification.
Authentication Password	Entrez le mot de passe qui sera utilisé pour valider la communication entre les appareils Omada et le serveur d'authentification RADIUS.
RADIUS Accounting	Cliquez sur la case à cocher pour activer RADIUS Accounting pour répondre aux besoins de facturation. Cette fonctionnalité n'est disponible que pour les EAP Omada avec Portal pour tenir compte des clients sans fil.
Interim Update	Cliquez sur la case à cocher pour activer la mise à jour intérimaire. Par défaut, le processus de comptabilité RADIUS n'a besoin que de démarrer et d'arrêter les messages sur le serveur de comptabilité RADIUS. Une mise à jour provisoire est activée, les appareils Omada envoient périodiquement une mise à jour Le paquet de demande de comptabilité RADIUS contenant une valeur « mise à jour intérimaire ») sur le serveur RADIUS. Une mise à jour intérimaire met à jour la durée de la session de l'utilisateur et l'utilisation actuelle des données.
Interim Update Interval	Entrez un intervalle approprié entre les mises à jour de la durée de la session des utilisateurs et l'utilisation actuelle des données.
Accounting Server IP	Entrez l'adresse IP du serveur de comptabilité RADIUS.
Accounting Port	Entrez le port de destination UDP sur le serveur RADIUS pour les demandes comptables.
Accounting Password	Entrez le mot de passe qui sera utilisé pour valider la communication entre les appareils Omada et le serveur comptable RADIUS.

4. 10 Services

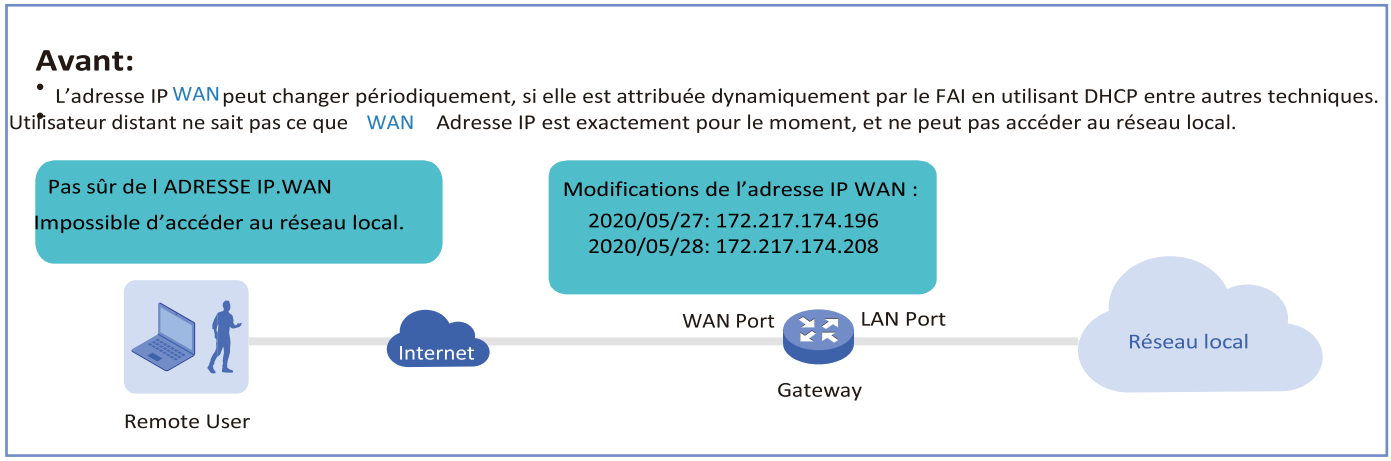
Les services fournissent des services réseau pratiques et facilitent la gestion du réseau. Vous pouvez configurer des serveurs ou des terminaux dans DDNS, SNMP, UPnP et SSH, planifier les périphériques dans la planification de redémarrage et la planification PoE et exporter les journaux en cours d'exécution dans Export Data.

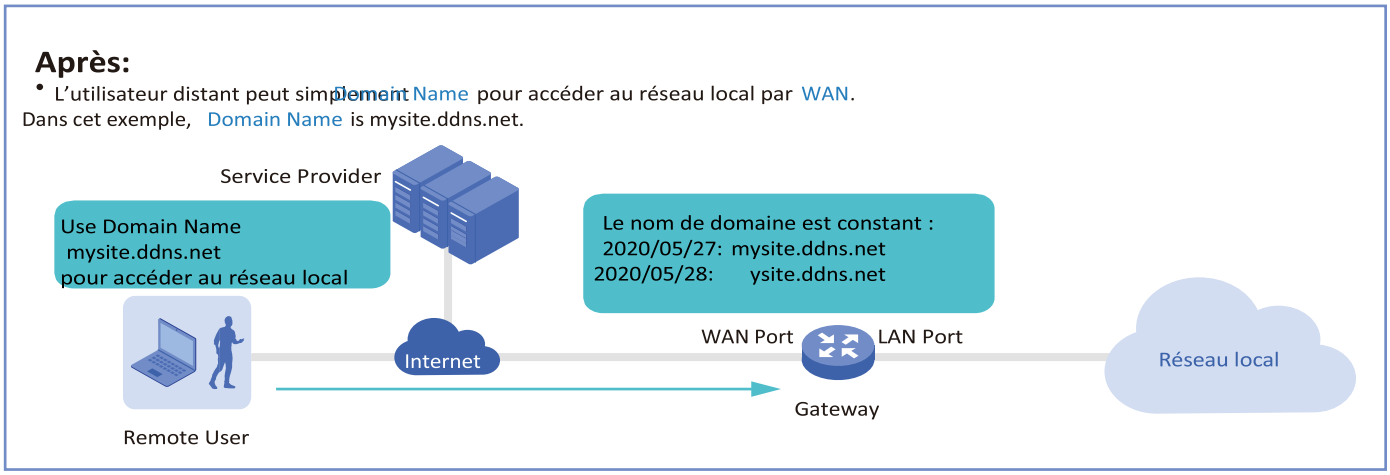
4. 10. 1 Dynamic DNS

Aperçu

L'adresse IP WAN de votre passerelle peut changer périodiquement car votre FAI utilise généralement DHCP parmi d'autres techniques. C'est là que Dynamic DNS entre en jeu. Le DNS dynamique attribue un nom de domaine fixe au port WAN de votre passerelle, ce qui facilite l'accès de vos utilisateurs distants à votre réseau local via le port WAN.

Illustrons comment Dynamic DNS fonctionne avec les chiffres suivants.



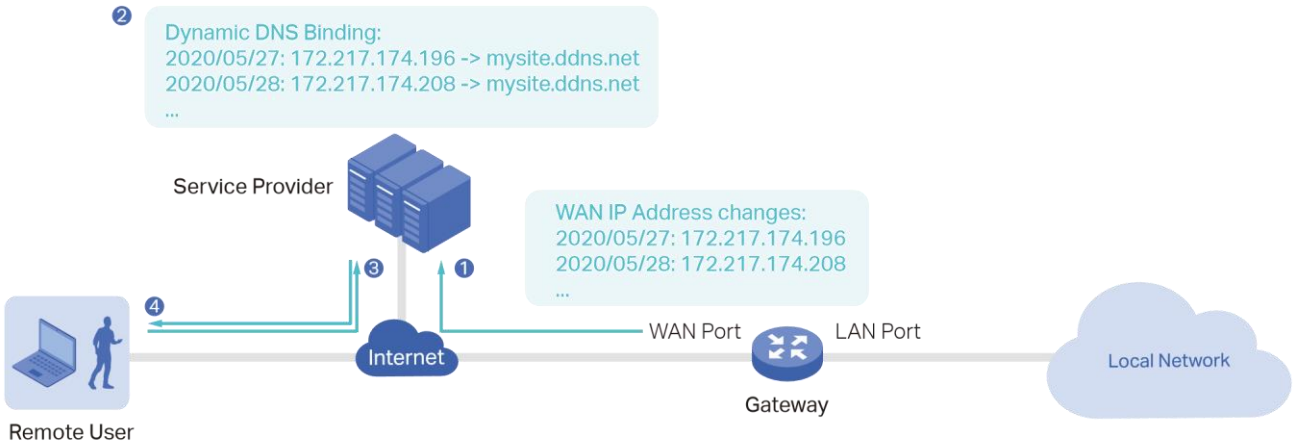


Prerequisite:

- Choose one Service Provider from the four that the controller supports, i.e. DynDNS, No-IP, Peanuthull, Comexe.
- Register at your Service Provider, then you get your Username and Password.
- Get your Domain Name from your Service Provider.

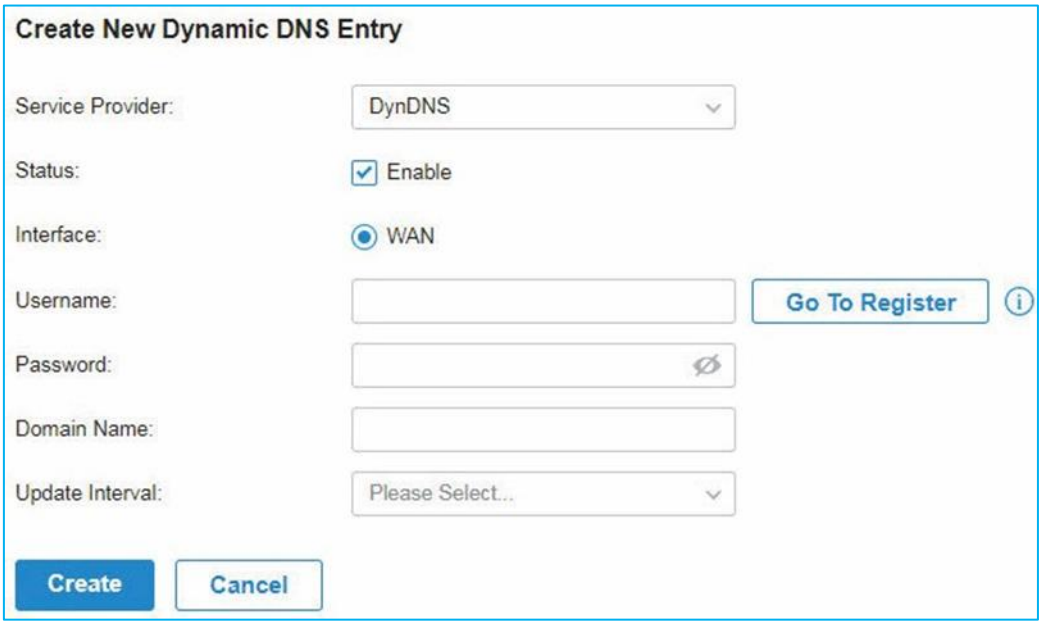
How Dynamic DNS works:

1. Gateway informs Service Provider of WAN IP Address.
2. Service Provider binds WAN IP Address with Domain Name and keeps it updated as WAN IP Address changes.
3. Remote User requests for WAN IP Address by sending Domain Name to Service Provider.
4. Service Provider replies with WAN IP Address, which Remote User actully uses to access Local Network through WAN Port.



Configuration

Dans Settings > Services > Dynamic DNS. Cliquez sur + Create New Dynamic DNS Entry, to charger la page suivante. Configurer les paramètres et cliquer sur Create.



Status	Activer ou désactiver l'entrée DNS dynamique.
Service Provider	Sélectionnez votre fournisseur de services avec lequel travaille Dynamic DNS
Interface	Sélectionnez le port WAN auquel l'entrée DNS dynamique s'applique.
Username	Entrez votre nom d'utilisateur pour le fournisseur de services. Si vous ne vous êtes pas inscrit au fournisseur de services, cliquez sur Go To Register.
Password	Entrez votre mot de passe pour le fournisseur de services.
Domain Name	Entrez le nom de domaine fourni par votre fournisseur de services. Les utilisateurs distants peuvent utiliser le nom de domaine pour accéder à votre réseau local via le port WAN.
Update Interval	Sélectionnez la fréquence à laquelle l'adresse IP WAN est mise à jour avec le nom de domaine.

4. 10. 2 SNMP

Aperçu

SNMP (Simple Network Management Protocol) vous fournit une méthode pratique et flexible pour configurer et surveiller les périphériques réseau. Une fois que vous avez configuré SNMP pour les périphériques, vous pouvez les gérer de manière centralisée avec un NMS (Station de gestion réseau).

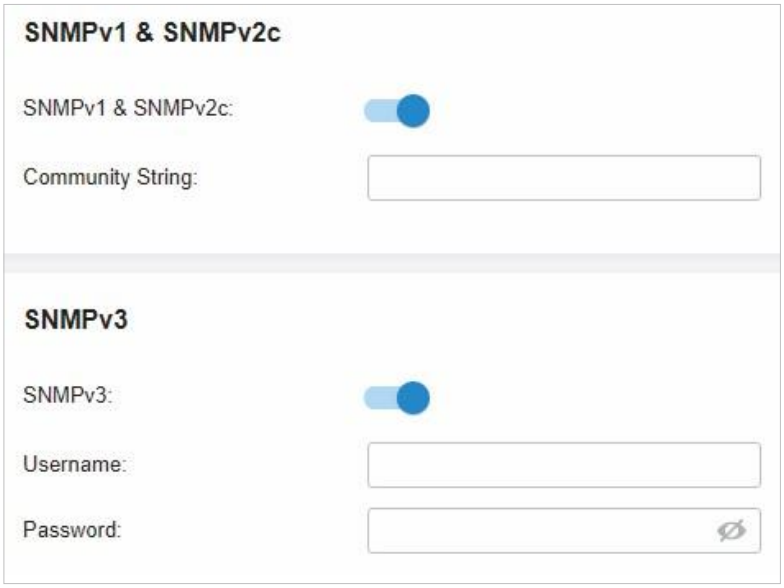
Le contrôleur prend en charge plusieurs versions SNMP, y compris SNMPv1, SNMPv2c et SNMPv3.

Note:

Si vous utilisez un NMS pour gérer les périphériques gérés par le contrôleur, vous ne pouvez lire mais pas écrire des objets SNMP.

Configuration

Dans Settings > Services > SNMP et configurer les paramètres. Cliquez ensuite sur Apply.



SNMPv1 & SNMPv2c	Activez ou désactivez SNMPv1 et SNMPv2c globalement.
Community String	Avec SNMPv1 & SNMPv2c activé, spécifiez la chaîne communautaire, qui est utilisée comme mot de passe pour que votre NMS accède à l'agent SNMP. Vous devez configurer la chaîne communautaire en fonction de votre NMS.
SNMPv3	Activer ou désactiver SNMPv3 globalement.
Username	Avec SNMPv3 activé, spécifiez le nom d'utilisateur de votre NMS pour accéder à l'agent SNMP. Vous devez configurer le nom d'utilisateur en fonction de votre NMS.
Password	Avec SNMPv3 activé, spécifiez le mot de passe pour que votre NMS accède à l'agent SNMP. Vous devez configurer le mot de passe correspondant sur votre NMS.

4. 10. 3 UPnP

Aperçu

UPnP (Universal Plug and Play) est essentiel pour les applications telles que les jeux multi-joueurs, les connexions peer-to-peer, la communication en temps réel (comme la VoIP ou la conférence téléphonique) et l'assistance à distance, etc. Avec l'aide d'UPnP, le trafic entre les points de terminaison de ces applications peut passer librement la passerelle, réalisant ainsi des connexions transparentes.

Configuration

Dans Settings > Services > UPnP. Activez UPnP globalement et configurez les paramètres. Cliquez ensuite sur Apply.



Interface	Sélectionnez le port WAN où UPnP prend effet.
Networks	Sélectionnez l'interface LAN où UPnP prend effet.

4. 10. 4 SSH

Aperçu

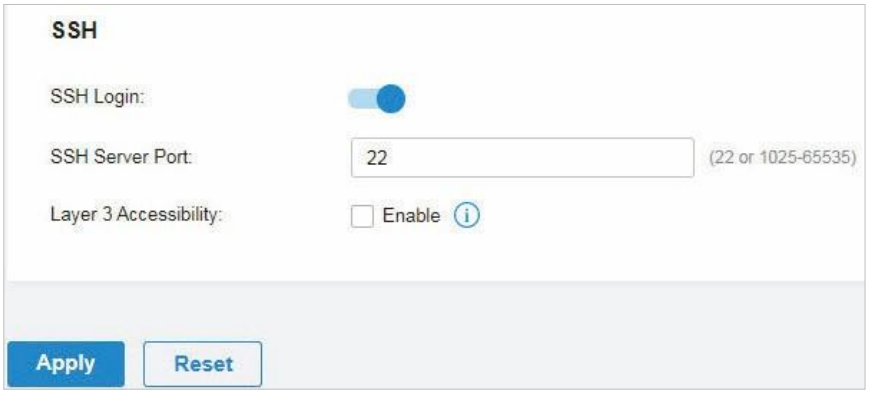
SSH (Secure Shell) vous fournit une méthode permettant de configurer et de surveiller en toute sécurité les périphériques réseau via une interface utilisateur de ligne de commande sur votre terminal SSH.

Note:

Si vous utilisez un terminal SSH pour gérer les périphériques gérés par le contrôleur, vous ne pouvez obtenir que le privilège Utilisateur.

Configuration

Dans Settings > Services > SSH. Activez la connexion SSH globalement et configurez les paramètres. Cliquez ensuite sur Apply.



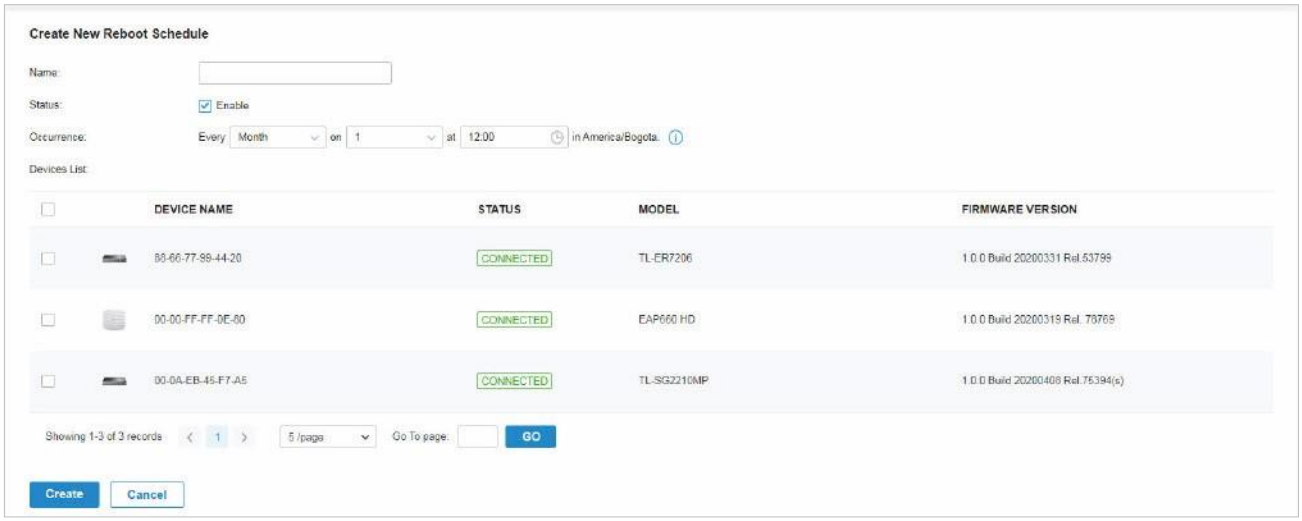
SSH Server Port	Spécifiez le port SSH Sever que vos périphériques réseau utilisent pour les connexions SSH. Vous devez configurer le port serveur SSH en fonction de votre terminal SSH.
Layer 3 Accessibility	Avec cette fonctionnalité activée, le terminal SSH d'un sous-réseau différent peut accéder à vos appareils via SSH. Avec cette fonctionnalité désactivée, seul le terminal SSH du même sous-réseau peut accéder à vos appareils via SSH.

4. 10. 5 Planification de redémarrage

Aperçu

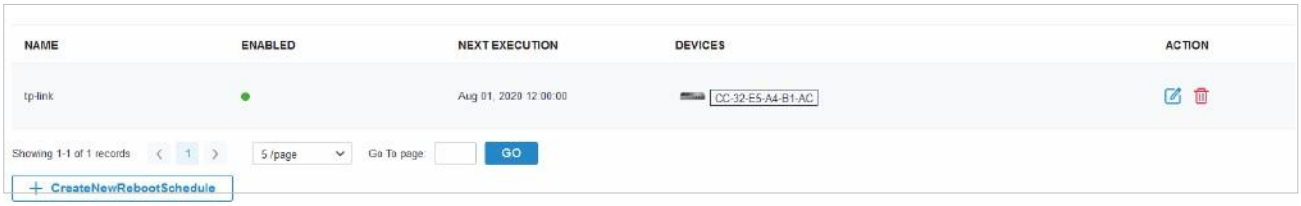
La planification de redémarrage peut faire redémarrer vos appareils périodiquement en fonction de vos besoins. Vous pouvez configurer la planification de redémarrage avec souplesse en créant plusieurs entrées de la planification de redémarrage.

1. Dans Settings > Services > Reboot Schedule. Cliquez sur + Create New Reboot Schedule pour charger la page suivante et configurer les paramètres.



Name	Entrez le nom pour identifier l'entrée Planification du redémarrage.
Status	Activez ou désactivez l'entrée Planification du redémarrage.
Occurrence	Spécifier la date et l'heure du redémarrage des périphériques.
Devices List	Sélectionnez les périphériques auxquels la planification de redémarrage s'applique.

Cliquez sur Create . La nouvelle entrée Planification de redémarrage est ajoutée à la table. You can click pour modifier l'entrée. Vous pouvez cliquer sur pour supprimer l'entrée.



4. 10. 6 programmation Horaire PoE

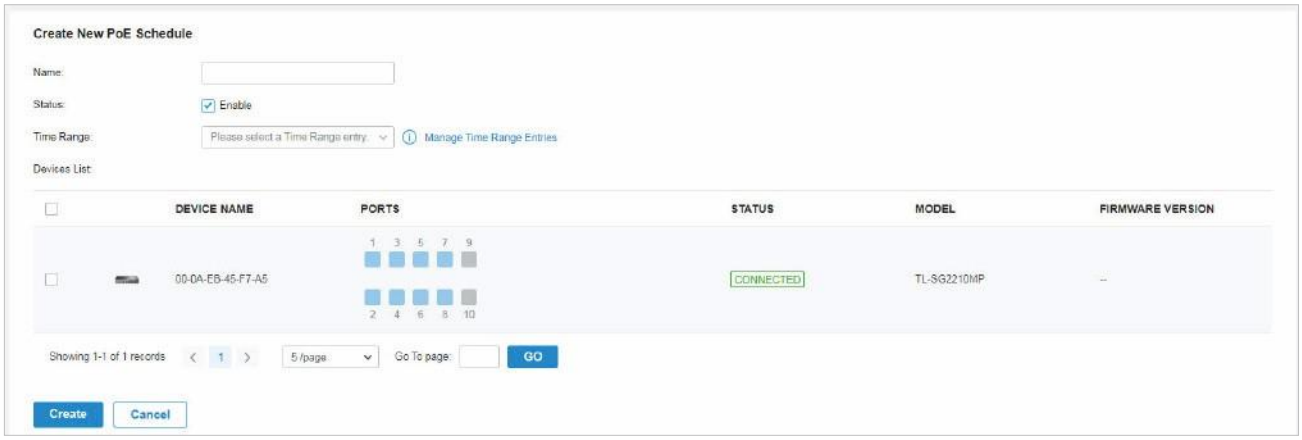
Aperçu

PoE Schedule peut rendre les périphériques PoE qui sont connectés à votre PoE commute l'alimentation et ne fonctionnent que dans la période de temps spécifique que vous le souhaitez. Vous pouvez configurer la planification PoE avec souplesse en créant plusieurs entrées de la planification PoE.

Configuration

1.

Dans Settings > Services > PoE Schedule. Cliquez sur + Create New PoE Schedule pour charger la page suivante et configurer les paramètres.



Name	Entrez le nom pour identifier l'entrée de l'annexe PoE.
Status	Activer ou désactiver l'entrée de la planification PoE.
Time Range	Sélectionnez la plage de temps lorsque les périphériques PoE fonctionnent. Vous pouvez créer une entrée de plage de temps en cliquant sur + Create New Time Range Entrée à partir de la liste déroulante de Time Range. Pour plus de détails, reportez-vous à Profiles.
Devices List	Sélectionnez les commutateurs PoE et les ports PoE auxquels l'annexe PoE s'applique. Vos appareils PoE connectés aux ports sélectionnés des commutateurs fonctionnent selon l'horaire PoE.

. 2. Cliquez sur Create La nouvelle entrée de l'annexe PoE est ajoutée à la table.

Vous pouvez cliquer sur

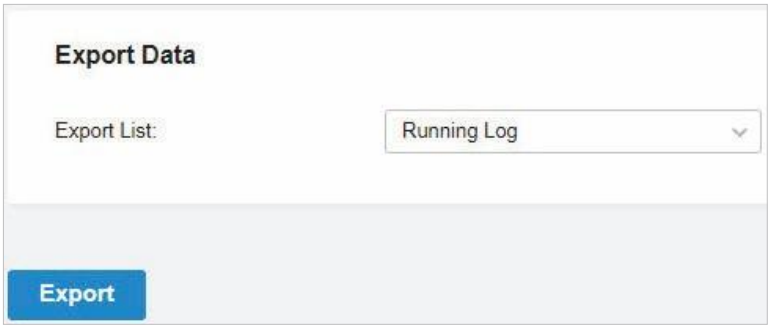


4. 10. 7 Export Data

Aperçu

Vous pouvez exporter des données pour surveiller ou déboguer vos appareils.

Dans Settings > Services > Export Data. Sélectionnez le type de données dans la liste d'exportation, puis cliquez sur Export.



Export List	Running Log: Exporter le journal d'exécution quotidien du contrôleur.

5

Configurer le contrôleur SDN Omada

Les paramètres du contrôleur contrôlent l'apparence et le comportement du contrôleur et fournissent des méthodes de sauvegarde, de restauration et de migration de données :

- Gérer le contrôleur
- Gérer votre contrôleur à distance via l'accès cloud
- Maintenance
- Migration
- Sauvegarde automatique

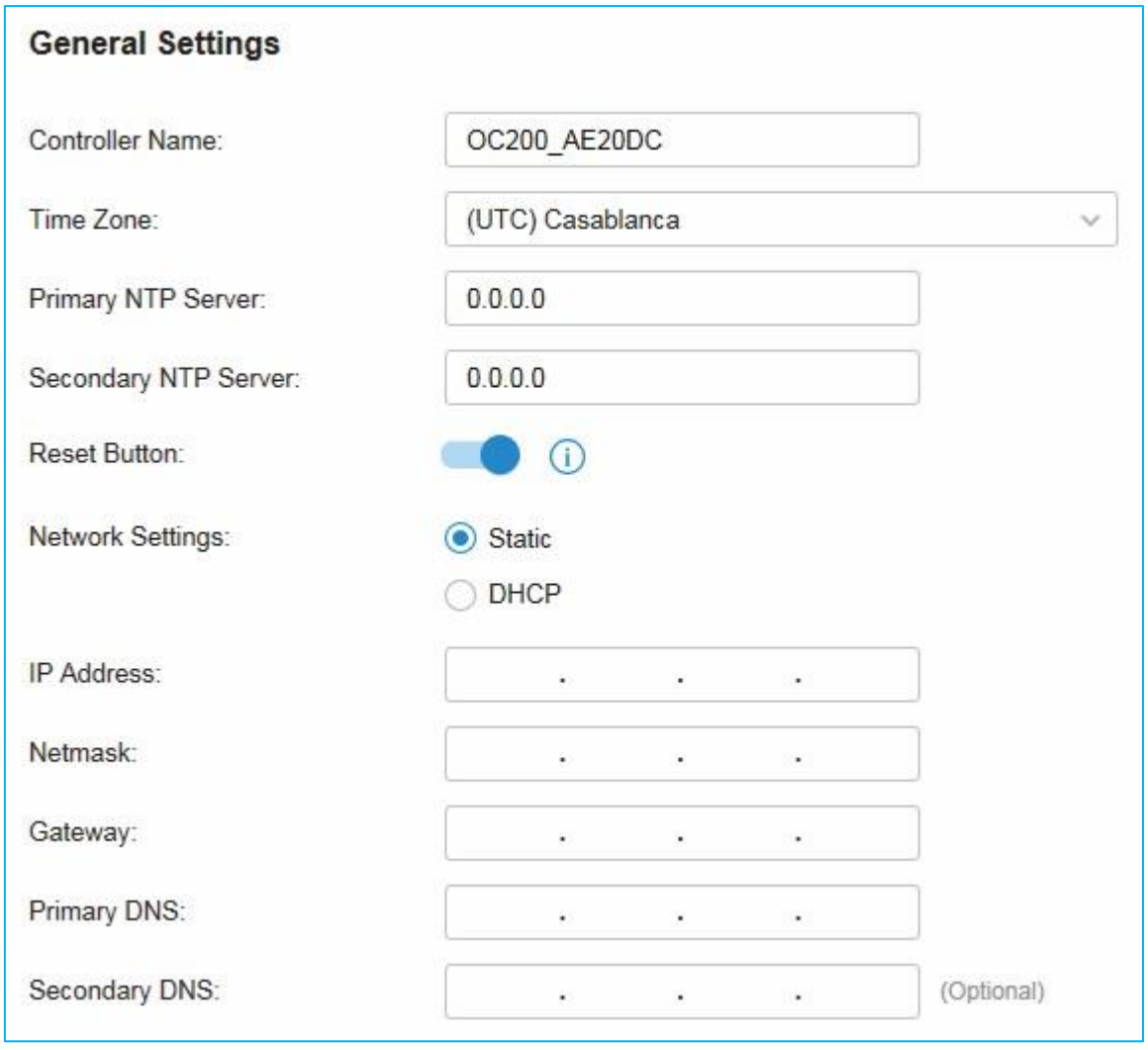
5. 1 Gérer le contrôleur

5. 1. 1 Paramètres généraux

Configuration

Dans Settings > Controller. dans General Settings, configurer les paramètres et cliquer sur Save.

- **Pour le contrôleur matériel Omada**



Controller Name	Spécifier le nom du contrôleur pour identifier le contrôleur.
Time Zone	Sélectionnez le fuseau horaire du contrôleur en fonction de votre région. Pour les paramètres et les statistiques du contrôleur, l'heure s'affiche en fonction du fuseau horaire.

Primary NTP Server/ Secondary NTP Server	Entrez l'adresse IP du serveur NTP (Network Time Protocol) principal et secondaire. Les serveurs NTP affectent du temps réseau au contrôleur.
Reset Button	Avec cette fonctionnalité activée, le contrôleur peut être réinitialisé via le bouton de réinitialisation.
Network Settings	Sélectionnez une façon pour le contrôleur d'obtenir des paramètres IP. Static: Vous devez spécifier l' IP address, Netmask, Gateway, Primary DNS, Et Secondary DNS pour le contrôleur. DHCP: Le contrôleur a obtenu des paramètres IP à partir du serveur DHCP. Si le contrôleur ne parvient pas à obtenir les paramètres IP du serveur DHCP, Fallback IP Address et le Fallback Netmask.

■ **Pour Omada Software Controller / Omada Cloud-Based Controller**



Controller Name	Spécifiez le nom du contrôleur pour identifier le contrôleur.
Time Zone	Sélectionnez le fuseau horaire du contrôleur en fonction de votre région. Pour les paramètres et les statistiques du contrôleur, le temps s'affiche en fonction du fuseau horaire.

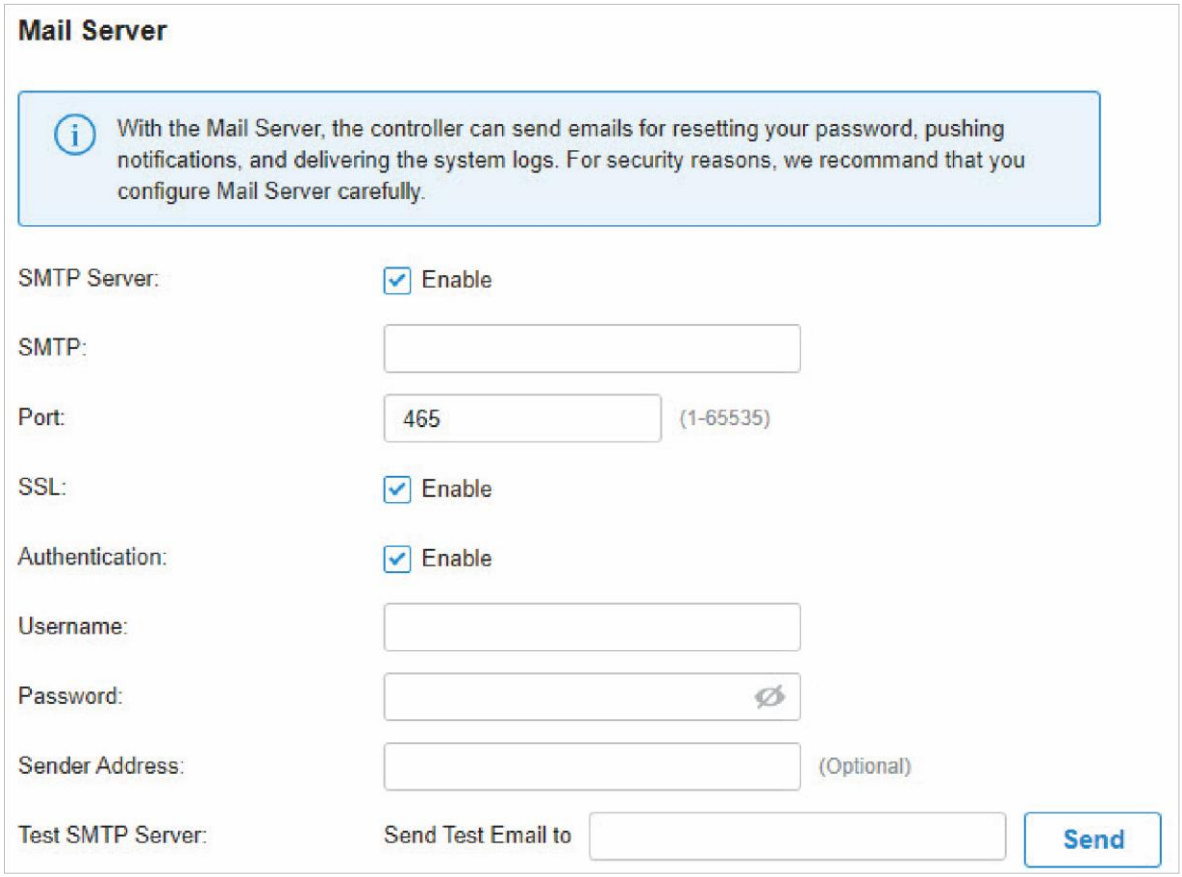
5. 1. 2 Serveur de messagerie

Aperçu

Avec le serveur de messagerie, le contrôleur peut envoyer des e-mails pour réinitialiser votre mot de passe, pousser les notifications et livrer les journaux système. La fonctionnalité Serveur de messagerie fonctionne avec le service SMTP (Simple Mail Transfer Protocol) fourni par un fournisseur de services de messagerie.

Configuration

1. Connectez-vous à votre compte de messagerie et activez le service SMTP (Simple Mail Transfer Protocol). Pour plus de détails, consultez les instructions de votre fournisseur de services de messagerie.
2. Allez Settings > Controller. In Mail Server, activer SMTP Server et configurer les paramètres. Cliquez ensuite sur Save.



SMTP	Entrez l'URL ou l'adresse IP du serveur SMTP selon les instructions du fournisseur de services de messagerie.
Port	Configurez le port utilisé par le serveur SMTP selon les instructions du fournisseur de services de messagerie.
SSL	Activez ou désactivez SSL selon les instructions du fournisseur de services de messagerie. SSL (Secure Sockets Layer) est utilisé pour créer un lien chiffré entre le contrôleur et le serveur SMTP.
Authentication	Activer ou désactiver l'authentification selon les instructions du fournisseur de services de messagerie. Si l'authentification est activée, le serveur SMTP nécessite le nom d'utilisateur et le mot de passe pour l'authentification.
Username	Lorsque l'authentification est activée, entrez votre adresse e-mail comme nom d'utilisateur.
Password	Lorsque l'authentification est activée, entrez le code d'authentification comme mot de passe, qui est fourni par le fournisseur de services de messagerie lorsque vous activez le service SMTP.

Sender Address	(Facultatif) Spécifiez l'adresse d'expéditeur de l'e-mail. Si vous le laissez vide, le contrôleur utilise votre adresse e-mail comme adresse de l'expéditeur.

5. 1. 3 Conservation des données d'historique

Aperçu

Avec la conservation des données historiques, vous pouvez spécifier comment le contrôleur conserve ses données.

Configuration

Dans Settings > Controller. allez dans History Data Retention, configure the parameters and click Save.

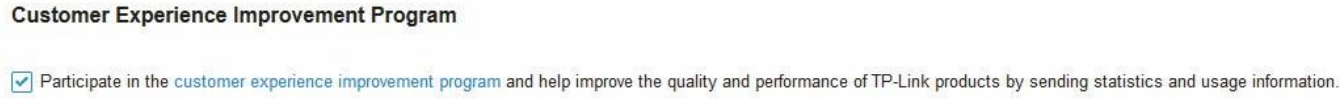


Data Retention	Sélectionnez la durée pendant la quoi le contrôleur conserve ses données. Toutes les données d'historique au-delà de la plage de temps sont supprimées.
Collect Clients' History Data	Grâce à l'activation des données historiques des clients, les données d'historique des clients sont incluses dans celle du contrôleur.

5. 1. 4 Programme d'amélioration de l'expérience client

Configuration

Cliquez sur la case à cocher si vous acceptez de participer au programme d'amélioration de l'expérience client et aidez à améliorer la qualité et les performances des produits TP-Link en envoyant des statistiques et des informations d'utilisation.



5. 1. 5 Certificat HTTPS

Aperçu

Si vous avez attribué un nom de domaine au contrôleur pour la connexion, afin d'éliminer le message d'erreur « certificat non approuvé » qui apparaîtra dans le processus de connexion, vous pouvez importer le certificat SSL correspondant et la clé privée ici. Le certificat et la clé privée sont délivrés par l'autorité du certificat.

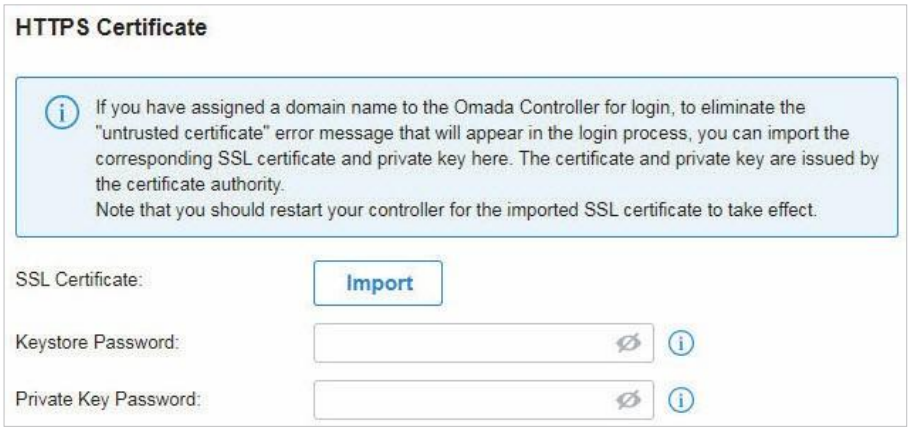
Note:

- La configuration du certificat HTTPS n'est disponible que pour omada Software Controller et Omada Hardware Controller.

1. Vous devez redémarrer votre contrôleur pour que le certificat SSL importé prenne effet.

Configuration

Dans Settings > Controller. In HTTPS Certificate, importer votre certificat SSL et configurer les paramètres. Ensuite, Cliquez sur Save.



Keystore Password	Entrez le mot de passe keystore si votre certificat SSL a le mot de passe keystore. Sinon, laissez-le vide.
Private Key Password	Entrez le mot de passe de clé privée si votre certificat SSL a le mot de passe de clé privée. Sinon, laissez-le vide.

5. 1. 6 Access Port Config

Aperçu

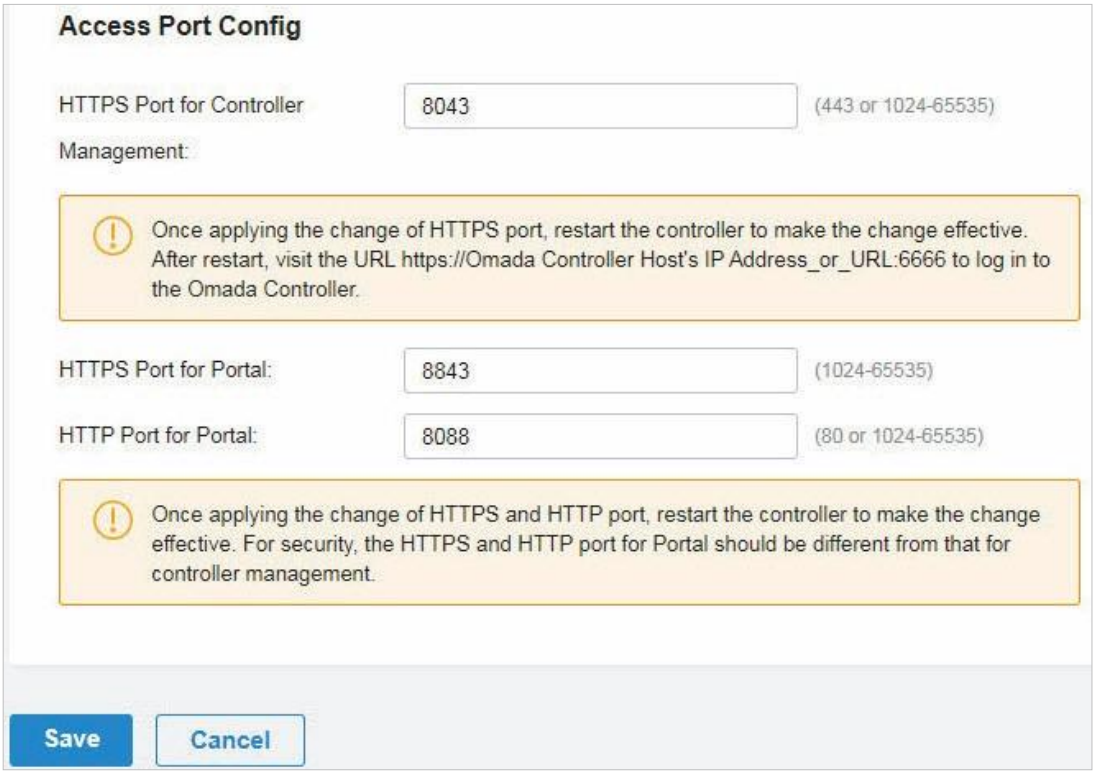
Avec Access Port Config, vous pouvez spécifier le port utilisé par le contrôleur pour la gestion et le portail.

Note:

- Access Port Config n'est disponible que sur Omada Software Controller et Omada Hardware Controller.
- Une fois que vous appliquez le changement de port HTTPS et HTTP, redémarrez le contrôleur pour rendre la modification efficace.
- Pour la sécurité, le port HTTPS et HTTP pour Potal doit être différent de celui de la gestion du contrôleur.

Configuration

Dans Settings > Controller. allez dans Access Port Config, configurer les paramètres et cliquer sur Save.



HTTPS Port for Controller Management	Spécifiez le port HTTPS utilisé par le contrôleur pour la gestion. Après avoir mis le port, Vous pouvez visiter l'adresse IP ou l'URL de l'hôte du contrôleur d'Omada]:[Port] pour vous connecter au contrôleur Omada.
HTTPS Port for Portal	Spécifier le port HTTPS utilisé par le contrôleur pour Portal.
HTTP Port for Portal	Spécifier le port HTTP utilisé par le contrôleur pour Portal.

5. 2 Gérer votre contrôleur à distance via l'accès cloud

Aperçu

Avec Cloud Access, il est pratique pour vous de gérer votre contrôleur de n'importe où, tant que vous avez accès à Internet.

Configuration

Pour gérer votre contrôleur de n'importe où, procédez comme suit :

1. Préparez votre contrôleur pour l'accès au cloud

■ **Pour Le contrôleur logiciel Omada / Contrôleur matériel Omada:**

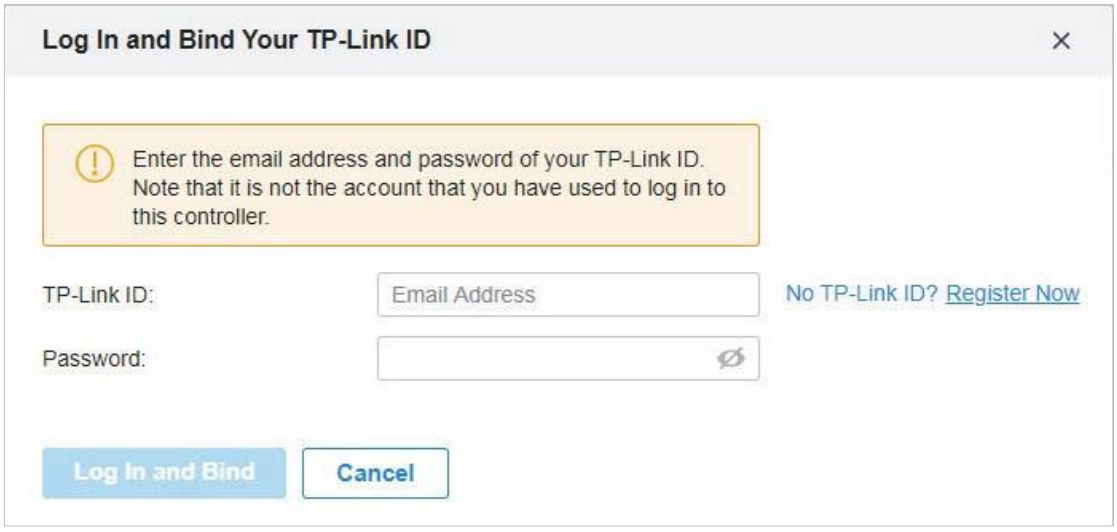
Note:

- Avant de commencer, assurez-vous que votre hôte de contrôleur logiciel Omada ou votre contrôleur matériel **Omada a accès à Internet.**
- Si vous avez activé l'accès au cloud et lié votre ID TP-Link dans l'Assistant Configuration rapide, sautez cette étape.

1) Allez dans Settings **>** Cloud Access. Activer l'accès au cloud.



2) Entrez votre IDENTIFIANT TP-Link et votre mot de passe. Cliquez ensuite sur Log In and Bind.



■ **Pour le contrôleur cloud d'Omada**

Votre contrôleur cloud Omada est basé sur le Cloud, il est donc naturellement accessible via le service Cloud. Aucune préparation supplémentaire n'est nécessaire.

3. Accédez à votre contrôleur via le service Cloud

Allez dans Omada Cloud et connectez-vous avec votre IDENTIFIANT TP-Link et votre mot de passe. Une liste de contrôleurs qui ont been

Lié à votre ID TP-Link s'affiche. Cliquez ensuite sur Launch pour gérer le contrôleur.



5. 3 Maintenance

5. 3. 1 État du contrôleur

Allez dans Settings > Maintenance. In Controller Status, vous pouvez afficher les informations et l'état liés au contrôleur.



Controller Name	Affiche le nom du contrôleur, qui identifie le contrôleur. Vous pouvez spécifier le nom du contrôleur dans General Settings.
MAC Address	Affiche l'adresse MAC du contrôleur.
System Time	Affiche l'heure du système du contrôleur. L'heure du système est basée sur le fuseau horaire que vous configurez dans General Settings.
Uptime	Affiche la durée de travail du contrôleur.
Controller Version	Affiche la version logicielle du contrôleur.

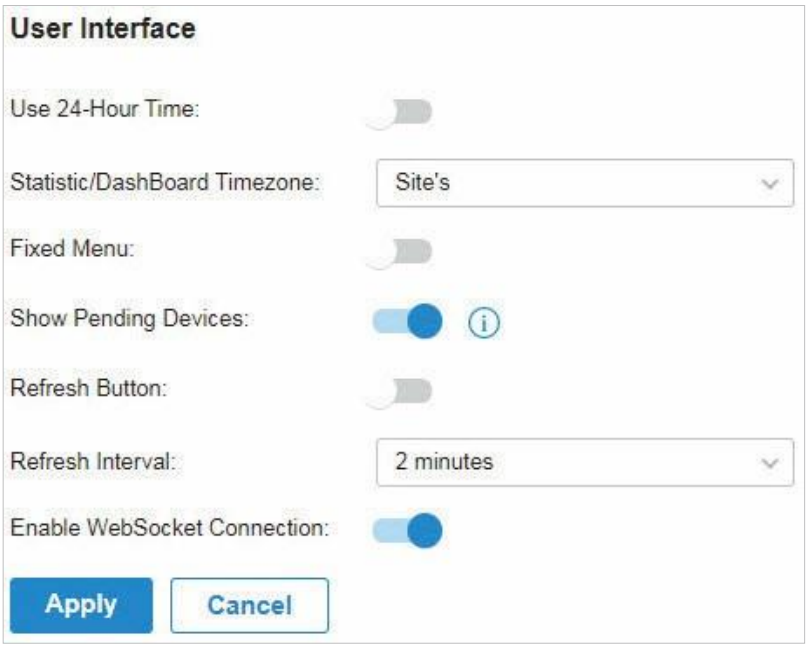
5. 3. 2 Interface utilisateur

Aperçu

Vous pouvez personnaliser les paramètres d'interface utilisateur du contrôleur en fonction de vos préférences.

Configuration

Allez dans Settings > Maintenance. dans User Interface, configurer les paramètres et cliquer sur Apply.



Use 24-Hour Time	Avec l'utilisation 24 heures dans l'heure activée, le temps s'affiche dans un format de 24 heures. Avec l'heure d'utilisation 24 Heures désactivée, le temps s'affiche dans un format de 12 heures.
Statistic/Dashboard Timezone	Sélectionnez le fuseau horaire sur lequel l'heure des statistiques et le tableau de bord est basé sur. Site's: Le fuseau horaire du site est défini dans Configuration du site du site correspondant. Browser's: Le fuseau horaire du navigateur est synchronisé avec la configuration du navigateur. Controller's: Le fuseau horaire du contrôleur est défini dans paramètres généraux du contrôleur. UTC: UTC (Coordinated Universal Time) est la norme de temps courante à travers le monde.
Fixed Menu	Avec menu fixe activé, les icônes de menu sont fixes et n'invitent pas les textes de menu lorsque votre souris les survole.
Show Pending Devices	Avec cette option activée, les périphériques en attente s'affichent et vous pouvez déterminer s'ils doivent les adopter. Avec cette option désactivée, ils ne seront pas affichés, donc vous ne pouvez pas adopter de nouveaux appareils.
Refresh Button	Activer ou désactiver le bouton Actualiser dans le coin supérieur droit de la page de configuration.
Refresh Interval	Sélectionnez la fréquence à laquelle le contrôleur actualise automatiquement les données affichées sur la page.

Enable WebSocket Connection	Avec la connexion WebSocket activée, le contrôleur met à jour en temps réel une partie de ses données sur l'interface Web, qui est transmise à l'aide du service WebSocket, de sorte que vous n'avez pas besoin de les actualiser manuellement.

5. 3. 3 Backup & Restore

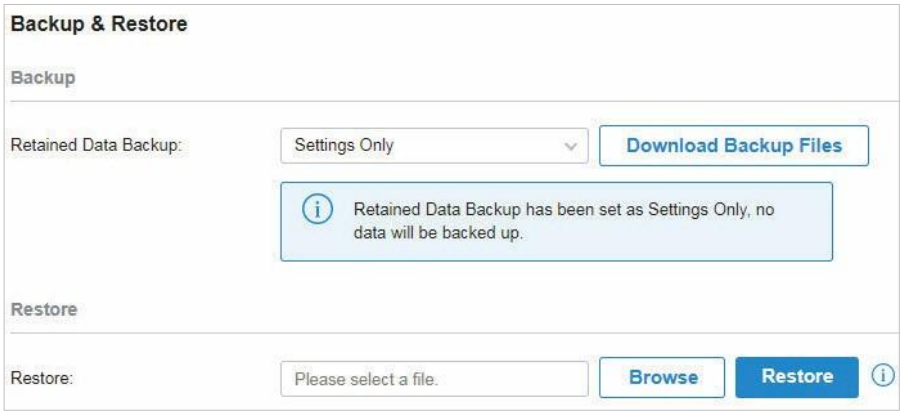
Aperçu

Vous pouvez sauvegarder la configuration et les données de votre contrôleur pour éviter toute perte d'informations importantes. Si nécessaire, restaurer le contrôleur à un état précédent à l'aide du fichier de sauvegarde.

Configuration

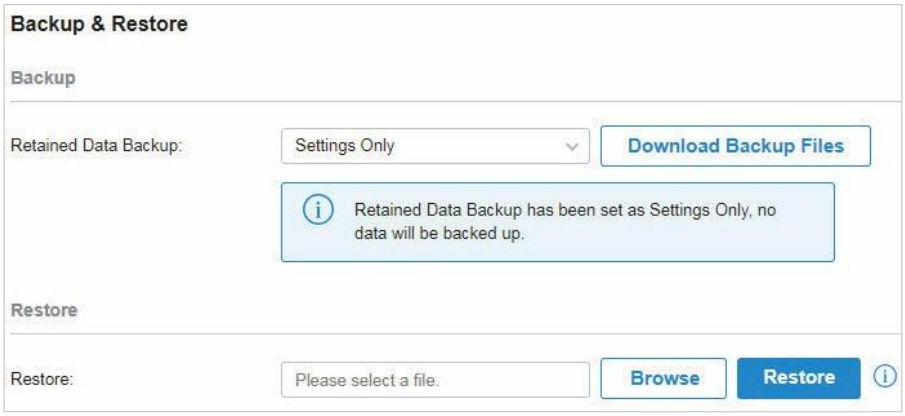
- **Backup**

Allez dans Settings > Maintenance. In Backup & Restore, sélectionnez la plage d'heure dans le menu déroulant de Sauvegarde de données conservées. Seules la configuration et les données dans la plage de temps sont sauvegardées. Si vous sélectionnez Paramètres uniquement, seule la configuration (aucune donnée) est sauvegardée. Cliquez su rDownload Backup Files pour télécharger le fichier de sauvegarde sur votre ordinateur.



- **Restore**

Allez dans Settings > Maintenance. In Backup & Restore section, Cliquez sur Browse et sélectionnez un fichier de sauvegarde à partir de votre ordinateur. Cliquez sur Restore.



5. 4 Migration

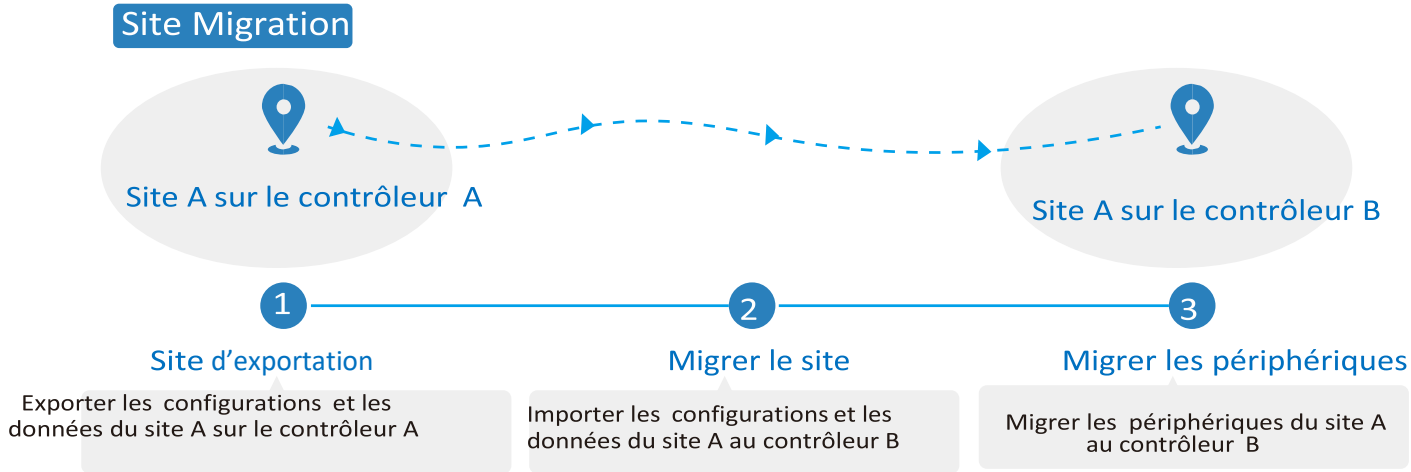
Les services de migration permettent aux utilisateurs de migrer les configurations et les données vers n'importe quel autre contrôleur. Les services de migration incluent Site Migration et Controller Migration, couvrant tous les besoins de migrer à la fois un seul site et l'ensemble du contrôleur.

5. 4. 1 Site Migration

Aperçu

La migration de site permet aux administrateurs d'exporter un site du contrôleur actuel vers tout autre contrôleur qui possède la même version. Toutes les configurations et données du site seront migrées vers le contrôleur cible.

Le processus de migration des configurations et des données d'un site vers un autre contrôleur peut être résumé en trois étapes : Exporter le site, migrer le site et migrer les périphériques.



Étape1 : Site d'exportation

Exportez les configurations et les données du site à migrer en tant que fichier de sauvegarde.

Étape2 : Migrer le site

Dans le contrôleur cible, importez le fichier de sauvegarde du site d'origine.

Étape3 : Migrer les périphériques

Migrez les périphériques qui se trouvent sur le site d'origine vers le contrôleur cible.

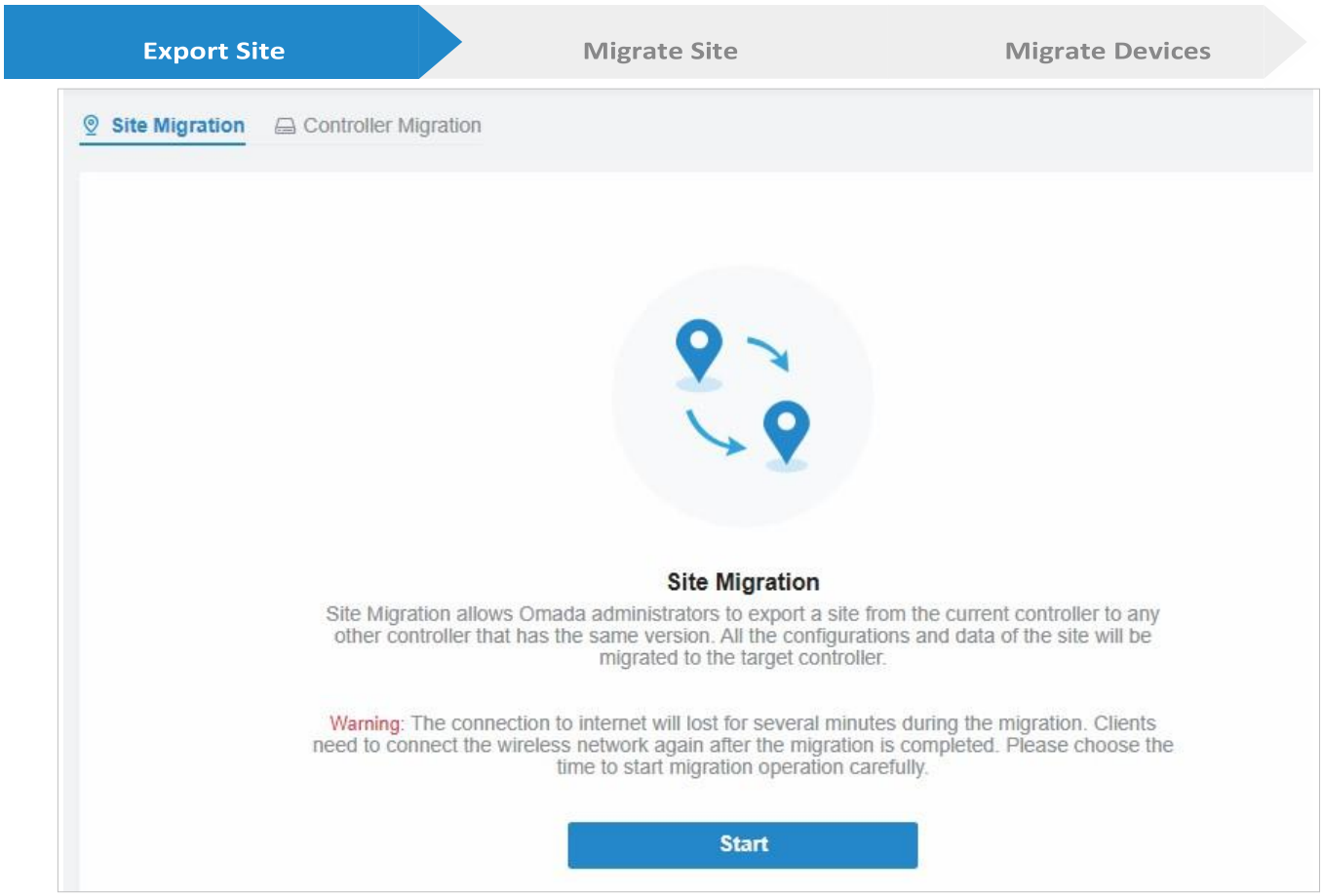
Configuration

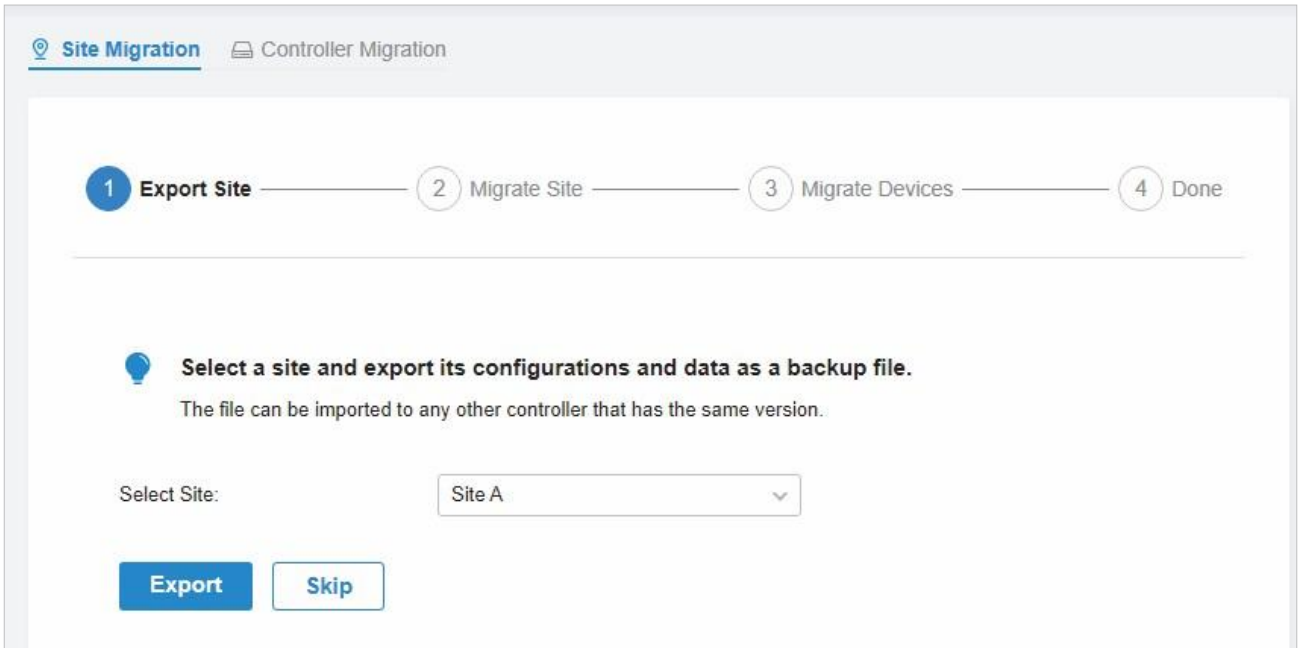
Pour migrer un site vers un contrôleur anthère, procédez ci-dessous.

Note:

La connexion à Internet sera perdue pendant plusieurs minutes pendant la migration. Les clients doivent à nouveau connecter le réseau sans fil une fois la migration terminée. Veuillez choisir soigneusement le moment de commencer l'opération de migration.

1. Allez dans Settings > Migration. Sous l'onglet Migration de site, cliquez sur le bouton démarrer de la page suivante.

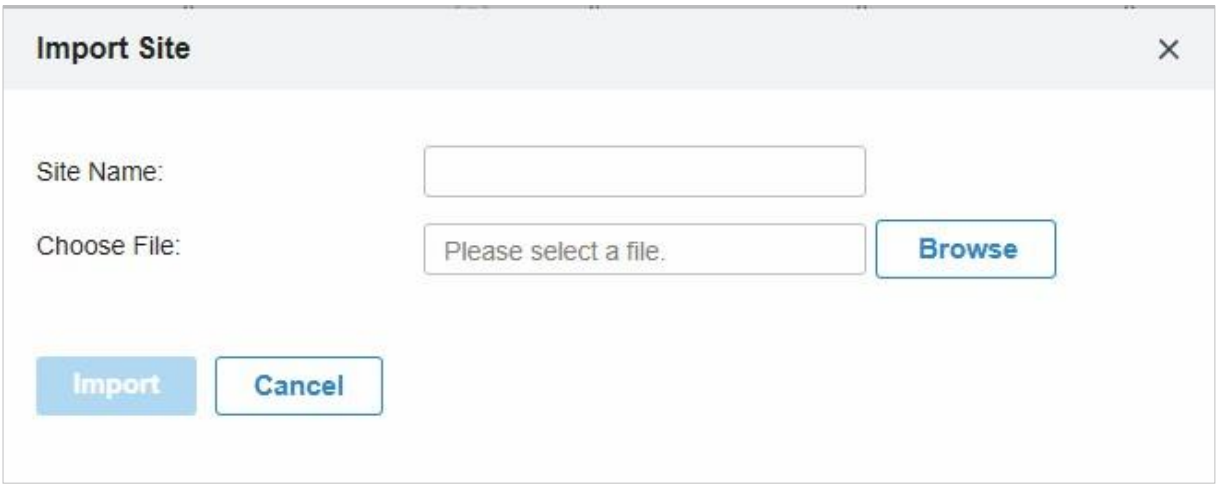




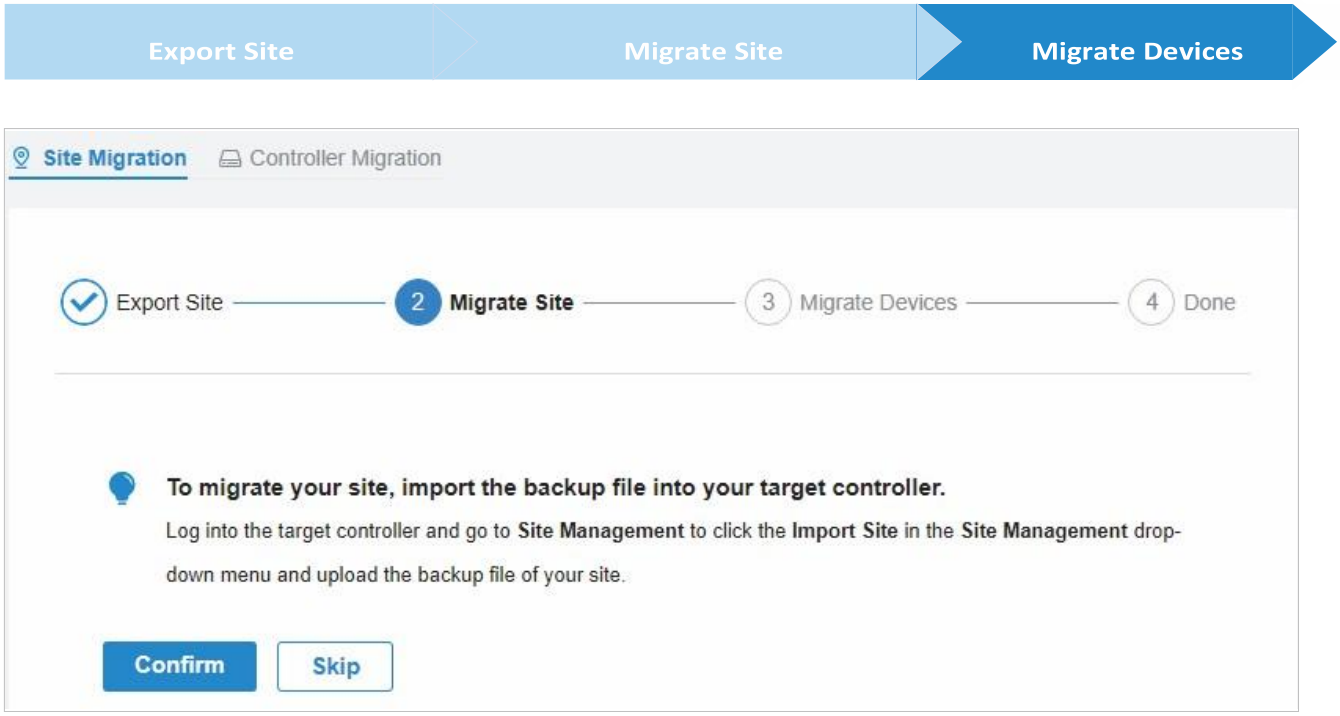
1. Sélectionnez le site à importer dans le deuxième contrôleur dans le Select Site liste déroulante. Cliquez sur Export pour télécharger le fichier du site actuel. Si vous avez sauvegardé le fichier, cliquez sur Skip.



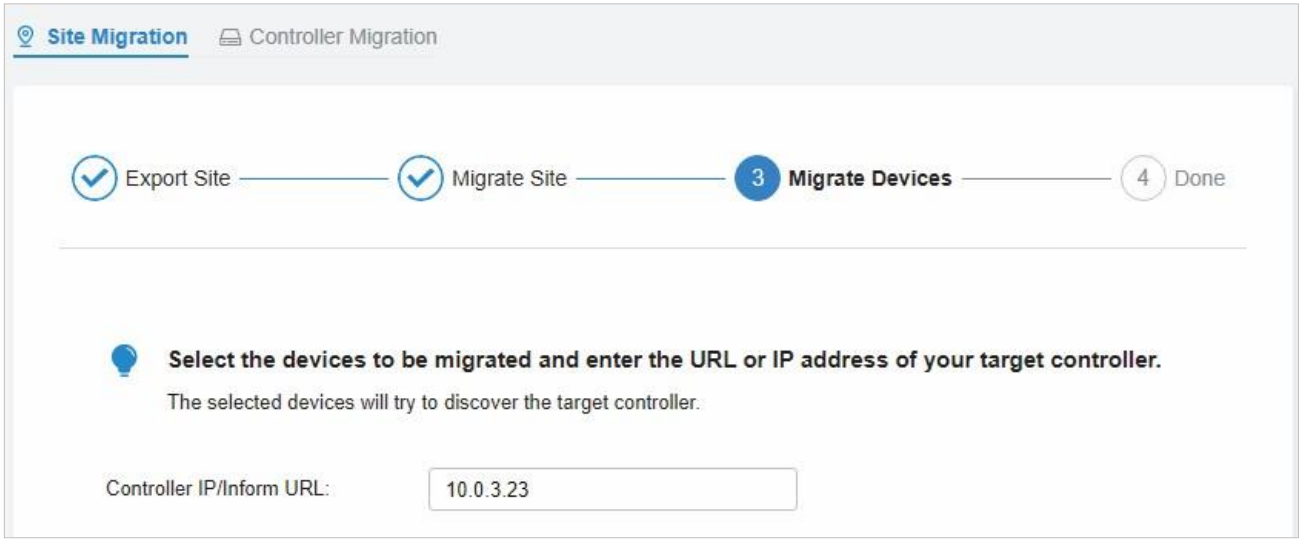
1. Démarrer et se connecter au contrôleur cible, Sites: Site A le coin supérieur droit de l'écran et sélectionner Import Site , et puis la fenêtre suivante apparaîtra.



2. Entrez un nom unique pour le nouveau site. Cliquez sur Browse pour télécharger le fichier du site à importer et cliquez surImport pour importer le site.
3. Une fois que le fichier a été importé au contrôleur cible, retournez au contrôleur précédent et cliquez sur Confirm.



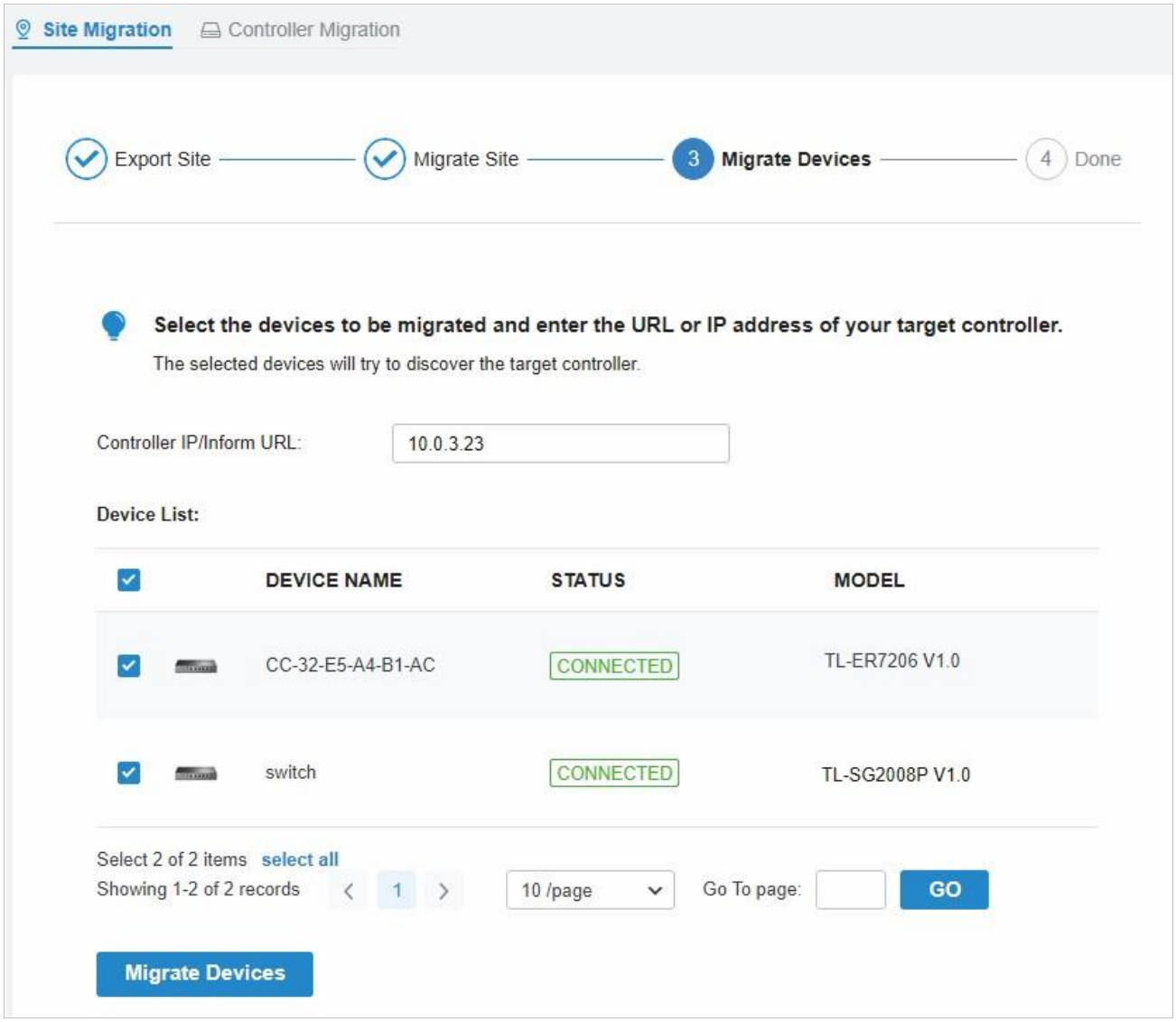
1. Entrez l'adresse IP ou l'URL de votre contrôle cible dans l'entrée d'URL IP/Inform du contrôle. Dans ce cas, l'adresse IP du contrôle cible est 10.0.3.23.



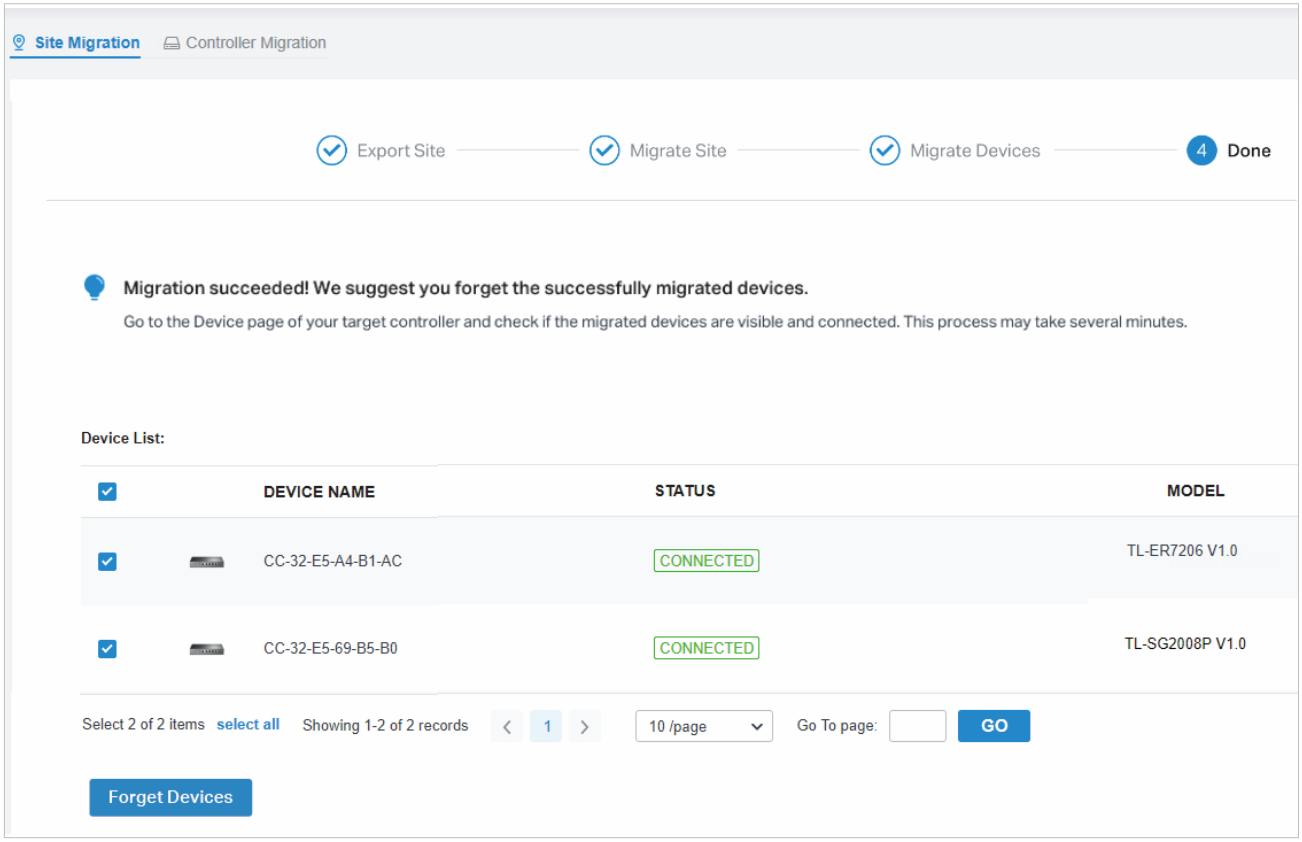
Note:

Assurez-vous d'entrer l'adresse IP ou l'URL correcte du contrôleur cible pour établir la communication entre les périphériques gérés par Omada et votre contrôleur cible. Dans le cas contraire, les périphériques gérés par Omada ne peuvent pas être adoptés par le contrôleur cible.

1. Sélectionnez les périphériques à migrer en cliquant sur la zone à côté de chaque appareil. Par défaut, tous les périphériques sont sélectionnés. Cliquez sur Migrate Devices pour migrer les périphériques sélectionnés vers le contrôleur cible.



2. Vérifier que tous les périphériques migrés sont visibles et connectés sur le contrôleur cible. Lorsque tous les périphériques migrés sont en état connecté dans la page Périphérique du contrôleur cible, cliquez sur Forget Devices pour terminer le processus de migration.

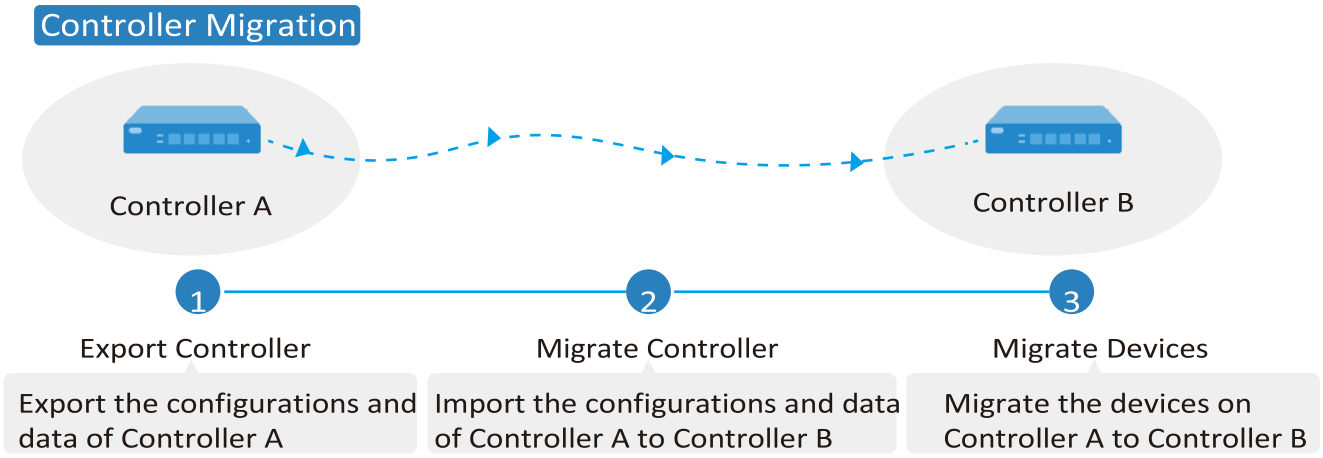


1. Lorsque le processus de migration est terminé, toutes les configurations et données sont migrées vers le contrôleur cible. Vous pouvez supprimer le site précédent si nécessaire.

4. 2 Controller Migration

Aperçu

La migration du contrôleur permet aux administrateurs Omada de migrer les configurations et les données du contrôleur actuel vers tout autre contrôleur qui possède la même version.
Le processus de migration des configurations et des données du contrôleur actuel vers un autre contrôleur peut être résumé en trois étapes : Contrôleur d'exportation, Contrôleur de migration et Périphériques de migration.



Étape1 : Contrôleur d'exportation

Exportez les configurations et les données du contrôleur actuel en tant que fichier de sauvegarde.

Étape2 : contrôle de migration

Dans le contrôleur cible, importez le fichier de sauvegarde du contrôleur actuel.

Étape3 : migrer les périphériques

Migrer les périphériques du contrôleur actuel vers le contrôleur cible.

Configuration

Pour migrer votre contrôleur, procédez ci-dessous.

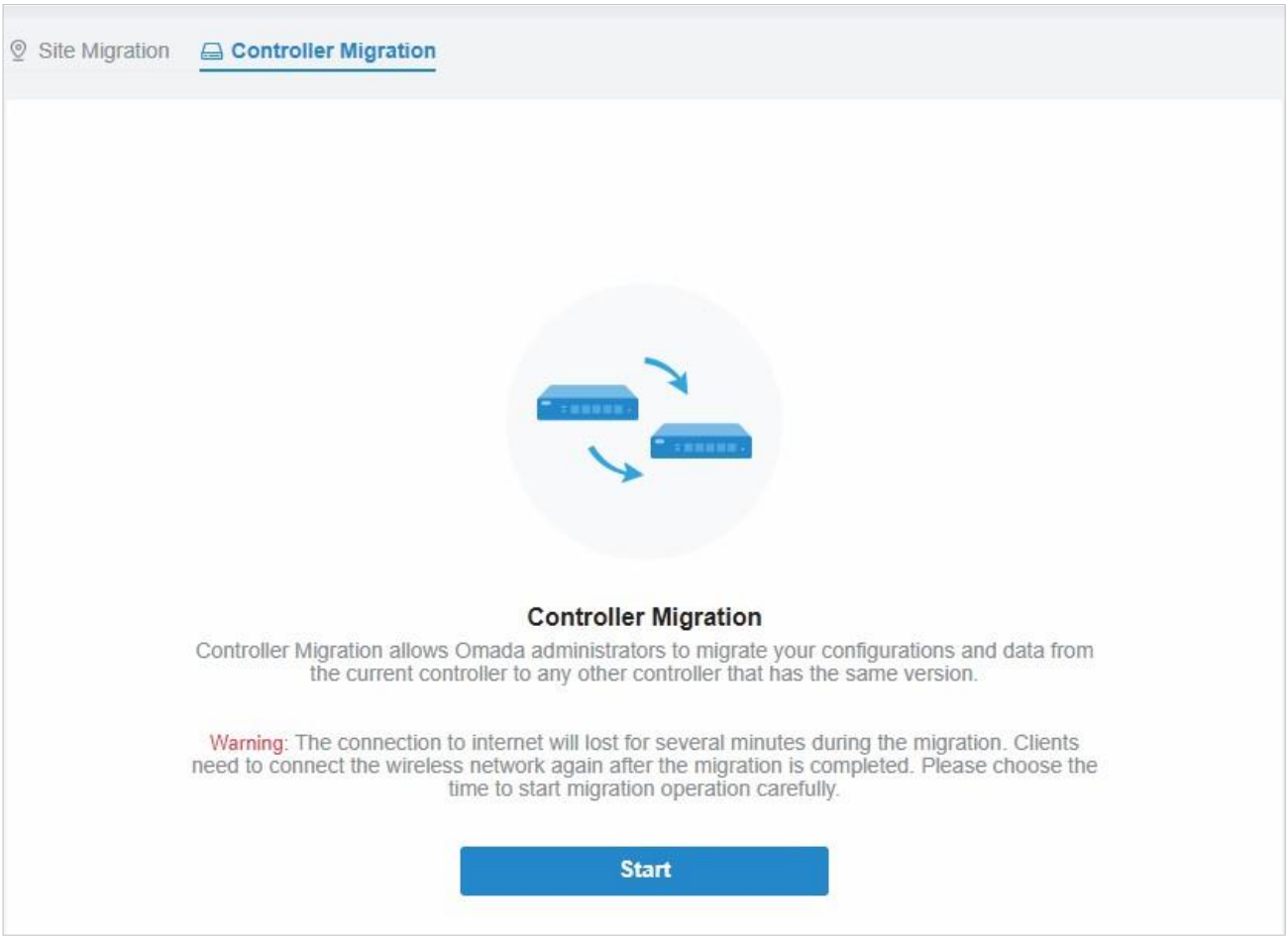
Note:

La connexion à Internet sera perdue pendant plusieurs minutes pendant la migration. Les clients doivent à nouveau connecter le réseau sans fil une fois la migration terminée. Veuillez choisir le moment de commencer soigneusement l'opération de migration.

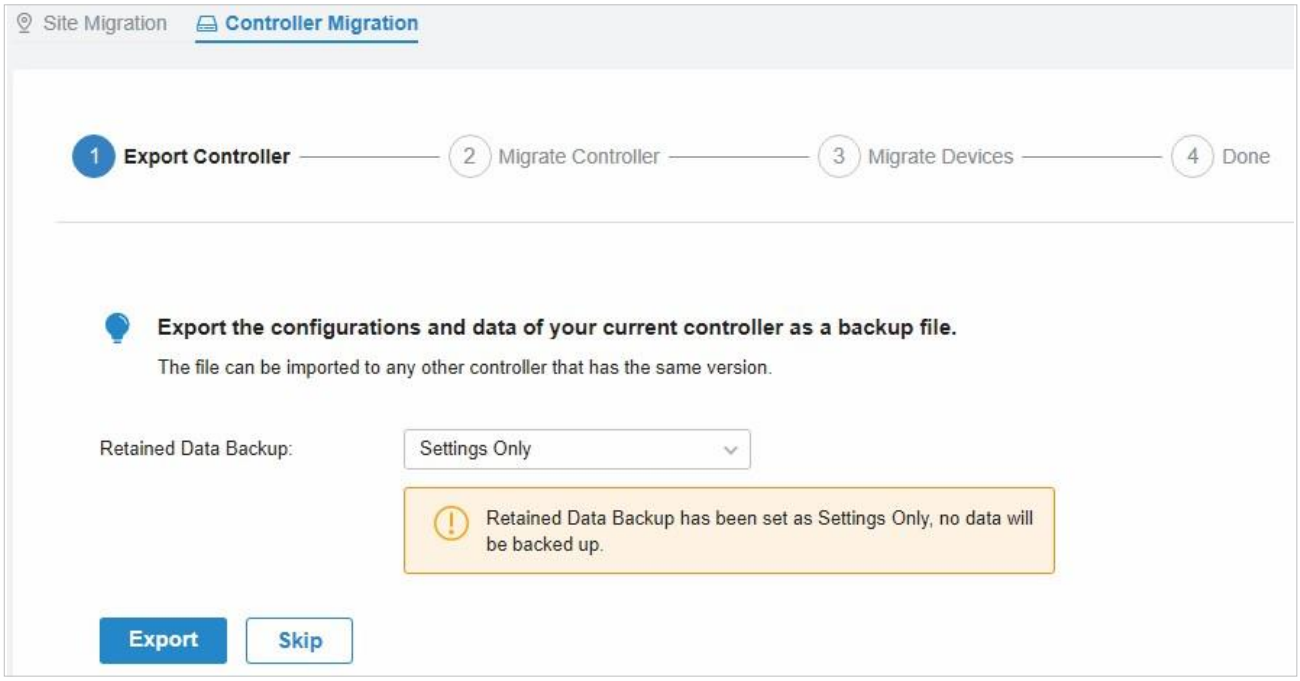
1.



Allez dans Settings > Migration. Sous l'onglet Migration du contrôleur, cliquez sur le bouton Démarrer dans la page suivante.

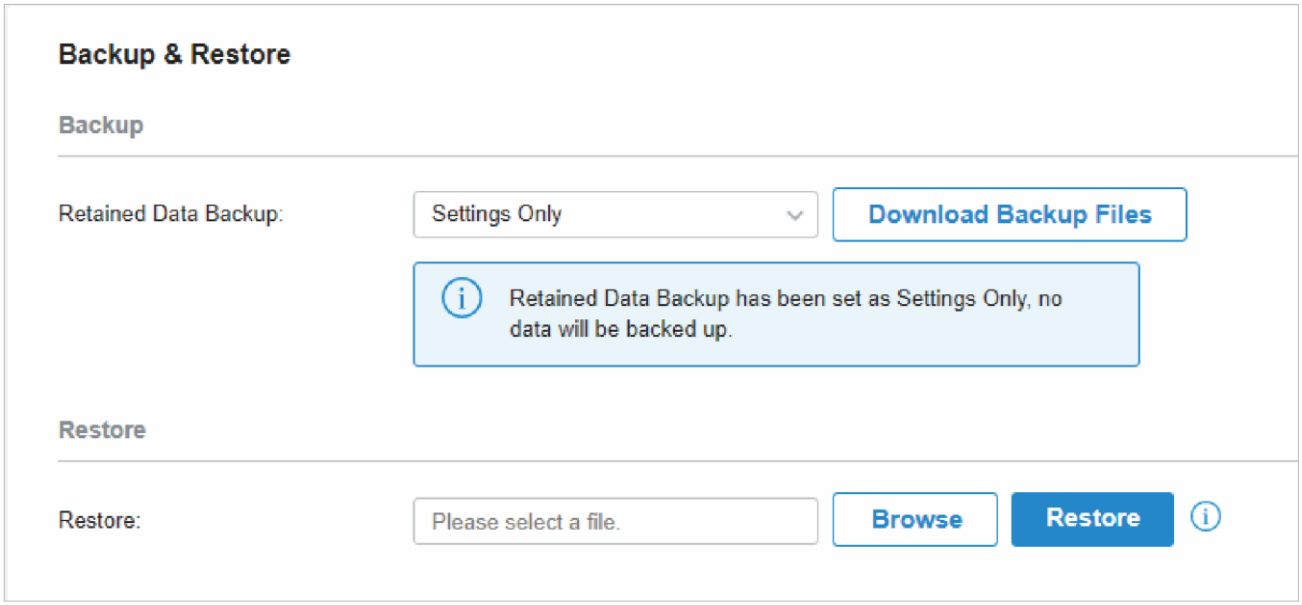


Sélectionnez la durée de la sauvegarde des données dans le Retained Data Backup, et cliquez sur Export pour exporter les configurations et les données de votre contrôleur actuel en tant que fichier de sauvegarde. Si vous avez sauvegardé le fichier, cliquez sur Skip.

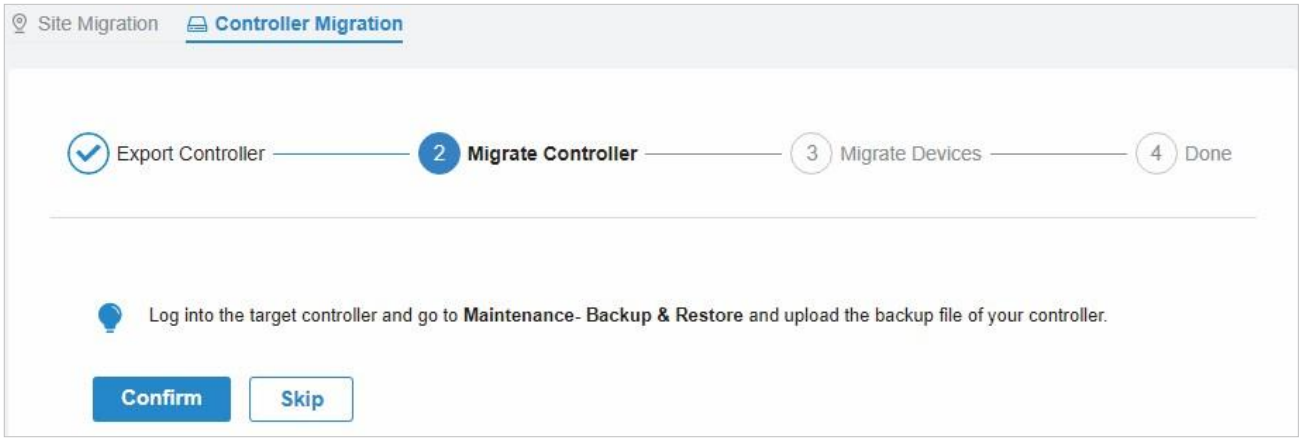




1. Connectez-vous au contrôleur cible, accédez à Settings > Maintenance > Backup & Restore. Click Browse pour localiser et choisir le fichier de sauvegarde du contrôleur précédent. Cliquez ensuite sur Restore pour télécharger le fichier.

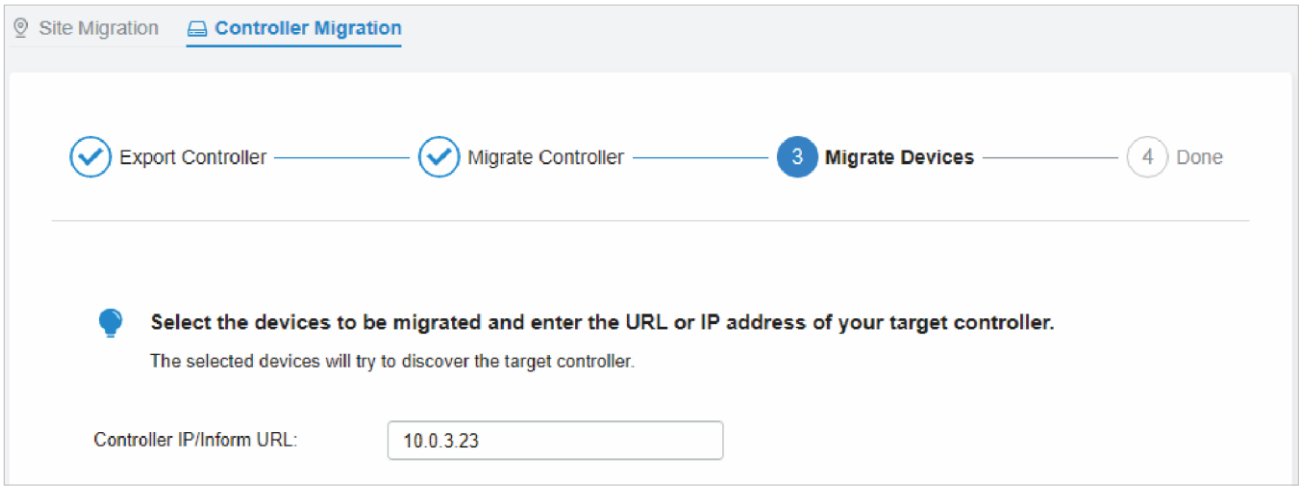


Une fois que le fichier a été importé au contrôleur cible, retournez au contrôleur précédent et cliquez sur Confirm.





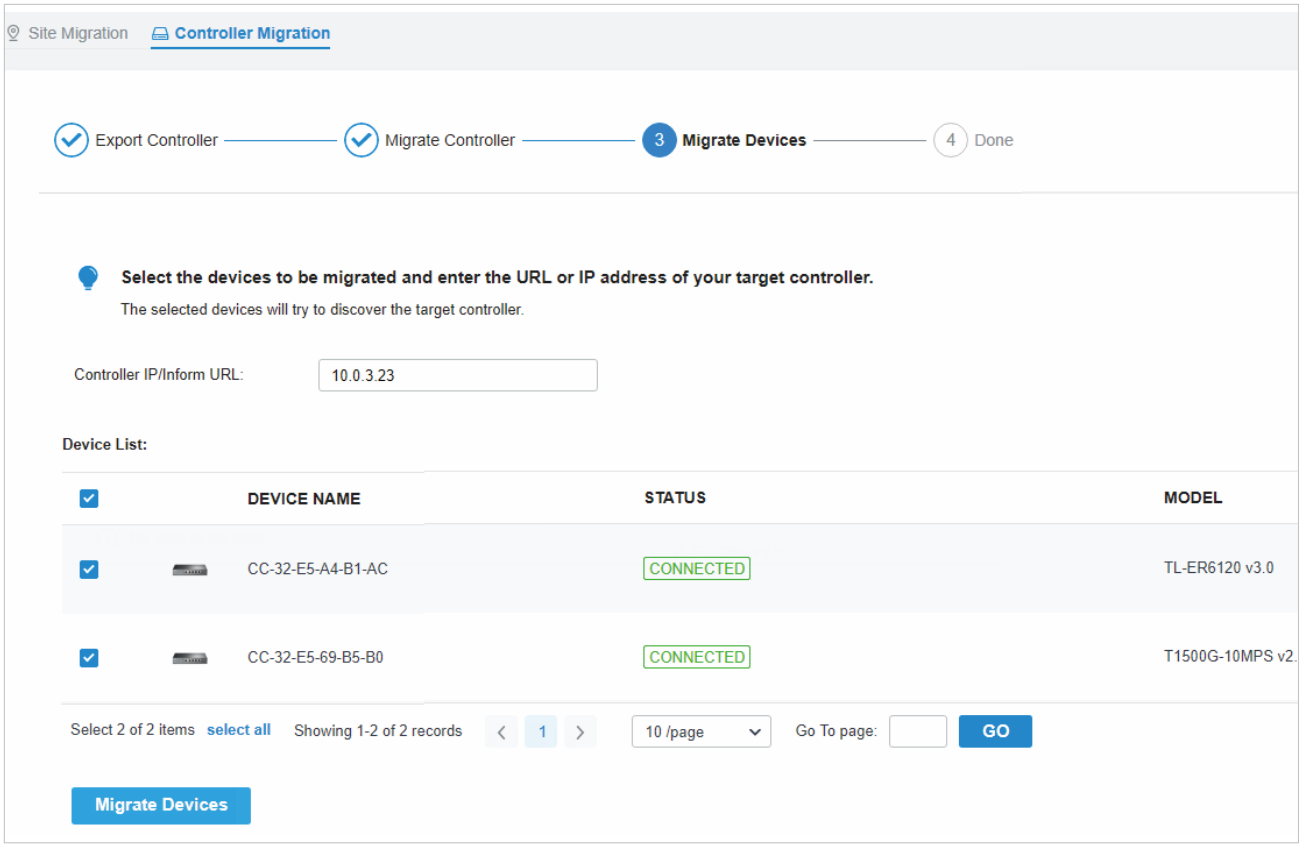
2. Enter the IP address or URL of your target controller into Controller IP/Inform URL input filed. In this case, the IP address of the target controller is 10.0.3.23.



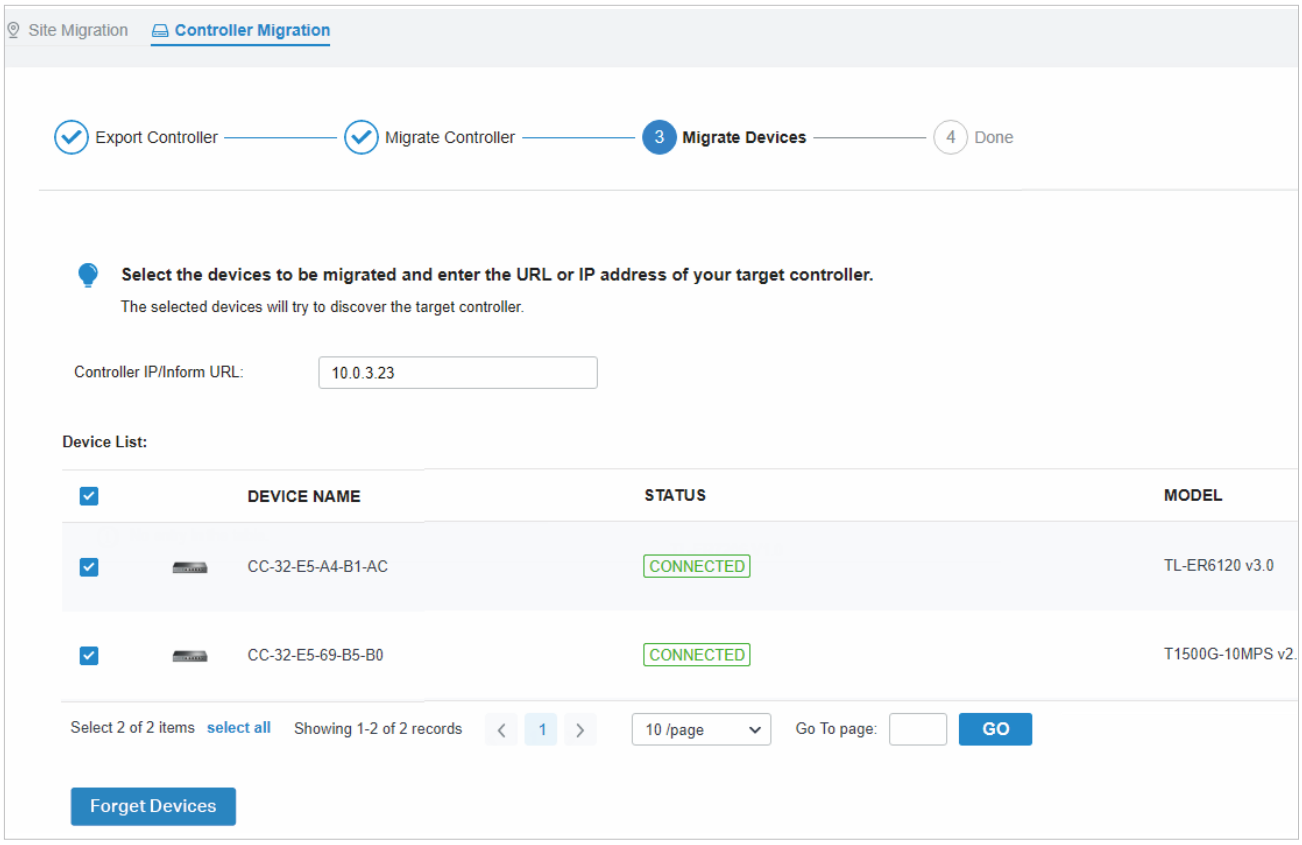
Note:

Assurez-vous d'entrer l'adresse IP ou l'URL correcte du contrôleur cible pour établir la communication entre les périphériques gérés par Omada et votre contrôleur cible. Dans le cas contraire, les périphériques gérés par Omada ne peuvent pas être adoptés par le contrôleur cible.

2. Sélectionnez les périphériques à migrer en cliquant sur la zone à côté de chaque appareil. Par défaut, tous les périphériques sont sélectionnés. Cliquez sur Migrate Devices pour migrer les périphériques sélectionnés vers le contrôleur cible.



3. Vérifiez que tous les périphériques migrés sont visibles et connectés sur le contrôleur cible. Lorsque tous les périphériques migrés sont en état connecté dans la page Périphérique du contrôleur cible, cliquez sur Oublier les périphériques pour terminer le processus de migration.



Lorsque le processus de migration est terminé, toutes les configurations et données sont migrées vers le contrôleur cible. Vous pouvez désinstaller le contrôleur précédent si nécessaire.

5. 5 Auto Backup

Aperçu

Avec la sauvegarde automatique activée, le contrôleur sera programmé pour sauvegarder automatiquement les configurations et les données à l'heure spécifiée. Vous pouvez facilement restaurer les configurations et les données en cas de besoin.

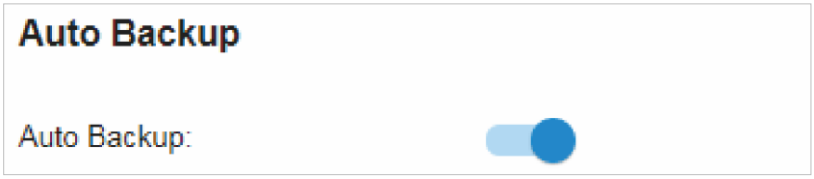
Note:

1. Pour OC200, la sauvegarde automatique n'est disponible que lorsqu'elle est alimentée par un périphérique PoE et qu'un périphérique de stockage est connecté à son port USB.
2. Sur le contrôleur cloud d'Omada, vous n'avez pas besoin de configurer la sauvegarde automatique. Il enregistrera automatiquement vos configurations et données sur le cloud.

Configuration

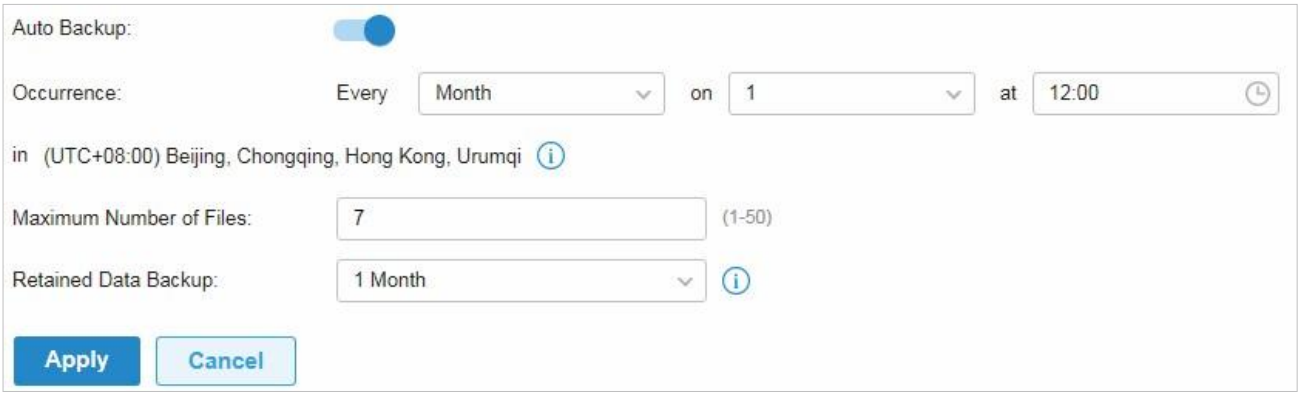
Pour configurer la sauvegarde automatique, procédez

1. Allez dans Settings > Auto Backup. Cliquez sur pour activer la sauvegarde



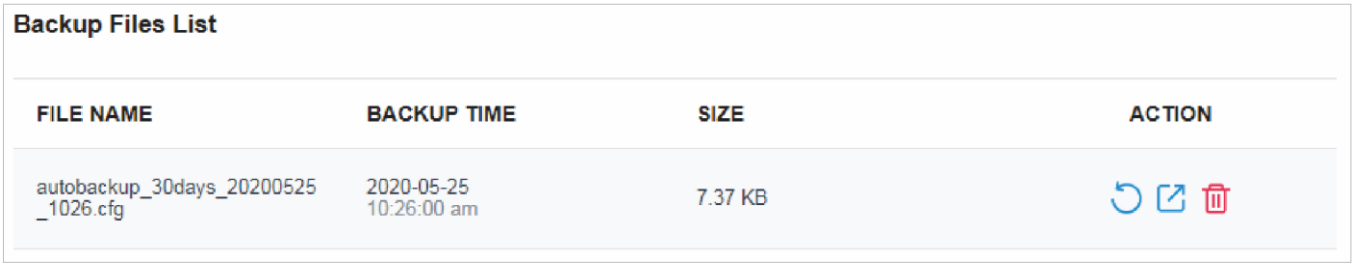
Occurrence	Spécifiez quand effectuer régulièrement la sauvegarde automatique. Sélectionnez d'abord chaquejour, semaine, moisou année, Year puis définissez un temps pour sauvegarder les fichiers. Notez la disponibilité de l'heure lorsque vous choisissez Chaque mois. Par exemple, si vous choisissez de sauvegarder automatiquement les données le 31 de chaque mois, la sauvegarde automatique n'entrera pas en vigueur lorsqu'il s'agit du mois sans 31, comme février, avril et juin.
Nombre maximal de fichiers	Spécifiez le nombre maximal de fichiers de sauvegarde à enregistrer.

2. Configurez les paramètres suivants pour spécifier les règles de sauvegarde automatique. Cliquez sur Apply.



Retained Data Backup	Sélectionnez la durée de la sauvegarde des données en jours. Settings Only: Sauvegarder uniquement les paramètres du contrôleur. 7 Days/1 Month/2 Months/3 Months/6 Months/1 Year: Sauvegarder les données des 7 derniers jours/1 mois/2 mois/3 mois/6 mois/1 an. All Time: (Uniquement pour le contrôleur logiciel Omada) Sauvegarder toutes les données du contrôleur.
Saving Path	(Uniquement pour Omada Hardware Controller) Sélectionnez un chemin d'accès pour enregistrer les fichiers de sauvegarde.

Vous pouvez afficher le nom, le temps de sauvegarde et la taille des fichiers de sauvegarde dans Backup Files List.



Pour restaurer, exporter ou supprimer le fichier de sauvegarde, cliquez sur l'icône de la colonne Action

	Restore the configurations and data in the backup file. All current configurations will be replaced après la restauration. Pour assurer la sécurité des données de sauvegarde, veuillez attendre la fin de l'opération. Cela prendra plusieurs minutes.
	Exporter le fichier de sauvegarde. Le fichier exporté sera enregistré dans le chemin d'enregistrement de votre navigateur Web.
	Supprimer le fichier de sauvegarde.

Note:

•Pour sauvegarder manuellement les données et restaurer les données sur le contrôleur, Backup & Restore pour configurer Backup&Restore.

- La configuration des utilisateurs de cloud ne peut être ni sauvegardée ni restaurée. Pour ajouter des utilisateurs de cloud, veuillez Manage and Create

6

Configurer et surveiller les périphériques gérés par Omada

Ce chapitre vous guide sur la configuration et le suivi des périphériques gérés par Omada, y compris les passerelles, les commutateurs et les EAP. Vous pouvez configurer les périphériques individuellement ou par lots pour modifier les configurations de certains appareils. Le chapitre comprend les sections suivantes :

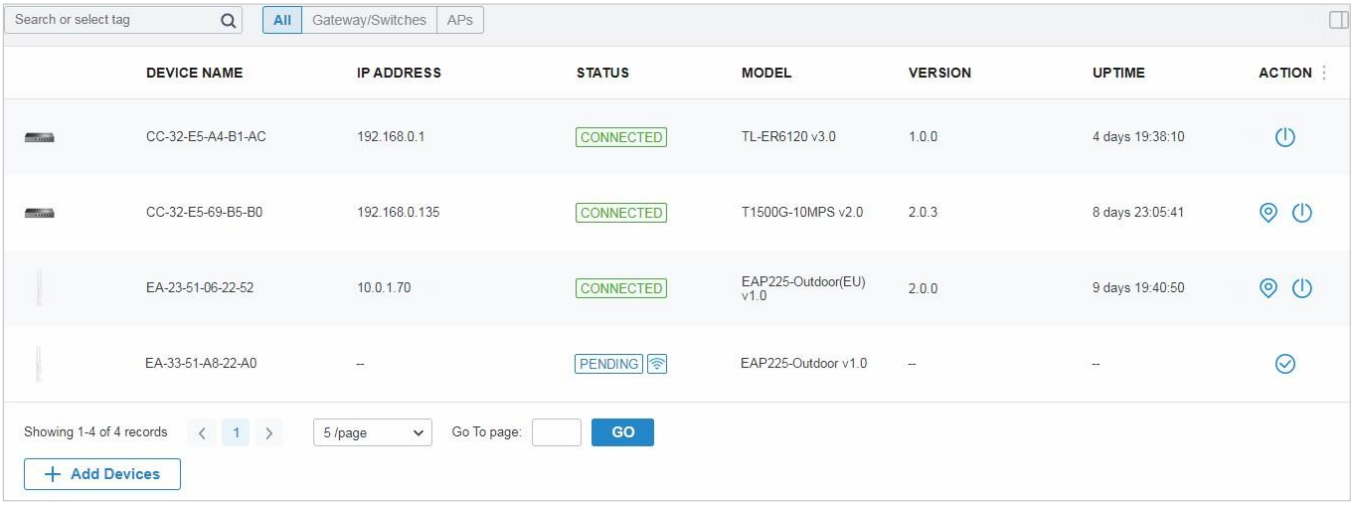
- Introduction à la page Périphériques
- Configurer et surveiller la passerelle
- Configurer et surveiller les commutateurs
- Configurer et surveiller les EAP

6. 1 Introduction à la page Périphériques

Aperçu

La page Périphériques affiche tous les périphériques TP-Link découverts par le contrôleur et leurs informations générales.

Pour une surveillance facile des appareils, vous pouvez personnaliser la colonne et filtrer les appareils pour une meilleure vue d'ensemble des informations de l'appareil. En outre, les opérations rapides et batch edit sont disponibles pour les configurations.



Selon l'état de connexion, les périphéries ont l'état suivant: En attente, isolé, connecté, géré par d'autres, Heartbeat Missed, et Déconnecté. Les icônes de la colonne État sont expliquées comme suit :

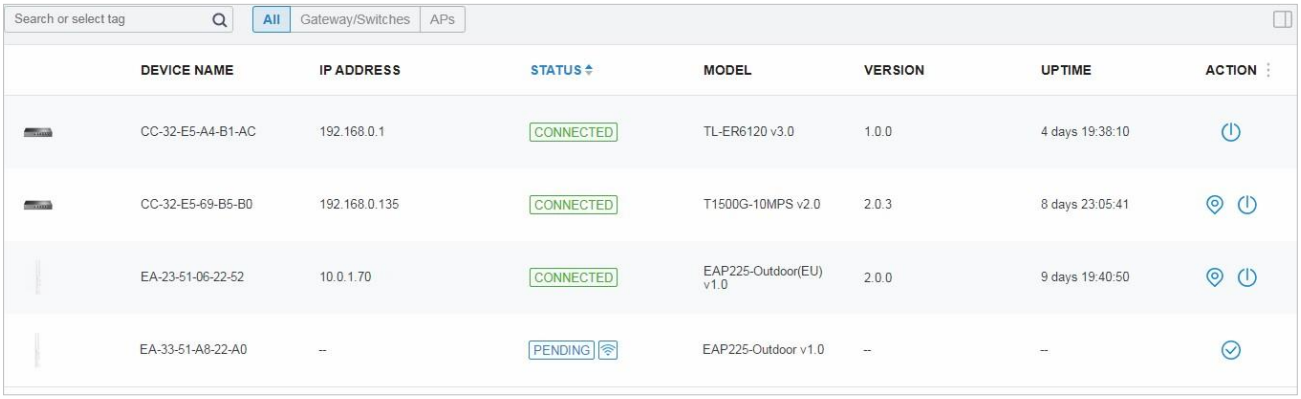
PENDING	L'appareil est en mode autonome ou avec des paramètres d'usine, et n'a pas été adopté par le contrôleur. Pour adopter l'appareil, cliquez sur, et le contrôleur utilisera le nom d'utilisateur et le mot de passe par défaut pour l'adopter. Lors de l'adoption, son statut passera de l'adoption, de l'approvisionnement, de la configuration à la configuration éventuellement.
ISOLATED	(Pour les AP dans le réseau de maillage) L'AP autrefois géré par le contrôleur via une connexion sans fil ne peut plus atteindre la passerelle. Vous pouvez reconstruire le réseau de maillage en le connectant à un AP dans l'état connecté, puis l'AP isolé se transformera en un réseau connecté. Pour une configuration détaillée, reportez-vous à Mesh.
CONNECTED	L'appareil a été adopté par le contrôleur et vous pouvez le gérer de manière centralisée. Un appareil connecté se transformera en un dispositif en attente après que vous
MANAGED BY OTHERS	L'appareil a déjà été géré par un autre contrôleur. Vous pouvez réinitialiser l'appareil ou fournir le nom d'utilisateur et le mot de passe pour le délier d'un autre contrôleur et l'adopter dans le contrôleur actuel.
HEARTBEAT MISSED	Un statut de transition entre connecté et déconnecté. Une fois connecté au contrôleur, l'appareil enverra des paquets d'information au contrôleur dans un intervalle régulier pour maintenir la connexion. Si le contrôleur ne reçoit pas ses paquets d'information en 30 secondes, l'appareil se transformera en état Heartbeat Missed. Pour un appareil manqué par le cœur, si le contrôleur reçoit un paquet d'information de l'appareil en 5 minutes, son état redeviendra connecté ; sinon, son statut deviendra déconnecté.

DISCONNECTED	Le périphérique connecté a perdu la connexion avec le contrôleur pendant plus de 5 minutes.
	(Pour les AP du réseau de maillage) Lorsque cette icône apparaît avec une icône d'état, elle indique EAP avec fonction maillage et aucune connexion câblée n'est détectée par le contrôleur. Vous pouvez le connecter à un AP uplink à Mesh
	Lorsque cette icône s'affiche avec une icône d'état, elle indique le périphérique dans le, Heartbeat Missed, Isolated, ou Deconnected status est migrating. Pour plus d'informations à propos de la migration, reportez-vous à Migration

Configuration

- **Personnaliser la colonne**

Pour personnaliser les colonnes, cliquez sur À côté de Action et cochez les cases du type d'information. Pour modifier l'ordre de liste, cliquez sur la tête de colonne et semble indiquer l'ascendant ou l'ordre décroissant.



- **Filtrer les périphériques**

Utilisez la zone de recherche et la barre d'onglets au-dessus de la table pour filtrer les périphériques.

Pour rechercher les périphériques, entrez le texte dans la zone de recherche ou sélectionnez une balise dans la liste déroulante. En ce qui concerne la balise de périphérique, reportez-vous à la configuration générale de switches Et des EAPs.



Pour filtrer les périphériques, une barre 

Filtre letype d'appareil. Elle est au-dessus de la table pour filtrer les appareils.

Si vous sélectionnez APs tab,o u un autre onglet 

seront disponibles pour modifier la colonne rapidement.

Mesh	Affiche les informations des périphériques du réseau maillé, y compris le nom du périphérique, l'adresse IP, l'état, le modèle, le périphérique de liaison, le canal, l'alimentation Tx et le nombre de périphériques, de clients et de sauts de liaison vers le bas par défaut.
Overview	Affiche par défaut le nom du périphérique, l'adresse IP, l'état, le modèle, la version du firmware, le temps de disponibilité, le canal et l'alimentation Tx.
Performance	Affiche le nom de l'appareil, l'adresse IP, l'état, le temps de disponibilité, le canal, l'alimentation Tx, le nombre de clients de 2,4 GHz et 5 GHz, le taux Rx et le taux Tx par défaut.
Config	Affiche le nom, l'état, la version, le groupe WLAN et les paramètres radio pour 2,4 GHz et 5 GHz par défaut.

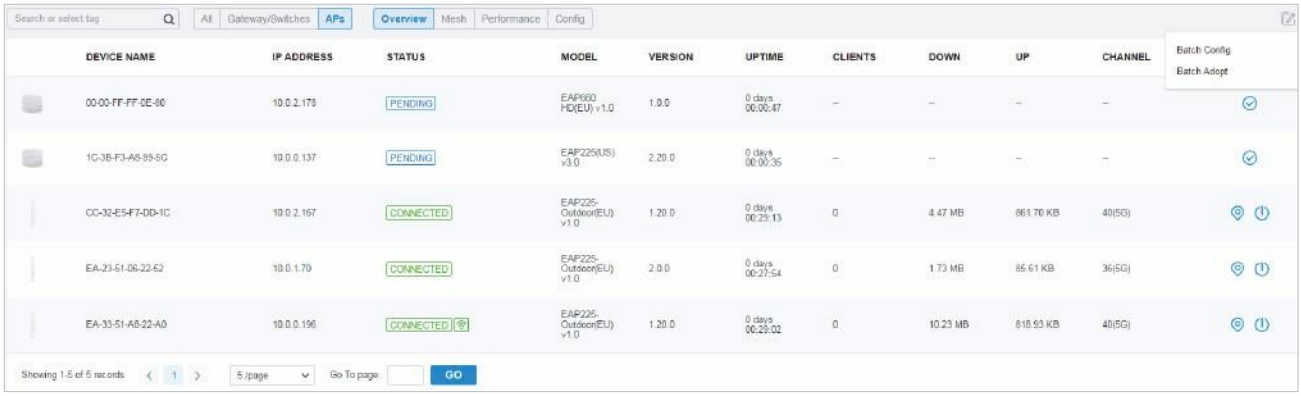
■ **Opérations rapides**

Cliquez sur les icônes de la colonne Action pour adopter, localiser, mettre à niveau ou redémarrer rapidement l'appareil.

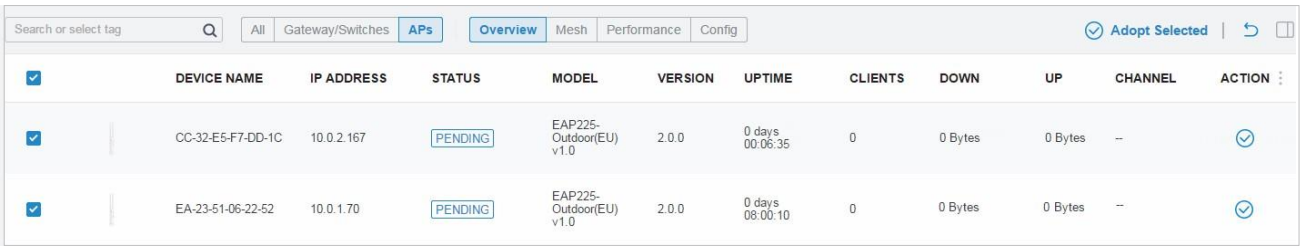
	(Pour les périphériques en attente) Cliquez pour adopter
	(Pour les commutateurs connectés et les AP) Cliquez sur cette icône et les LED de l'appareil pour indiquer l'emplacement de l'appareil. Les LED continueront à clignoter pendant 10 minutes, cliquez sur pour arrêter le clignotement.
	(Pour les périphériques connectés) Cliquez pour redémarrer
	Cliquez pour mettre à niveau la version du firmware de l'appareil. Cette icône s'affiche lorsque l'appareil a une nouvelle version du firmware. Pour les mises à niveau, Services

■ **Modification de lot (pour commutateurs et EAP)**

Après avoir sélectionné l'onglet Passerelle/Commutateurs ou AP, vous pouvez adopter ou configurer les commutateurs ou les EAP par lots. Batch Config est disponible uniquement pour les périphériques en état connecté/déconnecté/heartbeat manqué/isolé, tandis que Batch Adopt est disponible pour les périphériques dans l'état En attente/géré par d'autres.



Cliquez, sélectionnez Batch Adopt, cliquez sur les cases à cocher des appareils, puis cliquez sur Adopt Selected. Si les périphériques sélectionnés sont tous dans l'état En attente, le contrôleur adoptera alors avec le nom d'utilisateur et le mot de passe par défaut. Si ce n'est pas le cas, entrez manuellement le nom d'utilisateur et le mot de passe pour adopter les appareils.

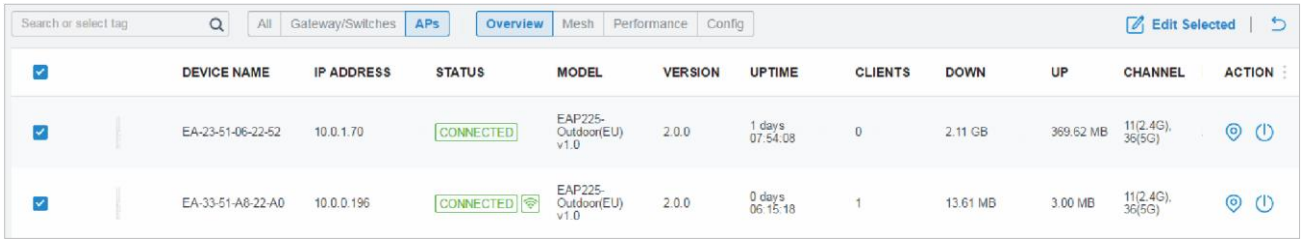


Cliquez sur , selectionnez Batch Config
cliquez sur l cases à cocher des appareils, puis Edit Selected

Ensuite, la fenêtre Propriétés s'affiche. Il y a deux onglets dans la fenêtre : Périphériques et Config.

Dans Périphériques, vous pouvez cliquer pour supprimer l'appareil de la configuration du lot en cours.

Dans Config, tous les paramètres sont conservés l'existant par défaut. Pour des configurations détaillées, reportez-vous à la configuration des commutateurs et des EAP.

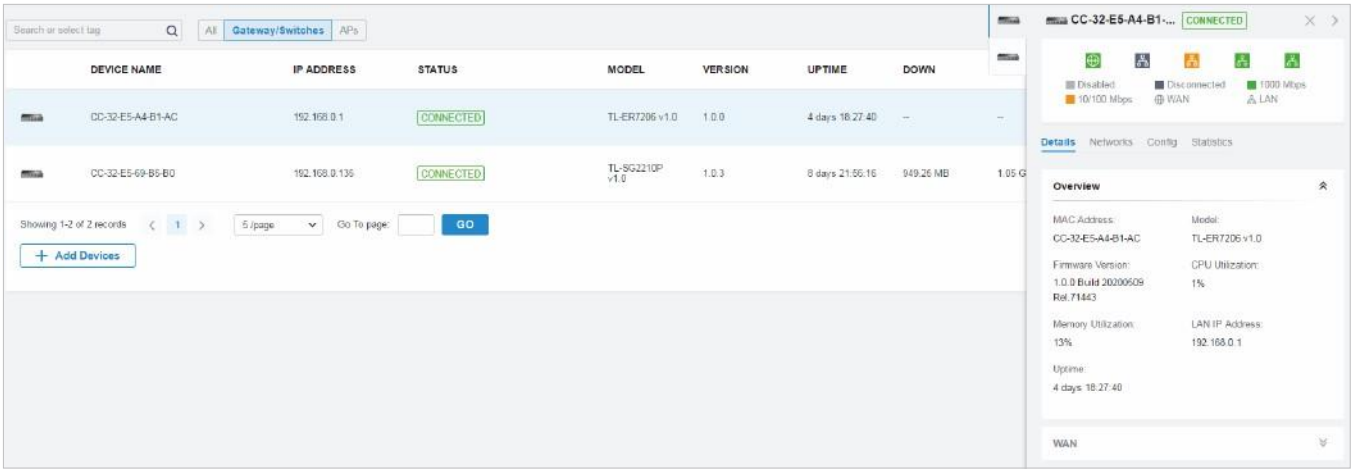


	Cliquez pour sélectionner plusieurs périphériques et ajoutez-les à la fenêtre Propriétés pour le lot suivi et gestion.
	Cliquez pour réduire au minimum la fenêtre Propriétés sur une icône. Pour rouvrir les propriétés minimisées .
	Cliquez pour maximiser la fenêtre Propriétés. Vous pouvez également utiliser l'icône sur la page Périphériques.
	Cliquez pour fermer la fenêtre Propriétés de l'ou des périphériques choisis. Notez que les non-s configuration sera perdue.
	Le nombre en bas à droite affiche le nombre d'appareils dans la configuration du lot

6. 2 Configurer et surveiller la passerelle

Dans la fenêtre Propriétés, vous pouvez configurer la passerelle gérée par le contrôleur et surveiller les performances et les statistiques. Par défaut, toutes les configurations sont synchronisées avec le site actuel.

Pour ouvrir la fenêtre Propriétés, cliquez sur l'entrée d'un routeur. Un panneau de moniteur et plusieurs onglets sont répertoriés dans la fenêtre Propriétés. La plupart des fonctionnalités à configurer sont rassemblées dans l'onglet Config, telles que IP, SNMP, IPTV et Hardware Offload, tandis que d'autres onglets sont principalement utilisés pour surveiller les périphériques.



Note:

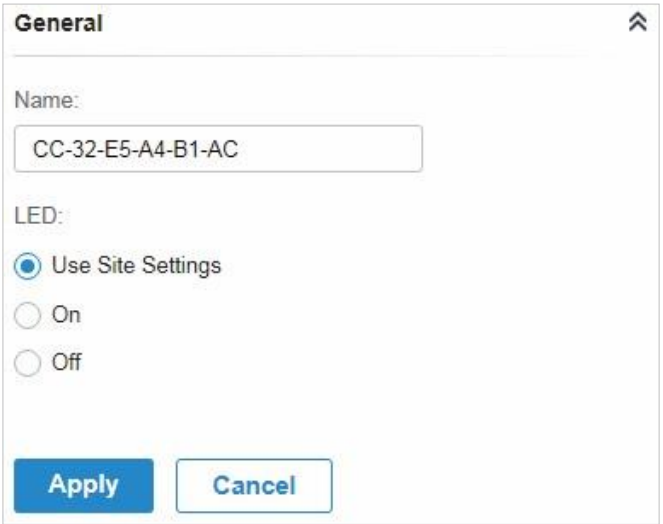
- **Vous ne pouvez adopter qu'un seul routeur sur un seul site.**
- Les fonctions disponibles dans la fenêtre varient en raison du modèle et de l'état de l'appareil.

6. 2. 1 Configurer la Gateway

Dans la fenêtre Propriétés, cliquez sur Config, puis sur les sections pour configurer les fonctionnalités appliquées au routeur, y compris les paramètres généraux, le SNMP, l'IPTV et les fonctions avancées.

■ **Généralités**

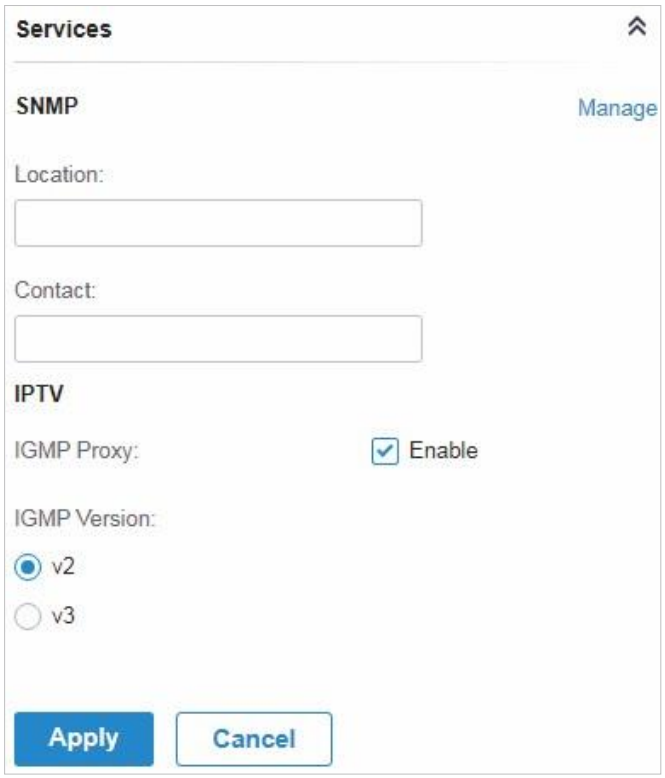
En général, vous pouvez spécifier le nom de l'appareil et les paramètres LED du routeur.



Name	Specify a name of the device.
LED	Sélectionnez le fonctionnement des LED de cet appareil. Use Site Settings: La LED de l'appareil fonctionnera en suivant les paramètres du site. Pour afficher et modifier les paramètres du site, reportez-vous à Services. On/Off: La LED de l'appareil se maintiendra/.

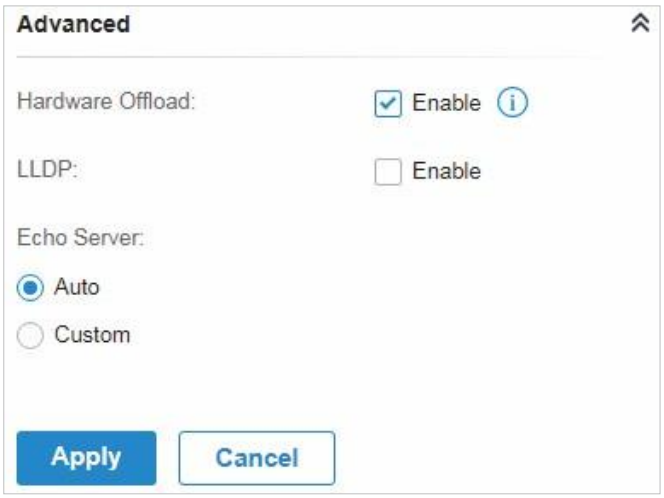
■ Services

Dans Services, vous pouvez configurer SNMP pour noter l'emplacement et les détails de contact, et activer le proxy IGMP détecter les appartenances de groupes de numéros multidiffusion. Vous pouvez également cliquer sur Manage pour sauter à Settings > Services > SNMP, et pour la configuration détaillée du service SNMP, reportez-vous à SNMP.



Avancé

Dans Advanced, vous pouvez configurer Hardware Offload, LLDP (Link Layer Discovery Protocol) et Echo Server pour mieux utiliser les ressources réseau.

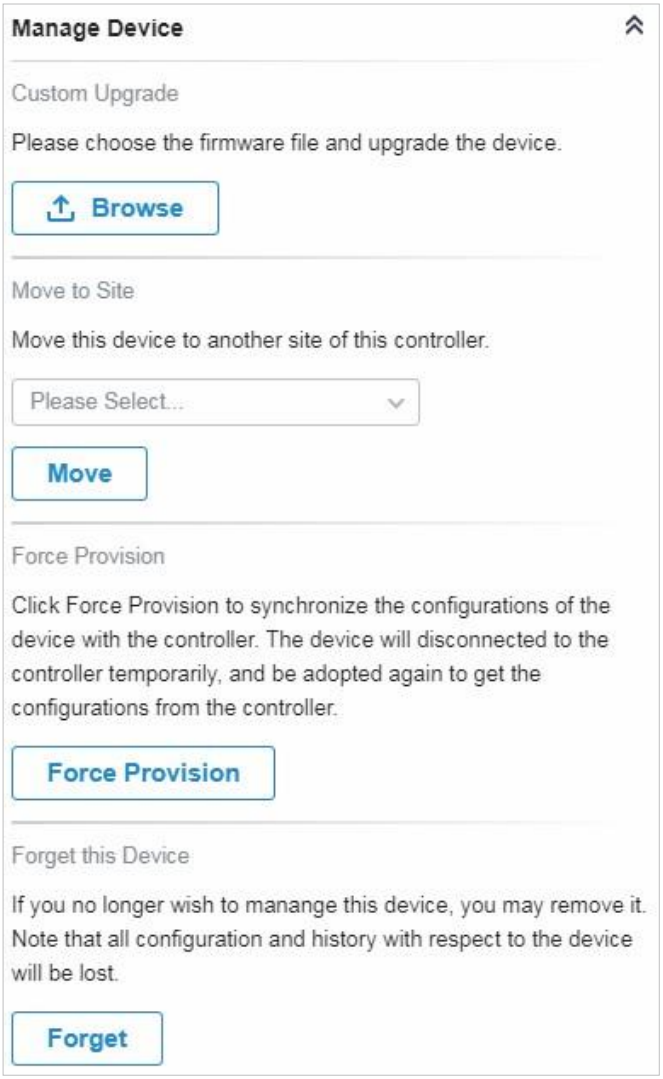


Hardware Offload	Le déchargement matériel peut améliorer les performances et réduire l'utilisation du processeur en utilisant le matériel pour décharger le traitement des paquets. Notez que cette fonctionnalité ne peut pas prendre effet si QoS, Contrôle de bande passante ou Limite de session est activé. Pour configurer le contrôle de bande passante et la limite de session pour le routeur, reportez-vous à Transmission.
LLDP	LLDP peut aider à découvrir des appareils.
Echo Server	Echo Server est utilisé pour tester la connectivité et surveiller la latence du réseau automatiquement ou manuellement. Si vous cliquez sur Custom, entrez l'adresse IP ou le nom d'hôte de votre serveur personnalisé.

Gérer le périphérique

Dans Gérer le périphérique, vous pouvez mettre à niveau manuellement la version du firmware de l'appareil, le déplacer vers un autre site, synchroniser les configurations avec le contrôleur et oublier le routeur.

■



Custom Upgrade	Cliquez sur Browse et choisissez un fichier à partir de votre ordinateur pour mettre à niveau l'appareil. Lors de la mise à niveau, l'appareil sera redémarré et réadopté par le contrôleur.
Move to Site	Sélectionnez un site vers lequel l'appareil sera déplacé. Après avoir déménagé sur un autre site, les configurations de périphériques sur le site précédent seront remplacées par celle du nouveau site, et son historique de trafic sera effacé.
Force Provision	Cliquez sur Force Provision pour synchroniser les configurations de l'appareil avec le contrôleur. L'appareil perdra temporairement la connexion et sera à nouveau adopté au contrôleur pour obtenir les configurations du contrôleur.
Forget	Cliquez sur Forget et puis l'appareil sera retiré du contrôleur. Une fois oubliées, toutes les configurations et l'historique liés à l'appareil seront effacés.

Paramètres communs

Dans Paramètres communs, vous pouvez cliquer rapidement sur le chemin d'accès pour accéder aux modules correspondants.



6. 2. 2 Surveiller la passerelle

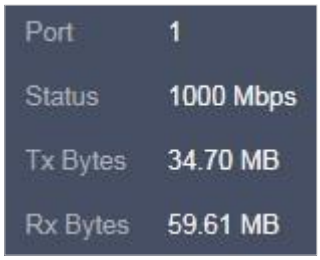
Un panneau et trois onglets sont fournis pour surveiller l'appareil dans la fenêtre Propriétés : Panneau de suivi, Détails, Réseaux et Statistiques.

Panneau de moniteur

Le panneau moniteur affiche les ports du routeur et utilise des couleurs et des icônes pour indiquer l'état de la connexion différent. and port types. When the router is pending or disconnected, all ports are disabled.



Vous pouvez placer le curseur au-dessus de l'icône de port pour plus de détails.



Détails

Dans Les détails, vous pouvez afficher les informations de base du routeur et les statistiques des ports WAN pour connaître brièvement l'état d'exécution de l'appareil.

- **Aperçu**

  Dans **Overview**, vous pouvez afficher les informations de base de l'appareil. Les informations répertoriées varient en fonction de l'état de l'appareil.



- **WAN**

  Dans WAN, vous pouvez afficher les informations et statistiques de base du port WAN, telles que l'adresse IP, la vitesse, le duplex, et le téléchargement et le téléchargement du trafic.



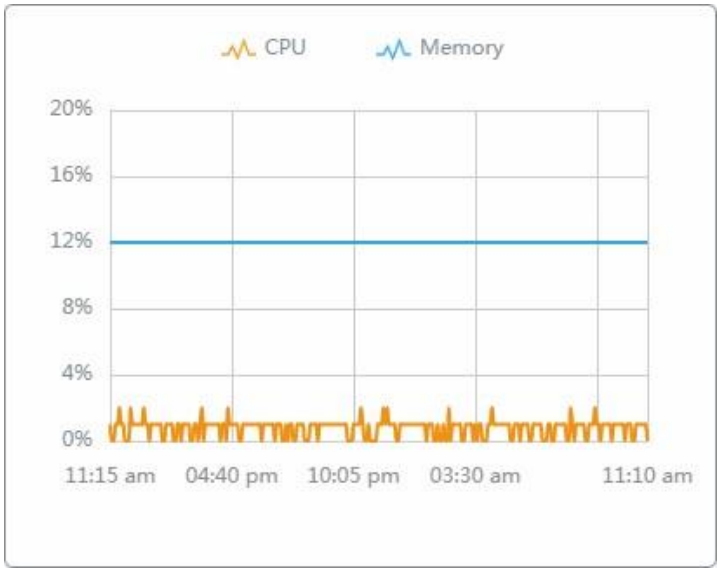
Network

Dans Réseau, vous pouvez afficher les informations réseau du routeur, y compris le nom du réseau, l'adresse IP, les trafics transmis et reçus d'interfaces RÉSEAU dans le réseau et le nombre de clients.

Network	IP Address	Tx Bytes	Rx Bytes	Clients
LAN	192.168.0.1	596.1 MB	1.0 GB	0

Statistiques

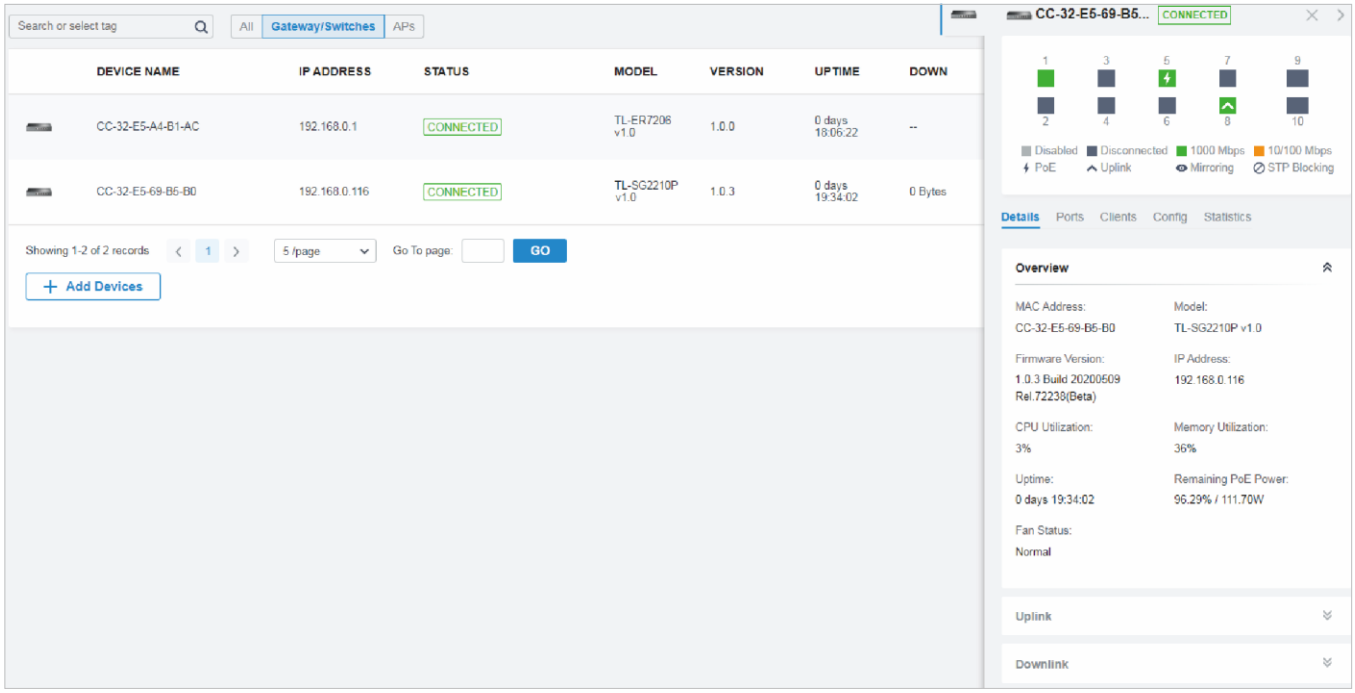
Dans Les statistiques, vous pouvez surveiller le processeur et la mémoire de l'appareil au cours des dernières 24 heures via des graphiques. Pour afficher les statistiques de l'appareil dans une certaine période, cliquez sur le graphique pour View the Statistics of the Network.



6. 3 Configurer et surveiller les commutateurs

Dans la fenêtre Propriétés, vous pouvez configurer un ou certains commutateurs connectés au contrôleur et surveiller les performances et les statistiques. Les configurations modifiées dans la fenêtre Propriétés seront appliquées uniquement au(e)s de commutateur(es) sélectionné. Par défaut, toutes les configurations sont synchronisées avec le site actuel.

Pour ouvrir la fenêtre Propriétés, cliquez sur l'entrée d'un commutateur ou cliquez sur l'icône pour sélectionner les commutateurs pour la configuration du lot. Un panneau de moniteur et plusieurs onglets sont répertoriés dans la fenêtre Propriétés. La plupart des fonctionnalités à configurer sont rassemblées dans l'onglet Ports et Config, telles que la mise en miroir de port, l'adresse IP et la gestion VLAN, tandis que d'autres onglets sont principalement utilisés pour surveiller les périphériques.



Note:

- Les fonctions disponibles dans la fenêtre varient en raison du modèle et de l'état de l'appareil.
- Dans Batch Config, vous ne pouvez configurer que les périphériques sélectionnés et les configurations inchangées conserveront les paramètres actuels.

6. 3. 1 Configurer les commutateurs

Dans la fenêtre Propriétés, vous pouvez afficher et configurer les profils appliqués aux ports dans ports, et dans Config, vous pouvez configurer les fonctionnalités de commutateur.

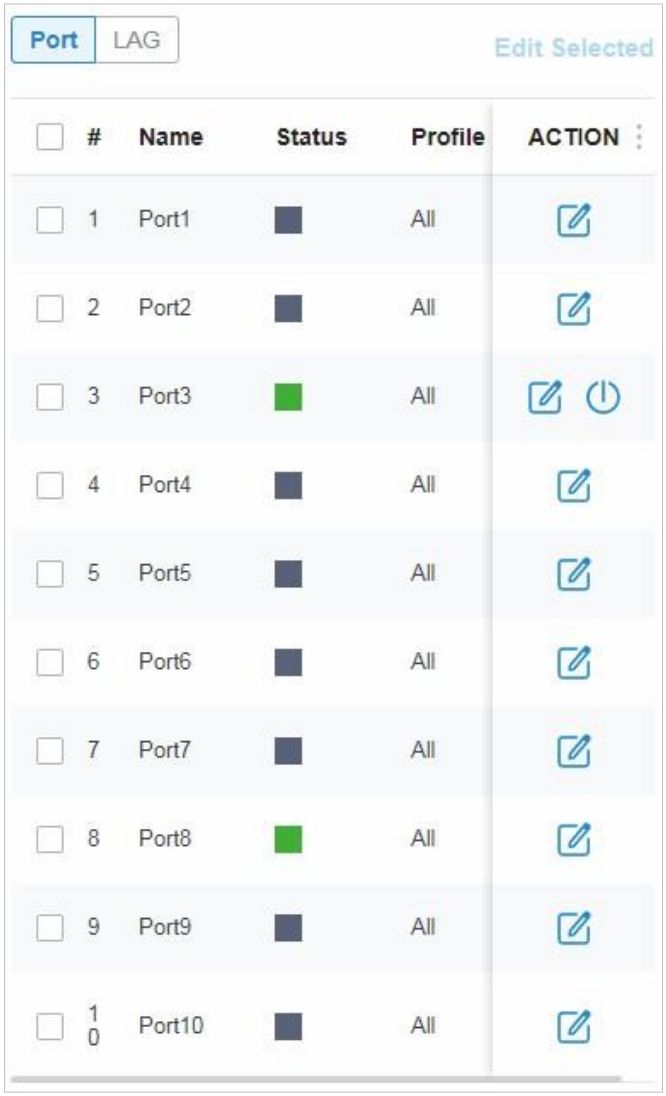
Ports

Le port et le LAG sont deux onglets conçus pour les ports physiques et les LAG (Link Aggregation Groups), respectivement. Sous la balise Port, tous les ports sont répertoriés, mais vous pouvez configurer uniquement les ports physiques, y compris la suppression des profils appliqués, la configuration de la mise en miroir de port et la spécification des ports en tant que LAG.

Sous la balise LAG, tous les GAL sont répertoriés et vous pouvez afficher et modifier les configurations des LAG existants.

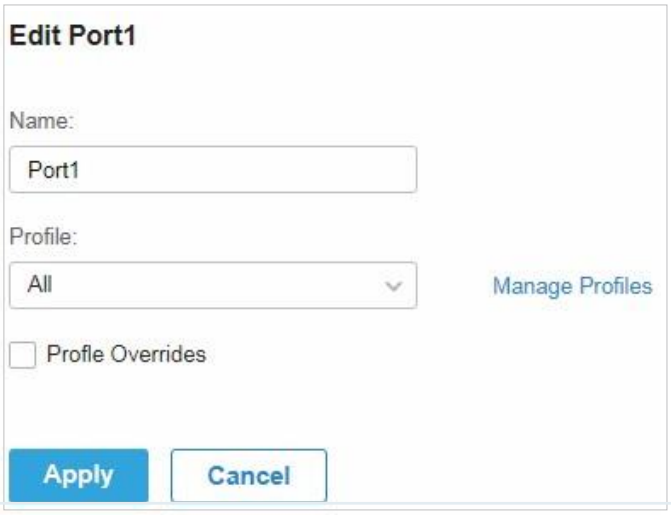
- **Port**

  Dans port, vous pouvez afficher et configurer tous les noms et profils appliqués de tous les ports.



Status	Affiche l'état du port dans différentes couleurs. : Le profil de port est désactivé. Pour l'activer, cliquez pour modifier le profil. : Le port est activé, mais aucun périphérique ou client n'y est connecté. : Le port fonctionne à 1000 Mbps. : Le port fonctionne à 10/100 Mbps.
Profile	Affiche le profil appliqué au port.
Action	: Cliquez pour modifier le nom du port et configurer le profil appliqué au port. : (Pour les ports PoE) Cliquez pour redémarrer les périphériques connectés (PD).

Pour configurer un seul port, cliquez dans le tableau. Pour configurer les ports par lots, cliquez sur les cases à cocher, puis sur Modifier sélectionner. Ensuite, vous pouvez configurer le nom et le profil du port. Par défaut, tous les paramètres sont conservés existants pour la configuration du lot.

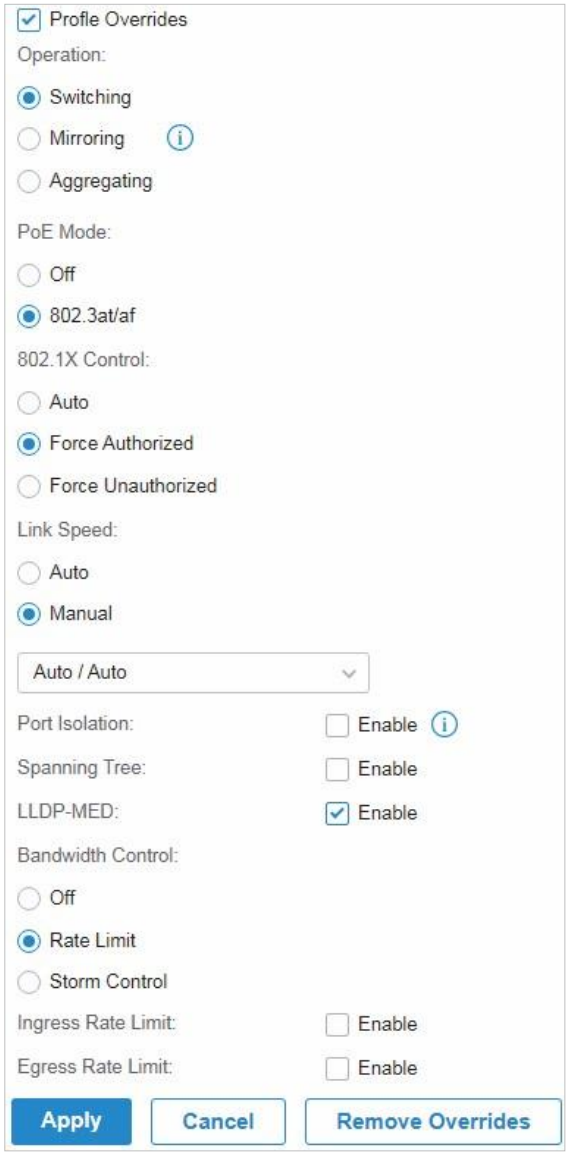


Name	Entrez le nom du port .
Profile	Sélectionnez le profil appliqué au port dans la liste déroulante. Cliquez sur Manage Profiles pour afficher et gérer les profils. Pour plus de détails, reportez-vous à Configure Wired Networks.
Profile Overrides	Cliquez sur la case à cocher pour remplacer le profil appliqué. Les paramètres à configurer varient dans les modes Opération,

Cliquez sur la case à cocher pour remplacer le profil appliqué. Les paramètres à configurer varient dans les modes Opération, override the applied profile, configure a mirroring port, ou configure a LAG.

1. **Remplacer le profil appliqué**

   Si vous sélectionnez Switching Pour Opération, configurez les paramètres suivants et cliquez sur Apply pour remplacer le profil appliqué. Pour supprimer les modifications, cliquez sur Remove Overrides et toutes les configurations de profil deviendront les mêmes que le profil appliqué.



PoE Mode	(Uniquement pour les ports PoE) Sélectionnez le mode PoE (Power over Ethernet) pour le port. Disable : Désactiver la fonction PoE sur le port PoE. 802.3at/af : Activer la fonction PoE sur le port PoE.

802.1X Control	Sélectionnez le mode de contrôle 802.1X pour les ports. Pour configurer l'authentification 802.1X à l'échelle mondiale, Settings > Authentication > 802.1X. Auto: Le port n'est pas autorisé jusqu'à ce que le client soit authentifié par le serveur d'authentification avec succès. Force Authorized: Le port reste dans l'état autorisé, envoie et reçoit le trafic normal sans 802.1X authentification du client. Force Unauthorized: Le port reste dans l'état non autorisé, et le client connecté au port ne peut s'authentifier avec aucun moyen. Le commutateur ne peut pas fournir des services d'authentification au client via le port.
Link Speed	Sélectionnez le mode de vitesse du port. Auto : Le port négocie automatiquement la vitesse et le duplex. Manuel : Spécifiez manuellement la vitesse et le duplex de la liste déroulante.
Port Isolation	Cliquez sur la case à cocher pour activer l'isolement des ports. Un port isolé ne peut pas communiquer directement avec d'autres ports isolés, tandis que le port isolé peut envoyer et recevoir du trafic vers des ports non isolés.
Spanning Tree	Cliquez sur la case à cocher pour activer le Spanning Tree. Il permet de s'assurer que vous ne créez pas de boucles lorsque vous avez des chemins redondants dans le réseau. Pour s'assurer que le Spanning Tree prend effet sur le port, aller à l'Onglet **Configuration** et activer l'arborescence enjambant sur le commutateur.
LLDP-MED	Cliquez sur la case à cocher pour activer LLDP-MED (Link Layer Discovery Protocol-Media Endpoint Discovery) pour la découverte de périphériques et la configuration automatique des périphériques VoIP (Voice over Internet Protocol).
Bandwidth Control	Sélectionnez le type de fonctions de contrôle de bande passante pour contrôler le taux de trafic et spécifiez le seuil de trafic sur chaque port afin de faire bon usage de la bande passante réseau. Désactivé : désactivez le contrôle de bande passante pour le port. Rate limit : Sélectionnez rate limit pour limiter le taux de trafic d'entrée/sortie sur chaque port. Avec cette fonction, la bande passante réseau peut être raisonnablement distribuée et utilisée. Stomr control : sélectionnez Storm Control pour permettre au commutateur de surveiller les images de diffusion, les images multidiffusions et les cadres UL (cadres unicast inconnus) dans le réseau. Si le taux de transmission des images dépasse le taux spécifié, les images seront automatiquement écartées pour éviter la tempête de diffusion réseau.
Ingress Rate Limit	Avec la limite de taux sélectionnée, cliquez sur la case à cocher et spécifiez la limite de taux supérieure pour recevoir les paquets sur le port.

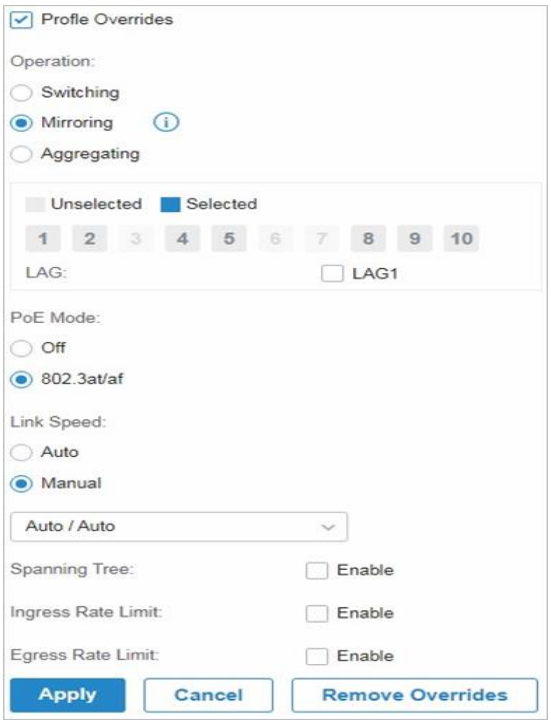
Egress Rate Limit	Lorsque la limite de taux est activée, cliquez sur la case à cocher et spécifiez la limite de taux supérieure pour l'envoi de paquets sur le port.
Broadcast Threshold	Avec **storm control** sélectionné, cliquez sur la case à cocher et spécifiez la limite de taux supérieure pour recevoir les images de diffusion. Le trafic de diffusion dépassant la limite sera traité selon les configurations Action.
Multicast Threshold	Avec storm control sélectionné, cliquez sur la case à cocher et spécifiez la limite de débit supérieure pour recevoir des images multidiffusion. Le trafic multidiffusion dépassant la limite sera traité selon les configurations Action.
UL-Frame Threshold	Avec **Storm Control** sélectionné, cliquez sur la case à cocher et spécifiez la limite de débit supérieure pour recevoir des images unicast inconnues. Le trafic dépassant la limite sera traité selon les configurations Action.
Action	Lorsque Storm Control a été sélectionné, sélectionnez l'action que le commutateur prendra lorsque le trafic dépasse sa limite correspondante. Drop: Avec Drop sélectionné, le port baisse les images suivantes lorsque le trafic dépasse la limite. **Shutdown**: Avec shutdown sélectionné, le port sera arrêté lorsque le trafic dépasse la limite.

- **Configure a Mirroring Port**

Si vous sélectionnez Mirroring en tant qu'opération, le port modifié peut être configuré en tant que port de mise en miroir. Spécifiez d'autres ports comme port en miroir, et le commutateur envoie une copie des trafics passant par le port en miroir au port de mise en miroir. Vous pouvez utiliser la mise en miroir pour analyser le trafic réseau et résoudre les problèmes de réseau.

Pour configurer la mise en miroir, sélectionnez le port en miroir ou le LAG, spécifiez les paramètres suivants, puis cliquez sur Apply. Pour supprimer les modifications, cliquez sur Remove Overrides et toutes les configurations de profil deviennent les mêmes que le profil appliqué.

Notez que les ports de mise en miroir et les ports membres de LAG ne peuvent pas être sélectionnés comme ports en miroir.



PoE Mode	(Only for PoE ports) Select the PoE mode for the port. Off: Disable PoE on the PoE port. 802.3at/af: Enable PoE on the PoE port.
Link Speed	Select the speed mode for the port. Auto: The port negotiates the speed and duplex automatically. Manual: Specify the speed and duplex from the drop-down list manually.
Spanning Tree	Cliquez sur la case à cocher pour activer l'arborescence enjambant. Il permet de s'assurer que vous ne créez pas de boucles lorsque vous avez des chemins redondants dans le réseau.
Ingress Rate Limit	Cliquez sur la case à cocher et spécifiez la limite de taux supérieure pour la réception des paquets sur le port. Avec cette fonction, la bande passante réseau peut être raisonnablement distribuée et utilisée.
Egress Rate Limit	Cliquez sur la case à cocher et spécifiez la limite de taux supérieure pour l'envoi de paquets sur le port. Avec cette fonction, la bande passante réseau peut être raisonnablement distribuée et utilisée.

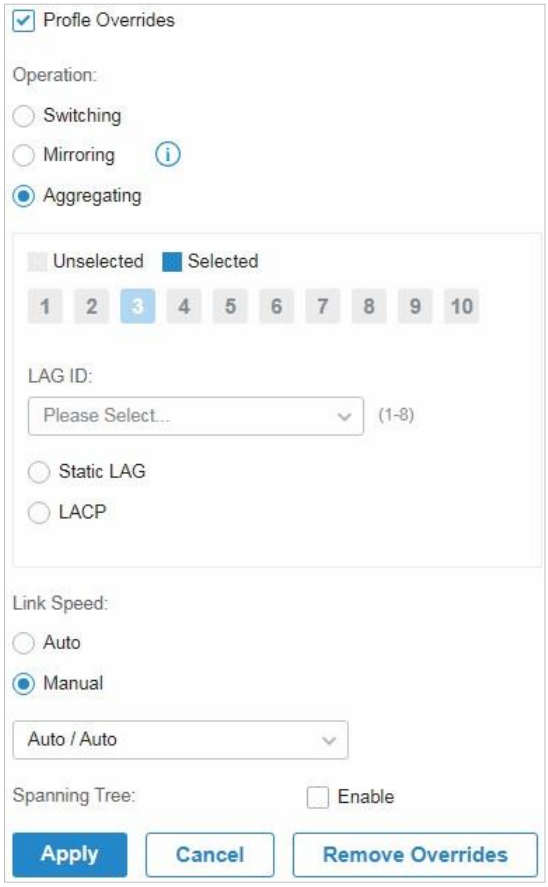
1. **Configurer un LAG**

   Si vous sélectionnez Aggregating en tant qu'opération, vous pouvez regrouper plusieurs ports physiques en une interface logique, ce qui peut augmenter la bande passante des liens et améliorer la fiabilité de la connexion.

   Recommandations de configuration :

- Assurez-vous que les deux extrémités du lien d'agrégation fonctionnent dans le même mode LAG. Par exemple, si l'extrémité locale fonctionne en mode LACP, la fin de l'homologue doit également être définie en mode LACP.
- Assurez-vous que les périphériques situés aux deux extrémités du lien d'agrégation utilisent le même nombre de ports physiques avec le même mode de contrôle de vitesse, duplex, jumbo et débit.
- Un port ne peut pas être ajouté à plus d'un GAL en même temps.
- **LACP ne prend pas en charge les liaisons demi-duplex.**
- Un LAG statique prend en charge jusqu'à huit ports membres. Tous les ports membres partagent la bande passante uniformément. Si un lien actif échoue, les autres liens actifs partagent la bande passante uniformément.
- Un LAG LACP prend en charge plusieurs ports membres, mais au plus huit d'entre eux peuvent fonctionner simultanément, et les autres ports membres sont des sauvegardes. À l'aide du protocole LACP, les commutateurs négocient les paramètres et déterminent les ports de travail. Lorsqu'un port de travail tombe en panne, le port de sauvegarde ayant la priorité la plus élevée remplace le port défectueux et commence à transférer des données.
- Le port membre d'un GAL suit la configuration du GAL mais pas la sienne. Une fois supprimé, le membre LAG sera configuré comme opération par défaut Tout le profil et la commutation.
- Le port activé avec port security, port mirror, MAC Address Filtering ou 802.1X ne peut pas être ajouté à un GAL, et le port membre d'un LAG ne peut pas être activé avec ces fonctions.

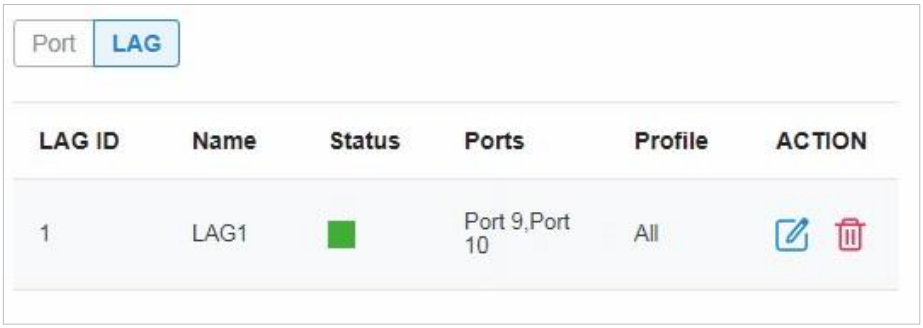
   Pour configurer un nouveau GAL, sélectionnez d'autres ports à ajouter au LAG, spécifiez l'ID LAG et choisissez un type DEG. Cliquez sur Apply. Pour supprimer les modifications, cliquez sur Remove Overrides et toutes les configurations de profil deviennent les mêmes que le profil appliqué. Pour d'autres paramètres, configurez-les sous l'onglet LAG.



LAG ID	Spécifiez l'ID LAG du LAG. Notez que l'ID LAG doit être unique. La valeur valide de l'ID LAG est déterminée par le nombre maximal de LAG pris en charge par votre commutateur. Par exemple, si votre commutateur prend en charge jusqu'à 14 LAG, la valeur valide varie de 1 à 14.
Static LAG	Sélectionnez le type LAG comme GAL statique et les ports membres sont ajoutés manuellement au LAG.
LACP	Sélectionnez le type LAG comme LACP (Link Aggregation Control Protocol) et le commutateur utilise LACP pour implémenter l'agrégation dynamique des liens et la désagrégation. LACP étend la flexibilité des configurations LAG.
Link Speed	Sélectionnez le mode de vitesse du port. Auto: Le port négocie automatiquement la vitesse et le duplex. Manuel: Spécifier manuellement la vitesse et le duplex de la liste déroulante.
Spanning Tree	Cliquez sur la case à cocher pour activer l'arborescence enjambant. Il permet de s'assurer que vous ne créez pas de boucles lorsque vous avez des chemins redondants dans le réseau. Pour vous assurer que l'arbre enjambe prend effet sur le GAL, accédez à l'onglet Config et activez Spanning tree

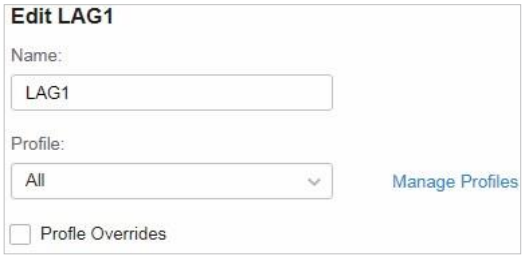
■ LAG

LAGs (Liens Groupes d'agrégation) sont des interfaces logiques agrégées, ce qui peut augmenter la bande passante de liaison et améliorer la fiabilité de la connexion. Vous pouvez afficher et modifier les GAL sous l'onglet GAL. Pour configurer les ports physiques en tant que LAG, reportez-vous à Configure a LAG.



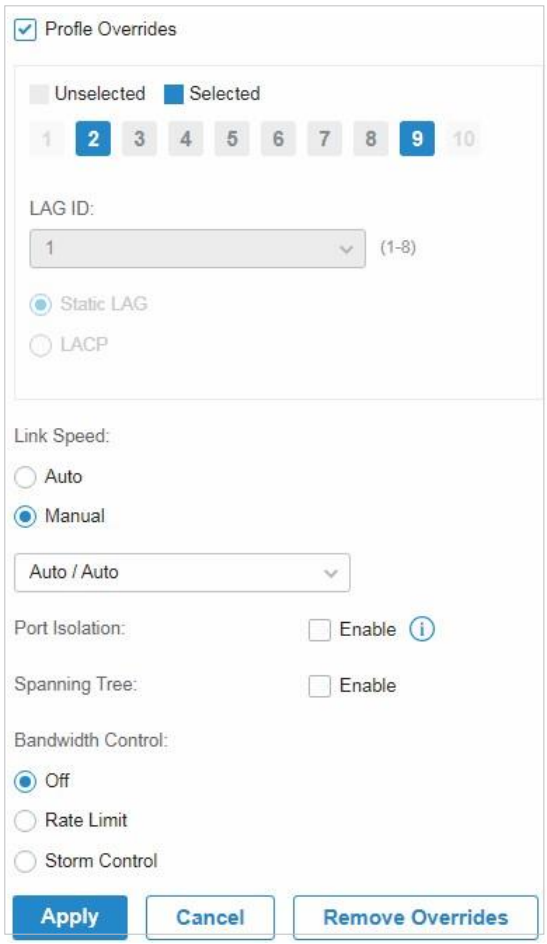
Status	Affiche l'état dans différentes couleurs. : Le profil LAG est Désactivé. Pour l'activer, cliquez pour modifier le profil. : Le port est activé, mais aucun périphérique ou client n'y est connecté. : Les ports LAG fonctionnent à 1000 Mbps. : Le port LAG fonctionne à 10/100 Mbps.
Ports	Affiche le nombre de ports lag.
Profile	Affiche le profil appliqué au port.
Action	: Cliquez pour modifier le nom du port et configurer le profil appliqué au port. : Cliquez pour supprimer le GAL. Une fois supprimés, les ports seront configurés comme opération par défaut Tout le profil et la commutation. Vous pouvez configurer les ports sous l'onglet Port.

Cliquez sur pour configurer le nom LAG et le profil appliqué.



Name	Entrez le nom du port .
Profile	Sélectionnez le profil appliqué au port dans la liste déroulante. Cliquez sur Manage Profiles pour afficher et gérer les profils. Pour plus de détails, reportez-vous à Configure Wired Networks.
Profile Overrides	Cliquez sur la case à cocher pour remplacer le profil appliqué. Les paramètres à configurer varient dans les modes Opération.

Avec les substitutions de profil activées, vous pouvez resélectionner les membres LAG et configurer les paramètres suivants.



Link Speed	Sélectionnez le mode de vitesse du port. Auto: Le port négocie automatiquement la vitesse et le duplex. Manuel: Spécifiez manuellement la vitesse et le duplex de la liste déroulante.
Spanning Tree	Cliquez sur la case à cocher pour activer Spanning Tree. Il permet de s'assurer que vous ne créez pas de boucles lorsque vous avez des chemins redondants dans le réseau. Pour vous assurer que l'arborescence s'étend sur le GAL, accédez à l'onglet Config et activez Spanning tree

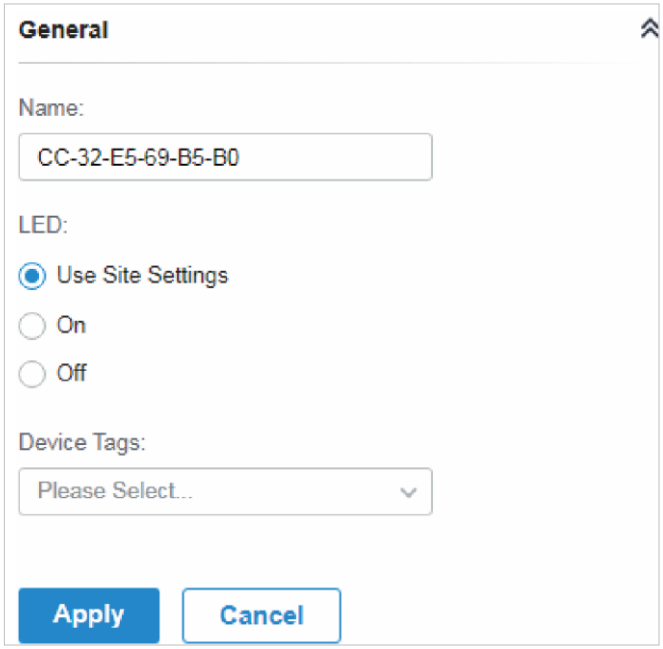
Bandwidth Control	Sélectionnez le type de fonctions de contrôle de bande passante pour contrôler le taux de trafic et le seuil de trafic sur chaque port afin d'assurer les performances du réseau. Off: Désactiver Bandwidth Control pour le port. Rate Limit: Sélectionnez limite tarifaire pour limiter le taux de trafic d'entrée/sortie sur chaque port. Avec cette fonction, la bande passante réseau peut être raisonnablement distribuée et utilisée. Storm Control: Sélectionnez Storm Control pour permettre au commutateur de surveiller les images de diffusion, les images multidiffusions et les cadres UL (cadres unicast inconnus) dans le réseau. Si le taux de transmission des images dépasse le taux spécifié, les images seront automatiquement écartées pour éviter la tempête de diffusion réseau.
Ingress Rate Limit	Avec la limite de taux sélectionnée, cliquez sur la case à cocher et spécifiez la limite de taux supérieure pour recevoir les paquets sur le port.
Egress Rate Limit	Avec la limite de taux sélectionnée, cliquez sur la case à cocher et spécifiez la limite de taux supérieure pour l'envoi de paquets sur le port.
Broadcast Threshold	Avec storm control sélectionné, cliquez sur la case à cocher et spécifiez la limite de taux supérieure pour recevoir les images de diffusion. Le trafic de diffusion dépassant la limite sera traité selon les configurations Action.
Multicast Threshold	Avec storm control sélectionné, cliquez sur la case à cocher et spécifiez la limite de débit supérieure pour recevoir des images multidiffusion. Le trafic multidiffusion dépassant la limite sera traité selon les configurations Action.
UL-Frame Threshold	Avec Storm Control sélectionné, cliquez sur la case à cocher et spécifiez la limite de débit supérieure pour recevoir des images unicast inconnues. Le trafic dépassant la limite sera traité selon les configurations Action.
Action	Avec Storm Control sélectionné, sélectionnez l'action que le commutateur prendra lorsque le trafic dépasse sa limite correspondante. Drop: Avec Drop sélectionné, le port dépose les images suivantes lorsque le trafic dépasse la limite. Shutdown: Avec shutdown sélectionné, le port sera arrêté lorsque le trafic dépasse la limite.

Configuration

DansConfig, cliquez sur les sections pour configurer les fonctionnalités appliquées au(s) commutateur(s) sélectionné(s), y compris les paramètres généraux, les services et les réseaux.

- **Généralités**

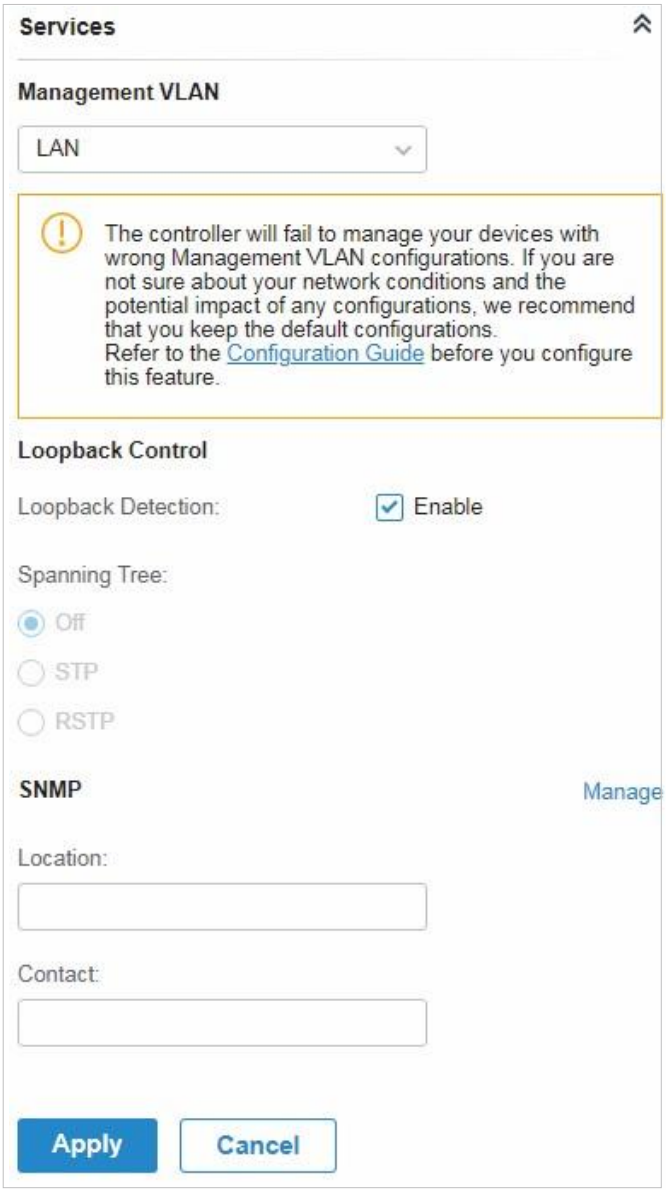
  En général, vous pouvez spécifier le nom de l'appareil et les paramètres LED du commutateur, et le catégoriser via les balises de périphérique.



Name	Uniquement pour la configuration d'un seul périphérique) Spécifiez le nom de l'appareil.
LED	Sélectionnez le fonctionnement des LED de cet appareil. Use Site Settings: La LED de l'appareil fonctionnera en suivant les paramètres du site. Pour afficher et modifier les paramètres du site, reportez-vous à Services. On/Off: La LED de l'appareil se maintiendra/.
Device Tags	Sélectionnez une balise dans la liste déroulante ou créez une nouvelle balise pour catégoriser l'appareil.

■ Services

Dans Services, vous pouvez configurer Management VLAN, Loopback Control et SNMP.



Management VLAN	Pour configurer Management VLAN, créez d'abord un réseau dans LAN, puis sélectionnez-le comme VLAN de gestion sur cette page. Pour plus de détails, reportez-vous àConfigure Wired Networks. La gestion VLAN est un VLAN créé pour améliorer la sécurité du réseau. Sans Management VLAN, les commandes de configuration et les paquets de données sont transmis dans le même réseau. Il existe des risques que des utilisateurs non autorisés accèdent à la page de gestion et modifient les configurations. Une gestion VLAN peut séparer le réseau de gestion du réseau de données et réduire les risques.
Loopback Detection	Lorsqu'il est activé, le commutateur vérifie régulièrement le réseau pour détecter le retour en boucle. **Notez que la détection de loopback et l'arborescence enjambant ne sont pas disponibles en même temps.**

Spanning Tree	Sélectionnez un mode pour l'arborescence enjambant. Cette fonctionnalité n'est responsable que lorsque la détection loopback est désactivée. Désactivé: Désactiver l'arborescence enjambant sur le commutateur. STP: Activer STP (Spanning Tree Protocal) pour empêcher les boucles dans le réseau. STP aide à bloquer des ports spécifiques des commutateurs pour créer une topologie sans boucle et détecter les changements de topologie et générer automatiquement une nouvelle topologie sans boucle. RSTP: Activer RSTP (Rapid Spanning Tree Protocal) pour empêcher les boucles dans le réseau. RSTP fournit les mêmes fonctionnalités que STP avec une convergence ree plus rapide. Priorité : Lorsque STP/RSTP activé, spécifiez la priorité pour le swith dans l'arborescence enjambant. Dans STP/RSTP, le commutateur ayant la plus haute priorité sera sélectionnée comme racine de l'arbre enjambant. Le commutateur avec la valeur inférieure a la priorité plus élevée.
SNMP	(Uniquement pour la configuration d'un seul périphérique), configurez SNMP pour écrire l'emplacement et les détails de contact. Vous pouvez également cliquer sur Gérer pour accéder aux paramètres > Services > SNMP, et pour la configuration détaillée du serviceSNMP, reportez-vous à SNMP.

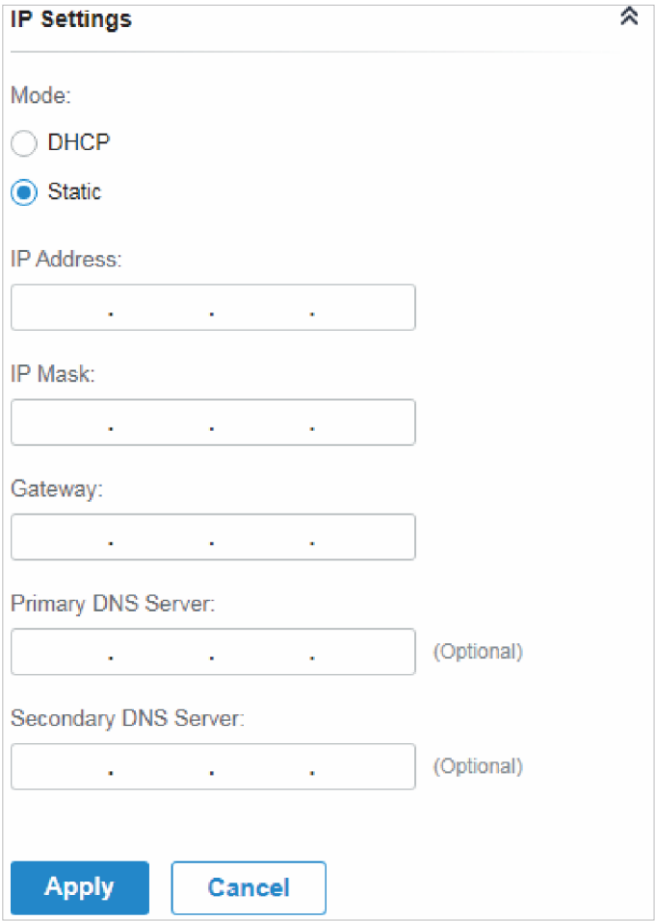
■ Paramètres IP (uniquement pour la configuration d'un seul périphérique)

Dans Paramètres IP, sélectionnez un mode IP et configurez les paramètres du périphérique.

Si vous sélectionnez DHCP comme mode, assurez-vous qu'il y a un serveur DHCP dans le réseau, puis l'appareil obtiendra automatiquement l'adresse IP dynamique à partir du serveur DHCP. Vous pouvez définir une adresse IP de secours pour conserver une adresse IP en réserve pour la situation dans laquelle l'appareil ne parvient pas à obtenir une adresse IP dynamique. Activer l'ip de secours, puis définir l'adresse IP, le masque IP et la passerelle.

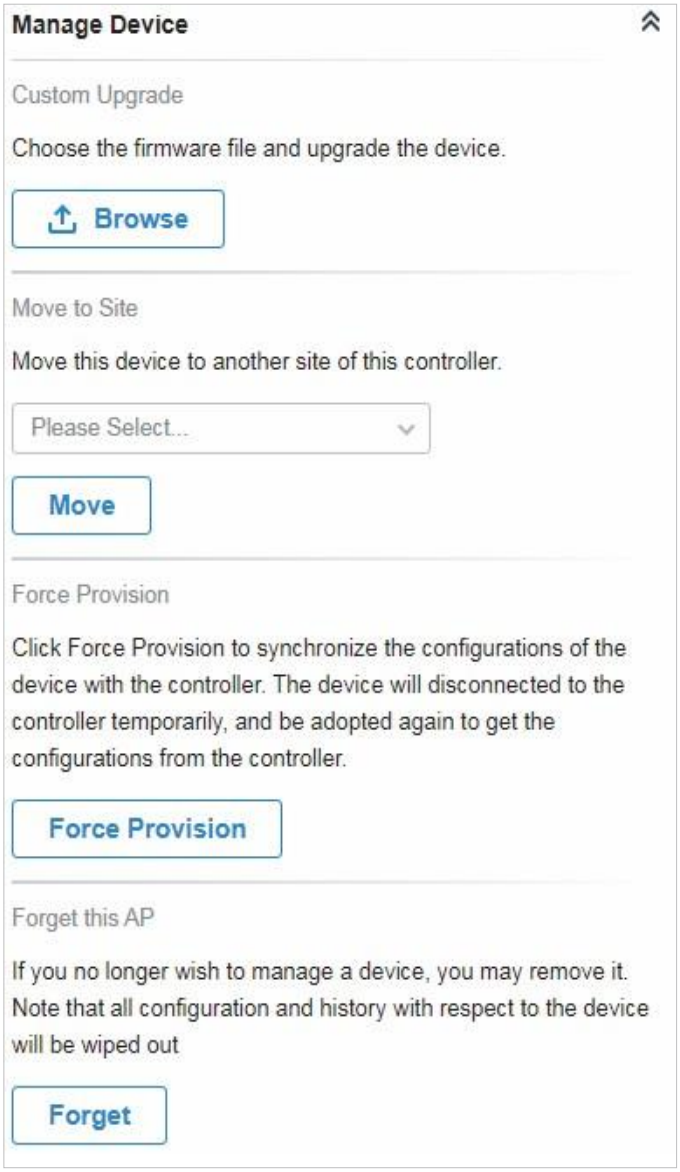


Si vous sélectionnez Statique comme mode, définissez l'adresse IP, le masque IP, la passerelle et le serveur DNS pour l'adresse statique.



■ **Gérer le périphérique**

Dans Gérer le périphérique, vous pouvez mettre à niveau manuellement la version du firmware de l'appareil, le déplacer vers un autre site, synchroniser les configurations avec le contrôleur et oublier le commutateur.



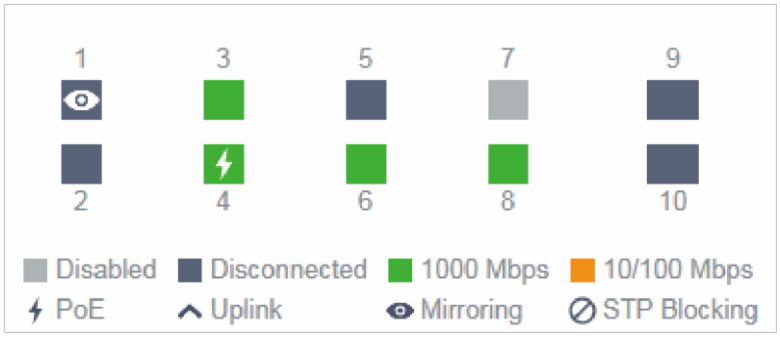
Custom Upgrade	Cliquez sur Browse et choisissez un fichier à partir de votre ordinateur pour mettre à niveau l'appareil. Lors de la mise à niveau, l'appareil sera redémarré et réadopté par le contrôleur.
Move to Site	Sélectionnez un site vers lequel l'appareil sera déplacé. Après avoir déménagé sur un autre site, les configurations d'appareils sur le site précédent seront remplacées par celle du nouveau site, et son historique de trafic sera effacé.
Force Provision	(Uniquement pour la configuration d'un seul périphérique) Cliquez sur Force Provision pour synchroniser les configurations de l'appareil avec le contrôleur. L'appareil perdra temporairement la connexion et sera adopté à nouveau au contrôleur pour obtenir les configurations du contrôleur.
Forget	Cliquez sur Forget et puis l'appareil sera retiré du contrôleur. Une fois oubliées, toutes les configurations et l'historique liés à l'appareil seront effacés.

6. 3. 2 Moniteur des Switches

Un panneau et quatre onglets sont fournis pour surveiller l'appareil dans la fenêtre Propriétés : Panneau de suivi, Détails, Clients et Statistiques.

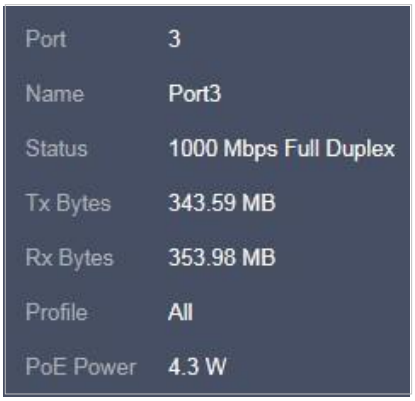
Panneau de moniteur

Le panneau moniteur affiche les ports du commutateur et utilise des couleurs et des icônes pour indiquer l'état de connexion et le type de port. Lorsque le commutateur est en attente ou déconnecté, tous les ports sont désactivés.



PoE	Un port PoE connecté à un dispositif alimenté (PD).
Uplink	Port de liaison vers l'avant connecté à WAN.
Mirroring	Un port de mise en miroir qui reflète un autre port d'interrupteur.
STP Blocking	Port dans l'état Blocage dans un Spanning tree. Il reçoit et envoie des paquets BPDU (Bridge Protocal Data Unit) pour maintenir le Spanning Tree. D'autres paquets sont supprimés.

Pour plus de détails, vous pouvez placer le curseur au-dessus de l'icône de port (à l'exception des ports désactivés). Les informations affichées varient en fonction de l'état de connexion et du type de port.



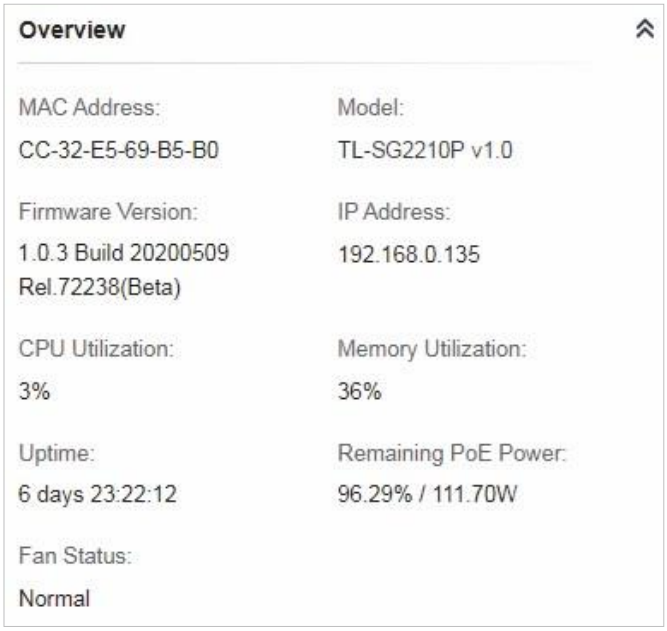
Status	Affiche la vitesse de négociation du port
Tx Bytes	Affiche la quantité de données transmises sous forme d'octets
Rx Bytes	Affiche la quantité de données reçues sous forme d'octets.
Profile	Affiche le nom du profil appliqué au port, qui définit la façon dont les paquets dans les deux instructions d'entrée et d'évacuation sont traités. Pour une configuration détaillée, reportez-vous à Créer des profils
PoE Power	Affiche le pourcentage de paquets reçus qui présentent des erreurs et le pourcentage de paquets qui ont été supprimés
Uplink	Affiche le nom du périphérique connecté au port uplink
Mirroring From	Affiche le nom du port qui est miroir
LAG ID	Affiche le nom des ports agrégés dans une interface logique.

Détails

Dans les détails, vous pouvez consulter les informations de base, les informations de trafic et les informations radio de l'appareil pour connaître l'état d'exécution de l'appareil.

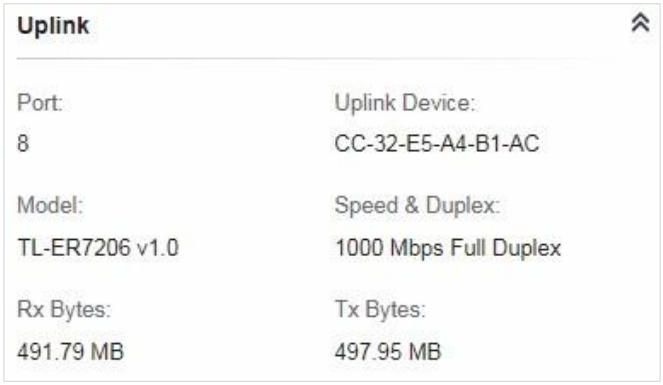
- **Aperçu**

  Dans Overview, vous pouvez afficher les informations de base de l'appareil. Les informations énumérées seront variées en raison du modèle et de l'état de l'appareil.



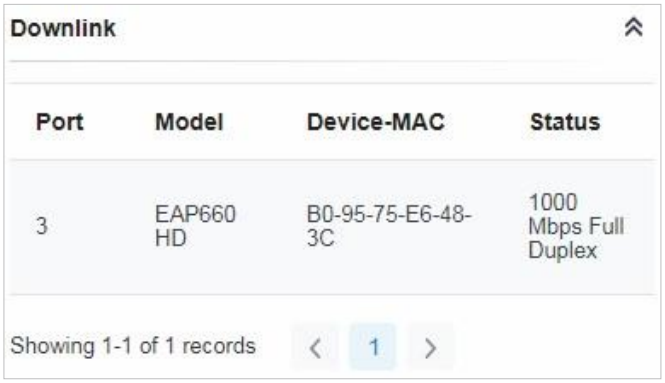
■ **Uplink (uniquement pour le commutateur connecté à un routeur/commutateur géré par Omada dans l'état connecté)**

Cliquez sur Uplink pour afficher les informations de liaison vers le haut, y compris le port de liaison, le périphérique de liaison vers le haut, la vitesse de négociation et le taux de transmission.



■ **Downlink (uniquement pour le commutateur connecté aux périphériques gérés par Omada dans l'état connecté)**

Cliquez sur Downlink pour afficher les informations de liaison vers le bas, y compris les ports de liaison vers le bas, le nom et le modèle des périphériques ainsi que la vitesse de négociation.



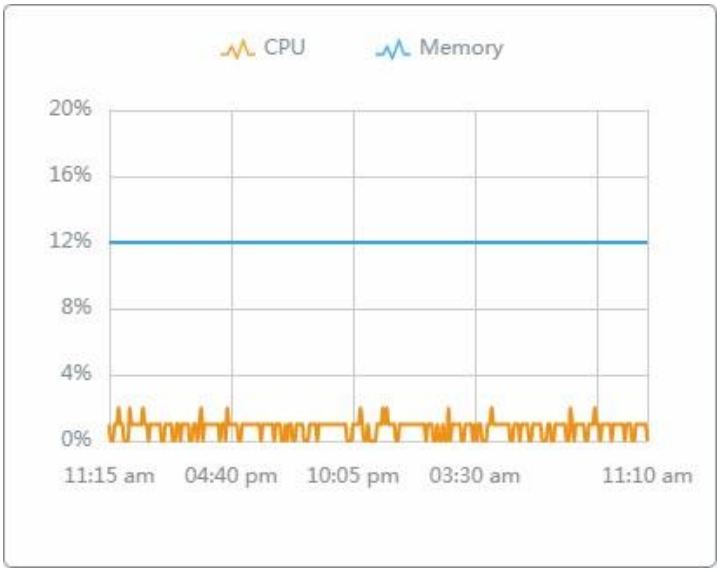
Clients

Dans Clients, vous pouvez afficher les informations des clients connectés au commutateur, y compris le nom du client, l'adresse IP et le port connecté. Vous pouvez cliquer sur le nom du client pour ouvrir sa fenêtre Propriétés.



Statistiques

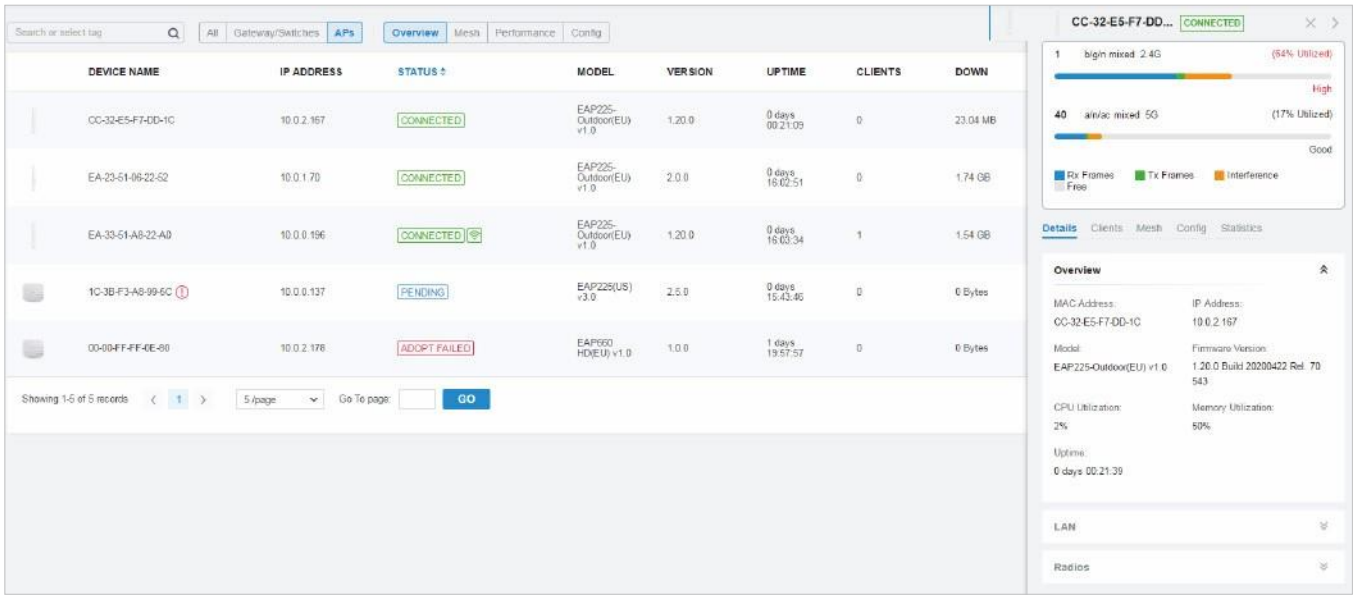
Dans Les statistiques, vous pouvez surveiller le processeur et la mémoire de l'appareil au cours des dernières 24 heures via des graphiques. Pour afficher les statistiques de l'appareil dans certaines périodes, cliquez sur le graphique pour View the Statistics of the Network.



6. 4 Configurer et surveiller les EAP

Dans la fenêtre Propriétés, vous pouvez configurer un ou certains EAP connectés au contrôleur et surveiller les performances et les statistiques. Les configurations modifiées dans la fenêtre Propriétés seront appliquées uniquement aux AP(s) sélectionnés. Par défaut, toutes les configurations sont synchronisées avec le site actuel.

Pour ouvrir la fenêtre Propriétés, cliquez sur l'entrée d'un AP ou cliquez sur l'icône pour sélectionner les AP pour la configuration du lot. Un panneau de moniteur et plusieurs onglets sont répertoriés dans la fenêtre Propriétés. La plupart des fonctionnalités à configurer sont rassemblées dans l'onglet Config, telles que IP, radios, SSID et VLAN, tandis que d'autres onglets sont principalement utilisés pour surveiller l'appareil.



Note:

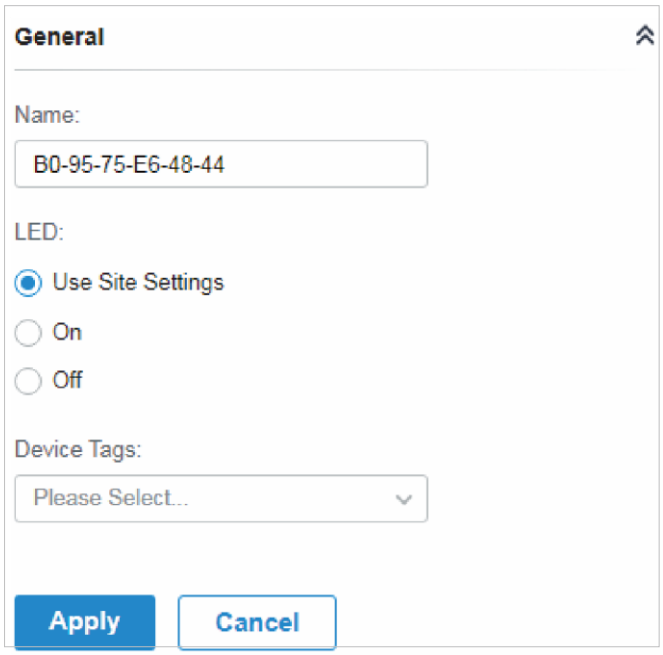
- Les fonctions disponibles dans la fenêtre varient en raison du modèle et de l'état de l'appareil.
- Dans Batch Config, vous ne pouvez configurer que les périphériques sélectionnés et les configurations inchangées conserveront les paramètres actuels.
- Dans Batch Config, si certaines fonctions, telles que la bande de 5 GHz, ne sont disponibles que sur certains EAP sélectionnés, les configurations correspondantes ne prendront pas effet. Pour les configurer avec succès, vérifiez d'abord le modèle des périphériques sélectionnés.

6. 4. 1 Configurer les EAP's

Dans la fenêtre Propriétés, cliquez sur Config, puis sur les sections pour configurer les fonctionnalités appliquées aux AP(s) sélectionnés), y compris les paramètres généraux, les paramètres IP, les radios, les SSID, le VLAN, le SNMP et les fonctions avancées.

Généralités

En général, vous pouvez spécifier le nom de l'appareil et les paramètres LED de l'AP, et le catégoriser via des balises de périphérique.

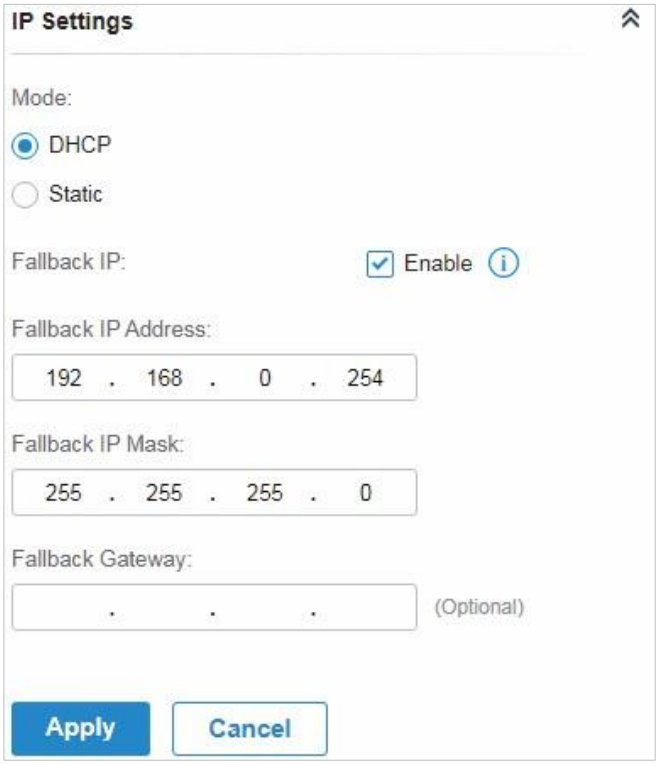


LED	Sélectionnez le fonctionnement des LED de cet appareil. Paramètres du site: la LED de l'appareil fonctionnera en suivant les paramètres du site. Pour afficher et modifier les paramètres du site, reportez-vous aux Services. On/Off:La LED de l'appareil se maintiendra/s'en va.
Name	Uniquement pour la configuration d'un seul périphérique) Spécifier un nom de l'appareil
Device Tags	Sélectionnez une balise dans la liste déroulante ou créez une nouvelle balise pour catégoriser l'appareil

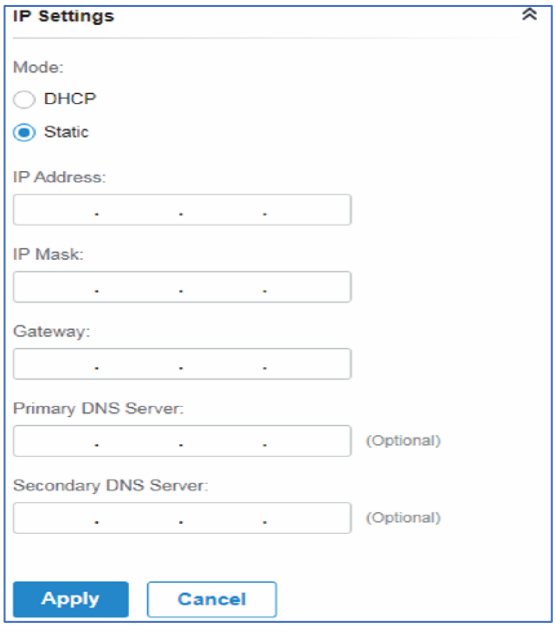
■ **Paramètres IP (uniquement pour la configuration d'un seul périphérique)**

Dans Paramètres IP, sélectionnez un mode IP et configurez les paramètres du périphérique.

Si vous sélectionnez DHCP comme mode, assurez-vous qu'il y a un serveur DHCP dans le réseau, puis l'appareil obtiendra automatiquement l'adresse IP dynamique à partir du serveur DHCP. Vous pouvez définir une adresse IP de secours pour conserver une adresse IP en réserve pour la situation dans laquelle l'appareil ne parvient pas à obtenir une adresse IP dynamique. Activez l'ip de secours, puis définissez l'adresse IP, le masque IP et la passerelle.

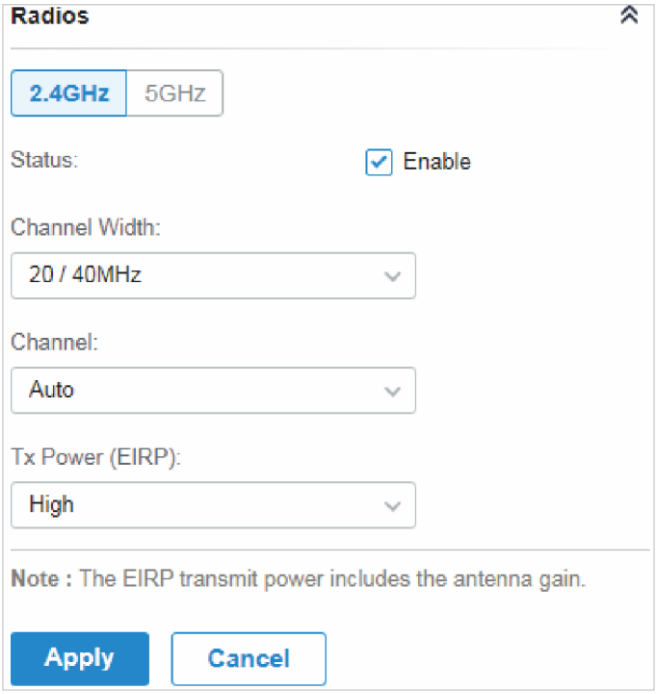


Si vous sélectionnez Statique comme mode, définissez l'adresse IP, le masque IP, la passerelle et le serveur DNS pour l'adresse statique.



■ Radios

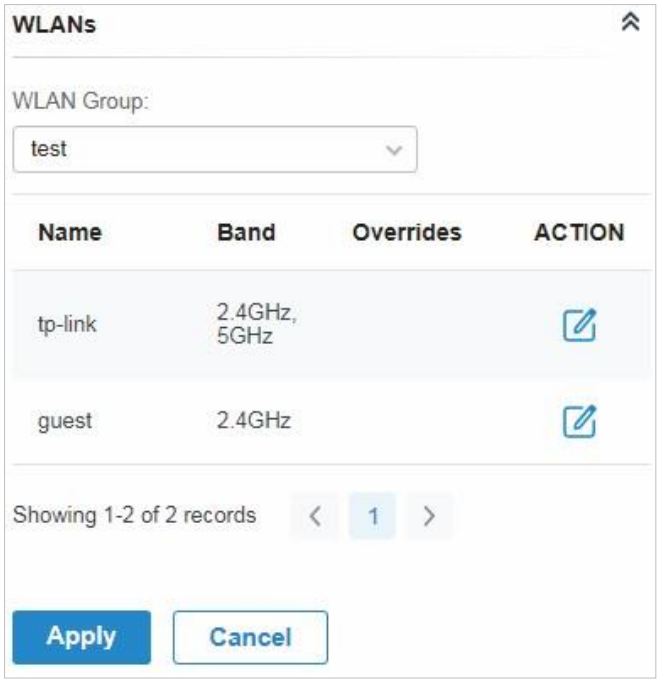
Dans radios, vous pouvez contrôler comment et quel type de signaux radio le PAE émet. Sélectionner la bande fréquence 2.4GHz 5GHz et configurer les paramètres suivants.



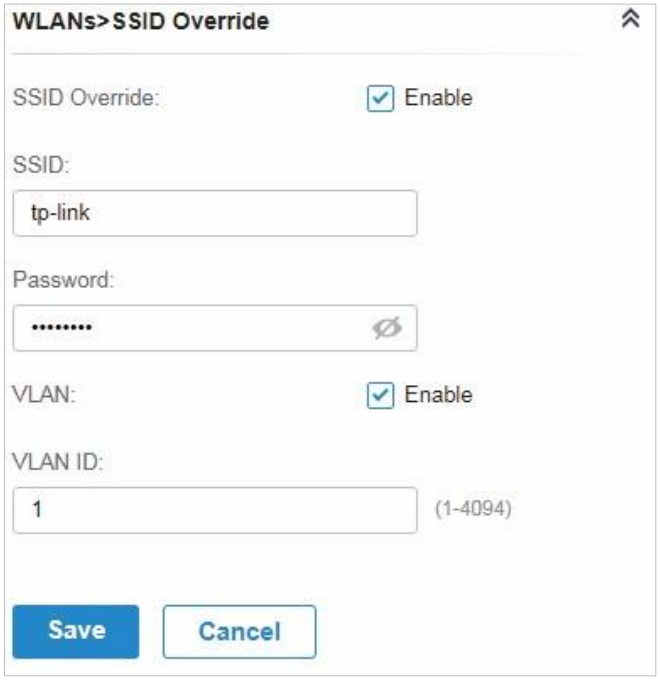
Status	Si vous désactivez la bande de fréquences, la radio allumée s'éteint.
Channel Width	Spécifiez la largeur du canal de la bande. Deux bandes ont des options différentes : 20 MHz, 40 MHz et 20/40 MHz pour 2,4 GHz, et 20 MHz, 40 MHz, 80 MHz et 20/40/80 MHz pour 5 GHz. Notez que les canaux d'option 20/40 MHz et 20/40/80 MHz permettent des débits de données plus élevés, mais laissent moins de canaux disponibles pour les autres appareils de 2,4 GHz et 5 GHz.
Channel	Spécifiez le canal d'exploitation de l'EAP pour améliorer les performances sans fil. Si vous sélectionnez Automatique pour le paramètre de canal, le PAE analyse les canaux disponibles et sélectionne le canal où le trafic le moins est détecté.
Tx Power	Spécifiez la puissance Tx (Transmission Power) dans les 4 options : Faible, Moyenne, Haute et Personnalisée. La puissance réelle de Low, Medium et High est basée sur la puissance de transmission minimale (Min. Txpower) et la puissance de transmission maximale (Max. TxPower), qui peut varier selon les pays et les régions. Faible: Min. TxPower + (Max. TxPower-Min. TxPower) * 20% (arrondir la valeur) Moyen: Min. TxPower + (Max. TxPower-Min. TxPower) * 60% (arrondir la valeur) Haut: Max. TxPower Personnalisé: Spécifiez manuellement la valeur.

- **Wlan**

Dans les WLAN, vous pouvez appliquer le groupe WLAN au EAP et spécifier un autre nom et mot de passe SSID pour remplacer le SSID du groupe WLAN. Après cela, les clients ne peuvent voir le nouveau SSID et utiliser le nouveau mot de passe pour accéder au réseau. Pour créer ou modifier des groupes WLAN, reportez-vous à Configure Wireless Networks.



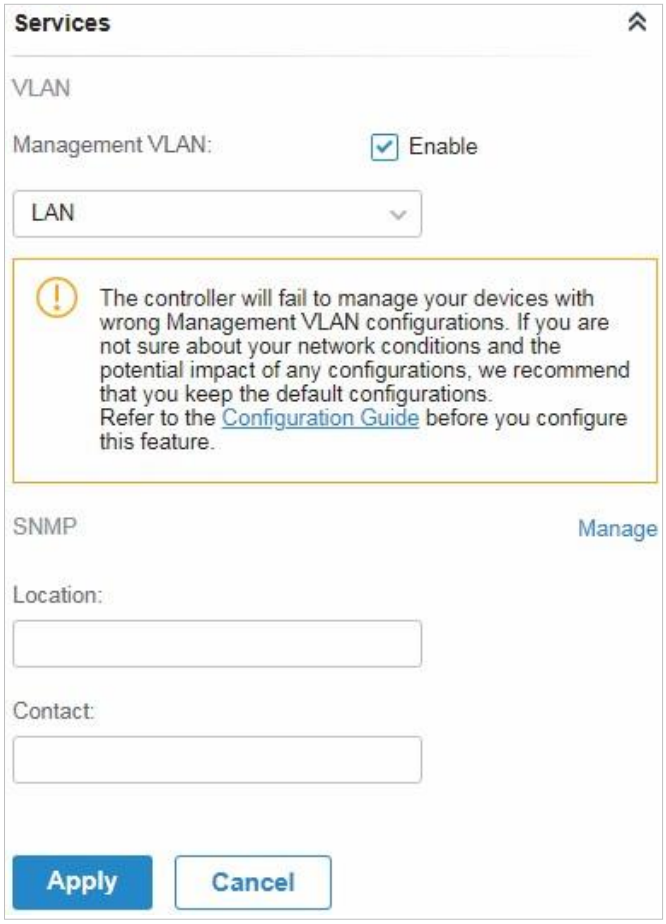
(Uniquement pour la configuration d'un seul périphérique) Pour remplacer le SSID, sélectionnez un groupe WLAN, cliquez dans l'entrée, puis la page suivante s'affiche.



SSID Override	Activer ou désactiver la substitution SSID sur le PAE. Si SSID Override activé, spécifiez le nouveau SSID et le mot de passe pour remplacer le paramètre actuel.
VLAN	Activer ou désactiver VLAN. Si VLAN est activé, entrez un ID VLAN pour ajouter le nouveau SSID au VLAN.

- **Services**

Dans Services, vous pouvez configurer Management VLAN pour protéger votre réseau et SNMP pour noter l'emplacement et les coordonnées.

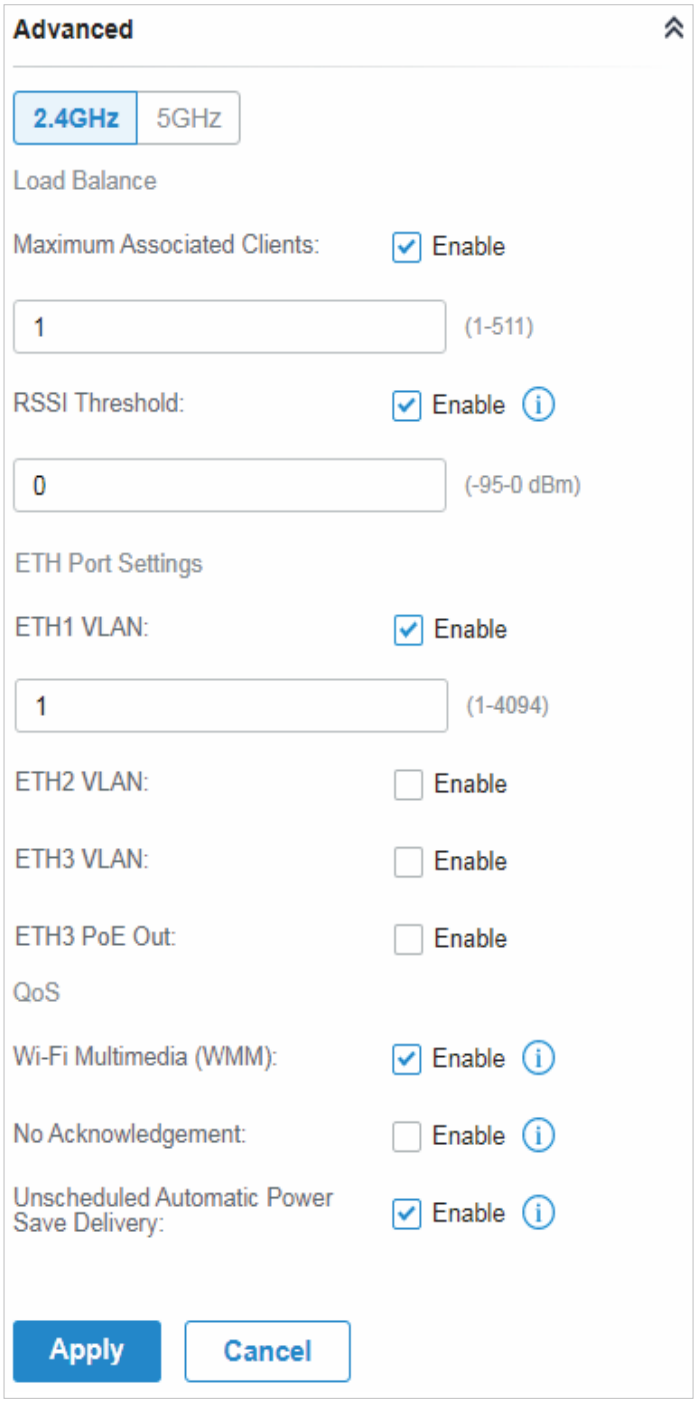


Management VLAN	Pour configurer Management VLAN, créez d'abord un réseau dans LAN, puis sélectionnez-le comme VLAN de gestion sur cette page. Pour plus de détails, reportez-vous à Configure Wired Networks. La gestion VLAN est un VLAN créé pour améliorer la sécurité du réseau. Sans Management VLAN, les commandes de configuration et les paquets de données sont transmis dans le même réseau. Il existe des risques que des utilisateurs non autorisés accèdent à la page de gestion et modifient les configurations. Une gestion VLAN peut séparer le réseau de gestion du réseau de données et réduire les risques.
SNMP	(Uniquement pour la configuration d'un seul périphérique) Configurez SNMP pour noter l'emplacement et les détails de contact. Vous pouvez également cliquer sur Manage dans Settings > Services > SNMP, et pour la configuration détaillée du service SNMP, reportez-vous à SNMP.

■ **Avancé**

Dans Advanced, configurez Load Balance et QoS pour mieux utiliser les ressources réseau. Load Balance peut contrôler le numéro de client associé au PAE, tandis que QoS peut optimiser les performances lors de la gestion de trafics sans fil différenciés, y compris les données IP traditionnelles, VoIP (Voice-over Internet Protocol), et d'autres types de médias audio, vidéo, streaming.

Sélectionner la bande de fréquen 2.4GHz 5GHz



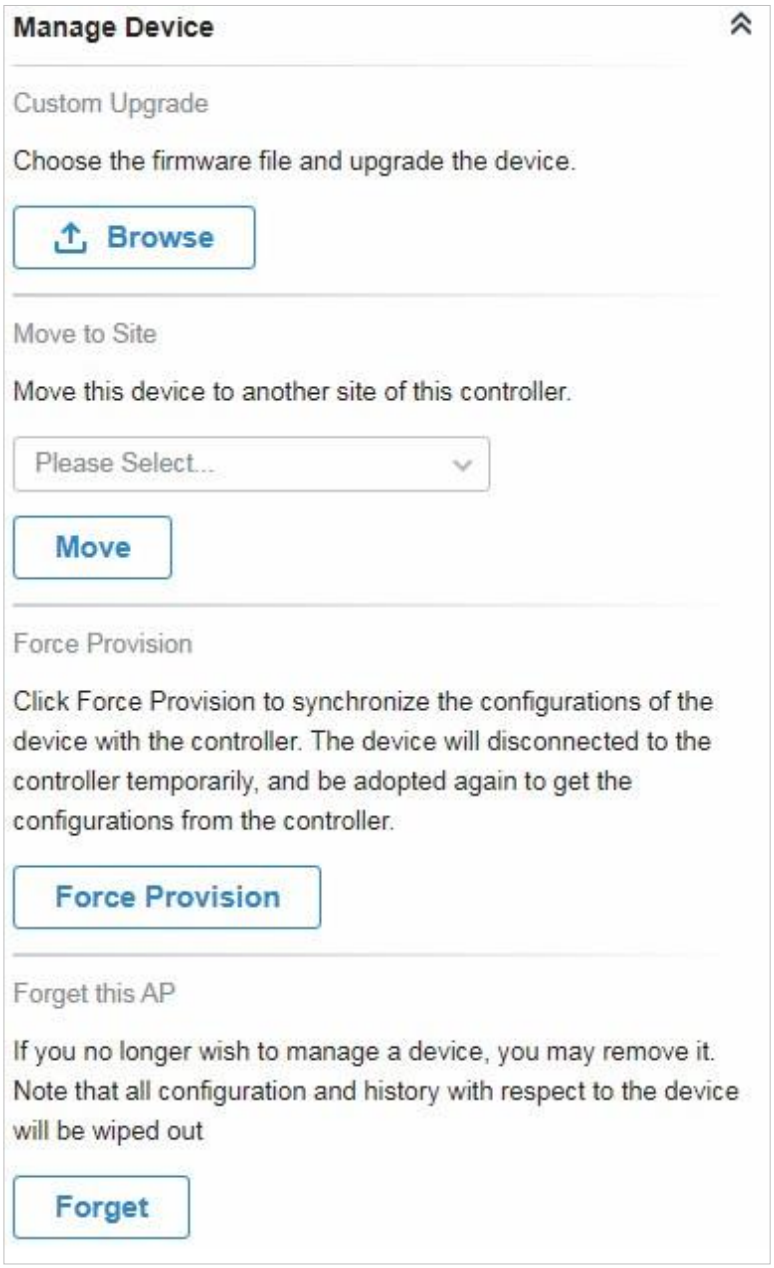
et configurer les paramètres et fonctionnalités suivants.

Max Associated Clients	Activez cette fonction et spécifiez le nombre maximal de clients connectés. Si le client connecté atteint le nombre maximal, l'EAP déconnecte ceux qui ont des signaux plus faibles pour faire de la place aux autres clients qui demandent des connexions.
RSSI Threshold	Activez cette fonction et entrez le seuil de RSSI (Indication de force du signal reçu). Si la force du signal du client est plus faible que le seuil, le client perdra sa connexion avec le EAP.

ETH VLAN/ETH2 VLAN/ ETH3 VLAN	(Uniquement pour Wall Plate AP) Activez cette fonction et ajoutez le port LAN de l'AP correspondant au VLAN spécifié ici. Ensuite, les hôtes connectés à ce EAP ne peuvent communiquer qu'avec les appareils de ce VLAN.
ETH3 PoE Out	(Uniquement pour Wall Plate AP avec le port PoE out) Activez cette fonction pour alimenter le périphérique connecté à ce port.
Wi-Fi Multimedia (WMM)	Avec wmm activé, le EAP maintient la priorité des paquets audio et vidéo pour une meilleure performance des médias.
No Acknowledgment	Permettre à cette fonction de spécifier que les EAP ne reconnaîtront pas les images avec QoS No Ack. Activing No Misacnowledge peut apporter un activage plus efficace, mais il peut augmenter les taux d'erreur dans un environnement de fréquence radio (RF) r bruyant.
Unscheduled Automatic Power Save Delivery	Lorsqu'elle est activée, cette fonction peut grandement améliorer la capacité d'économie d'énergie des clients.

■ Gérer le périphérique

Dans Gérer le périphérique, vous pouvez mettre à niveau manuellement la version du firmware de l'appareil, le déplacer vers un autre site, synchroniser les configurations avec le contrôleur et oublier l'AP.



Custom Upgrade	Cliquez sur Browse et choisissez un fichier à partir de votre ordinateur pour mettre à niveau l'appareil. Lors de la mise à niveau, l'appareil sera redémarré et réadopté par le contrôleur.
Move to Site	Sélectionnez un site vers lequel l'appareil sera déplacé. Après avoir déménagé sur un autre site, les configurations d'appareils sur le site précédent seront remplacées par celle du nouveau site, et son historique de trafic sera effacé.

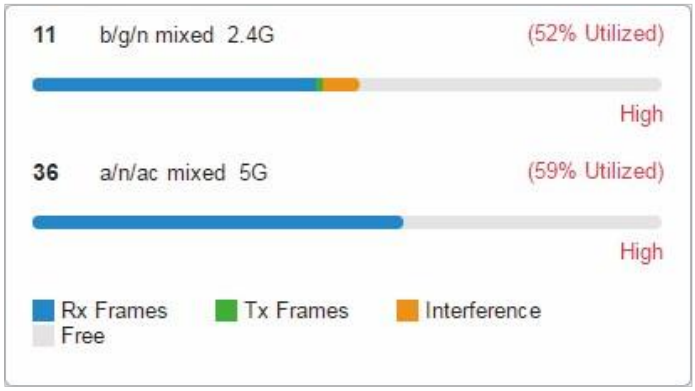
Force Provision	(Uniquement pour la configuration d'un seul périphérique) Cliquez sur Force Provision pour synchroniser les configurations de l'appareil avec le contrôleur. L'appareil perdra temporairement la connexion et sera adopté à nouveau au contrôleur pour obtenir les configurations du contrôleur.
Forget this AP	Cliquez sur Oublier, puis l'appareil sera supprimé du contrôleur. Une fois oubliées, toutes les configurations et l'historique liés à l'appareil seront effacés.

6. 4. 2 Surveiller les EAP's

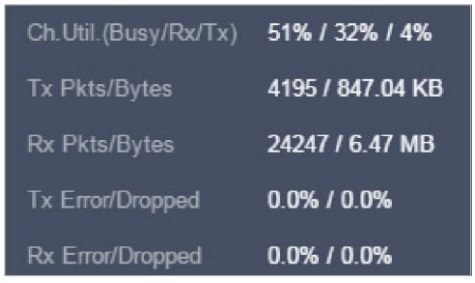
Un panneau et quatre onglets sont fournis pour surveiller l'appareil dans la fenêtre Propriétés : Panneau de suivi, Détails, Clients, Maillage et Statistiques.

Panneau de moniteur

Le panneau de surveillance illustre les informations actives sur les canaux de chaque bande de radio, y compris le canal de fonctionnement des EAP's, le mode radio et l'utilisation des canaux. Quatre couleurs sont utilisées pour indiquer le pourcentage de cadres Rx (bleu), Tx Frames (vert), Interférence (orange) et bande passante libre (gris).



Vous pouvez placer le curseur au-dessus de la barre de canal pour plus de détails.



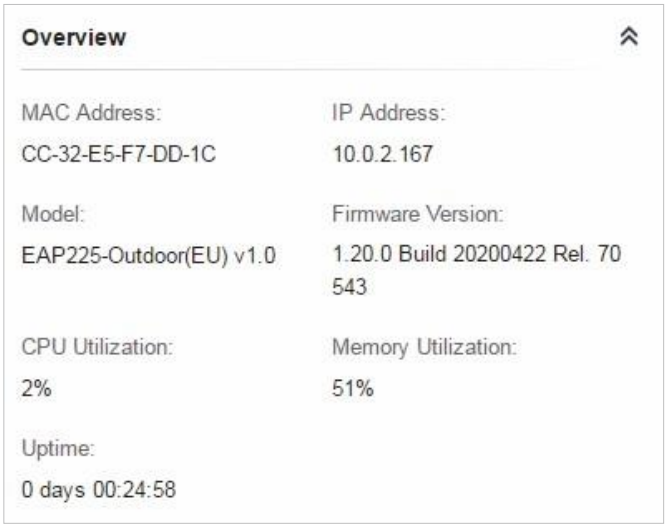
Ch.Util.(Busy/Rx/Tx)	Affiche les statistiques d'utilisation des canaux. **Occupé**: Affiche la somme de Tx, Rx, et aussi les interférences non-WiFi, ce qui indique à quel point le canal est occupé. **Rx**: Indique la fréquence à laquelle la radio est en mode de réception active. **Tx**: Indique la fréquence à laquelle la radio est en mode de transmission active.
Tx Pkts/Bytes	Affiche la quantité de données transmises sous forme de paquets et d'octets.
Rx Pkts/Bytes	Affiche la quantité de données reçues sous forme de paquets et d'octets.
Tx Error/Dropped	Affiche le pourcentage de paquets de transmission qui présentent des erreurs et le pourcentage de paquets qui ont été supprimés.
Rx Error/Dropped	Affiche le pourcentage de paquets de réception qui présentent des erreurs et le pourcentage de paquets qui ont été supprimés.

Détails

Dans les détails, vous pouvez afficher les informations de base, les informations de trafic et les informations radio de l'appareil pour connaître l'état d'exécution de l'appareil.

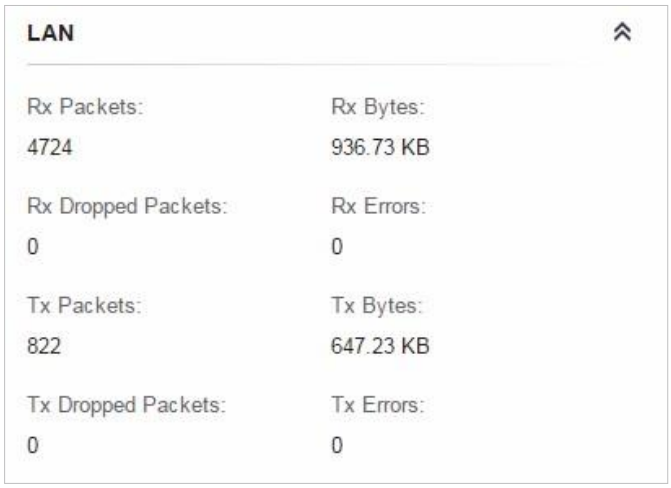
- **Aperçu**

  Dans Overview, vous pouvez afficher les informations de base de l'appareil. Les informations répertoriées varient en fonction de l'état de l'appareil.



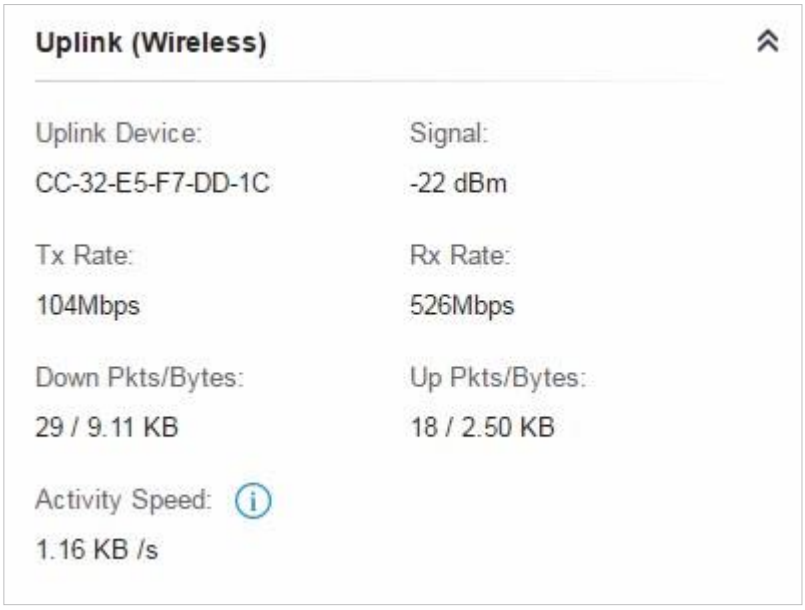
■ **LAN (Uniquement pour les périphériques dans l'état connecté)**

Cliquez sur LAN pour afficher les informations de trafic du port LAN, y compris le nombre total de paquets, la taille totale des données, le nombre total de pertes de paquets et la taille totale des données d'erreur dans le processus de réception et de transmission des données.



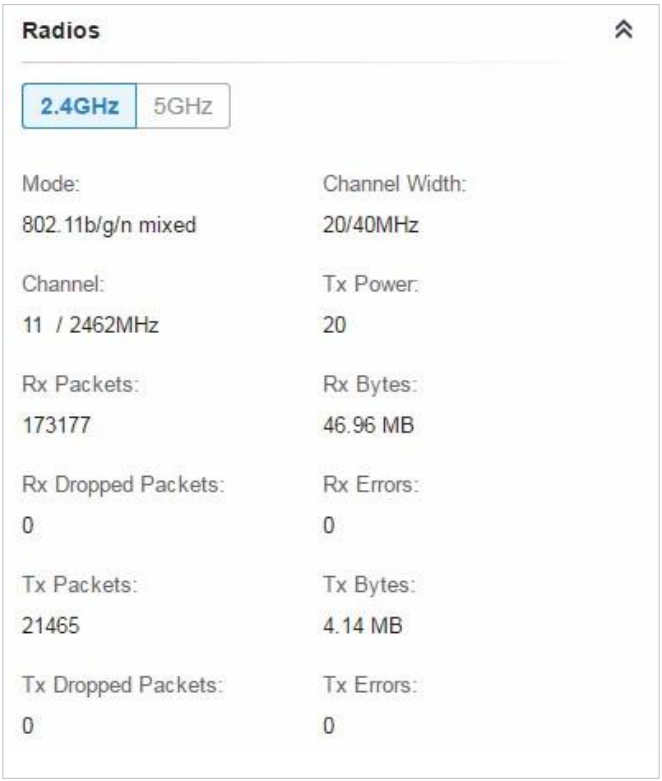
■ **Uplink (Sans fil) (uniquement pour les périphériques dans l'état connecté)**

Cliquez sur Uplink (Wireless) pour afficher les informations de trafic relatives à l'AP de liaison, y compris la force du signal, le taux de transmission, le rapport entre le nombre et la taille des paquets et le taux dynamique en aval.



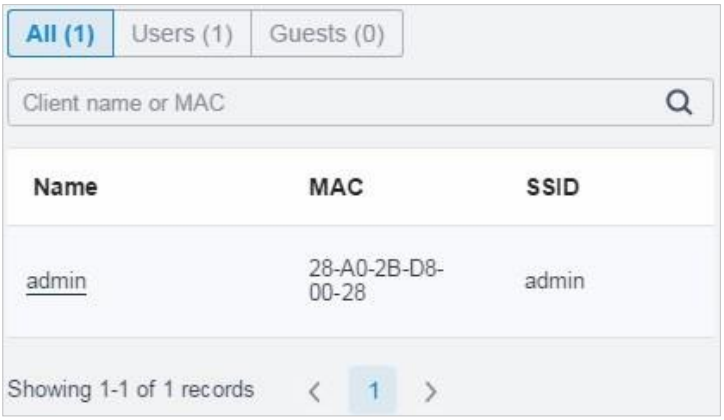
■ **Radios (uniquement pour les appareils dans l'état connecté)**

Cliquez sur Radio pour afficher les informations radio, y compris la bande de fréquences, le mode sans fil, la largeur du canal, le canal et la puissance de transmission. Vous pouvez également afficher les paramètres de réception/transmission de données sur chaque bande radio.



Clients

Dans Clients, vous pouvez afficher les informations des utilisateurs et des invités qui se connectent à l'AP, y compris le nom du client, l'adresse MAC et le SSID connecté. Les utilisateurs sont des clients connectés au SSID de l'AP avec guest network désactivé, tandis que les clients sont des clients connectés à cela avec Guest Network activé. Vous pouvez cliquer sur le nom du client pour ouvrir sa fenêtre Propriétés.



Maillage (uniquement pour les périphériques en attente/connectés/isolés prenant en charge Mesh)

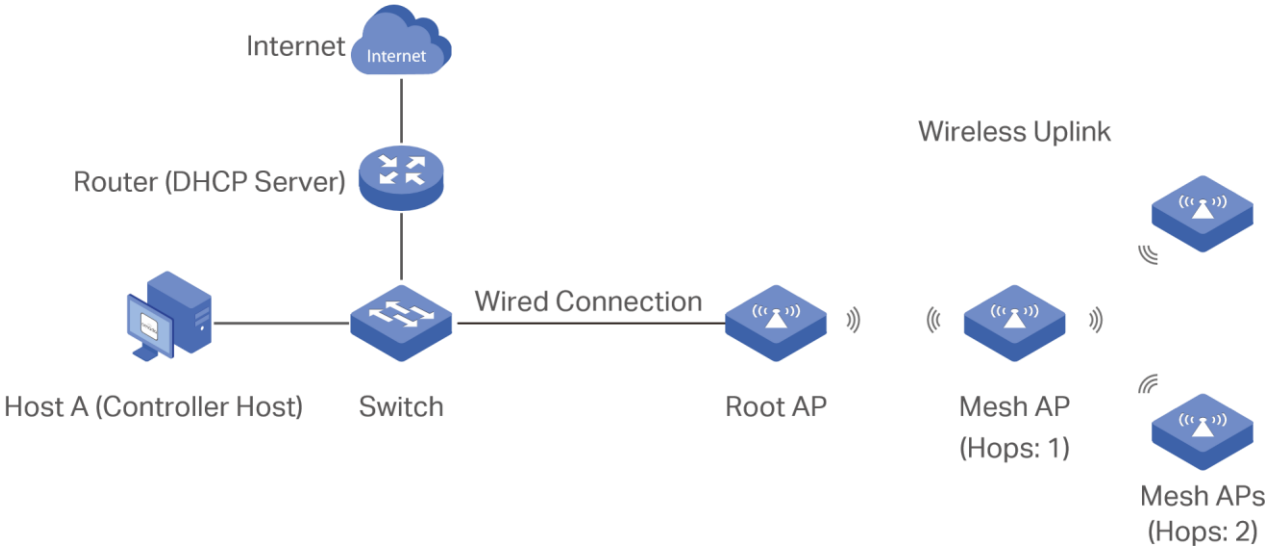
Mesh est utilisé pour établir un réseau sans fil ou développer un réseau câblé via une connexion sans fil sur une bande radio de 5 GHz. Dans l'application pratique, il peut aider les utilisateurs à déployer facilement des AP sans avoir besoin du câble Ethernet. Une fois le réseau de maillage établi, les EAP peuvent être configurés et gérés dans le contrôleur Omada de la même manière que les EAP câblés. Pendant ce temps, en raison de la capacité de s'auto-organiser et de s'autoconfigurer, maillage peut également réduire efficacement la configuration.

Notez que seuls certains modèles de PAE 1 000 000 000 000 000 doivent être disponibles sur le même site pour établir un réseau Mesh.

Pour comprendre comment le maillage peut être utilisé, les termes suivants utilisés dans le contrôleur Omada seront introduits :

Root AP	L'AP est géré par Omada Controller avec une connexion de données câblée qui peut être configurée pour relayer les données vers et depuis les AP mesh (downlink AP).
Isolated AP	Lorsque l'EAP qui a été géré par Omada Controller avant se connecte au réseau sans fil et ne peut pas atteindre la passerelle, il va dans l'état isolé.
Mesh AP	Un AP isolé deviendra un MAS après avoir établi une connexion sans fil à l'AP avec accès au réseau.
Uplink AP/Downlink AP	Parmi les AP maillés, l'AP qui offre la connexion sans fil pour d'autres AP est appelé UPlink AP. Un AP racine ou un AP intermédiaire peut être l'AP uplink. Et l'AP qui se connecte à l'AP uplink est appelé downlink AP. Un AP uplink peut offrir une connexion sans fil directe pour 4 AP downlink tout au plus.
Wireless Uplink	Action qu'un AP downlink se connecte à l'AP de liaison uplink.
Hops	Dans un déploiement qui utilise un AP racine et plus d'un niveau de liaison vers le haut sans fil avec les ap's intermédiaires, les niveaux de liaison vers le haut peuvent être mentionnés par racine, premier saut, deuxième saut et ainsi de suite. **Le nombre de sauts ne doit pas être plus de 3.**

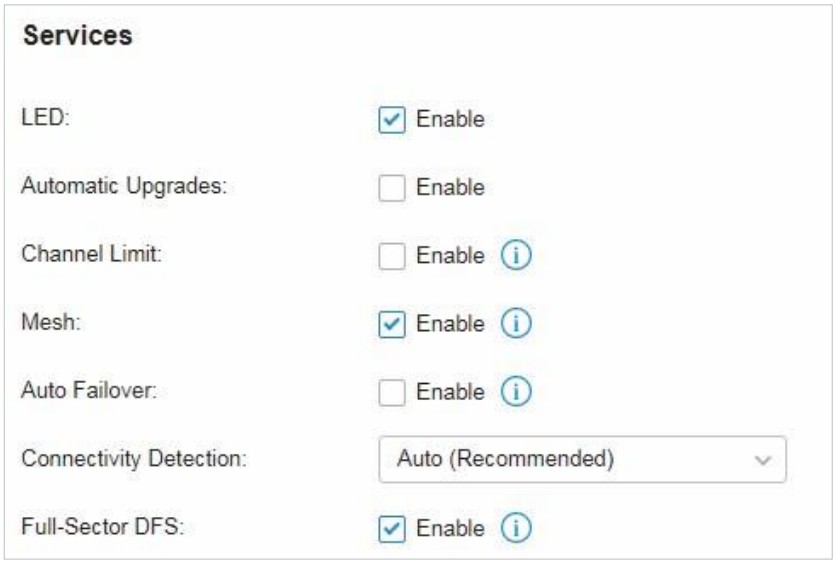
Un réseau de maillage commun est affiché comme ci-dessous. Seul l'AP racine est connecté par un câble Ethernet, tandis que les autres AP n'ont pas de connexion de données câblées. Mesh permet aux AP isolés de communiquer avec ap racine préconfigurée sur le réseau. Une fois mis sous tension, les EAP par défaut ou non intégrés de l'usine peuvent détecter l'EAP en portée et se rendre disponible pour adoption dans le contrôleur.



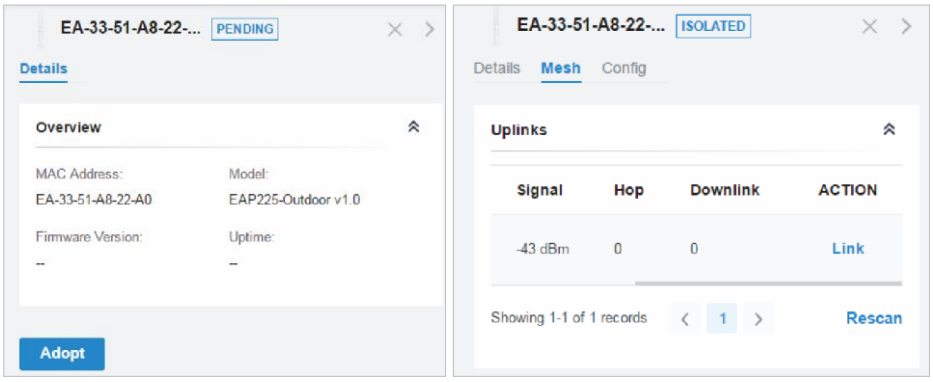
Une fois tous les PAE adoptés, un réseau de mailles est établi. Les EAP connectés au réseau via la connexion sans fil peuvent également diffuser des SSID et relayer le trafic réseau vers et depuis le réseau via l'AP uplink.

Pour créer un réseau de maillage, procédez comme suit :

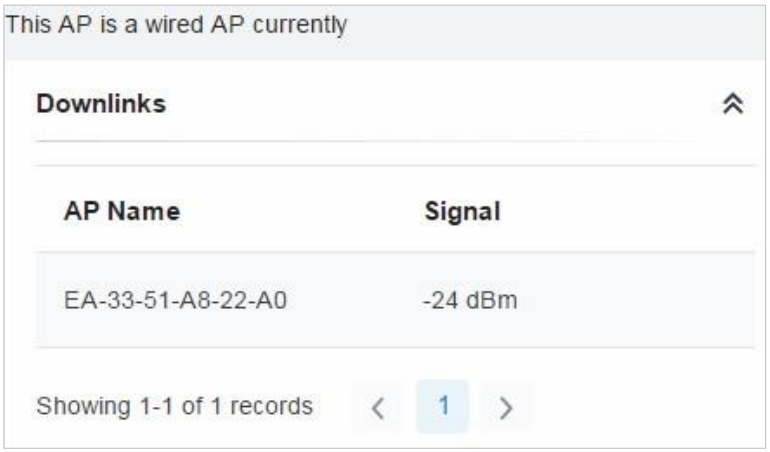
1. Allez dans Settings > Site pour s'assurer que Mesh est activé.



2. Allez dans Devices d'adopter un EAP AP ou lier un AP isolé.



Dans Mesh, si l'AP sélectionné est un AP de liaison uplink, cette page répertorie tous les AP de liaison vers le bas connectés à l'AP.

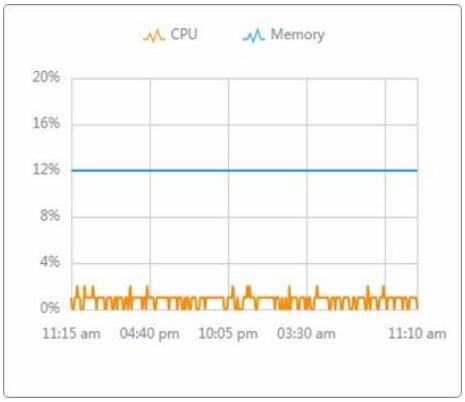


Si l'AP sélectionné est un AP downlink, cette page répertorie tous les AP de liaison vers le haut disponibles et leur canal, la force du signal, le saut et le nombre d'AP de liaison vers le bas. Vous pouvez cliquer sur Rescan pour rechercher les AP de liaison up disponibles et actualiser la liste, puis cliquer sur Lien pour connecter l'AP de liaison et créer un réseau de maillage.



Statistiques

Dans Les statistiques, vous pouvez surveiller l'utilisation de l'appareil au cours des dernières 24 heures via des graphiques, y compris le processeur/ moniteur de mémoire, l'utilisation des canaux, les paquets abandonnés et les paquets rejugés. Pour afficher les statistiques de l'appareil dans certaines périodes, cliquez sur le graphique pour View the Statistics of the Network.





Surveiller et gérer les clients

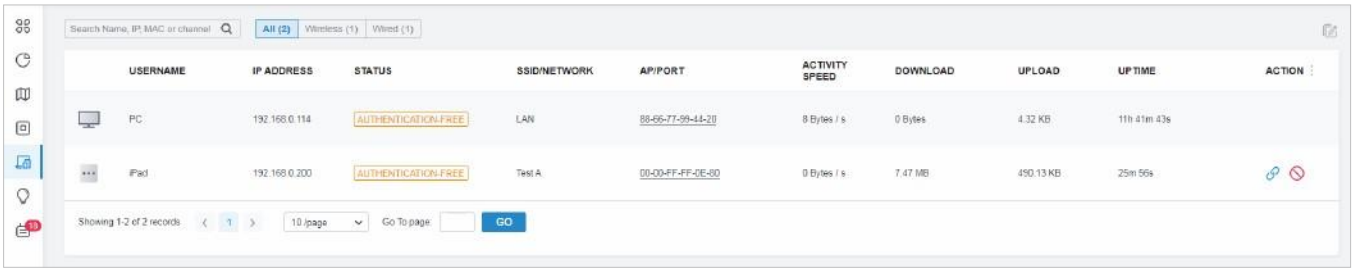
Ce chapitre vous guide sur la façon de surveiller et de gérer les clients à travers la page Clients à l'aide de la table des clients et de la fenêtre propriétés et du système Hotspot Manager. Pour afficher les clients qui se sont connectés au réseau dans le passé, reportez-vous à Afficher les statistiques au cours de la période spécifiée avec Insight. Ce chapitre comprend les sections suivantes :

- Gérer les clients filaires et sans fil dans la page clients
- Gérer l'authentification du client dans le Gestionnaire de points d'accès

7. 1 Gérer les clients filaires et sans fil dans la page clients

7. 1. 1 Page Introduction aux clients

La page Clients offre un moyen simple de gérer et de surveiller les clients. Il affiche tous les clients connectés câblés et sans fil dans le site choisi et leurs informations générales. Vous pouvez également ouvrir la fenêtre Propriétés pour des informations détaillées et des configurations.



PENDING	Le client n'a pas passé l'authentification du portail et il n'est pas connecté à Internet.
AUTHORIZED	Le client a été autorisé et est connecté à Internet.
CONNECTED	Le client est connecté à Internet via un réseau non portail.
AUTHENTICATION-FREE	Le client n'a pas besoin d'être autorisé et il est connecté à Internet.

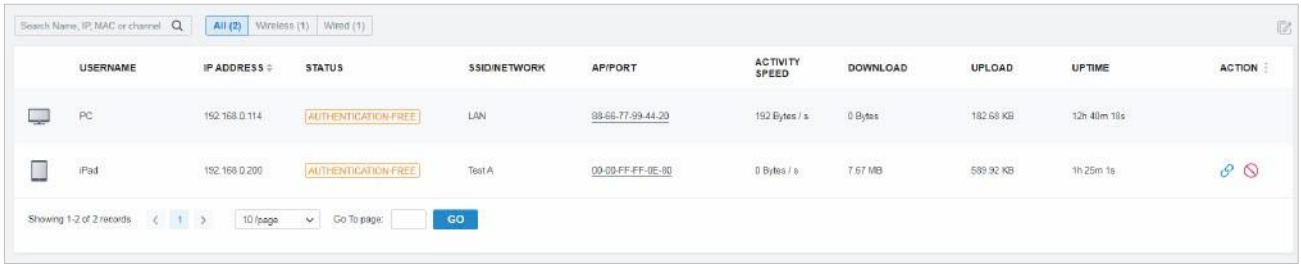
7. 1. 2 Utilisation de la Table clients pour surveiller et gérer les clients

Pour surveiller et gérer rapidement les clients, vous pouvez personnaliser les colonnes et filtrer les clients pour une meilleure vue d'ensemble de leurs informations. En outre, des opérations rapides et la configuration du lot sont disponibles.

- **Personnaliser les colonnes d'informations**

  Cliquez en regard de la colonne Action et vous avez trois choix : Colonnes par défaut, Toutes les colonnes et Personnaliser les colonnes. Pour personnaliser les informations affichées dans le tableau, cliquez sur les cases à cocher du type d'information.

  Pour modifier l'ordre de liste, cliquez sur la tête de colonne et l'icône vous semble choisir le ordre croissant ou descendant.



- **Filtrer les clients**

  Pour rechercher des clients spécifiques, utilisez la zone de recherche au-dessus de la table. Pour filtrer les clients par leur type de connexion, utilisez les barres d'onglets au-dessus de la table. Pour les clients sans fil, vous pouvez les filtrer par la bande de fréquences et le type de réseau sans fil connecté.

Search Name, IP, MAC or channel	Filtrer les clients à l'aide de la zone de recherche en fonction du nom d'utilisateur, de l'adresse IP, de l'adresse MAC ou du canal.
All (2) Wireless (1) Wired (1)	Filtrer les clients en fonction de leur type de connexion.
All (2) 2.4 GHz (0) 5 GHz (2)	(Pour les clients sans fil) Filtrer les clients sans fil en fonction de la bande de fréquences qu'ils utilisent
All (2) Users (0) Guests (2)	(Pour les clients sans fil) Filtrer les clients sans fil en fonction du type de réseau sans fil connecté. Les clients sont clients connectés au réseau invité, que vous pouvez définir pendant Quick Setup creating wireless networks

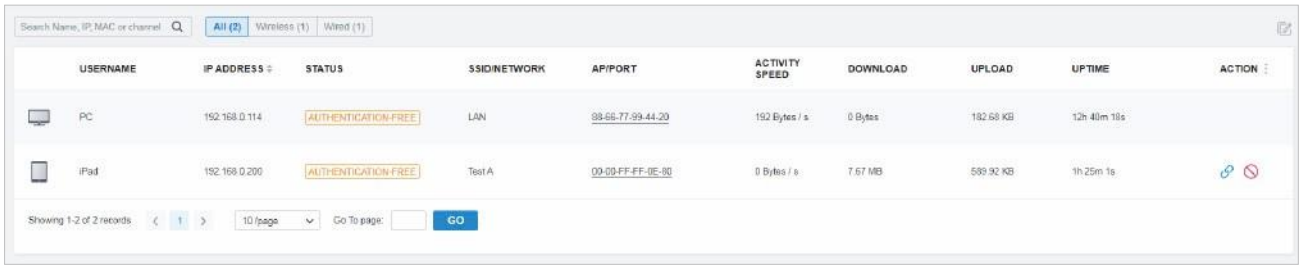
■ **Opérations rapides**

Pour des opérations rapides sur un seul client, cliquez sur les icônes de la colonne Action. Les icônes disponibles varient en fonction de l'état du client et du type de connexion.

	Cliquez pour bloquer le client dans le site choisi. Vous pouvez afficher les clients bloqués dans Known Clients
	Avec l'authentification du portail activée) Cliquez pour autoriser manuellement le client qui n'a pas passé l'authentification du portail.
	(Avec l'authentification du portail activée) Cliquez pour désautoriser le client qui a passé l'authentification du portail.
	(Pour les clients sans fil) Cliquez pour reconnecter le client sans fil au réseau sans fil.

■ **Sélectionner plusieurs pour la configuration du lot**

Pour sélectionner plusieurs clients et les ajouter à la fenêtre Propriétés, cliquez en haut à droite, puis cochez les cases. Lorsque vous avez terminé de choisir les clients, cliquez sur Edit Selected et les clients choisis seront ajoutés à la fenêtre Propriétés pour la configuration du client par lots.



7. 1. 3 Utilisation de la fenêtre Propriétés pour surveiller et gérer les clients

Dans la fenêtre Propriétés, vous pouvez afficher des informations plus détaillées sur les clients connectés et les gérer. Pour ouvrir la fenêtre Propriétés, cliquez sur l'entrée d'un seul client ou cliquez sur la configuration du lot fot de plusieurs clients.

. Utiliser les icônes suivantes pour la fenêtre Propriétés.

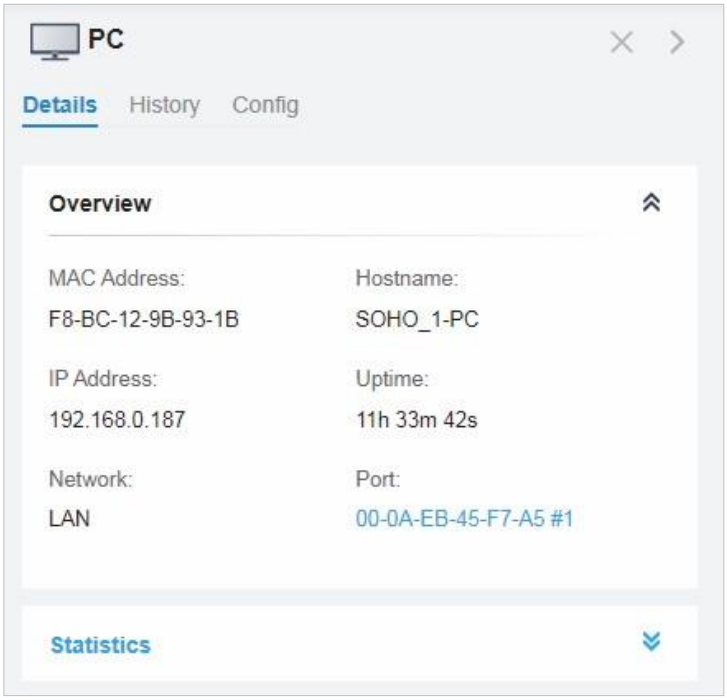
	Cliquez pour sélectionner plusieurs clients et ajoutez-les à la fenêtre Propriétés pour la surveillance par lots et la gestion
	Cliquez pour réduire au minimum la fenêtre Propriétés sur une icône. Pour rouvrir la fenêtre Propriétés minimisées, cliquez sur
	Cliquez pour maximiser la fenêtre Propriétés. Vous pouvez également utiliser l'icône sur des pages autres que la page clients
	Cliquez pour fermer la fenêtre Propriétés du ou des clients choisis. Notez que **les configurations non-sauvés pour le(s) client(s) sera perdu**
	Le numéro en bas à droite affiche le nombre de clients dans la configuration du client par lots.

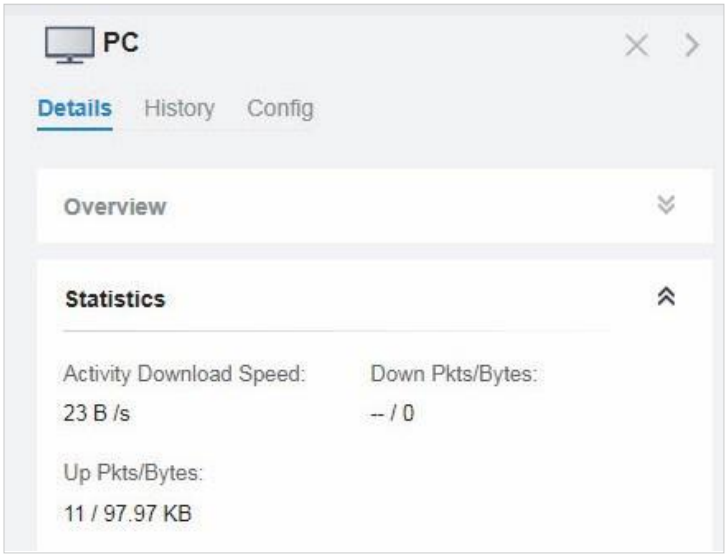
Surveiller et gérer un seul client

- **Surveiller un seul client**

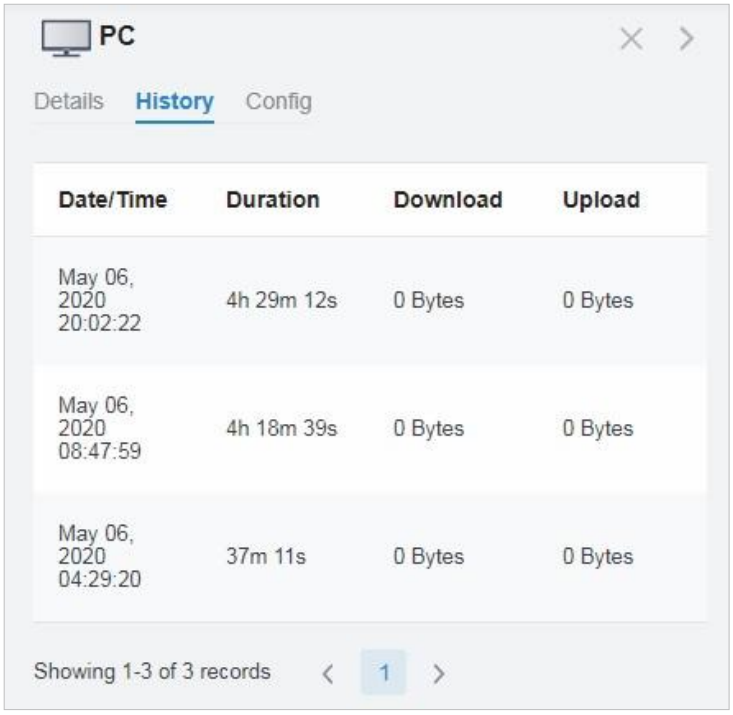
  Après avoir ouvert la fenêtre Propriétés d'un seul client, vous pouvez afficher les informations de base, les statistiques de trafic et l'historique des connexions sous les onglets Détails et historique.

  Sous l'onglet Détails, Overview et Statistics affichent les informations de base et les statistiques de trafic du client, respectivement. Les informations répertoriées varient en fonction de l'état et du type de connexion du client.



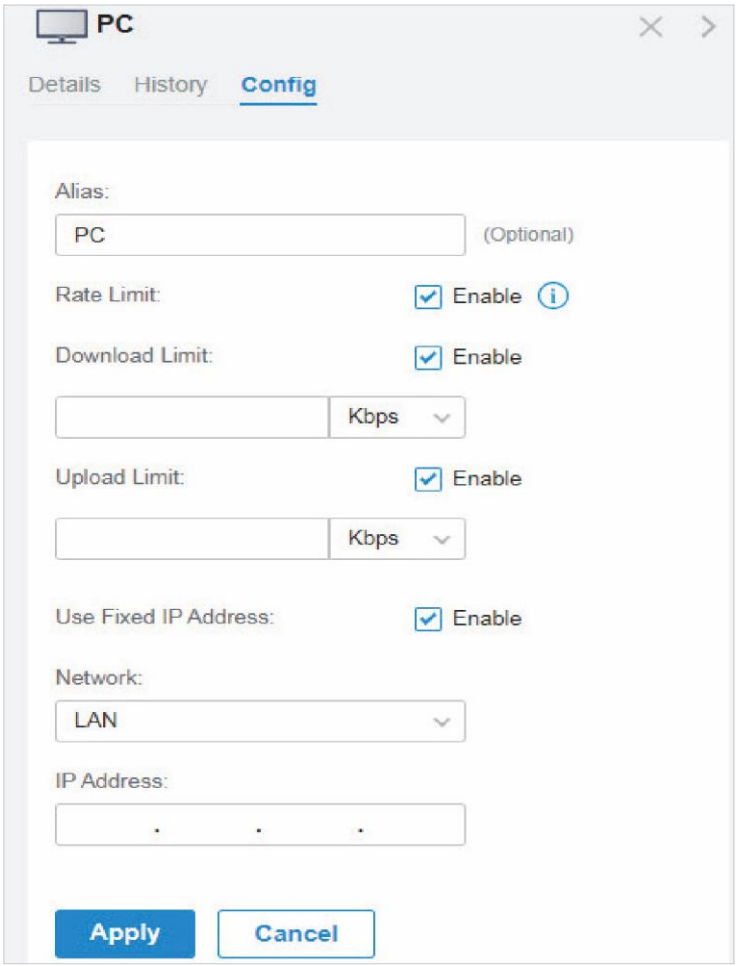


Sous l'onglet Historique, vous pouvez afficher l'historique de connexion du client.



■ **Gérer un client unique**

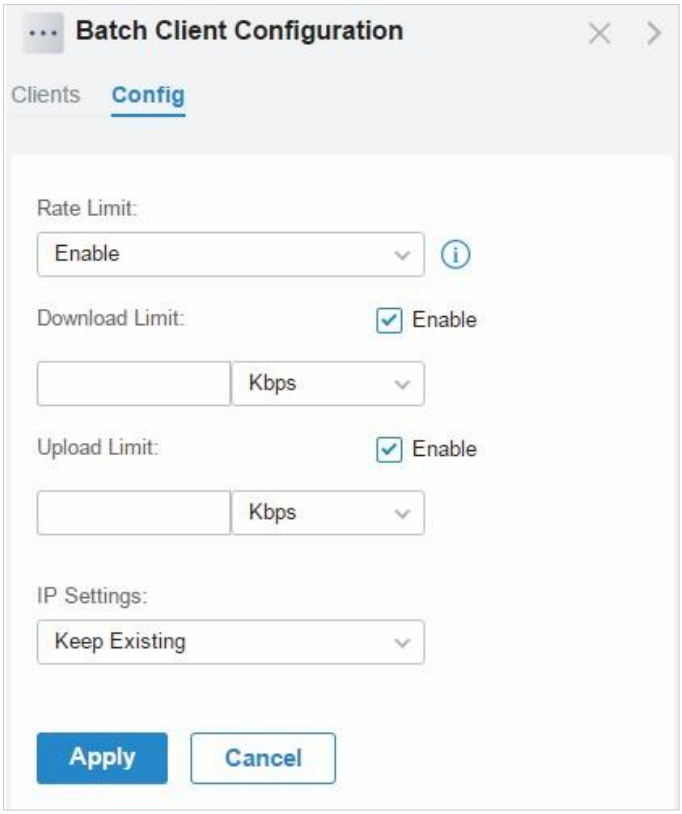
Dans Config, vous pouvez configurer les paramètres suivants :



Alias	Spécifiez l'alias du client pour mieux identifier les différents clients, et l'alias est utilisé comme nom d'utilisateur du client dans le tableau de la page Clients.
Limite de taux	Cliquez sur la case à cocher pour activer la limite de taux pour le client. Avec la fonction activée, vous pouvez définir davantage des limites pour le taux de téléchargement et de téléchargement. Si la limite tarifaire est désactivée, la limite tarifaire du client reste son paramètre par défaut. Remarque : La limite tarifaire de cette page n'est disponible que pour les clients connectés aux EAP's Pour limiter le taux de clients connectés à la passerelle ou au commutateur, accédez à la page Contrôle de bande passante.
Use Fixed IP Address	Cliquez sur la case à cocher pour configurer une adresse IP fixe pour le client. Avec cette fonction activée, sélectionnez un réseau et spécifiez une adresse IP pour le client. Pour afficher et configurer les réseaux, reportez-vous à Configure Wired Networks. Remarque : une passerelle gérée par Omada est requise pour cette fonction. Sinon, vous ne pouvez pas définir une adresse IP fixe pour le client.

Surveiller et gérer plusieurs clients

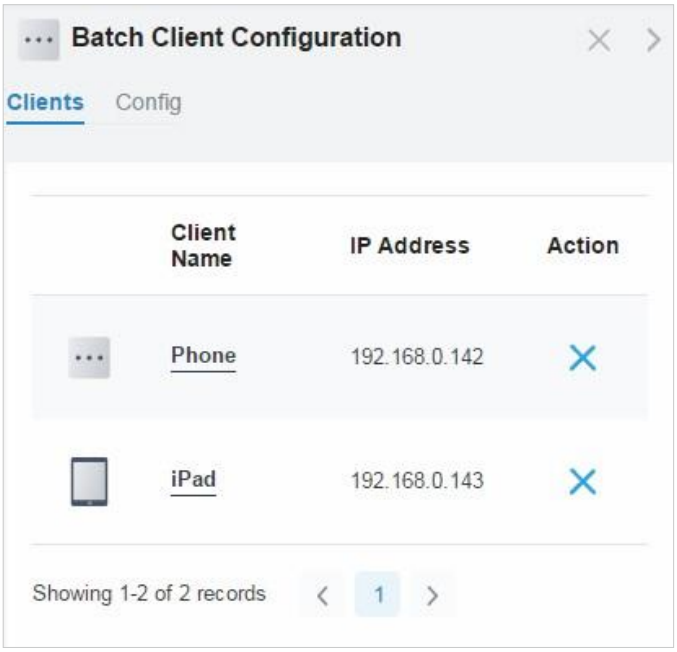
Pour gérer plusieurs clients en même temps, cliquez sur , sélectionnez plusieurs clients, puis cliquez Edit Selected. Ensuite, vous pouvez configurer les paramètres suivants sous l'onglet Config.



Rate Limit	Keeping existing: La limite de taux des clients choisis reste leur cadre actuel. Enable: Avec la limite de taux activée, spécifiez des limites pour le téléchargement et/ou le taux de téléchargement pour tous les clients choisis. Disable: Avec la limite de taux désactivée, il n'y a pas de limite tarifaire pour les clients choisis. Remarque : La limite de taux de cette page n'est disponible que pour les clients connectés aux PAE. Pour limiter le taux de clients connectés à la passerelle ou au commutateur, accédez à la page Contrôle de bande passante.
IP Setting	Keeping existing: Le paramètre IP des clients choisis reste leurs paramètres actuels. Use DHCP: Les adresses IP des clients sont automatiquement attribuées par le serveur DHCP, telles que le commutateur Layer 3 et la passerelle. Use Fixed IP Address: Sélectionnez un réseau et affectez manuellement des adresses IP fixes aux clients sélectionnés. Pour afficher et configurer des réseaux, reportez-vous à Configure Wired Networks. Notez qu'une passerelle gérée par Omada est requise pour cette fonction. Sinon, vous ne pouvez pas définir d'adresses IP fixes pour les clients sélectionnés.

Vous pouvez afficher leurs noms et adresses IP dans l'onglet Clients et supprimer les clients du client Batch

Pour la configuration cliquez sur ✕ dans la colonne Action.



7. 2 Gérer l'authentification du client dans le Gestionnaire de points d'accès

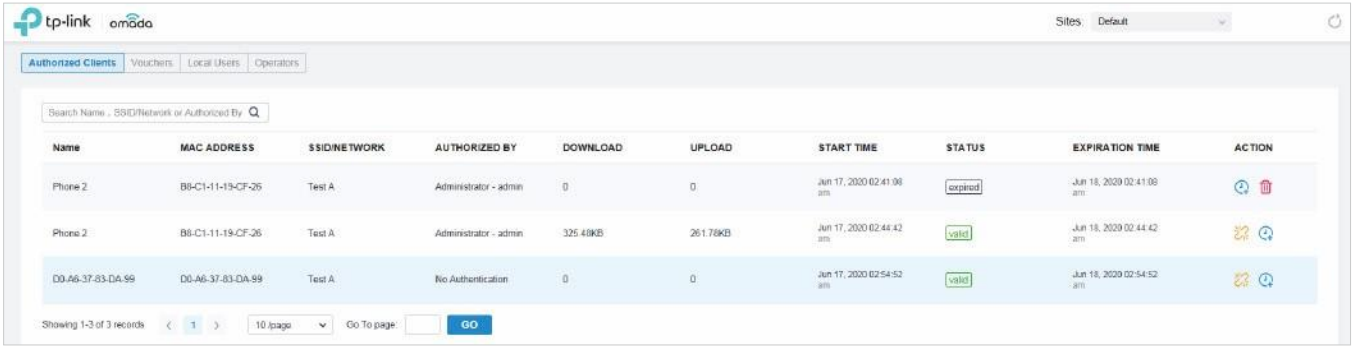
Hotspot Manager est un système de gestion de portail pour la surveillance et la gestion centralisées des clients autorisés par authentification de portail. Les quatre onglets suivants sont fournis dans le système pour une gestion facile et directe.

Authorized Clients	Affichez les enregistrements des clients portail connectés et expirés.
Vouchers	Créez des bons pour l'authentification du portail, affichez et gérez les informations associées.
Local Users	Créer des comptes d'utilisateurs locaux pour l'authentification portal, afficher leurs informations et les gérer.
Operators	Créer des comptes d'opérateur pour la gestion des points chauds, afficher leurs informations et les gérer.

7. 2. 1 Clients autorisés

L'onglet Clients autorisés est utilisé pour afficher et gérer les clients autorisés par le système de portail, y compris les clients expirés et les clients dans la période valide.

Pour ouvrir la liste des clients autorisés, cliquez sur Gestionnaire de points d'accès à partir de la liste déroulante des sites et cliquez sur Clients autorisés dans la page contextuelle**.** Vous pouvez rechercher certains clients à l'aide de la zone de recherche, afficher leurs informations détaillées dans le tableau et les gérer à l'aide de la colonne d'action.



	Cliquez pour prolonger la période valide du client autorisé. Vous pouvez choisir l'heure prédéfinie La longueur ou définir une période personnalisée en fonction des besoins.
	Cliquez pour déconnecter le ou les clients autorisés. Lorsque vous déconnectez un client autorisé, le client doit être ré-authentifié pour la connexion suivante.
	Cliquez pour supprimer le client expiré de la liste.

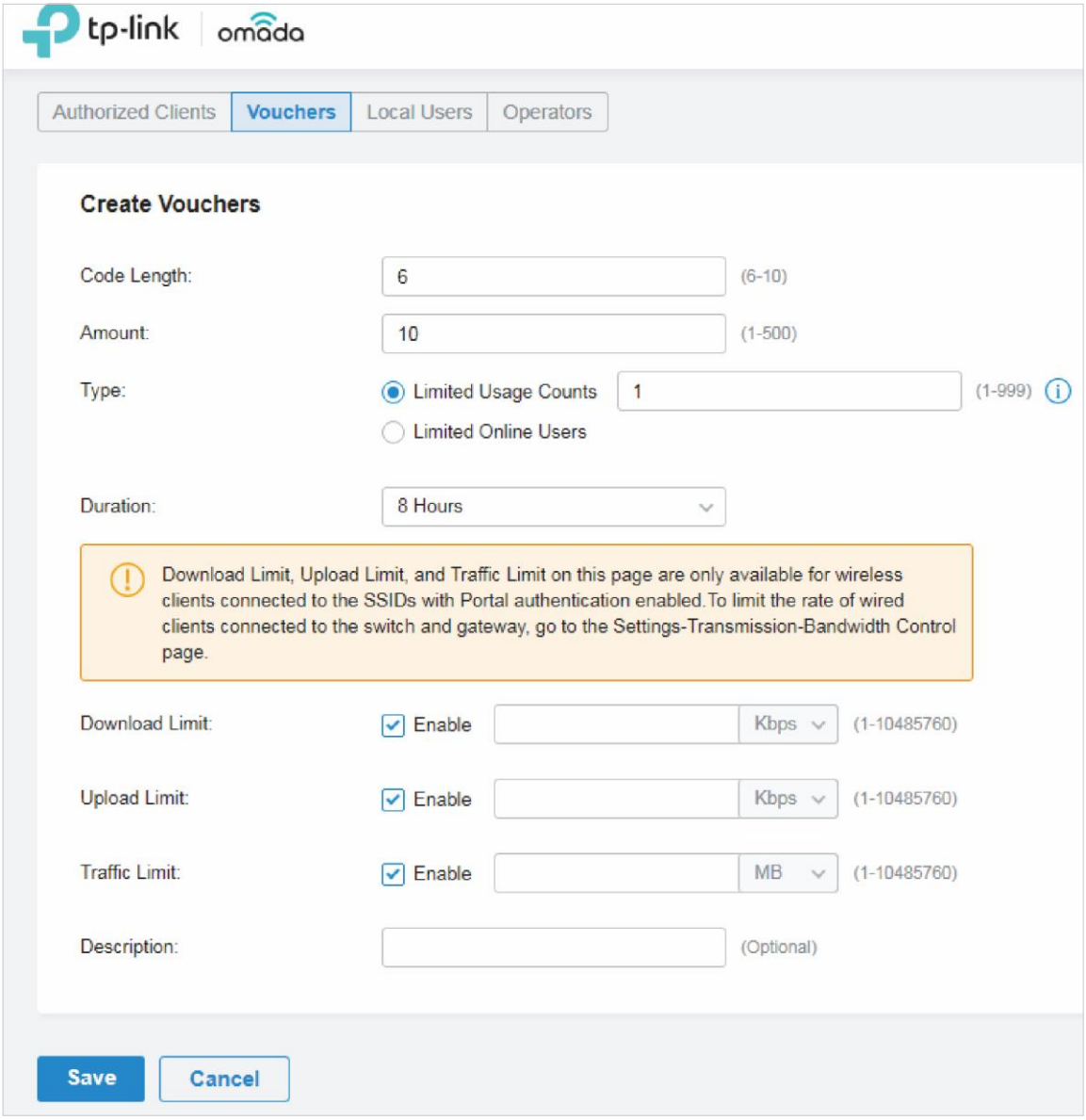
7. 2. 2 Vouchers

L'onglet vouchers est utilisé pour créer des bons et gérer les codes de bons inutilisés. Avec les bons configurés et les codes créés, vous pouvez distribuer les codes de bons générés par le contrôleur aux clients pour qu'ils accèdent au réseau via l'authentification du portail. Pour les configurations détaillées, reportez-vous à Portal.

Créer vouchers

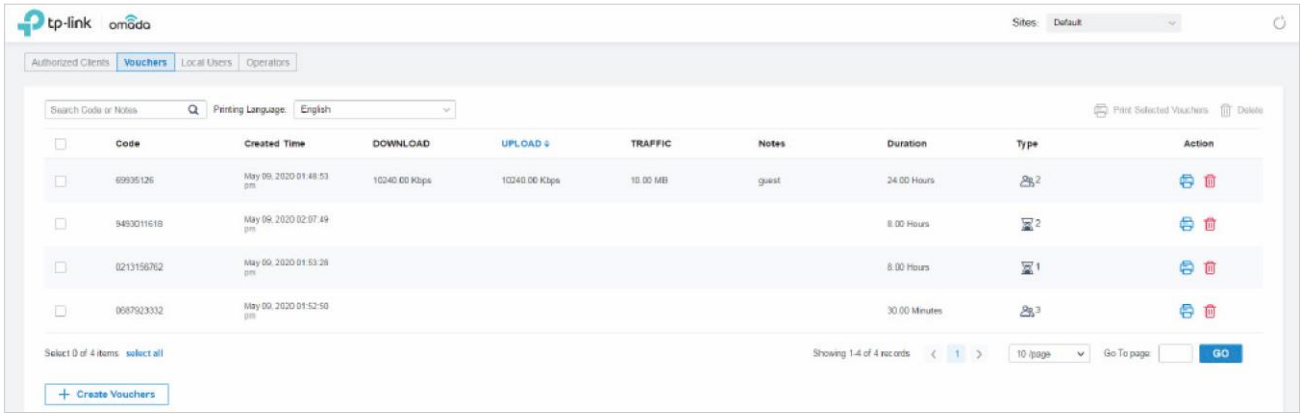
Procédez comme suit pour créer des bons d'authentification :

1. Cliquez sur Hotspot Manager à partir de la liste déroulante de Sites et cliquez sur Vouchers dans la page contextuelle.
2. Cliquez sur +Create Vouchers en bas à gauche, et la fenêtre suivante apparaît. Configurer les paramètres suivants et cliquer sur Save.



Amount	Spécifiez le nombre de codes de bons à créer.
Code Length	Spécifiez la longueur du(s) code(s) de 6 à 10 chiffres.
Type	Sélectionnez un type pour limiter le nombre d'utilisations ou le nombre d'utilisateurs autorisés d'un voucher code. Limited Usage Counts: Le code de bon ne peut être utilisé que pour un nombre limité de fois dans sa période valide. Limited Online Users: Le code de bon peut être utilisé pour un nombre illimité de fois dans sa période valide, mais seul un nombre limité de clients sans fil peuvent accéder au réseau avec ce code de coupon en même temps.
Duration	Sélectionnez la période valide pour les codes de bons d'achat.
Download/Upload Limit	Cliquez sur la case à cocher et spécifiez la limite tarifaire pour le téléchargement/téléchargement pour les clients sans fil à l'aide du(s) code(s) des bons d'achat. La valeur du taux de téléchargement et de téléchargement peut être définie dans Kbps ou Mbps. Remarque : La limite de téléchargement/téléchargement sur cette page n'est disponible que pour les clients sans fil connectés aux SSID avec l'authentification portal activée. Pour limiter le taux de clients câblés connectés au commutateur et à la passerelle, Settings >Transmission > Bandwidth Control.
Traffic Limit	Cliquez sur la case à cocher et spécifiez la limite de trafic totale pour le bon, et la valeur de la limite de trafic peut être définie en MB ou GB. Une fois le limité atteint, le(s) client(s) ne peut plus accéder au réseau à l'aide de voucher. Remarque : les limites de trafic de cette page ne sont disponibles que pour les clients sans fil connectés aux SSID avec l'authentification Portal activée. Pour limiter le taux de clients câblés connectés au commutateur et à la passerelle, Settings > Transmission > Bandwidth Control.
Description (optional)	Entrez les notes pour le ou les codes de bons créés et la description d'entrée s'affiche dans la liste des bons sous l'onglet bon.

1. Les codes de bons sont générés et affichés dans le tableau.



2	Le code de bon peut être utilisé pour un nombre illimité de fois dans sa période valide, mais seul un nombre limité de clients sans fil peuvent accéder à Internet avec ce voucher code en même temps. Le nombre à droite indique le nombre limité d'utilisateurs.
2	Le code de bon ne peut être utilisé que pour un nombre limité de fois dans sa période valide. Le nombre à droite indique le nombre limité de temps d'authentification.

4. Imprimez les bons. Cliquez pour imprimer un seul bon, ou cliquez sur cases à cocher des bons d'achat

Print Selected Vouchers

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

4. Distribuez les bons aux clients, puis ils peuvent utiliser les codes pour passer l'authentification. Si un code de bon expire, il sera automatiquement supprimé de la liste.

5. Pour supprimer manuellement certains bons, cliquez pour supprimer un seul bon ou supprimer pour supprimer plusieurs codes de bons à la fois.

7. 2. 3 Utilisateurs locaux

L'onglet Utilisateurs locaux est utilisé pour créer des comptes d'utilisateur pour l'authentification. Avec l'utilisateur local configuré, les clients sont tenus d'entrer le nom d'utilisateur et le mot de passe pour passer l'authentification. Vous pouvez créer plusieurs comptes et les affecter à différents utilisateurs. Pour les configurations détaillées, reportez-vous à Portal.

Créer des utilisateurs locaux

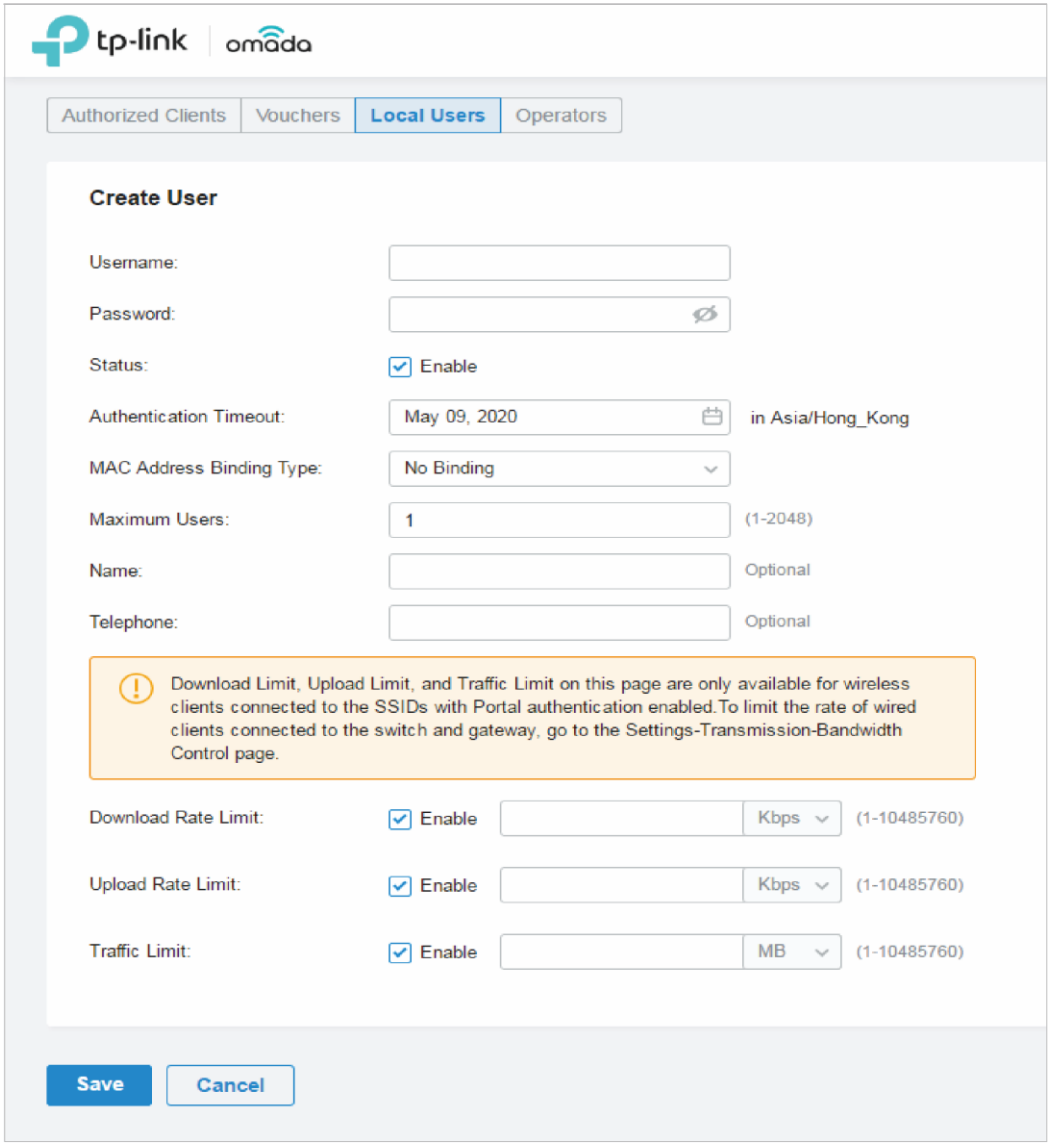
Il existe deux façons de créer des comptes d'utilisateurs locaux : créer des comptes sur la page et importer à partir d'un fichier.
Pour créer des comptes d'utilisateurs locaux, procédez comme suit.

1. Cliquez sur Gestionnaire de points d'accès dans la liste déroulante des sites, puis cliquez surLocal Utilisateurs dans la page contextuelle.

2 Créer des comptes d'utilisateurs locaux de deux façons différentes.

■ **Créer des comptes utilisateur locaux**

Cliquez sur +Create User en bas à gauche, et la fenêtre suivante apparaît. Configurer les paramètres suivants et cliquer sur Save.

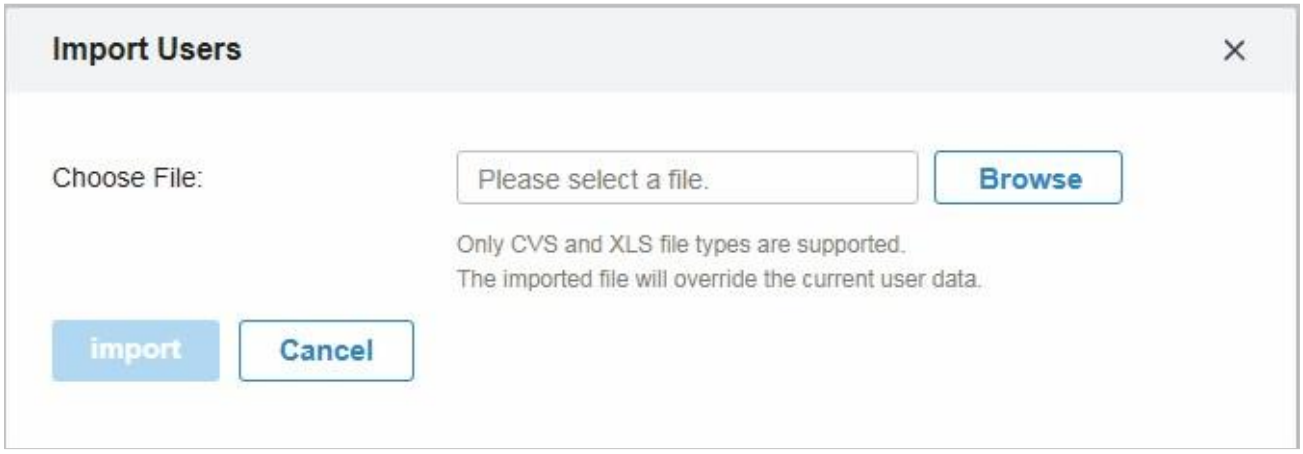


Username	Spécifiez le nom d'utilisateur. Le nom d'utilisateur doit être différent des noms existants, et il n'est pas modifiable une fois qu'il est créé.
Password	Spécifiez le mot de passe. Les utilisateurs locaux sont tenus d'entrer le nom d'utilisateur et le mot de passe pour passer l'authentification et accéder au réseau.
Status	Lorsque l'état est activé, cela signifie que le compte d'utilisateur est valide. Vous pouvez désactiver le compte d'utilisateur et l'activer ultérieurement au besoin.
Authentication Timeout	Spécifiez le délai d'expiration d'authentification pour les utilisateurs locaux. Après le délai d'expiration, les utilisateurs doivent se connecter à nouveau sur la page d'authentification pour accéder au réseau.

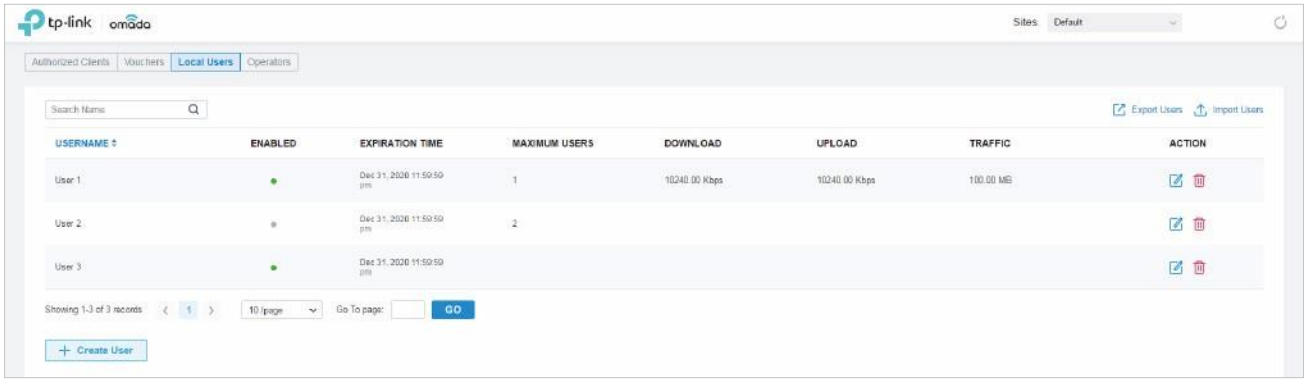
MAC Address Binding Type	Il existe trois types de liaison MAC : pas de liaison, de liaison statique et de liaison dynamique. No Binding: Aucune adresse MAC n'est liée au compte d'utilisateur local. Static Binding: Lier manuellement une adresse MAC à ce compte d'utilisateur. Ensuite, seul l'utilisateur avec cette adresse MAC peut utiliser le nom d'utilisateur et le mot de passe pour passer l'authentification. Dynamic Binding: L'adresse MAC du premier utilisateur qui passe l'authentification sera liée à ce compte. Ensuite, seul cet utilisateur peut utiliser le nom d'utilisateur et le mot de passe pour passer l'authentification.
Maximum Users	Spécifiez le nombre maximal d'utilisateurs qui peuvent utiliser ce compte pour passer l'authentification.
Name (optional)	Spécifier un nom pour l'identification.
Telephone (optional)	Spécifiez un numéro de téléphone pour identification.
Download/Upload Limit	Cliquez sur la case à cocher et spécifiez la limite de taux de téléchargement/téléchargement pour les utilisateurs du compte d'utilisateur local. La valeur du taux de téléchargement/téléchargement peut être définie dans Kbps ou Mbps. Remarque : La limite de téléchargement/téléchargement sur cette page n'est disponible que pour les clients sans fil connectés aux SSID avec l'authentification portal activée. Pour limiter le taux de clients câblés connectés au commutateur et à la passerelle, Settings >Transmission > Bandwidth Control.
Traffic Limit	Cliquez sur la case à cocher et spécifiez la limite de trafic totale pour le compte d'utilisateur local, et la valeur de la limite de trafic peut être définie en Mo ou GB. Une fois le limité atteint, l'utilisateur(s) ne peut plus accéder au réseau à l'aide de ce compte. Remarque : les limites de trafic de cette page ne sont disponibles que pour les clients sans fil connectés aux SSID avec l'authentification Portal activée. Pour limiter le taux de clients câblés connectés au commutateur et à la passerelle, Settings > Transmission > Bandwidth Control.

■ **Créez des comptes d'utilisateurs locaux à partir de fichiers.**

Cliquez Import Users en haut à droite, et la fenêtre suivante apparaît. Sélectionnez un fichier au format CVS ou Excel, puis cliquez sur Import. Pour voir les paramètres requis et l'explication correspondante, reportez-vous à Create Local User accounts. Notez que le fichier importé remplacera les données utilisateurs actuels.



3. Le ou les comptes d'utilisateur locaux seront créés et affichés dans le module. Vous pouvez afficher les informations des utilisateurs locaux créés, rechercher certains comptes via le nom et utiliser des icônes pour la gestion.



Import Users	Cliquez pour ajouter des utilisateurs locaux à partir de fichiers au format CVS ou Excel. Il est recommandé lorsque vous devez créer des utilisateurs locaux par lots Notez que le fichier importé remplacera les données utilisateurs actuels.
Export Users	Cliquez pour exporter l'ou les utilisateurs locaux vers des fichiers au format CVS ou Excel.
	Cliquez pour modifier les paramètres de l'utilisateur local.
	Cliquez pour supprimer l'utilisateur

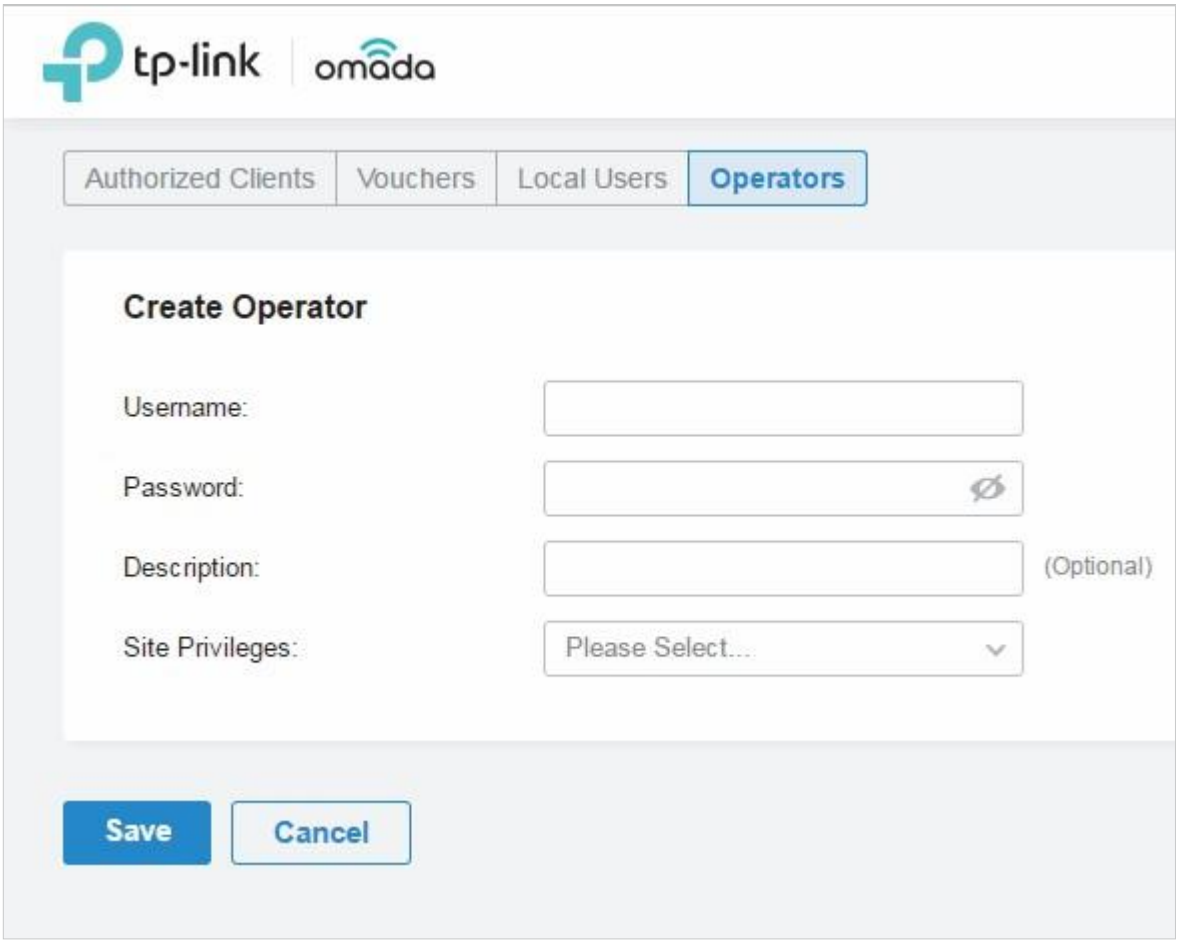
7. 2. 4 Opérateurs

L'onglet Opérateurs est utilisé pour gérer et créer des comptes d'opérateur qui ne peuvent être utilisés que pour se connecter à distance au système Hotspot Manager et gérer les bons et les utilisateurs locaux pour les sites spécifiés. Les opérateurs n'ont aucun privilège de créer des comptes d'opérateur, ce qui offre la commodité et assure la sécurité pour l'authentification client.

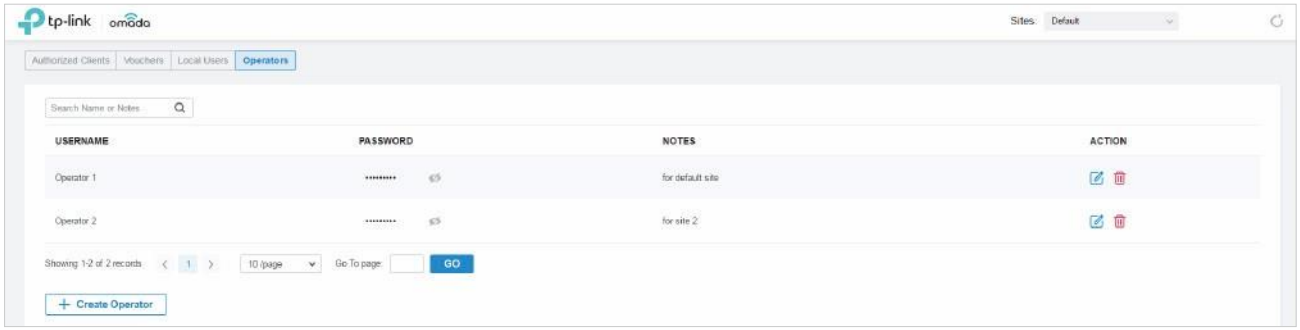
Créer des opérateurs

Pour créer des comptes d'opérateur, procédez comme suit.

1. Cliquez sur Gestionnaire de points d'accès dans la liste déroulante des sites et cliquez sur Opérateurs dans la page contextuelle.
2. Cliquez sur + Create Operator en bas à gauche, et la fenêtre suivante apparaît.



3. Spécifiez le nom d'utilisateur, le mot de passe et la description (facultatif) pour le compte de l'opérateur. Sélectionnez ensuite des sites dans la liste déroulante du site Privileges. Cliquez sur Save.
4. Les comptes de l'opérateur sont créés et affichés dans la table. Vous pouvez afficher les informations des comptes d'opérateur de création sur la page, rechercher certains comptes à travers le nom et les notes, et utiliser des icônes pour la gestion.



	Cliquez pour modifier les paramètres du compte de l'opérateur.
	Cliquez pour supprimer le compte de l'opérateur.

5. Ensuite, vous pouvez utiliser un compte d'opérateur pour vous connecter au système **Hotspot Manager** :

- **Pour contrôleur de logiciel**

  Visitez l'URL https://Omada l'adresse IP de l'hôte du contrôleur:8043/hotspot (par exemple : https://192.168.0.174:8043/hotspot) et utilisez le compte de l'opérateur pour entrer dans le système de gestionnaire de hotspot.

- **Pour contrôleur matériel**

  Visitez l'URL https://Omada l'adresse IP de l'hôte contrôleur :443/h**Gestion de hotspots otspot**(par exemple : https://192.168.0.174:443/hotspot), et utilisez le compte de l'opérateur pour entrer dans le système gestionnaire de hotspots.

- **Pour contrôleur cloud**

  Visitez l'URL https://omada.tplinkcloud.com/hotspot et utilisez le compte de l'opérateur pour entrer dans le système gestionnaire de points d'accès.



Surveillance du réseau

Ce chapitre vous guide sur la façon de surveiller les périphériques réseau, les clients et leurs statistiques. Grâce à des présentations visuelles et en temps réel, le contrôleur SDN d'Omada vous tient au courant de l'état précis du réseau géré. Ce chapitre comprend les sections suivantes :

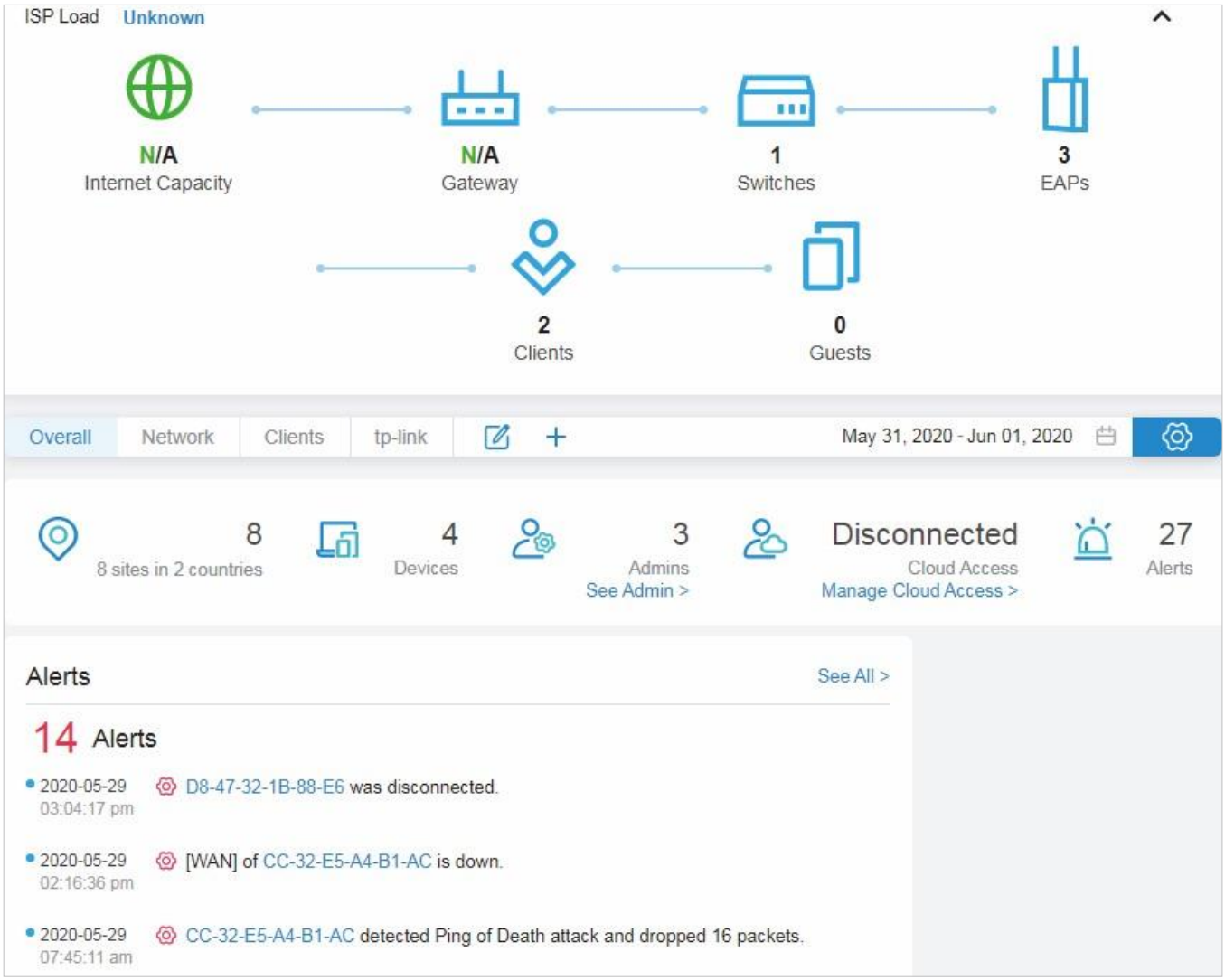
1. Afficher l'état du réseau avec le tableau de bord
2. Voir les statistiques du réseau
3. Surveiller le réseau avec la carte
4. Afficher les statistiques pendant la période spécifiée avec Insight
5. Afficher et gérer les journaux

■

❤ 8. 1 Afficher l’état du réseau avec le tableau de bord

8. 1. 1 Disposition de page du tableau de bord

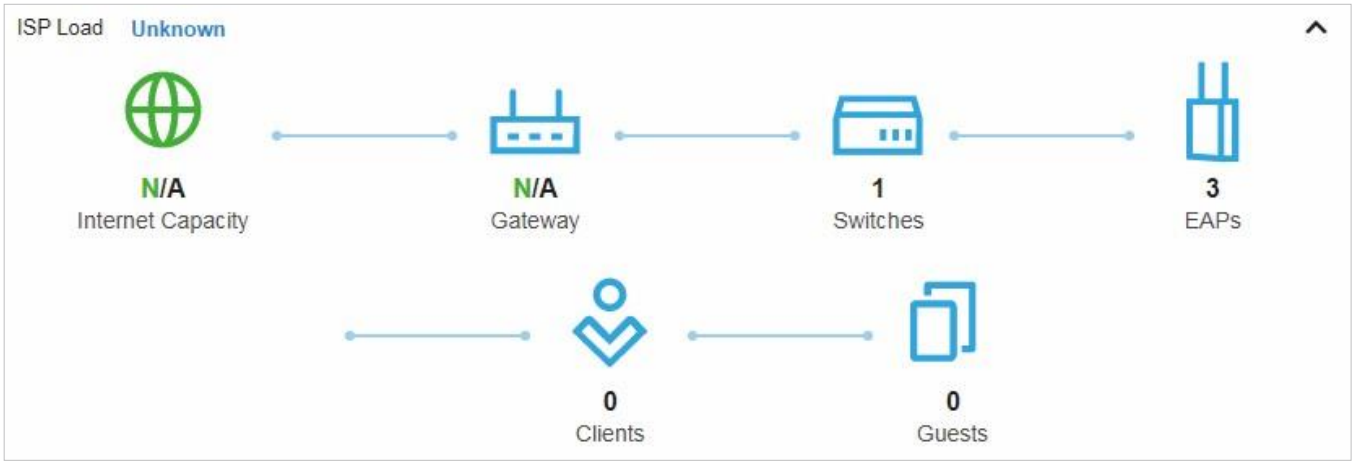
Dashboard est conçu pour un moniteur rapide en temps réel du réseau du site. Une vue d’ensemble de la topologie réseau est en haut du tableau de bord, et ci-dessous est une barre d’onglets suivie avec des widgets personnalisés.



Vue d’ensemble de la topologie

Vue d’ensemble de la topologie en haut montre l’état de la charge du FAI et le nombre d’appareils, de clients et d’invités. La charge du FAI a quatre statuts : Inconnu, Bon, Moyen, Pauvre.

■



Vous pouvez placer le curseur au-dessus de la passerelle, du commutateur, de l'AP, du client ou des icônes invitées pour vérifier leur état. Pour plus d'informations, cliquez sur l'icône ici pour accéder à la section Périphériques ou clients.



Barre d'onglets

Vous pouvez personnaliser les widgets affichés sous l'onglet de la page Tableau de bord. Trois onglets sont créés par défaut et ne peuvent pas être supprimés.



Overall	(Uniquement pour les administrateurs) Affichage de la vue d'ensemble du contrôleur et défaillances d'association par défaut.
Network	Affiche les alertes, la distribution de trafic Wi-Fi, le résumé Wi-Fi et les activités de trafic par défaut.
Clients	Affiche la plupart des clients actifs, clients Frequents Distribution et activités client par défaut.

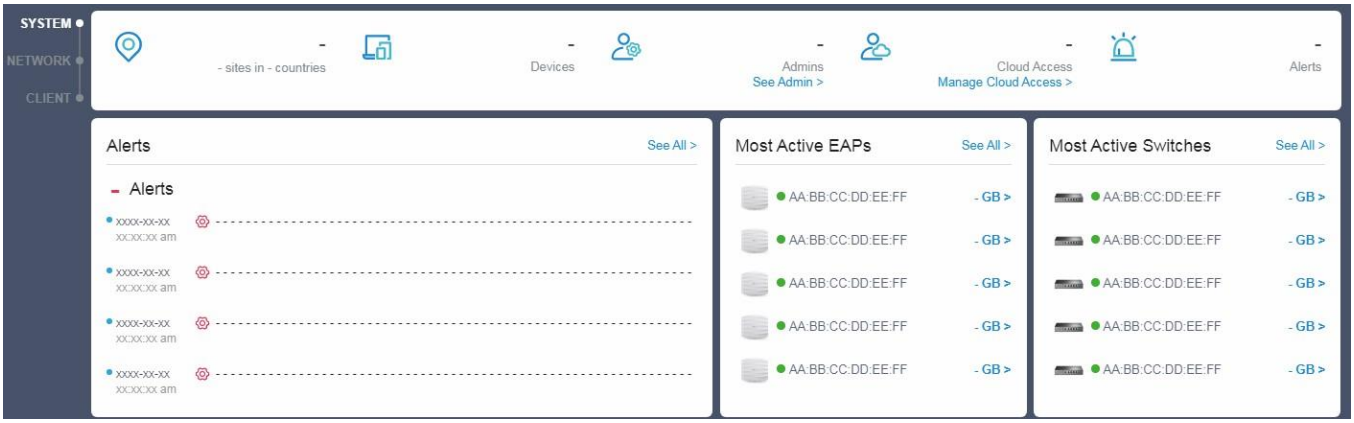
Dans la barre d'onglets, vous pouvez prendre l'action suivante pour modifier les onglets et personnaliser le widget à afficher.

■

	Cliquez sur l'icône pour modifier les onglets. Pour les onglets par défaut, vous pouvez les réinitialiser aux paramètres par défaut. Pour un onglet créé, vous pouvez modifier son nom ou le supprimer.
	Cliquez sur l'icône et entrez le nom dans la fenêtre contextuelle pour créer un nouvel onglet.
May 28, 2020 - May 29, 2020	Cliquez sur la date pour afficher un calendrier. Cliquez deux fois sur une date spécifique dans le calendrier pour que les widgets affichent ses statistiques. Pour afficher la statistique d'une plage d'heure, cliquez sur la date de début et la date de fin du calendrier.
	Cliquez sur un onglet, puis cliquez sur le widget dans la page contextuelle pour l'ajouter à cet onglet ou retirez-le

8. 1. 2 Explication des widgets

Les widgets sont divisés en trois catégories : Système, Réseau, Client. Vous pouvez cliquer sur l'icône pour ajouter ou supprimer les widgets.



System	(Uniquement pour l'onglet Global) Vue d'ensemble du contrôleur
Network	Alertes, EAPs les plus actifs, commutateurs les plus actifs, distribution de trafic Wi-Fi, résumé Wi-Fi, Distribution du trafic, distribution des clients, activités de trafic, taux de rejugé/taux abandonné
Client	Clients les plus actifs, plus longs temps de disponibilité du client, distribution freq clients, activités clients, Échecs d'association

■

Système

Vue d'ensemble du contrôleur dans le système ne peut être affichée que dans l'onglet Global. Il fournit une vue d'ensemble du contrôleur en temps réel, y compris le nombre total de sites, périphériques, comptes d'administration, alertes et état d'accès au cloud.



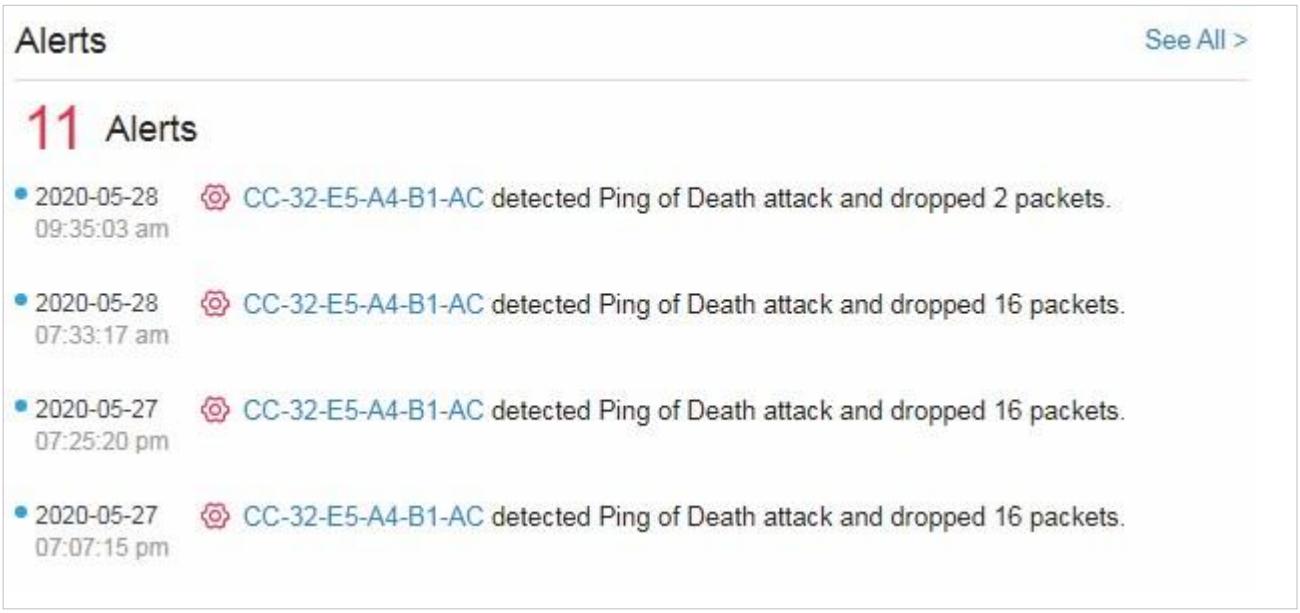
Pour afficher et modifier des comptes d'administrateur, cliquez sur See Admin > pour aller sur la section Admin.Pour configurer l'accès au cloud, cliquez sur Manage Cloud Access > et aller sur Settings > Cloud Access. Pour une configuration détaillée, reportez-vous à Manage Administrator Accounts of Omada SDN Controller et Manage Your Controller Remotely via Cloud Access dans ce guide.

Réseau

Les widgets du réseau utilisent des listes et des graphiques pour illustrer l'état du trafic des réseaux câblés et sans fil dans le site, y compris les appareils les plus actifs, les statistiques de trafic et la distribution.

- **Alertes**

  Le widget Alertes affiche le nombre total d'alertes nonarchived qui se sont produites dans le site et les détails des cinq dernières. Pour afficher toutes les alertes et les archiver, cliquez sur Details allez sur Log > Alerts. Pour spécifier les événements apparus dans Alertes, accédez à Log > Notifications et configurez les événements comme niveau d'alerte. Pour plus de détails, reportez-vous à View and Manage Logs.



■

■ **Les commutateurs les plus actifs/commutateurs les plus actifs**

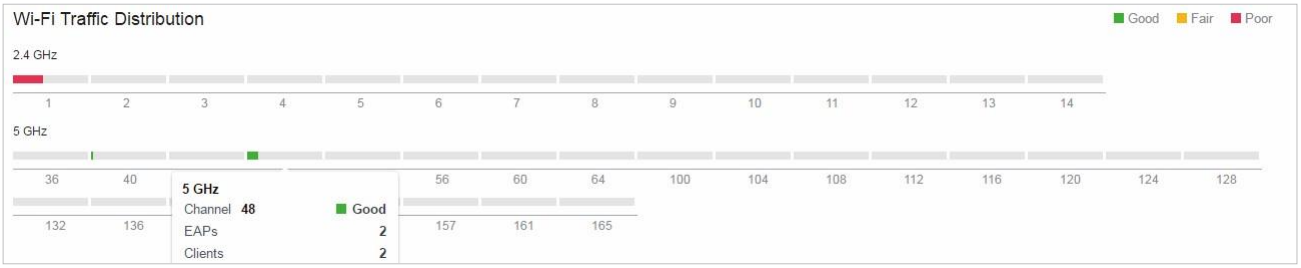
Ces deux widgets peuvent afficher, respectivement, 15 EAP et commutateurs les plus actifs dans le site en fonction du nombre total de trafic dans la plage de temps. Seuls les périphériques adoptés par le contrôleur seront affichés.

Pour afficher tous les périphériques découverts par le contrôleur, cliquez sur Détails pour accéder à la section Devices. Vous pouvez également cliquer sur le numéro de trafic dans le widget pour ouvrir la fenêtre Propriétés de l'appareil pour d'autres configurations et surveillance. Pour plus de détails, reportez-vous à Configure and Monitor Omada Managed Devices.



■ **Distribution de trafic Wi-Fi**

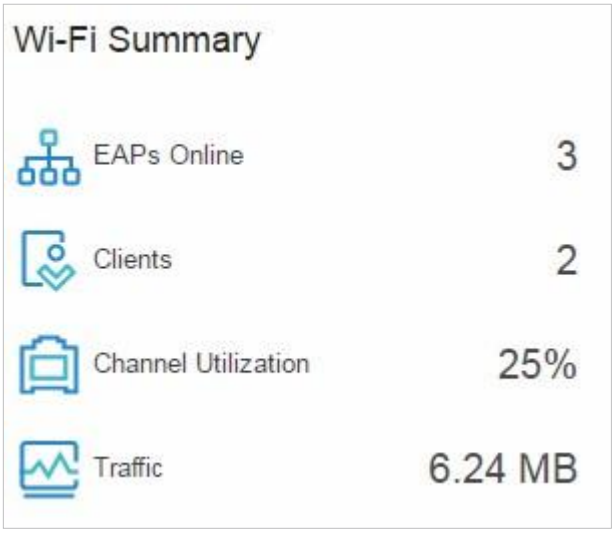
Le widget Distribution de trafic Wi-Fi affiche la distribution par canal de tous les EAP connectés sur le site. Good, Fair et Poor sont utilisés pour décrire l'état du canal qui indique l'interférence du canal de bas en haut. Vous pouvez placer votre curseur au-dessus de la bande pour afficher le nombre d'EAP et de clients sur le canal.



■

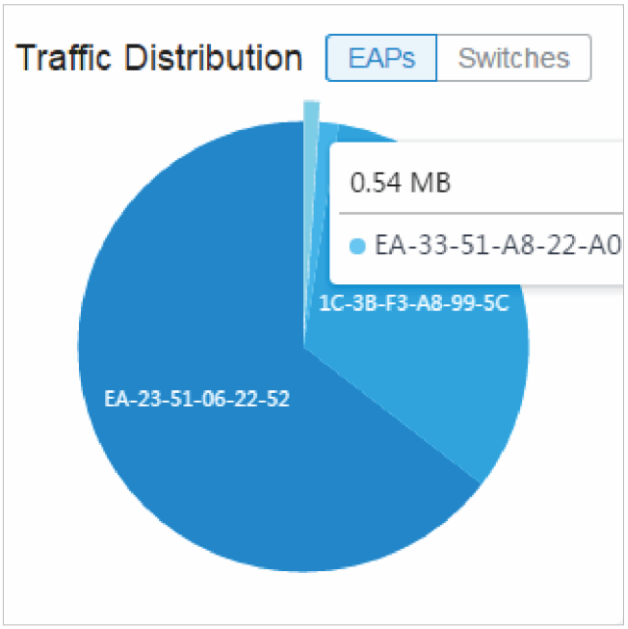
■ **Résumé Wi-Fi**

Le widget Résumé Wi-Fi résume l'état en temps réel des réseaux sans fil dans le site, y compris le nombre de PAE et de clients connectés, l'utilisation du canal et le nombre total de trafic dans la plage de temps.



■ **Distribution de trafic**

Le widget Distribution de trafic utilise un graphique en secteurs pour afficher la distribution du trafic sur les PAE et les commutateurs dans le site dans la plage de temps. Cliquez sur l'onglet pour afficher la statistique des EAP ou des commutateurs, puis cliquez sur la tranche pour afficher le nombre total de trafic, sa proportion et le nom de l'appareil.



■

■ **Client Distribution**

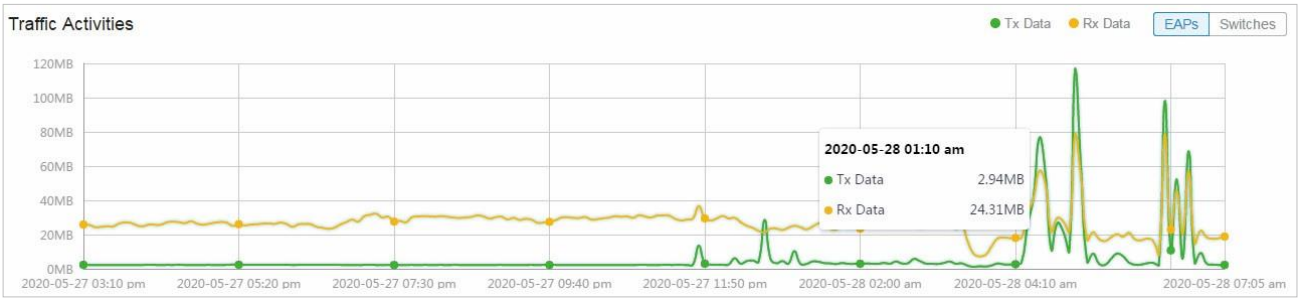
Le widget Distribution client utilise un graphique sunburst pour afficher la distribution en temps réel des clients connectés sur le site. Le graphique a jusqu'à trois niveaux. Le cercle intérieur est divisé par la catégorie d'appareil à laquelle les clients sont connectés, le milieu est par le nom de l'appareil et l'extérieur est par la bande de fréquences. Vous pouvez placer le curseur au-dessus de la tranche pour afficher des valeurs spécifiques.



■ **Activités de circulation**

Le widget Activités de trafic affiche les données Tx et Rx des EAP et des commutateurs dans la plage de temps. Seules les activités des périphériques de l'état connecté seront actuellement comptabilisées.

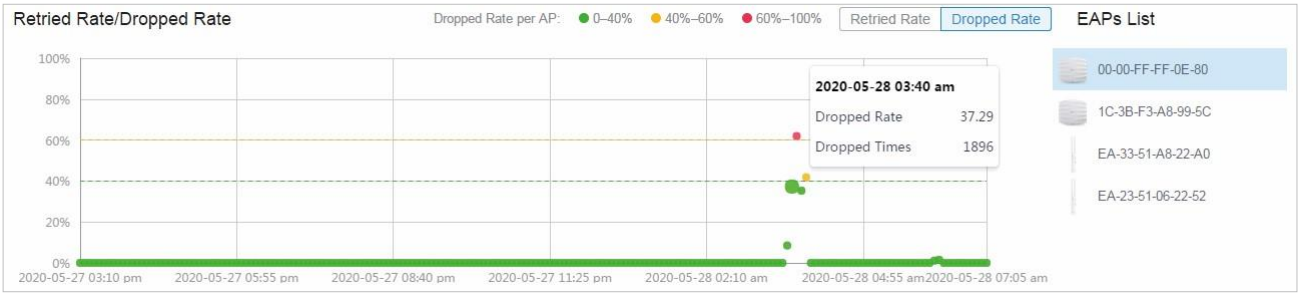
Cliquez sur l'onglet pour afficher la statistique des EAP ou des commutateurs, puis déplacez le curseur sur le graphique en ligne pour afficher des valeurs spécifiques de trafic. Pour obtenir des statistiques détaillées sur certains appareils dans un délai, View the Statistics of the Network.



■ **Taux rejugé/taux abandonné**

Le widget Taux/taux d'abandon rejugé affiche le taux de rejugé et de paquets abandonnés des EAP connectés dans la plage de temps. Sélectionnez un AP dans la liste et cliquez sur l'onglet pour afficher le graphique du taux de rejugé ou du taux de chute. Vous pouvez déplacer le curseur sur le point pour afficher des valeurs spécifiques.

■



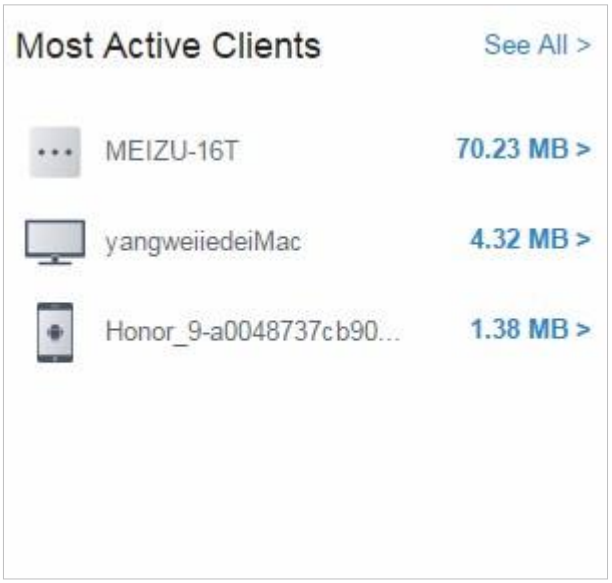
Client

Les widgets des clients utilisent des listes et des graphiques pour illustrer l'état du trafic des clients câblés et sans fil dans le site, y compris les clients les plus actifs, les statistiques d'activité et la distribution.

■ **Clients les plus actifs**

Le widget Clients les plus actifs peut afficher 15 clients les plus actifs. Seuls les clients dans le statut connecté actuellement seront affichés.

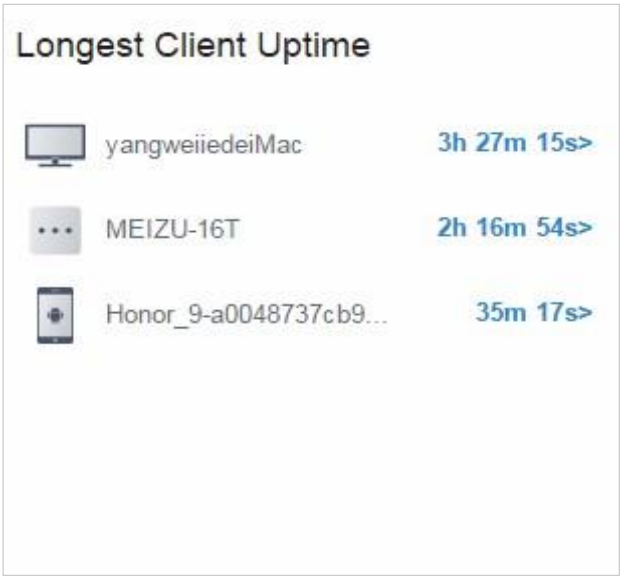
Pour afficher tous les clients connectés au réseau, cliquez sur Details allez dans la section Clients. Vous pouvez également cliquer sur le numéro de trafic dans le widget pour ouvrir la fenêtre Propriétés du client pour d'autres configurations et surveillance. Pour plus de détails, reportez-vous à Client.



■ **Le plus long temps d'attente du client**

Le widget Plus long temps de disponibilité du client peut afficher jusqu'à 15 clients triés par le temps de disponibilité. Seuls les clients dans le statut connecté actuellement seront affichés. Vous pouvez également cliquer sur le temps de disponibilité dans le widget pour ouvrir la fenêtre Propriétés du client pour d'autres configurations et surveillance. Pour plus de détails, reportez-vous à Client.

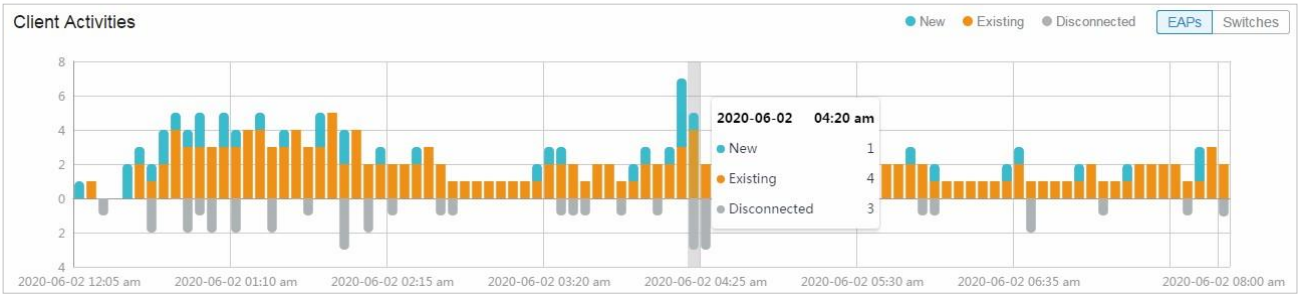
■



■ **Activités clients**

Le widget Activités clients affiche comment le nombre de clients connectés change au fil du temps dans la plage de temps. Dans le graphique empilé, vous pouvez facilement comparer le nombre total de clients et analyser la variation de chaque période de temps.

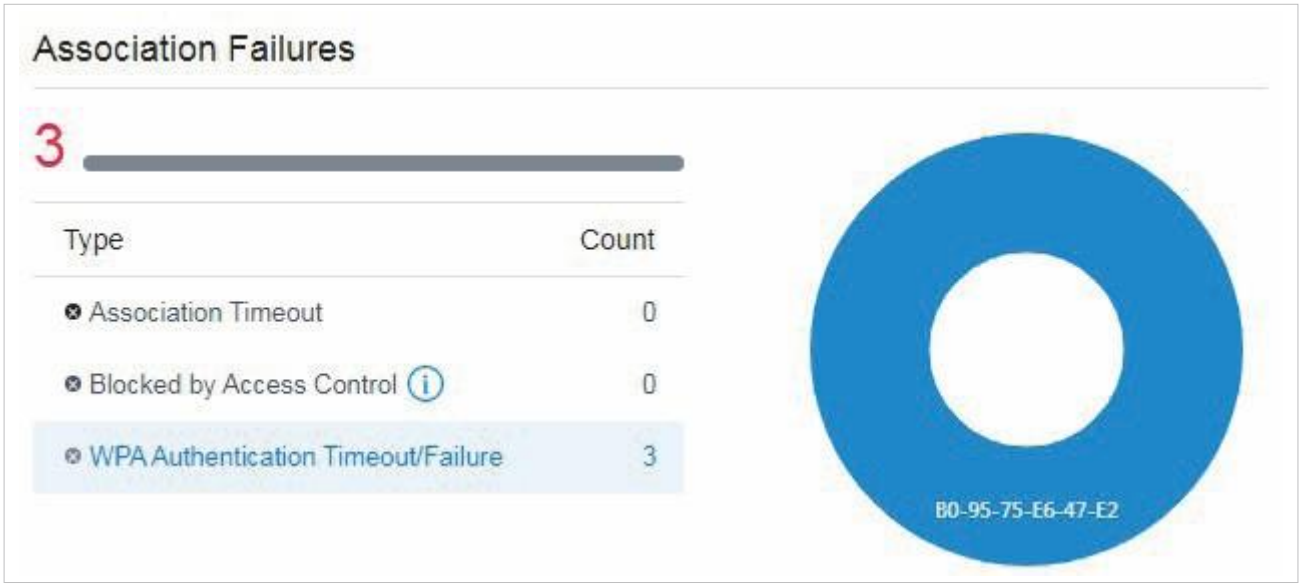
La valeur totale d'une colonne affiche le nombre total de clients connectés au cours de cette période, et les segments en trois couleurs montrent le changement de numéro de client par rapport à la dernière période. Blue représente les clients nouvellement connectés, orange est les clients ont été connectés dans la dernière période, et le gris est les clients nouvellement déconnectés.



■ **Échecs d'association**

Le widget Échecs de l'association répertorie trois types d'échec et les heures de connexion des clients n'ont pas réussi à se connecter aux réseaux des EAP's dans le site. Une seule barre est à côté du compte pour afficher la proportion des trois raisons d'échec en utilisant des couleurs grises de l'obscurité à la lumière. Cliquez sur la raison dans la liste pour afficher la distribution des échecs sur les EAP's.

■



Association Timeout	La connexion a échoué en raison du délai d'expiration de la
Blocked by Access Control	La connexion a échoué car le client a été bloqué. Pour plus d'informations sur les clients bloqués, reportez-vous à Known Clients.
WPA Authentication Timeout/Failure	La connexion a échoué parce que le client n'a pas réussi l'authentification en raison du délai d'expiration d'authentification ou d'un mauvais mot de passe.

8. 2 Voir les statistiques du réseau

Les statistiques fournissent une représentation visuelle des données de périphérique dans le contrôleur SDN d'Omada. Vous pouvez facilement surveiller le trafic réseau et les performances sous les onglets suivants, Performances, Statistiques de commutateur et Statistiques de test de vitesse.

8. 2. 1 Performance

Dans Performance, vous pouvez afficher les performances du périphérique dans une période spécifiée par graphiques, tels que le nombre d'utilisateurs, l'utilisation du processeur et de la mémoire, ainsi que les paquets transmis et reçus. Les graphiques varient en fonction du type et de l'état de l'appareil.

Barre d'onglets

Les onglets et le calendrier en haut sont utilisés pour spécifier les statistiques affichées et les légendes sur le compte droit pour les éléments dans les graphiques.

■



	Cliquez pour sélectionner un périphérique dans la liste déroulante pour afficher ses statistiques. Les onglets varient en raison du type de l'appareil sélectionné
	Cliquez sur la date pour afficher un calendrier. Cliquez deux fois sur une date spécifique dans le calendrier pour que les widgets affichent ses statistiques. Pour afficher la statistique d'une plage de temps, cliquez sur la date de début et la date de fin dans le calendrier, ou sélectionnez directement la plage d'heure à droite. La plage de temps disponible est limitée par l'intervalle de temps. Avant de sélectionner une longue plage de temps, sélectionnez Horaire ou quotidien comme intervalle de temps.
	Sélectionnez 5 minutes, Hourly, ou Daily pour spécifier l'intervalle de temps des données. Lors de la sélection longue plage de temps, un intervalle de temps plus long est recommandé pour une meilleure
	(Pour la passerelle) Cliquez pour sélectionner le port de passerelle de l'onglet pour afficher les statistiques.
	(Pour AP) Cliquez pour sélectionner la bande de l'AP pour afficher les statistiques.

Graphiques statistiques

Les graphiques statistiques varient selon le type d'appareils. Le tableau ci-dessous montre les graphiques statistiques qui correspondent à la passerelle, au commutateur et à l'AP.

Gateway	Nombre d'utilisateurs, Utilisation, Trafic, Paquets
Switch	Nombre d'utilisateurs, Utilisation
AP	Nombre d'utilisateurs, Utilisation, Trafic, Paquets, Dropped, Erreurs, Retries

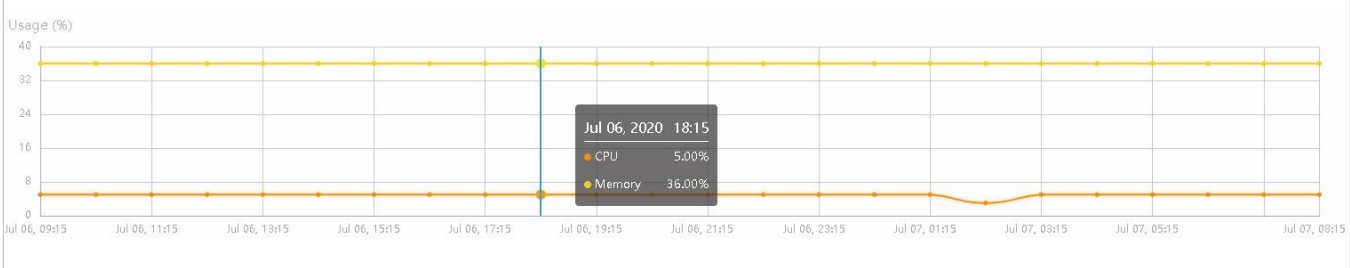
Nombre d'utilisateurs

Le graphique Nombre d'utilisateurs affiche le nombre d'utilisateurs connectés aux périphériques pendant la plage de temps sélectionnée. Placez le curseur au-dessus de la ligne pour afficher les valeurs spécifiques.



Utilisation

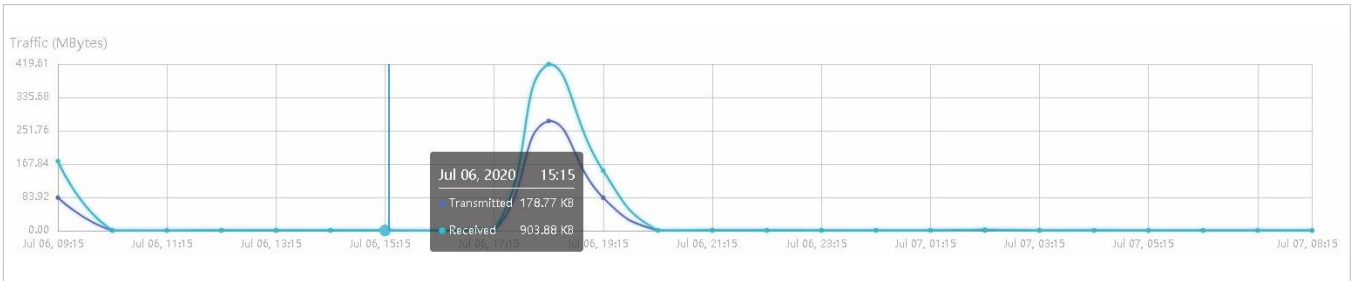
Le graphique Utilisation utilise la ligne orange et la ligne jaune pour afficher le pourcentage d'utilisation du processeur et de mémoire utilisée au cours de la plage de temps sélectionnée, respectivement. Placez le curseur sur les lignes pour afficher les valeurs spécifiques.



■

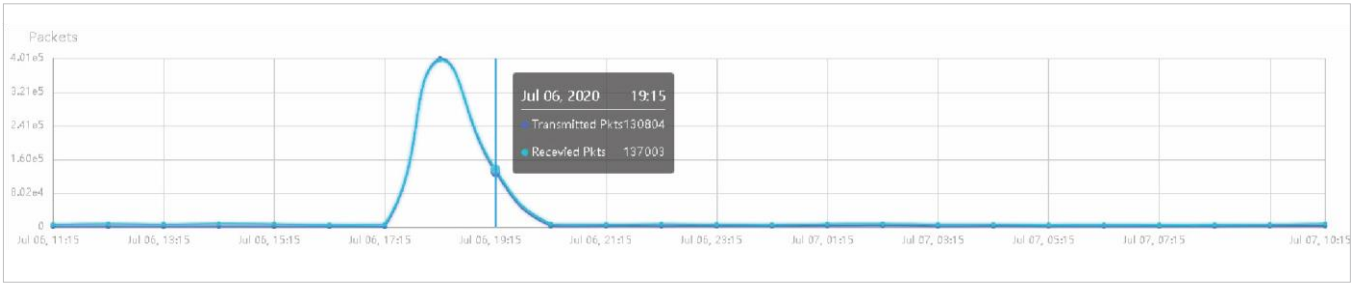
■ **Trafic**

Le graphique Traffic utilise la ligne bleu foncé et la ligne bleu clair pour afficher les octets des données transmises et reçues au cours de la plage de temps sélectionnée, respectivement. Placez le curseur sur les lignes pour afficher les valeurs spécifiques.



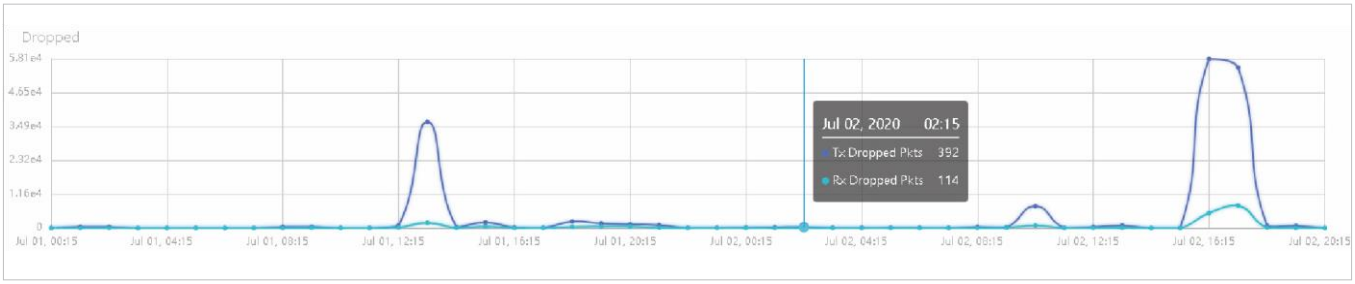
Paquets

Le graphique Packets utilise la ligne bleu foncé et la ligne bleu clair pour afficher le nombre de paquets transmis et reçus au cours de la plage de temps sélectionnée, respectivement. Placez le curseur sur les lignes pour afficher les valeurs spécifiques.



■ **Dropped**

Le graphique Dropped utilise la ligne bleu foncé et la ligne bleu clair pour afficher le nombre de paquets Tx et de paquets Rx abandonnés au cours de la plage de temps sélectionnée, respectivement. Planez le curseur sur les lignes pour afficher les valeurs spécifiques.



■

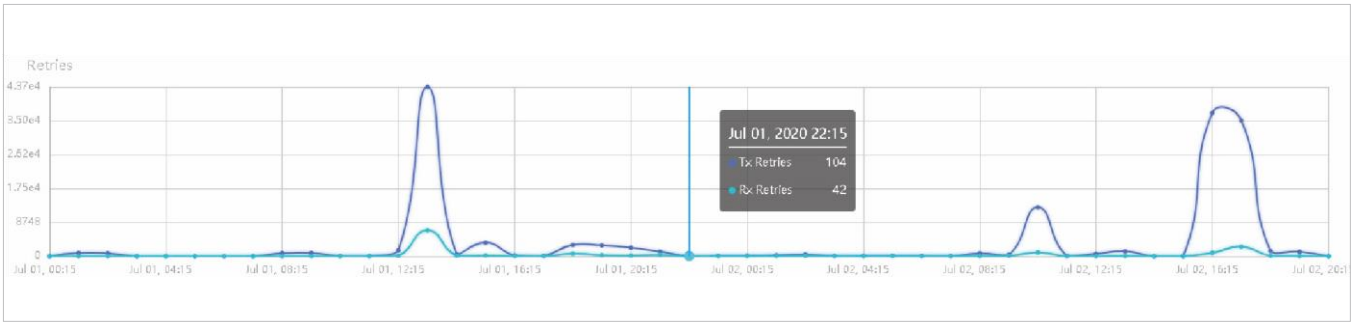
■ **Erreurs**

Le graphique Erreurs utilise la ligne bleu foncé et la ligne bleu clair pour afficher le nombre de paquets d'erreur envoyés à AP et reçus par AP au cours de la plage de temps sélectionnée, respectivement. Placez le curseur au-dessus de la ligne pour afficher les valeurs spécifiques.



Tentatives

Le graphique Retries utilise la ligne bleu foncé et la ligne bleue claire pour afficher le nombre de fois où les paquets de données sont transmis à nouveau et reçus à nouveau au cours de la période sélectionnée, respectivement. Placez le curseur sur les lignes pour afficher les valeurs spécifiques.



8. 2. 2 Statistiques de commutateur

Dans **Switch Statistics,** vous pouvez afficher l'état actuel des ports et leurs statistiques de trafic du commutateur sélectionné dans la plage de temps spécifiée via un panneau de moniteur et des graphiques.

Barre d'onglets

Les onglets et le calendrier en haut sont utilisés pour spécifier les statistiques affichées et les légendes sur le compte droit pour les éléments dans les graphiques.



Cliquez pour sélectionner un commutateur dans la liste déroulante pour afficher ses statistiques.



Cliquez sur la date pour afficher un calendrier. Cliquez deux fois sur une date spécifique dans le calendrier pour que les widgets affichent ses statistiques. Pour afficher la statistique d'une plage de temps, cliquez sur la date de début et la date de fin dans le calendrier, ou sélectionnez directement la plage d'heure à droite.

La plage de temps disponible est limitée par l'intervalle de temps. Avant de sélectionner une longue plage de temps, sélectionnez Horaire ou Quotidien comme intervalle de temps.



Select 5 minutes, Hourly, ou Daily pour spécifier l'intervalle de temps des données. Lors de la sélection d'un longue plage de temps, un intervalle de temps plus long est recommandé pour une meilleure vue.



Sélectionnez Naturel, Transmis, Reçu ou Tout pour spécifier l'ordre graphique des ports.

Natural: Affiche les graphiques de ligne dans l'ordre croissant du numéro de port.

Transmitted: Affiche les graphiques de ligne en ordre décroissant en fonction du volume de trafic des paquets transmis.

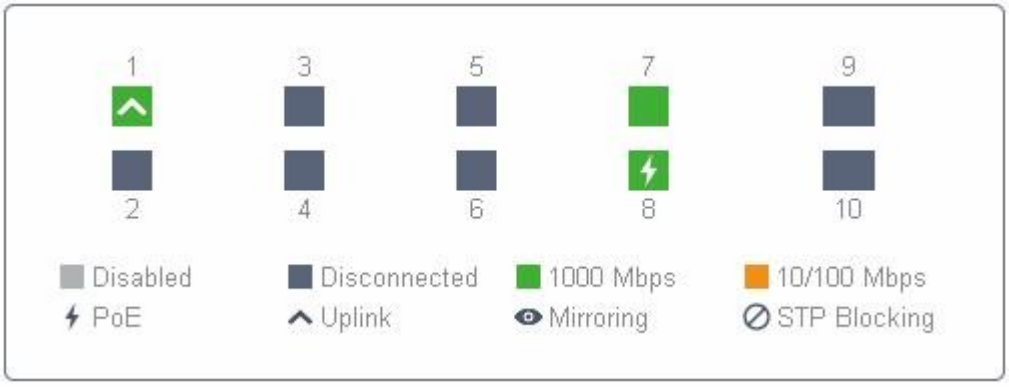
Received: Affiche les graphiques de ligne dans l'ordre décroissant en fonction du volume de trafic des paquets reçus.

All: Affiche les graphiques de ligne en ordre décroissant en fonction du volume total de trafic des paquets transmis et reçus.

bps Bytes Packets	Sélectionnez bps, octets ou paquets pour spécifier le type de données et l'unité de mesure. bps: Affiche le taux de trafic en bps. Bytes: Affiche les statistiques de trafic dans Bytes. Packets: Affiche le nombre total de paquets. , cliquez sur l'onglet pour spécifier le type de statistiques de paquets à afficher All: Affiche les statistiques de tous les paquets, y compris les paquets de diffusion et de diffusion multidiffusion. Broadcast: Affiche uniquement les statistiques des paquets de diffusion. Multicast: Affiche uniquement les statistiques des paquets multidiffusion.

Panneau de moniteur

Le panneau moniteur sous la barre d'onglets affiche l'état actuel des ports sur le commutateur sélectionné.

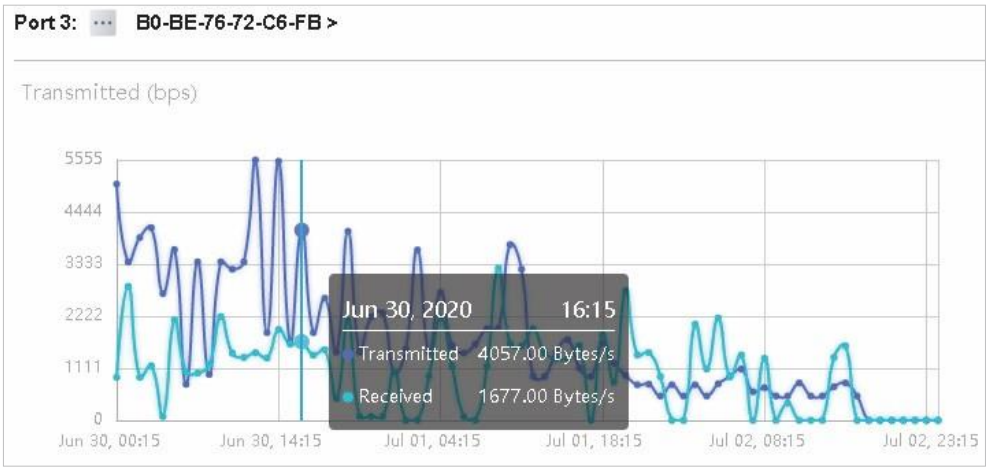


Disabled	Le profil de port est Désactiver. Pour l'activer, reportez-vous Configure and Monitor Switches
Disconnected	Le port est activé mais ne se connecte à aucun appareil ou client.
1000 Mbps	Le port fonctionne à 1000 Mbps.
10/100 Mbps	Le port fonctionne à 10/100 Mbps.
PoE	Un port PoE connecté à un dispositif alimenté (PD).
Uplink	Un port de liaison vers l'avant connecté à WAN.
Mirroring	Un port de mise en miroir qui reflète un autre port d'interrupteur.

⊘ STP Blocking	Port dans l'état Blocage dans Enjambent Tree. Il reçoit et envoie des paquets BPDU (Bridge Protocal Data Unit) pour maintenir l'arbre enjambant. D'autres paquets sont supprimés.

Graphiques statistiques

Les graphiques statistiques sous le panneau de surveillance affichent les statistiques de trafic des ports actifs. Vous pouvez spécifier le type de données et l'unité de mesure en cliquant sur l'onglet. Le bleu foncé et le bleu clair sont utilisés pour indiquer les statistiques transmises et reçues, respectivement. Placez le curseur sur les lignes pour afficher les valeurs spécifiques. Pour afficher et configurer le périphérique connecté au port, cliquez sur le nom du périphérique à côté du numéro de port. bps Bytes Packets



8. 2. 3 Statistiques des tests de vitesse

Speed Test Statistics affiche les résultats du test de vitesse périodique en cours d'exécution sur les ports WAN, y compris la latence et la vitesse du réseau. Pour activer le test de vitesse, Settings > Sites, activer le test de vitesse périodique en service et spécifier l'intervalle de test. Pour plus de détails, reportez-vous à Services.

Barre d'onglets

L'onglet et le calendrier en haut sont utilisés pour spécifier les statistiques affichées et les légendes sur le compte droit pour les éléments dans les graphiques.

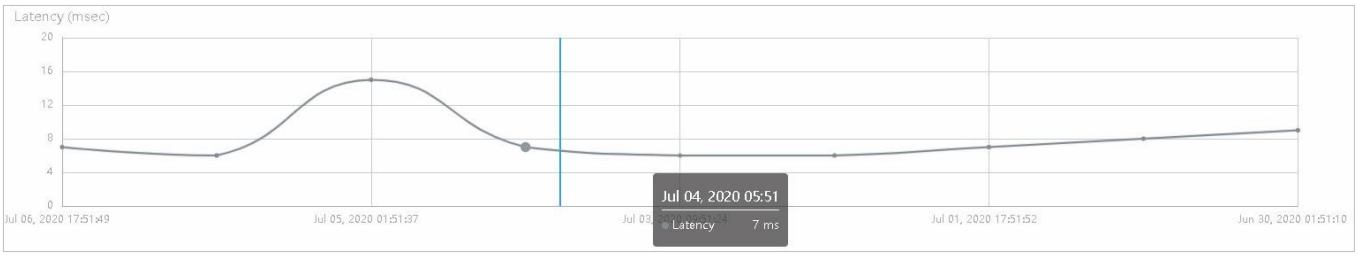
Jul 06, 2020 - Jul 07, 2020	Cliquez sur la date pour afficher un calendrier. Cliquez deux fois sur une date spécifique dans le calendrier widgets pour afficher ses statistiques. Pour afficher la statistique d'une plage de temps, cliquez sur la date et la date de fin dans le calendrier, ou sélectionnez directement la plage d'heure sur la droite.
WAN WAN/LAN1	Sélectionnez le port à afficher la latence et la vitesse.

Graphiques statistiques

Les graphiques statistiques sous la barre d'onglets affichent la latence réseau et la vitesse du port WAN.

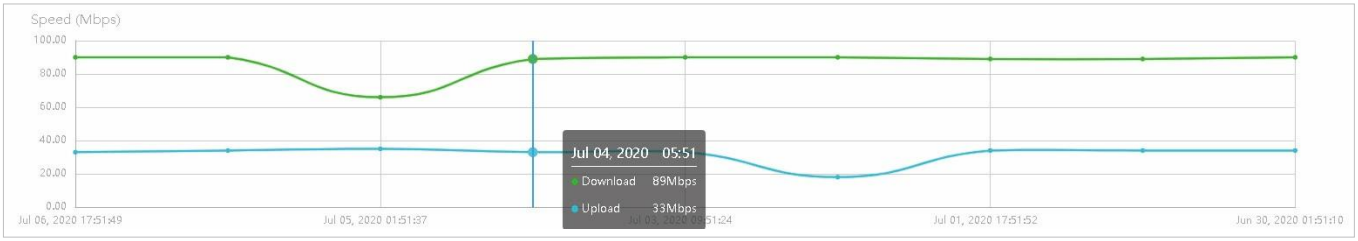
- **Latence**

Le graphique de latence affiche le temps qu'il faut pour qu'un paquet se déplace de la passerelle vers la passerelle du fournisseur de services.



- **Vitesse**

Le graphique Speed utilise la ligne bleue et la ligne verte pour afficher la vitesse de téléchargement et de téléchargement du port WAN, respectivement.



8. 3 Surveiller le réseau avec la carte

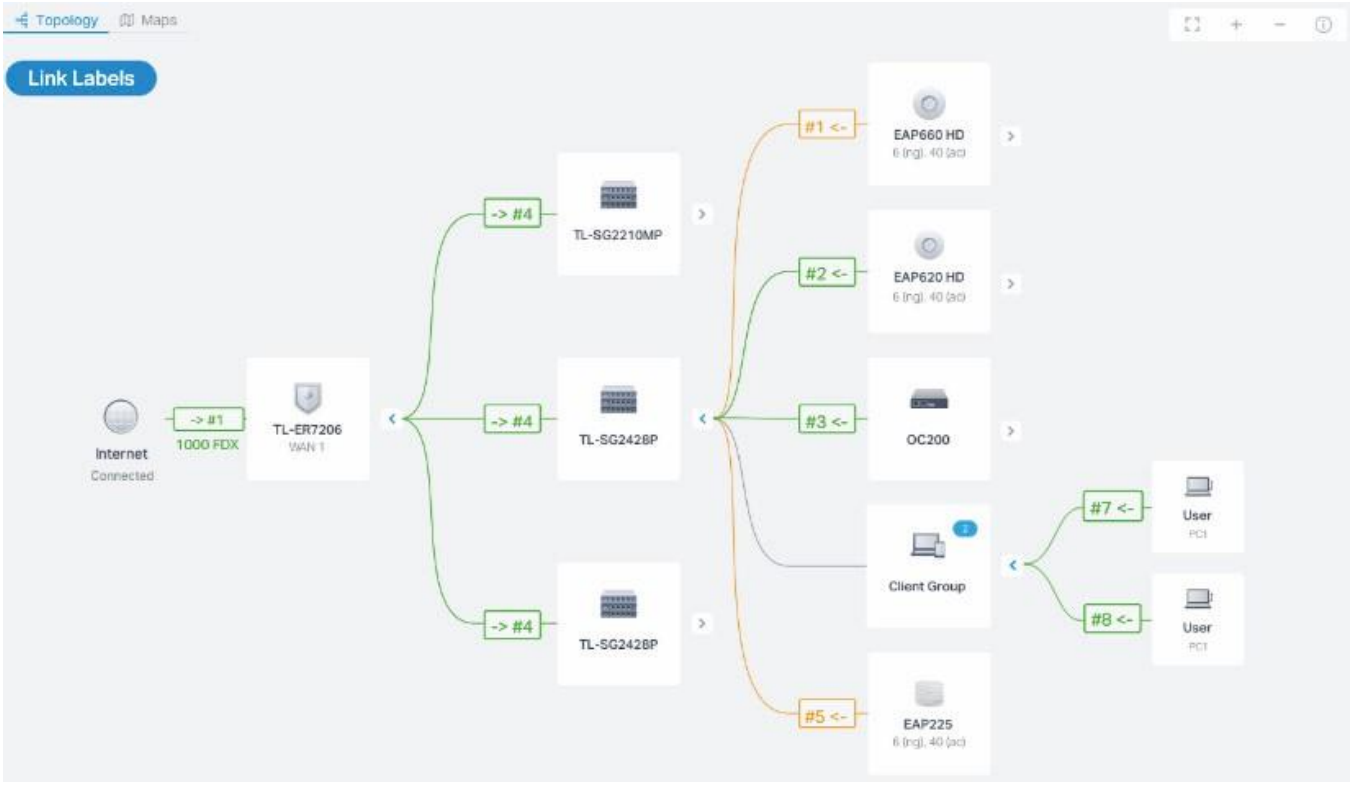
Dans le **Map section**, vous pouvez examiner la topologie et l'approvisionnement en périphériques du réseau dans Topology et personnaliser une représentation visuelle de votre réseau dans Map.

8. 3. 1 Topologie

Allez dans Map > Topology, et vous pouvez afficher automatiquement la topologie générée par le contrôleur. Vous pouvez cliquer sur l'icône des périphériques pour ouvrir la fenêtre Propriétés. Pour une configuration et une surveillance détaillées dans la fenêtre Propriétés, reportez-vous à Configure and Monitor Omada Managed Devices.



Pour une meilleure vue d'ensemble de la topologie réseau, vous pouvez contrôler l'affichage des branches, la taille du diagramme et les étiquettes de lien.



■ **Affichage des branches**

La vue par défaut affiche tous les appareils connectés par des lignes solides et pointillées. Cliquez sur l'icône du groupe client pour afficher les clients connectés au même appareil. Cliquez sur les hochements de tête pour déplier ⊕ ou plier les branches. ⊖

■ **Taille du diagramme**

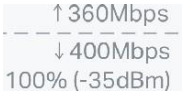
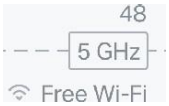
Cliquez sur les icônes dans le coin droit pour ajuster la taille de la topologie et afficher les légendes.

	Cliquez pour adapter la topologie à la page Web.
	Cliquez pour zoomer sur la topologie.
	Cliquez pour zoomer sur la topologie.
	Cliquez pour voir la signification des lignes dans la topologie. Des lignes solides et pointillées sont utilisées pour indiquer les connexions filaires et sans fil, respectivement, et quatre couleurs sont utilisées pour indiquer la vitesse de liaison

■

Link Labels

Cliquez sur Link Labels dans le coin gauche, et les étiquettes semblent afficher l'état du lien. Les informations sur les étiquettes varient en raison des connexions de lien.

	(Pour le port WAN du routeur connecté à Internet) affiche le nom du port, vitesse de liaison et type duplex.
	Pour les connexions câblées simples) affiche la vitesse de liaison, le type duplex et numéro de port connecté. Notez que seul le numéro de port du commutateur peut être affiché dans l'étiquette.
	(Pour l'agrégation de liens) affiche la vitesse du LAG, le type duplex, l'ID LAG et le port nombre de membres du LAG.
	(Pour les connexions sans fil entre les AP) affiche le RSSI (affiché dans pourcentage et dBm) et le taux de négociation de la liaison.
	(Pour les connexions sans fil entre les AP et les clients) Affiche le canal d'AP, connecté SSID, et sa force de signal.

8. 3. 2 Map

Dans Map > Map, et une carte par défaut est affichée ci-dessous avec les périphériques non placés répertoriés sur la gauche. Vous pouvez télécharger vos images de carte locales et faire glisser dans les appareils pour personnaliser une représentation visuelle de votre réseau.

Personnaliser la carte

Cliquez sur les icônes suivantes pour ajouter, modifier et sélectionner la carte. Après avoir sélectionné une carte, cliquez et faites glisser dans les périphériques à partir de la Devices list to place it on the map according to the actual locations.

	Cliquez pour ajouter une carte. Dans la fenêtre contextuelle, entrez la description et upload an image in the .jpg, .jpeg, .gif, .png, .bmp, .tiff format.
	Cliquez pour modifier des cartes dans la fenêtre Cliquez sur  pour modifier la description de la carte. Cliquez sur  pour supprimer la
	Cliquez pour sélectionner une carte dans la liste déroulante pour placer les périphériques.

- Placez votre curseur au-dessus de l'icône du périphérique pour afficher les informations de base de celui-ci, y compris le nom de l'appareil, l'adresse MAC, l'adresse IP et les clients connectés.



Vous pouvez cliquer sur l'icône de l'appareil pour révéler des icônes d'action supplémentaires :

	Indique que l'appareil est déverrouillé et que vous pouvez cliquer dessus pour verrouiller périphérique à l'emplacement actuel. Lorsqu'il est déverrouillé, vous pouvez déplacer l'appareil sur la carte et cliquez sur les icônes d'action qui l'entourent.
	Indique que l'appareil est verrouillé sur la carte et que vous ne pouvez cliquer que sur licone le produit est bloqué
	Affiche la fenêtre Propriétés de l'appareil. Pour une configuration détaillée et surveiller dans la fenêtre Propriétés, reportez-vous à Configure and Monitor Omada Managed Devices.
	Cliquez pour renvoyer le périphérique sélectionné dans la liste Périphérique.
	(Uniquement pour les commutateurs connectés et les AP) Cliquez pour flasher la LED de sur la carte. Ensuite, la LED clignotera pendant 10 minutes ou jusqu'à ce que l'annulation est de nouveau cliqué.
	Cliquez pour empêcher la LED de clignoter.

Taille du diagramme

Cliquez sur les icônes dans le coin droit pour ajuster la taille de la topologie et afficher les légendes.

	Cliquez pour adapter la carte à la page Web.
	Cliquez pour zoomer sur la carte.
	Cliquez pour zoomer sur la carte.

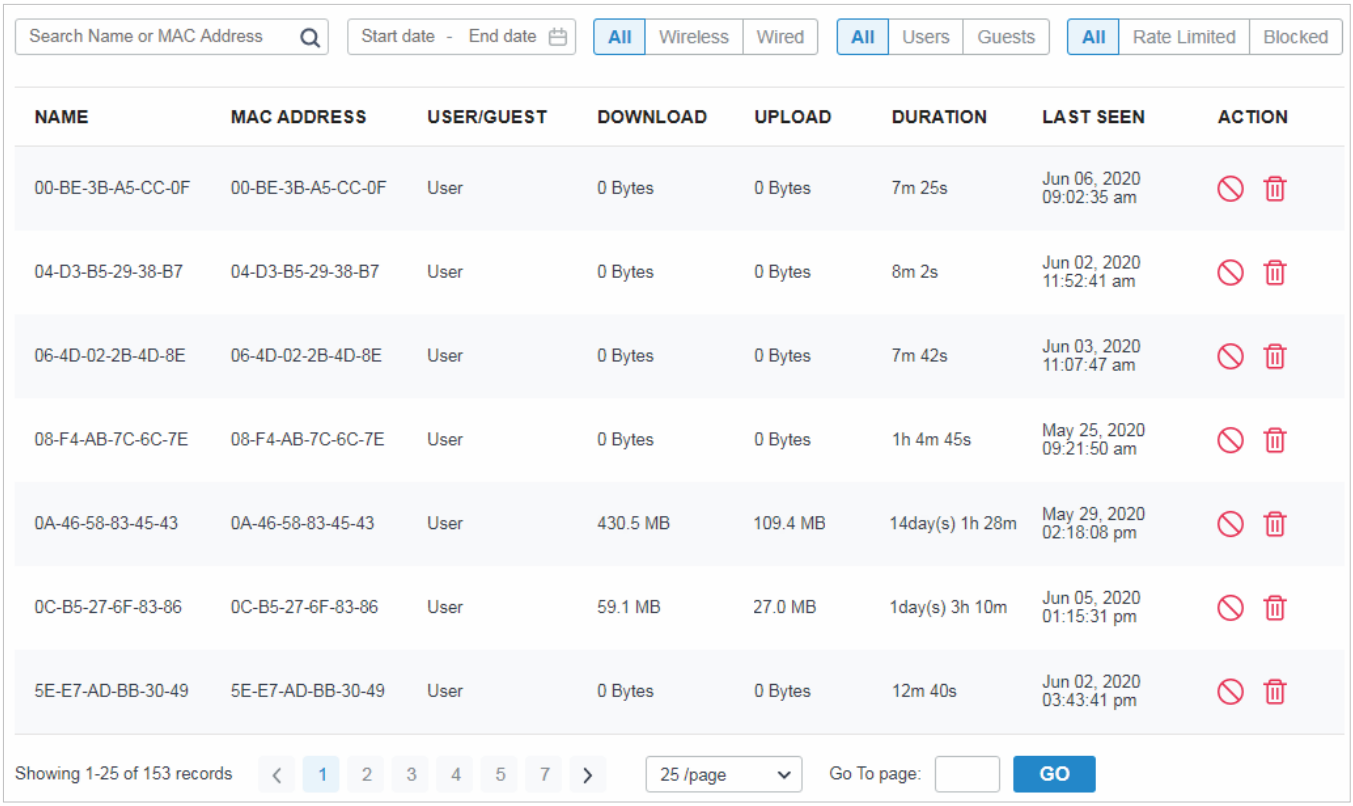
8. 4 Afficher les statistiques pendant la période spécifiée avec Insight

Dans la page Insight, vous avez surveillé l'historique du site des clients connectés, des autorisations de portail et des AP rouges. Pour une meilleure surveillance, vous avez versé spécifique la période et classer les clients et les AP.

8. 4. 1 Known Clients

Dans Clients connus, un tableau répertorie tous les clients qui se sont connectés au réseau auparavant sur le site.

Dans le tableau, vous pouvez afficher les informations de base, les statistiques de rôle et de connexion du client, y compris les trafics de téléchargement et de téléchargement, la durée de la connexion et la dernière fois qu'il s'est connecté au réseau.



Une barre de recherche, un sélecteur de temps et trois onglets sont au-dessus de la table pour la recherche et le filtrage.

Search Name or MAC Address	Entrez le nom du client ou l'adresse MAC pour rechercher les clients.
Start date - End date	Filtrer les clients en fonction de Last Seen. Cliquez sur le sélecteur pour ouvrir le calendrier. Cliquez deux fois sur une date spécifique dans le calendrier pour afficher les enregistrements de la journée. Pour afficher les enregistrements d'une plage de temps, cliquez sur la date de début et la date de fin dans le calendrier.

All Wireless Wired	Cliquez sur les onglets pour filtrer les clients répertoriés dans le tableau. Les trois onglets peuvent prendre effet simultanément.
All Users Guests	All/Wireless/Wired: Click All pour afficher les clients sans fil et câblés. Cliquez sur Wireless ouWired Pour afficher uniquement les clients sans fil ou
All Rate Limited Blocked	All/Users/Guests: Cliquez sur All pour afficher à la fois les utilisateurs et les invités. Cliquez sur Users or Gusets pour afficher uniquement les utilisateurs ou les invités. Les clients sont des utilisateurs connectés au réseau d'invités sans fil. Pour configurer le réseau invité, reportez-vous à Configure Wireless Networks.
	All/Rate Limitted/Blocked: Cliquez sur All pour afficher les clients à taux limité et bloqué. Cliquez sur Taux limité ou bloqué pour afficher uniquement les clients limités ou bloqués. Pour configurer la limite de taux, reportez-vous au client. Pour bloquer les clients, cliquez sur l'icône du tableau.

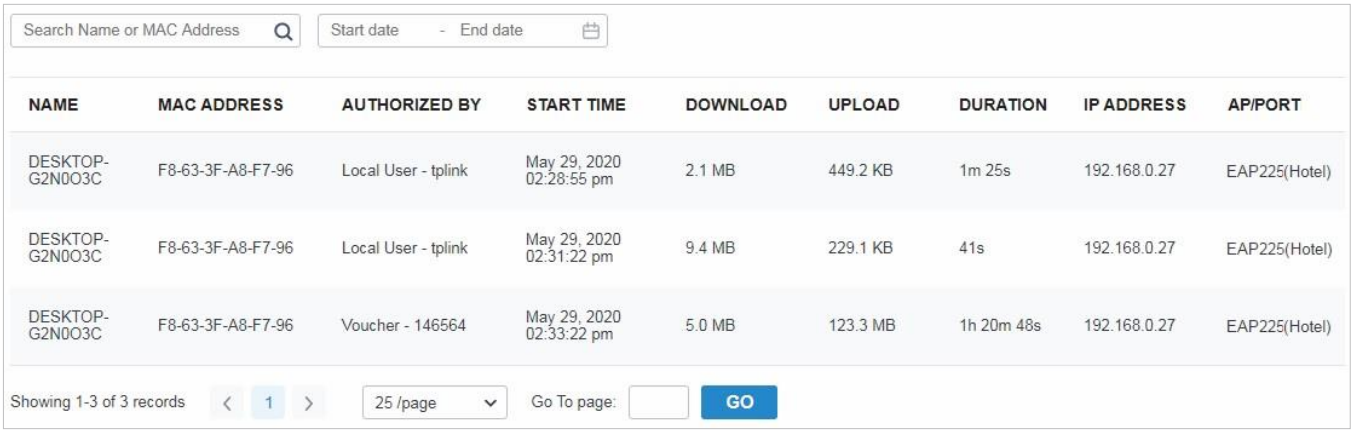
Vous pouvez également prendre des mesures pour bloquer ou oublier le client. Pour un moniteur et une gestion détaillée, cliquez sur l'entrée dans le tableau pour ouvrir la fenêtre Propriétés du client. Pour plus de détails, reportez-vous à Using the Clients Table to Monitor and Manage the Clients.

	(For unblocked clients) Click to block the client in the site. Once blocked, the client is banned from connecting to the network in the site.
	(For blocked clients) Click to unblock the client in the site.
	Click to forget the client. Once forget, all statistics and history of the client in the site are dropped.

8. 4. 2 Autorisations de portail passées

Dans l'autorisation du portail précédent, un tableau répertorie tous les clients qui ont déjà passé l'autorisation du portail.

Dans le tableau, vous pouvez afficher le nom du client, l'adresse MAC, les informations d'identification d'autorisation, les trafics de liaison et de liaison vers le bas, le temps et la durée de l'autorisation, l'adresse IP et le réseau/port à laquelle il est connecté. Pour un suivi et une gestion détaillée, reportez-vous à Manage Client Authentication in Hotspot Manager.



Une barre de recherche et un sélecteur de temps sont au-dessus de la table pour la recherche et le filtrage.



Entrez le nom du client ou l'adresse MAC pour effectuer une recherche



Filtrer les clients en fonction de l'heure de

Cliquez sur le sélecteur pour ouvrir le calendrier. Cliquez deux fois sur une date spécifique dans le calendrier pour afficher les clients autorisés le jour. Pour afficher les clients autorisés pendant une plage de temps, cliquez sur la date de début et la date de fin dans le calendrier.

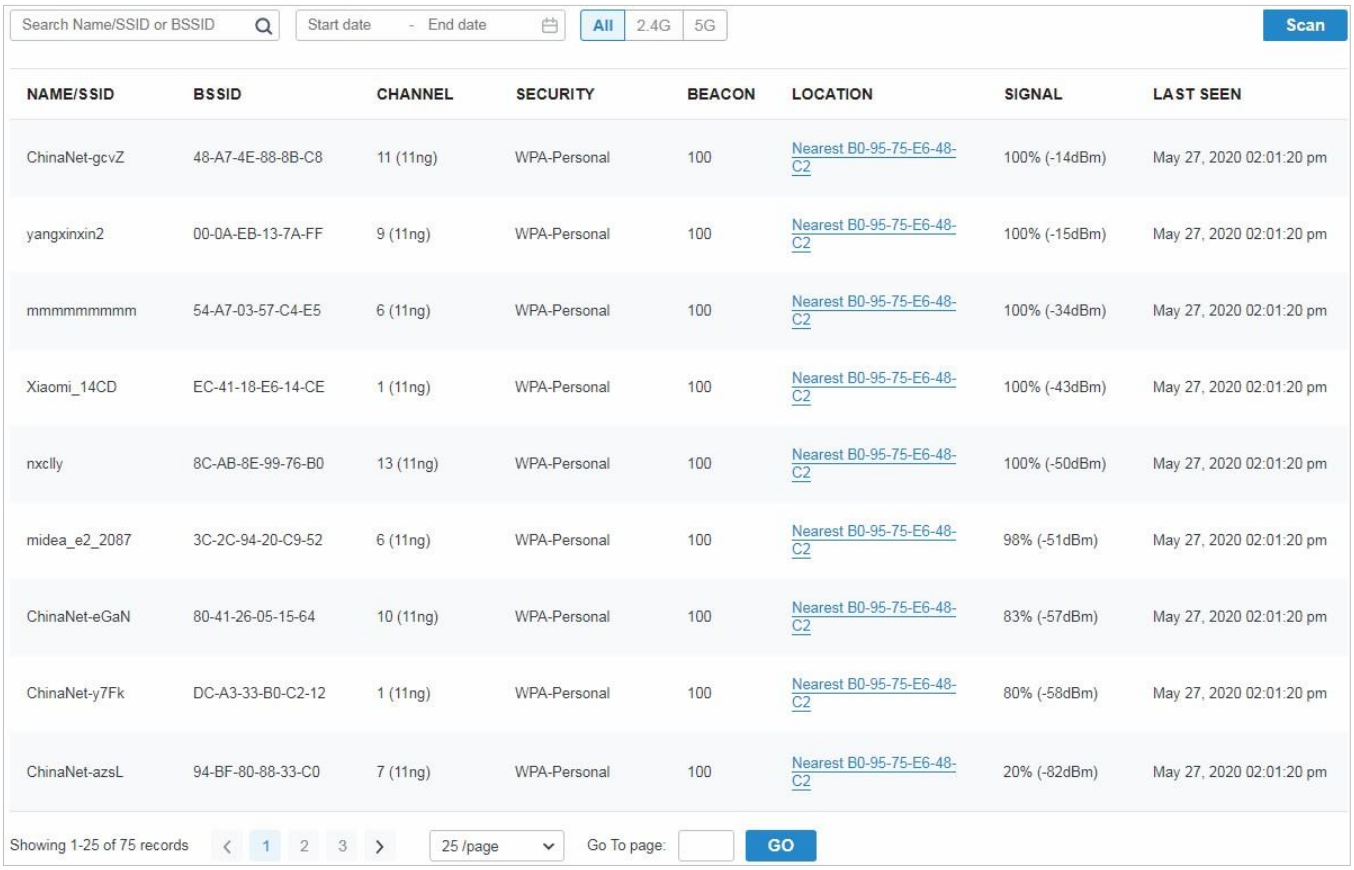
8. 4. 3 Rogue APs

un rogue AP est un point d'accès qui a été installé sur un réseau sécurisé sans autorisation explicite d'un administrateur système. Dans Rogue AP, vous pouvez scanner les AP voyous et afficher les AP voyous scannés



Cliquez sur l'onglet pour filtrer les AP voyous répertoriés dans le tableau en fonction de la bande de fréquences.

avant.



Search Name or MAC Address	Entrez le nom du client ou l'adresse MAC pour effectuer une recherche auprès des clients.
Start date - End date	Filtrer les AP voyous basés sur Last SeenFiltrer les AP voyous basés sur Last Seen. Cliquez sur le sélecteur pour ouvrir le calendrier. Cliquez deux fois sur une date spécifique dans le calendrier pour afficher les AP voyous scannés le jour. Pour afficher l'AP numérisée pendant une plage de temps, cliquez sur la date de début et la date de fin dans le calendrier.
Scan	Cliquez pour numériser les AP voyous. Cela peut prendre plusieurs minutes, et le service sans fil peut être influencé lors de la numérisation.
BSSID	Chaîne avec un formulaire similaire à l'adresse MAC pour reconnaître les points d'accès.
Channel	Affiche le canal d'opération et la norme de l'AP voyous.
Security	Affiche la stratégie de sécurité de l'AP voyous.

Beacon	Affiche l'intervalle de balise de l'AP voyous. Les balises sont transmises périodiquement par le PAE pour annoncer la présence d'un réseau sans fil pour les clients, et l'intervalle signifie combien de fois l'AP envoie une balise aux clients.
Location	Affiche l'AP géré le plus proche de l'AP voyous. Vous pouvez cliquer sur l'AP le plus proche pour ouvrir sa fenêtre Propriétés.
Signal	Affiche la force du signal en pourcentage et en dBm).
Last Seen	Affichez la dernière fois que l'AP voyou a été scanné par le contrôleur.

8. 5 Afficher et gérer les journaux

Le contrôleur utilise des journaux pour enregistrer les activités du système, des périphériques, des utilisateurs et des administrateurs, qui fournit des supports puissants pour surveiller les opérations et diagnostiquer les anomalies. Dans la page Journaux, vous pouvez surveiller les journaux Alerts et Events, et configurer leurs niveaux de notification dans Notifications.

Tous les journaux peuvent être classés à partir des quatre aspects suivants.

- **Occurred Hierarchies**

  Deux catégories dans les hiérarchies se sont produites sont Controller et Site, qui indiquent que les activités de journal se sont produites, respectivement, au niveau du contrôleur et dans certains sites. Seuls les administrateurs maîtres peuvent afficher les journaux arrivés au niveau du contrôleur.

- **Notifications**

  Deux catégories dans les notifications sont Event et Alert, et vous pouvez classer les journaux en eux par vous-même.

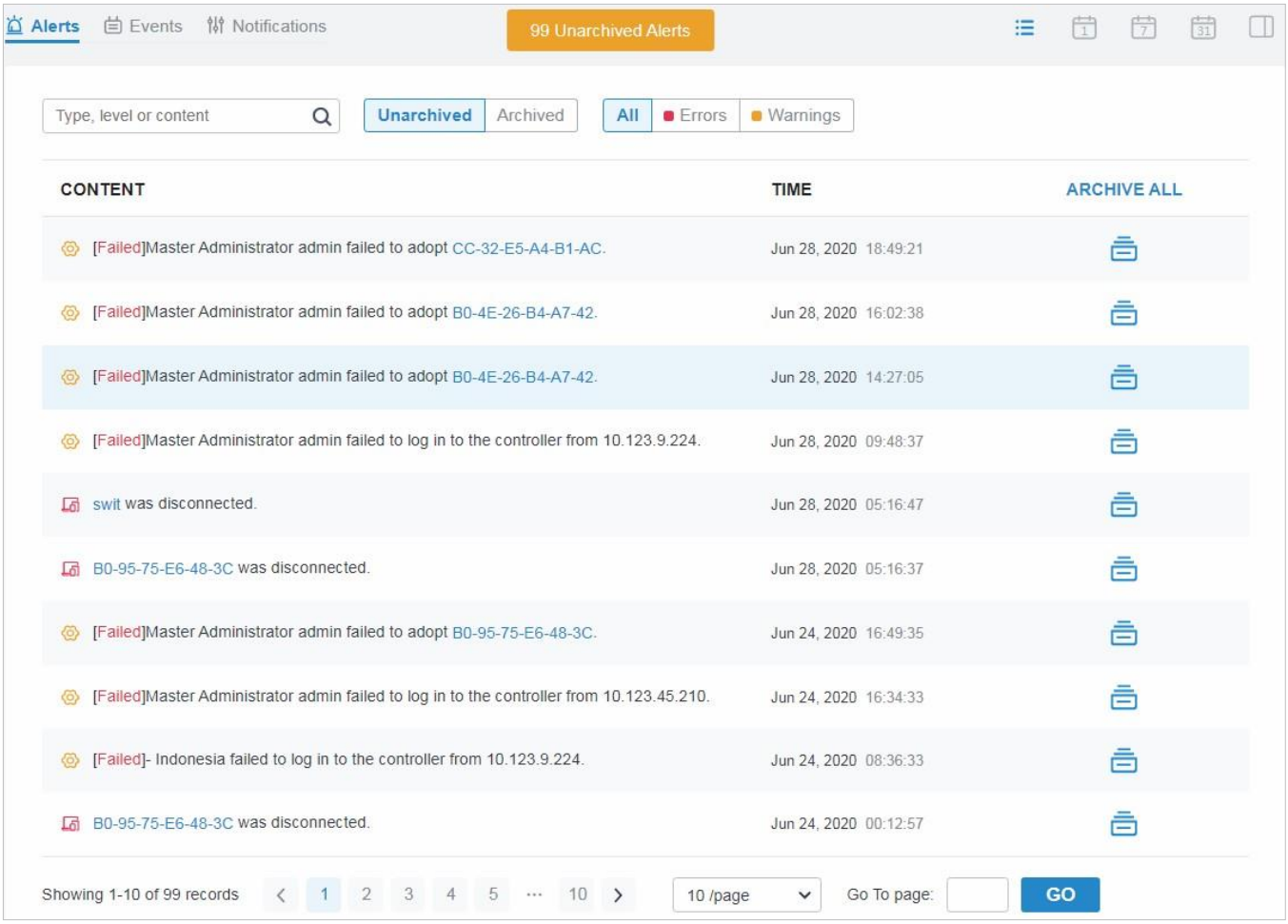
- **Sévérités**

  Trois niveaux de sévérités sont Erreur, Avertissement et Info, dont les influences sont classées de haut en bas.

- **Contenu**
  Quatre types dans le contenu sont Operation, System, Device et Client, qui indiquent le contenu du journal.

8. 5. 1 Alertes

Les alertes sont les journaux qui doivent être remarqués et archivés spécialement. Vous pouvez configurer les journaux en tant qu'alertes dans notifications, et tous les journaux configurés comme alertes sont répertoriés sous l'onglet Alertes pour que vous puissiez rechercher, filtrer et archiver.



Cliquez pour modifier le mode d'affichage pour une meilleure vue d'ensemble.

: Affiche les journaux dans une table.

/ / : Affiche les journaux en un jour/semaine/mois. Pour modifier l'heure, cliquez sur ou .

Type, level or content

Entrez les types de contenu, les niveaux de gravité ou les mots clés pour rechercher les journaux.

Unarchived Archived

All Errors Warnings

Cliquez sur les onglets pour filtrer les journaux répertoriés dans le tableau. Les deux onglets peuvent prendre effet simultanement

Unarchived : Archived : Cliquez sur l'onglet pour filtrer les journaux non archivés et archivés. Vous can click and Archive All to archiver un journal unique et tous, respectivement.

All/Errors/Warnings: Cliquez sur Tout pour afficher les journaux dans les niveaux Erreur, Avertissement et Info. Cliquez sur Erreurs ou avertissements pour afficher uniquement les journaux dans les niveaux d'erreur ou d'avertissement.

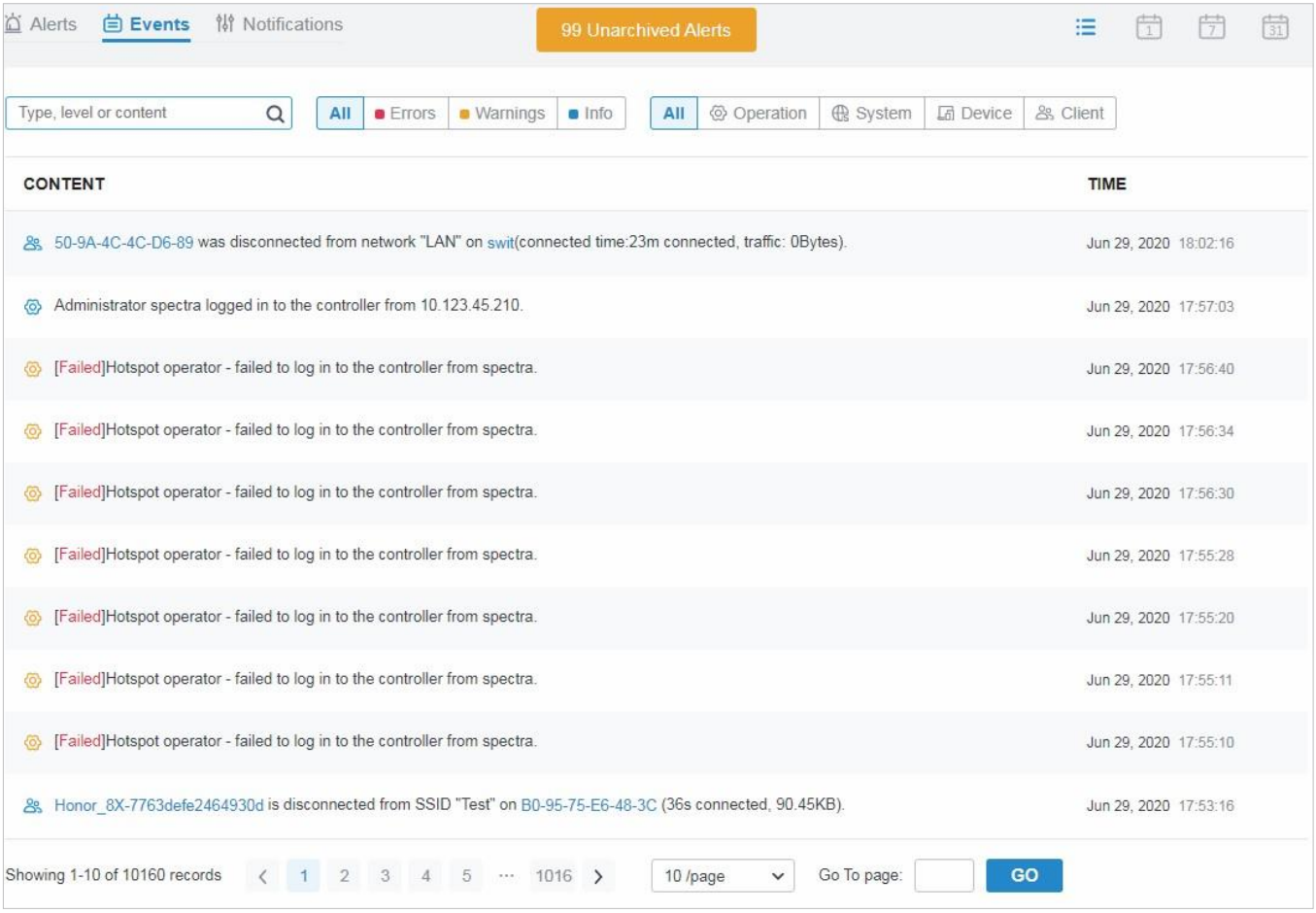
Content

Affiche les types de journaux et le message détaillé. Vous pouvez cliquer sur le nom de l'appareil, le nom du client pour ouvrir sa fenêtre Propriétés pour obtenir des informations détaillées.

Time	Affiche lorsque l'activité s'est produite.
Archive All	Cliquez pour archiver tous les journaux non archivés.
	Cliquez pour archiver l'entrée du journal.

8. 5. 2 Events

Les événements sont les journaux qui peuvent être consultés mais qui n'ont pas de notifications. Vous pouvez configurer les journaux en tant qu'événements dans notifications, et tous les journaux configurés comme Événements sont répertoriés sous l'onglet Événements pour que vous puissiez rechercher et filtrer.

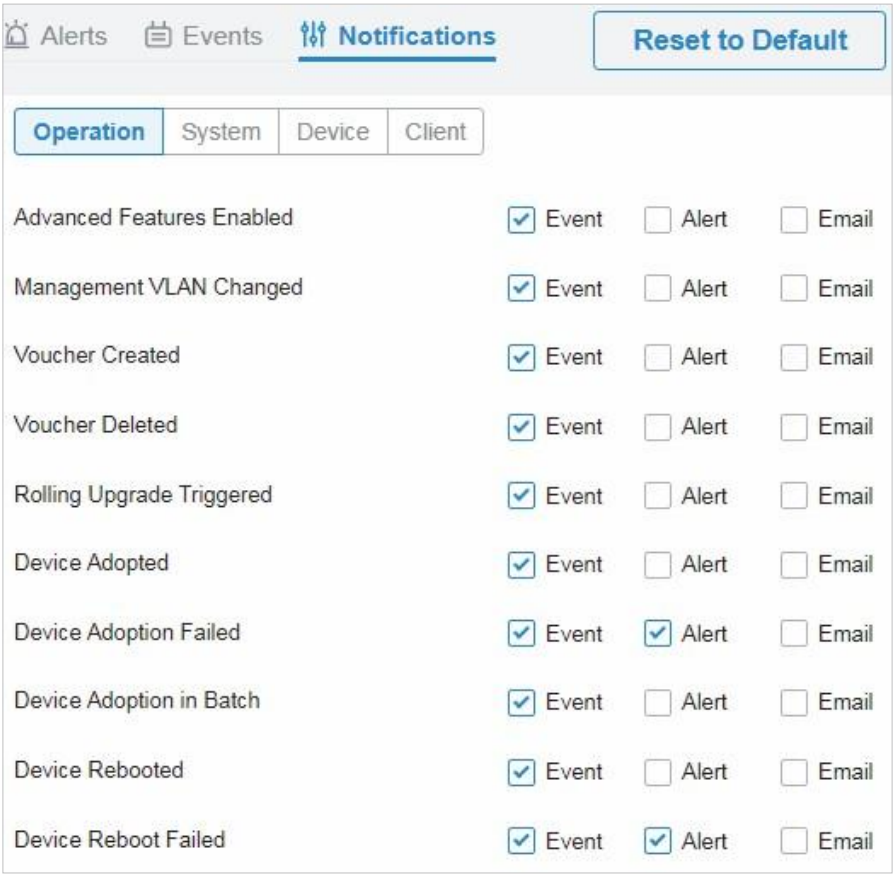


	Click to change the view mode. : Displays the logs in a table. / / :Affiche les journaux en un jour/semaine/mois. Pour modifier l'heure, cliquez s ou . pour revenir à l'état actuel, cliquez sur Today /This Week /This Month

	Entrez les types de contenu, les niveaux de gravité ou les mots clés pour rechercher les journaux.
	Cliquez sur les onglets pour filtrer les journaux répertoriés dans le tableau. Les deux onglets peuvent prendre effet simultanément. All/Errors/Warnings/Info: Cliquez sur All pour afficher les journaux dans les niveaux d'erreur et d'avertissement. Erreurs de clic, Warnings ou Info pour afficher les journaux dans le niveau correspondant uniquement. All/Operation/System/Device/Client: Click All to display all types of logs. Click Operation or System or Device or Client to display the corresponding type of logs only.
Content	Affiche les types de journaux et le message détaillé. Vous pouvez cliquer sur le nom de l'appareil, le nom du client pour ouvrir sa fenêtre Propriétés pour obtenir des informations détaillées.
Time	Affiche lorsque l'activité s'est produite.

8. 5. 3 Notifications

Dans Notifications, vous pouvez trouver toutes sortes de journaux d'activité classés par le contenu et spécifier leurs catégories de notifications en tant qu'événement et alerte pour le site actuel. En outre, vous pouvez activer e-mail pour les journaux. Avec les configurations appropriées, le contrôleur enverra des e-mails aux administrateurs lorsqu'il enregistre les journaux.



Pour spécifier les journaux comme Alerte/Événement, cliquez sur les cases à cocher correspondantes des journaux, puis sur Apply. Les icônes et onglets suivants sont fournis en tant qu'auxiliaires.

Reset to Default	Cliquez pour réinitialiser toutes les configurations de notification du site actuel à la valeur par défaut.
Operation System Device Client	Cliquez sur les onglets pour afficher les configurations des types de journaux correspondants.
Event Alert	Activez les cases à cocher pour spécifier les journaux d'activité en tant qu'événements/alertes, puis les journaux enregistrés s'afficheront sous l'onglet Événements/Alertes. Si les deux sont désactivés, le contrôleur n'enregistrera pas les journaux d'activité.
Email	Activez les cases à cocher pour spécifier les journaux d'activité en tant que journaux d'alerte. Avec les paramètres appropriés dans le site et l'administrateur, le contrôleur peut envoyer des e-mails pour informer les administrateurs et les téléspectateurs des journaux d'alerte du site une fois générés.
	Cette icône s'affiche lorsque la configuration d'un journal est modifiée mais n'a pas été appliquée. Cliquez dessus pour réinitialiser la configuration du journal à la valeur par défaut.

Les cases à cocher E-mail sont utilisées pour activer les e-mails d'alerte pour les journaux. Pour vous assurer que les administrateurs et les téléspectateurs peuvent recevoir des courriels d'alerte du site, procédez comme suit :

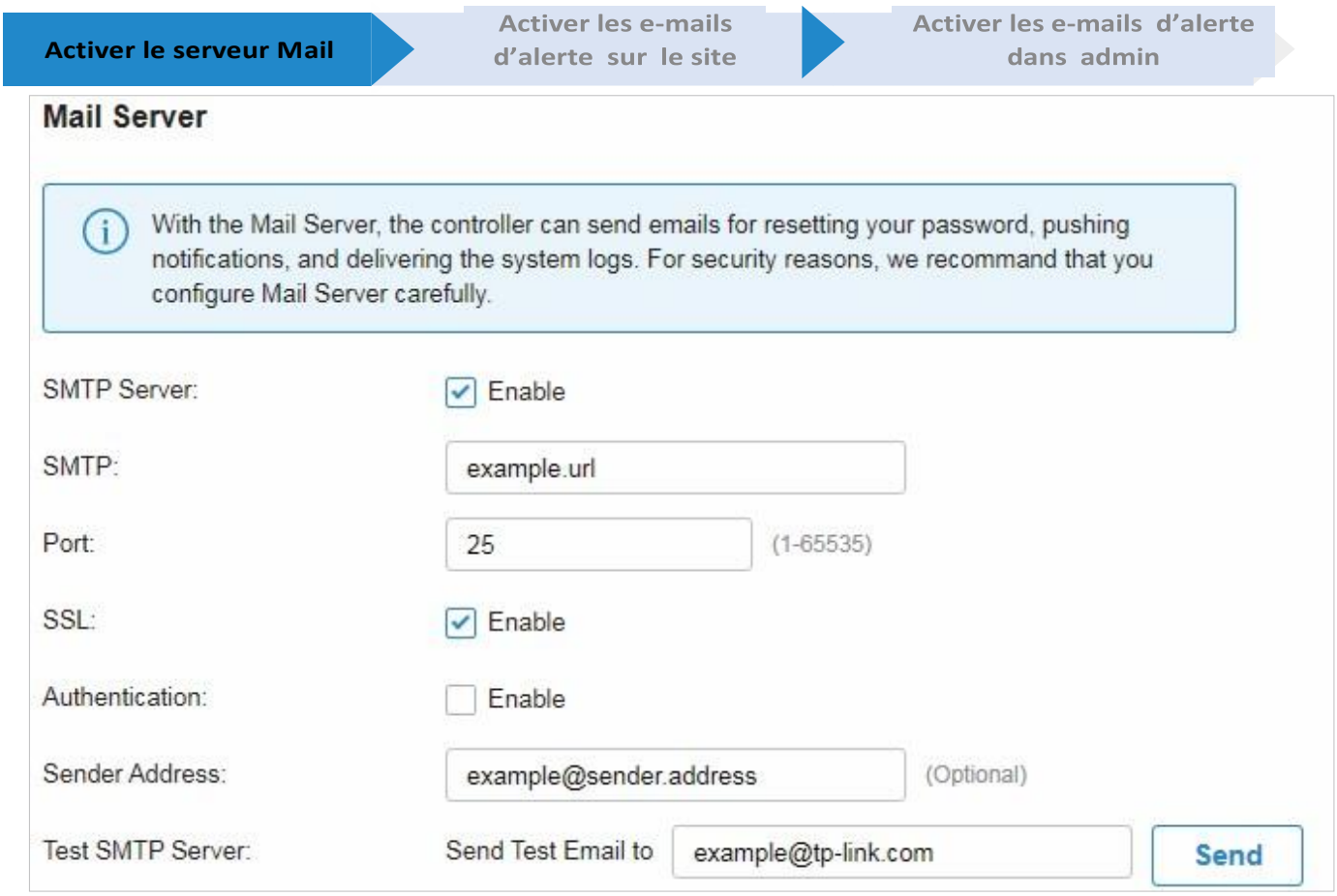
1.) Activer le serveur de messagerie

2.) Activer les e-mails d'alerte sur le site

3.) Activer les e-mails d'alerte dans admin

4.) Activer les e-mails d'alerte dans les journaux

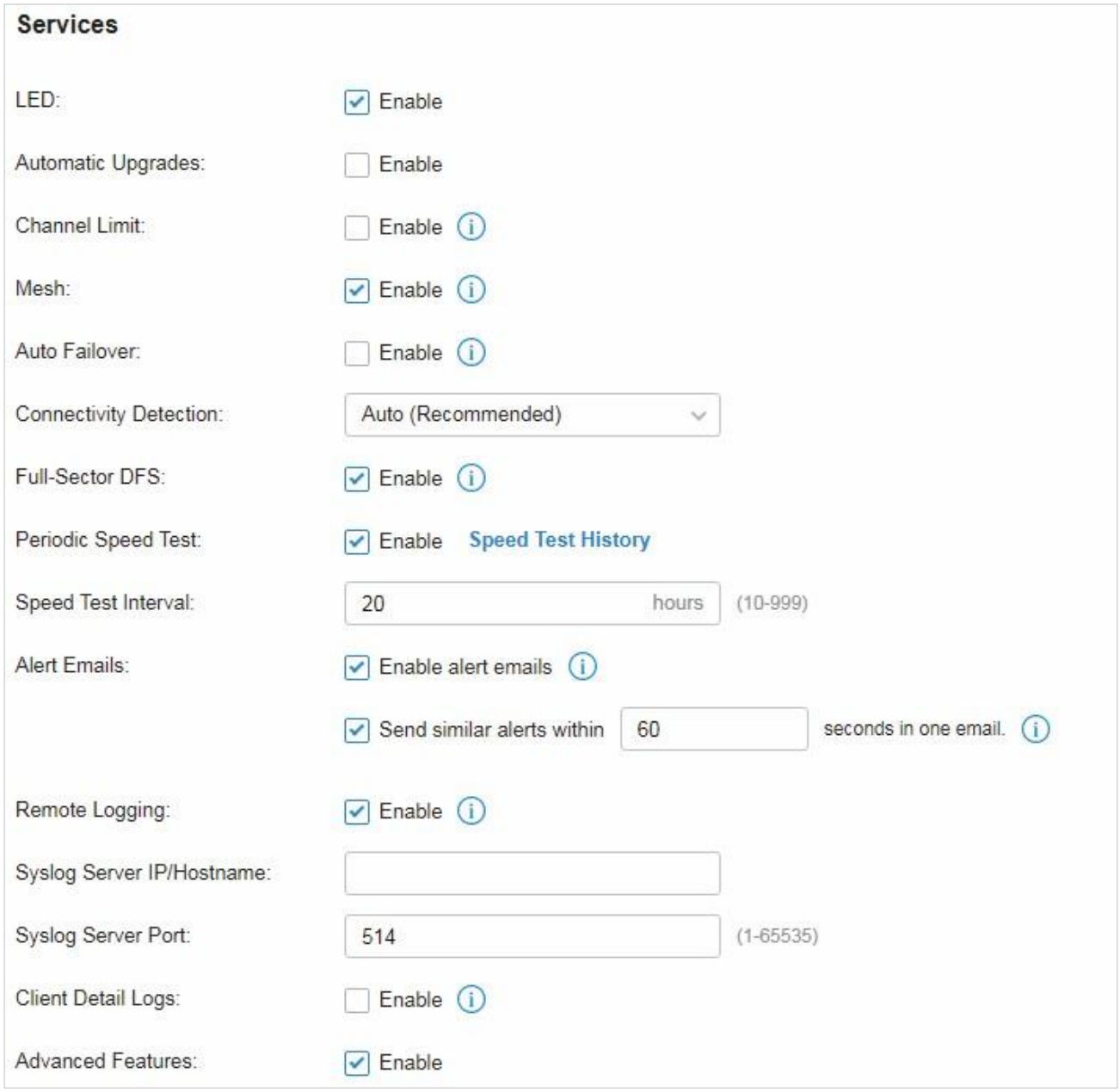
Allez dans Settings > Controller.et dans Mail Server activez SMTP Server et configurez les paramètres. Cliquez ensuite sur Save. **Enable Mail Server**



SMTP	Entrez l'URL ou l'adresse IP du serveur SMTP selon les instructions du fournisseur de services de messagerie.
Port	Configurer le port utilisé par le serveur SMTP selon les instructions du fournisseur de services de messagerie.
SSL	Activez ou désactivez SSL selon les instructions du fournisseur de services de messagerie. SSL (Secure Sockets Layer) est utilisé pour créer un lien chiffré entre le contrôleur et le serveur SMTP.
Authentication	Activer ou désactiver l'authentification selon les instructions du fournisseur de services de messagerie. Si l'authentification est activée, le serveur SMTP nécessite le nom d'utilisateur et le mot de passe pour l'authentification.
Username	Entrez le nom d'utilisateur de votre compte de messagerie si l'authentification est activée.

Password	Enter the password for your email account if Authentication is enabled.
Sender Address	(Optional) Specify the sender address of the email.
Test SMTP Server	Test the Mail Server configuration by sending a test email to an email address that you specify.

Allez dans Settings > Site et activer les e-mails d'alerte dans la section Services.

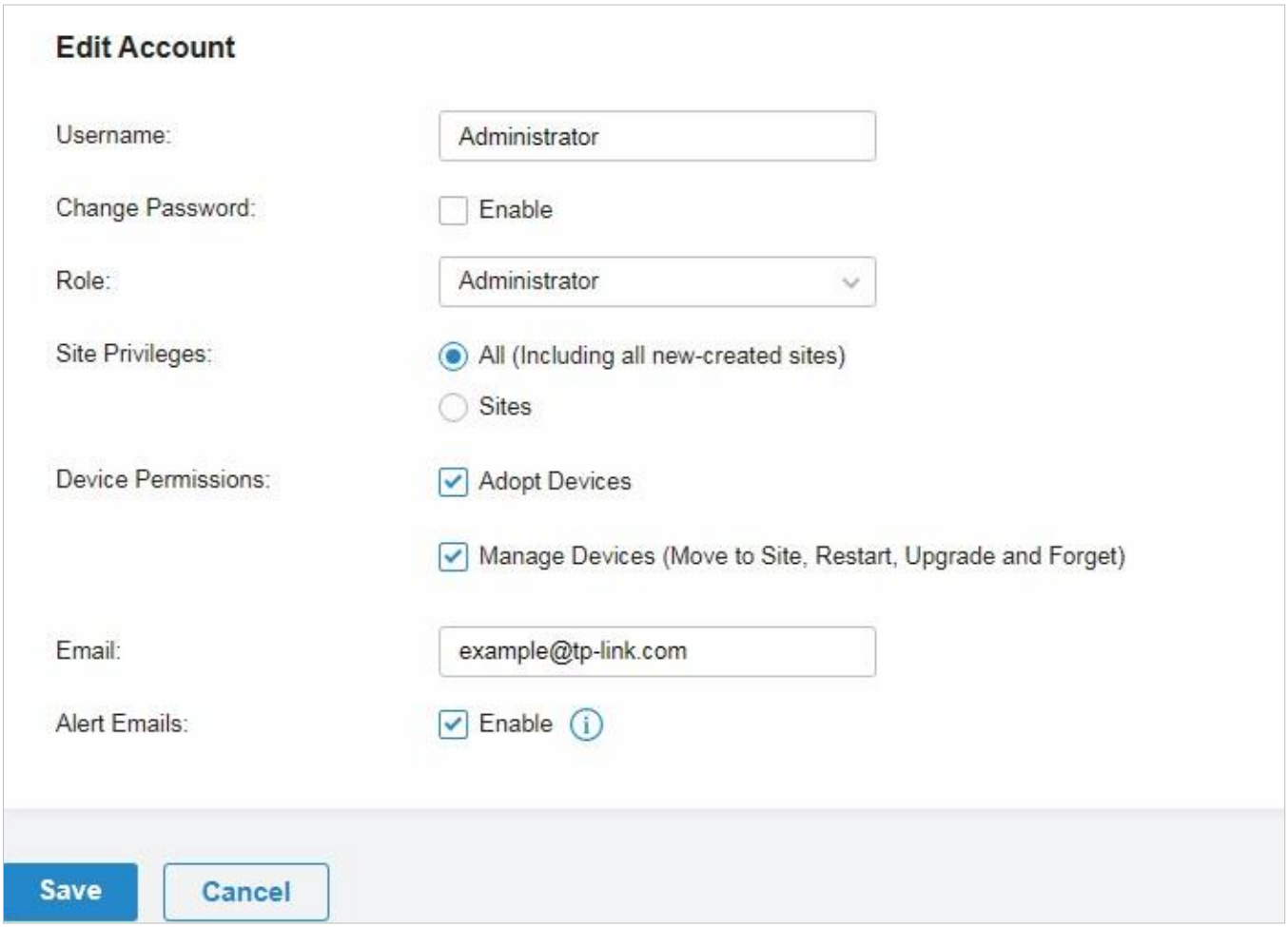


1. (Optional) On the same page, enable Send similar alerts within seconds in one email et spécifiez l'intervalle de temps. Lorsqu'elles sont activées, les alertes similaires générées à chaque période sont collectées et envoyées aux administrateurs et aux téléspectateurs dans un seul e-mail.



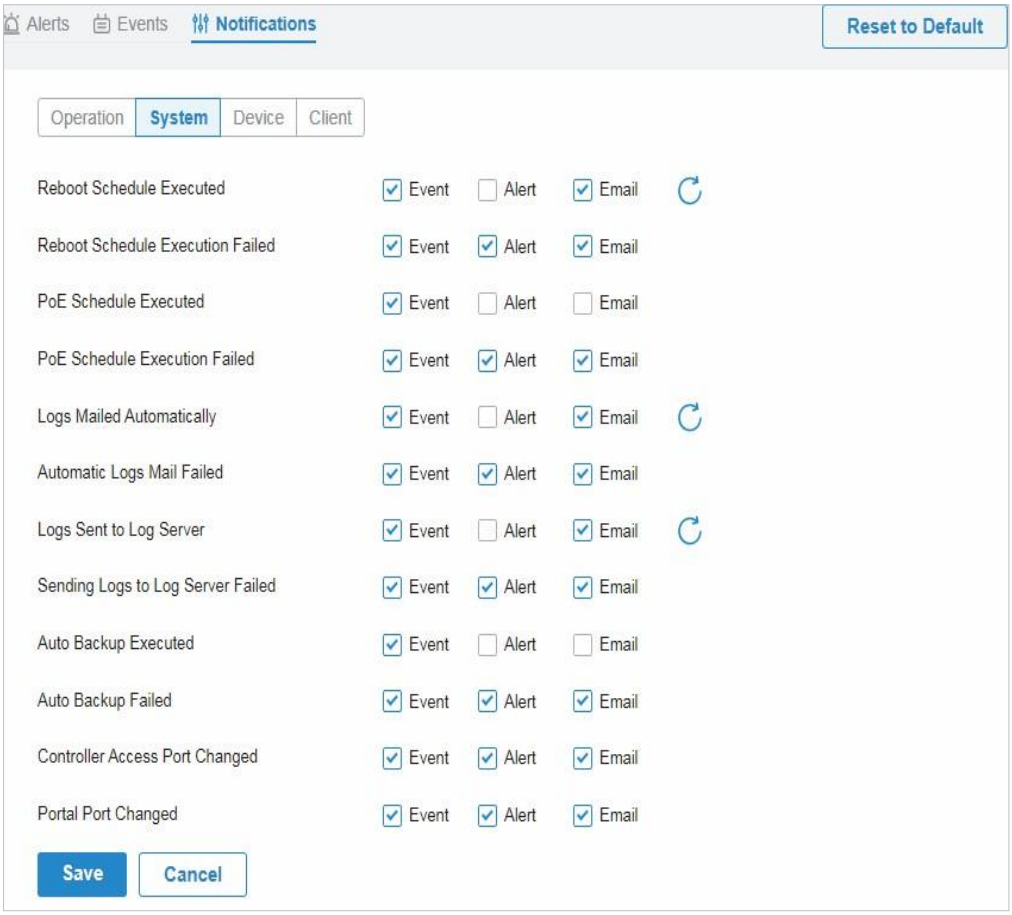
Cliquez sur Apply.

Accédez à Admin et configurez les e-mails d'alerte pour que les administrateurs et les téléspectateurs reçoivent les e-mails. Cliquez sur + Add New Admin Account Pour créer un compte ou cliquez sur Entrez l'adresse e-mail Dans Email et activer Alert Emails. Cliquez sur Create. ou Apply



Activer les e-mails d'aler sur le site > Activer les e-mails d'alerte dans admin > Activer les emails d'alerte dans les journaux

Go to Logs and click Notifications. Click a tab of content types and enable Email for the activity logs that the controller emails administrators. Click Save.



9

Gérer les comptes d’administrateur du contrôleur SDN Omada

Ce chapitre donne une introduction aux différents niveaux d’utilisateur des comptes d’administrateur et vous guide sur la façon de les créer et de les gérer dans la page Administrateur. Le chapitre comprend les sections suivantes :

- Introduction aux comptes d’utilisateurs
- Gérer et créer des comptes d’utilisateurs locaux
- Gérer et créer des comptes utilisateur cloud

9. 1 Introduction aux comptes d'utilisateurs

Le contrôleur SDN d'Omada offre trois niveaux d'accès disponibles pour les utilisateurs : administrateur principal, administrateur et visionneuse. Étant donné que le contrôleur peut être consulté à la fois localement et via l'accès au cloud, les utilisateurs peuvent être regroupés davantage dans les utilisateurs locaux et les utilisateurs de cloud. Le compte administratif à plusieurs niveaux présente une hiérarchie d'autorisations pour différents niveaux d'accès au contrôleur au besoin. Cette approche assure la sécurité et donne de la commodité pour la gestion.

- **Master Administrator**

Il n'y a qu'un seul administrateur principal qui a accès à toutes les fonctionnalités. Le compte qui lance le contrôleur sera l'administrateur principal et ne peut pas être modifié et supprimé.

- **Administrator**

Les administrateurs peuvent créer et supprimer des utilisateurs dans la page Administrateur, mais ils peuvent être créés et supprimés uniquement par l'administrateur principal. Dans la page Paramètres, les administrateurs n'ont pas l'autorisation de certains modules, y compris l'accès au cloud, la migration, la sauvegarde automatique, etc.

- **Viewer**

Les utilisateurs ne peuvent afficher que l'état et les paramètres du réseau, et ils ne peuvent pas modifier les paramètres. L'entrée de la page Admin est masquée pour les téléspectateurs, et ils peuvent être créés ou supprimés par l'administrateur principal et l'administrateur.

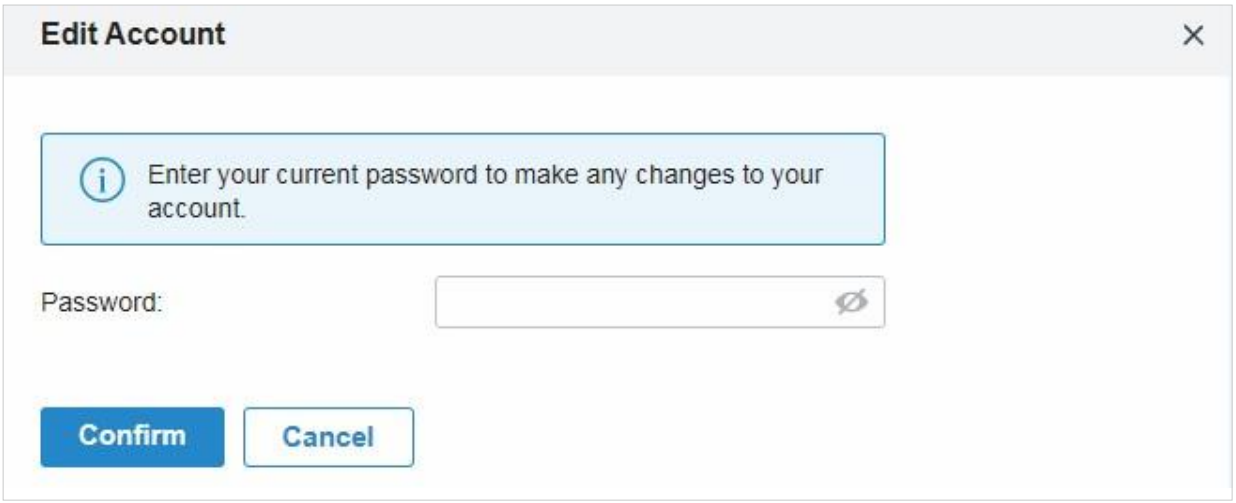
9. 2 Gérer et créer des comptes d'utilisateurs locaux

Par défaut, le contrôleur SDN Omada définit automatiquement un utilisateur local avec le rôle appelé administrateur principal en tant qu'administrateur principal. Le nom d'utilisateur et le mot de passe de l'administrateur principal sont les mêmes que ceux du compte contrôleur par défaut. L'administrateur maître ne peut pas être supprimé et il peut créer, modifier et supprimer d'autres niveaux de comptes d'utilisateurs.

9. 2. 1 Modifier le compte d'administrateur principal

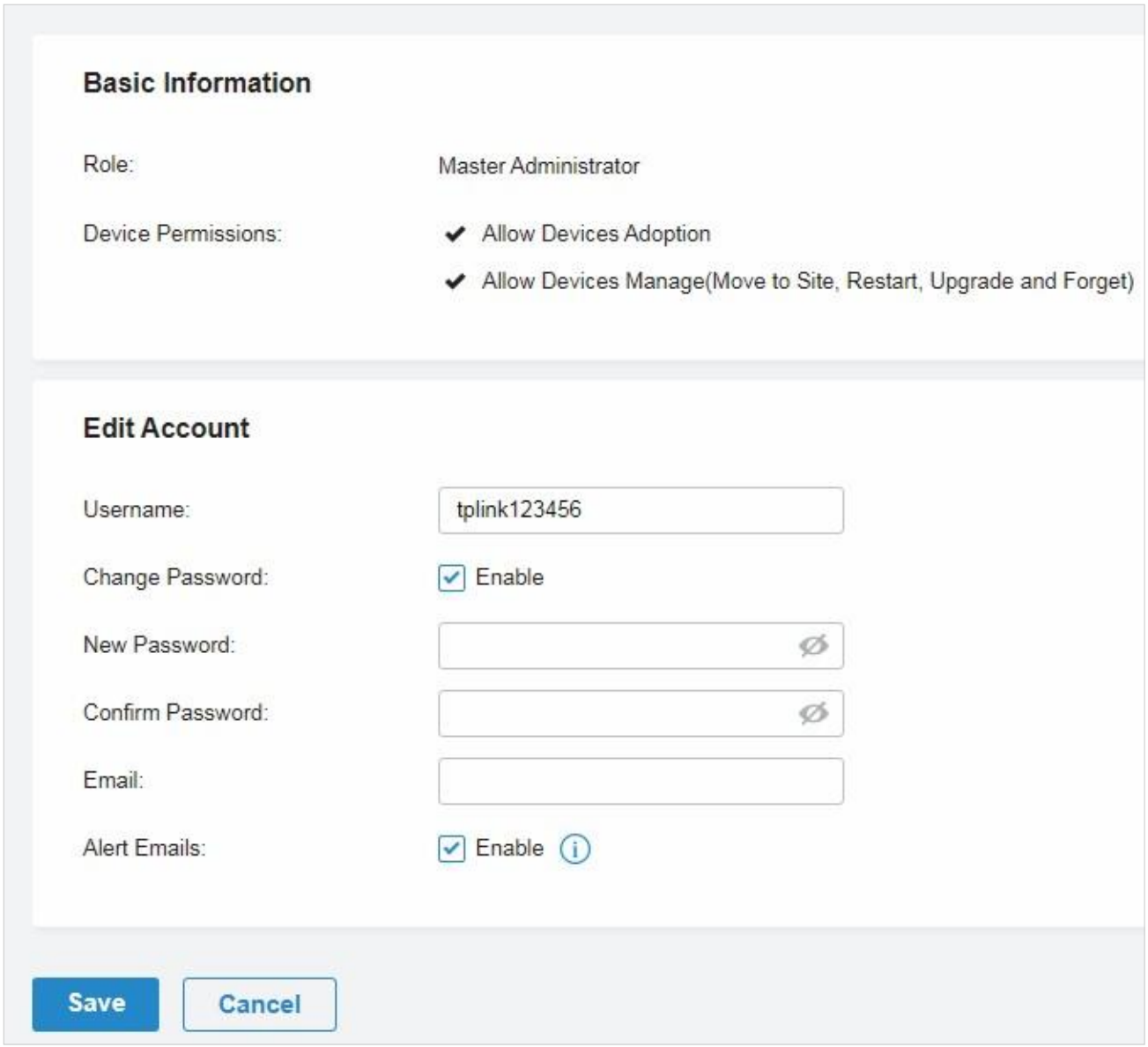
Pour afficher les informations de base et modifier le compte d'administrateur principal, procédez comme

Allez dans Admin, cliquez sur dans la colonne Action. Entrez le mot de passe et cliquez sur Confirm (Par defaut,mot de passe de l'administrateur principal est le même que le compte de contrôleur).



1.

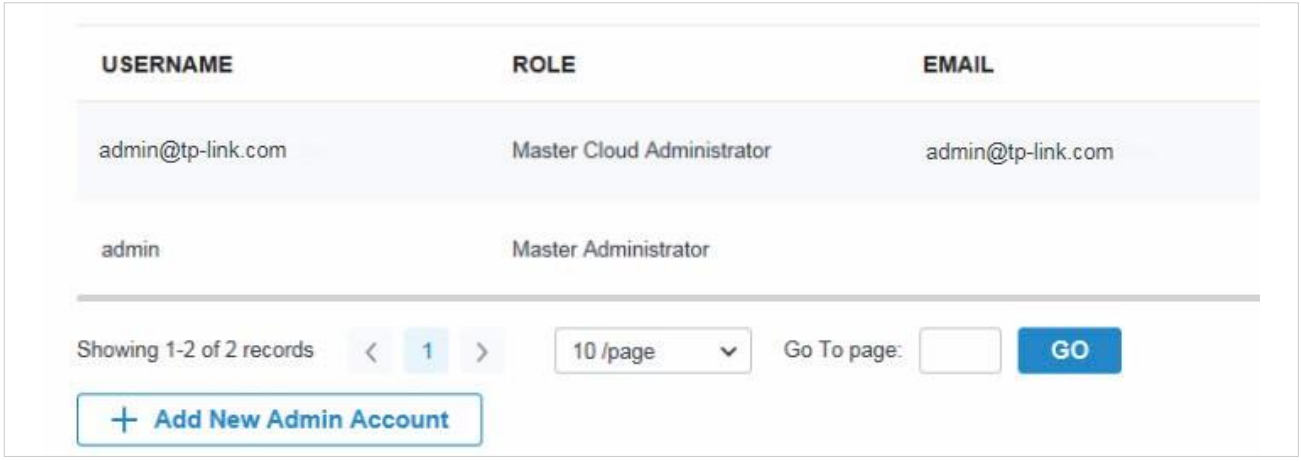
2. Les informations de base, y compris les autorisations de rôle et de périphérique, s'affichent. Vous pouvez modifier le mot de passe et activer les e-mails d'alerte en cochant la case. Cliquez sur Save.



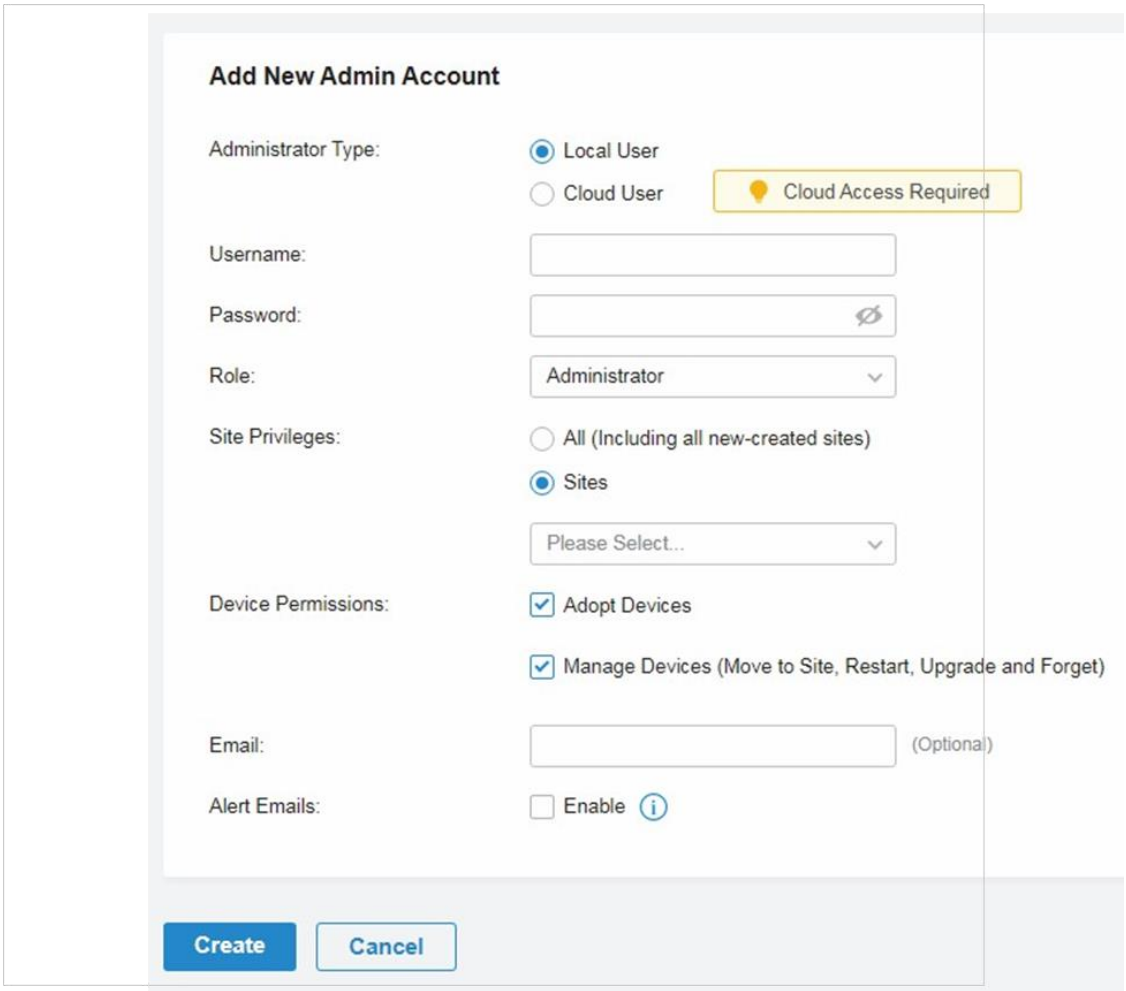
9. 2. 2 Créer et gérer l'administrateur et le visionneur

Pour créer et gérer un compte d'utilisateur local, procédez comme suit :

1. Cliquez sur + Add New Admin Account.



2. Sélectionnez Utilisateur local pour le type d'administrateur dans la fenêtre contextuelle.



3. Personnalisez les paramètres et cliquez sur Create.

Username	Spécifiez le nom d'utilisateur. Le nom d'utilisateur doit être différent des noms existants.
Password	Spécifier le mot de passe.
Role	Sélectionner un rôle pour le compte d'utilisateur créé. Administrator: Ce rôle a l'autorisation d'adopter et/ou de gérer les périphériques des sites choisis dans les privilèges du site, de se modifier, de créer/modifier/supprimer des comptes de visionneuse dans ses sites privilégiés. Toutefois, il ne peut pas se supprimer ou modifier/supprimer l'administrateur principal et d'autres comptes d'administrateur. Viewer: Ce rôle peut afficher les informations des sites choisis dans les privilèges du site. Il ne peut que se modifier.
Site Privileges	Affectez les autorisations de site à l'utilisateur local créé. All: L'utilisateur créé dispose d'autorisations de périphérique dans tous les sites, y compris tous les sites créés. Sites: L'utilisateur créé dispose de l'autorisation de périphérique dans les sites sélectionnés. Sélectionnez les sites en cochant la case avant eux.
Device Permissions (when creating a local administrator)	Accorder l'autorisation suivante à l'utilisateur créé dans le rôle d'administrateur en cochant la case(es). Adopt Devices: Le compte d'administrateur créé peut afficher les périphériques en instance dans les sites privilégiés, et le compte d'administrateur a les autorisations d'adopter les périphériques. Device Manage: le compte d'administrateur créé peut gérer les périphériques dans les sites privilégiés.
Email (optional)	Entrez une adresse e-mail pour recevoir des e-mails d'alerte.
Alert Emails	Cochez la case si vous souhaitez que l'utilisateur créé reçoive des courriels concernant les alertes des sites privilégiés. Pour des configurations détaillées, reportez-vous aux Services.

Pour modifier et supprimer les comptes, cliquez sur icônes dans la colonne Action.

	Pour modifier les paramètres de l'utilisateur. L'administrateur principal peut modifier tous les comptes d'utilisateurs, l'Administrateur peut modifier lui-même et visionner les comptes de ses sites privilégiés, et le spectateur ne peut se modifier que lui-même.
	Pour supprimer le compte. L'administrateur principal peut supprimer tous les comptes d'utilisateurs en dehors de lui-même, l'administrateur peut supprimer les comptes de visionneuse de ses sites privilégiés, et le visionneur ne peut supprimer aucun compte.

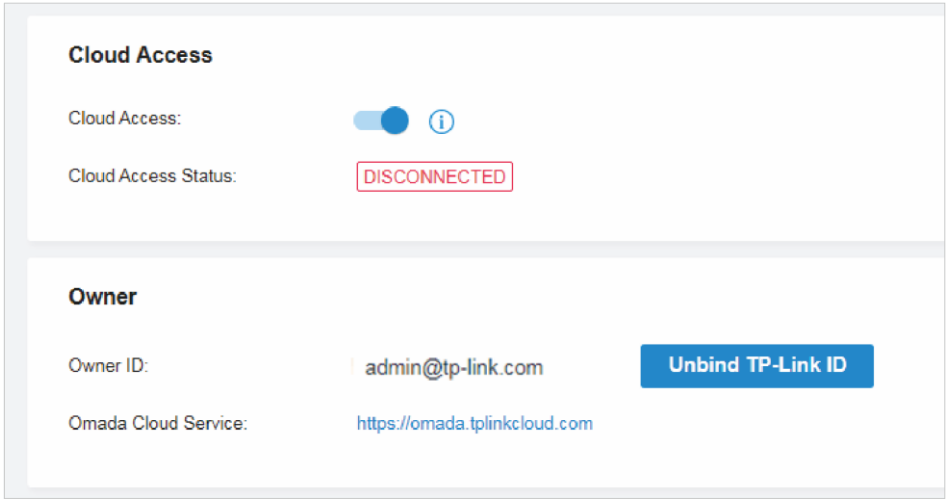
9. 3 Gérer et créer des comptes utilisateur cloud

Pour le contrôleur cloud, l'accès au cloud est activé par défaut et le contrôleur définit automatiquement l'administrateur principal du cloud. Le contrôleur logiciel et matériel configure automatiquement l'administrateur principal cloud si vous avez activé l'accès au cloud et lié le compte contrôleur avec un ID TP-Link dans la configuration rapide. Le nom d'utilisateur et le mot de passe sont les mêmes que ceux de l'ID TP-Link. L'administrateur maître cloud ne peut pas être supprimé et il peut créer, modifier et supprimer d'autres niveaux de comptes d'utilisateurs.

9. 3. 1 Configurer l'administrateur maître cloud

Pour le contrôleur logiciel et matériel, si vous n'avez pas activé l'accès au cloud et lié le contrôleur avec un ID TP-Link en configuration rapide, pour configurer l'administrateur principal du cloud, procédez comme suit :

1. Allez dans Settings > Cloud Access pour activer l'accès au cloud et lier votre ID TP-Link.

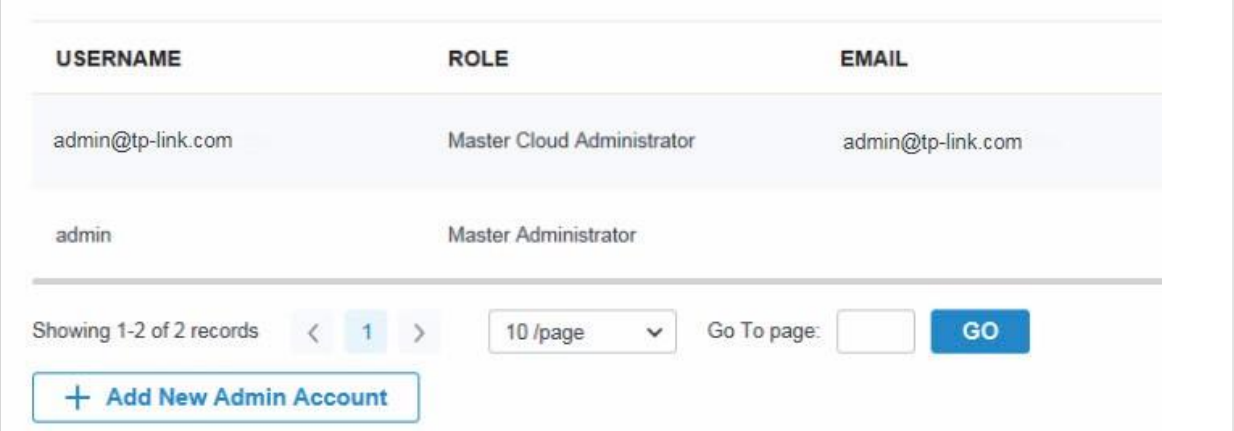


2. Dans Admin, un administrateur maître cloud ayant le même nom d'utilisateur que l'ID TP-Link sera automatiquement créé. Impossible de supprimer l'administrateur principal du cloud. Vous pouvez vous connecter avec l'administrateur maître cloud lorsque l'accès au cloud est activé.

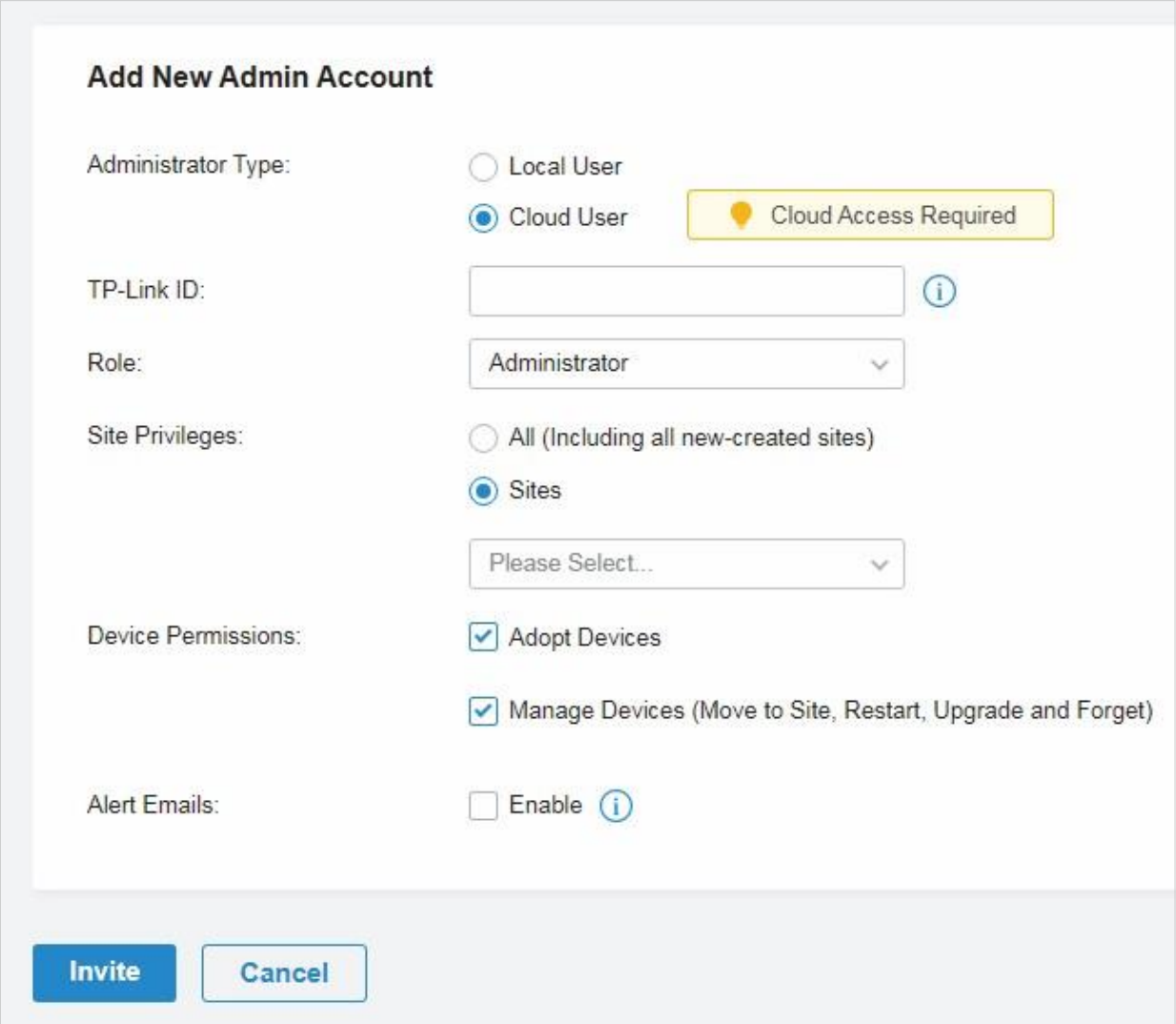
9. 3. 2 Créer et gérer l'administrateur cloud et l'observateur de cloud

Pour créer et gérer le compte d'utilisateur cloud, procédez comme suit:

1. Cliquez sur + Add New Admin Account.



2. Sélectionnez Cloud User pour l'administrateur, tapez la fenêtre contextuelle. Spécifier les paramètres et click Invite.



TP-Link ID	Entrez une adresse e-mail de l'utilisateur du cloud créé, puis un e-mail d'invitation sera envoyé à l'adresse e-mail. Si l'adresse e-mail a déjà été enregistrée en tant qu'ID TP-Link, elle deviendra un utilisateur cloud valide après avoir accepté l'invitation. Si l'adresse e-mail n'a pas été enregistrée, elle recevra un courriel d'invitation pour l'inscription. Après avoir terminé l'inscription, il deviendra automatiquement un utilisateur de cloud valide
Role	Sélectionnez un rôle pour l'utilisateur de cloud créé. Administrator: Ce rôle a l'autorisation d'adopter et/ou de gérer les périphériques des sites choisis dans les privilèges du site, de se modifier, de créer/modifier/supprimer des comptes de visionneuse dans ses sites privilégiés. Toutefois, il ne peut pas se supprimer ou modifier/supprimer l'administrateur principal et d'autres comptes d'administrateur. Viewer: Ce rôle peut afficher les informations des sites choisis dans les privilèges du site. Il ne peut que se modifier.
Site Privileges	Attribuez l'autorisation de site à l'utilisateur de cloud créé. All: L'utilisateur créé dispose d'une autorisation dans tous les sites, y compris tous les sites créés par les nouveaux. Sites: L'utilisateur créé dispose d'une autorisation dans les sites sélectionnés. Sélectionnez les sites en cochant la case devant eux.
Device Permissions (when creating a cloud administrator)	Accorder l'autorisation suivante à l'utilisateur créé dans le rôle de l'administrateur cloud en cochant la(es) case(es). Adopt Devices: Le compte d'administrateur créé peut afficher les périphériques en instance dans les sites privilégiés, et le compte d'administrateur a la permission d'adopter les périphériques. Device Manage: Le compte d'administrateur créé a des privilèges pour gérer les périphériques dans les sites privilégiés.
Alert Emails	Cochez la case si vous souhaitez que l'utilisateur créé reçoive des courriels concernant les alertes des sites privilégiés. Pour les configurations détaillées, reportez-vous à Services

L'administrateur maître du cloud peut modifier tous les comptes d'utilisateurs, l'administrateur peut modifier et supprimer les comptes, cliquez sur icônes dans la colonne Action

 Pour modifier les paramètres de l'utilisateur.

L'administrateur maître du cloud peut modifier modifier lui-même et visionner les comptes de ses sites privilégiés, le spectateur ne peut se modifier que.

 Pour supprimer le compte.

L'administrateur maître du cloud peut supprimer tous les comptes d'utilisateurs en dehors de l'administrateur maître et lui-même, l'administrateur peut supprimer les comptes de visionneuse de ses sites privilégiés, visionneuse ne peut pas supprimer de comptes.

DROITS D’AUTEUR ET MARQUES DE COMMERCE

Les spécifications peuvent être modifiées sans préavis est une marque déposée de TP-Link Technologies Co., Ltd. D’autres marques et noms de produits sont des marques de commerce ou des marques déposées de leurs titulaires respectifs.

Aucune partie des spécifications ne peut être reproduite sous quelque forme que ce soit, ni par quelque moyen que ce soit, ni utilisée pour fabriquer des dérivés tels que la traduction, la transformation ou l’adaptation sans l’autorisation de TP-Link Technologies Co., Ltd.

Copyright © 2020 TP-Link Technologies Co., Ltd. Tous droits réservés.