Guide de l’utilisateur

Contrôleur cloud Omada

OC200

Guide d’installation en Français REV1.2.0

Aout 2020

1 Démarrage rapide

Le contrôleur cloud Omada (OC200), préinstallé avec le contrôleur logiciel Omada, peut gérer de manière centralisée plusieurs EAP tout comme le contrôleur logiciel Omada. La différence est que le contrôleur de logiciel Omada doit s'exécuter dans un hôte de gestion, ce qui n'est pas nécessaire pour l'OC200. Vous n'avez qu'à déployer un OC200 dans le réseau et le maintenir en cours d'exécution, puis vous pouvez configurer les EAP par lots et effectuer une surveillance en temps réel des EAP localement ou à distance via le service Omada Cloud.

Suivez les étapes ci-dessous pour compléter les paramètres de base d'OC200.

1. Déployer l'OC200
2. Déterminer la méthode de gestion
3. Informer les EAP de l'adresse de l'OC200
4. Connectez-vous à l'OC200
5. Créer des sites et adopter les EAP
6. Surveiller et gérer les EAP

1.1 Déployer l'OC200

Il existe deux types de topologies réseau qui conviennent au déploiement OC200 :

■ Les OC200 et les EAP sont dans le même sous-réseau.

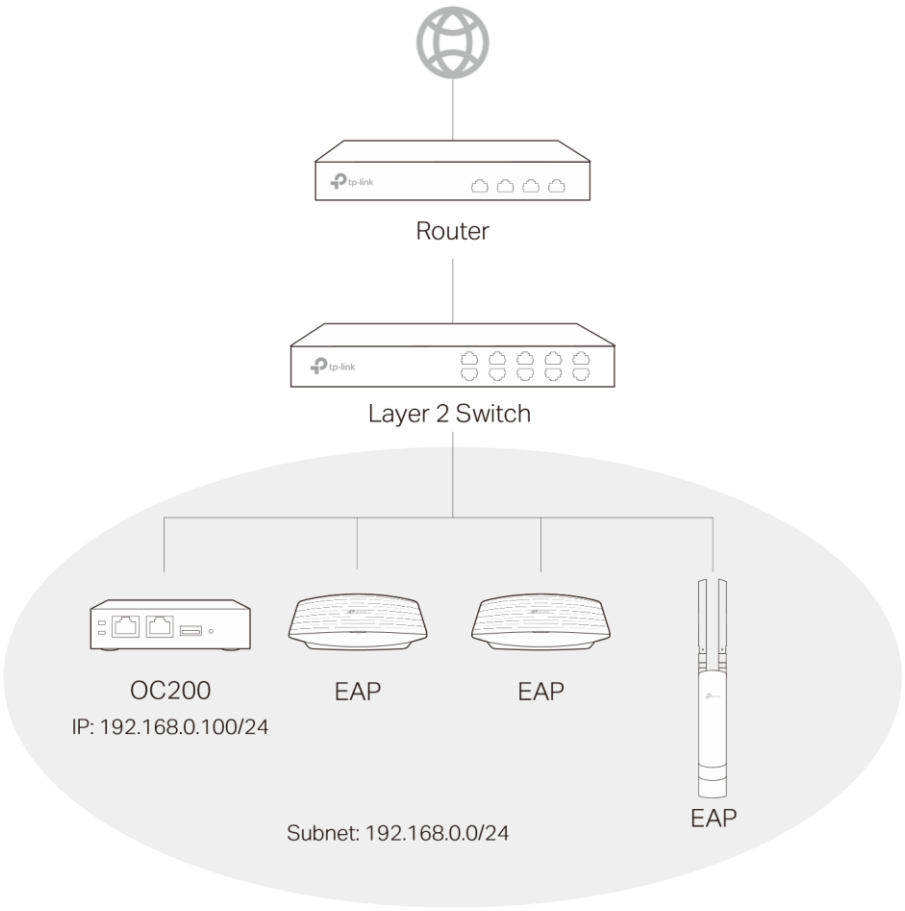
■ Les OC200 et les EAP sont dans différents sous-réseaux.

Déterminez votre topologie en fonction de vos besoins et reportez-vous aux introductions suivantes pour créer votre topologie réseau.

1.1.1 Déployer les OC200 et les EAP dans le même sous-réseau

Si vous devez déployer les PROTOCOLES OC200 et EA dans le même sous-réseau, reportez-vous à la topologie réseau suivante.

Un routeur agit en tant que serveur DHCP pour affecter des adresses IP aux EAP, aux clients et à OC200. L'OC200 et les EAP se trouvent dans le même sous-réseau.

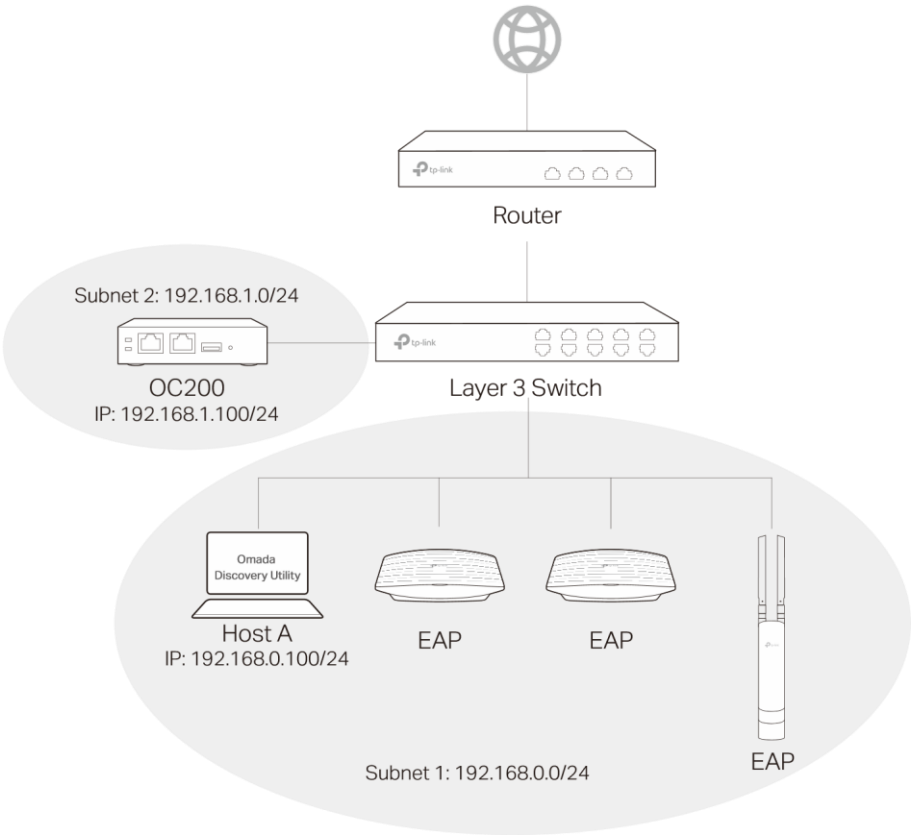


1.1.2 Déployer les OC200 et les EAP dans différents sous-réseaux

Si vous devez déployer les PROTOCOLES OC200 et EAP dans différents sous-réseaux, reportez-vous à la topologie réseau suivante.

Un routeur agit comme la passerelle du réseau. Un commutateur Layer 3 agit comme un serveur DHCP pour affecter des adresses IP aux EAP, OC200 et aux clients. Les EAP sont dans le sous-groupe 1, dont le segment du réseau IP est de **192.168.0.0/24** ; l'OC200 se trouve dans le sous-réseau 2, dont le segment de réseau IP est **192.168.1.0/24.**

Étant donné que les EAP et l'OC200 se trouvent dans le segment de réseau différent, les EAP ne peuvent pas trouver directement l'OC200. Pour aider les EAP à trouver l'OC200, vous devez installer un utilitaire Omada Discover sur un hôte qui se trouve dans le même sous-réseau avec les EAP. Pour savoir comment utiliser Omada Discovery Utility, reportez-vous aux EAP de l'adresse de l'OC200.



1.2 Déterminer la méthode de gestion

OC200 prend en charge deux méthodes de gestion flexibles pour gérer de façon centralisée les EAP :

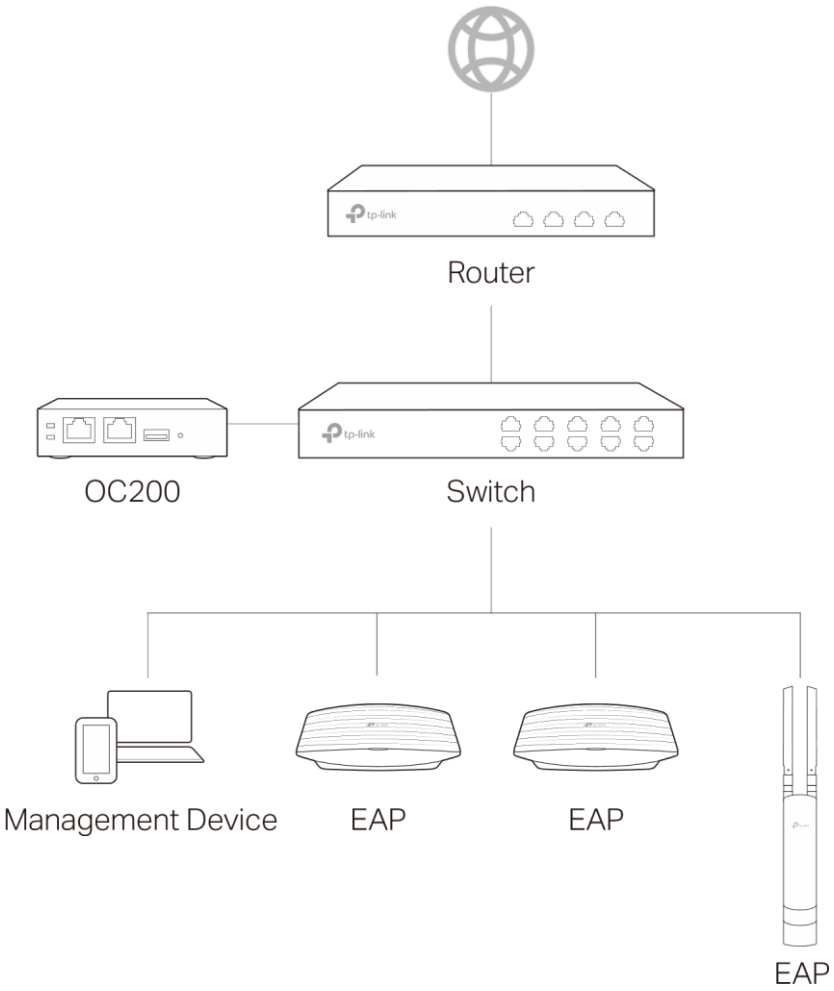
■ Gestion sur le réseau local

■ Gestion via Cloud Access

Déterminez votre méthode de gestion en fonction de vos besoins et reportez-vous aux introductions suivantes pour créer votre topologie réseau

1.2.1 Gestion du réseau local

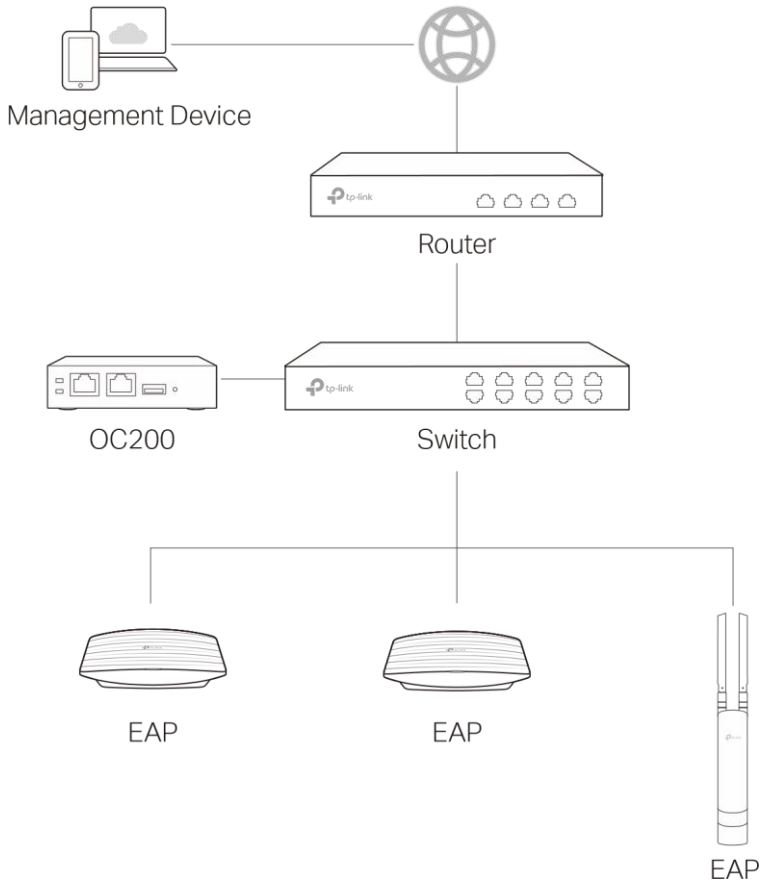
Pour lancer l'OC200 localement, déployez votre périphérique de gestion sur le réseau local. La topologie suivante est un exemple pour le déploiement du périphérique de gestion. Tant qu'il existe un itinéraire permettant au périphérique de gestion d'accéder à l'OC200, le périphérique de gestion peut se connecter à l'OC200 pour gérer les EAP. Pour savoir comment vous connecter à l'OC200, veuillez consulter Le réseau local.



1.2.2 Gestion via Cloud Access

Si vous devez vous connecter à l'OC200 à distance, par exemple, vos EAP et OC200 sont dans votre bureau mais vous souhaitez les gérer à la maison, vous pouvez lancer l'OC200 pour gérer les EAP via Cloud Access.

La topologie suivante est un exemple typique. Vous n'avez qu'à déployer vos OC200 et EAP sur votre réseau local et utiliser un périphérique de gestion pour les contrôler à distance. Sur le périphérique de gestion, vous pouvez ouvrir un navigateur Web pour lancer à distance l'OC200 via Omada Cloud. Pour plus de détails sur Cloud Access, reportez-vous à Omada Cloud Service.



1.3 Informer les EAP de l’adresse de l’OC200

Si vos OC200 et vos EAP se trouvent dans le même sous-réseau réseau, vous pouvez ignorer cette section.

Si vos OC200 et EAP se trouvent dans des sous-réseaux différents, vous devez installer Omada Discovery Utility sur un hôte qui se trouve dans le même segment réseau avec les EAP. Omada Discovery Utility peut aider les FAI à trouver l’OC200.

Exigences du système

Windows 7/8/10/Server

Mac OS X 10.7/10.8/10.9/10.10/10.11

Installer et utiliser l’utilitaire de découverte Omada

Suivez les étapes ci-dessous pour installer Omada Discovery Utility et utilisez-le pour informer les EAP de l’adresse IP de l’OC200 :

Suivez les étapes ci-dessous pour installer Omada Discovery Utility et utilisez-le pour informer les EAP de l’adresse IP de l’hôte contrôleur :

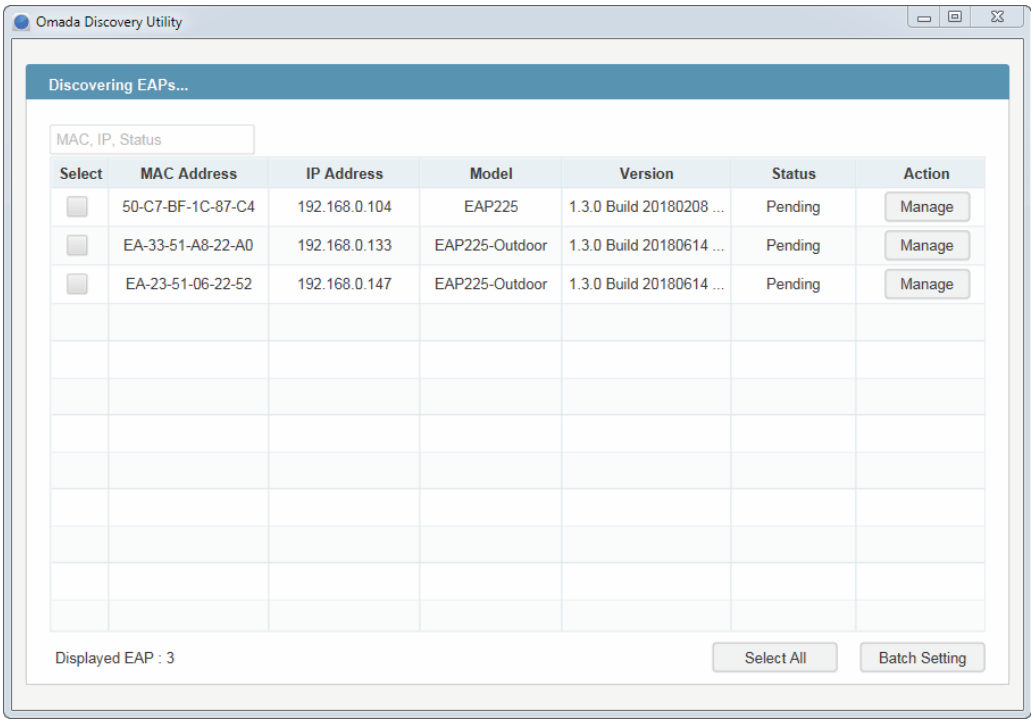
1. Téléchargez le fichier d’installation avec la dernière version du site

   https://www.tp-link.com/en/download/EAP-Controller.html#EAP_Discovery_Tool

2. Assurez-vous d'avoir JRE (Java Runtime Environment) avec la version 1.8 installée sur votre système avant l'installation. Si votre système perd JRE, téléchargez JRE à partir du site https://www.oracle.com/technetwork/java/javase/downloads/jre8-downloads-213315.html

3. et installez-le sur votre système.

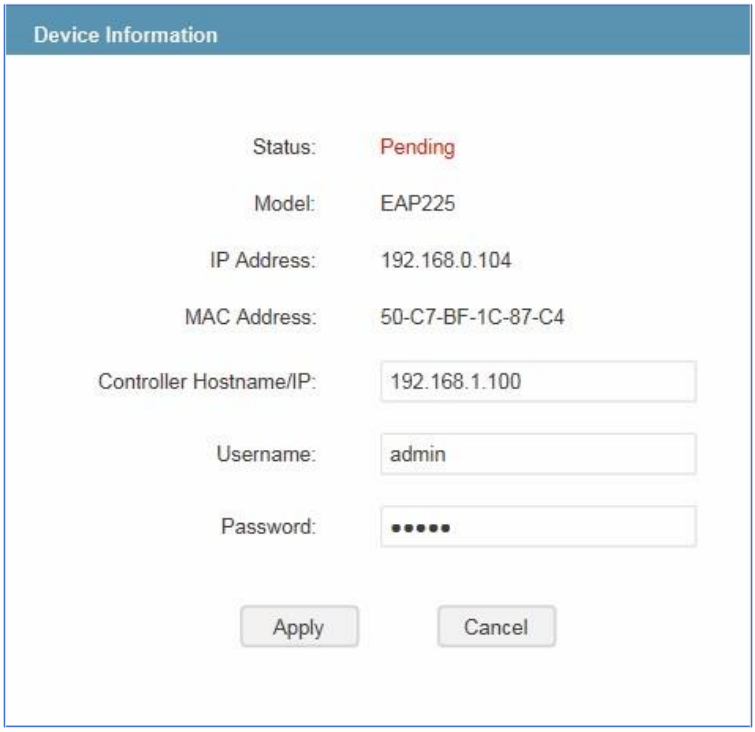
4. Pour Windows OS, exécutez le start-omada-discovery-utility.bat pour ouvrir l'utilitaire de découverte Omada. Pour Mac OS, utilisez la commande java –jar ** pour ouvrir l'utilitaire de découverte Omada. Ensuite, la fenêtre suivante apparaîtra. Cette fenêtre affiche les informations de tous les EAP dans le même réseau local.



5. Cliquez sur Gérer dans la colonne Action ou sélectionnez plusieurs EAP, puis cliquez sur Paramètre par lots.

6. Entrez le nom d'hôte ou l'adresse IP de l'OC200.

7. Entrez le nom d'utilisateur et le mot de passe du EAP (les deux sont admin par défaut).



8. Cliquez sur Appliquer pour informer le EAP du nom d'hôte ou de l'adresse IP de l'OC200. Ensuite, la connexion peut être établie entre le EAP et l'OC200.

1.4 Connectez-vous à l'OC200

Pour utiliser l'OC200 pour gérer les EAP, vous devez d'abord vous connecter à l'OC200. Il y a deux situations :

■ Connectez-vous à l'OC200 sur le réseau local

■ Connectez-vous à l'OC200 via Omada Cloud

Conseils :

L'application Omada offre un moyen pratique d'accéder à l'OC200 et d'adopter des EAP. Avec la fonction Accès local et accès au cloud sur l'application Omada, vous pouvez gérer l'OC200 sur les sites locaux et distants. Pour plus d'informations sur l'application Omada, reportez-vous à l'annexe : Omada App.

1.4.1 Sur le réseau local

Suivez les étapes ci-dessous pour entrer l'interface de gestion d'OC200 sur le réseau local :

1. Assurez-vous que votre périphérique de gestion dispose de l'itinéraire pour accéder à l'OC200.
2. Vérifiez le serveur DHCP (généralement un routeur) pour l'adresse IP d'OC200. L'adresse IP de secours par défaut d'OC200 est 192.168.0.253.

   Conseil : L'adresse IP de secours est utilisée lorsque OC200 ne parvient pas à obtenir l'adresse IP dynamique à partir du serveur DHCP.
3. Lancez un navigateur Web et tapez l'adresse IP d'OC200 dans la barre d'adresses, puis appuyez sur Entrée (Windows) ou Retour (Mac).

1.4.2 Via Omada Cloud

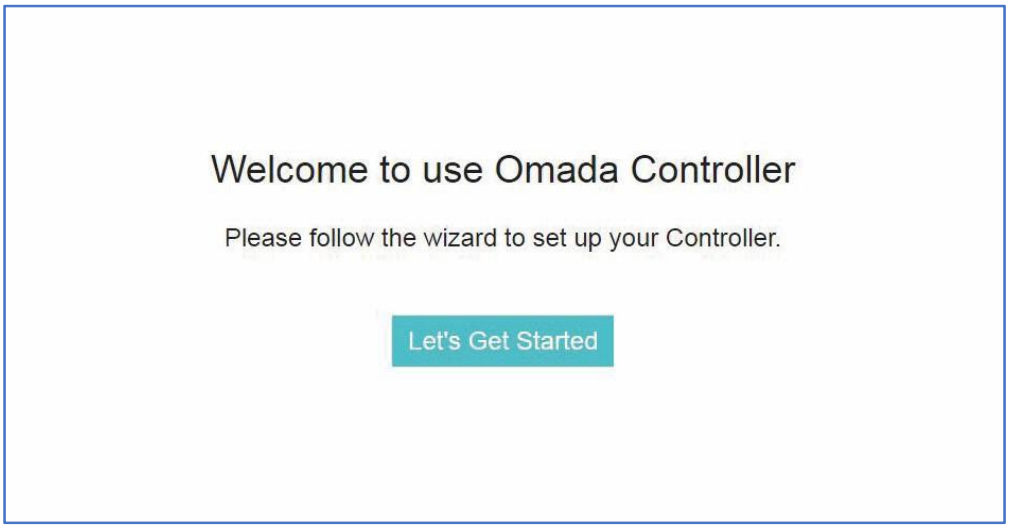
Suivez les étapes ci-dessous pour vous connecter à OC200 via le cloud Omada :

1. Assurez-vous que votre appareil de gestion et OC200 peuvent accéder à Internet.
2. Lancez un navigateur Web et visitez https://omada.tplinkcloud.com dans la barre d'adresses, puis appuyez sur Entrée (Windows) ou Retour (Mac).
3. Entrez votre ID TP-Link et votre mot de passe pour vous connecter. Cliquez ensuite sur Ajouter un contrôleur de nuage et suivez les instructions pour ajouter votre OC200.
4. Cliquez sur Lancer dans la colonne Action pour visiter l'interface de gestion d'OC200.

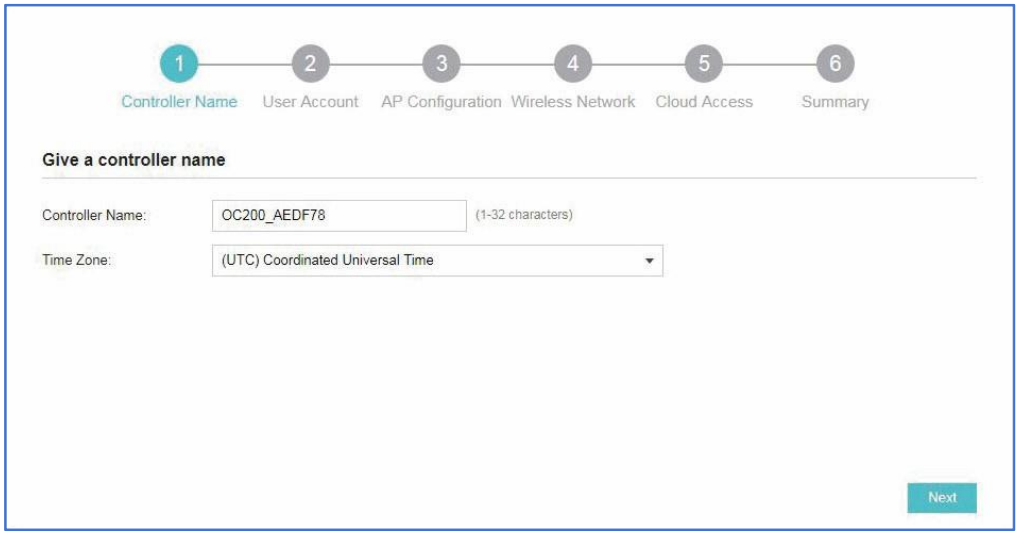
1.4.3 Effectuer les configurations de base

Dans le navigateur Web, vous pouvez voir la page de configuration. Suivez l'Assistant Configuration pour compléter les paramètres de base d'OC200.

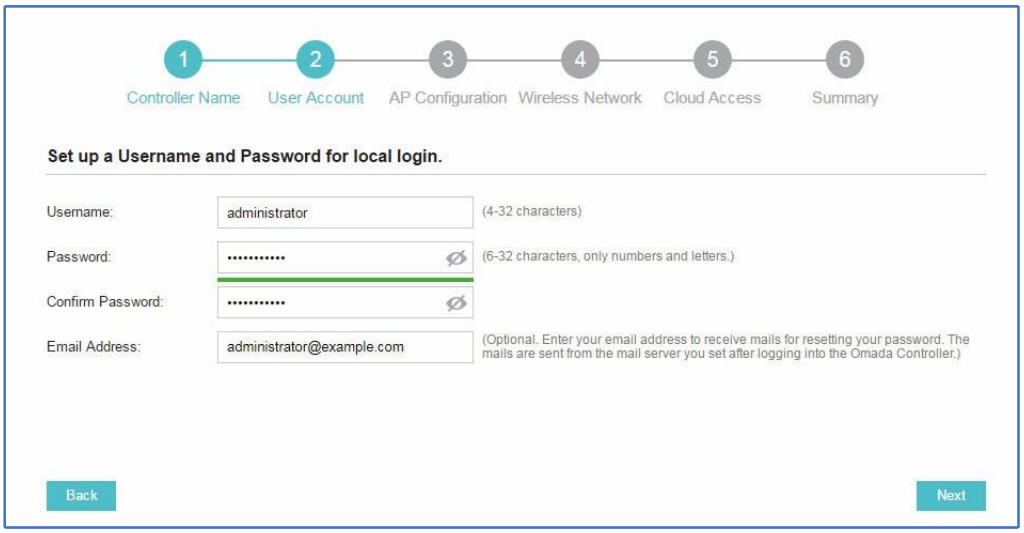
1. Cliquez sur Let's Get Started.



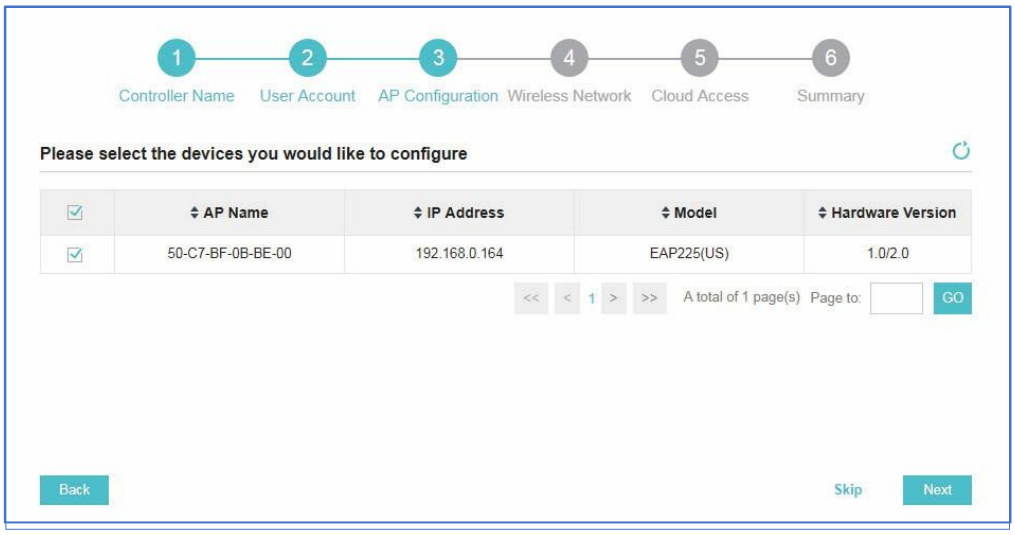
2. Spécifiez un nom pour OC200 et sélectionnez le fuseau horaire. Cliquez sur Suivant.



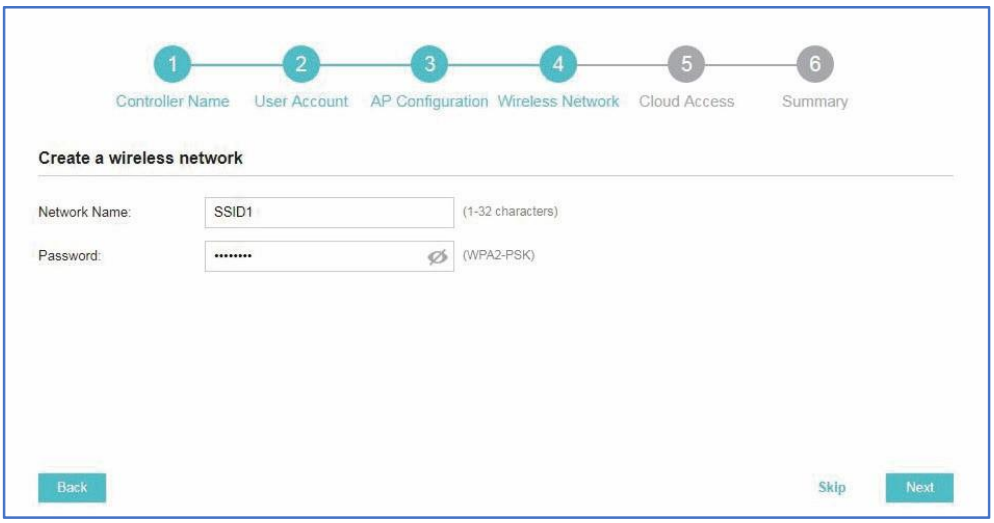
3. Spécifiez un nom d'utilisateur et un mot de passe pour le compte de connexion. Spécifiez l'adresse e-mail pour réinitialiser votre mot de passe au cas où vous oublieriez le mot de passe. Après vous être connecté à OC200, définissez un serveur de messagerie pour que vous puissiez recevoir des e-mails et réinitialiser votre mot de passe. Pour définir un serveur de messagerie, reportez-vous à Configure Mail Server. Cliquez sur Suivant.



4. La page d'installation affiche tous les EAP détectés dans le réseau. Sélectionnez un ou plusieurs EAP à gérer et cliquez sur Suivant.

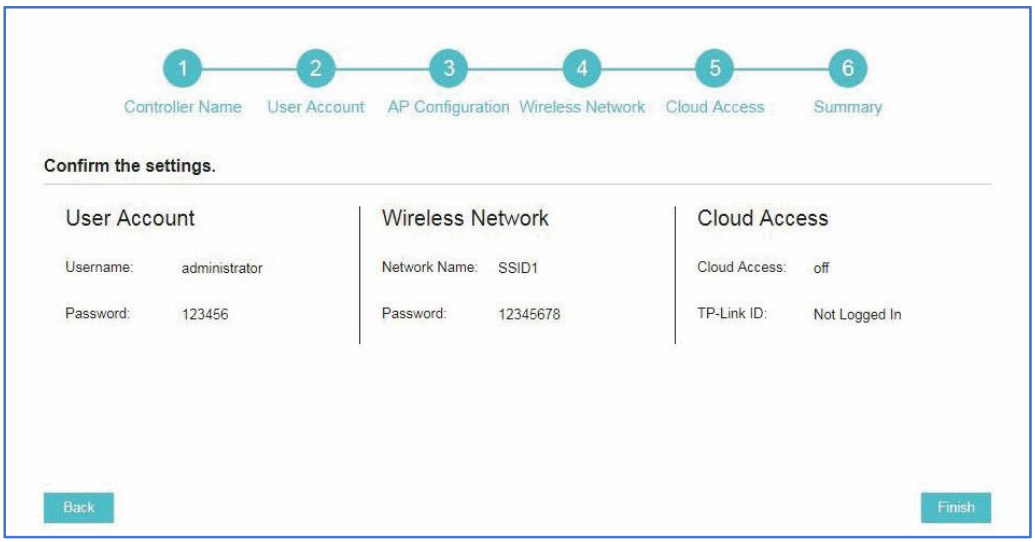


5. Définissez un nom SSID (nom du réseau sans fil) et un mot de passe pour que les EAP soient gérés. OC200 créera deux réseaux sans fil, un 2,4 GHz et un 5GHz, tous deux cryptés en mode WPA2-PSK. Cliquez sur Suivant.



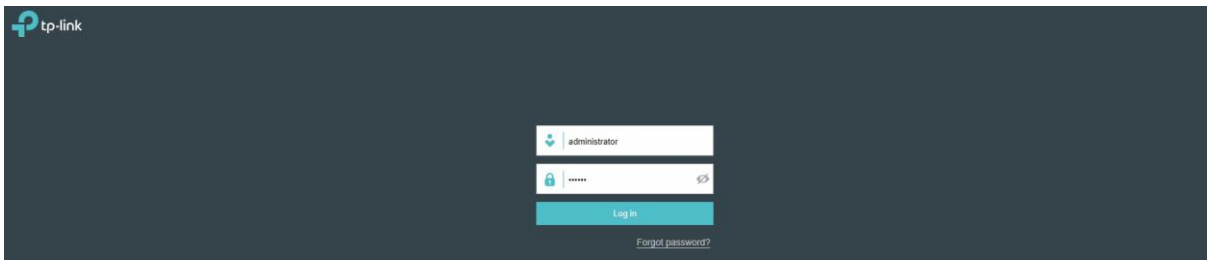
6. Si vous souhaitez gérer les EAP via le cloud Omada, activez le bouton **Acceptation du nuage** et lier votre ID TP-Link à votre OC200, puis cliquez sur Suivant. Si vous souhaitez gérer les EAP sur le réseau local, vous pouvez simplement cliquer sur Ignorer. Pour plus de détails sur Omada Cloud, veuillez consulter Omada Cloud Service.

7. Examinez vos paramètres et cliquez sur Terminer.



1.4.4 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.



1.5 Créer des sites et adopter les EAP

OC200 peut gérer plusieurs réseaux de EAP, appelés sites. Plusieurs sites sont logiquement séparés, et chaque site a ses propres configurations. Il existe un site initial nommé Par défaut. Le site Par défaut ne peut pas être supprimé. Si vous n'avez pas besoin de gérer des EAP avec différents sites, vous pouvez modifier le site par défaut et ignorer la section Créer des sites. Toutefois, Adopter les EAP est une étape nécessaire pour gérer les EAP.

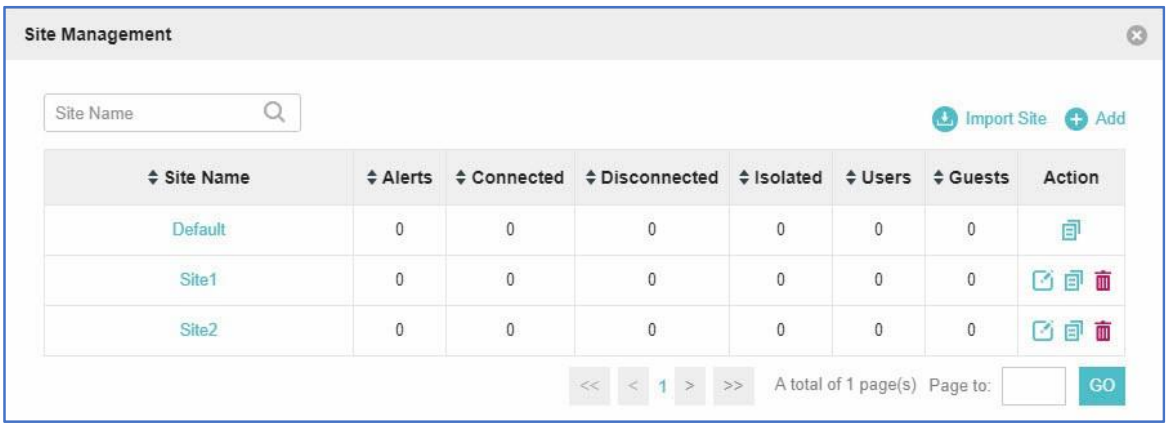
1.5.1 Créer des sites

Il existe trois méthodes pour créer des sites : Ajouter des sites, importer des sitesset copier des sites. Déterminez la méthode en fonction de vos besoins et reportez-vous aux introductions suivantes pour créer des sites.

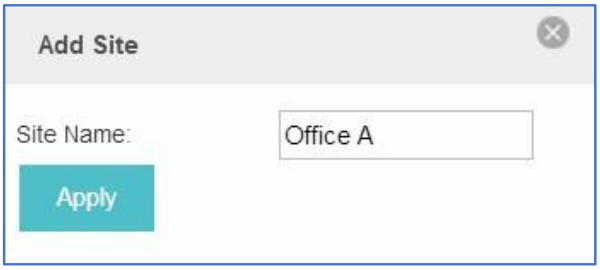
Ajouter des sites

Suivez les étapes ci-dessous pour ajouter un nouveau site directement.

. 1. Cliquez Sites: Default Dans l'onglet supérieure gauche de la Page et Site Manager
Pour pouvoir personnaliser votre réseau



2 Cliquez sur Add Et entrez un nom unique pour le nouveau site.



3. Appliquer pour créer le site

Importer des sites

Vous pouvez importer le site à partir d'un autre OC200. Les paramètres du site et les EAP du site seront importés sur le nouveau site.

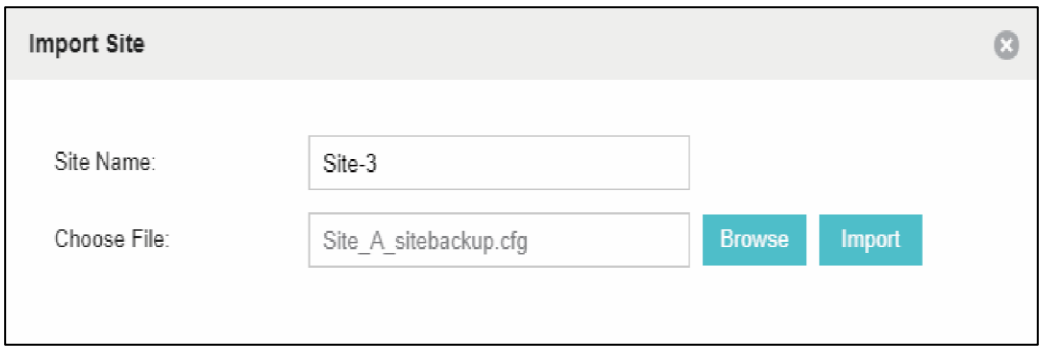
Notes

1 . Cliquez Sites: Default dans l'onglet de la Page Site Manager et, pour créer et personnaliser un site

- Cette fonction n'est disponible que pour les utilisateurs connectés locaux.
- Le site à importer doit provenir d'un AUTRE OC200.

2. Import Site Entrez un nom unique pour le nouveau site.

3. Cliquez sur Parcourir pour télécharger le fichier de sauvegarde d'un autre site, puis cliquez sur Importer pour importer le site.



Pour exporter des sites (y compris les paramètres de site et les EAP dans les sites) d'un OC200 à un autre, utilisez la fonction Migrer. Pour plus de détails sur Migrer, reportez-vous à Migrer.

Copier les sites

Avec La copie de site, vous pouvez créer un nouveau site avec les mêmes paramètres que les sites existants de votre contrôleur. Notez que seuls les paramètres du site seront copiés. Les EAP seront toujours gérés sur le site d'origine.

1. Cliquez Sites: Default Dans Site Manager puis personnaliser le site

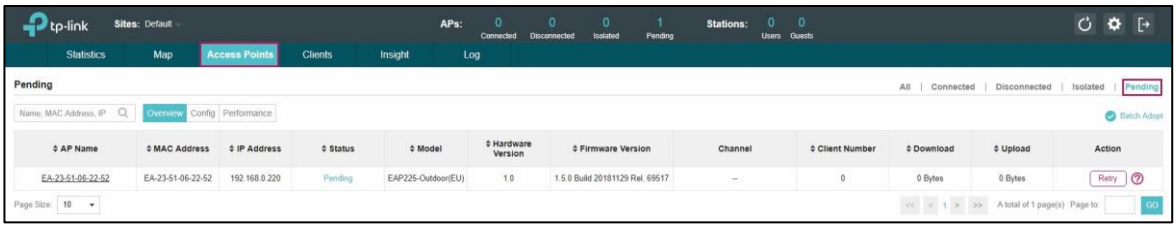
2 . Sélectionnez le Site dont vous voulez Copier tous les paramètres et Nom Unique pour importer le paramétrage vers le site.

3. Appliquer pour créer le Site

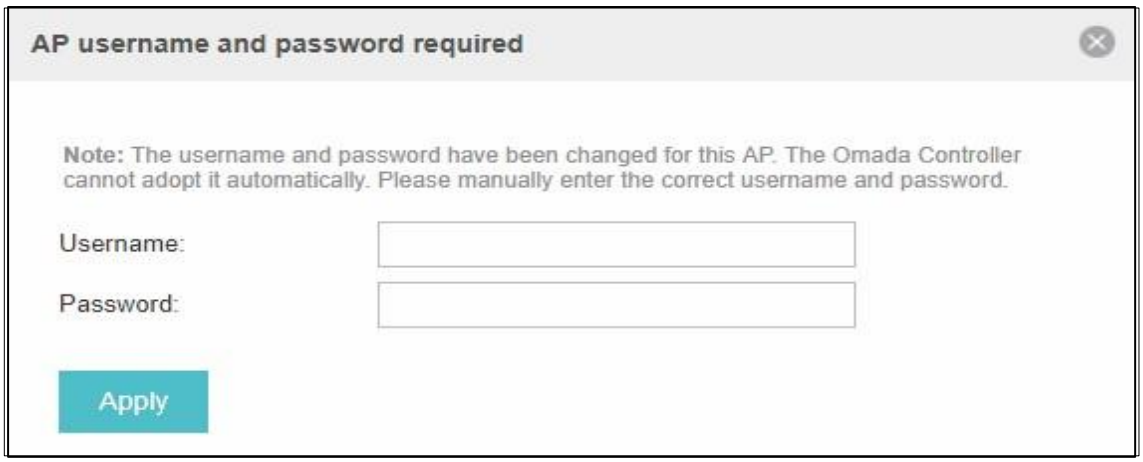
1.5.2 Adopter les EAP

OC200 peut découvrir tous les EAP actuellement connectés dans le réseau et afficher leur statut de connexion. Tous les EAP sont en attente lorsqu'ils sont découverts pour la première fois par OC200. Pour gérer les EAP, vous devez les adopter. Dans le processus d'installation rapide, OC200 adoptera automatiquement les EAP sélectionnés à l'aide du nom d'utilisateur et du mot de passe par défaut (les deux sont admin). Toutefois, si vous avez modifié le nom d'utilisateur ou le mot de passe de vos EAP auparavant, OC200 ne peut pas les adopter automatiquement, et vous devez vous référer aux étapes suivantes pour les adopter manuellement. Pour s'assurer que tous les EAP sont adoptés, procédez comme suit :

1. Sélectionnez un site et accédez aux points d'accès > En attente. Le tableau affiche tous les EAP qui n'ont pas été adoptés.



2. Cliquez sur le bouton Réessayez dans la colonne Action et entrez le nom d'utilisateur et le mot de passe actuels du EAP. Cliquez sur Appliquer.



- Si vous avez un nouveau EAP découvert, vous pouvez cliquer sur le bouton Adopter dans la colonne Action pour adopter le EAP. OC200 adoptera automatiquement le EAP à l'aide du nom d'utilisateur et du mot de passe par défaut (les deux sont admin).
- Si vous avez plusieurs nouveaux EAP découverts et que tous ont le nom d'utilisateur et le mot de passe par défaut (les deux sont administrateurs), vous pouvez cliquer sur le bouton Adopter un lot pour les adopter par lots. Mais s'il y a des EAP avec le bouton Réessayer, cela signifie que le nom d'utilisateur et le mot de passe de ces EAP ont été modifiés. Vous devez d'abord les adopter avant que le lot adopte les EAP reste.

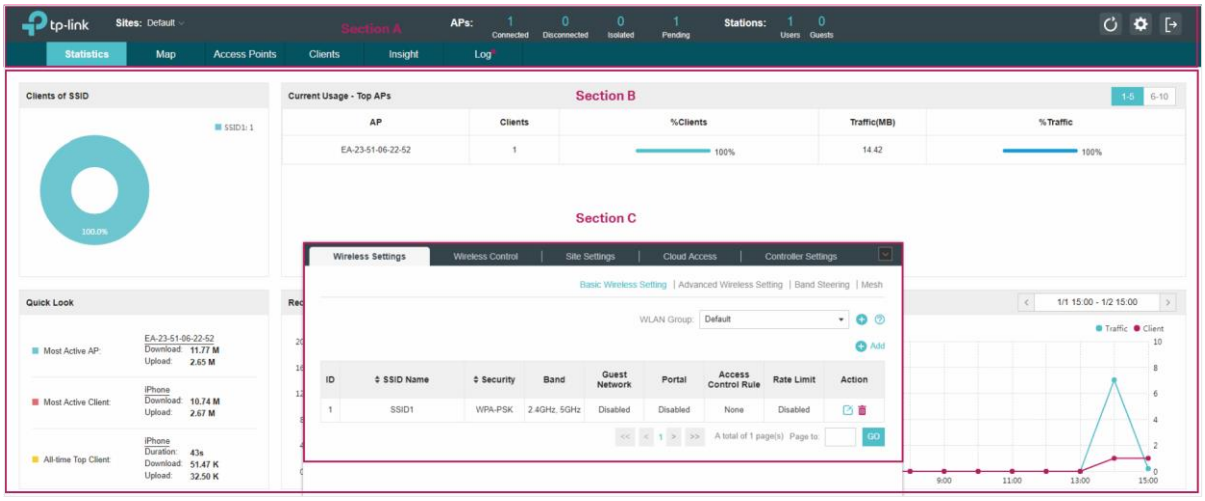
3. Une fois les EAP adoptés, le statut passera de l'attente à la connexion. Tous les noms d'utilisateur et mot de passe des EAP deviendront les mêmes que ceux du compte d'administrateur oc200 que vous avez créé dans les Configurations de base.

Conseil :

Si vous souhaitez modifier le nom d'utilisateur et le mot de passe des EAP, reportez-vous au compte de périphérique.

1.6 Surveiller et gérer les EAP

Lorsque toutes les configurations ci-dessus sont terminées, vous pouvez surveiller et gérer de manière centralisée les EAP via l'interface de gestion de l'OC200. L'interface de gestion est divisée en trois sections comme le montre la figure suivante.



Section A	Dans la section A, vous pouvez vérifier l'état des EAP et des clients du réseau. En outre, vous pouvez cliquer pour actualiser la page en cours, cliquer pour configurer globalement le réseau sans fil, puis cliquer pour vous déconnecter de l'interface de gestion.  En outre, les Sites vous permettent de regrouper vos EAP et de les gérer par lots. Pour configurer des sites, reportez-vous à Créer des sites.
Section B	Dans la section B, vous pouvez surveiller de façon centralisée les EAP et les clients.
Section C	Dans la section C, vous pouvez configurer globalement le réseau sans fil. Les configurations globales entreront en vigueur sur tous les EAP adoptés.

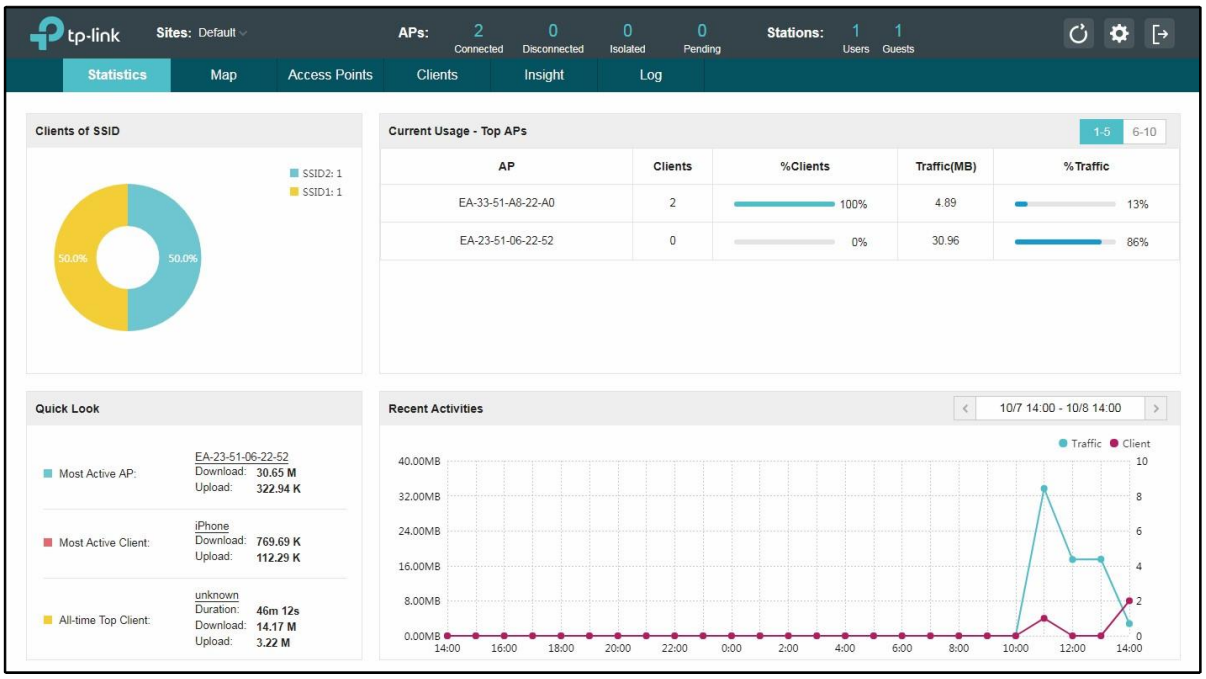
2 Surveiller et gérer le Réseau

Avec OC200, vous pouvez surveiller les EAP et gérer de manière centralisée votre réseau sans fil. Ce chapitre comprend les sections suivantes :

- Voir les statistiques du réseau
- Surveiller le réseau avec la carte
- Surveiller et gérer les EAP
- Surveiller et gérer les clients
- Afficher les statistiques des clients au cours de la période spécifiée
- Gérer la liste des AP voyous
- Afficher l'autorisation d'invité passé
- Afficher les journaux

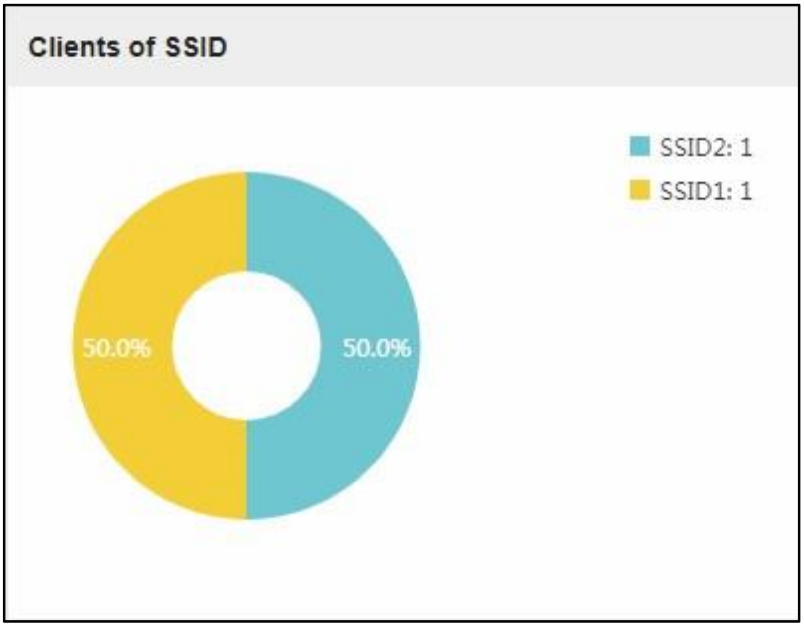
2.1 Voir les statistiques du réseau

OC200 recueille toutes les statistiques des EAP gérés et affiche les informations statistiques via des graphiques, des graphiques en secteurs et des tableaux, fournissant une vue d'ensemble de votre réseau sans fil.



2.1.1 Afficher la distribution client sur SSID

Un graphique en secteurs visuel affiche la distribution client sur chaque SSID. Par exemple, le SSID1 a un client, qui occupe 50% de tous les clients.



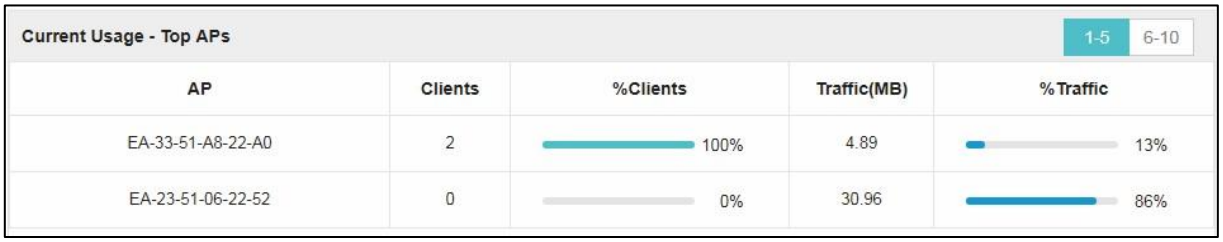
2.1.2 Examinez rapidement les EAP et les clients

Cet onglet affiche l'AP le plus actif, les clients les plus actifs et le client le plus actif. Vous pouvez cliquer sur l'adresse MAC du EAP ou du client pour en voir plus de détails.

AP le plus actif	Le courant connecté AP avec le trafic maximum.
Client le plus actif	Client connecté actuel avec le trafic maximum.
Meilleur client de tous les temps	Le client avec le trafic maximum parmi tous les clients qui n'ont jamais accédé au réseau EAP.

2.1.3 Afficher les EAP actuels

Cet onglet répertorie le nombre de clients connectés et l'état de trafic de données des dix AP qui utilisent le plus de trafic actuellement.



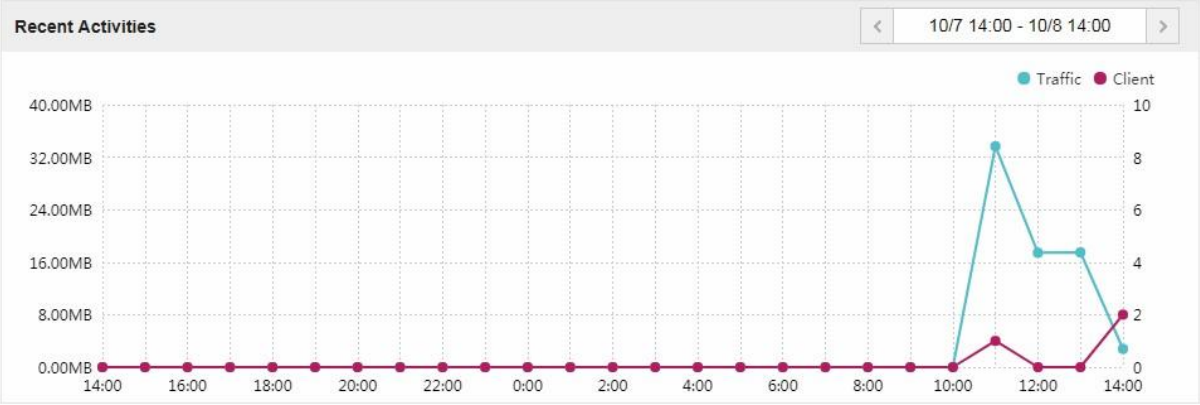
Clients	Nombre de clients connectés à ce EAP.
%Clients	Proportion des clients connectés actuels au montant total du client des PNE.

Trafic (MO)	La quantité totale de données transmises par ce EAP, qui équivaut à la somme du trafic de transmission de tous les clients actuels qui se connectent à l'AP.
%Trafic	La proportion de la transmission de données actuelle du EAP s'élève au montant total de transmission des EAP supérieurs.

2.1.4 Voir les activités récentes

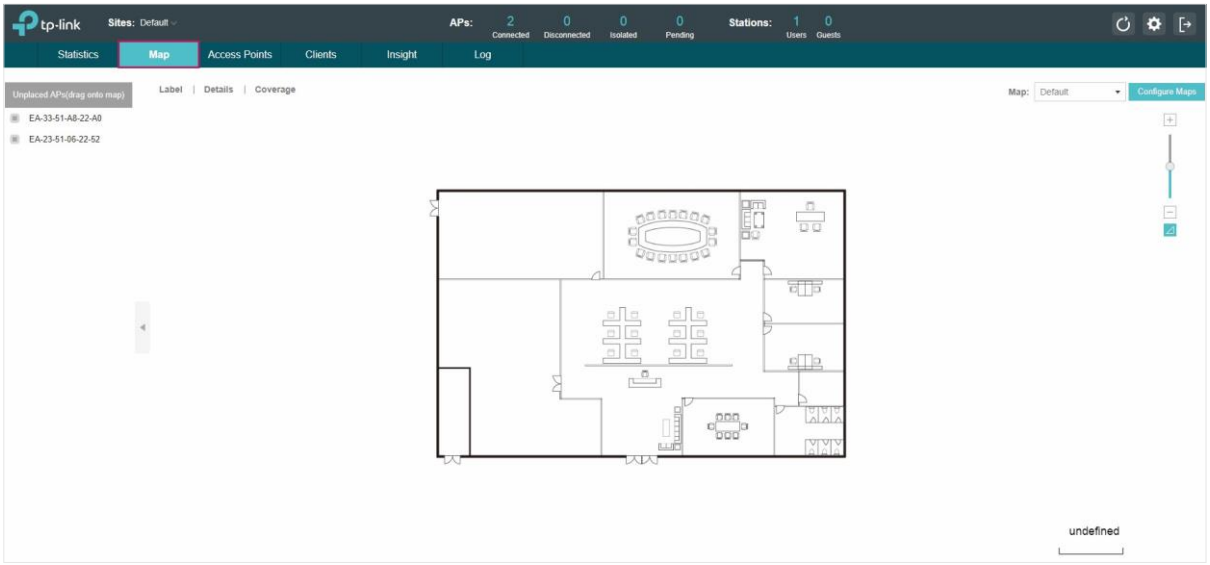
Les statistiques sur les activités récentes peuvent être oscillées entre une vue des 24 dernières heures spécifiques et une pour les 30 derniers jours spécifiques.

L'axe de l'ordre gauche indique le trafic et le bon représente le nombre des clients. L'axe des abscisses indique la période de temps sélectionnée. Le trafic indique un graphique visuel du trafic réseau au cours de la période sélectionnée. Le client indique un graphique visuel du nombre des clients connectés au cours de la période sélectionnée. Par exemple, les statistiques de 15h00 indiquent la taille du trafic et le numéro de client de 14h00 à 15h00. Dans le chiffre suivant, à 11 heures, le trafic est d'environ 34 Mo et il y a 1 clients connectés à l'AP.



2.2 Surveiller le réseau avec la carte

Vous pouvez télécharger vos images de carte locales et surveiller l'état et la plage de couverture de chaque EAP avec la carte. Lorsque vous lancez initialement l'OC200, une carte par défaut s'affiche au fur et à mesure que la figure suivante s'affiche. Suivez les instructions ci-dessous pour ajouter votre propre carte et gérer les EAP via la carte.

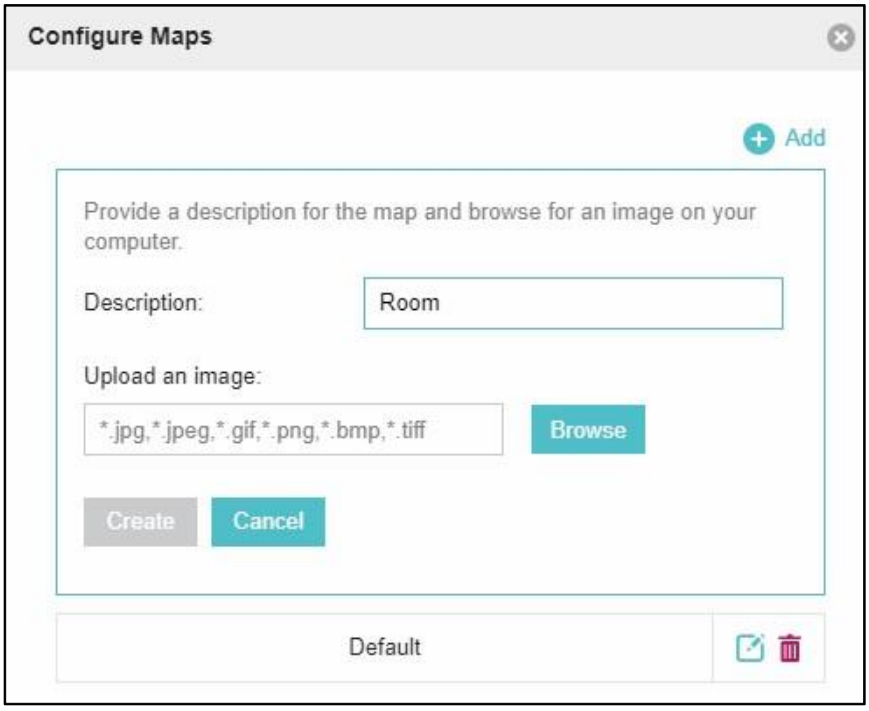


2.2.1 Ajouter une carte

Préparer une image de carte au format ***.jpg, .jpeg, .gif, .png, .bmp, .tiff***. Et suivez ensuite les étapes ci-dessous pour ajouter la carte à l'OC200.

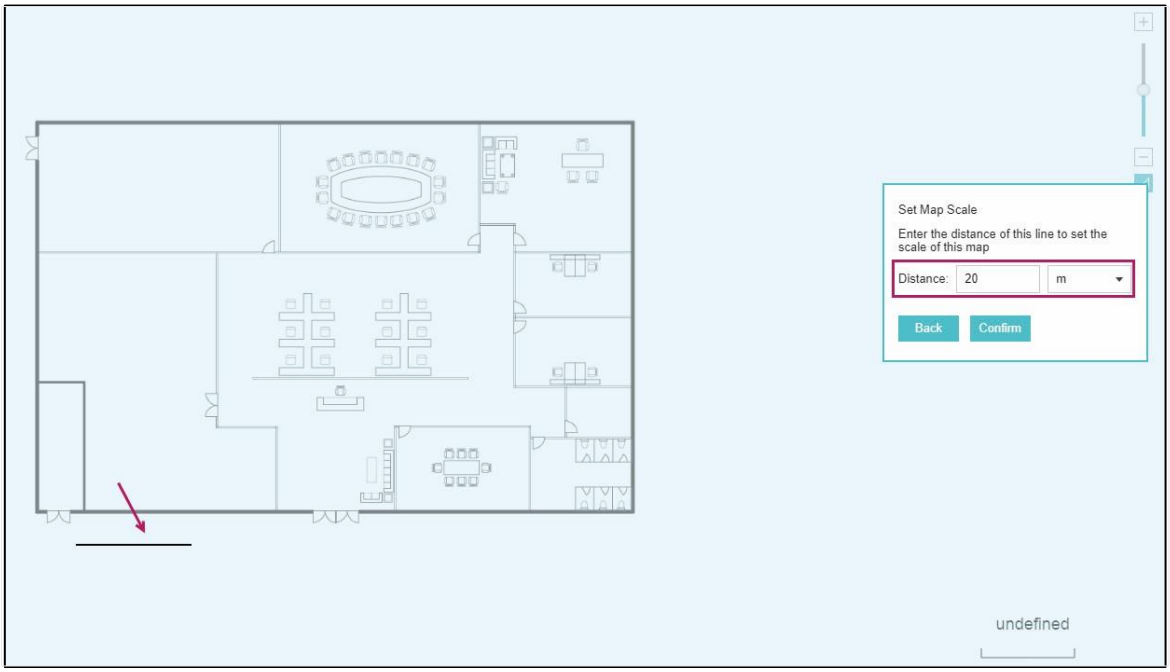
1. Cliquez sur Configurer les cartes dans le coin supérieur droit de la carte, puis sur Ajouter.

2. Entrez la description de la carte, sélectionnez l'image de votre carte, puis cliquez sur Créer.

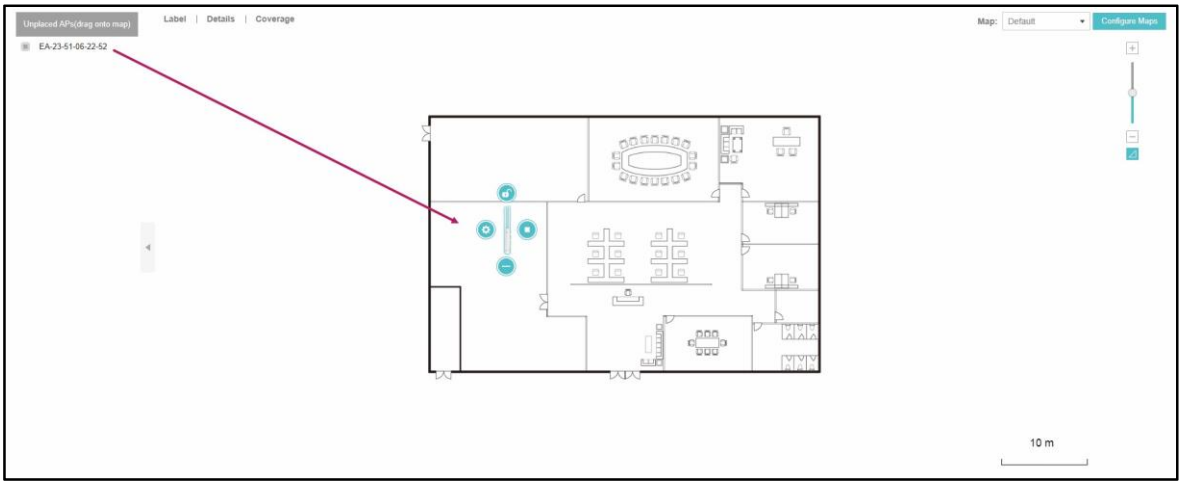


3. Sélectionnez votre carte locale dans la liste déroulante dans le coin supérieur droit de la zone de carte.

4. Cliquez sur. Tracez une ligne sur la carte et entrez la distance que représente la ligne. Ensuite, le contrôleur Omada calculera et générera automatiquement l'échelle de la carte en fonction de votre configuration.



5. Faites glisser les EAP de la liste des AP non placés vers les emplacements appropriés sur la carte en fonction de leurs emplacements réels.



Cliquez sur le produit Afin d'accéder à d'autres Options :

	Verrouiller l'EAP à l'emplacement actuel de la carte.
	Débloquez l'EAP sélectionné et vous pouvez le faire glisser à un autre
	Affichez les détails de l'EAP et configurez les paramètres sans fil . Se référer au menu Configurateur les EAPs
	Supprimer l'EAP dans la liste et les AP non-remplacés .
	Flashez la Led de l'EAP sur la carte. La LED clignotera pendant 10 Minutes ou jusqu'à ce que le bouton soit accessible de nouveau.
	Cliquez sur le bouton Verser la Led de clignoter.

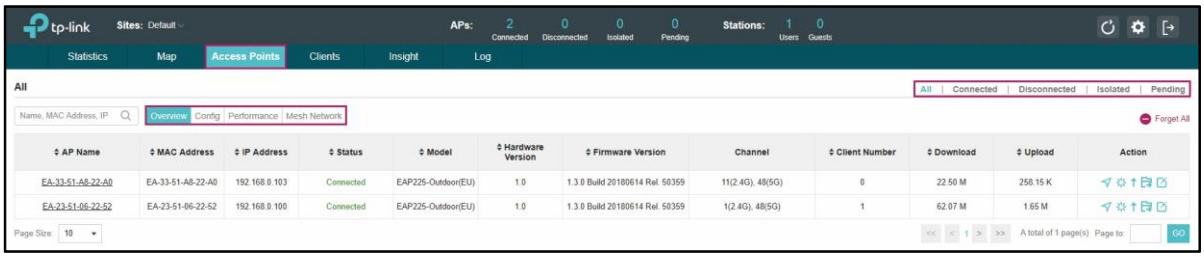
2.2.2 Surveiller les EAP sur la carte

Cliquez sur l'une des options suivantes pour afficher l'étiquette, les détails et la couverture du EAP sur la carte.

Étiquette	Affichez le nom du EAP. Le nom par défaut est l'adresse MAC du EAP.
Détails	Affichez le nom du EAP, l'adresse MAC, l'adresse IP, le canal de transmission/réception, le nombre d'utilisateurs connectés et le nombre d'invités connectés.
Couverture	Affichez une représentation visuelle de la plage sans fil couverte par les EAP. La couverture réelle du signal peut être plus petite que la couverture visuelle sur la carte parce que les obstacles autour des EAP affaibliront le signal.

2.3 Surveiller et gérer les EAP

OC200 peut découvrir tous les EAP actuellement connectés au réseau et afficher les informations de ceux-ci sur la page Points d'accès.



2.3.1 Gérer les EAP à statut différent

Selon leur statut de connexion, les EAP sont divisés en quatre catégories : connecté, déconnecté, isolé et en attente. Vous pouvez afficher les EAP en différents statuts sur différentes pages :

Tous	Affiche les informations de tous les EAP dans un statut différent.
Connecté	Affiche les EAP connectés. L'état des EAP connectés comprend deux cas : connecté et connecté (sans fil). Connecté : une fois que vous avez adopté un EAP câblé en instance, son statut deviendra provisioning, puis configuration et connecté éventuellement. Connecté (sans fil) : dans un réseau maillé, si un EAP a une liaison vers le haut sans fil réussie, son statut deviendra **Adopting** (Wireless) puis **Connected** (Wireless). Seuls les EAP connectés peuvent être gérés. Un EAP connecté se transformera en un en attente après que vous l'oubliez. Vous pouvez vous référer à Oubliez cet AP pour oublier un EAP ou cliquez sur Oubliez tout sur la page pour oublier tous les EAP connectés.
Déconnecté	Affiche les EAP déconnectés. Si un EAP connecté s'éteint ou se déconnecte de l'OC200, il sera en état déconnecté. Lorsqu'un EAP déconnecté est réinitialisé en défaut d'usine ou oublié, il se transforme à nouveau en un EAP en attente. Vous pouvez vous référer à Oubliez cet AP pour oublier un EAP ou cliquez sur Oubliez tout sur la page pour oublier tous les EAP déconnectés.
En attente	Affiche les EAP en attente. L'état des EAP en instance comprend trois cas : en instance, en attente (sans fil) et géré par d'autres. En attente : tous les EAP avec connexion réseau câblée sont en attente d'état par défaut lorsqu'ils sont découverts par Omada Controller. En attente (Sans fil) : le EAP par défaut de l'usine avec des fonctions de maillage et aucune connexion réseau câblée n'est en attente (sans fil) lorsqu'il est découvert par l'OC200.

	Géré par d'autres : un EAP est situé sur le même réseau que le contrôleur mais a déjà été géré par un contrôleur existant auparavant. Vous pouvez fournir le nom d'utilisateur/mot de passe pour délier le EAP du contrôleur existant et commencer l'adoption dans le contrôleur actuel. Ce n'est qu'une fois que les EAP en attente sont adoptés et connectés que vous pouvez les gérer. Pour adopter des EAP en attente, reportez-vous à Adopter les EAP.
Isolé	Affiche les EAP isolés. Dans un réseau de maillage, lorsque le EAP qui a été géré auparavant par l'OC200 se connecte au réseau sans fil et ne peut pas atteindre la passerelle, il entre dans l'état isolé. Le EAP isolé recherche le lien vers le haut sans fil et la LED sur l'appareil devient vert et clignote toutes les 5 secondes. Pour en savoir plus sur le réseau de maillage, reportez-vous à Configure Mesh.

2.3.2 Voir les informations détaillées des EAP

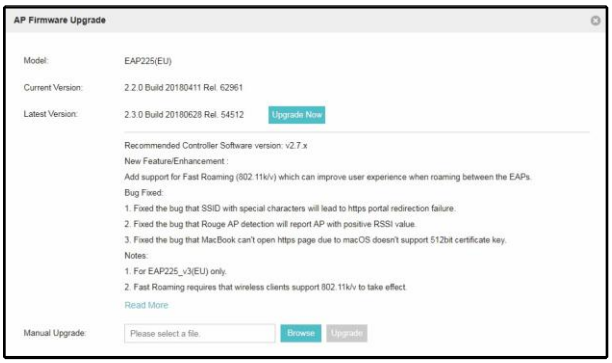
Vous pouvez cliquer sur l'onglet Vue d'ensemble, Configuration, Performance ou Réseau mesh pour afficher les différentes informations détaillées des EAP.

Aperçu	Affiche le nom du EAP, l'adresse MAC, l'adresse IP, l'état, le modèle, la version matérielle, la version du firmware, le nombre de canaux de clients connectés et les octets de téléchargement/téléchargement.
Config	Affiche le nom du EAP, l'adresse MAC, l'adresse IP, l'état, le modèle, la version matérielle, la version du firmware, le groupe WLAN délimité par la 2G et la 5G du EAP et la radio de la 2G et de la 5G.
Performance	Affiche le nom du EAP, l'adresse MAC, l'adresse IP, l'état, le modèle, la version matérielle, la version du firmware, le nombre de clients 2G connectés et les clients 5G, TX(Downloaded Traffic), RX(Uploaded Traffic), TX 2G et TX 5G.
Réseau Mesh	Affiche le nom du EAP, l'adresse MAC, l'adresse IP, l'état, le modèle, la version matérielle, la version du firmware, le nombre de clients connectés, les sauts, les AP de liaison vers le haut et les aps de liaison vers le bas.

2.3.3 Gérer les EAP dans la colonne Action

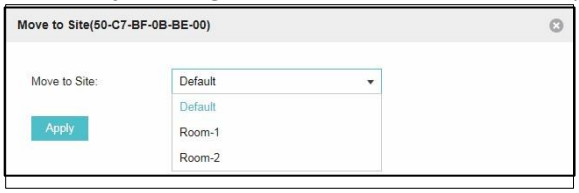
Vous pouvez exécuter l'opération correspondante au EAP en cliquant sur une icône dans la colonne Action.

	Localisez l'EAP dans la carte.
	Redémarrez l'EAP.
	Mettre à niveau l'EAP. Deux options sont disponibles pour la mise à niveau : mettre à niveau en ligne et mettre à niveau manuellement. Mise à niveau en ligne : avec l'accès au cloud activé sur l'OC200 et un ID TP-Link lié à l'OC200, le dernier firmware pour le EAP peut être détecté automatiquement par l'OC200. Et vous pouvez mettre à niveau le EAP en ligne en cliquant sur Mise à niveau maintenant. Pour plus de détails sur Cloud Access, reportez-vous à Omada Cloud Service. Mise à niveau manuelle : cliquez sur Parcourir pour localiser et choisir le fichier de mise à niveau de votre ordinateur, puis cliquez sur Mise à niveau pour installer le dernier firmware EAP. L'état apparaîtra sous forme de mise à niveau jusqu'à ce que le processus soit terminé et que le EAP se reconnecte à l'OC200.



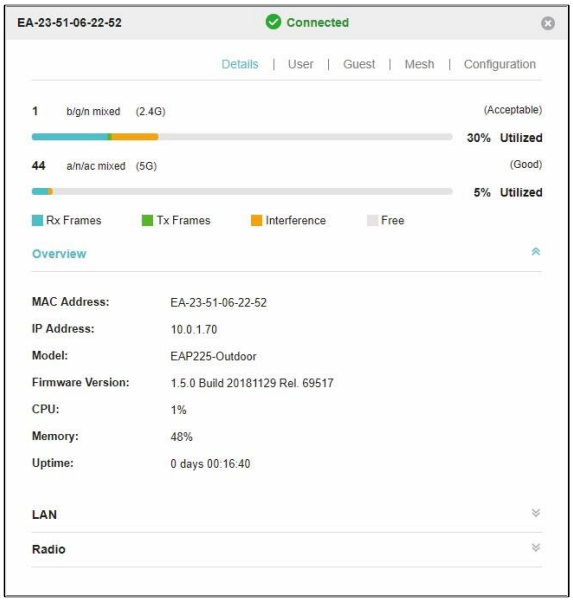
Déplacement de l'EAP vers un Site.

Sélectionnez un site créé et cliquez sur Appliquer. Vous pouvez regrouper tous les EAP de cette façon et les gérer de manière centralisée sur chaque site.



Configurez l'EAP

Pour obtenir des Instructions sur la Configuration de l'EAP dans cette fenêtre,, Configurateur les EAP

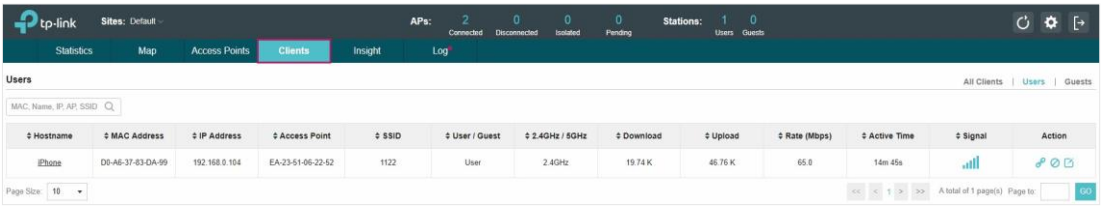


Notes

- Seuls les EAP gérés peuvent être redémarrés ou mis à niveau.
- Le EAP géré par l'OC200 ne peut pas être connecté à sa propre interface de gestion. Pour vous connecter à l'interface de gestion du EAP, oubliez d'abord le EAP dans l'OC200.

2.4 Surveiller et gérer les clients

L'onglet Clients affiche les clients connectés au réseau EAP.



2.4.1 Voir les informations actuelles des clients

Les clients sont divisés en deux types : utilisateur et invité. Les utilisateurs sont les clients connectés au réseau sans fil EAP sans l'authentification du portail. Les clients sont les clients qui passent l'authentification du portail.

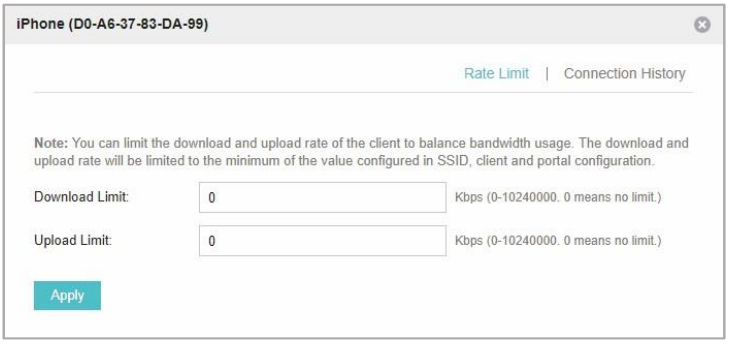
Vous pouvez cliquer sur les onglets suivants pour afficher respectivement les informations détaillées des utilisateurs et des invités.

Tous les clients	La page affiche les informations de tous les clients, y compris les utilisateurs et les invités.
Utilisateurs	La page affiche les informations des utilisateurs.
Invités	La page affiche les informations des invités.

2.4.2 Gérer les clients dans la colonne Action

Vous pouvez exécuter l'opération correspondante au EAP en cliquant sur une icône dans la colonne Action :

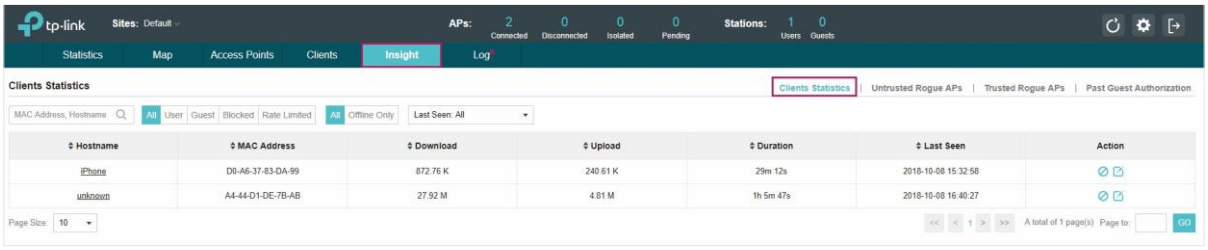
	Reconnectez le Client au réseau.
	Restreindre l'accès du client au réseau.
	Configurez la limite de taux du client et affichez l'historique de connexion. Entrez la limite de téléchargement et la limite de téléchargement, puis cliquez sur Appliquer.



Si le client est invité, vous pouvez cliquer sur cette icône pour annuler l'autorisation

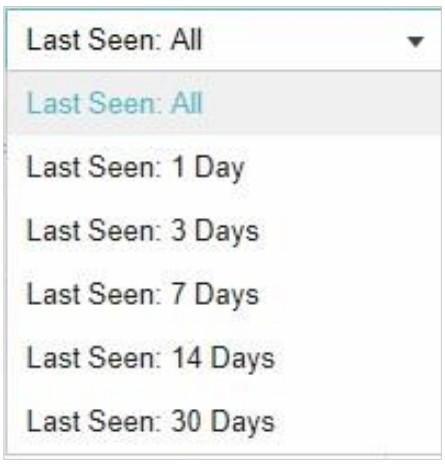
2.5 Afficher les statistiques des clients au cours de la période spécifiée

La page Statistiques clients sous l'onglet Insight affiche les informations des clients qui se sont connectés au réseau EAP au cours d'une période spécifiée.



2.5.1 Sélectionner une période spécifiée

Sélectionnez une période dans le menu déroulant. Ensuite, la page affichera les clients qui se sont connectés au réseau EAP au cours de la période.



2.5.2 Afficher l’historique des clients

Vous pouvez cliquer sur le nom d’hôte du client pour obtenir son historique de connexion et configurer la fonctionnalité Limite de taux pour ce client. En outre, vous pouvez cliquer sur les onglets suivants pour afficher les informations des différents types de clients :

Tous	La page affiche les informations historiques de tous les clients.
Utilisateur	La page affiche les informations d’historique des utilisateurs. Les utilisateurs sont les clients connectés au réseau sans fil EAP sans l’authentification du portail.
Invités	La page affiche les informations historiques des invités. Les clients sont les clients qui passent l’authentification du portail.
Bloqué	La page affiche les clients qui ont été bloqués.
Tarif limité	La page affiche les clients qui ont été limités taux de téléchargement ou de téléchargement.
	
Tous	La page affiche les informations d’historique de tous les clients.
Hors connexion uniquement	La page affiche les informations d’historique des clients hors ligne.

2.5.3 Gérer les clients dans la colonne Action

Vous pouvez exécuter l’opération correspondante au EAP dans la colonne Action :

	Bloquez l’accès du client au réseau.
	Reprise l’accès du client.
	Configurez la limite de taux du client et affichez l’historique de connexion .
	Supprimez la limite aux taux de téléchargement ou de téléchargement du

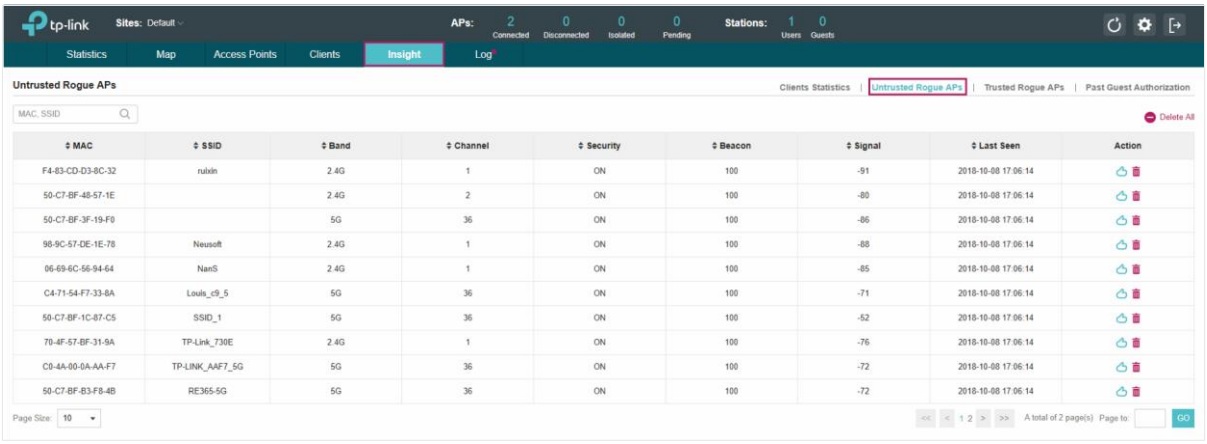
2.6 Gérer la liste des AP voyous

Un Rogue AP est un point d'accès qui a été installé sur un réseau sécurisé sans autorisation explicite d'un administrateur système. L'OC200 peut analyser tous les canaux pour détecter tous les EAP à proximité. Si des AP voyous sont détectés, ils seront affichés sur la liste des aps voyous non approuvés. En outre, vous pouvez déplacer les AP voyous non approuvés vers la liste des aps rogue approuvés.

Par défaut, la fonctionnalité De détection d'AP Rogue est désactivée. Pour permettre à votre EAP de détecter les API à proximité, vous devez activer cette fonctionnalité pour ce EAP. Vous pouvez vous référer à Rogue AP Detection.

2.6.1 Gérer la liste des AP voyous non approuvés

La page Des AP voyous non approuvés affiche les informations détaillées des AP voyous non approuvés.

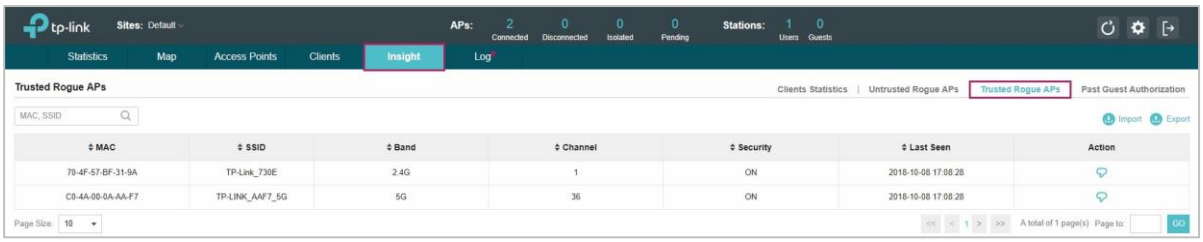


Vous pouvez exécuter l'opération correspondante au EAP dans la colonne Action :

	Déplacement de l'AP pirate non approuvé vers la liste des APS d indésirables .
	Supprimez cet enregistrement.
Delete All	Supprimez tous les enregistrements.

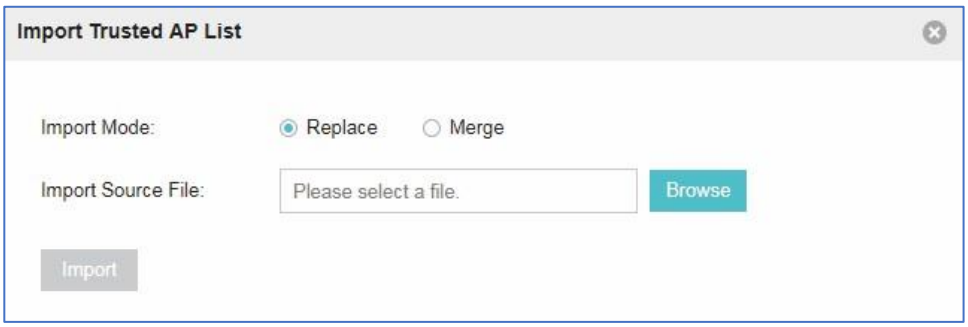
2.6.2 Gérer la liste des aps voyous approuvés

La page Trusted Rogue AP affiche les informations détaillées des AP voyous approuvés.



Vous pouvez exécuter l'opération correspondante au EAP en cliquant sur une icône dans la colonne Action :

	Déplacement l'AP voyou approuvé vers la liste des aps voyous non-approuvé .
Export	Exportez et téléchargez la liste actuelle trusted Rogue AP et enregistrez-la sur votre PC.
Import	Importateur une liste d'adresses IP's par Rogue Si Adresse Mac d'un Ap est dans la liste Ne pas être détecté comme un Ap authorisé

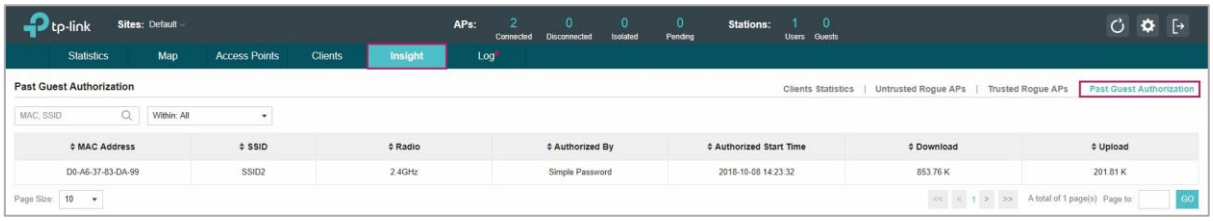


Veuillez suivre les étapes ci-dessous :

1. Sélectionnez Remplacer (remplacer la liste des AP approuvés en cours par celle que vous importez) ou Fusionner (ajouter les AP dans le fichier à la liste des AP approuvés en cours).
2. Cliquez sur Parcourir pour localiser le fichier et choisissez-le.
3. Cliquez sur Importer pour importer la liste Des aps approuvés par Rogue.

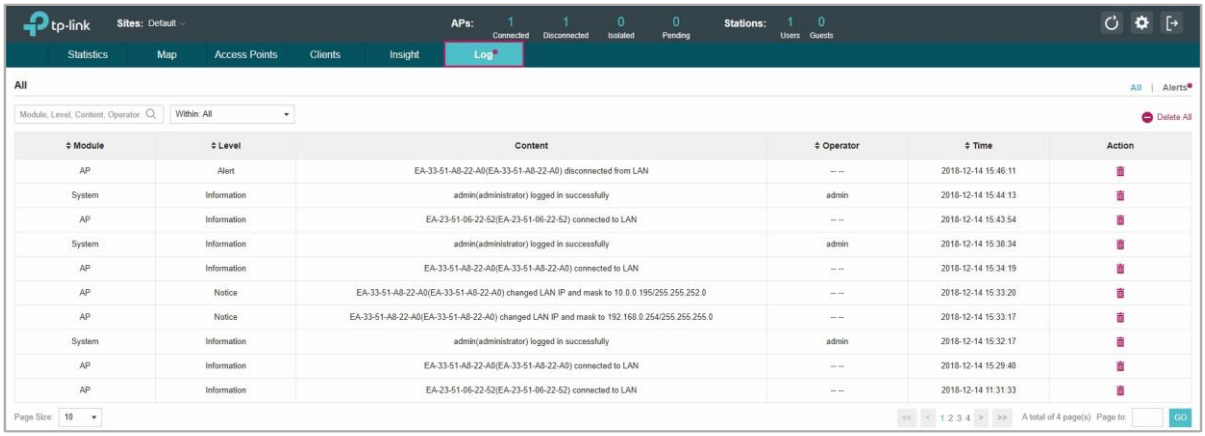
2.7 Afficher l'autorisation d'invité passé

La page Autorisation d'invité précédent affiche les détails sur tous les clients qui ont accédé au réseau au cours d'une certaine période de temps. Vous pouvez sélectionner une période dans la liste déroulante.



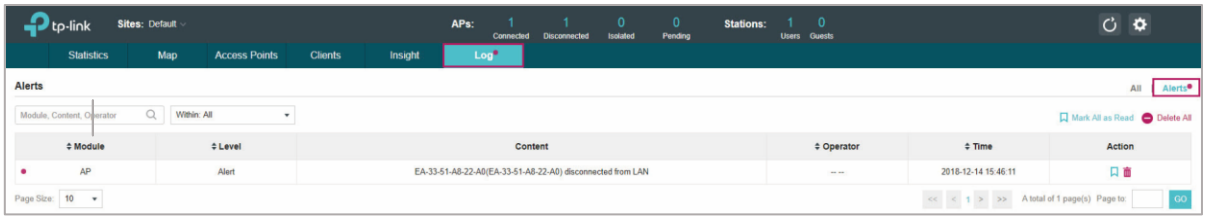
2.8 Afficher les journaux

Les journaux d'OC200 peuvent enregistrer, classer et gérer efficacement les informations système des EAP gérés, vous fournissant un support puissant pour surveiller le fonctionnement du réseau et diagnostiquer les dysfonctionnements. La page Journaux affiche le module, le niveau, le contenu, l'opérateur et l'heure du journal.



Vous pouvez afficher les alertes sur une page séparée en cliquant sur Alertes dans le coin supérieur droit de la page.

Personnalisation des alertes et des journaux de logs.



Notes : Les journaux et les alertes de l'OC200 avec la version 1.0.3 du firmware ou ci-dessous seront jetés après que le firmware est mis à niveau vers la version 1.1.0 ou plus.

3 Configurer les EAP à l’échelle mondiale

Ce chapitre présente les configurations globales appliquées à tous les EAP gérés. Pour configurer un EAP spécifique, veuillez consulter le chapitre 5 Configurer les EAP séparément.

Dans les configurations globales, vous pouvez configurer les éléments suivants :

- Réseau sans fil
- Contrôle d’accès
- Authentification du portail
- Stratégie d’authentification gratuite
- Filtre MAC
- Planificateur
- QoS
- Paramètres du site

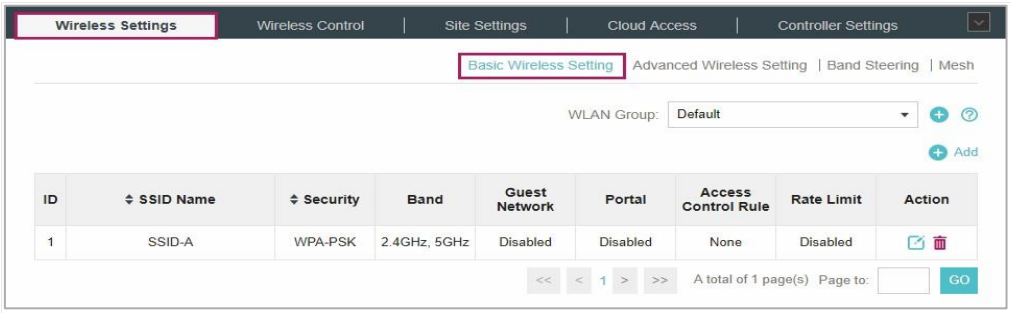
3.1 Réseau sans fil

En plus du réseau sans fil que vous avez créé dans Quick Start, vous pouvez ajouter plus de réseaux sans fil et configurer les paramètres sans fil avancés pour améliorer la qualité du réseau.

3.1.1 Ajouter des réseaux sans fil

Pour ajouter des réseaux sans fil, suivez les étapes ci-dessous.

1. Accédez aux paramètres sans fil > Paramètre sans fil de base.



2 Cliquez à droite pour ajouter un groupe WLAN. Les groupes WLAN sont un moyen facile de déployer rapidement les EAP en créant un ensemble de SSID basés sur des modèles avec des paramètres sans fil. Différents groupes WLAN peuvent être appliqués à différents EAP.

Si vous n'avez pas besoin de regrouper vos réseaux sans fil, vous pouvez utiliser le groupe WLAN par défaut et sauter cette étape. 

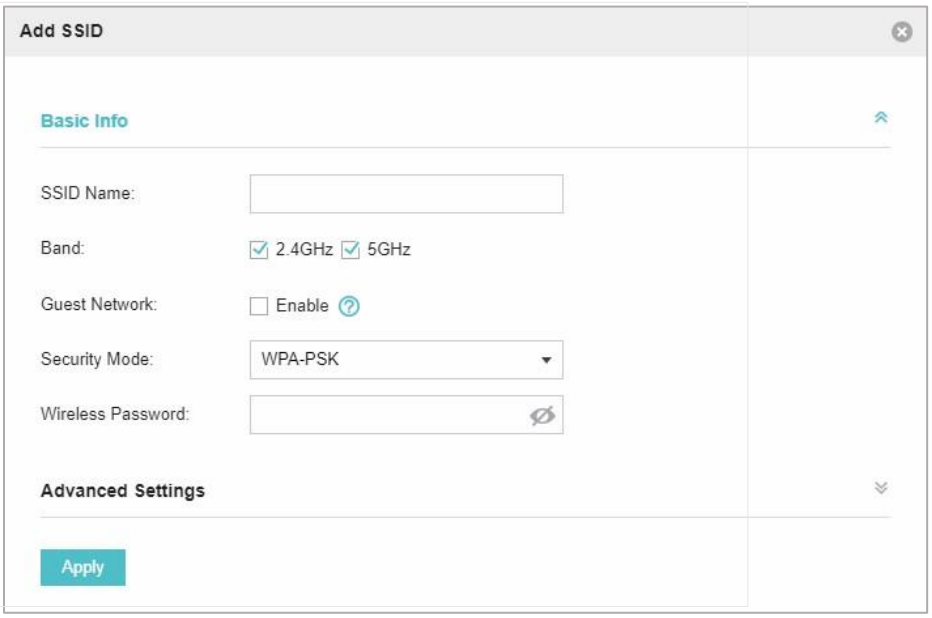
Spécifiez un nom pour le groupe et cliquez sur Appliquer.

Sélectionner le groupe **Wlan** 

Et cliquez sur 

Ajouter un SSID Groupe WLAN spécifique.

Configurez les paramètres de la fenêtre suivante.



Nom SSID	Entrez un nom SSID contient jusqu'à 32 caractères.
Bande	Sélectionnez la bande radio pour ajouter le SSID.
Réseau invité	Avec cette option activée, le réseau invité bloquera les clients d'atteindre n'importe quel sous-réseau IP privé.
Mode de sécurité	Sélectionnez le mode de sécurité du réseau sans fil. Aucun : Les hôtes peuvent accéder au réseau sans fil sans authentification. WEP/WPA-Enterprise/WPA-PSK : Les hôtes doivent être authentifiés avant d'accéder au réseau sans fil. Pour la sécurité du réseau, il est suggéré de chiffrer votre réseau sans fil. Les paramètres varient selon les modes de sécurité et les détails sont dans l'introduction suivante.

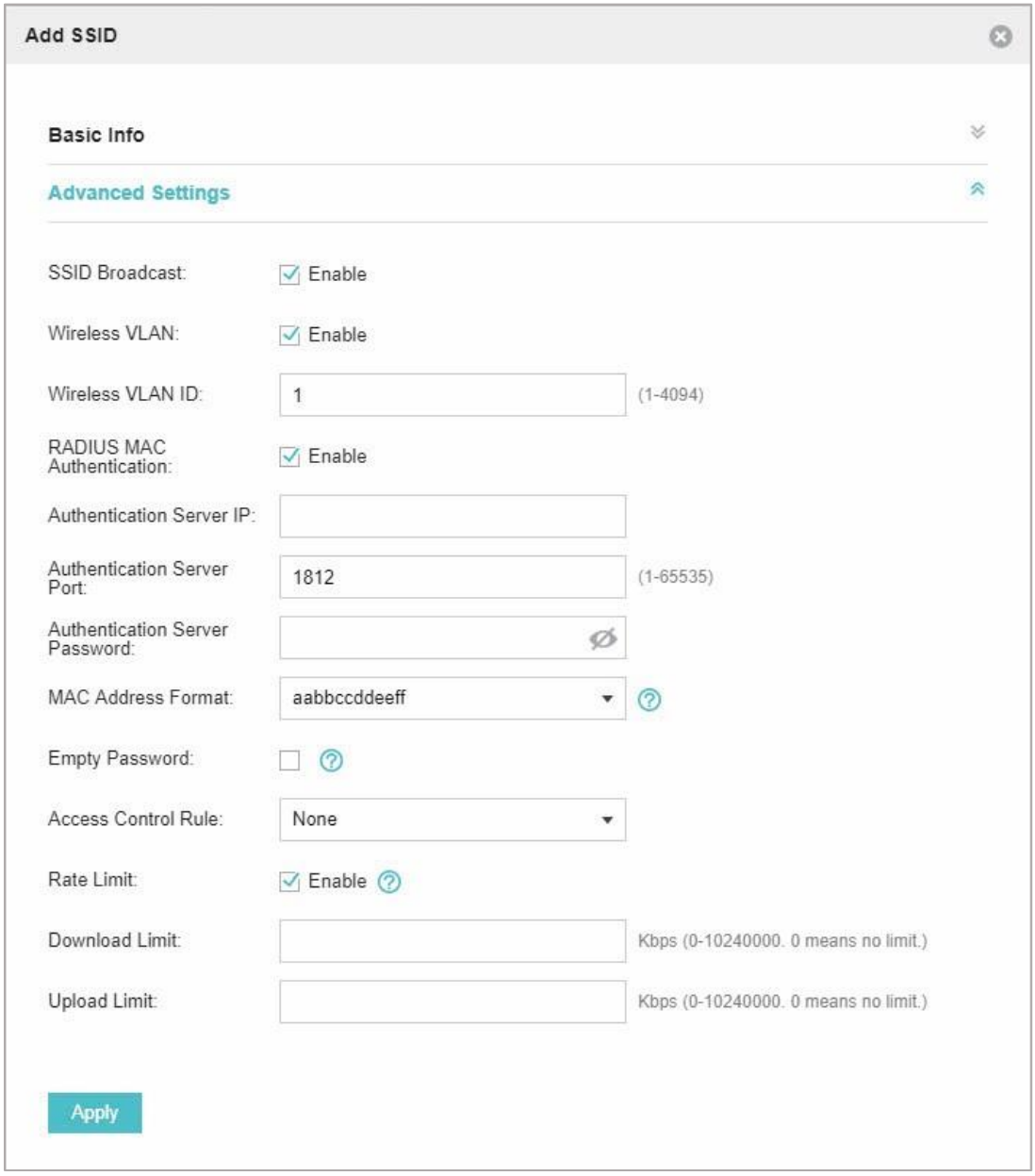
Notes

- 8 SSID peuvent être créés sur chaque bande tout au plus.
- Le SSID sur différentes bandes de radio du même nom sera considéré comme une entrée SSID identique. Lorsque vous mettez à niveau votre OC200 ou restaurez les fichiers de sauvegarde à partir du contrôleur avec la version 3.0.5 ou inférieure, les entrées SSID du même nom seront fusionnées si elles sont sur 2,4 GHz et 5GHz dans le même groupe WLAN. Toutes les configurations de l'entrée seront modifiées en paramètres du SSID d'origine sur la bande radio de 2,4 GHz.

Voici l'introduction détaillée de None, WEP, WPA-Enterprise et WPA-PSK.

Aucun

Les hôtes peuvent accéder au réseau sans fil sans authentification. Configurez les paramètres avancés dans la fenêtre suivante.



VLAN sans fil	Avec cette option activée, le EAP peut travailler de plus en plus avec les commutateurs prenant en charge 802.1Q VLAN. Le trafic des clients dans différents réseaux sans fil est ajouté avec différentes balises VLAN en fonction des paramètres VLAN des réseaux sans fil. Ensuite, les clients sans fil dans différents VLAN ne peuvent pas communiquer directement les uns avec les autres. Pour définir un VLAN sans fil pour le réseau sans fil, activez l'option et définissez un ID VLAN dans l'ID VLAN sans fil.

Diffusion SSID	Avec l'option activée, les EAP diffuseront le SSID aux hôtes voisins, afin que ces hôtes puissent trouver le réseau sans fil identifié par ce SSID. Si cette option est désactivée, les utilisateurs doivent saisir le SSID manuellement pour se connecter au EAP. L'option est activée par défaut.
ID VLAN sans fil	Entrez un ID VLAN pour le VLAN sans fil. Les réseaux sans fil avec le même ID VLAN sont regroupés sur un VLAN. La valeur varie **de 1 à 4094**.
RAYON MAC Authentification	Avec cette option activée, le EAP enverra l'adresse MAC du client au serveur RADIUS en tant que nom d'utilisateur et mot de passe pour l'authentification. Si l'autorisation réussit, le serveur RADIUS accorde au client l'accès au réseau. Pour définir l'authentification RADIUS MAC, activez l'option et configurez les paramètres suivants : IP du serveur d'authentification, port serveur d'authentification, mot de passe du serveur d'authentification, format d'adresse MAC et mot de passe vide.
Authentification IP du serveur	Avec l'authentification RADIUS MAC activée, entrez l'adresse IP du serveur d'authentification.
Authentification Port serveur	Avec l'authentification RADIUS MAC activée, entrez le numéro de port que vous avez défini sur le serveur RADIUS pour les demandes d'authentification. Le paramètre par défaut est **1812**.
Authentification Mot de passe du serveur	Avec l'authentification RADIUS MAC activée, entrez le mot de passe d'authentification. Le serveur d'authentification et l'OC200 utilisent le mot de passe pour chiffrer les mots de passe et échanger des réponses.
Adresse MAC Format	Avec l'authentification RADIUS MAC activée, sélectionnez le format pour convertir l'adresse MAC d'un client au nom d'utilisateur RADIUS.
Mot de passe vide	Avec l'option activée, un mot de passe vide pour l'authentification RADIUS MAC sera autorisé. Avec l'option désactivée, le mot de passe sera le même que le nom d'utilisateur.
Contrôle d'accès Règle	Sélectionnez une règle de contrôle d'accès pour ce SSID. Pour plus d'informations, reportez-vous au contrôle d'accès.
Limite de taux	Avec cette option activée, le taux de téléchargement et de téléchargement de chaque client qui se connecte au SSID sera limité à l'utilisation de la bande passante d'équilibre. Vous pouvez limiter le taux de téléchargement et de téléchargement pour certains clients spécifiques en configurant la limite de taux dans la liste des clients, reportez-vous à Gérer les clients dans la colonne Action pour obtenir plus de détails.

	Notez que le taux de téléchargement et de téléchargement sera limité au minimum de la valeur configurée en configuration SSID, client et portail.
Limite de téléchargement	Avec la limite de taux activée, spécifiez la limite de taux de téléchargement. 0 signifie illimité.
Limite de téléchargement	Avec la limite de taux activée, spécifiez la limite de taux de téléchargement. 0 signifie illimité.

Wep

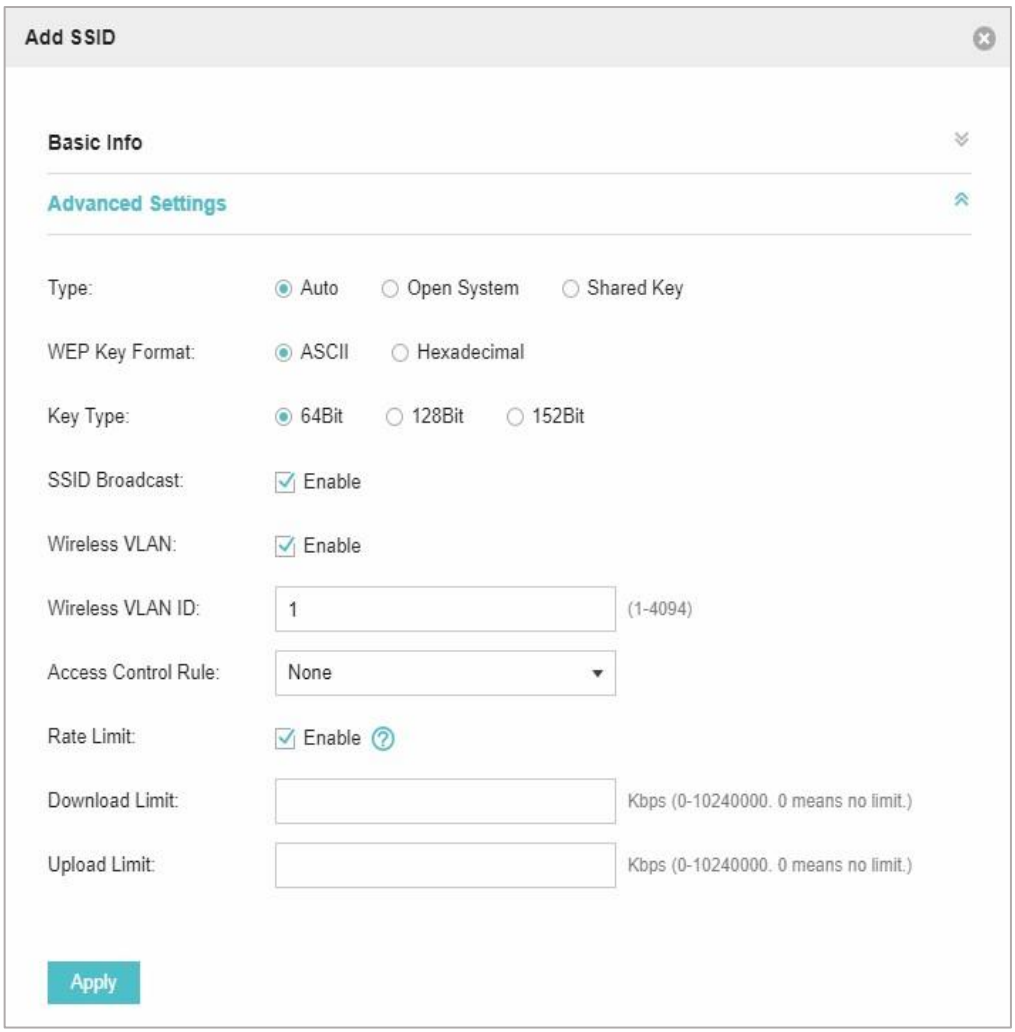
WEP est basé sur la norme IEEE 802.11 et moins sûr que WPA-Enterprise et WPA-PSK.

Notes

WEP n'est pas pris en charge en mode 802.11n ou mode 802.11ac. Si le WEP est appliqué en mode mixte 802.11n, 802.11 ac ou 802.11n/ac, les clients peuvent ne pas être en mesure d'accéder au réseau sans fil. Si le WEP est appliqué en mode 11b/g/n (2,4 GHz) ou 11a/n (5 GHz), le EAP peut fonctionner à un faible taux de transmission.

Clé sélectionnée	Sélectionnez une clé à spécifier. Vous pouvez configurer quatre touches tout au plus.
Valeur clé	Entrez les touches WEP. La longueur et les caractères valides sont affectés par le type de clé.

Configurez les paramètres avancés dans la fenêtre suivante.



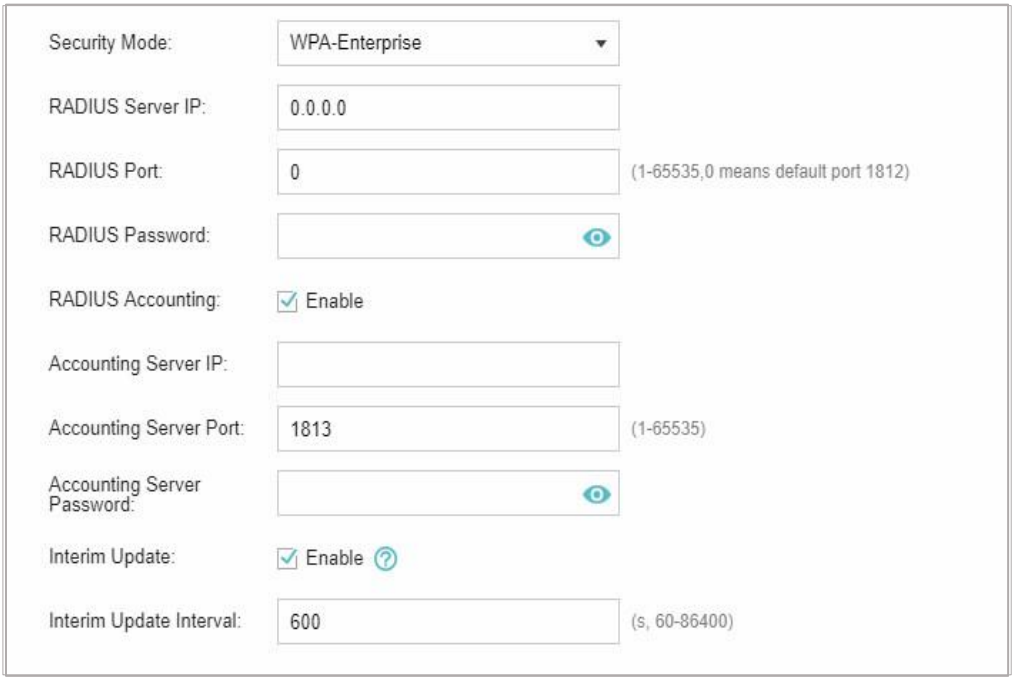
Type	Sélectionnez le type d'authentification pour WEP. Automatique : l'O200 peut sélectionner automatiquement Open System ou Shared Key en fonction de la capacité et de la demande de la station sans fil. Système d'ouverture : les clients peuvent passer l'authentification et s'associer au réseau sans fil sans mot de passe. Toutefois, un mot de passe correct est nécessaire pour la transmission de données. Clé partagée : les clients doivent entrer le mot de passe pour passer l'authentification, sinon il ne peut pas s'associer au réseau sans fil ou transmettre des données.
Format de clé WEP	Sélectionnez ASCII ou Hexadécimal comme format de clé WEP. ASCII : Le format ASCII représente toute combinaison de caractères clavier de la longueur spécifiée. Hexadécimal : Le format hexadécimal représente n'importe quelle combinaison de chiffres hexadécimales (0-9, a-f, A-F) avec la longueur spécifiée.

Type de clé	Sélectionnez la longueur de la clé WEP pour le chiffrement. 64Bit : Entrez 10 chiffres hexadécimaux ou 5 caractères ASCII. 128Bit : Entrez 26 chiffres hexadécimaux ou 13 caractères ASCII. 152Bit : Entrez 32 chiffres hexadécimaux ou 16 caractères ASCII.
Valeur clé	Entrez les touches WEP. La longueur et les caractères valides sont affectés par le type de clé.
Diffusion SSID	Avec l'option activée, les EAP diffuseront le SSID aux hôtes voisins, afin que ces hôtes puissent trouver le réseau sans fil identifié par ce SSID. Si cette option est désactivée, les utilisateurs doivent saisir le SSID manuellement pour se connecter au EAP. L'option est activée par défaut.
VLAN sans fil	Avec cette option activée, le EAP peut travailler de plus en plus avec les commutateurs prenant en charge 802.1Q VLAN. Le trafic des clients dans différents réseaux sans fil est ajouté avec différentes balises VLAN en fonction des paramètres VLAN des réseaux sans fil. Ensuite, les clients sans fil dans différents VLAN ne peuvent pas communiquer directement les uns avec les autres. Pour définir un VLAN sans fil pour le réseau sans fil, activez l'option et définissez un ID VLAN dans l'ID VLAN sans fil.
ID VLAN sans fil	Entrez un ID VLAN pour le VLAN sans fil. Les réseaux sans fil avec le même ID VLAN sont regroupés sur un VLAN. La valeur varie de **1 à 4094.**
Contrôle d'accès Règle	Sélectionnez une règle de contrôle d'accès pour ce SSID. Pour plus d'informations, reportez-vous au contrôle d'accès.
Limite de taux	Avec cette option activée, le taux de téléchargement et de téléchargement de chaque client qui se connecte au SSID sera limité à l'utilisation de la bande passante d'équilibre. Vous pouvez limiter le taux de téléchargement et de téléchargement pour certains clients spécifiques en configurant la limite de taux dans la liste des clients, reportez-vous à Gérer les clients dans la colonne Action pour obtenir plus de détails. Notez que le taux de téléchargement et de téléchargement sera limité au minimum de la valeur configurée en configuration SSID, client et portail.
Limite de téléchargement	Avec la limite de taux activée, spécifiez la limite de taux de téléchargement. 0 signifie illimité.

WPA-Entreprise

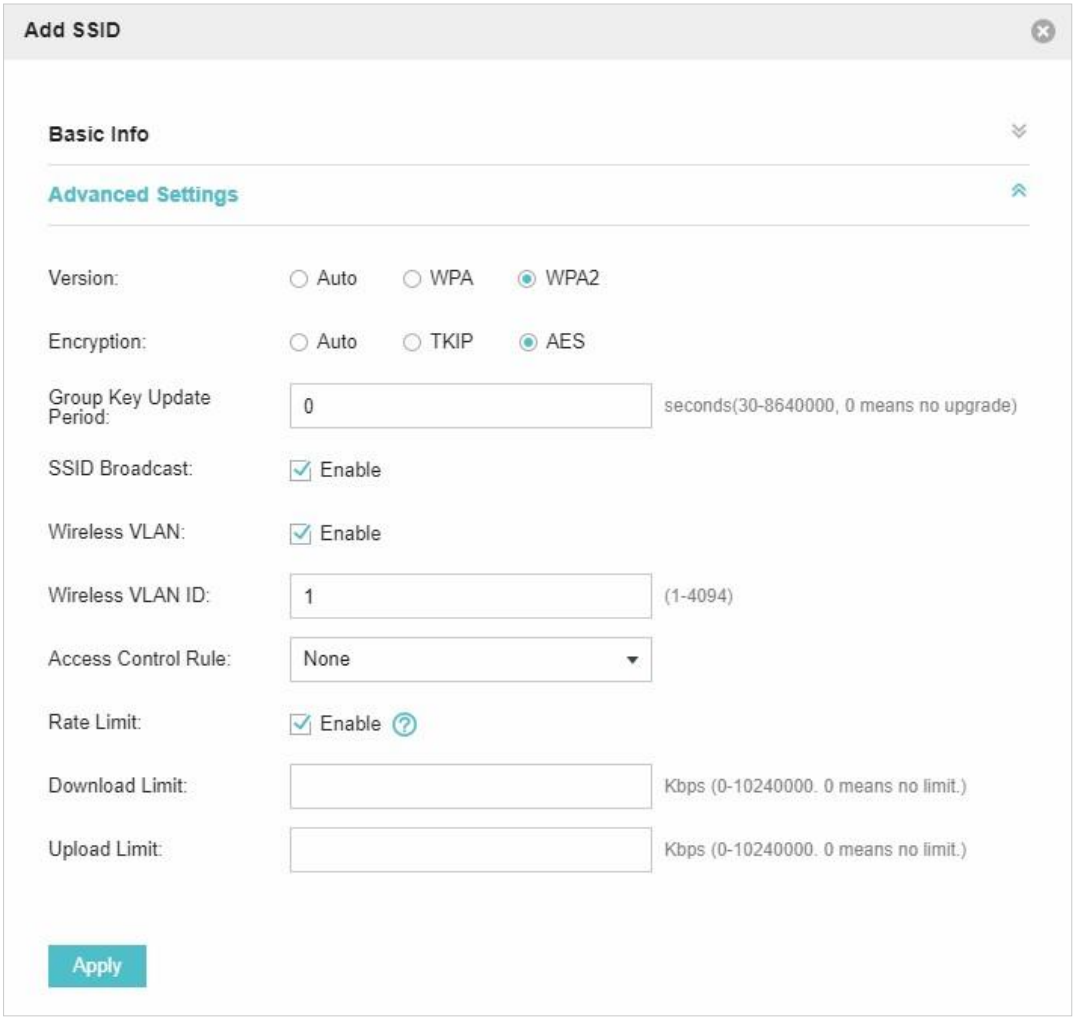
Le mode WPA-Enterprise nécessite un serveur RADIUS pour authentifier les clients. Étant donné que la WPA Enterprise peut générer différents mots de passe pour différents clients, il est beaucoup plus sûr que WPA-PSK.

Cependant, il coûte beaucoup plus cher à entretenir et est généralement utilisé par l'entreprise.



RADIUS Server IP	Entrez l'adresse IP du serveur RADIUS.
RADIUS Port	Entrez le numéro de port du serveur RADIUS.
Mot de passe RADIUS	Entrez la clé secrète partagée du serveur RADIUS.
Radius Accounting	Activer ou désactiver la fonctionnalité de comptabilité RADIUS.
IP du serveur comptable	Entrez l'adresse IP du serveur comptable.
Serveur comptable Port	Entrez le numéro de port du serveur comptable.
Serveur comptable mot de passe	Entrez la clé secrète partagée du serveur comptable.
Mise à jour provisoire	Avec cette option activée, vous pouvez spécifier la durée entre les mises à jour d'informations comptables. Par défaut, la fonction est désactivée. Entrez la durée appropriée entre les mises à jour pour les EAP dans l'intervalle de mise à jour intérimaire.
Mise à jour provisoire Intervalle	Avec mise à jour intérimaire activée, spécifiez la durée appropriée entre les mises à jour pour les EAP. La durée par défaut est de 600 secondes.

Configurez les paramètres avancés dans la fenêtre suivante.



Version	Sélectionnez la version WPA-Enterprise. Auto : le EAP choisira automatiquement la version utilisée par chaque périphérique client. WPA/WPA2 : Deux versions de l'accès protégé wi-fi.
Cryptage	Sélectionnez le type de chiffrement. Auto : le paramètre par défaut est automatique et le EAP sélectionnera TKIP ou AES automatiquement en fonction de la demande du périphérique client. TKIP : Protocole d'intégrité des clés temporelles. TKIP n'est pas pris en charge en mode 802.11n, mode 802.11ac ou 802.11n/ac mode mixte. Si TKIP est appliqué en mode mixte 802.11n, 802.11 ac ou 802.11n/ac, les clients peuvent ne pas être en mesure d'accéder au réseau sans fil du EAP. Si le TKIP est appliqué en mode 11b/g/n (2,4 GHz) ou en mode 11a/n (5 GHz), l'appareil peut fonctionner à un faible taux de transmission. AES : Norme de chiffrement avancée. Nous vous recommandons de sélectionner AES comme type de chiffrement car il est plus sécurisé que TKIP.

Mise à jour de la clé de groupe Période	Spécifiez une période de mise à jour de clé de groupe, qui indique au EAP la fréquence à laquelle il doit modifier les clés de chiffrement. La valeur peut être de 0 ou 30~8640000 secondes. 0 signifie pas de changement de la clé de chiffrement à tout moment.
Diffusion SSID	Avec l'option activée, les EAP diffuseront le SSID aux hôtes voisins, afin que ces hôtes puissent trouver le réseau sans fil identifié par ce SSID. Si cette option est désactivée, les utilisateurs doivent saisir le SSID manuellement pour se connecter au EAP. L'option est activée par défaut.
VLAN sans fil	Avec cette option activée, le EAP peut travailler de plus en plus avec les commutateurs prenant en charge 802.1Q VLAN. Le trafic des clients dans différents réseaux sans fil est ajouté avec différentes balises VLAN en fonction des paramètres VLAN des réseaux sans fil. Ensuite, les clients sans fil dans différents VLAN ne peuvent pas communiquer directement les uns avec les autres. Pour définir un VLAN sans fil pour le réseau sans fil, activez l'option et définissez un ID VLAN dans l'ID VLAN sans fil.
ID VLAN sans fil	Entrez un ID VLAN pour le VLAN sans fil. Les réseaux sans fil avec le même ID VLAN sont regroupés sur un VLAN. La valeur varie de 1 à 4094.
Règle de contrôle d'accès	Sélectionnez une règle de contrôle d'accès pour ce SSID. Pour plus d'informations, reportez-vous au contrôle d'accès.
Limite de taux	Avec cette option activée, le taux de téléchargement et de téléchargement de chaque client qui se connecte au SSID sera limité à l'utilisation de la bande passante d'équilibre. Vous pouvez limiter le taux de téléchargement et de téléchargement pour certains clients spécifiques en configurant la limite de taux dans la liste des clients, reportez-vous à Gérer les clients dans la colonne Action pour obtenir plus de détails. Notez que le taux de téléchargement et de téléchargement sera limité au minimum de la valeur configurée en configuration SSID, client et portail.
Limite de téléchargement	Avec la limite de taux activée, spécifiez la limite de taux de téléchargement. 0 signifie illimité.
Limite de téléchargement	Avec la limite de taux activée, spécifiez la limite de taux de téléchargement. 0 signifie illimité.

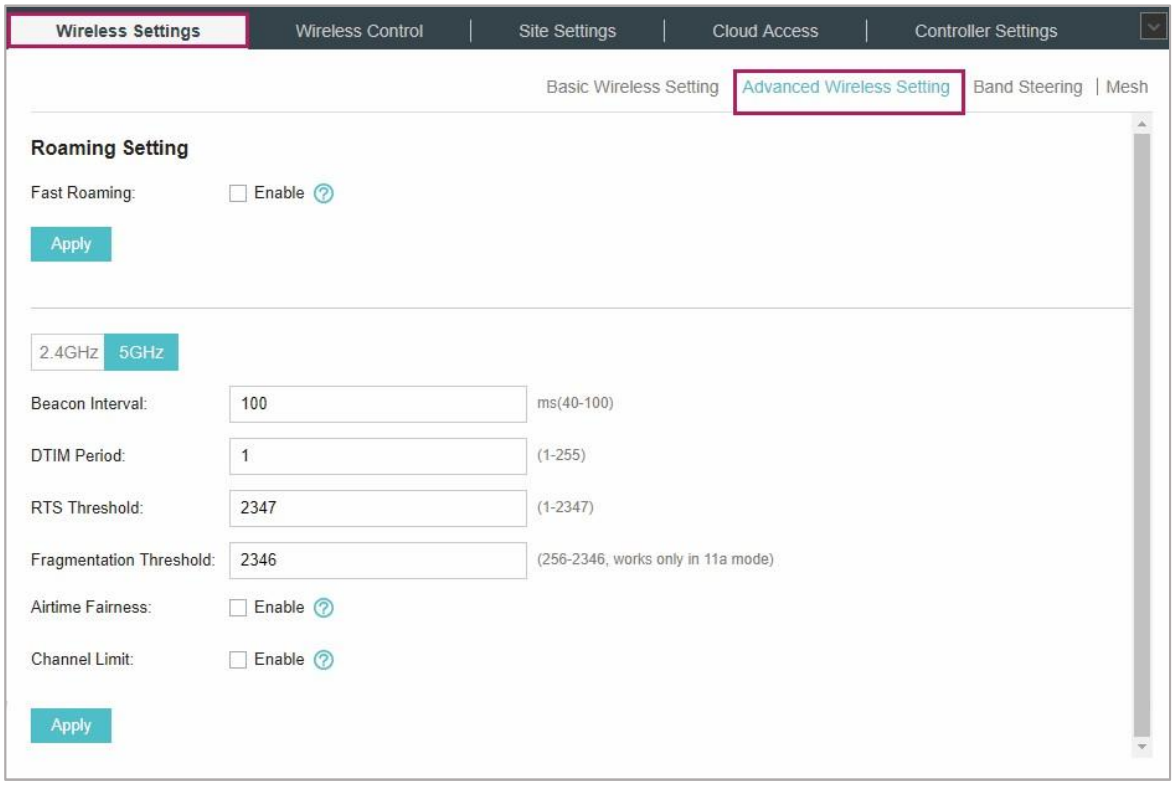
WPA-PSK

3.1.2 Configurer les paramètres sans fil avancés

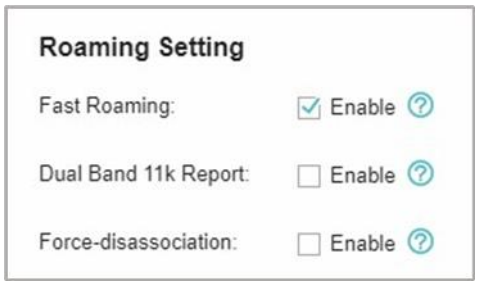
Des paramètres sans fil appropriés peuvent améliorer la stabilité, la fiabilité et l'efficacité de communication du réseau. Les paramètres sans fil avancés sont constitués d'itinérance rapide, d'intervalle de balise, de période DTIM, de seuil de RTS, de seuil de fragmentation et d'équité en temps d'antenne.

Pour configurer les paramètres sans fil avancés, procédez comme suit.

1. Accédez à Paramètres sans fil > Paramètre sans fil avancé.



2. Activez l'itinérance rapide et configurez les paramètres correspondants.



Itinérance rapide	Avec cette option activée, les clients capables de 11k/v peuvent avoir amélioré l'expérience d'itinérance rapide lors du déplacement entre différents AP.
Rapport Double Band 11k	Cette fonctionnalité étant désactivée, l'OC200 fournit un rapport AP candidat qui contient les AP dans la même bande que les clients. Avec cette fonctionnalité activée, l'OC200 fournit un rapport AP candidat qui contient les AP dans les bandes 2.4GHz et 5GHz.

Dissociation de la force	L'OC200 surveille dynamiquement la qualité des liens de chaque client associé. Lorsque la qualité de lien actuel du client descend en dessous du seuil prédéfini et qu'il y a d'autres AP avec un meilleur signal, l'AP actuel émet une suggestion d'itinérance 11v au client. Avec la dissociation de force désactivée, l'AP émet uniquement une suggestion d'itinérance, mais le client détermine si vous devez errer ou non. Avec force-dissociation activée, l'AP émet non seulement une suggestion d'itinérance, mais dissocie également le client après un certain temps. Ainsi, le client est pris en charge pour se réassocier à un meilleur AP. Cette fonction est recommandée lorsqu'il y a des clients collants qui n'errent pas.

3. Cliquez sur Appliquer.
4. Sélectionnez la fréquence de la bande 

.

5. Configurer les paramètres suivants.

Intervalle de balise	Les balises sont transmises périodiquement par le EAP pour annoncer la présence d'un réseau sans fil pour les clients. La valeur De l'intervalle de balise détermine l'intervalle de temps des balises envoyées par l'appareil. Vous pouvez spécifier une valeur comprise entre 40 et 100 m. La valeur par défaut est de 100ms.
Période DTIM	Le DTIM (Message d'indication de trafic de livraison) est contenu dans certains cadres Beacon. Il indique si le EAP a tamponné les données pour les périphériques clients. La période DTIM indique à quelle fréquence les clients desservis par ce EAP devraient vérifier les données tamponnées qui sont toujours sur le EAP en attente de ramassage. Vous pouvez spécifier la valeur entre 1-255 intervalles de balise. La valeur par défaut est 1, indiquant aux clients de vérifier les données tamponnées sur le EAP à chaque balise. Un intervalle DTIM excessif peut réduire les performances des applications multidiffusion, nous vous recommandons donc de le conserver par défaut.
Seuil RTS	RTS (Demande d'envoi) peut assurer une transmission efficace des données. Lorsque RTS est activé, le client enverra un paquet RTS au EAP pour informer qu'il enverra des données avant d'envoyer des paquets. Après avoir reçu le paquet RTS, le EAP avise d'autres clients dans le même réseau sans fil de retarder leur transmission des données et informe le client demandeur d'envoyer des données, évitant ainsi le conflit de paquet. Si la taille du paquet est supérieure au seuil RTS, le mécanisme RTS sera activé. Si vous spécifiez une valeur seuil faible, les paquets RTS sont envoyés plus fréquemment et aident le réseau à récupérer des interférences ou des collisions qui peuvent se produire sur un réseau occupé. Cependant, il consomme également plus de bande passante et réduit le débit du paquet. Nous vous recommandons de le conserver par défaut. La valeur recommandée et par défaut est 2347.

Fragmentation Seuil	La fonction de fragmentation peut limiter la taille des paquets transmis sur le réseau. Si un paquet dépasse le seuil de fragmentation, la fonction de fragmentation est activée et le paquet sera fragmenté en plusieurs paquets. 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 causées par le travail supplémentaire de division et de remontage des cadres et l'augmentation du trafic de messages. La valeur recommandée et par défaut est de 2346 octets.
Équité du temps d'antenne	Grâce à cette option activée, chaque client qui se connecte au EAP peut obtenir le même temps pour transmettre des données, évitant ainsi aux clients à faible débit d'occuper une trop grande bande passante réseau et améliorant le débit du réseau. Nous vous recommandons d'activer cette fonction sous des réseaux sans fil multi-taux.
Limite de canal	Pour les **EAP qui soutiennent le DFS*** en version UE, il existe une option De limite de canal. Grâce à cette option activée, les EAP extérieurs n'utiliseront pas la plage de fréquences 5150MHz-5350MHz pour respecter les lois locales et les limites réglementaires dans les États membres de l'UE et l'AELE.

6. Cliquez sur Appliquer.

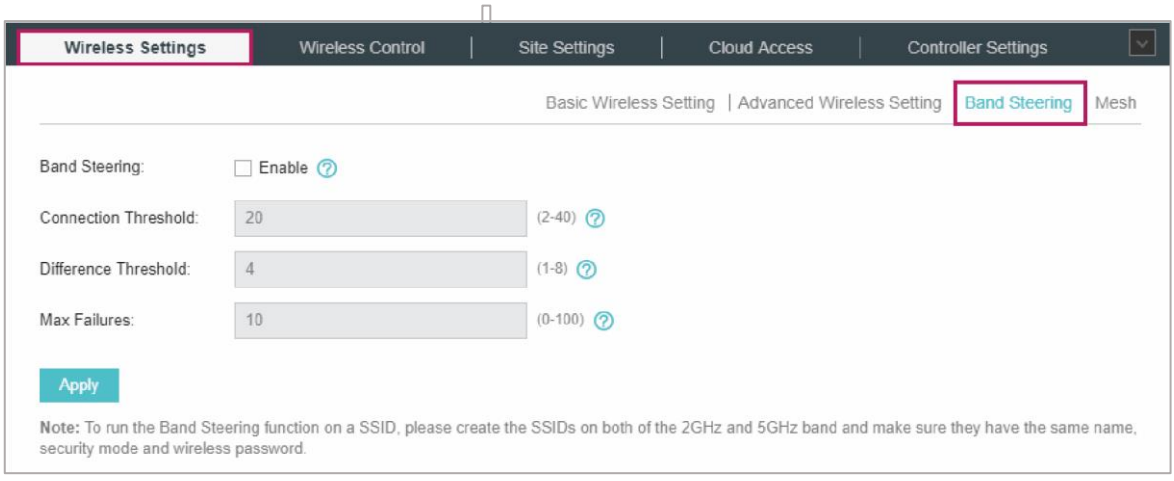
3.1.3 Configurer la direction de bande

Un appareil client qui peut communiquer sur les bandes de fréquences 2,4 GHz et 5 GHz se connecte généralement à la bande de 2,4 GHz. Toutefois, si trop d'appareils clients sont connectés à un EAP sur la bande de 2,4 GHz, l'efficacité de la communication sera diminuée.

Band Steering peut orienter les clients à double bande vers la bande de fréquences 5GHz qui prend en charge des taux de transmission plus élevés et plus d'appareils clients, et donc d'améliorer considérablement la qualité du réseau.

Pour configurer la direction de bande, suivez les étapes ci-dessous.

1 . Aller dans Paramètres sans fil > Direction



2. Cochez la case pour activer la fonction De direction de bande.

3. Configurez les paramètres suivants pour équilibrer les clients sur les deux bandes de fréquences :

Seuil de connexion/ Seuil de différence	Seuil de connexion définit le nombre maximal de clients connectés à la bande 5GHz. La valeur du seuil de connexion est de 2 à 40, et la valeur par défaut est de 20. Seuil de différence définit la différence maximale entre le nombre de clients sur la bande 5GHz et la bande de 2,4 GHz. La valeur du seuil de différence est de 1 à 8, et la valeur par défaut est 4. Lorsque les deux conditions suivantes sont remplies, le EAP préfère refuser la demande de connexion sur la bande 5GHz et ne dirige plus les autres clients vers la bande 5GHz : 1. Le nombre de clients de la bande 5GHz atteint la valeur Seuil de connexion. 2. La différence entre le nombre de clients de la bande 2,4 GHz et de la bande 5GHz atteint la valeur seuil de différence.
Pannes maximales	Si un client tente à plusieurs reprises de s'associer au EAP sur la bande 5GHz et que le nombre de rejets atteint la valeur des défaillances maximales, le EAP acceptera la demande. La valeur est de 0 à 100, et la valeur par défaut est 10.

4. Cliquez sur Appliquer.

3.1.4 Configurer le maillage

Mesh est utilisé pour établir un réseau sans fil ou développer un réseau câblé par connexion sans fil sur la bande radio 5GHz. 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 OC200 de la même manière que les EAP câblés. Pendant ce temps, en raison de la capacité de s'autoorganiser et d'autoconfigurer, maillage peut également réduire efficacement la configuration au-dessus.

Notes

- Seuls les EAP avec firmware spécifique sont disponibles pour la fonction de maillage, y compris EAP225-Outdoor_1.0 avec la version firmware 1.3.0 ou plus et EAP225_3.0 avec la version firmware 2.5.0 ou plus.
- Seuls les EAP du même site peuvent établir un réseau de maillage.

Pour comprendre comment le maillage peut être utilisé, les termes suivants utilisés dans OC200 seront introduits :

■ **Root AP** : L'AP est géré par OC200 avec une connexion de données câblée qui peut être configurée pour relayer des données vers et depuis les AP mesh (**Downlink AP**).

■ **Ap isolé** : Lorsque le EAP qui a été géré auparavant par OC200 se connecte au réseau sans fil et ne peut pas atteindre la passerelle, il entre dans l'état isolé.

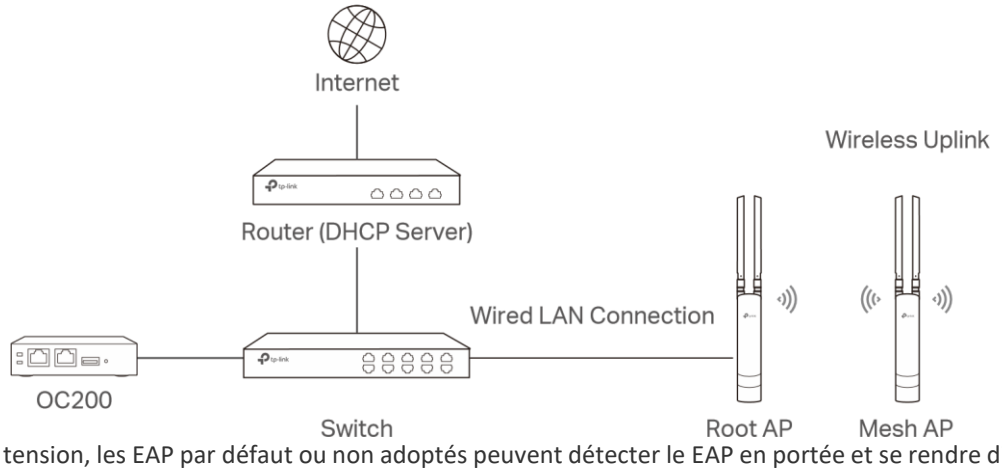
■ **Mesh AP** : Un AP isolé sera un maillage AP après avoir établi une connexion sans fil à l'AP avec accès réseau.

■ **Uplink AP/Downlink AP :** Parmi les AP maillage, l'AP qui offre la connexion sans fil pour d'autres AP est **Uplink AP.** Un AP racine ou un AP intermédiaire peut être l'A**P 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.

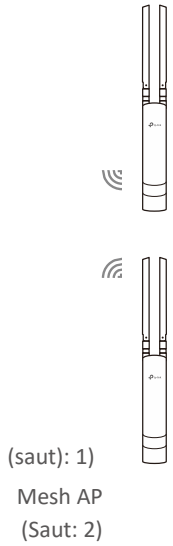
■ **Liaison vers le haut sans fil** : action qu'un **AP Downlink** connecte au lien vers le haut de l'action AP.

■ **Saut** : dans un déploiement qui utilise un AP racine et plus d'un niveau de liaison vers le haut sans fil avec les AP intermédiaires, les niveaux de liaison vers le haut peuvent être mentionnés par racine, premier saut, deuxième saut et ainsi de suite. Le houblon ne peut pas être plus de 3.

Dans un réseau de maillage de base comme indiqué ci-dessous, il existe un AP racine qui est connecté par le câble Ethernet, tandis que d'autres AP isolés n'ont pas de connexion de données câblées. Mesh permet aux AP isolés de communiquer avec l'AP racine préconfigurée sur le réseau. Une fois mis sous



tension, les EAP par défaut ou non adoptés peuvent détecter le EAP en portée et se rendre disponible pour adoption au sein de l'OC200.



Une fois que tous les EAP ont été adoptés, un réseau de mailles est établi. Ensuite, les EAP connectés au réseau sans fil peuvent également diffuser des SSID et relayer le trafic réseau vers et depuis le réseau via l'AP uplink.

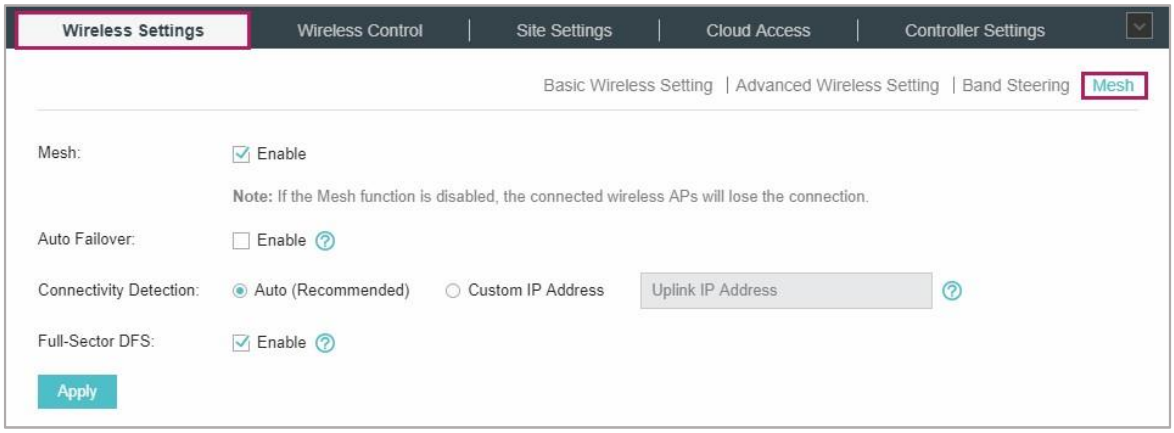
Pour établir un réseau de maillage, suivez les étapes ci-dessous.

■ Activer la fonction Mesh.

■ Adoptez l'AP racine.

■ Configurer le lien d'accès sans fil en adoptant des AP en attente (sans fil) ou dans un statut isolé.

1. Accédez à Paramètres sans fil > Mesh.



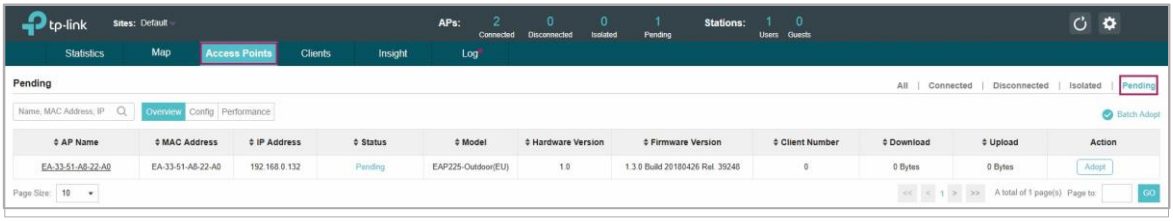
2. Cochez la case pour activer la fonction Mesh.

3. Configurez les paramètres suivants pour maintenir le réseau de maillage :

Basculement automatique	Activer ou désactiver le basculement automatique. Le basculement automatique est utilisé pour l'OC200 pour maintenir automatiquement le réseau de maillage. Avec cette fonctionnalité activée, l'OC200 peut sélectionner automatiquement un AP de liaison vers le haut pour le EAP isolé afin d'établir un lien vers le haut sans fil. Ainsi, l'OC200 sélectionnera automatiquement un nouvel AP de liaison uplink pour les EAP de maille lorsque le lien d'origine échoue.
Détection de connectivité	Spécifiez la méthode de détection de connexion. 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. Automatique (recommandé) : sélectionnez cette méthode et les AP de maillage enverront des paquets de demande ARP à la passerelle par défaut pour la détection. Adresse IP personnalisée : 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.
DFS secteur complet	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.

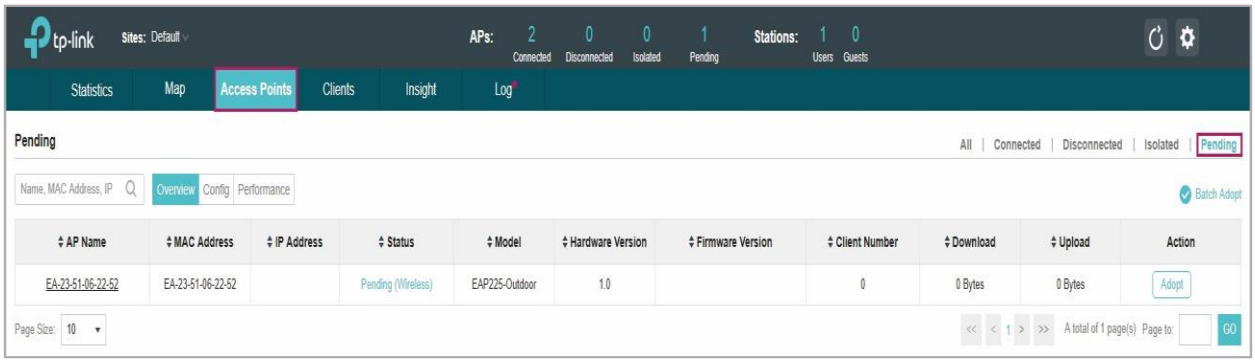
4. Cliquez sur Appliquer.

5. Accédez aux points d'accès > En attente et adoptez l'AP racine. Ensuite, l'état de l'AP racine se transformera en Connecté.



6. Installez le EAP qui reliera l'AP racine sans fil. Assurez-vous que l'emplacement prévu se trouve dans la plage de Root AP. Les EAP qui attendent Wireless Uplink incluent deux cas : les EAP par défaut d'usine et les EAP qui ont été gérés par OC200 auparavant.

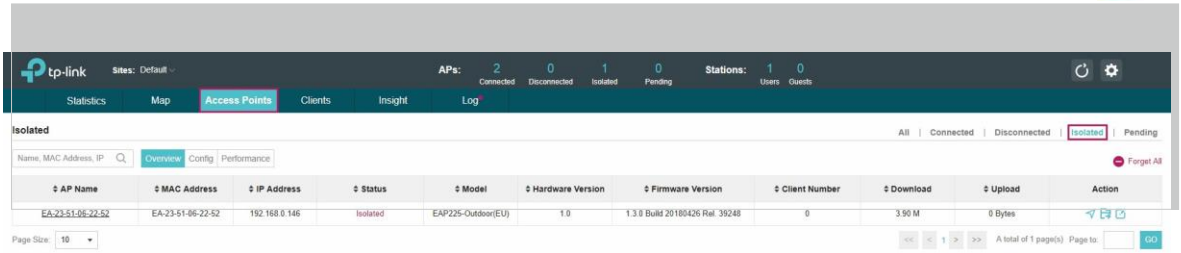
   1) Pour le EAP par défaut de l'usine, après mise sous tension sur l'appareil, le EAP sera en attente (sans fil). Accédez aux points d'accès > En attente et adoptez l'état EAP en attente (sans fil).



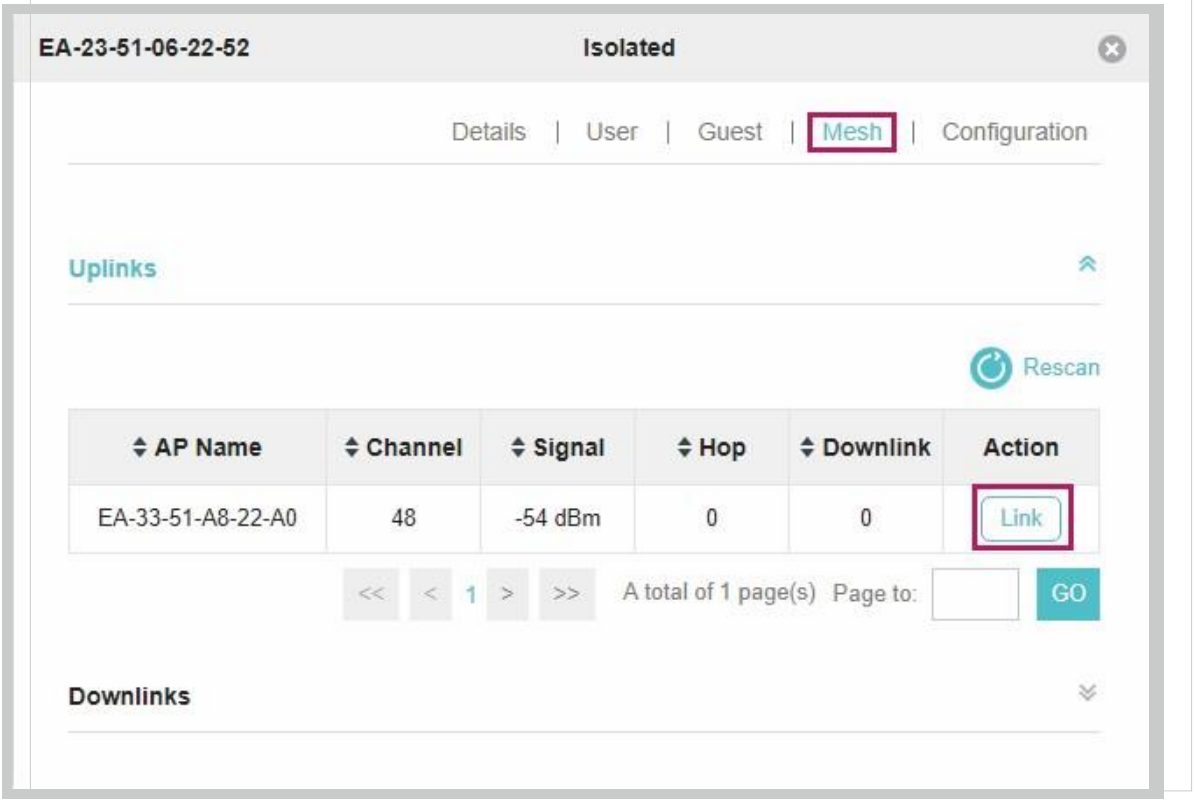
Après le début de l'adoption, le statut du EAP en attente (sans fil) deviendra adopté (sans fil) puis connecté (sans fil). Il devrait prendre environ 2 minutes pour apparaître connecté (sans fil) dans votre OC200.

2) Pour le EAP qui a été géré par OC200 auparavant et qui ne peut pas atteindre la passerelle, il

Statut isolé : quand ‘il est découvert à nouveau. Aller à **Points d’accès > Isolated** , cliquez 



La Page suivante s’affiche, pour le Mesh , puis cliquez Link Pour connecter l’AP Uplink.



Une fois l’adoption terminée, votre appareil peut être géré par l’OC200 de la même manière qu’un EAP câblé. Vous pouvez cliquer sur le nom du EAP sous l’onglet Points d’accès pour afficher et configurer les paramètres de maillage du EAP dans la fenêtre contextuelle. Veuillez consulter l’adresse pour voir les informations mesh du EAP.

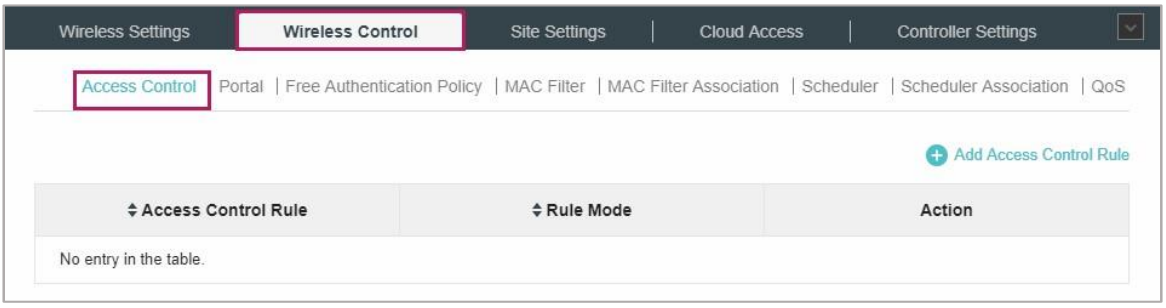
Conseils :

- Vous pouvez sélectionner manuellement l’AP de liaison uplink que vous souhaitez connecter dans la liste EAP de liaison vers le haut. Pour créer un réseau de maillage avec de meilleures performances, nous vous recommandons de sélectionner l’AP Uplink avec le signal le plus fort, le moins de saut et moins Downlink AP.
- Vous pouvez activer le basculement automatique pour que l’OC200 sélectionne automatiquement un AP de liaison vers le haut pour le EAP isolé afin d’établir un lien d’accès sans fil. Et l’OC200 sélectionnera automatiquement un nouvel AP de liaison uplink pour les EAP de maille lorsque le lien d’ouverture d’origine échoue.

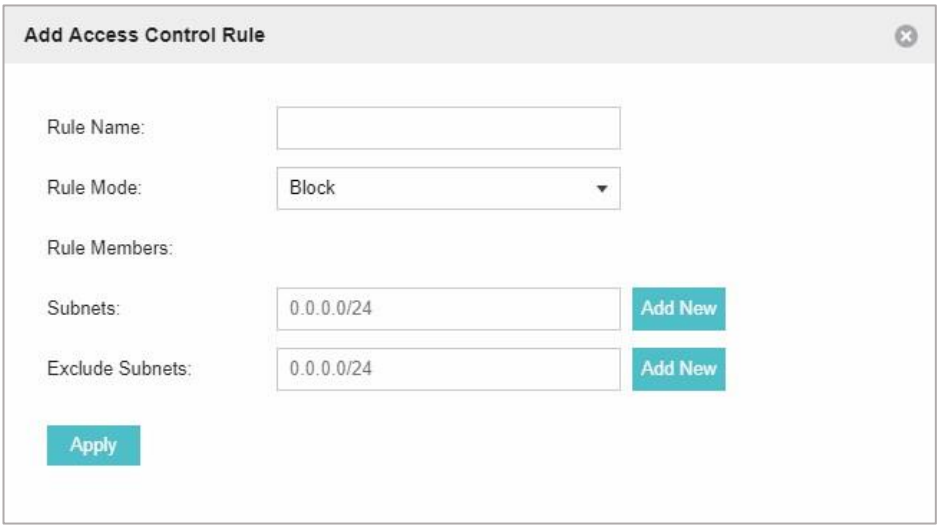
3.2 Contrôle d’accès

Access Control est utilisé pour bloquer ou permettre aux clients d’accéder à des sous-réseaux spécifiques. Pour configurer les règles de contrôle d’accès, suivez les étapes ci-dessous.

1. Aller à Contrôle sans fil > Contrôle d’accès.



2. Cliquez sur Add Access Control Rule Et Ajouter une nouvelle règle de contrôle d’accès .



. 3 Configuration des règles de connexions

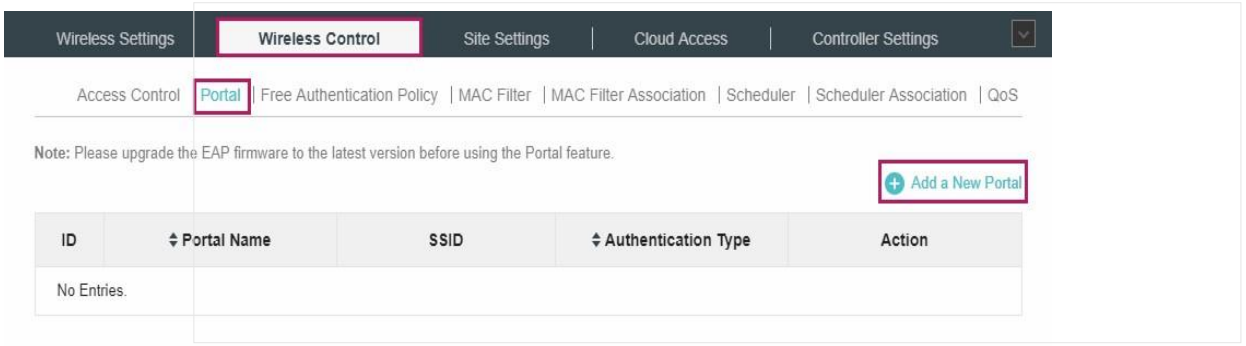
Nom de la règle	Spécifiez un nom pour cette règle.
Mode règle	Sélectionnez le mode de cette règle. Bloquer : sélectionnez ce mode pour bloquer les clients pour accéder aux sous-réseaux spécifiques. Autoriser : sélectionnez ce mode pour permettre aux clients d’accéder aux sous-réseaux spécifiques.
Membres de la règle	Spécifiez les sous-réseaux de membres pour cette règle. Sous-réseaux : entrez le sous-réseau qui suivra le mode règle au format X.X.X.X/X et cliquez sur. Add New Jusqu’à 16 sous-réseaux peuvent être ajoutés. Sauf sous-réseaux : entrez le sous-réseau excepté au format X.X.X.X/X et cliquez sur Add New. Jusqu’à 16 sous-réseaux peuvent être ajoutés. Le mode règle ne s’applique pas au sous-réseau qui se trouve dans la liste Subnets et la liste Except Subnets.

4. Cliquez sur Appliquer.
5. Accédez à Paramètres sans fil > Paramètre sans fil de base et activer la fonction Contrôle d'accès d'un SSID sélectionné.

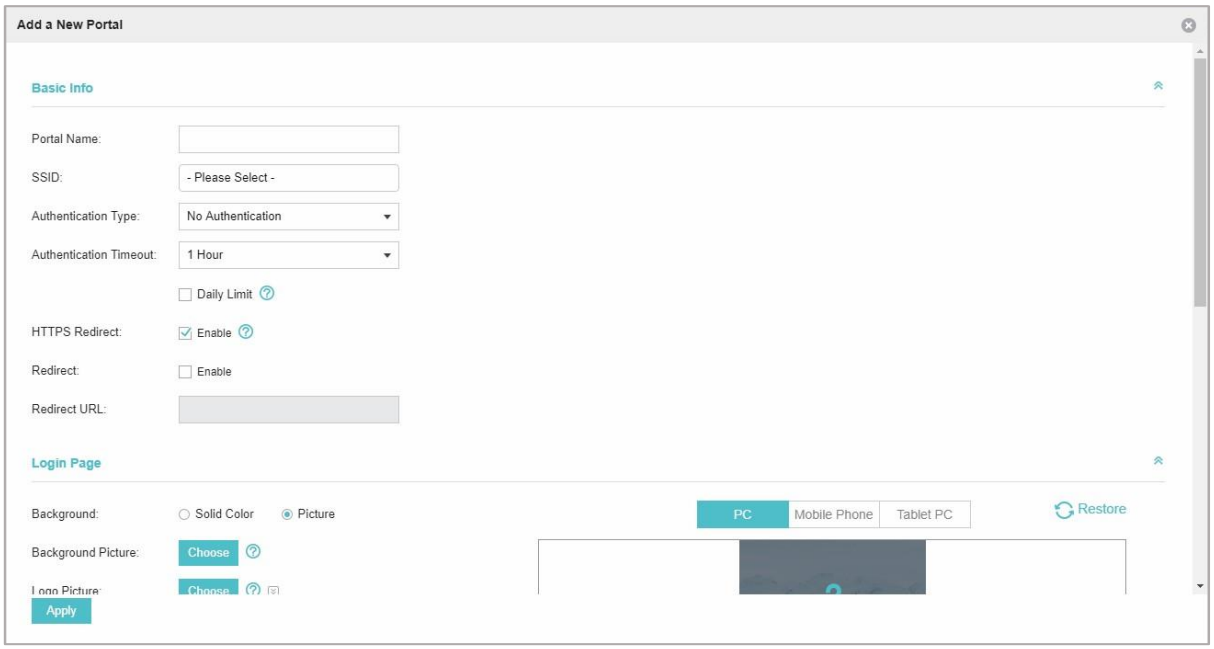
3.3 Authentification du portail

L'authentification du portail améliore la sécurité du réseau en fournissant un service d'authentification aux clients qui n'ont besoin que d'un accès temporaire au réseau sans fil. Ces clients doivent se connecter à une page Web pour établir la vérification, après quoi ils accéderont au réseau en tant qu'invités. De plus, vous pouvez personnaliser la page de connexion d'authentification et spécifier une URL vers laquelle les clients nouvellement authentifiés seront redirigés.

Configuration de l'authentification du portail, Sélectionnez Contrôle sans fil > Portail et sur Add a New Portal.



Fenêtre principale



Ces méthodes d'authentification sont disponibles : Pas d'authentification, Mot de passe simple, Utilisateur local, Bon d'achat, SMS, Facebook, Serveur RADIUS externe et serveur portail externe. Les sections suivantes introduisent comment configurer chaque authentification pour chaque portail.

3.3.1 Pas d'authentification

Sans authentification configurée, les clients peuvent accéder au réseau sans aucune authentification.

Procédez comme suit pour configurer Aucune authentification :

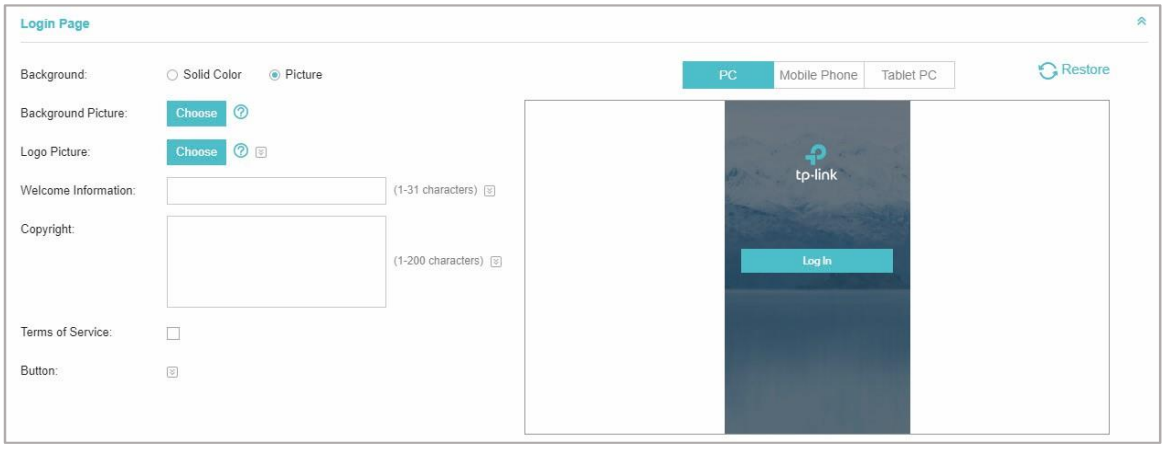
1. Accédez aux paramètres sans fil > Paramètres sans fil de base et créez un SSID pour le portail.
2. Retournez à la page de configuration du portail. Dans la section Informations de base, remplissez les paramètres de base de l'authentification du portail.

Configurer les paramètres suivants :

Nom du portail	Spécifiez un nom pour le portail.

SSID	Sélectionnez un SSID pour le portail.
Type d'authentification	Sélectionnez Aucune authentification.
Authentification Timeout	Avec la limite quotidienne désactivée, l'authentification du client expirera après la période que vous définissez et le client doit se connecter à nouveau sur la page d'authentification Web pour accéder au réseau. Les options incluent 1 heure, 8 heures, 24 heures, 7 jours et personnalisé. La coutume vous permet de définir l'heure en jours, heures et minutes. La valeur par défaut est d'une heure. Avec la limite quotidienne activée, l'authentification du client expirera après la période de temps que vous définissez et le client ne peut pas se connecter à nouveau dans la même journée. Les options incluent 30 minutes, 1 heure, 2 heures, 4 heures et personnalisée. La coutume vous permet de définir l'heure en heures et en minutes. La valeur par défaut est de 30 minutes.
Limite quotidienne	Avec Daily Limit activé, après les heures d'authentification, l'utilisateur ne peut pas se faire authentifier à nouveau dans la même journée.
Redirection HTTPS	Avec cette fonction activée, les clients non autorisés seront redirigés vers la page Portail lorsqu'ils tentent de parcourir les sites Web HTTPS. Cette fonction ayant été désactivée, les clients non autorisés ne peuvent pas parcourir les sites Web HTTPS et ne sont pas redirigés vers la page Portail.
Rediriger	Si vous activez cette fonction, le portail redirigera les clients nouvellement authentifiés vers l'URL configurée.
Rediriger l'URL	Si la fonction De redirection ci-dessus est activée, entrez l'URL vers laquelle un client nouvellement authentifié sera redirigé.

3. Dans la section Page de connexion, configurez la page de connexion du portail.



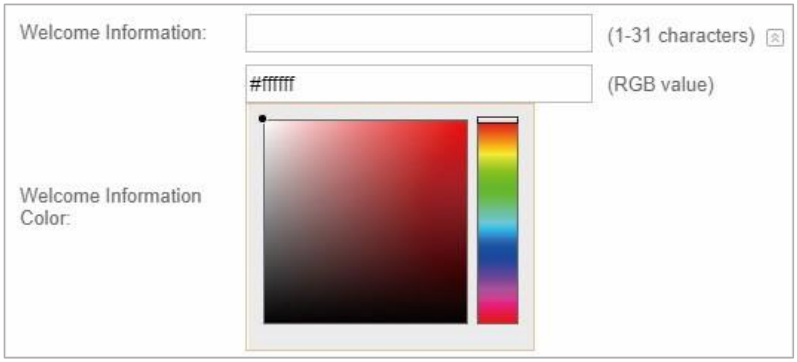
Configuration des paramètres du Portail

Fond	Sélectionnez le type d'arrière-plan. Deux types sont pris en charge : Couleur solide et image.
Couleur d'arrière-plan	Si **Solid Color** est sélectionné, configurez la couleur d'arrière-plan souhaitée via le sélecteur de couleurs ou en entrant manuellement la valeur RGB.
Image d'arrière-plan	Si l'image est sélectionnée, cliquez sur le bouton Choisir et sélectionnez une image à partir de votre PC. Faites glisser et mettre à l'échelle la zone de découpage pour modifier l'image, puis cliquez sur Confirmer.
Image du logo	Choisir sélectionnez une image à partir de votre PC. Faites glisser et mettre à l'échelle la zone de découpage pour modifier l'image, puis cliquez sur Confirmer. Dans addition, vous pouvez cliquer et configurer la position du logo. Les options incluent le moyen, le haut et le bas.

Informations de bienvenue Spécifiez les informations de bienvenue.

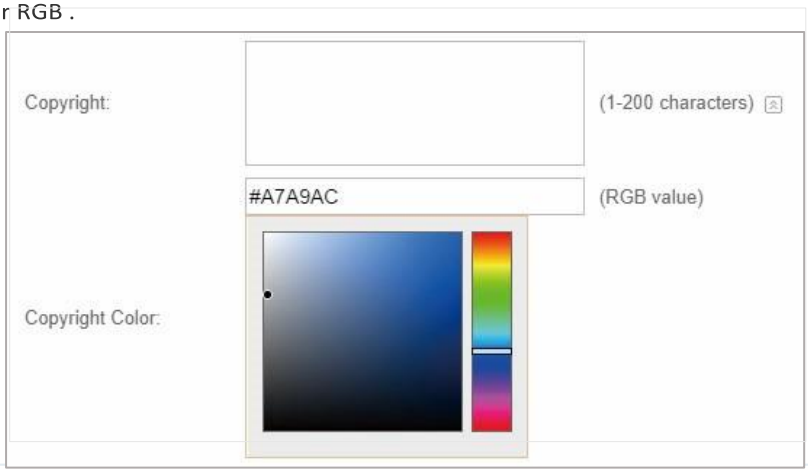
Dans addition, vous cliquez sur et choisir la couleur de texte

Editez les Informations de bienvenue en selectionneant la couleur ou en entrant la valeur RGB



Copyright Spécialistes les informations sur le droit

Dans addition, vous sur et la couleur de texte copier et éditer le Copyright Informations via le sélecteur de couleurs ou en entrant manuellement la valeur RGB .



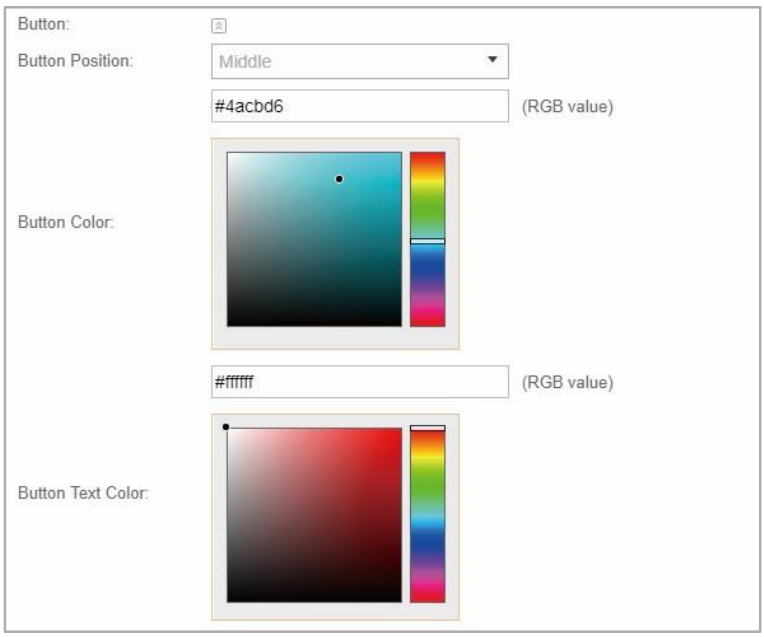
Conditions d'utilisation Activer ou désactiver les conditions d'utilisation. Avec cette option activée, spécifiez les conditions d'utilisation dans la zone suivante.

Bouton Cliquez et configurez le bouton.

Position du bouton : définissez la position du bouton de connexion. Les options incluent le moyen, le haut et le bas.

Couleur du bouton : sélectionnez la couleur du bouton de connexion souhaité par l'intermédiaire du sélecteur de couleurs ou en entrant manuellement la valeur RGB.

Couleur du texte du bouton : sélectionnez la couleur de texte souhaitée pour le bouton via le sélecteur de couleurs ou en entrant manuellement la valeur RGB.



4. Dans la section Publicité, sélectionnez afficher des images publicitaires pour les utilisateurs et configurer les paramètres connexes.

Configurer les paramètres personnalisés :

Publicité	Spécifier, s'il faut 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. Vous pouvez également autoriser les utilisateurs à ignorer la publicité en permettant aux utilisateurs de sauter la publicité. L'image publicitaire doit être inférieure à 2 Mo. Et seuls les types de fichiers JPG, PNG, BMP, GIF et JPEG sont pris en charge.
Ressource d'image	Téléchargez des photos publicitaires. Lorsque plusieurs images sont ajoutées, elles seront jouées en boucle.

Publicité Durée	Spécifiez la durée de l'affichage de la publicité. 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.
Carrousel d'images Intervalle	Spécifiez l'intervalle du 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.
Autoriser les utilisateurs à sauter Publicité	Spécifiez si vous devez activer cette fonctionnalité. Avec cette fonctionnalité activée, l'utilisateur peut cliquer sur le bouton Ignorer pour sauter la publicité.

5. Cliquez sur Appliquer.

3.3.2 Mot de passe simple

Avec ce mot de passe simple configuré, les clients sont tenus d'entrer le mot de passe correct pour passer l'authentification.

Procédez comme suit pour configurer le portail No Simple Password Portal :

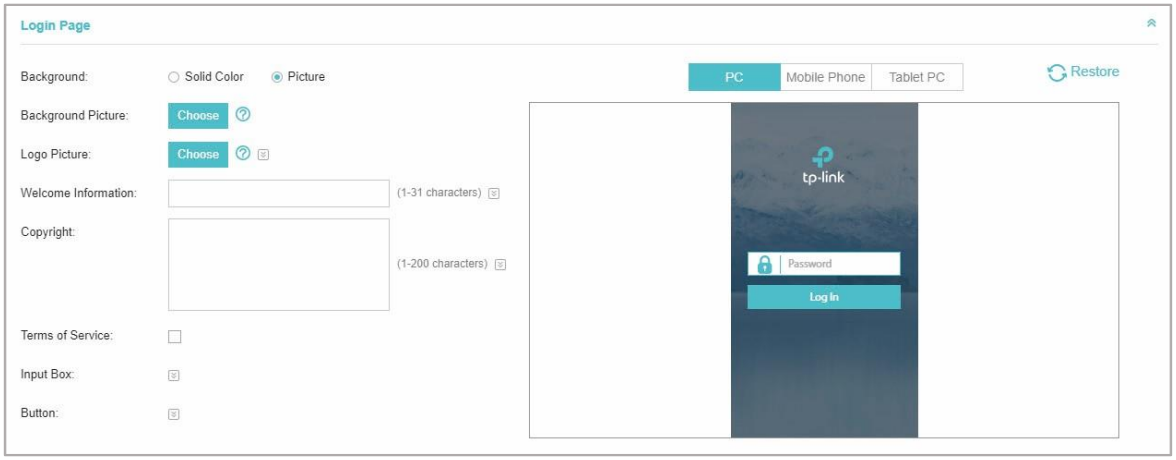
1. Accédez aux paramètres sans fil > Paramètres sans fil de base et créez un SSID pour le portail.
2. Retournez à la page de configuration du portail. Dans la section Informations de base, remplissez les paramètres de base de l'authentification du portail.

Configurer les paramètres suivants :

Nom du portail	Spécifiez un nom pour le portail.
SSID	Sélectionnez un SSID pour le portail.
Type d'authentification	Sélectionnez Mot de passe simple.
Mot de passe	Définissez le mot de passe pour l'authentification.

Authentification Timeout	L'authentification du client expirera après la période que vous avez définie et le client doit se connecter à nouveau sur la page d'authentification Web pour accéder au réseau. Les options incluent 1 heure, 8 heures, 24 heures, 7 jours et personnalisé. La coutume vous permet de définir l'heure en jours, heures et minutes. La valeur par défaut est d'une heure.
Redirection HTTPS	Avec cette fonction activée, les clients non autorisés seront redirigés vers la page Portail lorsqu'ils tentent de parcourir les sites Web HTTPS. Cette fonction ayant été désactivée, les clients non autorisés ne peuvent pas parcourir les sites Web HTTPS et ne sont pas redirigés vers la page Portail.
Rediriger	Si vous activez cette fonction, le portail redirigera les clients nouvellement authentifiés vers l'URL configurée.
Rediriger l'URL	Si la fonction De redirection ci-dessus est activée, entrez l'URL vers laquelle un client nouvellement authentifié sera redirigé.

3. Dans la section Page de connexion, configurez la page de connexion du portail.



Configurer les paramètres suivants :

Fond	Sélectionnez le type d'arrière-plan. Deux types sont pris en charge : Couleur solide et image.
Couleur d'arrière-plan	Si la couleur solide est sélectionnée, configurez la couleur d'arrière-plan souhaitée via le sélecteur de couleurs ou en entrant manuellement la valeur RGB.
Image d'arrière-plan	Si l'image est sélectionnée, cliquez sur le bouton Choisir et sélectionnez une image à partir de votre PC. Faites glisser et mettre à l'échelle la zone de découpage pour modifier l'image, puis cliquez sur Confirmer.
Image du logo	Cliquez sur le bouton Choisir et sélectionnez une image à partir de votre PC. Faites glisser et mettre à l'échelle la zone de découpage pour modifier l'image, puis cliquez sur Confirmer.

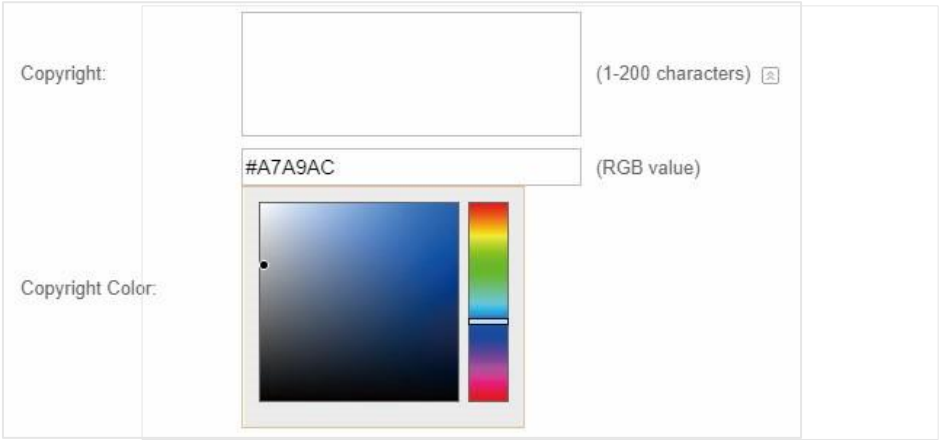
Dans addtion, vous sur et Configurateur la position du Logo. Les Options Inclure Moyen, Supérieur Inférieur .

Informations de bienvenue Spécifiez les informations de bienvenue.

Dans addition, vous cliquez sur Et la couleur de texte Informations de bienvenue via le sélecteur de couleurs ou en entrant la valeur RGB .

Copyright Spécifiez les informations sur le droit

Dans addition, vous pouvez cliquer sur et sélectionnez la couleur de texte souhaitée a le sélecteur de couleurs ou en entrant manuellement la valeur RGB.



Conditions d'utilisation Activer ou désactiver les conditions d'utilisation. Avec cette option activée, spécifiez les conditions d'utilisation dans la zone suivante.

Boîte Cliquez sur et Configurer la zone d'entrée.

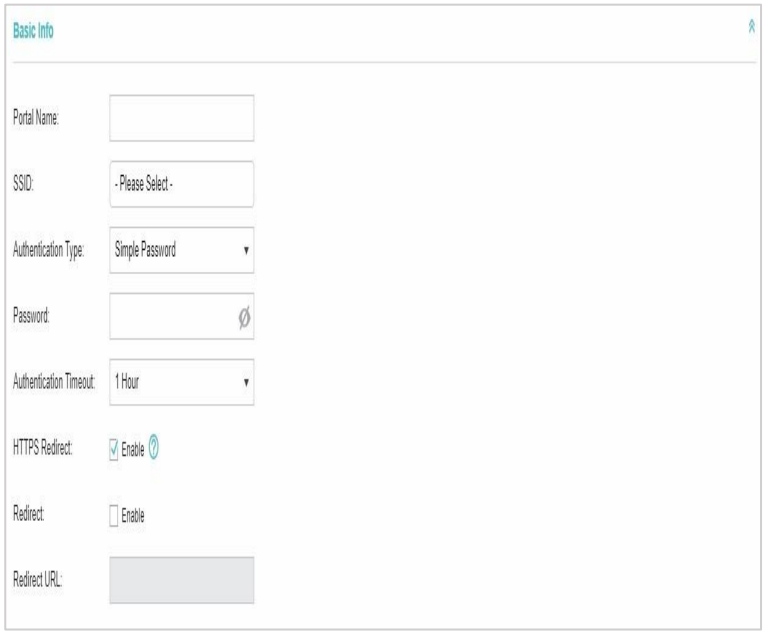
Sélectionnez la couleur souhaitée pour la zone d'entrée via le sélecteur de couleurs ou en entrant manuellement la valeur RGB.

Bouton Cliquez sur et configurer le bouton.

Position du bouton : définissez la position du bouton de connexion. Les options incluent le moyen, le haut et le bas.

Couleur du bouton : sélectionnez la couleur du bouton de connexion souhaité par l'intermédiaire du sélecteur de couleurs ou en entrant manuellement la valeur RGB.

Couleur du texte du bouton : sélectionnez la couleur de texte souhaitée pour le bouton via le sélecteur de couleurs ou en entrant manuellement la valeur R GB



4. Dans la section Publicité, sélectionnez afficher des images publicitaires pour les utilisateurs et configurer les paramètres connexes.

Configurer les paramètres :

Publicité	Spécifiez si l'option doit 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. Vous pouvez également autoriser les utilisateurs à ignorer la publicité en permettant aux utilisateurs de sauter la publicité. L'image publicitaire doit être inférieure à 2 Mo. Et seuls les types de fichiers JPG, PNG, BMP, GIF et JPEG sont pris en charge.
Ressource d'image	Téléchargez des photos publicitaires. Lorsque plusieurs images sont ajoutées, elles seront jouées en boucle.
Publicité Durée	Spécifiez la durée de l'affichage de la publicité. 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.
Carrousel d'images Intervalle	Spécifiez l'intervalle du 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.
Autoriser les utilisateurs à sauter Publicité	Spécifiez si vous devez activer cette fonctionnalité. Avec cette fonctionnalité activée, l'utilisateur peut cliquer sur le bouton Ignorer pour sauter la publicité.

5. Cliquez sur Appliquer.

3.3.3 Utilisateur local

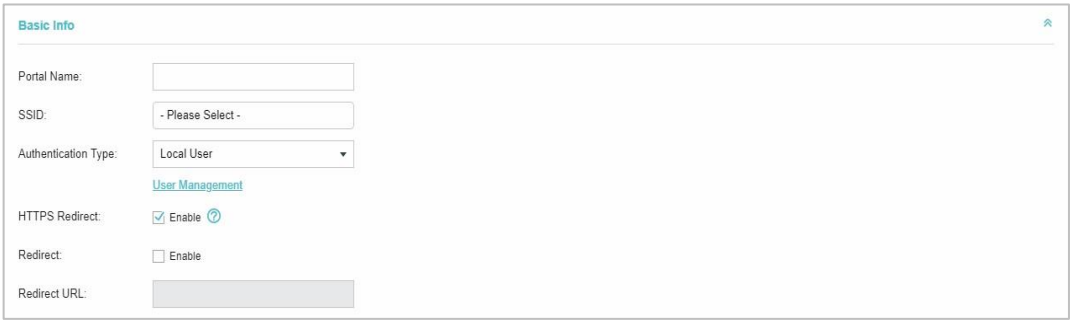
Avec cet utilisateur local configuré, les clients sont tenus d'entrer le nom d'utilisateur et le mot de passe corrects du compte de connexion pour passer l'authentification. Vous pouvez créer plusieurs comptes et affecter des comptes différents pour différents utilisateurs.

Configurer le portail utilisateur local

Procédez comme suit pour configurer le portail utilisateur local :

1. Accédez aux paramètres sans fil > Paramètres sans fil de base et créez un SSID pour le portail.

2. Retournez à la page de configuration du portail. Dans la section Informations de base, remplissez les paramètres de base de l'authentification du portail.



Configurer les paramètres suivants :

Nom du portail	Spécifiez un nom pour le portail.
SSID	Sélectionnez un SSID pour le portail.
Type d'authentification	Sélectionnez Utilisateur local.
Gestion des utilisateurs	Vous pouvez cliquer sur ce bouton pour configurer ultérieurement les comptes d'utilisateur pour l'authentification. Veuillez consulter Create Create Local User Accounts .
Redirection HTTPS	Avec cette fonction activée, les clients non autorisés seront redirigés vers la page Portail lorsqu'ils tentent de parcourir les sites Web HTTPS. Cette fonction ayant été désactivée, les clients non autorisés ne peuvent pas parcourir les sites Web HTTPS et ne sont pas redirigés vers la page Portail.
Rediriger	Si vous activez cette fonction, le portail redirigera les clients nouvellement authentifiés vers l'URL configurée.
Rediriger l'URL	Si la fonction De redirection ci-dessus est activée, entrez l'URL vers laquelle un client nouvellement authentifié sera redirigé.

3.

3. Dans la section Page de connexion, configurez la page de connexion du portail.

Configuration des paramètres :

Couleur d'arrière-plan	Si Solid Color est sélectionné, configurez la couleur d'arrière-plan souhaitée via le sélecteur de couleurs ou en entrant manuellement la valeur RGB.
Arrière-plan	Sélectionnez le type d'arrière-plan. Deux types sont pris en charge : Solid Color et image.
Image d'arrière-plan	Si l'image est sélectionnée, cliquez sur le bouton Choisir et sélectionnez une image à partir de votre PC. Faites glisser et mettre à l'échelle la zone de découpage pour modifier l'image, puis cliquez sur Confirmer.
Image du logo	Cliquez sur le bouton Choisir et sélectionnez une image à partir de votre PC. Faites glisser et mettre à l'échelle la zone de découpage pour modifier l'image, puis cliquez sur Confirmer.

Conditions d'utilisation Activer ou désactiver les conditions d'utilisation. Avec cette option activée, Spécifiez les conditions d'utilisation dans la zone suivante.

Boîte d'entrée Cliquez sur et configurer la zone d'entrée.

Sélectionnez la couleur souhaitée pour la zone d'entrée via le sélecteur de couleurs ou en entrant manuellement la valeur RGB.

4. Dans la section Publicité, sélectionnez afficher des images publicitaires pour les utilisateurs et configurer les paramètres connexes.

Configuration des paramètres :

Publicité	Spécifiez si l'option doit 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. Vous pouvez également autoriser les utilisateurs à ignorer la publicité en permettant aux utilisateurs de sauter la publicité. L'image publicitaire doit être inférieure à 2 Mo. Et seuls les types de fichiers JPG, PNG, BMP, GIF et JPEG sont pris en charge.
Ressource d'image	Téléchargez des photos publicitaires. Lorsque plusieurs images sont ajoutées, elles seront jouées en boucle.
Publicité Durée	Spécifiez la durée de l'affichage de la publicité. 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.
Carrousel d'images Intervalle	Spécifiez l'intervalle du 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.
Autoriser les utilisateurs à éviter lar Publicité	Spécifiez si vous devez activer cette fonctionnalité. Avec cette fonctionnalité activée, l'utilisateur peut cliquer sur le bouton Ignorer pour sauter la publicité.

5. Cliquez sur Appliquer.

Créer des comptes d’utilisateurs locaux

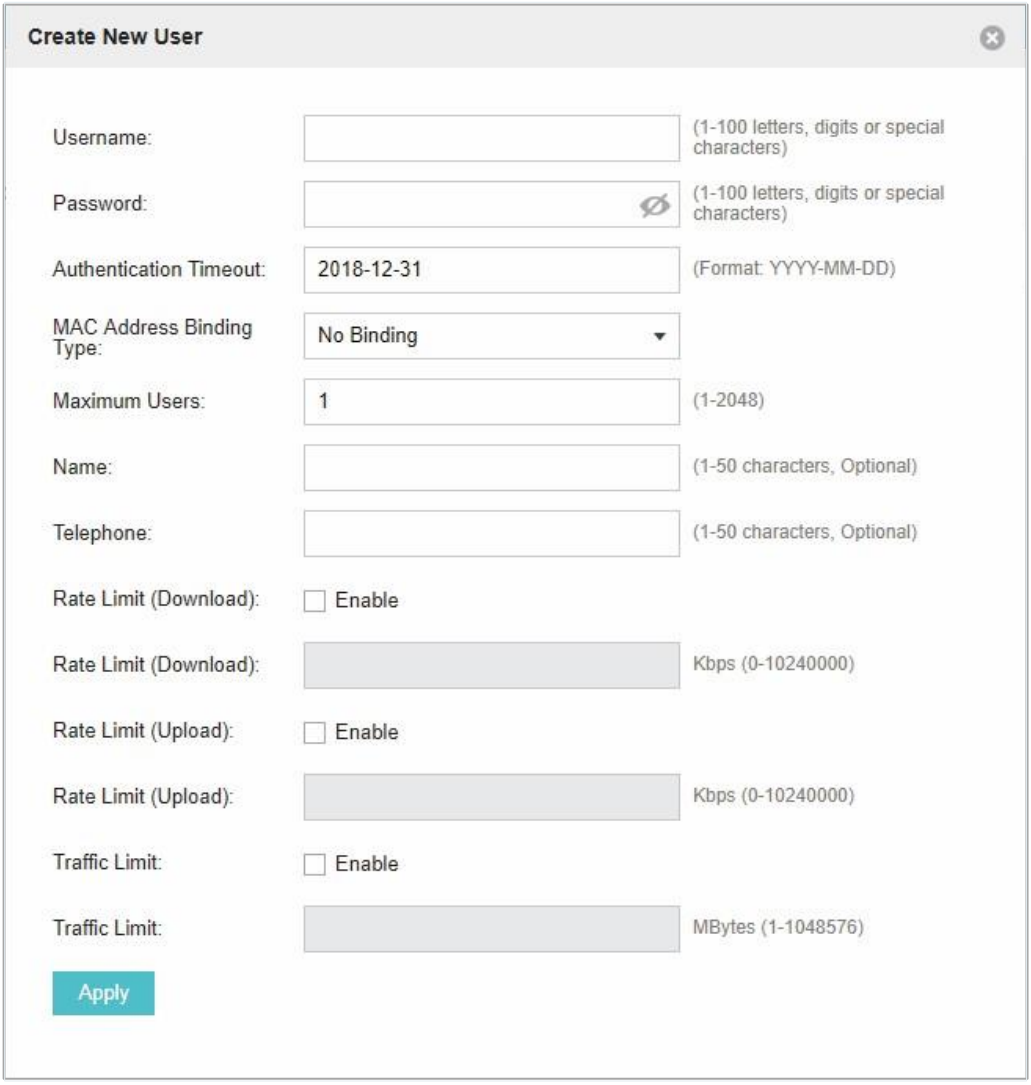
Procédez comme suit pour créer les comptes utilisateur pour l’authentification :

1. Dans la section Informations de base de la page de configuration du portail, cliquez sur Gestion des utilisateurs. Ou vous pouvez

Clique Sites: Default dans Hotspot Manager

Allez à la hotspot et cliquez sur Create User .

2. La fenêtre suivante apparaîtra. Configurez les paramètres requis et cliquez sur Appliquer.

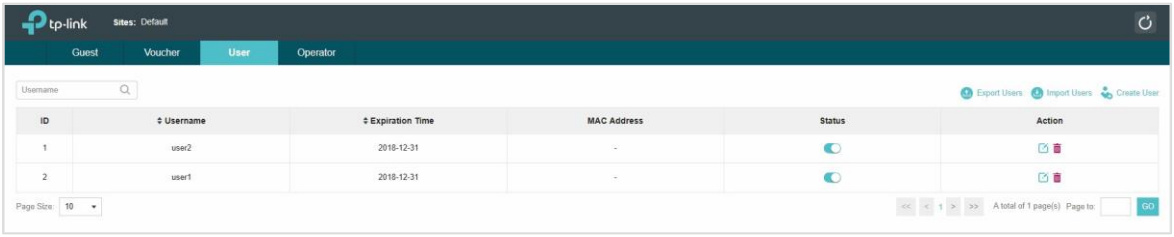


Configurer les paramètres suivants :

Nom d'utilisateur	Spécifiez le nom d'utilisateur. Le nom d'utilisateur ne doit pas être le même que celui existant.
Mot de passe	Spécifiez le mot de passe. Les utilisateurs devront entrer le nom d'utilisateur et le mot de passe lorsqu'ils tentent d'accéder au réseau.
Authentification Timeout	Spécifiez le délai d'authentification pour les utilisateurs formels. Après le délai d'expiration, les utilisateurs doivent se connecter à nouveau sur la page d'authentification Web pour accéder au réseau.
Liaison d'adresses MAC Type	Il existe trois types de liaison MAC : pas de liaison, de liaison statique et de liaison dynamique. Liaison statique : spécifiez une adresse MAC pour 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. Liaison dynamique : l'adresse MAC du premier utilisateur qui passe l'authentification sera liée. Ensuite, seul cet utilisateur peut utiliser le nom d'utilisateur et le mot de passe pour passer l'authentification.
Nombre maximal d'utilisateurs	Spécifiez le nombre maximal d'utilisateurs qui peuvent utiliser ce compte pour réussir l'authentification.
Nom	Spécifiez un nom pour l'identification.
Téléphone	Spécifiez un numéro de téléphone pour identification.
Limite de taux (Télécharger)	Sélectionner s'il faut activer la limite de taux de téléchargement. Avec cette option activée, vous pouvez spécifier la limite du taux de téléchargement.
Limite de taux (Télécharger)	Sélectionne-s'il faut activer la limite de taux de téléchargement. Avec cette option activée, vous pouvez spécifier la limite du taux de téléchargement.
Limite de trafic	Sélectionnez, -s'il faut activer la limite de trafic. Avec cette option activée, vous pouvez spécifier la limite de trafic totale pour l'utilisateur. Une fois la limite atteinte, l'utilisateur ne peut plus utiliser ce compte pour accéder au réseau.

3. De la même manière, vous pouvez ajouter plus de comptes d'utilisateurs accounts. Les comptes d'utilisateurs créés s'affichent dans la liste. Les utilisateurs peuvent utiliser le nom d'utilisateur et le mot de passe du compte pour passer l'authentification du portail.

Par défaut, l'État du compte est , ce qui signifie que le compte d'utilisateur est activé et valide. Vous égalité sur ce bouton Verser le compte d'utilisateur. L'icône sera changée ce qui Signifient que le compte d'utilisateur est désactive.



Vous pouvez cliquer sur Export Users Pour sauvegarder toutes les informations du compte d'utilisateur Un fichier CSV ou XLS et enregistrer sur le fichier sur votre PC. Si nécessaire, vous pouvez cliquer et sélectionner le fichier pour importer les informations Import Users du compte dans la liste.

Notes

L'utilisation d'Excel pour ouvrir le fichier CSV peut entraîner des modifications de format numérique et le numéro peut être affiché incorrectement. Si vous utilisez Excel pour modifier le fichier CSV, définissez le format de la cellule sous forme de texte.

Créer des comptes d'opérateur

Le compte de l'opérateur peut être utilisé pour gérer à distance le portail utilisateur local et le portail de bons. D'autres utilisateurs peuvent visiter l'adresse IP **https://OC200** de **l'URL :443/hotspot** (par exemple : ***https://192.168.0.64:443/hotspot***) et utiliser le compte Opérateur pour entrer dans la page de gestion du portail.

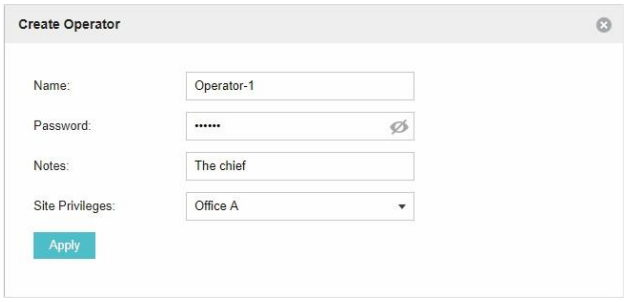
Notes

- Assurez-vous que l'hôte utilisé pour entrer la page de gestion du portail avec le compte de l'opérateur peut communiquer avec l'OC200.
- Seul l'utilisateur qui se connecte à l'OC200 avec le rôle d'administrateur peut ajouter ou supprimer le compte opérateur pour la gestion du portail.
- Les utilisateurs qui entrent dans la page de gestion du portail par compte d'opérateur ne peuvent créer que des comptes d'utilisateurs et des bons locaux et gérer les clients.

Suivez les étapes ci-dessous pour créer le compte Opérateur.

1. Aller à la page Opérateur

2. Create Operator et la fenêtre suivante apparaîtra -jusqu'à.



3. Spécifiez le nom, le mot de passe et les notes du compte opérateur.

4. Sélectionnez Privilèges de site dans la liste déroulante (plusieurs options disponibles) pour le compte Opérateur.

5. Cliquez sur Appliquer pour créer un compte opérateur. Ensuite, d'autres utilisateurs peuvent utiliser ce compte pour entrer la page de gestion des points d'accès.

3.3.4 Bon

Avec le bon configuré, vous pouvez distribuer les bons générés automatiquement par l'OC200 aux clients. Les clients peuvent utiliser les bons pour accéder au réseau.

Configurer le portail des bons

Suivez les étapes ci-dessous pour configurer le portail des bons :

1. Accédez aux paramètres sans fil > Paramètres sans fil de base et créez un SSID pour le portail.
2. Retournez à la page de configuration du portail. Dans la section Informations de base, remplissez les paramètres de base de l'authentification du portail.

Configurer les paramètres suivants :

Nom du portail	Spécifiez un nom pour le portail.
SSID	Sélectionnez un SSID pour le portail.
Type d'authentification	Sélectionnez Bon.
Gestion des utilisateurs	Vous pouvez cliquer sur ce bouton pour configurer les bons d'authentification ultérieurement. Veuillez consulter Create Vouchers. Create
Redirection HTTPS	Avec cette fonction activée, les clients non autorisés seront redirigés vers la page Portail lorsqu'ils tentent ***trying de*** parcourir les sites Web HTTPS. Avec cette fonction désactivée, les clients non autorisés ne peuvent pas parcourir les sites Web HTTPS ou être redirigés vers la page Portail.
Rediriger	Si vous activez cette fonction, le portail redirigera les clients nouvellement authentifiés vers l'URL configurée.
Rediriger l'URL	Si la fonction De redirection ci-dessus est activée, entrez l'URL vers laquelle un client nouvellement authentifié sera redirigé.

3. Dans la section Page de connexion, configurez la page de connexion du portail.

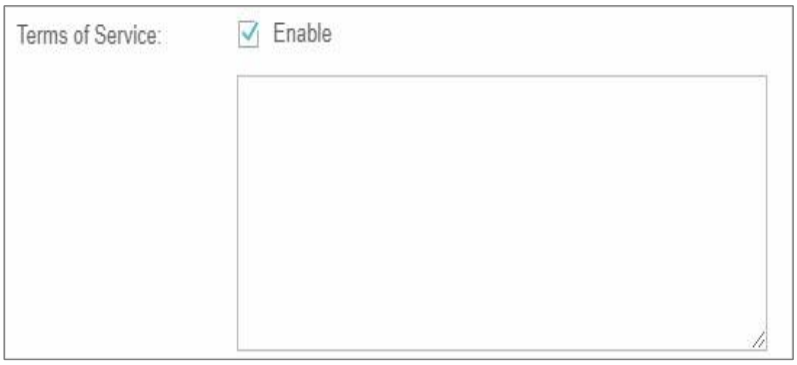
Configurer les paramètres suivants :

Fond	Sélectionnez le type d'arrière-plan. Deux types sont pris en charge : Couleur solide Color et image.
Couleur d'arrière-plan	Si Solid Color est sélectionné, configurez la couleur d'arrière-plan souhaitée via le sélecteur de couleurs ou en entrant manuellement la valeur RGB .
Image d'arrière-plan	Si l'image est sélectionnée, cliquez sur le bouton Choisir et sélectionnez une image à partir de votre PC. Faites glisser et mettre la région de découpage à l'échelle pour scale modifier l'image, picture puis cliquez sur Confirmer.
Image du logo	Cliquez sur le bouton Choisir et sélectionnez une image à partir de votre PC. Faites glisser et mettre la région de découpage à l'échelle pour scale modifier l'image, picture puis cliquez sur Confirmer.

Dans addtion, vous cliquez sur et Configurateur la position du Logo. Les Options Inclure Moyen, Supérieur Et Inférieur

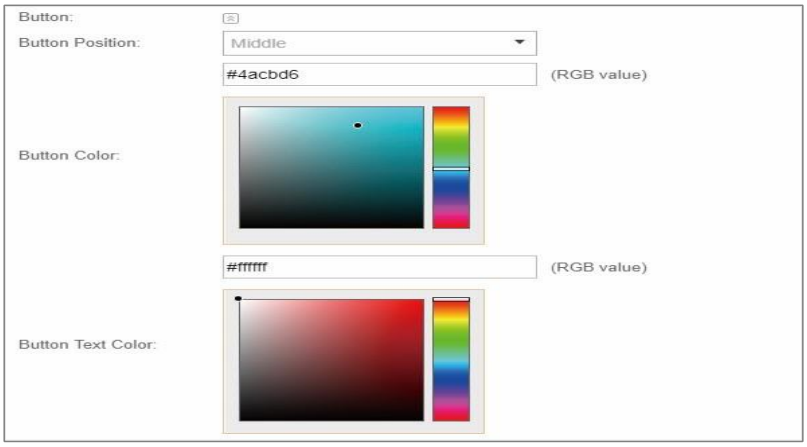
Informations de bienvenue Spécifiez les informations de bienvenue.

Dans addtion, vous cliquez sur et choisir la couleur de texte copier les informations de bienvenue Via le de couleurs ou en entrant la valeur Rvb .



Copyright Spécialistes les informations sur le droit

Dans addtion, sur et la couleur de texte Verser Copyright informations via le sélecteur de couleurs ou en entrant manuellement la valeur RGB .



Conditions d'utilisation Activer ou désactiver les conditions d'utilisation. Avec cette option activée, spécifiez les conditions de service dans la zone suivante.

Boîte d'entrée Cliquez sur et configurer la zone d'entrée.

Sélectionnez la couleur souhaitée pour la zone d'entrée via le sélecteur de couleurs ou en entrant manuellement la valeur RGB .

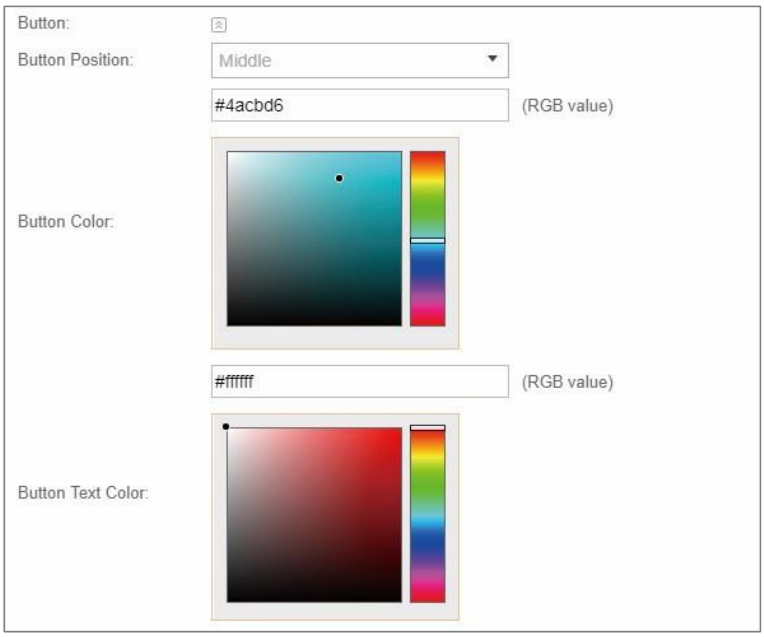
Bouton

Cliquez et configurer le bouton.

Position du bouton : définissez la position du bouton de connexion. Les options incluent le moyen, le haut et le bas.

Couleur du bouton : sélectionnez la couleur du bouton de connexion souhaité par l'intermédiaire du sélecteur de couleurs ou en entrant manuellement la valeur RGB .

Couleur du texte du bouton : sélectionnez la couleur de texte souhaitée pour le bouton via le sélecteur de couleurs ou en entrant manuellement la valeur RGB .



4. Dans la section Publicité, sélectionnez afficher whether des images publicitaires pour les utilisateurs et configurer les paramètres connexes .

Publicité	Spécifiez si l'option doit 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 . Vous pouvez également autoriser les utilisateurs à ignorer la publicité en permettant aux utilisateurs de sauter la publicité. L'image avertissement publicitaire doit être inférieure à 2 Mo. Et seuls les types de fichiers JPG, PNG, BMP, GIF et JPEG sont pris en charge.
Ressource d'image	Télécharger des photos publicitaires. Lorsque plusieurs images sont ajoutées, added elles seront jouées en boucle.
Publicité Durée	Spécifiez la durée de l'affichage de la publicité. 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 bien affiché.
Photo Carousel Intervalle	Spécifiez 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.
Autoriser les utilisateurs à sauter Publicité	Spécifie-s'il faut activer cette fonctionnalité. Avec cette fonctionnalité activée, l'utilisateur peut cliquer sur le bouton Ignorer pour ignorer la publicité.

5. Cliquez sur Appliquer.

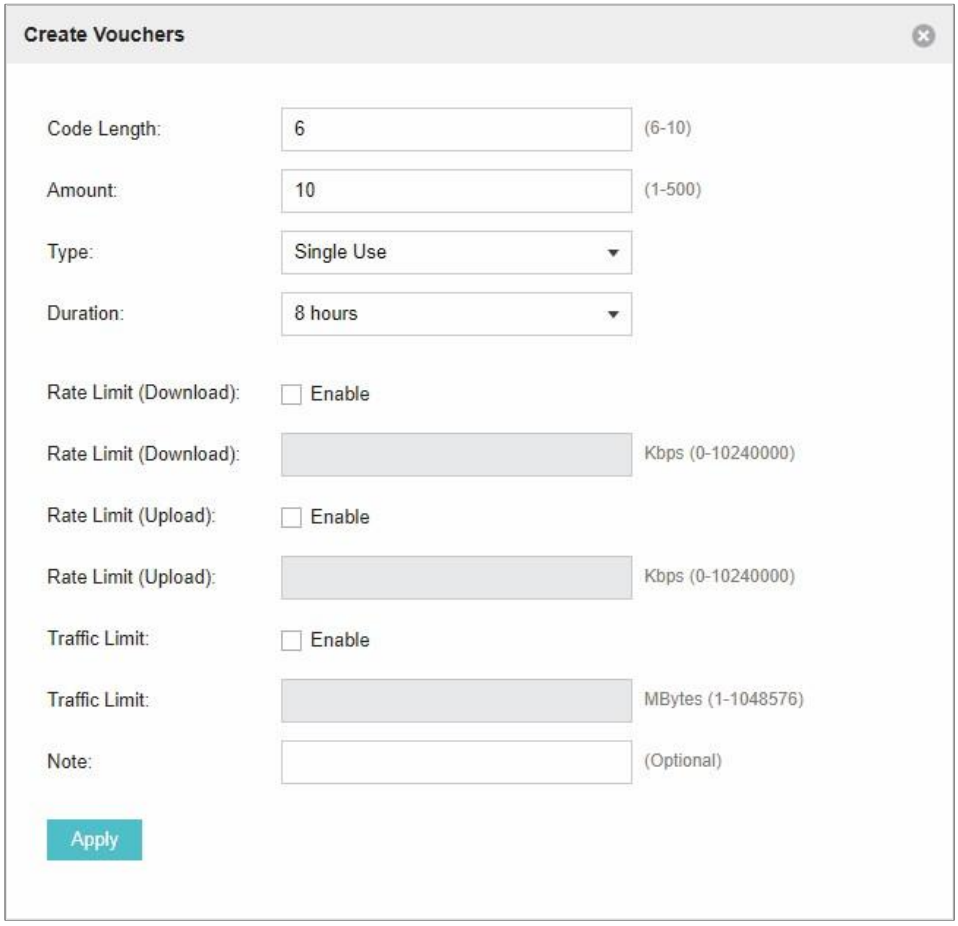
Créer des bons

Suivez les étapes ci-dessous pour créer des bons d'authentification :

1. Dans la section Informations de base, cliquez sur Gestionnaire de bons. Ou vous pouvez cliquer en Create User haut à gauche

   Pièce de la Page et Hotspot Manager. La page de gestion des bons s'affiche . Aller à la Bon. Page et cliquez Create Vouchers

2. La fenêtre suivante apparaît. Configurez les paramètres requis et cliquez sur Appliquer.

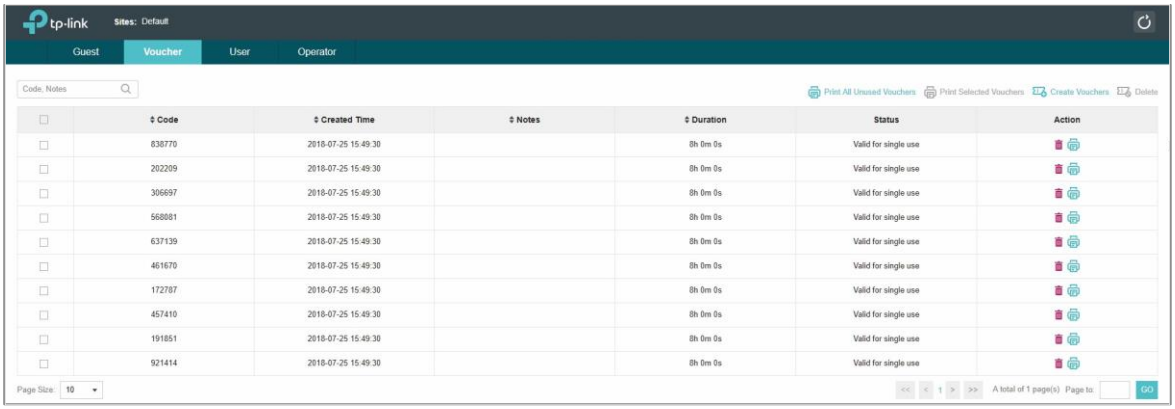


Configurer les paramètres suivants :

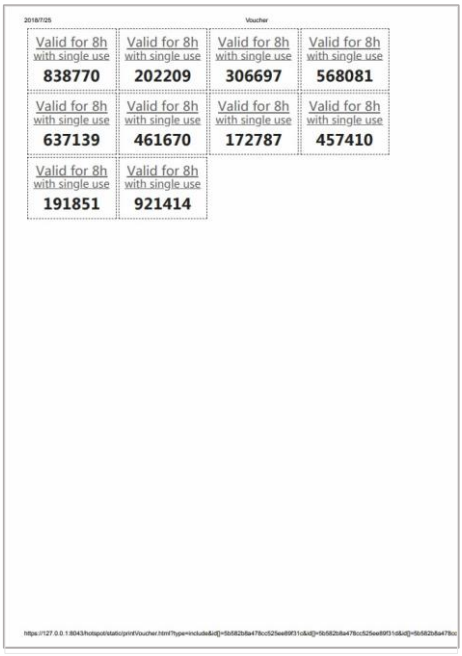
Longueur du code	Spécifiez la longueur des codes de bons à créer.
Montant	Entrez le montant du bon à générer.
Type	Sélectionnez Utilisation unique ou utilisation multi. Utilisation unique signifie qu'un seul bon ne peut être distribué seulement qu'à un seul client. Multi Use signifie qu'un bon peut être distribué à plusieurs clients, qui peuvent utiliser le même bon pour accéder au réseau en même temps. Si vous sélectionnez Utilisation multi, entrez la valeur des utilisateurs Max. Lorsque le nombre de clients connectés au réseau avec le même bon atteint la valeur, aucun client ne peut plus utiliser ce bon pour accéder au réseau.
Durée	Sélectionnez la période de validité du bon. Les options incluent 8 heures,2 jours et défini par l'utilisateur. La période de validité du bon est comptée à partir du moment où il est utilisé pour la première fois.
Limite de taux (Télécharger)	Sélectionne-s'il faut activer la limite de taux de téléchargement. Avec cette option activée, vous pouvez spécifier la limite du taux de téléchargement.

Limite de taux (Télécharger)	Sélectionne-s'il faut activer la limite de taux de téléchargement. Avec cette option activée, vous pouvez spécifier la limite du taux de téléchargement.
Limite de trafic	Spécifiez la limite de trafic totale pour un bon. Une fois la limite atteinte, le client ne peut plus accéder au réseau à l'aide du bon.
Notes	Entrez une description du bon (facultatif).

3. Les bons seront générés et affichés sur la page.



4. pour imprimer un seul bon; cl Print Selected Vouchers Pour imprimer vos bons sélectionnés; Cliqu Print All Unused Vouchers Pour imprimer tous les bons inutilisés.



5. Distribuez les bons aux clients, puis ils peuvent utiliser les codes pour passer l'authentification.

6. Lorsque les bons ne sont pas valides, vous pouvez cliquer pour supprimer le bon ou cliquer Delete pour supprimer les bons sélectionnés. selected

Créer des comptes d'opérateur

Le compte de l'opérateur peut être utilisé pour gérer à distance le portail utilisateur local et le portail de bons. D'autres utilisateurs peuvent visiter l'adresse IP https://OC200 de l'URL :443/hotspot (par exemple : https://192.168.0.64:443/hotspot) et utiliser le compte Opérateur pour entrer dans la page de gestion du portail.

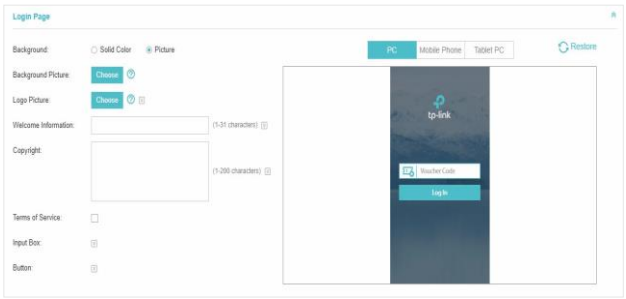
Otes

- Assurez-vous que l'hôte utilisé pour entrer la page de gestion du portail avec le compte de l'opérateur peut communiquer avec l'OC200.
- Seul l'utilisateur qui se connecte à l'OC200 avec le rôle d'administrateur peut ajouter ou supprimer le compte opérateur pour la gestion du portail.
- Les utilisateurs qui entrent dans la page de gestion du portail par compte d'opérateur ne peuvent créer que des comptes d'utilisateurs et des bons locaux et gérer les clients.

Suivez les étapes ci-dessous pour créer le compte Opérateur .

1. Aller à la Opérateur page.

2. et la fenêtre suivante apparaîtra.



3. Spécifiez le nom, le mot de passe et les notes du compte opérateur .
4. Sélectionnez Privilèges de site dans la liste déroulante (plusieurs options disponibles) pour le compte Opérateur .
5. Cliquez sur Appliquer pour créer un compte opérateur. Ensuite, d'autres utilisateurs peuvent utiliser ce compte pour entrer dans le système d'administration hotspot.

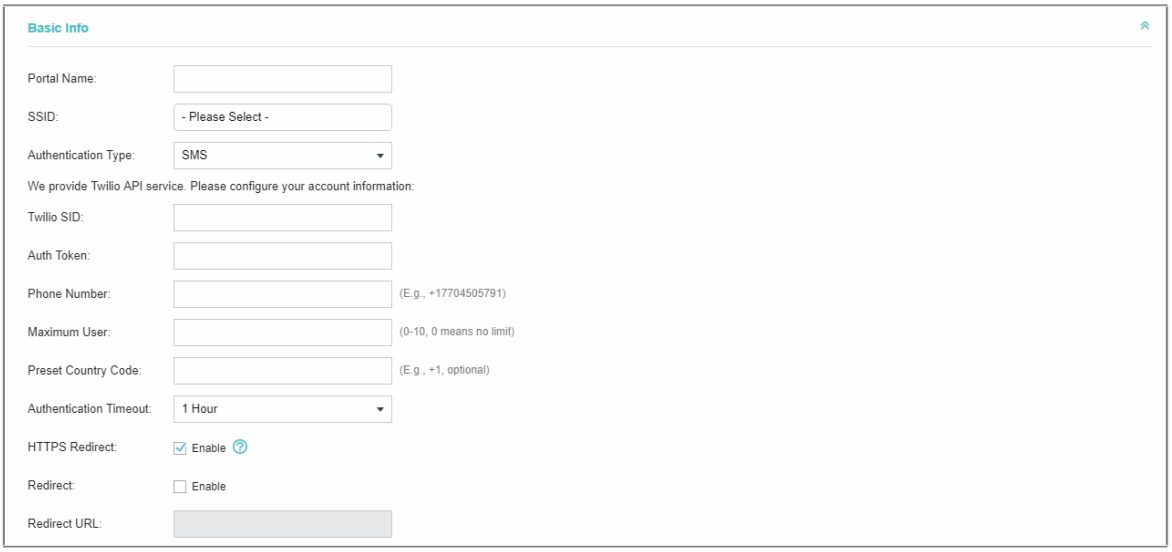
3.3.5 SMS

Avec le portail SMS configuré, le client peut obtenir des codes de vérification à l'aide de leurs téléphones mobiles et entrer les codes passes reçus **received** pour passer l'authentification.

Suivez les étapes ci-dessous pour configurer le portail SMS :

1. Accédez à http://www.twilio.com/try-twilio et obtenez un **compte Twilio** . Achetez le service Twilio pour SMS. Ensuite, obtenez les informations de compte, y compris LE SID DU COMPTE, AUTH TOKEN et numéro de téléphone number.

2. Accédez aux paramètres sans fil > Paramètres sans fil de base et créez un SSID pour le portail.
3. Retournez à la page de configuration du portail. Dans la section Informations de base, remplissez les paramètres de base de l'authentification du portail authentication.



Configurer les paramètres suivants :

Nom du portail	Spécifiez un nom pour le portail.
SSID	Sélectionnez un SSID pour le portail.
Type d'authentification	Sélectionnez SMS.
Twilio SID	Entrez le SID du 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 .
Numéro de téléphone	Entrez le numéro de téléphone utilisé pour envoyer des messages de vérification aux clients.

Nombre maximal d'utilisateurs	Un téléphone peut obtenir plusieurs codes via des messages un par un, et différents clients peuvent utiliser différents codes pour passer l'authentification. Toutefois, le nombre de clients autorisés à être authentifiés à l'aide du même téléphone en même temps a une limite supérieure . Spécifiez la limite supérieure dans ce champ.
Authentification Timeout	L'authentification du client expirera après la période que vous avez définie et le client doit se connecter à nouveau sur la page d'authentification Web pour accéder au réseau. Les options incluent 1 heure,8 heures,24 heures,7 jours et personnalisé. La coutume vous permet de définir l'heure en jours, heures et minutes. La valeur par défaut est d'une heure.
Code de pays prédéfinis	Définissez le code de pays par défaut qui sera rempli automatiquement sur la page d'authentification.
Redirection HTTPS	Avec cette fonction activée, les clients non autorisés seront redirigés vers la page Portail lorsqu'ils tentent de parcourir les sites Web HTTPS . Avec cette fonction désactivée, les clients non autorisés ne peuvent pas parcourir les sites Web HTTPS et ne sont pas redirigés vers la page Portail.
Rediriger	Si vous activez cette fonction, le portail redirigera les clients nouvellement authentifiés vers l'URL configurée.
Rediriger l'URL	Si la fonction De redirection ci-dessus est activée, entrez l'URL vers laquelle un client nouvellement authentifié sera redirigé.

4. Dans la section Page de connexion, configurez la page de connexion du portail.

Configurer les paramètres suivants :

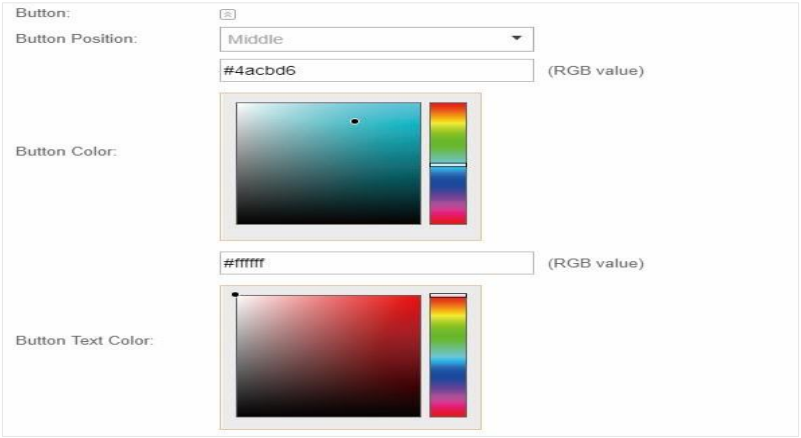
Fond	Sélectionnez le type d'arrière-plan. Deux types sont pris en charge : Couleur solide Color et image.
Couleur d'arrière-plan	Si Solid Color est sélectionné, configurez la couleur d'arrière-plan souhaitée via le sélecteur de couleurs ou en entrant manuellement la valeur RGB .
Image d'arrière-plan	Si l'image est sélectionnée, cliquez sur le bouton Choisir et sélectionnez une image à partir de votre PC. Faites glisser et mettre la région de découpage à l'échelle pour scale modifier l'image, picture puis cliquez sur Confirmer.
Image du logo	Cliquez sur le bouton Choisir et sélectionnez une image à partir de votre PC. Faites glisser et l'échelle pour scale modifier l'image, picture puis cliquez sur Confirmer. Dans addtion, vous pouvez cliquer et configurer la position du logo. Les options incluent le moyen, le haut et le bas. Mettre la région de découpage à

Informations de bienvenue Spécifiez les informations de bienvenue.

Dans addtion, vous sur et sélectionnez la couleur de texte souhaitée pour le Informations de bienvenue Via le de couleurs ou en entrant la valeur Rvb .

Copyright Spécialistes les informations sur le droit

Dans addtion, vous su et la couleur de texte Verser Copyright informations via le sélecteur de couleurs ou en entrant manuellement la valeur RGB .



Conditions d'utilisation Activer ou désactiver les conditions d'utilisation. Avec cette option activée, spécifiez les conditions de service dans la zone suivante.

Boîte d'entrée Cliquez sur et configurer la zone d'entrée.

Sélectionnez la couleur souhaitée pour la zone d'entrée via le sélecteur de couleurs ou en entrant manuellement la valeur RGB .

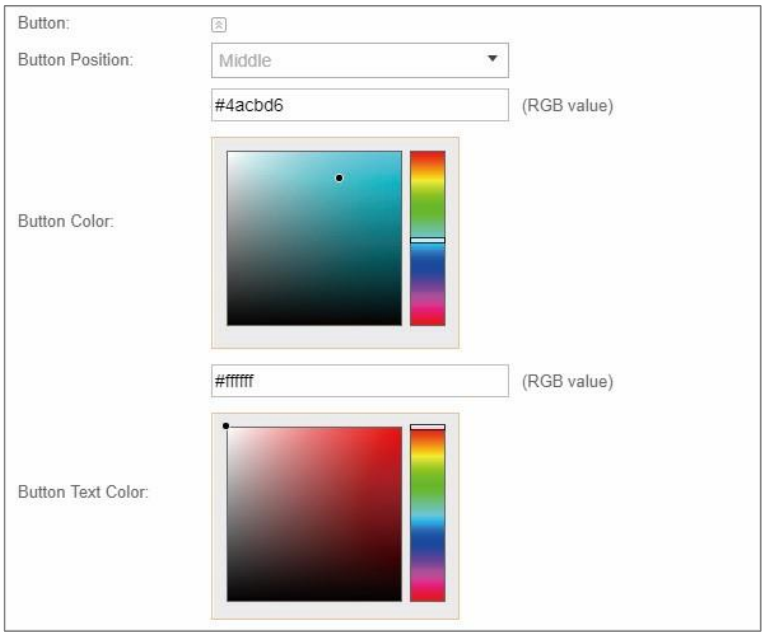
Bouton

Cliquez et Configurateur le bouton.

Position du bouton : définissez la position du bouton de connexion. Les options incluent le moyen, le haut et le bas.

Couleur du bouton : sélectionnez la couleur du bouton de connexion souhaité par l'intermédiaire du sélecteur de couleurs ou en entrant manuellement la valeur RGB .

Couleur du texte du bouton : sélectionnez la couleur de texte souhaitée pour le bouton via le sélecteur de couleurs ou en entrant manuellement la valeur RGB .



5. Dans la section Publicité, sélectionnez afficher whether des images publicitaires pour les utilisateurs et configurer les paramètres connexes .

Configurer les paramètres suivants :

Publicité	Spécifiez si l'option doit 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 appears. Vous pouvez également autoriser les utilisateurs à ignorer la publicité en permettant aux utilisateurs de sauter la publicité. L'image advertisement publicitaire doit être inférieure à 2 Mo. Et seuls les types de fichiers JPG, PNG, BMP, GIF et JPEG sont pris en charge.
Ressource d'image	Télécharger des photos publicitaires. Lorsque plusieurs images sont ajoutées, added elles seront jouées en boucle.
Publicité Durée	Spécifiez la durée de l'affichage de la publicité. 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 be affiché.
Photo Careusel Intervalle	Spécifiez 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.
Autoriser les utilisateurs à sauter Publicité	Spécifie-s'il faut activer cette fonctionnalité. Avec cette fonctionnalité activée, l'utilisateur peut cliquer sur le bouton Ignorer pour ignorer la publicité.

6.

7. Cliquez sur Appliquer.

Pour plus de détails sur la configuration du portail SMS, vous pouvez aller à https://www.tp-link.com/en/configuration-guides.html et télécharger le guide de configuration pour SMS Portal.

3.3.6 Facebook

Avec facebook portail configuré, lorsque les clients se connectent à votre Wi-Fi, ils seront redirigés vers votre page Facebook. Pour accéder à Internet, les clients doivent passer l'authentification sur la page.

Notes

OC200 will créera automatiquement des entrées de stratégie d'authentification gratuite pour le portail Facebook. Vous n'avez pas besoin de les créer manuellement.

Procédez comme suit pour configurer le portail Facebook :

1. Accédez à https://www.facebook.com/ et obtenez un compte Facebook. Créez votre page Facebook en fonction de vos besoins.
2. Accédez aux paramètres sans fil > Paramètres sans fil de base et créez un SSID pour le portail.
3. Retournez à la page de configuration du portail. Dans la section Informations de base, remplissez les paramètres de l'authentification du portail

Configurer les paramètres suivants :

Nom du portail	Spécifiez un nom pour le portail.
SSID	Sélectionnez un SSID pour le portail.
Type d'authentification	Sélectionnez Facebook.
Facebook Page Configuration	Cliquez sur ce bouton pour spécifier la Page Facebook.
Twitter Checking Emplacement	Si la page Facebook est obtenue avec succès par l'OC200, le nom de la page Facebook sera affiché ici.
Redirection HTTPS	Avec cette fonction activée, les clients non autorisés seront redirigés vers la page Portail lorsqu'ils tentent de parcourir les sites Web HTTPS . Avec cette fonction désactivée, les clients non autorisés ne peuvent pas parcourir les sites Web HTTPS et ne sont pas redirigés vers la page Portail.

Pour plus de détails sur la configuration du portail Facebook, vous pouvez aller à https://www.tp-link.com/en/configuration-guides.html et télécharger le guide de configuration pour Facebook Portal.

3.3.7 Serveur RADIUS externe

Si vous disposez d'un serveur RADIUS, vous pouvez configurer le portail serveur EXERUS externe. Avec ce type de portail, vous pouvez obtenir deux types de personnalisation de portail : portail Web local et portail Web externe.

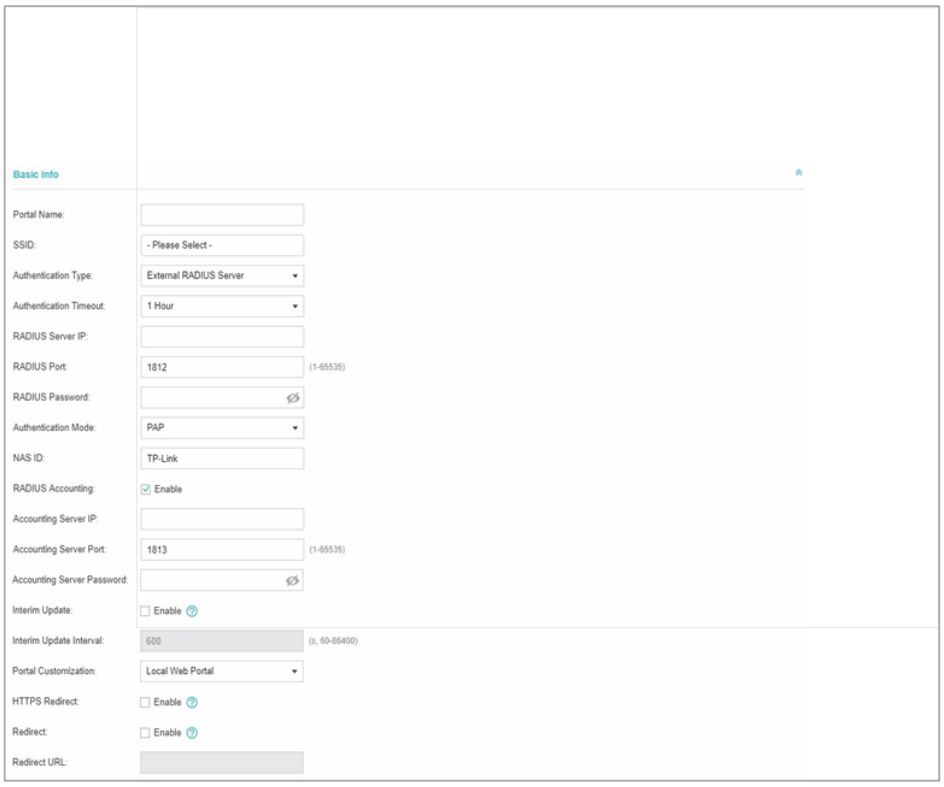
La page de connexion d'authentification du portail Web local est fournie par le serveur portail intégré de l'OC200. Le portail Web externe est fourni par un serveur portail externe.

Notes

OC200 créera automatiquement des entrées de stratégie d'authentification gratuite pour le portail RADIUS externe. l

Procédez comme suit pour configurer le portail serveur EXERUS externe :

1. Accédez aux paramètres sans fil > Paramètres sans fil de base et créez un SSID pour le portail.
2. Retournez à la page de configuration du portail. Dans la section Informations de base, remplissez les paramètres de base de l'authentification du portail.



Configurer les paramètres suivants :

Nom du portail	Spécifiez un nom pour le portail.
SSID	Sélectionnez un SSID pour le portail.
Type d'authentification	Sélectionnez Serveur RADIUS externe.

Délai d'expiration de l'authentification	L'authentification du client expirera après la période que vous avez définie et le client doit se connecter à nouveau sur la page d'authentification Web pour accéder au réseau. Options include 1 heure,8 heures,24 heures,7 jours, personnalisé. La personnalisation vous permet de définir l'heure en jours, heures et minutes. La valeur par défaut est d'une heure.
RADIUS Server IP	Entrez l'adresse IP du serveur RADIUS.
RADIUS Port	Entrez le numéro de port que vous avez défini sur le serveur RADIUS.
Mot de passe RADIUS	Entrez le mot de passe que vous avez défini sur le serveur RADIUS.
Mode d'authentification	Sélectionnez le protocole d'authentification pour le serveur RADIUS. Deux protocoles d'authentification sont disponibles : PAP et CHAP.
NAS ID	Configurez un identificateur nas (NAS ID) d'accès réseau à l'aide de 1 à 64 caractères sur le portail. L'ID NAS est envoyé au serveur RADIUS par le contrôleur via un paquet de demande d'authentification. Avec l'ID NAS qui classe les utilisateurs à différents groupes, le serveur RADIUS peut envoyer une réponse d'authentification personnalisée. La valeur par défaut est TP-Link.
Radius Accounting	Activer ou désactiver la fonctionnalité RADIUS Accounting .
IP du serveur comptable	Entrez l'adresse IP du serveur comptable.
Port serveur comptable	Entrez le numéro de port du serveur comptable. Le numéro de port par défaut est 1813.
Serveur comptable Mot de passe	Entrez la clé secrète partagée du serveur comptable.
Mise à jour provisoire	Avec cette option activée, vous pouvez spécifier la durée entre les mises à jour d'informations comptables. Par défaut, la fonction est désactivée. Entrez la durée appropriée entre les mises à jour pour les EAP dans l'intervalle de mise à jour intérimaire.

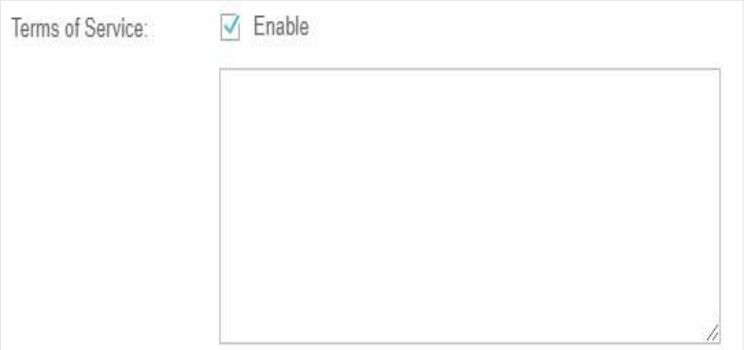
Intervalle de mise à jour intérimaire	Avec mise à jour intérimaire activée, spécifiez la durée appropriée entre les mises à jour pour les EAP. La durée par défaut est de 600 secondes.
Personnalisation du portail	Sélectionnez Portail Web local ou Portail Web externe. Portail Web local : si cette option est sélectionnée, reportez-vous à l'étape3 pour configurer la page de connexion et l'étape 4 pour configurer la publicité. Portail Web externe : si cette option est sélectionnée, suivez les étapes ci-dessous. 1. Configurez le serveur RADIUS externe. 2. Entrez l'URL de la page de connexion d'authentification fournie par le serveur de portail externe dans le champ URL du portail Web externe. Notez que vous devez mettre à jour le portail Web externe après avoir mis à niveau votre contrôleur avec your l'ancienne version à la version 3.1.4 ou au-dessus. Sinon, le portail Web externe n'entrera pas en vigueur.
Redirection HTTPS	Avec cette fonction activée, les clients non autorisés seront redirigés vers la page Portail lorsqu'ils tentent trying de parcourir les sites Web HTTPS. Avec cette fonction désactivée, les clients non autorisés ne peuvent pas parcourir les sites Web HTTPS et ne sont pas redirigés vers la page Portail.
Rediriger	Si vous activez cette fonction, le portail redirigera les clients nouvellement authentifiés vers l'URL configurée. Il est désactivé par défaut.
Rediriger l'URL	Si la fonction De redirection ci-dessus est activée, entrez l'URL vers laquelle un client nouvellement authentifié sera redirigé.

3. Portail Web local est configuré, configurez la page de connexion pour le portail dans la section Page de connexion.

Fond	Sélectionnez le type d'arrière-plan. Deux types sont pris en charge: Couleur solide Color et image.
Couleur d'arrière-plan	Si Solid Color est sélectionné, configurez la couleur d'arrière-plan souhaitée via le sélecteur de couleurs ou en entrant manuellement la valeur RGB .
Image d'arrière-plan	Si l'image est sélectionnée, cliquez sur le bouton Choisir et sélectionnez une image à partir de votre PC. Faites glisser et mettre la région de découpage à l'échelle pour scale modifier l'image, Picture puis cliquez sur Confirmer.
Image du logo	Cliquez sur le bouton Choisir et sélectionnez une image à partir de votre PC. Faites glisser et mettre la région de découpage à l'échelle pour modifier l'image, puis cliquez sur Confirmer. Dans addition, vous pouvez cliquer et configurer la position du logo. Les options incluent le moyen, le haut et le bas. 

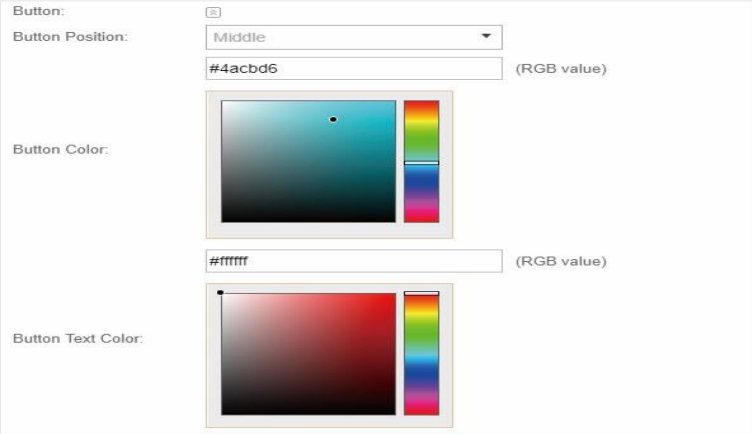
Informations de bienvenue Spécifiez les informations de bienvenue.

Dans addtion, vous su et la couleur de texte Verser le Informations de bienvenue Via la couleur ou en entrant la valeur Rvb .



Copyright Spécialistes les informations sur le droit

Dans addtion, vous su et la couleur de texte Verser Copyright Informations via le sélecteur de couleurs ou en entrant manuellement la valeur RGB .



Conditions d'utilisation Activer ou désactiver les conditions d'utilisation. Avec cette option activée, spécifiez les conditions de service dans la zone suivante.

Boîte

Cliquez et configurer la zone d'entrée.

Sélectionnez la couleur souhaitée pour la zone d'entrée via le sélecteur de couleurs ou en entrant manuellement la valeur RGB .

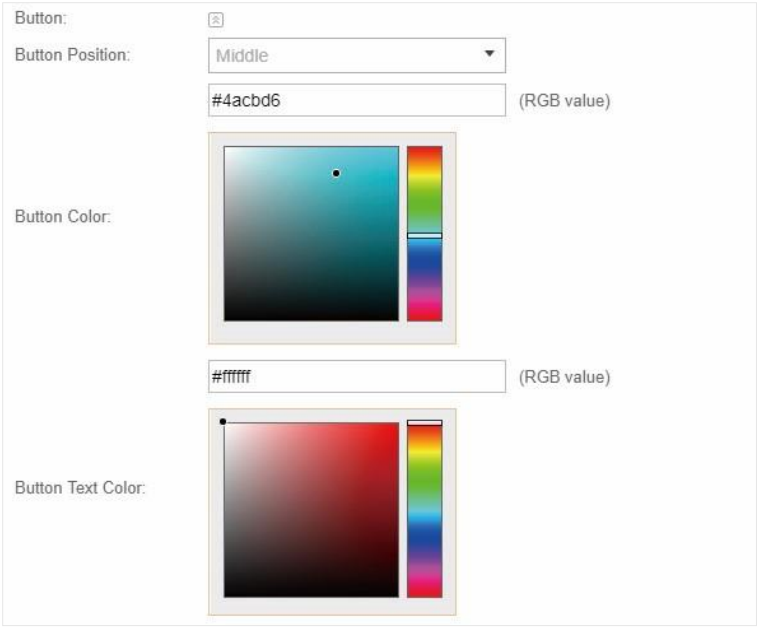
Bouton

Cliquez et Configurateur le bouton.

Position du bouton : définissez la position du bouton de connexion. Les options incluent le moyen, le haut et le bas.

Couleur du bouton : sélectionnez la couleur du bouton de connexion souhaité par l'intermédiaire du sélecteur de couleurs ou en entrant manuellement la valeur RGB .

Couleur du texte du bouton : sélectionnez la couleur de texte souhaitée pour le bouton via le sélecteur de couleurs ou en entrant manuellement la valeur RGB .



4. Si le portail Web local est configuré, sélectionnez s'il convient d'afficher des images publicitaires pour les utilisateurs et de configurer les paramètres connexes dans la section Publicité, .

Configurer les paramètres suivants :

Publicité	Spécifiez si l'option doit 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 appears. Vous pouvez également autoriser les utilisateurs à ignorer la publicité en permettant aux utilisateurs de sauter la publicité. L'image avertissement publicitaire doit être inférieure à 2 Mo. Et seuls les types de fichiers JPG, PNG, BMP, GIF et JPEG sont pris en charge.
Ressource d'image	Télécharger des photos publicitaires. Lorsque plusieurs images sont ajoutées, elles seront jouées en boucle.
Publicité Durée	Spécifiez la durée de l'affichage de la publicité. 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 be affiché.
Photo Carrousel Intervalle	Spécifiez 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.
Autoriser les utilisateurs à sauter Publicité	Spécifier s'il faut activer cette fonctionnalité. Avec cette fonctionnalité activée, l'utilisateur peut cliquer sur le bouton Ignorer pour ignorer la publicité.

5. Cliquez sur Appliquer.

3.3.8 Serveur portail externe

L'option Eternal Portal Server est conçue pour les développeurs. Ils peuvent personnaliser leur propre type d'authentification en fonction de l'interface fournie par OC200, par exemple l'authentification des messages et l'authentification WeChat, etc.

1. Accédez aux paramètres sans fil > Paramètres sans fil de base et créez un SSID pour le portail.
2. Retournez à la page de configuration du portail. Dans la section Informations de base, remplissez les paramètres de l'authentification du portail d'authentification.

Nom du portail	Spécifiez un nom pour le portail.
SSID	Sélectionnez un SSID pour le portail.
Type d'authentification	Sélectionnez Serveur portail externe.
Serveur portail externe	Entrez l'URL d'authentification complète qui redirige vers un serveur de portail externe, par exemple : http://192.168.0.147:8880/portal/index.php ou or http://192.168.0.147/portal/index.html
Redirection HTTPS	Avec cette fonction activée, les clients non autorisés seront redirigés vers la page Portail lorsqu'ils tentent trying de parcourir les sites Web HTTPS Avec cette fonction désactivée, les clients non autorisés ne peuvent pas parcourir les sites Web HTTPS et ne sont pas redirigés vers la page Portail.

3. Cliquez sur Appliquer.

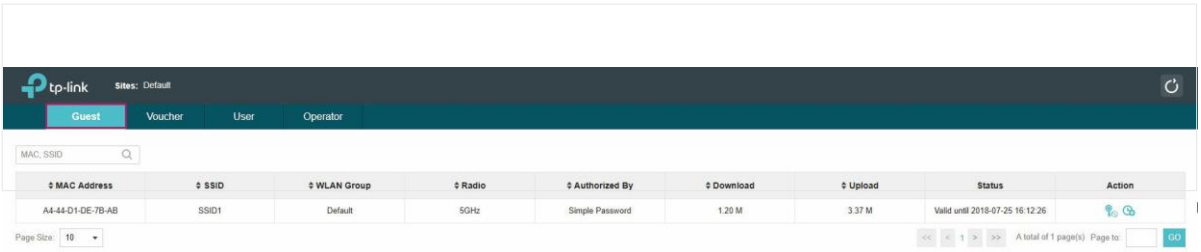
4.

3.3.9 Gérer les invités

Sur la page Invité, vous pouvez afficher les informations des clients qui ont passé le portail

L'authentification et la gestion des clients. Vous cliquez sur Create User

et  Sélectionner visiteur pour exécuter l'opération



Vous pouvez sélectionner une icône

	Restreindre le Client à l'accélération au réseau.
	Prolonger le temps effectif.

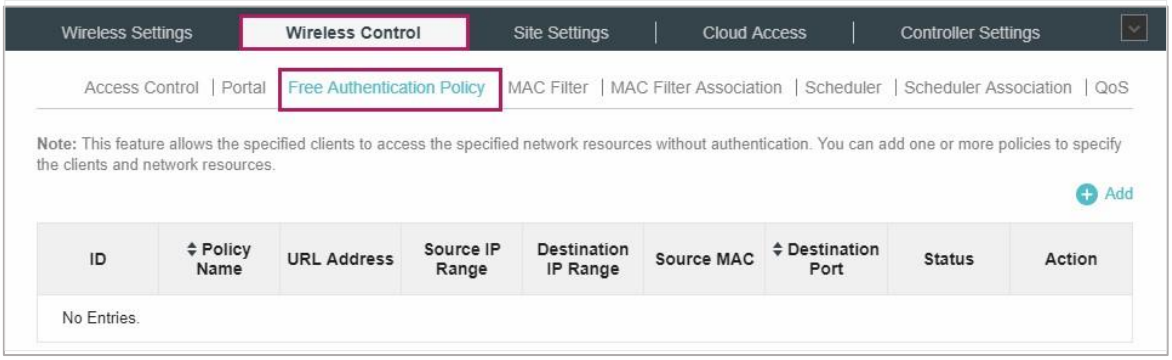
Details du compte

Avec le compte Opérateur, vous pouvez visiter l'adresse **IP https://OC200 :443/hotspot** (par exemple: https://192.168.0.64:443/hotspot) pour visiter à distance la page Invité. Pour plus d'informations sur le compte opérateur, reportez-vous à Créer des comptes d'opérateur détaillé.

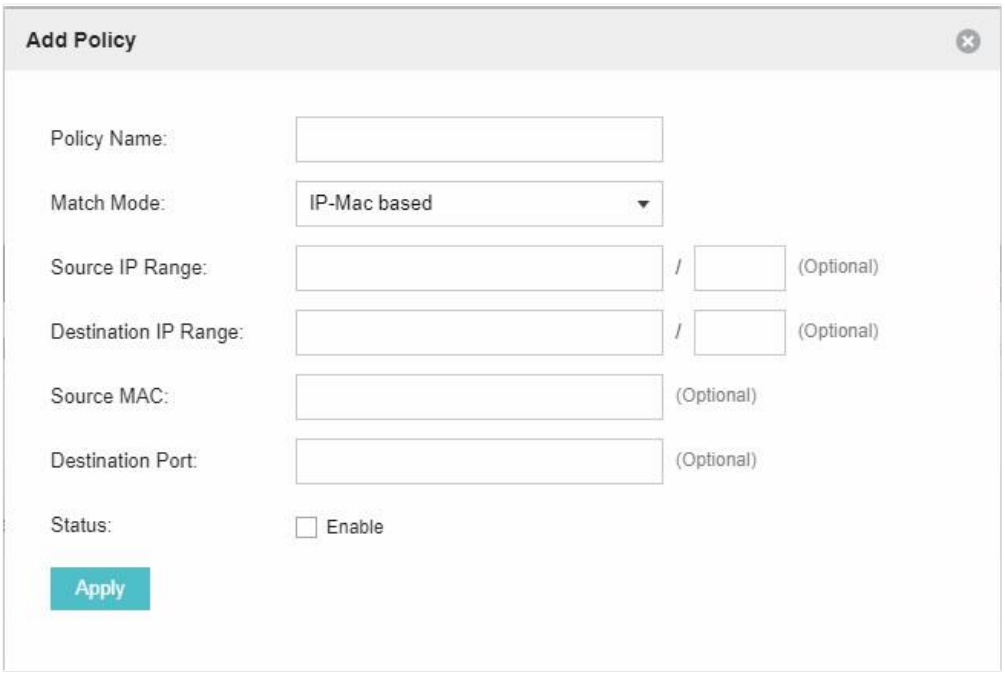
3.4 Stratégie d’authentification gratuite

La stratégie d’authentification gratuite permet à certains clients spécifiés d’accéder aux accès ressources réseau sans authentification. Suivez les étapes ci-dessous pour ajouter une stratégie d’authentification gratuite.

1. Accédez au contrôle sans fil > Stratégie d’authentification gratuite.



2. Add et la fenêtre suivante apparaîtra.



3. Configurer les paramètres suivants, lorsque toutes les conditions sont remplies, le client peut accéder au réseau sans authentification.

Nom de la stratégie	Spécifiez un nom pour la stratégie.
Match Mode	Sélectionnez le mode de correspondance de la stratégie. Deux options sont fournies : URL : Avec cette option sélectionnée, configurez une URL autorisée à être visitée par les clients sans authentification. IP-MAC Based: Avec cette option sélectionnée, configurez la plage IP source, la plage IP de destination, le MAC source et le MAC de destination pour spécifier les clients et le service spécifiques qui suivront la fonctionnalité d'authentification gratuite.
Url	Définissez l'URL.
Plage IP source	Définissez la plage IP source avec le sous-réseau et la longueur du masque des clients.
Plage IP de destination	Définissez la plage IP destination avec le sous-réseau et la longueur du masque du serveur.
Source MAC	Définissez l'adresse MAC du client.
Destination Port	Entrez le port utilisé par le service.
Statut	Cochez la case pour activer la stratégie.

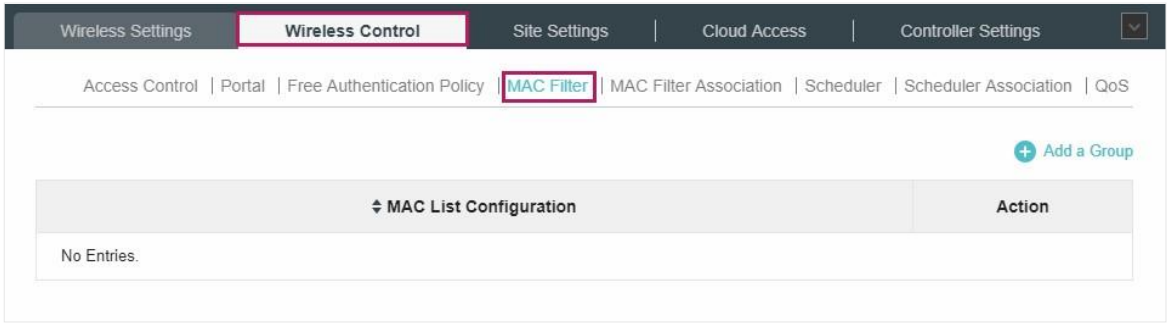
4. Cliquez sur Appliquer et la stratégie est ajoutée avec succès.

Filtre 3.5 MAC

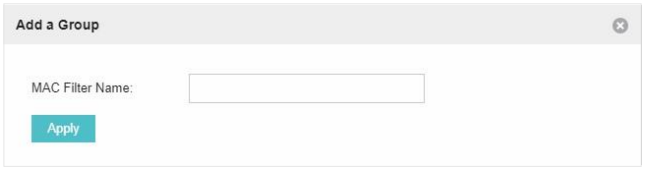
Le filtre MAC peut être utilisé pour permettre ou bloquer les clients répertoriés d'accéder access au réseau. Ainsi, il peut contrôler efficacement l'accès du client au réseau sans fil.

Suivez les étapes ci-dessous pour configurer le filtreMAC.

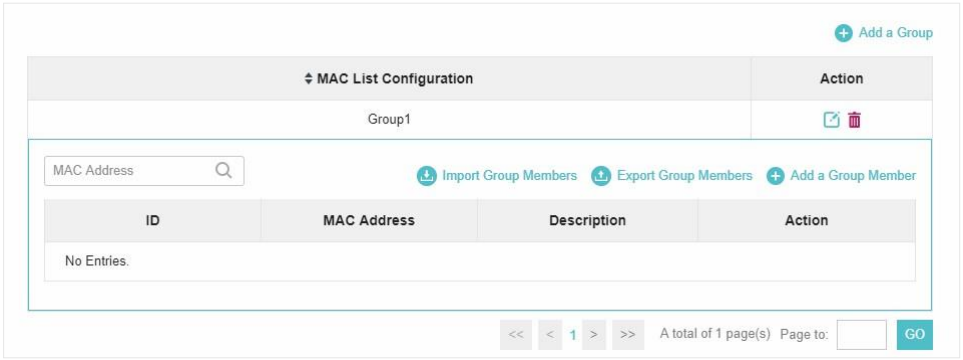
1. Accédez à Contrôle sans fil > Filtre MAC pour ajouter le groupe mac filter et les membres du groupe.



Cliquez Add a Group et préciser un nom de groupe.

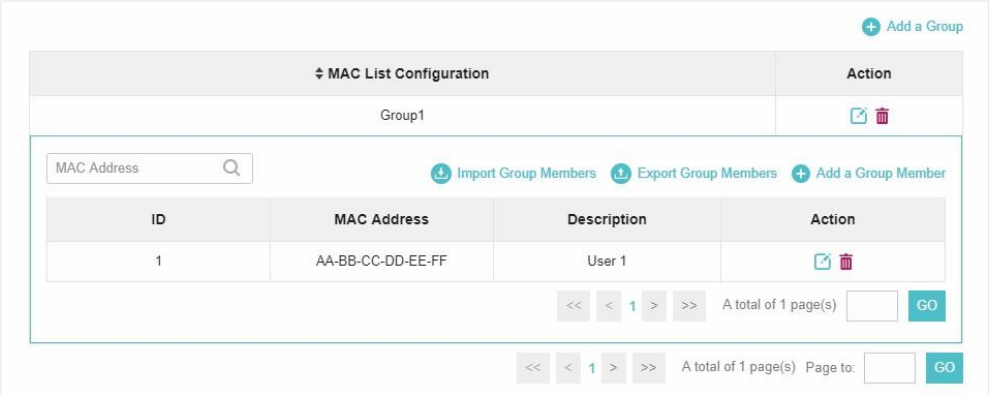


2) Cliquez sur Appliquer et le groupe sera ajouté avec succès comme indiqué ci-dessous.



3) Cliquez Add a Group Member et entrez une adresse Mac dans le Format ci-dessous.

4) Cliquez sur Appliquer pour ajouter l'adresse MAC dans le groupe de filtrage

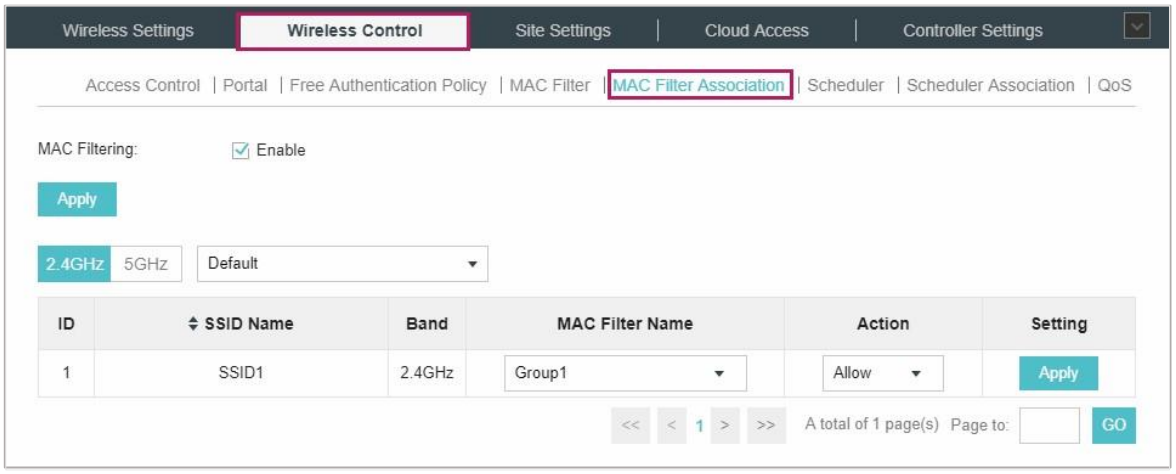


2. Vous pouvez ajouter plus de groupes ou de membres en fonction de vos besoins.

Notes

Vous pouvez cliquer sur Export Group Members pour exporter les membres du groupe vers un fichier Excel et enregistrer le fichier sur votre PC. Si nécessaire, vous pouvez également cliquer sur Import Group Members pour importer les membres du groupe dans l'OC200.

3. Accédez à Contrôle sans fil > MAC Filter Association pour associer le groupe de filtre MAC ajouté à SSID.



1) Cochez la case et cliquez sur Appliquer pour activer la fonction de filtrage MAC.

2) Sélectionnez une fréquence de bande (2,4 GHz ou 5 GHz) et un groupe WLAN.

3) Dans la colonne Nom du filtre MAC du SSID spécifié, sélectionnez un groupe filtre MAC dans la liste déroulante. Sélectionnez Ensuite Autoriser/Refuser dans la colonne Action pour permettre(allow)/refuser (deny) aux clients du groupe Filtre MAC Filter d'accéder et accèder au réseau.

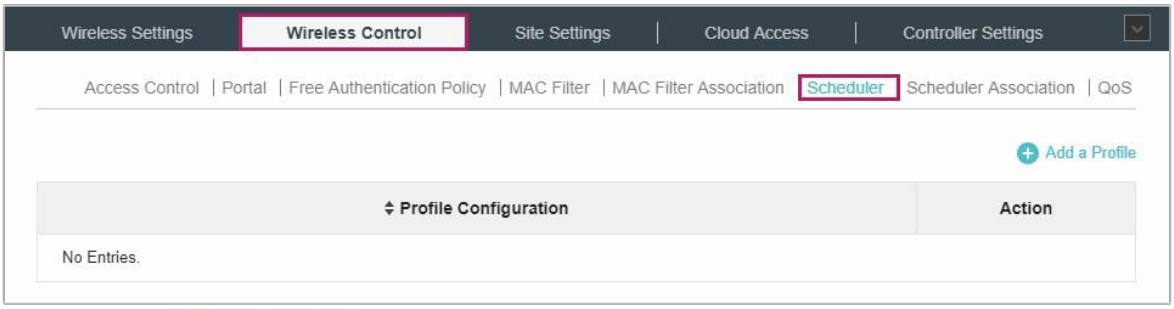
4) Cliquez sur Appliquer dans la colonne Paramètre.

3.6 Planificateur

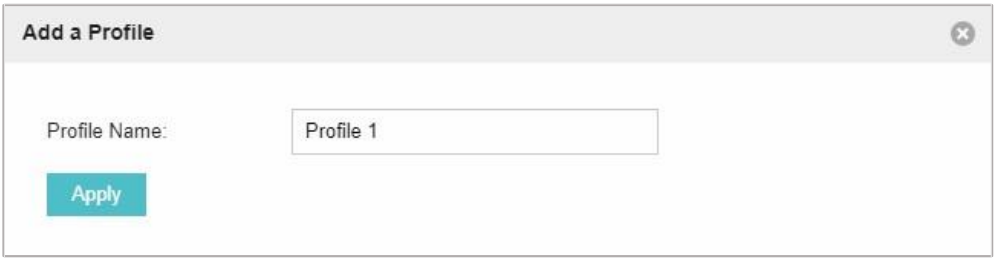
Avec le planificateur, les EAP ou son réseau sans fil peuvent automatiquement s'activer ou s'éteindre au moment où vous définissez. Par exemple, vous pouvez utiliser cette fonctionnalité pour planifier la radio pour fonctionner uniquement pendant le temps de travail au bureau afin d'atteindre les objectifs, d'assurer la sécurité et de réduire la consommation d'énergie . Vous pouvez également utiliser le planificateur pour que les clients ne puissent accéder au réseau sans fil que pendant la période que vous définissez dans la journée.

Suivez les étapes ci-dessous pour configurer le planificateur.

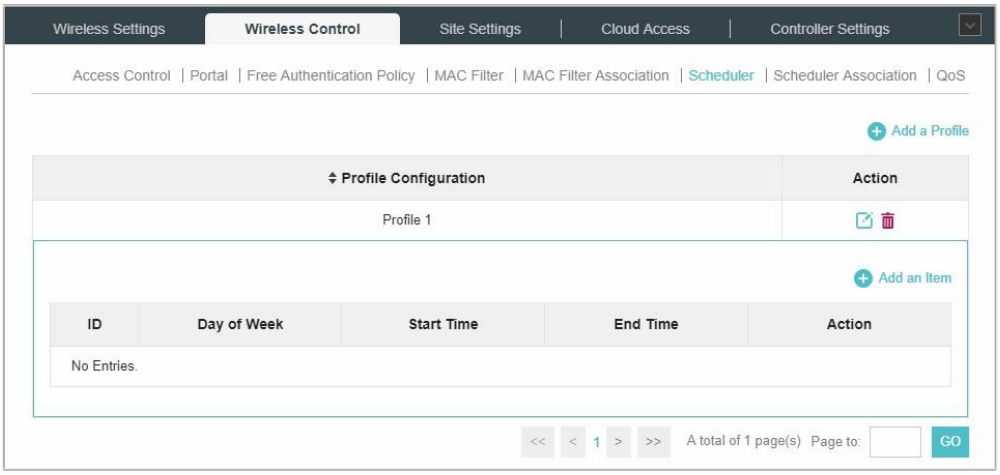
1. Aller à Contrôle sans fil > Planificateur



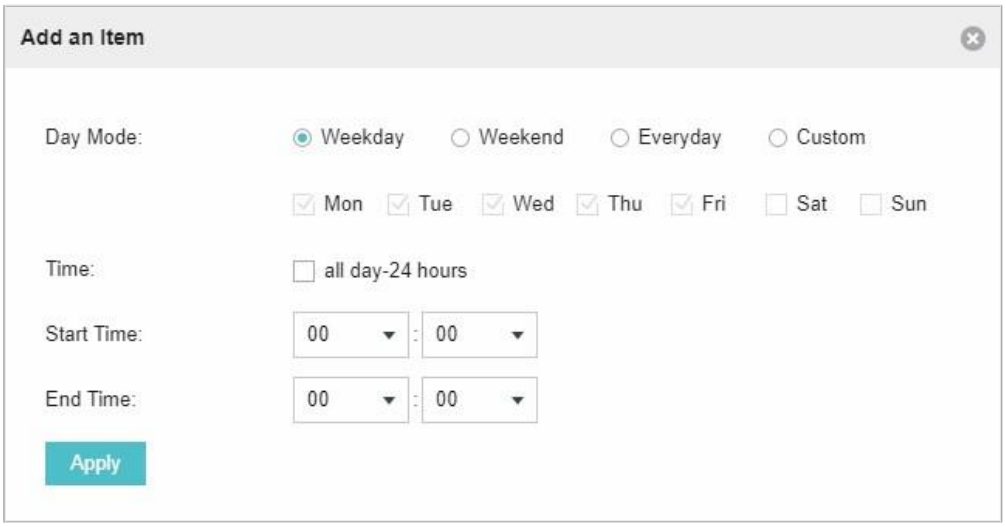
1) Clique Add a Profile et Onu nom Verser le profil.



2) Cliquez sur Appliquer et le profil will sera ajouté.

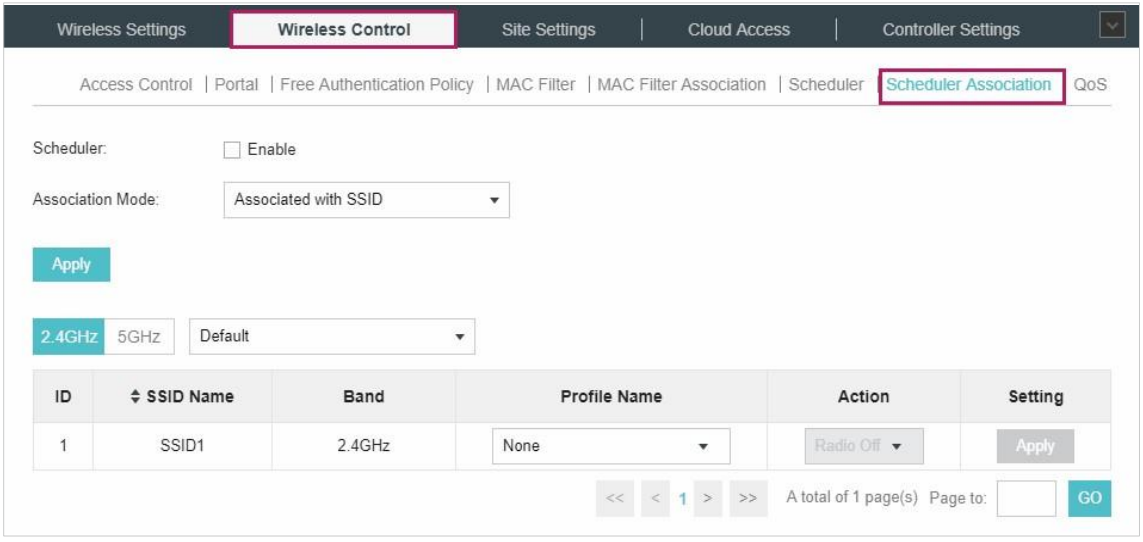


3) Clique Add an Item et Configurateur les paramètres Verser spécialiste une période de



4) Cliquez sur Appliquer et le profil est ajouté avec succès dans la liste.

2. Accédez à La Commande sans fil > Association des planificateurs.



1) Cochez la case pour activer la fonction **Scheduler** .

2) Sélectionner Associé à SSID (le profil sera appliqué au SID spécifique sur tous les EAP)ou associé à un AP (le profil sera appliqué à tous les SSID sur le EAP spécifique). Spécifique Cliquez ensuite sur Appliquer.

3) Sélectionnez une fréquence de bande (2,4 GHz ou 5 GHz) et un groupe WLAN.

4) Dans la colonne Nom du profil du SSID ou de l'AP spécifié, sélectionnez un profil que vous avez ajouté auparavant dans la liste déroulante. Sélectionnez Radio On/Radio Off pour activer ou désactiver le réseau sans fil pendant l'intervalle de temps défini pour le profil.

5) Cliquez sur Appliquer dans la colonne Paramètre.

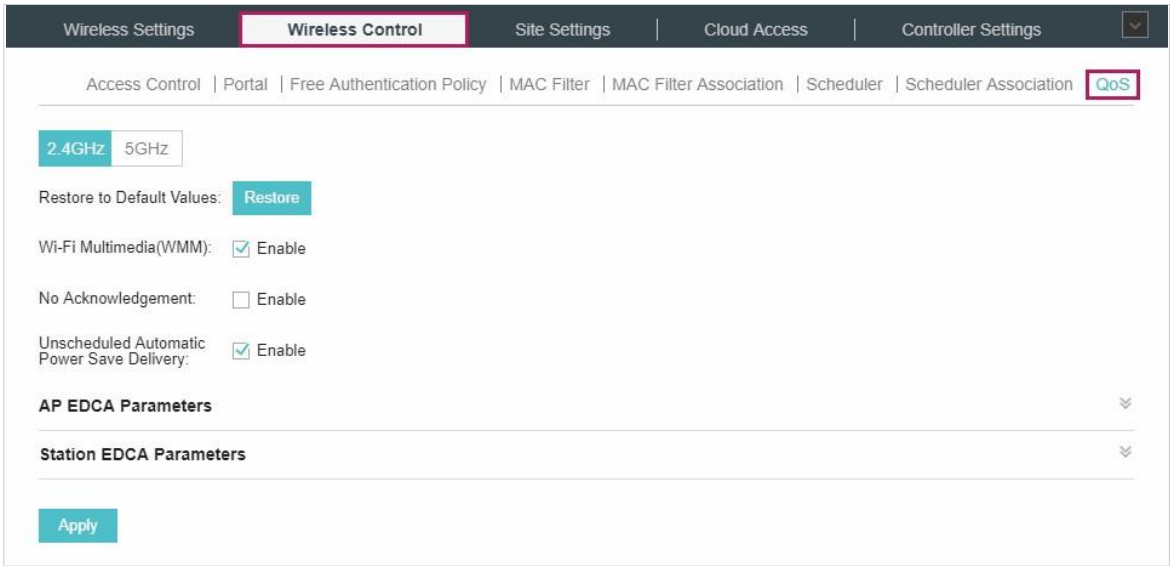
3.7 QoS

L'OC200 vous permet de configurer la qualité du service (QoS) sur le EAP pour un débit et des performances optimaux lors de la gestion du trafic sans fil différencié, tels que voice-over-IP(VoIP), d'autres types d'audio, vidéo, multimédia en streaming et données IP traditionnelles.

Pour configurer QoS sur le EAP, vous devez définir des paramètres sur les files d'attente de transmission pour différents types de trafic sans fil et spécifier des temps d'attente minimaux et maximums (via les fenêtres de contention) pour la transmission. En utilisation normale, nous vous recommandons de conserver les valeurs par défaut pour les EAP et la station EDCA (Accès canal distribué amélioré).

Suivez les étapes ci-dessous pour configurer QoS.

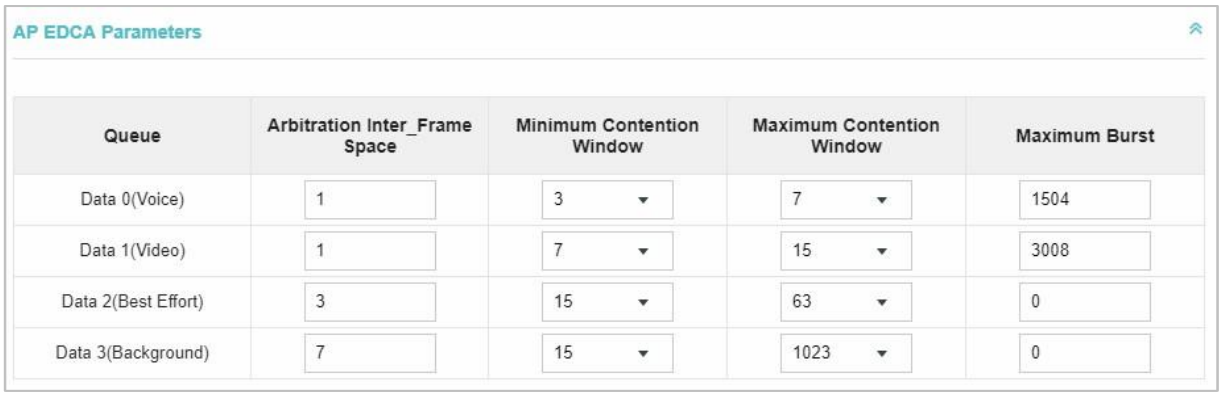
1. Accédez à Contrôle sans fil > QoS.



2. Activer ou désactiver les fonctionnalités suivantes.

Multimédia Wi-Fi (WMM)	Par défaut activé. Avec WMM activé, les EAP ont la fonction QoS pour garantir la haute priorité de la transmission de paquets audio et vidéo . Si le mode 802.11n seulement est sélectionné en mode mixte 2.4GHz (ou 802.11n seulement,802.11ac, ou802.11 n/ac en mode mixte 5GHz), le WMM doit être activé. Si WMM est désactivé, le mode 802.11n seulement ne peut pas être sélectionné en mode mixte 2.4GHz (ou 802.11n seulement,802.11ac ,ou 802.11 n/ac en mode mixte 5GHz).
Pas de reconnaissance	Par défaut désactivé. Vous pouvez activer cette fonction pour spécifier que les EAP ne doivent pas reconnaître les cadres avec QoS No Ack. L'activation d'aucune reconnaissance peut apporter un débit plus efficace, mais avec des taux d'erreur plus élevés dans un environnement bruyant de radiofréquence (RF). .
Automatique non planifiée Livraison d'économie d'énergie	Par défaut activé. En tant que méthode de gestion de l'énergie, elle peut grandement améliorer la capacité d'économie d'énergie des clients.

3. Cliquez sur Paramètres AP EDCA et la page suivante s'affiche. Les paramètres AP EDCA affectent le trafic qui s'écoule de l'EAP vers la station cliente. Nous vous recommandons d'utiliser les paramètres par défaut.



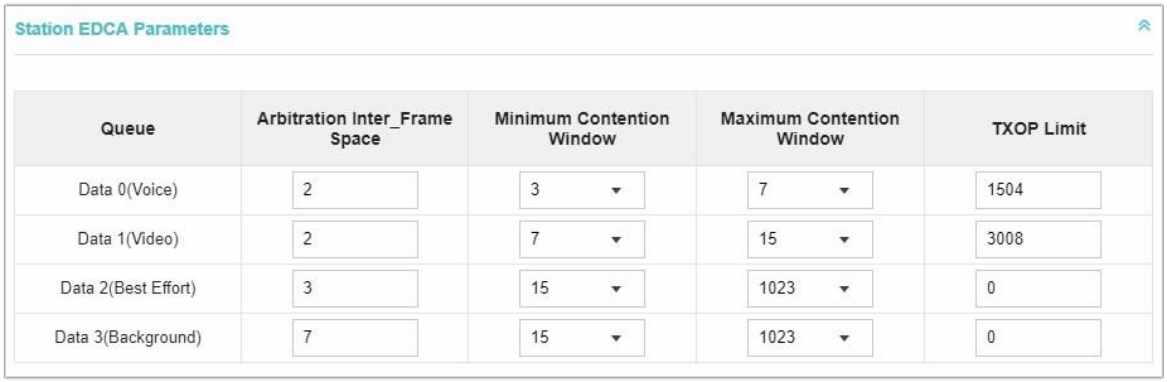
File d'attente	La file d'attente affiche la file d'attente de transmission. Par défaut, la priorité de haut en bas est data 0, data 1, data 2 et data 3. La priorité peut être modifiée si vous réinitialisez les paramètres DCA. Données 0 (Voix)— File d'attente prioritaire la plus élevée, délai minimum. Les données sensibles au temps telles que la VoIP et les supports de diffusion en continu sont automatiquement envoyées à cette file d'attente. Données 1 (Vidéo) — File d'attente prioritaire élevée, délai minimum. Les données vidéo sensibles au temps sont automatiquement envoyées à cette file d'attente. Données 2 (Meilleur effort) —File d'attente moyenne de priorité, débit moyen et retard. La plupart des données IP traditionnelles sont envoyées à cette file d'attente. Données 3 (Arrière-plan) — File d'attente prioritaire la plus basse, débit élevé. Les données en vrac qui nécessitent un débit maximal et sont non sensibles au temps sont envoyées à cette file d'attente (données FTP, par exemple).).

Arbitrage Inter-Espace cadre	Temps d'attente pour les images de données. Le temps d'attente est mesuré en créneaux horaires. Les valeurs valides pour l'espace inter-frame d'arbitrage sont de 0 à 15.
Contention minimale Fenêtre	Liste de l'algorithme qui détermine le temps d'attente aléatoire initial (fenêtre)pour la nouvelle tentative d'une transmission. Cette valeur ne peut pas être supérieure à la valeur de la fenêtre Contention maximale.
Contention maximale Fenêtre	Limite supérieure (en millisecondes)pour le doublement de la valeur de sauvegarde aléatoire. Ce doublement se poursuit jusqu'à ce que le cadre de données soit envoyé ou que la taille de la fenêtre contention maximale soit atteinte. Cette valeur doit être supérieure à la valeur de la fenêtre Contention minimale.
Rafale maximale	**Maximum Burp**t spécifie la longueur d'éclatement maximale autorisée pour les rafales de paquets sans fil sur le réseau. Une explosion de paquet est une collection de plusieurs images transmises sans informations d'en-tête. La diminution des frais généraux se traduit par un débit plus élevé et une meilleure performance.

4. Cliquez sur Paramètres **EDCA** de la station et la page suivante s'affiche.

   Les paramètres de la station EDCA affectent le trafic qui s'écoule de la station cliente vers le EAP.

   Nous vous recommandons d'utiliser les paramètres par défaut.



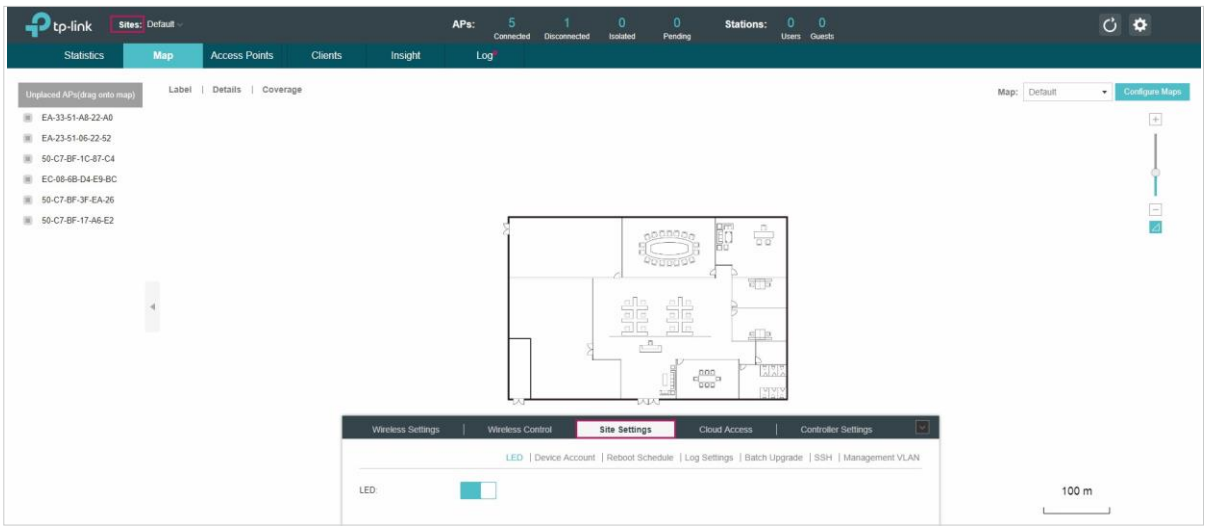
File d'attente	La file d'attente affiche la file d'attente de transmission. Par défaut, la priorité de haut en bas est data 0, data 1, data 2 et data 3. La priorité peut être modifiée si vous réinitialisez les paramètres EDCA. Données 0 (Voix)— File d'attente prioritaire la plus élevée, délai minimum. Les données sensibles au temps telles que la VoIP et les supports de diffusion en continu sont automatiquement envoyées à cette file d'attente. Données 1 (Vidéo) — File d'attente prioritaire élevée, délai minimum. Les données vidéo sensibles au temps sont automatiquement envoyées à cette file d'attente. Données 2 (Meilleur effort) —File d'attente moyenne de priorité, débit moyen et retard. La plupart des données IP traditionnelles sont envoyées à cette file d'attente. Données 3 (Arrière-plan) — File d'attente prioritaire la plus basse, débit élevé. Les données en vrac qui nécessitent un débit maximal et is non sensibles au temps sont envoyées à cette file d'attente (données FTP, par exemple).).

Arbitrage Inter-Espace cadre	Temps d'attente pour les images de données. Le temps d'attente est mesuré en créneaux horaires. Les valeurs valides pour l'espace inter-frame d'arbitrage sont de 0 à 15.
Contention minimale Fenêtre	Liste de l'algorithme qui détermine le temps d'attente aléatoire (fenêtre)pour la nouvelle tentative d'une transmission. Cette valeur ne peut pas être supérieure à la valeur de la fenêtre Contention maximale.
Contention maximale Fenêtre	Limite supérieure (en millisecondes) pour le doublement de la valeur de sauvegarde aléatoire. Ce doublement se poursuit jusqu'à ce que le cadre de données soit envoyé ou que la taille de la fenêtre contention maximale soit atteinte. Cette valeur doit être supérieure à la valeur de la fenêtre Contention minimale.
Limite TXOP	La limite TXOP est un paramètre EDCA de station et ne s'applique qu'au trafic qui circule de la station cliente vers le only EAP. L'opportunité de transmission (TXOP) est un intervalle de temps, en millisecondes, lorsqu'une station cliente WME a le droit d'initier des initiate transmissions sur le support sans fil (WM) vers le when EAP. Les valeurs valides sont des multiples de 32 entre 0 et 8192.

5. Cliquez sur Appliquer.

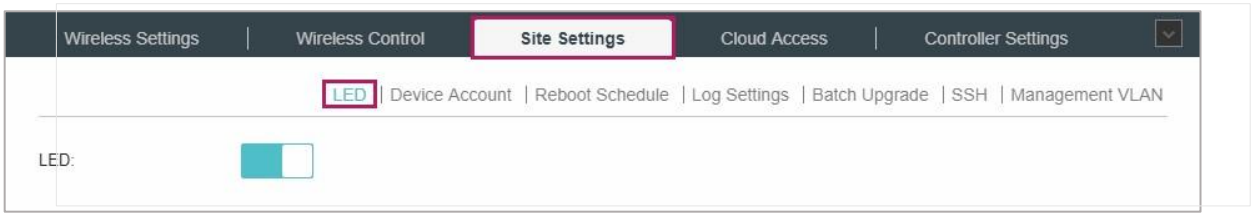
3.8 Paramètres du site

Vous pouvez configurer les paramètres spécifiques au site dans la page Paramètres du site. Pour changer de site, sélectionnez un site différent dans le menu déroulant Sites en haut de n'importe quel écran.



3.8.1 LED

Vous pouvez modifier l'état de la lumière LED sur les EAP de la page Paramètres du site > LED.



Par défaut, L'état LED est  ce qui signifient que les Lumières Led de tous les EAP sur le Site sont allumés

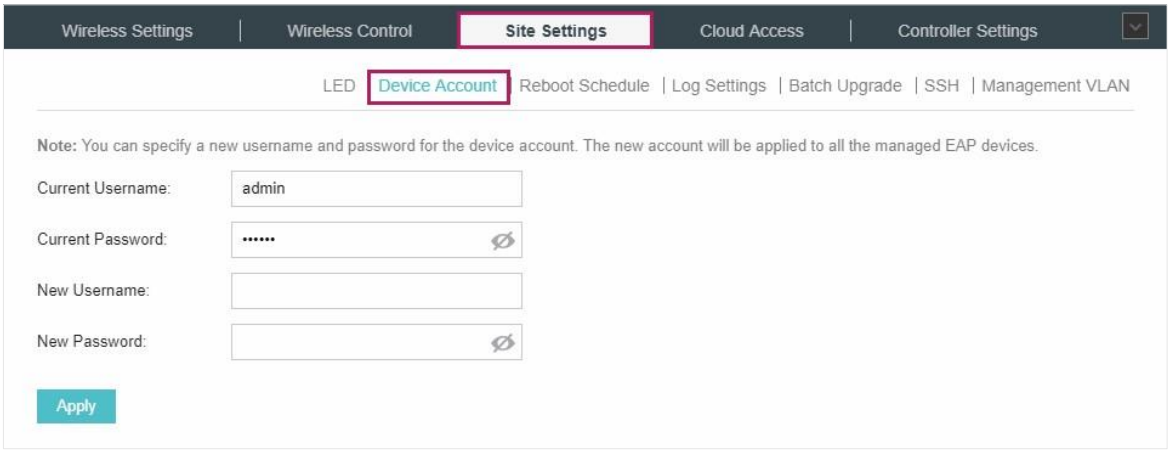
sur. Vous pouvez cliquer sur ce bouton pour modifier l'état de la lumière LED status. L'icône sera changée en  , ce qui signifie que toutes les lumières LED sont éteintes.

3.8.2 Compte de périphérique

Lorsque les EAP sont adoptés pour la première fois, leur nom d'utilisateur et leur mot de passe deviennent les mêmes que ceux des OC200 qui sont spécifiés dans configurations de base. Vous pouvez spécifier un nouveau nom d'utilisateur et mot de passe pour les EAP adoptés par lots.

Suivez les étapes ci-dessous pour modifier le nom d'utilisateur et le mot de passe des EAP.

1. Accédez aux paramètres du site > Compte de périphérique.



2. Spécifiez un nouveau nom d'utilisateur et mot de passe pour les EAP.

3. Cliquez sur Appliquer.

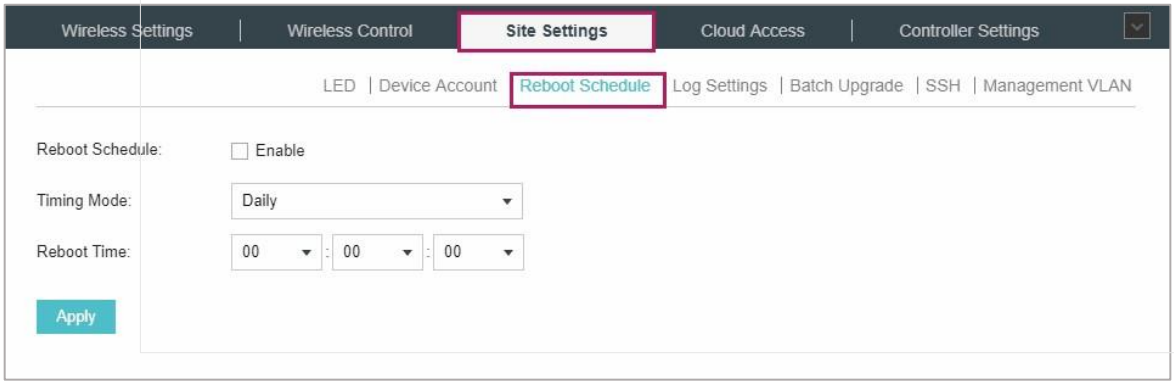
Notes

- Le nouveau compte sera appliqué aux EAP, mais pas à l'OC200. Pour modifier le nom d'utilisateur et le mot de passe de l'OC200, veuillez consulter le compte d'utilisateur Account.
- Le compte périphérique ne peut être consulté et modifié que lorsque vous vous connectez à l'OC200 en tant qu'administrateur Bien que l'opérateur et les comptes d'observateur n'ont pas l'autorisation.

3.8.3 Calendrier de redémarrage

Vous pouvez redémarrer tous les EAP du réseau périodiquement au besoin. Suivez les étapes ci-dessous pour configurer la planification du redémarrage.

1. Aller à Paramètres du site > Reboot Schedule (planification de redémarrage).



2. Cochez la case pour activer la fonction.

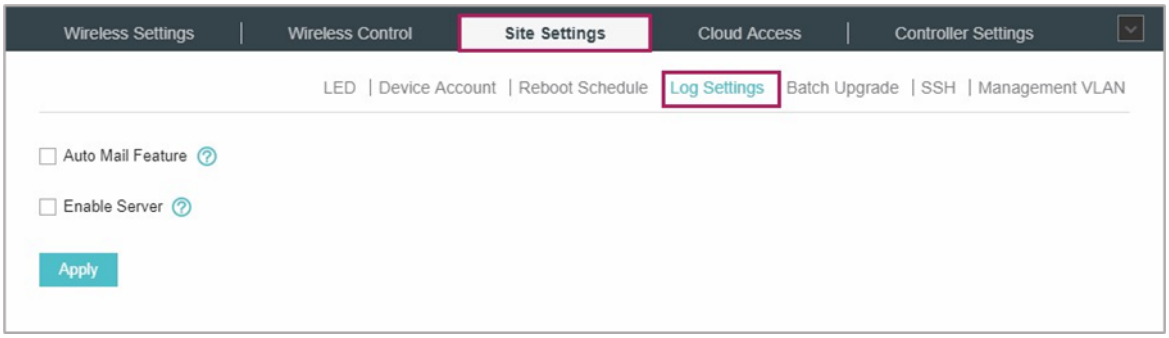
3. Choisissez Quotidien, hebdomadaire ou mensuel dans la liste déroulante Mode timing et définissez une heure spécifique pour redémarrer les EAP.

4. Cliquez sur Appliquer.

3.8.4 Paramètres du journal

Suivez les étapes ci-dessous pour choisir la façon de recevoir les journaux système.

1. Accédez aux paramètres du site > Paramètre de journal.



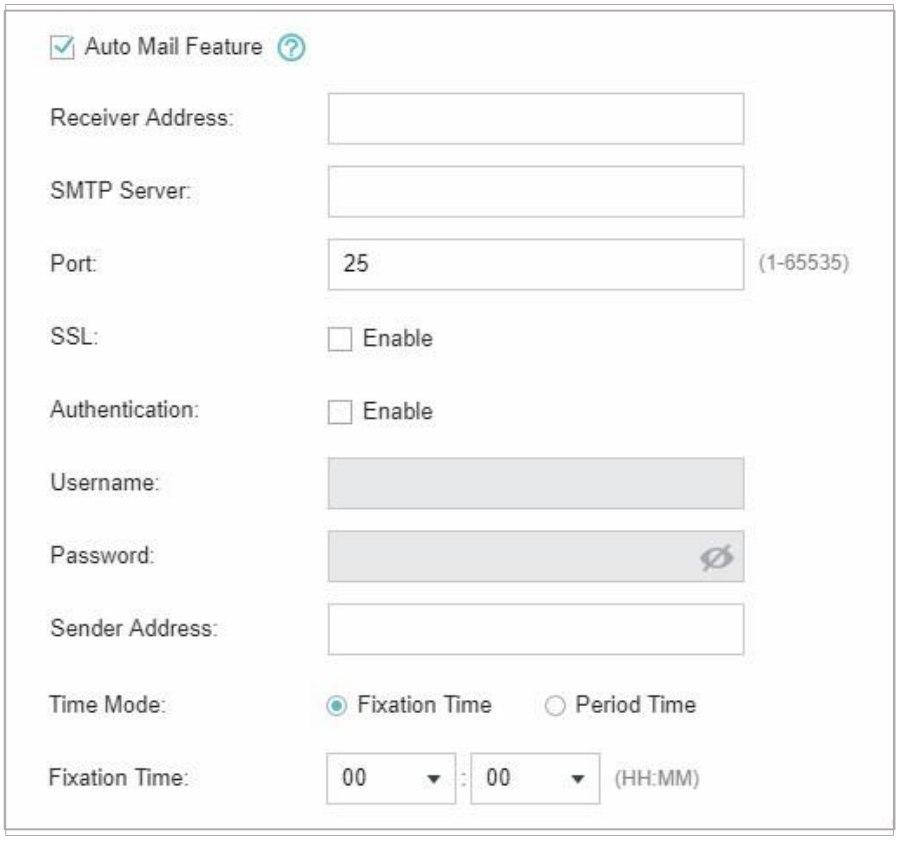
2. Cochez la case pour choisir les façons de recevoir les journaux système et cliquez sur Appliquer. Deux façons sont disponibles: Fonction de messagerie automatique et serveur. Vous pouvez choisir plus d'une façon.

Notes

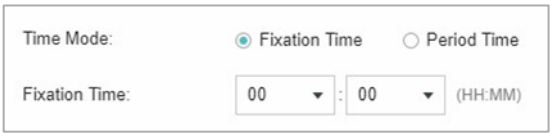
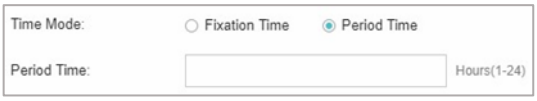
Les journaux et les alertes de l'OC200 avec la version 1.0.3 ou ci-dessous seront jetés après que l'OC200 a été mis à niveau vers la version 1.1.0 ou au-dessus.

Fonction de messagerie automatique

Si la fonctionnalité de messagerie automatique est activée, les journaux système seront envoyés à une boîte aux lettres spécifiées. Cochez la case pour activer la fonctionnalité et configurer les paramètres.



Adresse du récepteur	Entrez l'adresse e-mail du récepteur.
Serveur SMTP	Entrez l'adresse IP ou le nom de domaine du serveur SMTP.
Port	Le serveur SMTP utilise le port 25 comme valeur par défaut. Si SSL est activé, le numéro de port passera automatiquement à 465.
Ssl	Vous pouvez cocher la case pour activer SSL (Security Socket Layer) pour améliorer les communications sécurisées sur Internet.
Authentification	Vous pouvez cocher la case pour activer l'authentification du serveur de messagerie. Entrez le nom et le mot de passe du compte de messagerie de l'expéditeur.
nom d'utilisateur	Entrez le nom du compte de messagerie de l'expéditeur.
mot de passe	Entrez le mot de passe de messagerie de l'expéditeur.

Adresse de l'expéditeur	Entrez l'adresse de messagerie de l'expéditeur
Mode temps	Sélectionnez Le mode Heure. Les journaux système peuvent être envoyés à un moment ou à un intervalle de temps spécifiques.
Heure de fixation	Si vous sélectionnez Temps de fixation, spécifiez une heure fixe pour envoyer les journaux système. Par exemple, 08:30 indique que le courrier sera envoyé à 8h30 tous les jours. 
Durée	Si vous sélectionnez Période, spécifiez un délai pour envoyer régulièrement le courrier journal système. Par exemple,6 indique que le courrier sera envoyé toutes les six heures. 

Serveur

3.8.5 Mise à niveau par lots

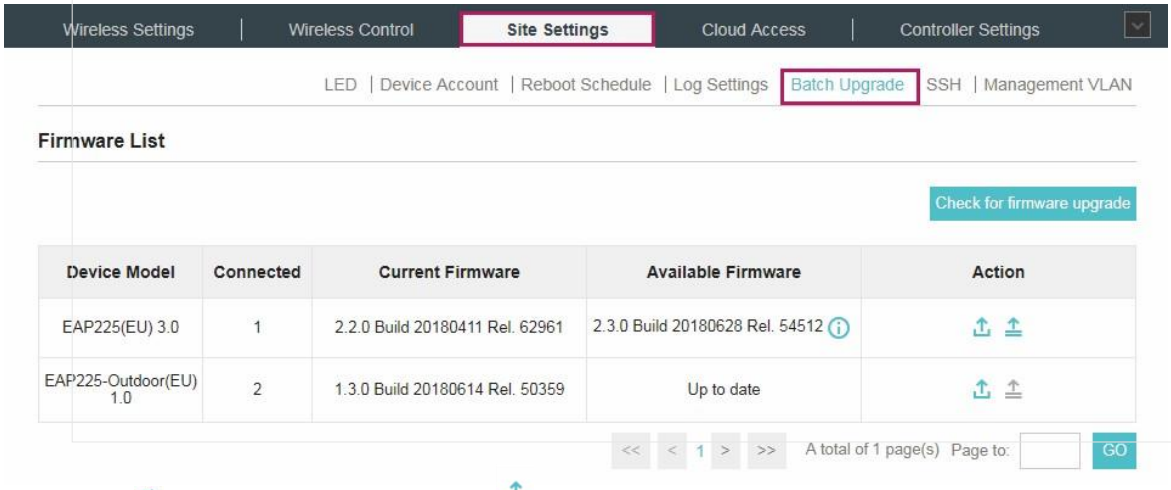
Vous pouvez mettre à niveau vos EAP du même modèle en lots à l'aide de la mise à niveau par lots. Deux options sont disponibles pour la mise à niveau : mettre à niveau en ligne et mettre à niveau manuellement.

Mise à niveau en ligne

Le dernier firmware pour les EAP peut être détecté par l'OC200 automatiquement, et vous pouvez mettre à niveau les EAP en ligne. Ainsi, vous n'avez pas besoin d'enregistrer les fichiers du firmware localement à l'avance. need

Suivez les étapes ci-dessous pour mettre à niveau les EAP en ligne en fonction de leur modèle.

1. Accédez aux paramètres du site > Mise à niveau par lots. Le modèle de l'appareil, le montant, le firmware actuel et le firmware disponible apparaîtront sur la liste du firmware .



2. Dans Action Cliquez sur pour mettre à niveau l'appareil

Après la mise à niveau, l'appareil redémarrera automatiquement.

Idées

- Vous pouvez cliquer Check for firmware upgrade pour vérifier si le dernier firmware est disponible.
- Vous pouvez cliquer dans la colonne Firmware disponible pour afficher la note de sortie du firmware, qui peut vous aider à connaître les nouvelles fonctionnalités ou améliorations de ce firmware.

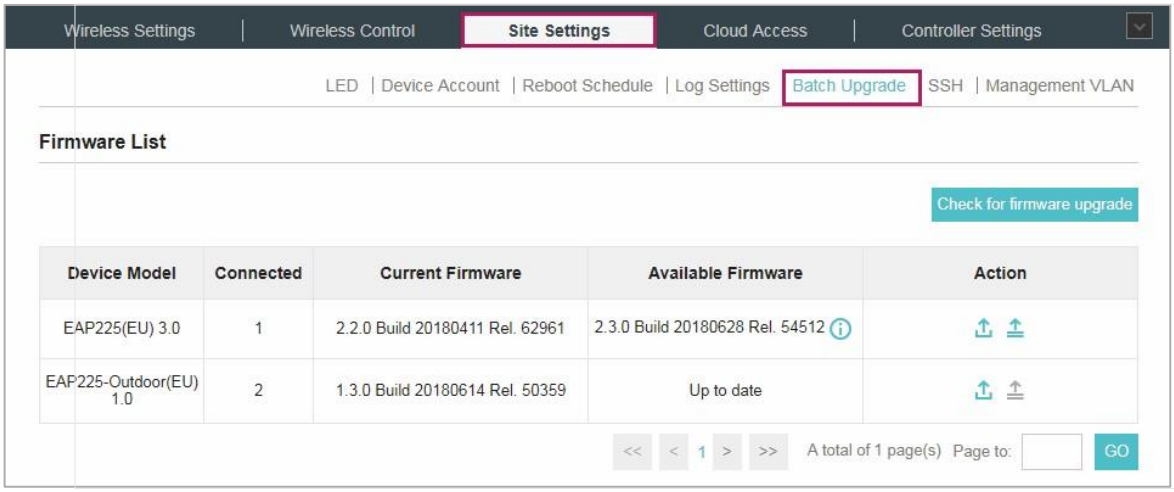
Mise à niveau manuelle

Les derniers fichiers firmware peuvent être téléchargés à partir du centre de téléchargement du site Web TP-Link. Ensuite, vous pouvez mettre à niveau les EAP manuellement.

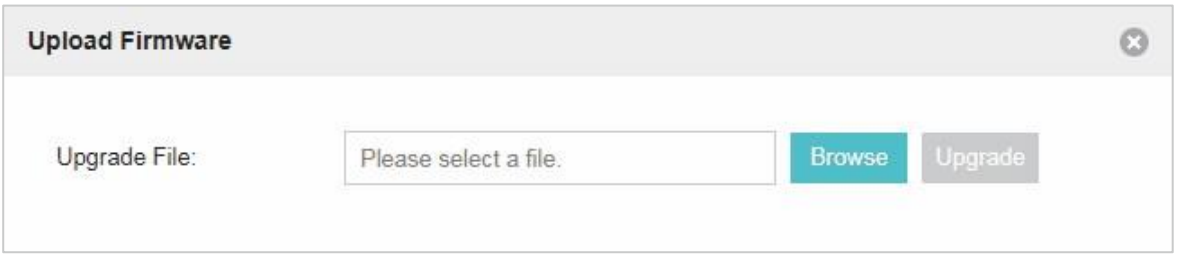
Suivez les étapes ci-dessous pour mettre à niveau les EAP maually selon leur modèle.

1. Visitez https://www.tp-link.com/en/support/download/ pour télécharger le dernier fichier firmware du modèle correspondant.

2. Aller àParamètres du site > Mise à niveau par



3. Dans le menu Action Cliquez sur pour mettre à niveau



4. Cliquez sur Parcourir pour localiser et choisir le fichier firmware approprié pour le modèle.

5. Cliquez sur Mise à niveau pour mettre à niveau l'appareil.

Après la mise à niveau,l'appareil redémarrera automatiquement.

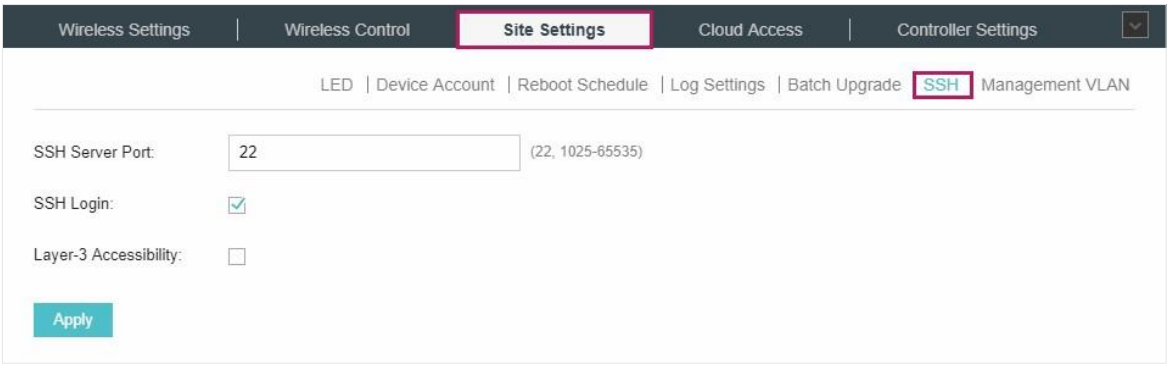
Notes

- Le EAP ne peut pas être mis à niveau manuellement lorsque vous accédez à l'OC200 via Omada Cloud.
- Pour éviter les dommages, veuillez ne pas éteindre l'appareil lors de la mise à niveau.

3.8.6 SSH

SSH est un protocole fonctionnant dans la couche d'application et la couche de transport. Il peut fournir une connexion sécurisée et distante à un appareil. Après avoir permis la connexion SSH ici, vous pouvez vous connecter aux EAP via SSH. Suivez les étapes ci-dessous pour configurer SSH sur l'OC200 :

1. Accédez au paramètre de site > SSH. Entrez le numéro de port du serveur SSH.



2. Cochez la case pour activer la connexion SSH. Si vous souhaitez vous connecter au EAP à partir d'un sous-réseau différent via SSH, activez l'accessibilité de la couche-3.

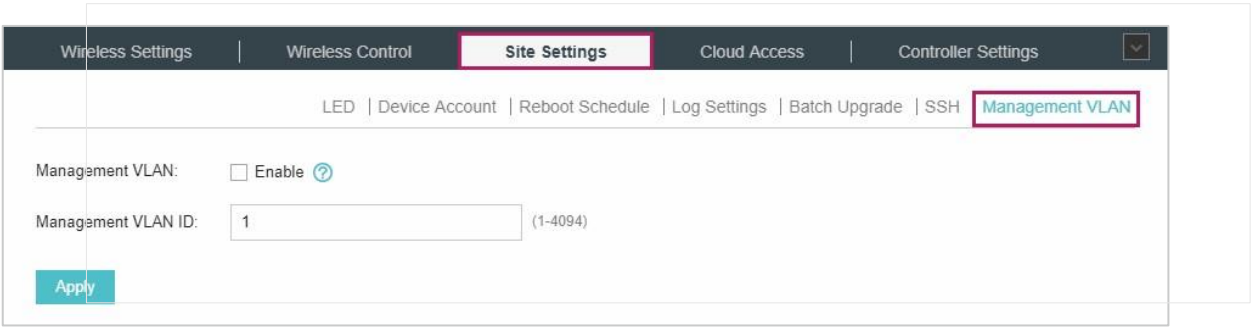
3. Cliquez sur Appliquer.

3.8.7 Gestion VLAN

Management VLAN vous offre un moyen plus sûr de gérer le EAP. Avec Management VLAN activé, seuls les hôtes de la gestion VLAN peuvent gérer le EAP. Étant donné que la plupart des hôtes ne peuvent pas traiter les TAG VLAN , connecter l'hôte de gestion au réseau via un commutateur et configurer les paramètres VLAN corrects pour les commutateurs du réseau afin d'assurer la communication entre l'hôte et le EAP dans la gestion VLAN.

Suivez les étapes ci-dessous pour configurer Management VLAN.

1. Accédez à Paramètres de site > Gestion VLAN. Cochez la case pour activer Management VLAN.



2. Spécifiez l'ID Gestion VLAN. L'ID VLAN par défaut est 1.

3. Cliquez sur Appliquer.

4 Service Cloud Omada

TP-Link Omada Cloud Service offre une meilleure façon de réaliser la gestion à distance. Avec l'accès cloud activé sur l'OC200 et un ID TP-Link lié à votre OC200, vous pouvez facilement surveiller et gérer votre réseau sans fil. Pour vous assurer que vos EAP restent nouveaux et s'améliorent avec le temps, l'Omada Omada Cloud vous informera lorsqu'une nouvelle mise à niveau du firmware sera disponible. Vous pouvez également gérer plusieurs OC200 avec un seul ID TP-Link.

Suivez les étapes ci-dessous pour configurer l'accès au cloud et accéder à l'OC200 via Omada Cloud :

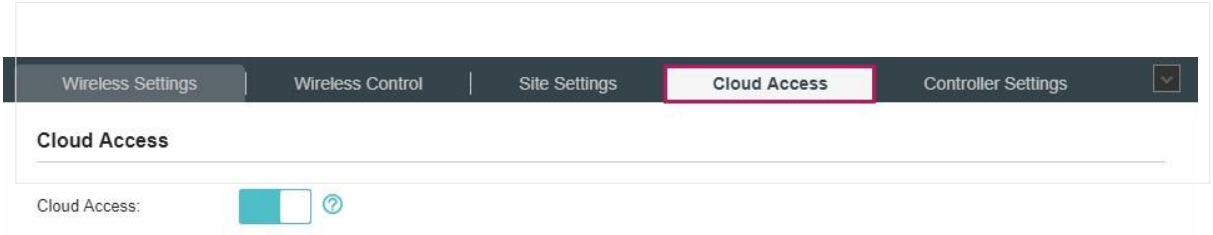
1. Configurer l'accès au cloud
2. Gérer l'OC200 via Omada Cloud

4.1 Configurer l'accès au cloud

4.1.1 Activer l'accès au cloud

Vous pouvez configurer l'OC200 via Omada Cloud uniquement lorsque l'accès cloud est activé sur l'OC200 et que vous avez été ajouté en tant qu'utilisateur cloud.

Sur la page Accès cloud, vous pouvez configurer Cloud Access. Cliquez sur le bouton pour activer le Cloud.



4.1.2 Gérer les utilisateurs du cloud

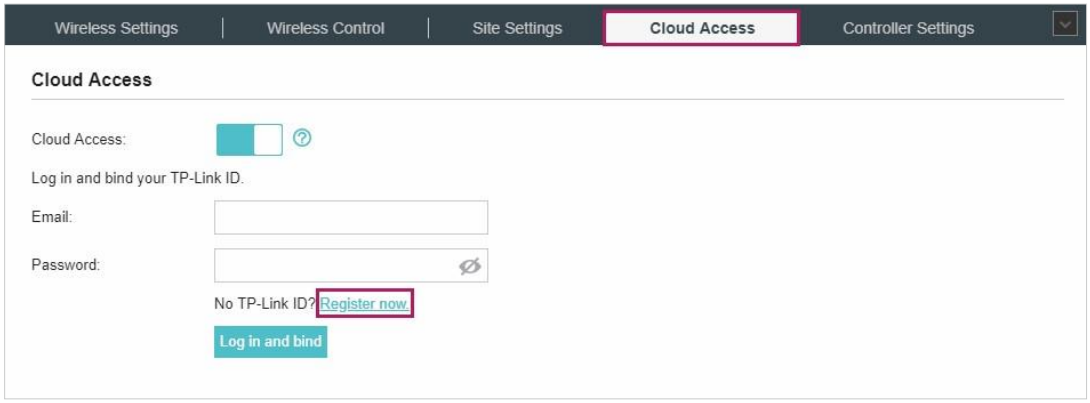
Pour configurer et gérer OC200 via le service Cloud, vous devez disposer d'un a ID TP-Link et lier votre ID TP-Link à l'OC200. Ensuite, vous pouvez accéder à distance à l'OC200 en tant qu'utilisateur a cloud.

Notes

Pour enregistrer un ID TP-Link et le lier à votre OC200, assurez-vous que l'hôte de gestion peut accéder à Internet. make

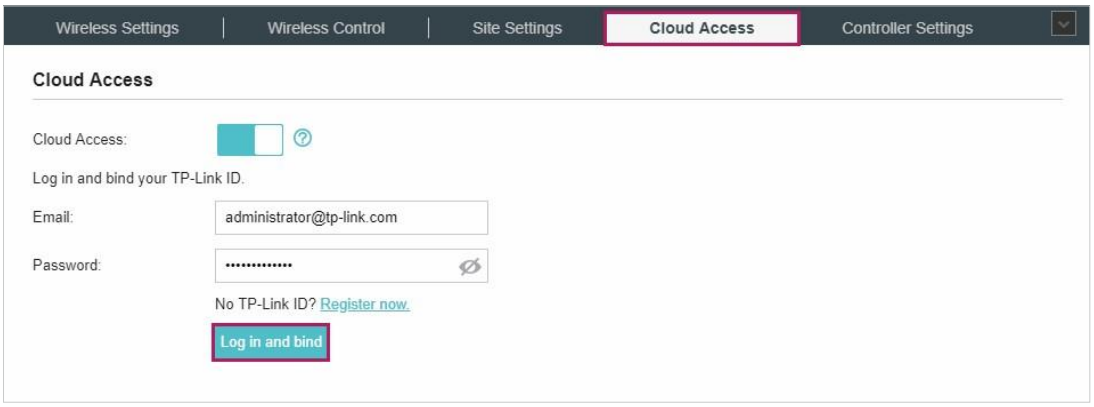
Enregistrer un ID TP-Link

Dans le processus d'installation rapide, vous pouvez enregistrer un ID TP-Link et le lier à votre OC200. Si vous avez ignoré l'enregistrement pendant le processus d'installation rapide, vous pouvez accéder à Accès cloud. Cliquez sur Inscrivez-vous maintenant et suivez les instructions pour enregistrer un ID TP-Link.



Connectez-vous et lier votre ID TP-Link

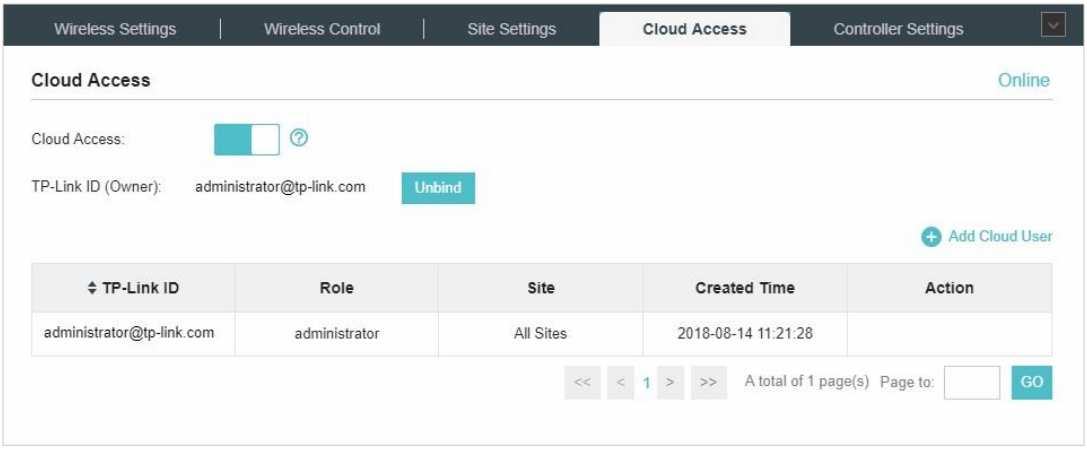
Après avoir activé votre ID TP-Link,revenez à la page Accès cloud pour vous connecter et lier votre ID TP-Link à votre OC200.



L'ID TP-Link qui est lié à l'OC200 pour la première fois sera automatiquement lié en tant qu'administrateur.

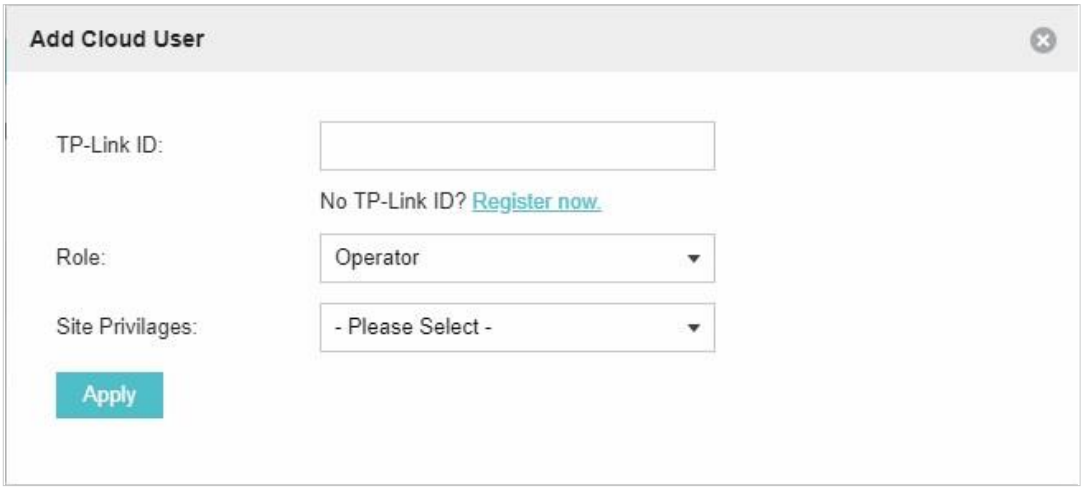
Et un seul **ID TP-Link** peut être lié à l'OC200 en tant qu'administrateur.

Un compte d'administrateur peut ajouter ou supprimer d'autres ID TP-Link vers ou depuis le même OC200 que les utilisateurs du cloud.



Ajouter de nouveaux utilisateurs cloud

Une fois que vous êtes connectez avec Id TP-Link administrateur, vous Ajouter de nouveaux utilisateurs Ou un autre Id TP-Link au besoin en cliquant sur Add Cloud User

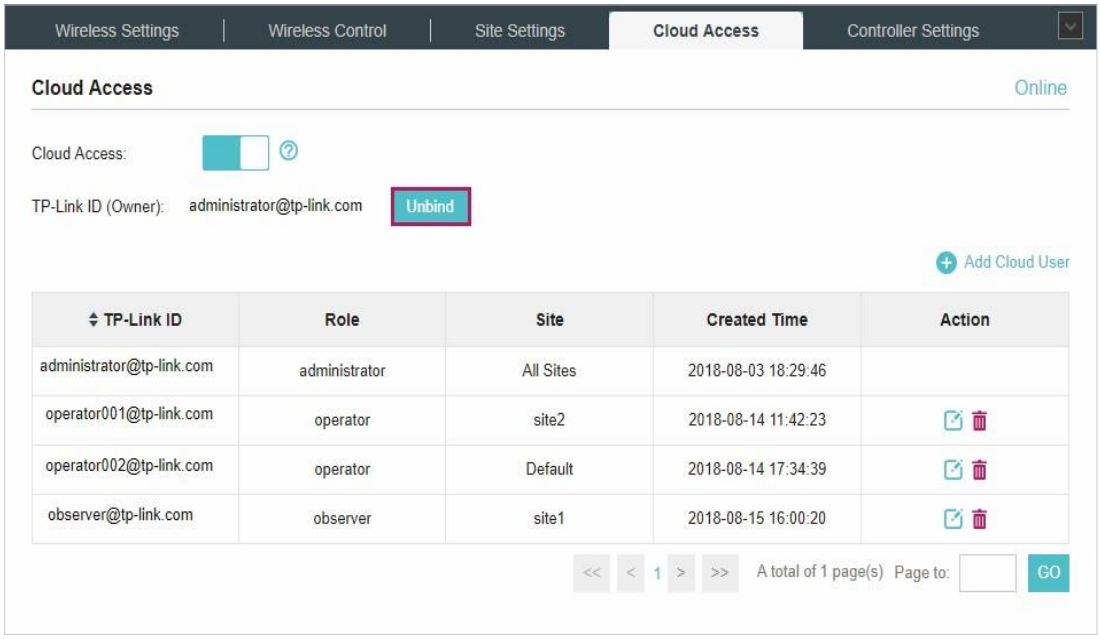


ID TP-Link	Entrez l'ID TP-Link que vous souhaitez ajouter en tant que nouvel utilisateur cloud. Si vous n'avez pas d'autre ID TP-Link, vous pouvez cliquer sur Enregistrer maintenant et suivre les instructions pour enregistrer un ID TP-Link.
Rôle	Sélectionnez le rôle du nouvel utilisateur du cloud dans la liste déroulante. Deux options sont fournies. **Opérateur :** Un compte opérateur peut modifier les paramètres des sites privilégiés qui sont donnés par l'administrateur . Et le compte Opérateur ne peut pas gérer les utilisateurs du cloud et modifier les paramètres. **Observateur** : un compte Observateur ne peut afficher que l'état et les paramètres des sites privilégiés qui sont donnés par l'administrateur, mais ne modifient pas les paramètres. Les comptes Opérateur et Observateur ne peuvent pas gérer les utilisateurs et les paramètres du cloud. Ainsi, les comptes opérateur et observateur ne peuvent être créés ou supprimés que par l'administrateur

Privilèges de site	Sélectionnez les sites privilégiés (plusieurs options disponibles)pour les comptes Opérateur ou Observateur dans la liste déroulante.

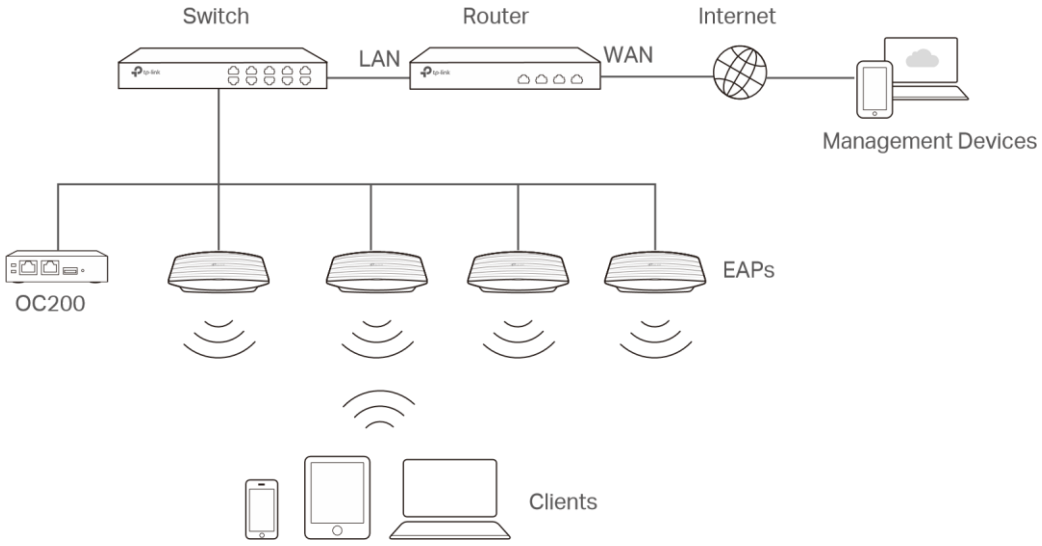
Délier un ID TP-Link

Vous pouvez cliquer sur Débiner pour délier votre ID TP-Link administrateur. Notez que l'opération Unbind ne peut pas être effectuée lorsque vous vous connectez au service OC200 via Omada Cloud. that



4.2 Gérer l’OC200 via Omada Cloud

Avec l’accès cloud activé, vous pouvez gérer votre OC200 à distance à l’aide de votre ID TP-Link. Vous pouvez vous référer à la topologie suivante.



Avant d’accéder à distance à votre OC200, assurez-vous que les exigences suivantes ont été remplies

■ L’accès au cloud est activé sur l’OC200.

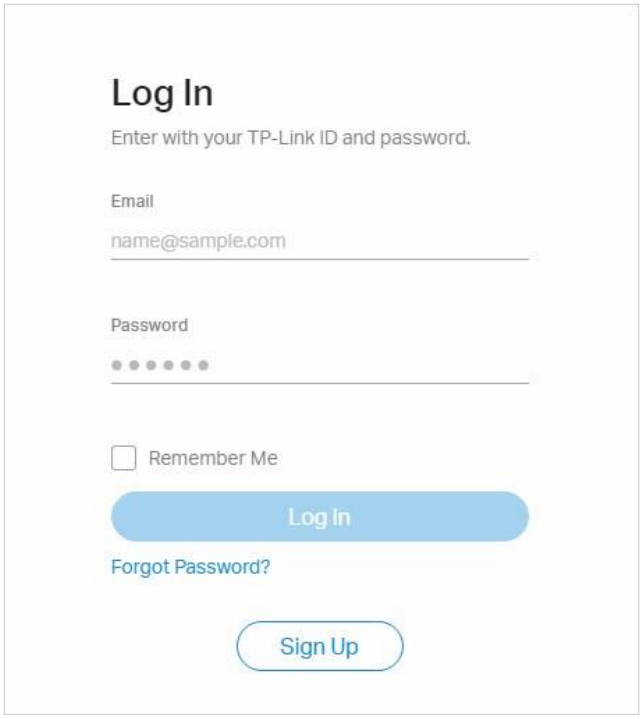
■ Votre OC200 a été lié par un ID TP-Link. Si vous n’avez pas d’ID a TP-Link, reportez-vous à Enregistrer un ID TP-Link pour en obtenir un.

■ Vos appareils OC200 et vos appareils de gestion ont accès à Internet.

4.2.1 Accédez à l’OC200 via Omada Cloud

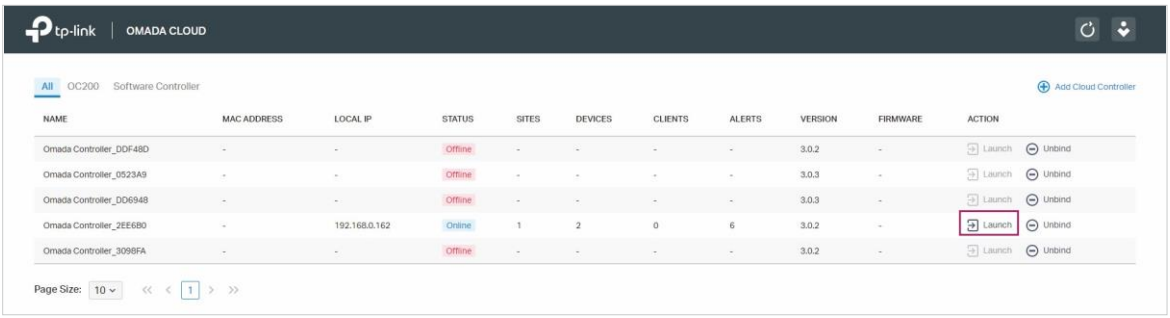
1. Lancez un navigateur Web et tapez https://omada.tplinkcloud.com dans la barre d’adresses, puis appuyez sur Entrée (Windows) ou Retour (Mac).

2. Entrez votre ID TP-Link et votre mot de passe, puis cliquez sur Connexion.

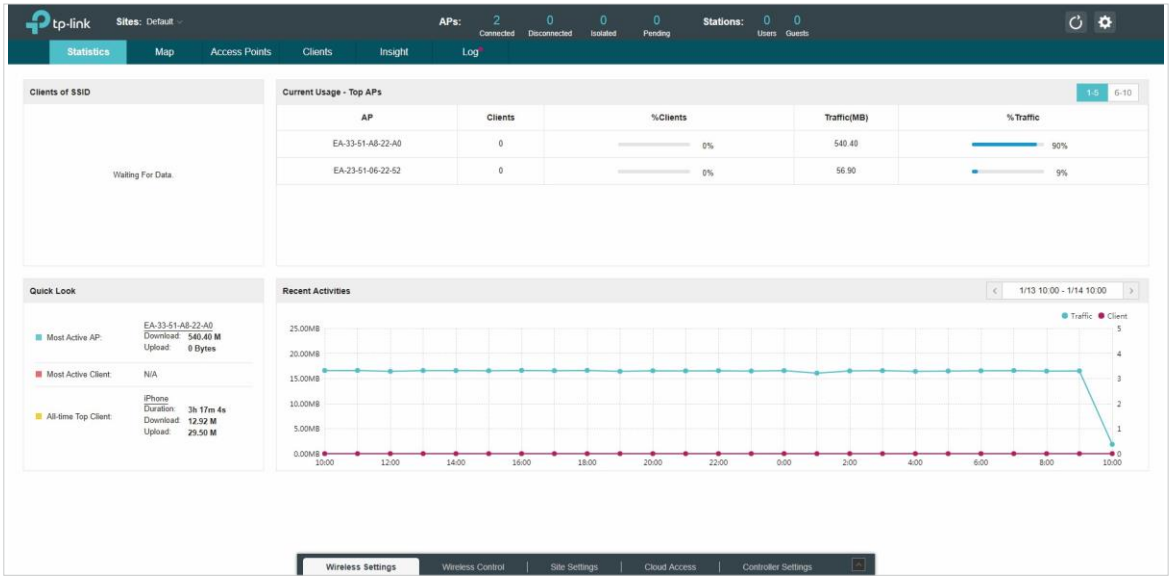


3. Une fois que vous vous êtes connecté à Omada Cloud, une liste de contrôleurs liés à votre ID TP-Link

. Si l’OC200 n’a-t-il pas dans la liste, vous sur Pour actualiser la page cours.



Cliquez sur Lancement pour accéder à votre OC200. Ensuite, vous pouvez configurer et gérer votre OC200.



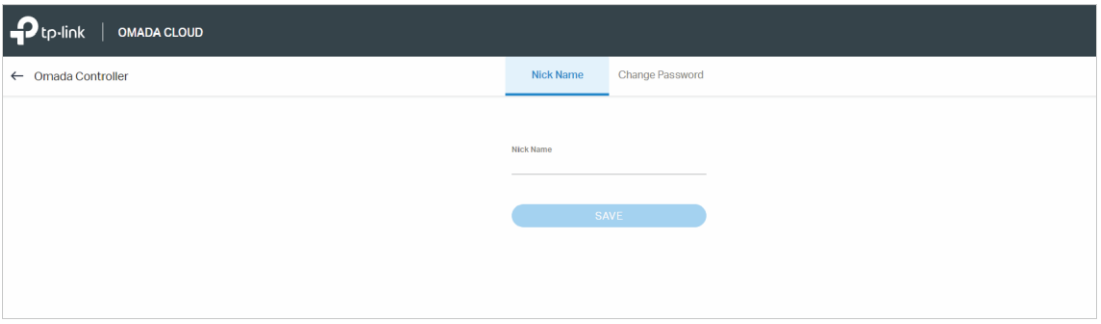
Notes

- Pour supprimer l'OC200 de votre compte cloud, vous pouvez cliquer sur Unbind.
- Pour déconnecter Omada Cloud, cliquez et sélectionnez Déconnecter.

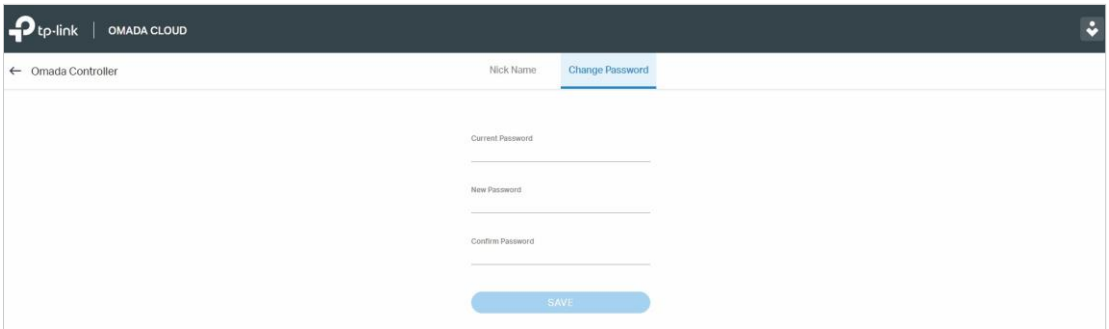
4.2.2 Modifier vos informations d'identification TP-Link

Vous pouvez modifier vos informations d'identification TP-Link sur la page Cloud d'Omada. Cliquez et sélectionnez Mon ID TP-Link, les paramètres de comptabilité cloud s'affichent .

Vous pouvez avoir un surnom pour votre ID TP-Link. Entrez votre nom de pseudo et cliquez sur Enregistrer.



Vous pouvez également modifier le mot de passe de votre ID TP-Link. Entrez le mot de passe actuel, puis un nouveau mot de passe deux fois et cliquez sur Enregistrer.



5 Configurer les EAP séparément

En plus de la configuration globale, vous pouvez configurer les EAP séparément et les résultats de configuration seront appliqués à un EAP spécifié.

Pour configurer un EAP spécifié, veuillez cliquer sur le nom du EAP sous l'onglet Points d'accès ou sur le EAP connecté sur la carte. EAP's Ensuite, vous pouvez afficher les informations détaillées du EAP et configurer le EAP dans la fenêtre contextuelle.

Ce chapitre comprend le contenu suivant :

■ Voir les informations du EAP

Voir les clients se connecter au EAP

■ Afficher les informations sur les mailles du EAP

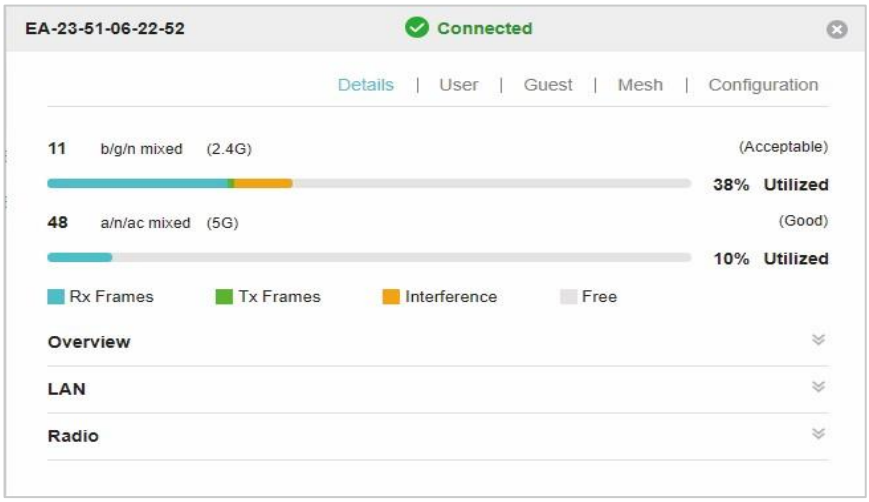
Configurer le EAP

5.1 Voir les informations du EAP

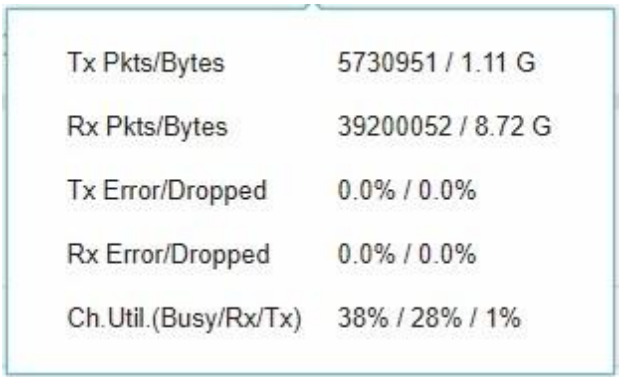
5.1.1 Vue d'ensemble

Les informations de canal actif sur chaque bande radio seront affichées dans un graphique à barres, qui indique ses pourcentages suivants :

- Rx Frames (bleu),
- Tx Frames (vert),
- Interférence (orange) et
- Bande passante libre (gris). Le pourcentage d'utilisation du canal s'affiche également avec l'évaluation correspondante .



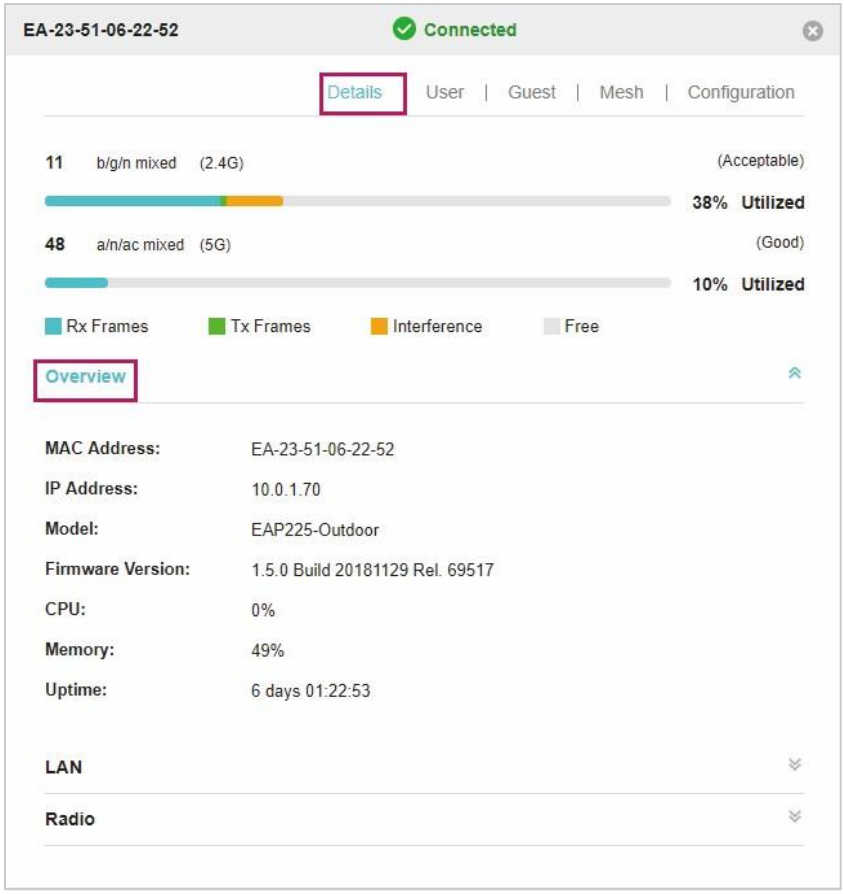
Vous pouvez cliquer sur un point sur l'un ou l'autre graphique à barres pour plus de détails:



Tx Pkts/Octets	Affiche la quantité de données transmises sous forme de paquets et d'octets.
Rx Pkts/Octets	Affiche la quantité de données reçues sous forme de paquets et d'octets.
ErreurTx/Dropped	Affiche le pourcentage de paquets de transmission qui présentent des erreurs et le pourcentage de paquets qui ont été supprimés .
Rx Erreur/Dropped	Affiche le pourcentage de paquets de réception qui présentent des erreurs et le pourcentage de paquets qui ont été supprimés .
Ch.Util.(Occupé /Rx/Tx)	Affiche channel les statistiques d'utilisation des canaux. Occupé : Ce nombre est la somme de Tx, Rx,et aussi non-interférence Wi-Fi , ce qui indique comment le canal est occupé . Rx: Ce numéro indique la fréquence à laquelle la radio est en mode de réception active. Tx: Ce numéro indique la fréquence à laquelle la radio est en mode de transmission active.

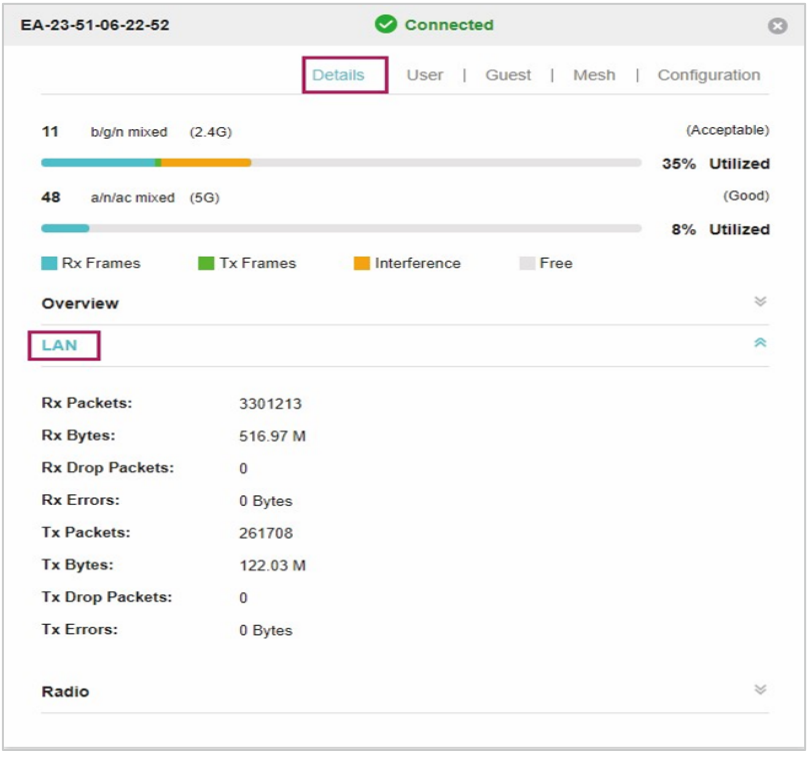
5.1.2 Informations de base

Cliquez sur Aperçu pour afficher les informations de base du EAP qui inclut l'adresse MAC du EAP (ou le nom que vous définissez), l'adresse IP, le modèle, la version du firmware, le taux d'utilisation du processeur et de la mémoire et le temps de disponibilité (indique combien de temps le EAP a été en cours d'exécution sans interruption).



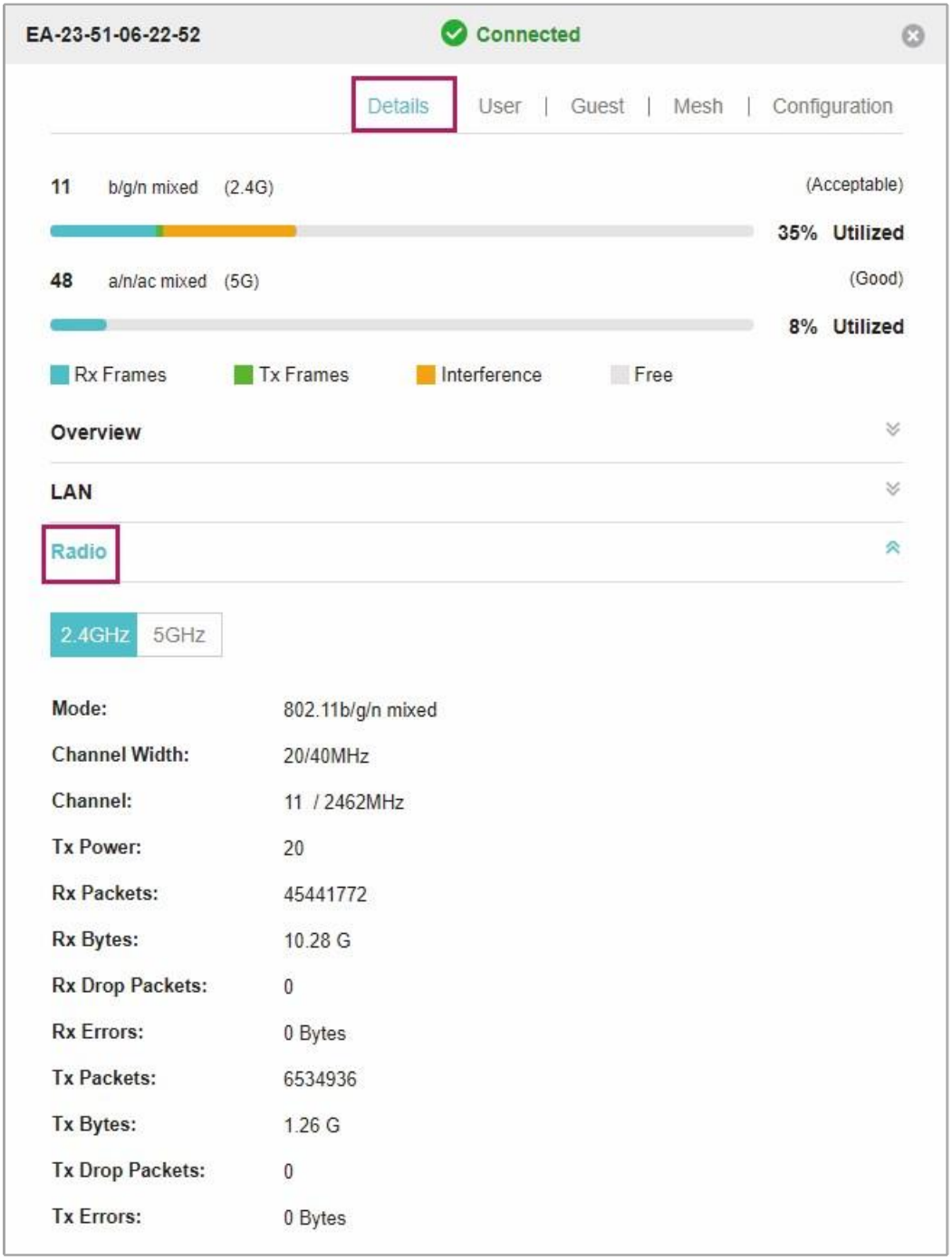
5.1.3 LAN

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.



5.1.4 Radio

Cliquez sur Radio pour afficher les informations radio, y compris la bande de fréquences, le mode sans fil, la largeur du canal, le canalet la puissance de transmission. Vous pouvez également afficher les paramètres de, réception/transmission de données sur chaque bande radio.

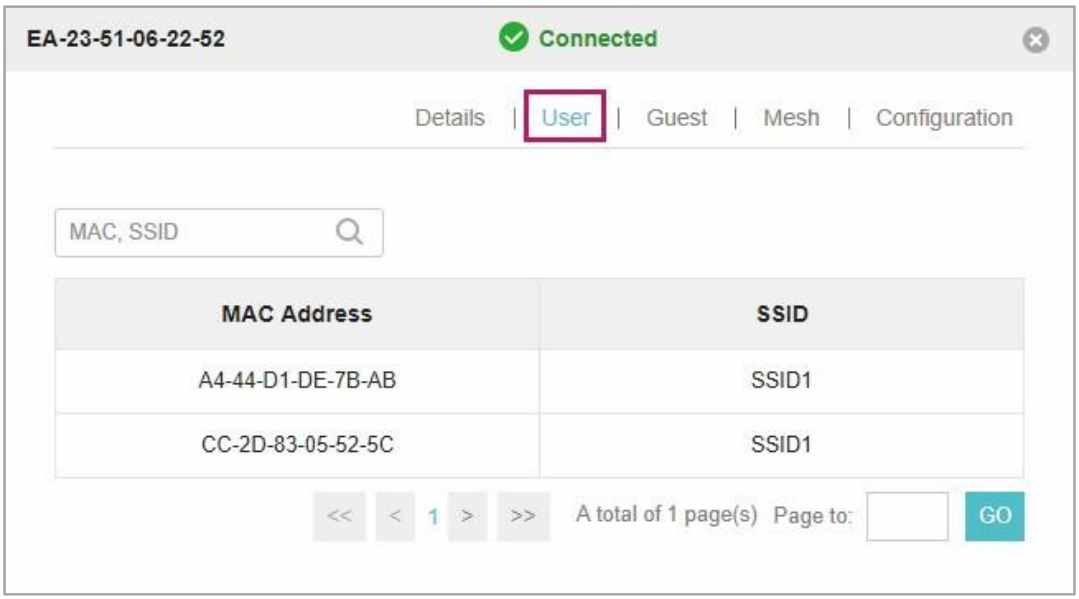


5.2 Afficher les clients se connectant au EAP

5.2.1 **Utilisateur**

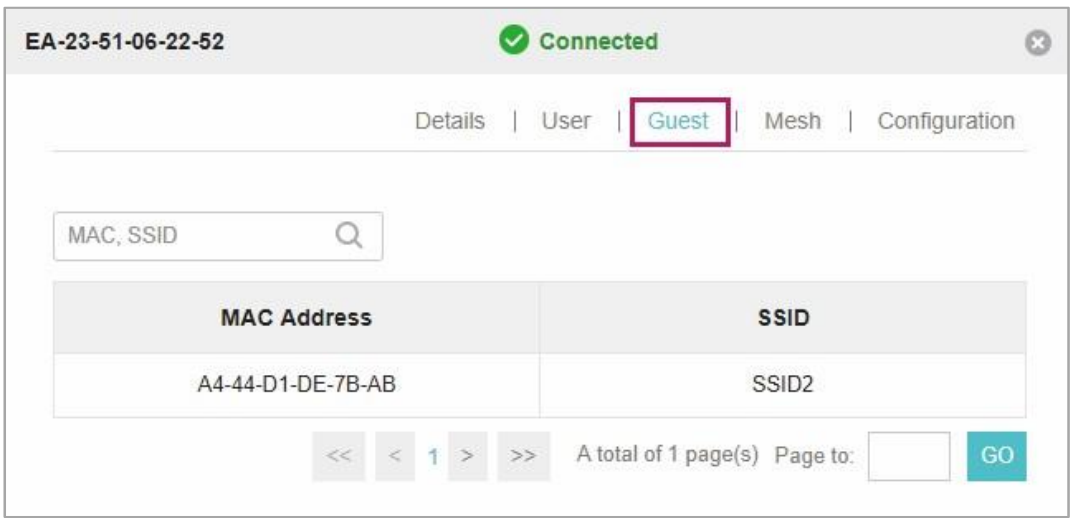
La page **Utilisateur** affiche les informations des clients se connectant au SSID avec le portail désactivé, y compris leurs adresses MAC et les SSID connectés.

Vous pouvez cliquer sur l'adresse MAC du client pour obtenir son historique de connexion.



5.2.2 Invité

La page Invité affiche les informations des clients se connectant au SSID avec portal activé, y compris leurs adresses MAC et SSID connectés. Vous pouvez cliquer sur l'adresse MAC s du client pour obtenir son historique de connexion.

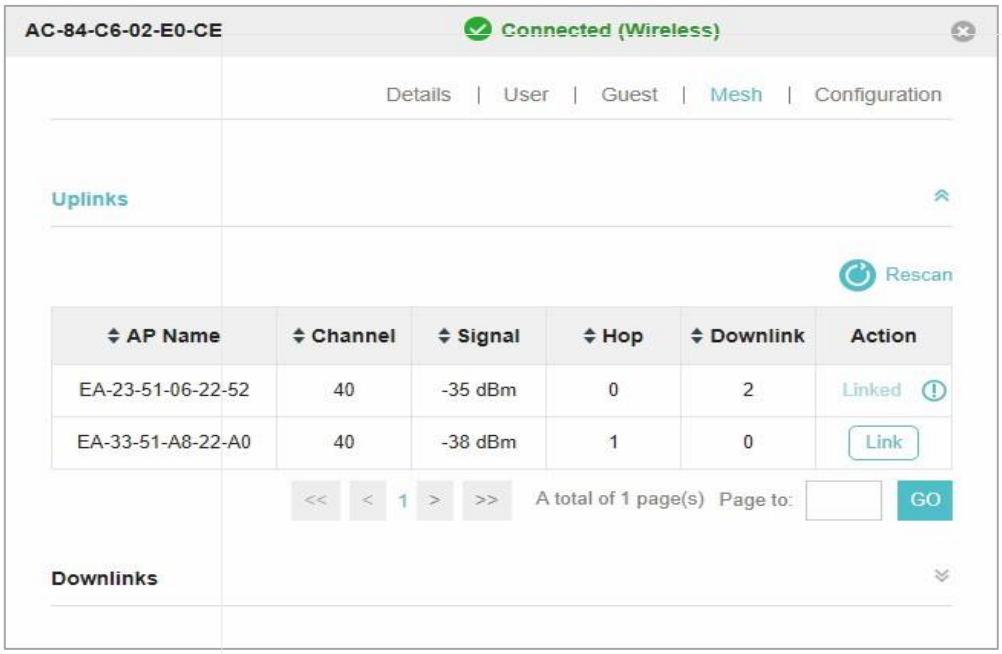


5.3 Afficher les informations sur les mailles du EAP

La page Mesh est utilisée pour afficher et configurer les paramètres de maillage du EAP.

5.3.1 Liens d'élicut

Ici, vous affichez les paramètres des Ap Liaison montante ou Link



Rescan

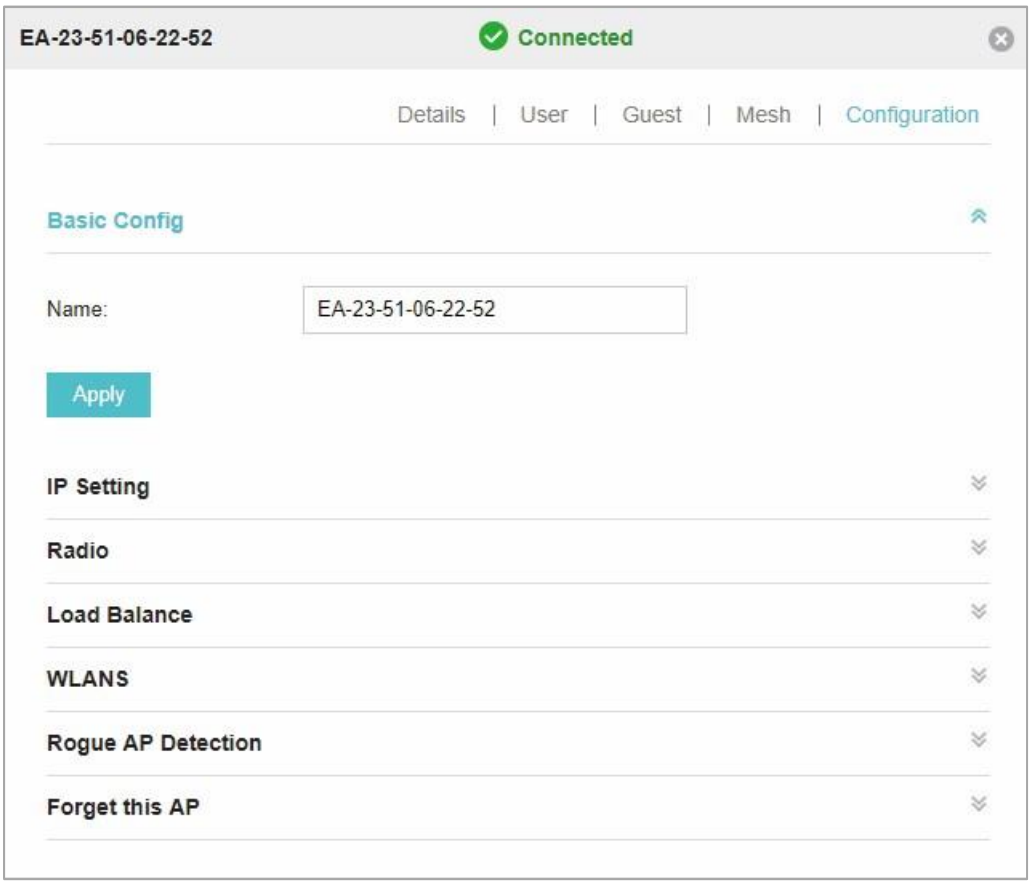
- À rechercher La Disponible Liaison montante Aps et le Liaison montante Liste sera Actualiser.
- Pour créer un réseau de maillage avec de meilleures performances, nous vous recommandons de sélectionner MESH with l'AP Uplink avec le signal le plus fort, le moins de saut et moins Downlink AP.

5.3.2 Liaisons vers le bas

Ici, vous voir les Ap Descendante.

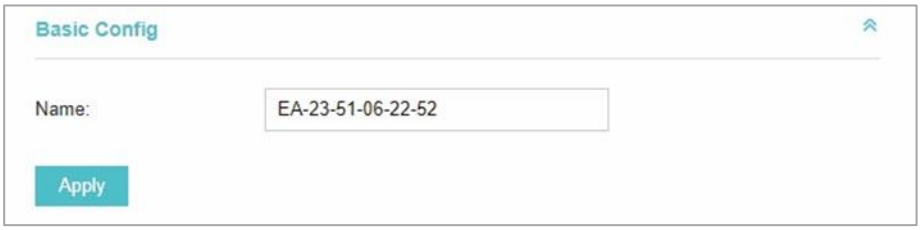
5.4 Configurer le EAP

La page Configuration est utilisée pour configurer le EAP. Toutes les configurations n'entreront en vigueur que sur cet appareil.



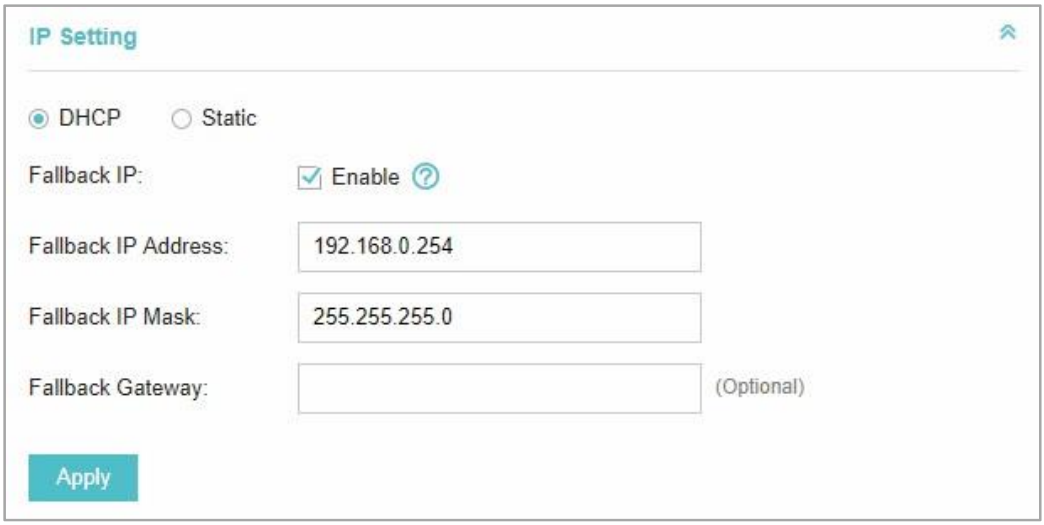
5.4.1 Configuration de base

Dans Basic Config, vous pouvez modifier le nom de l'EAP



5.4.2 Paramètre IP

Vous pouvez configurer une adresse IP pour ce EAP. Deux options sont fournies : DHCP et Static.



Obtenir une adresse IP dynamique à partir du serveur DHCP

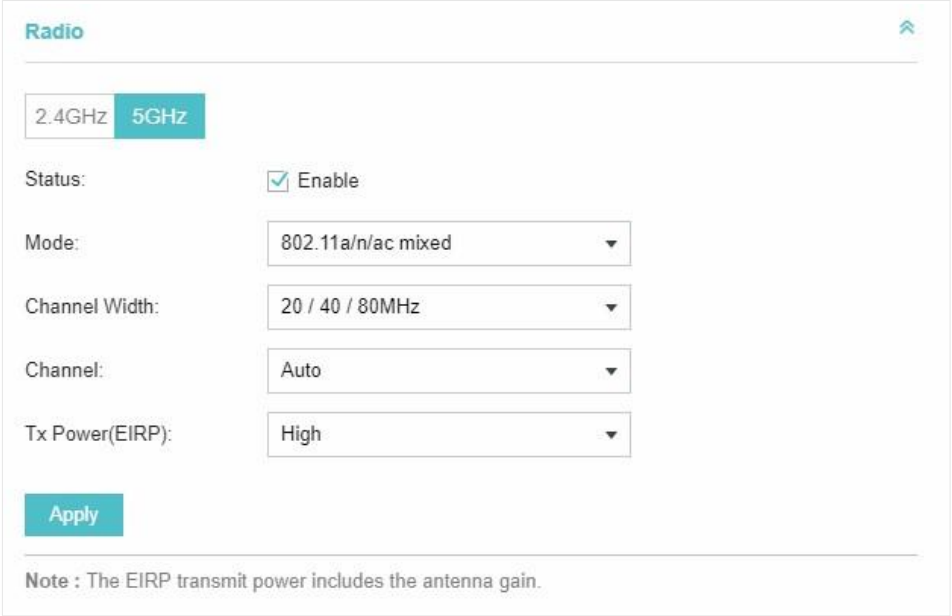
1. Configurez votre serveur DHCP.
2. Sélectionnez DHCP sur la page ci-dessus.
3. Activer la fonctionnalité IP de secours feature. Lorsque l'appareil device ne peut pas obtenir une adresse IP dynamique , l'adresse IP address de secours sera utilisée.
4. Définissez l'adresse IP, le masque IP et la passerelle pour l'adresse de secours, puis cliquez sur Appliquer.

Définir manuellement une adresse IP statique pour le EAP

1. Sélectionnez Statique.
2. Définissez l'adresse IP, le masque IP et la passerelle pour l'adresse statique, puis cliquez sur Appliquer.

5.4.3 Radio

Les paramètres radio contrôlent directement le comportement de la radio dans le EAP et son interaction avec le support physique;c'est-à-dire, comment et quel type de signal le EAP émet.



Sélectionnez la bande de fréquence (2,4 GHz/5 GHz) et configurez les paramètres suivants .

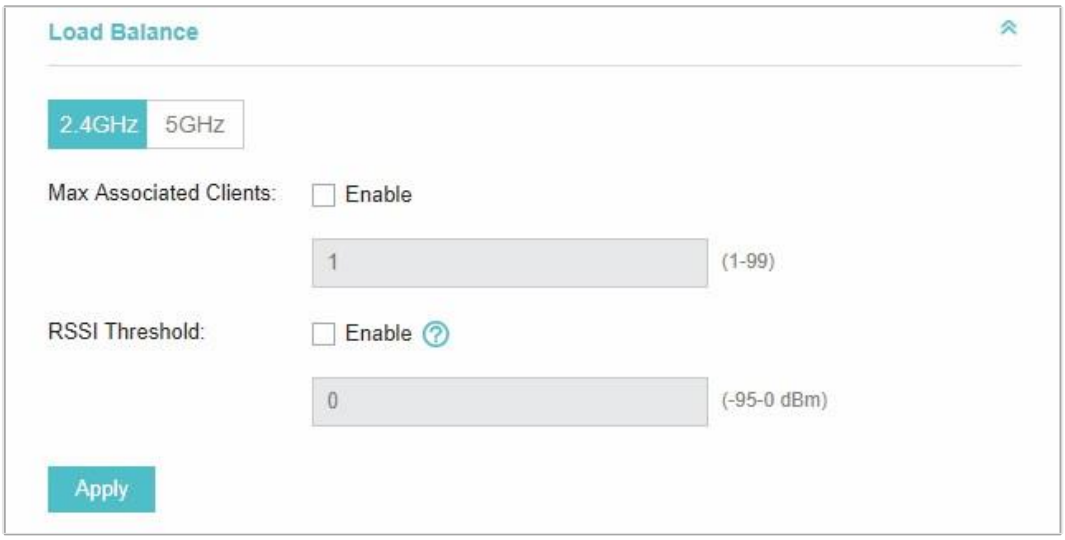
Statut	Activé par défaut. Si vous désactivez l'option, la radio de la bande de fréquence s'éteint.
Mode	Sélectionnez le mode IEEE 802.11 utilisé par la radio. Lorsque la fréquence de 2,4 GHz est sélectionnée,802,11b/g/n mixte, 802,11b/g mixte, et 802,11n modes seulement sont disponibles : 802.11b/g/n mixte : Tous les clients 802.11b, 802.11g et 802.11n opérant dans la fréquence de 2.4GHz peuvent se connecter au EAP. Nous vous recommandons de sélectionner le mode mixte 802.11b/g/n. 802.11b/g mixte : Les clients 802.11b et 802.11g peuvent se connecter au EAP. 802.11n seulement : Seuls 802.11n clients peuvent se connecter au EAP. Lorsque la fréquence de 5GHz est sélectionnée,802,11 n/ac mixte, 802,11a/n mixte, 802,11 ac seulement,802,11a seulement, et802,11n modes seulement sont disponibles : 802.11n/ac mixte: Les clients 802.11n et 802.11ac opérant dans la fréquence 5GHz peuvent se connecter au EAP. 802.11a/n mixte : Les clients 802.11a et 802.11n opérant dans la fréquence 5GHz peuvent se connecter au EAP. 802.11ac seulement : Seuls 802.11ac clients peuvent se connecter au EAP. 802.11a seulement : Seuls les clients 802.11a peuvent se connecter au EAP. 802.11n seulement : Seuls 802.11n clients peuvent se connecter au EAP.

Largeur du canal	Sélectionnez la largeur du canal du EAP. Les options disponibles diffèrent d'un ou l'autre des EAP. Pour certains EAP, les options disponibles incluent 20MHz, 40MHz et 20/40MHz. Pour les autres EAP, les options disponibles incluent 20MHz, 40MHz, 80MHz et 20/40/80MHz. Les canaux 20/40 MHz et 20/40/80MHz permettent des débits de données plus élevés mais laissent moins de canaux disponibles pour une utilisation par d'autres appareils 2,4 GHz et 5GHz. Lorsque le mode radio comprend 802.11n, nous vous recommandons de définir la bande passante du canal à 20/40 MHz ou 20/40/80MHz pour améliorer la vitesse de transmission.
Canal	Sélectionnez le canal utilisé par le EAP pour améliorer les performances sans fil. La gamme de canaux disponibles est déterminée par le mode radio et le paramètre de pays. Si vous sélectionnez Automatique pour le paramètre de amount canal, le EAP analyse les canaux disponibles et sélectionne un canal où le moins de trafic est détecté.
Tx Power (EIRP)	Sélectionnez la puissance Tx (Transmission Power) dans les 4 options : Faible, Moyenne, Haute et Personnalisée. Les basses, moyennes et hautes sont basées sur le Min. Txpower (Puissance de transmission minimale) et Max. TxPower (Puissance de transmission maximale. Il peut varier d'un pays à l'autre et d'une région à l'autre). ▪ 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 : entrez une valeur manuellement.

5.4.4 Balance de charge

En définissant le nombre maximal de clients accédant aux EAP,

Load Balance permet d'obtenir une utilisation rationnelle des ressources réseau.



Sélectionnez la bande de fréquence (2,4 GHz/5 GHz) et configurez les paramètres.

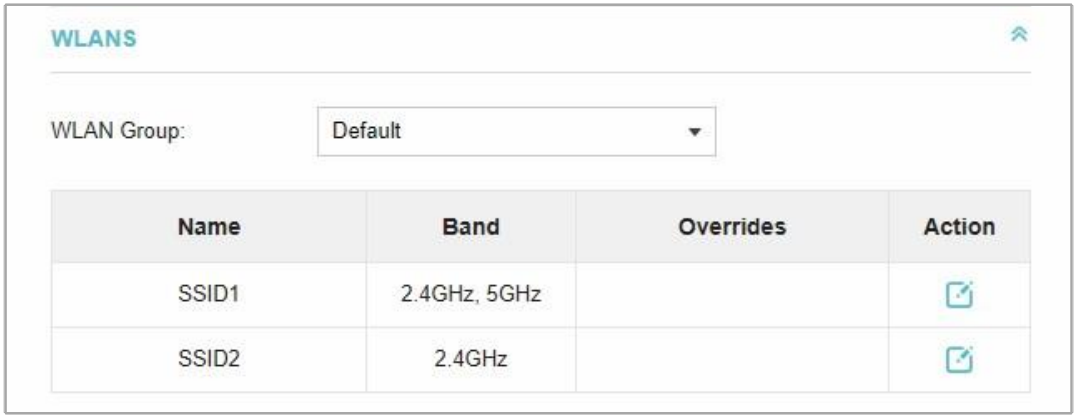
Max Associé Clients	Activez cette fonction et spécifiez le nombre maximal de clients connectés. Alors que plus de clients demandant à se connecter, le AP va déconnecter ceux avec des signaux plus faibles.
Seuil RSSI	Activez cette fonction et entrez le seuil de RSSI (Indication de force du signal reçu). Lorsque le signal des clients est plus faible que le seuil RSSI que vous avez défini, les clients seront déconnectés du EAP.

5.4.5 WLANs

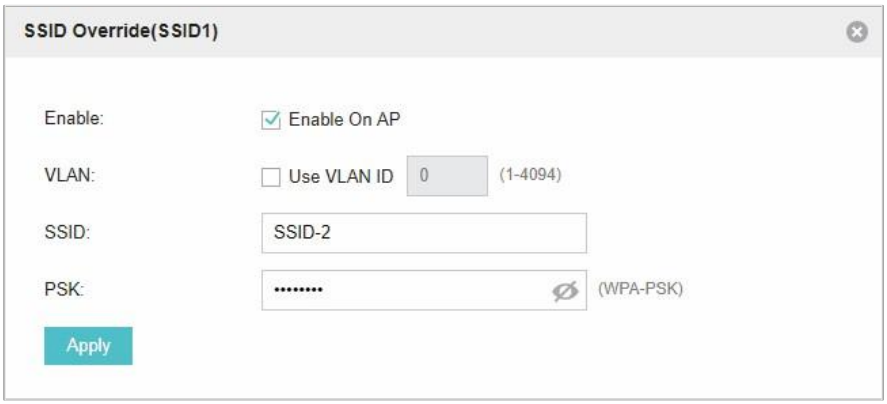
Vous pouvez spécifier un autre nom et mot de passe SSID pour remplacer le SSID précédent.

Après cela, les clients ne peuvent voir que le nouveau SSID et utiliser le nouveau mot de passe pour accéder au réseau.

Suivez les étapes ci-dessous pour remplacer le SSID.



1. Sélectionnez le groupe Wlan.
2. et la fenêtre suivante apparaîtra -jusqu'à.

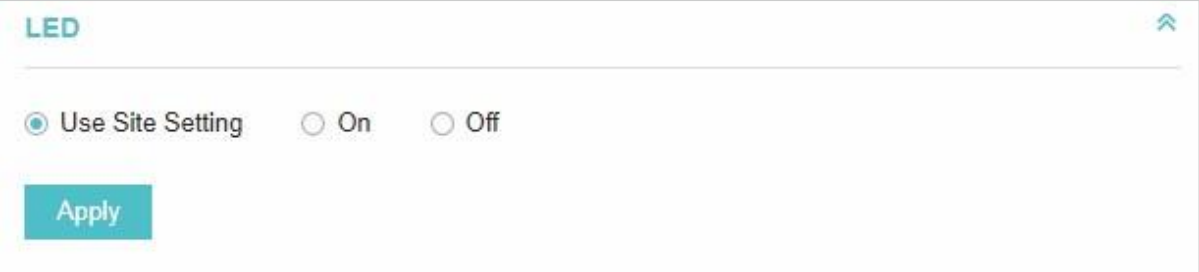


3. Cochez la case pour activer la fonctionnalité.
4. Vous pouvez rejoindre le SSID remplacé dans un VLAN. Cochez la case Utiliser l'ID VLAN et spécifiez un ID VLAN.
5. Spécifiez un nouveau nom et mot de passe pour le SSID.

6. Cliquez sur Appliquer pour enregistrer la configuration.

5.4.6 LED

Vous pouvez modifier l'état LED de chaque PAE.



Utilisation du paramètre de site	L'état LED sera le même que celui des paramètres du site.
Sur	Allumez la LED.
Hors tension	Éteignez la LED.

5.4.7 Paramètres du l'agrégation de liens Trunk (uniquement pour EAP330)

La fonction trunk peut regrouper plusieurs liens Ethernet dans un lien logique pour augmenter la bande passante et améliorer la fiabilité du réseau.

Statut	Activez cette fonction. L'EAP330 dispose de deux ports Ethernet de 1000 Mbps. Si la fonction Trunk est activée et que les ports sont à la vitesse du duplex complet de 1000 Mbps, toute la bande passante du lien du trunk est jusqu'à 4 Gbps (2000Mbps * 2).
Mode	Sélectionnez le mode appliqué de Trunk dans la liste déroulante. **MAC_DA + MAC_SA** : lorsque cette option est sélectionnée, l'arithmétique sera basée sur les adresses MAC source et destination des paquets. **MAC_ DA:** lorsque cette option est sélectionnée, l'arithmétique sera basée sur les adresses MAC de destination des paquets. **MAC_ SA**: lorsque cette option est sélectionnée, l'arithmétique sera basée sur les adresses MAC source des paquets.

5.4.8 Détection d'AP voyous

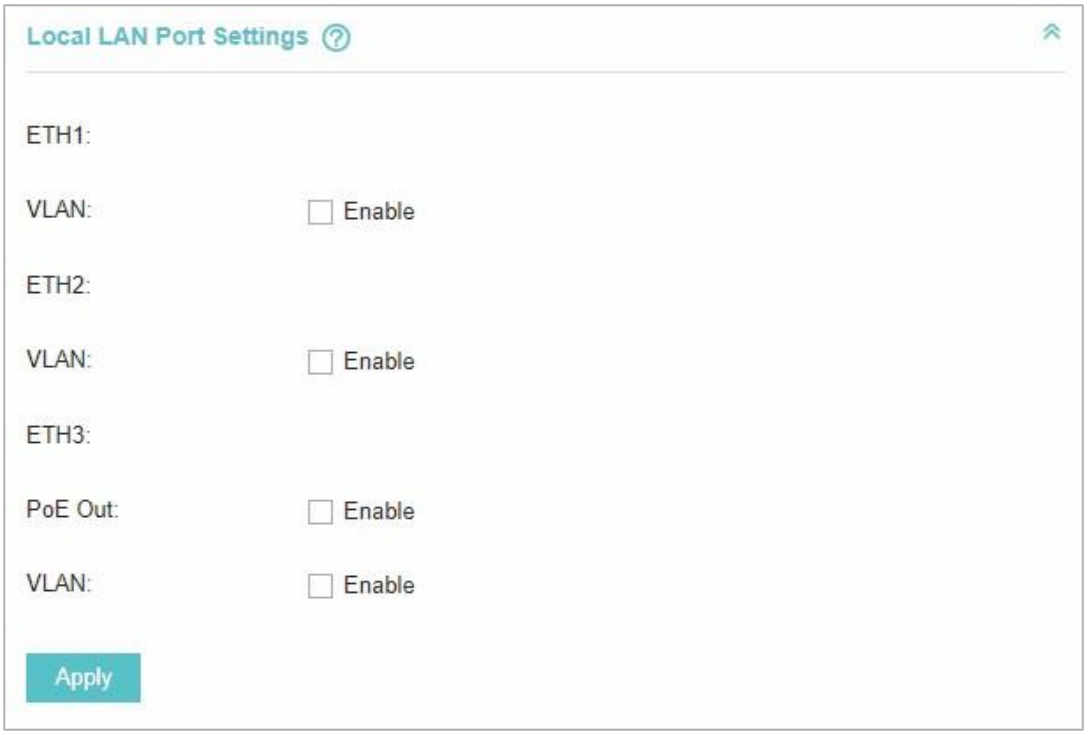
Avec cette option activée, leEAP détectera les AP voyous dans tous les canaux. Vous pouvez afficher les résultats dans la page Insight > Untrusted Rogue APs.

Notes

Pour certaines versions spécifiques du firmware, certains EAP détecteront automatiquement les AP voyous lorsque cette option est activée.

5.4.9 Paramètres locaux du port LAN (uniquement pour EAP115-Wall et EAP225-Wall)

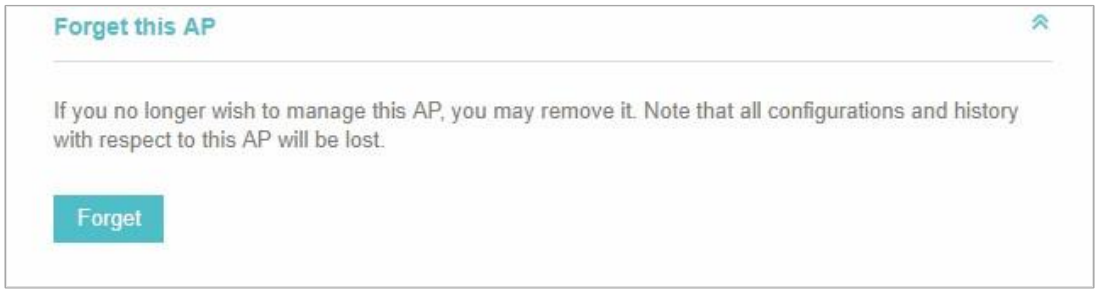
Vous pouvez configurer le port LAN du EAP. Ici, nous utilisons EAP225-Wall comme un exemple.



Vlan	Activez cette fonctionnalité et spécifiez le VLAN au laquelle le EAP est ajouté, puis les hôtes connectés à ce EAP ne peuvent communiquer qu'avec les périphériques de ce VLAN. Les valeurs valides sont de 1 à 4094, et la valeur par défaut est 1.
PoE Out	Si votre EAP dispose d'un port PoE OUT, vous pouvez activer cette option pour fournir de l'énergie à l'appareil connecté sur ce port. Le EAP qui n'a pas de port PoE OUT ne prend pas en charge cette fonctionnalité.

5.4.10 Oubliez cet AP

Si vous ne souhaitez plus gérer ce EAP, vous pouvez le supprimer. Toutes les configurations et l'historique de ce EAP seront supprimés. Il est recommandé de sauvegarder les configurations de ce EAP avant de l'oublier .



6 Gérer l’OC200

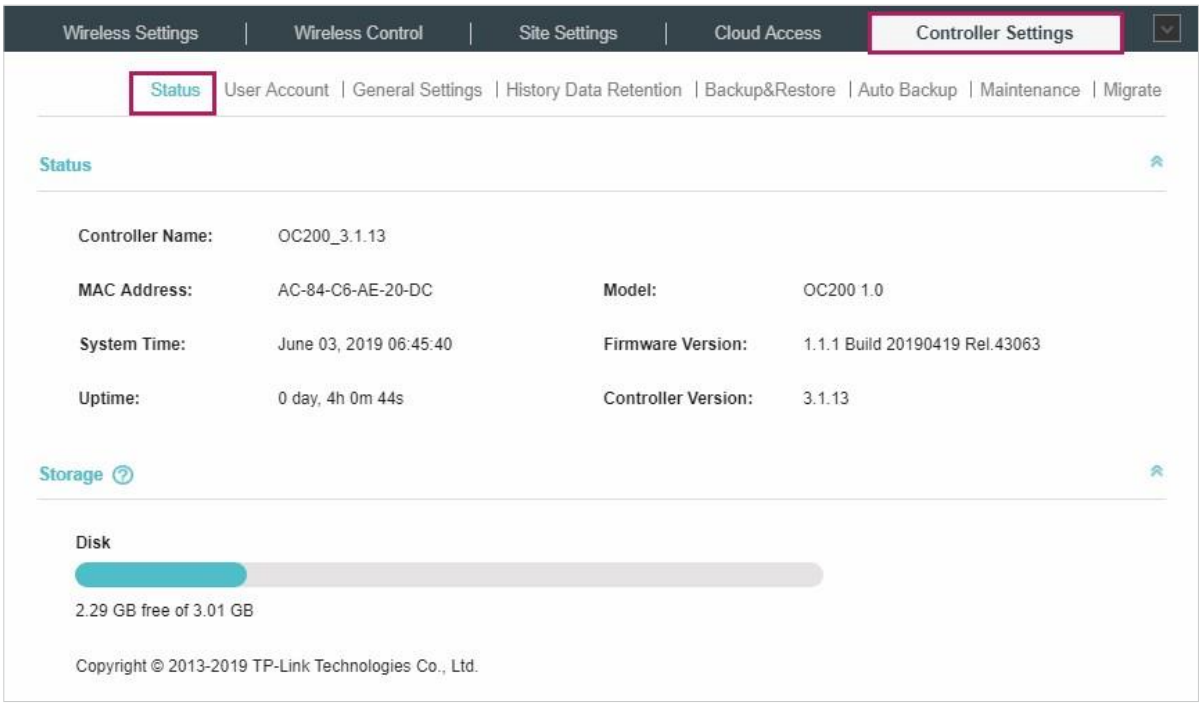
Ce chapitre présente principalement comment gérer le compte d’utilisateur et configurer les paramètres du système.

Ce chapitre comprend le contenu suivant.

- État
- Compte d’utilisateur « Account »
- Réglage général
- Historique Conservation des données
- Sauvegarde et restauration
- Sauvegarde automatique
- Entretien

6.1 État

La page État affiche les informations de base de l’OC200.



Statut	Affiche les informations de base de l'OC200.
Stockage	Affiche le stockage de l'OC200 et du périphérique de stockage USB externe. **Conseils** : Le périphérique de stockage USB externe apparaîtra ici après l'avoir branché sur le port USB. Le périphérique de stockage USB peut être utilisé pour sauvegarder automatiquement les données. Notez que cette fonction n'est disponible que lorsque OC200 est alimenté par un périphérique PoE.

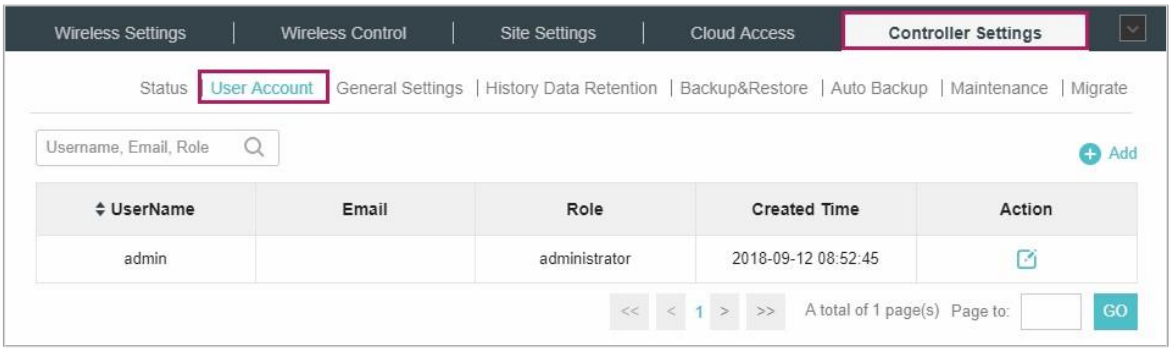
6.2 Compte d'utilisateur

Vous pouvez utiliser différents comptes d'utilisateur pour vous connecter à l'OC200. L'utilisateur a trois rôles : administrateur, opérateur et observateur. L'autorité d'administration varie d'un rôle à l'autre .

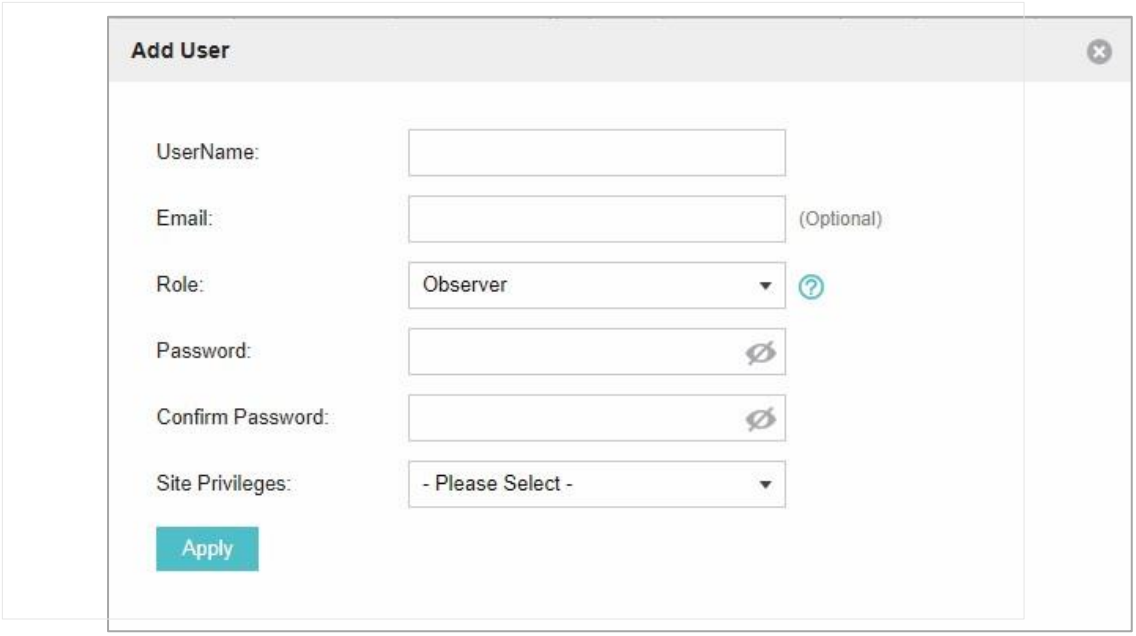
Administrateur	Le premier compte d'administrateur est créé dans le processus de configuration de base et ce compte ne peut pas être supprimé. Un administrateur peut modifier les paramètres du réseau EAP et créer et supprimer des comptes d'utilisateurs.
Opérateur	Un compte opérateur peut être créé ou supprimé par l'administrateur, L'opérateur « operator » peut modifier les paramètres du réseau EAP.
Observateur	Un compte observateur peut être créé ou supprimé par l'administrateur. L'observateur ne peut afficher que l'état statuts et les paramètres du réseau EAP, mais ne modifiez pas les paramètres.

Suivez les étapes ci-dessous pour ajouter un compte d'utilisateur.

1. Aller à Paramètres de Compte utilisateur de contrôleur >



2. Cliquez sur Add la fenêtre suivante apparaîtra.



3. Spécifiez le nom d'utilisateur, le courrier électronique et le mot de passe du compte.

4. Sélectionnez le rôle dans la liste déroulante.

Si vous sélectionnez opérateur ou observateur, vous devez également sélectionner les privilèges du site.

■ Si vous sélectionnez administrateur, l'option Privilèges de site n'apparaîtra pas et tous les sites sont disponibles pour l'utilisateur administrateur.

5. Cliquez sur Appliquer pour ajouter le compte d'utilisateur.

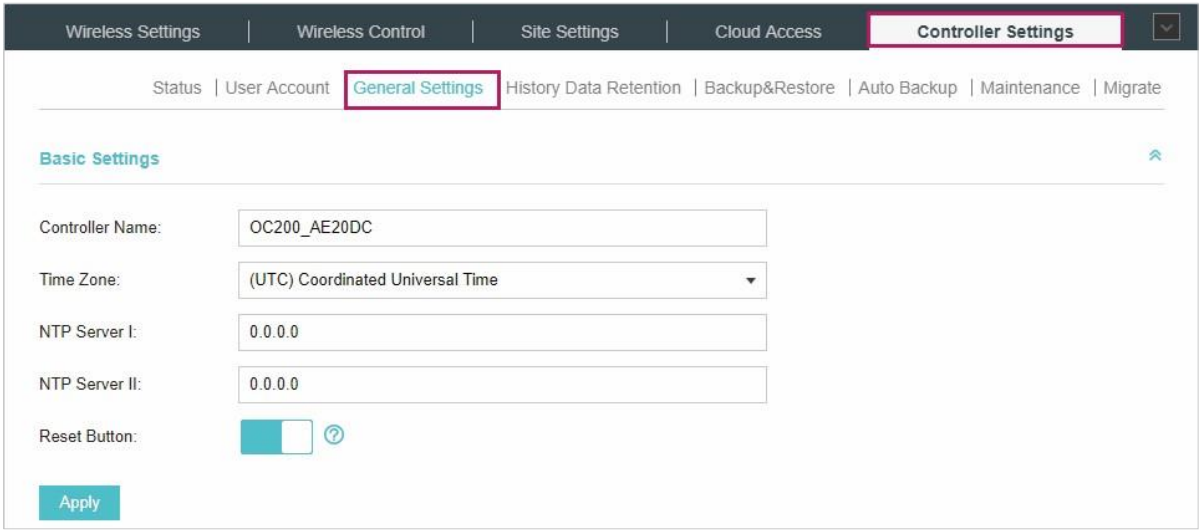
Notes

- Vous pouvez vous référer à la page Rôle pour afficher le type du rôle utilisateur, les informations de description, l'étendue d'autorisation et le temps créé.
- Le compte d'utilisateur ne peut pas être utilisé pour se connecter à l'OC200 via Omada Cloud Service. Pour accéder à l'OC200 via Cloud Access, vous devez être un utilisateur de cloud. Pour ajouter un utilisateur de cloud, reportez-vous à Manage the Cloud Users.

6.3 Cadre général

Accédez à Paramètres du contrôleur > Paramètre général et configurez les paramètres de base de'OC200.

6.3.1Configurer les paramètres de base



Nom du contrôleur	Spécifiez un nom pour l'OC200.
Fuseau horaire	Spécifiez le fuseau horaire pour OC200.
Serveur NTP I	Spécifiez le serveur NTP principal pour l'OC200.
NTP Server II	Spécifiez le serveur NTP secondaire pour l'OC200.
Bouton Réinitialiser	Avec cette option activée, l'OC200 peut être réinitialisé via son bouton de réinitialisation matérielle ; sinon ne peut être réinitialisé que dans la page Maintenance.

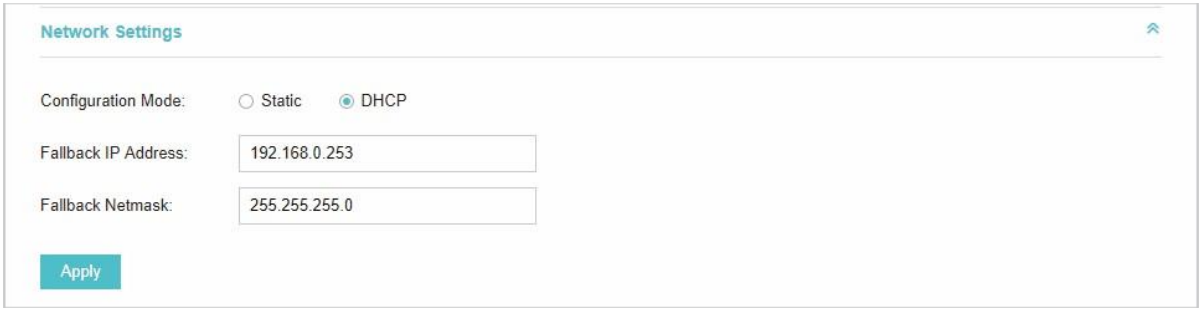
Notes

Seuls les utilisateurs connectés locaux peuvent configurer le fuseau horaire, le serveur NTP I, le serveur NTP II et le bouton Réinitialisation.

6.3.2 Configurer les paramètres réseau

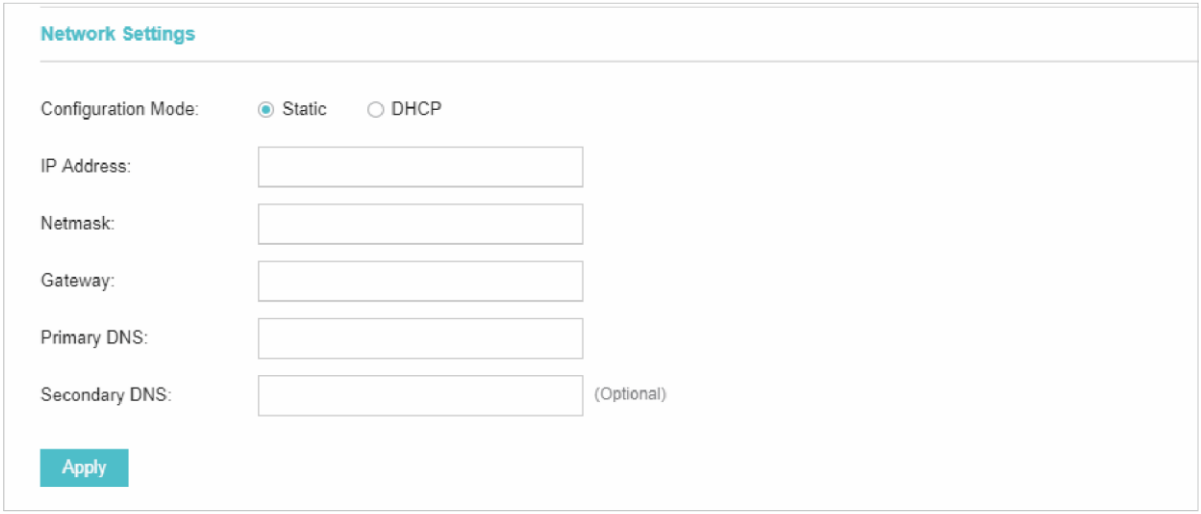
Choisissez la façon d'obtenir les paramètres IP de l'OC200. Par défaut, il s'agit de DHCP.

■ **Choisissez le mode de configuration en tant que DHCP**



Configuration Mode	Choisissez le mode de configuration en tant que DHCP
Adresse IP de secours	Spécifiez l'adresse IP de secours pour l'OC200. Le repli est utilisé lorsque l'OC200 n'a pas réussi à obtenir une adresse IP à partir du serveur DHCP.
Netmask de secours	Spécifiez le masque de l'adresse IP de secours .

■ **Choisir le mode de configuration ap statique**



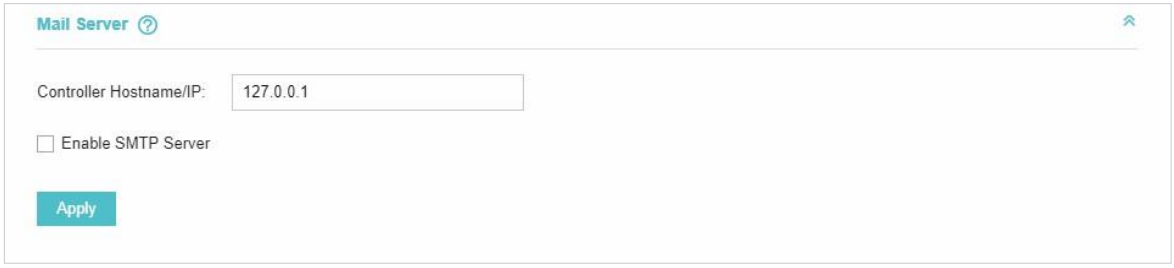
Configuration Mode	Choisissez le mode de configuration comme statique.
Adresse IP	Entrez une adresse IP pour l'OC200.
Netmask	Entrez le masque de l'adresse IP
Passerelle	Entrez l'adresse IP de la passerelle par défaut pour l'OC200.
DNS primaire	Entrez l'adresse IP du serveur DNS principal.
DNS secondaire	(Facultatif) Entrez la propriété intellectuelle l'adresse du serveur DNS secondaire.

6.3.3 Configurer le serveur de messagerie

Avec le serveur de messagerie, vous pouvez réinitialiser le mot de passe de connexion du compte d'utilisateur si nécessaire. Un courriel avec le lien de réinitialisation du mot de passe sera envoyé à partir de l'OC200. Il est différent du serveur SMTP, qui est juste pour les e-mails de journal système envoyant.

Suivez les étapes ci-dessous pour configurer le serveur de messagerie.

1. Accédez à **Paramètres du contrôleur > Paramètre général**, puis cliquez sur Serveur de messagerie.

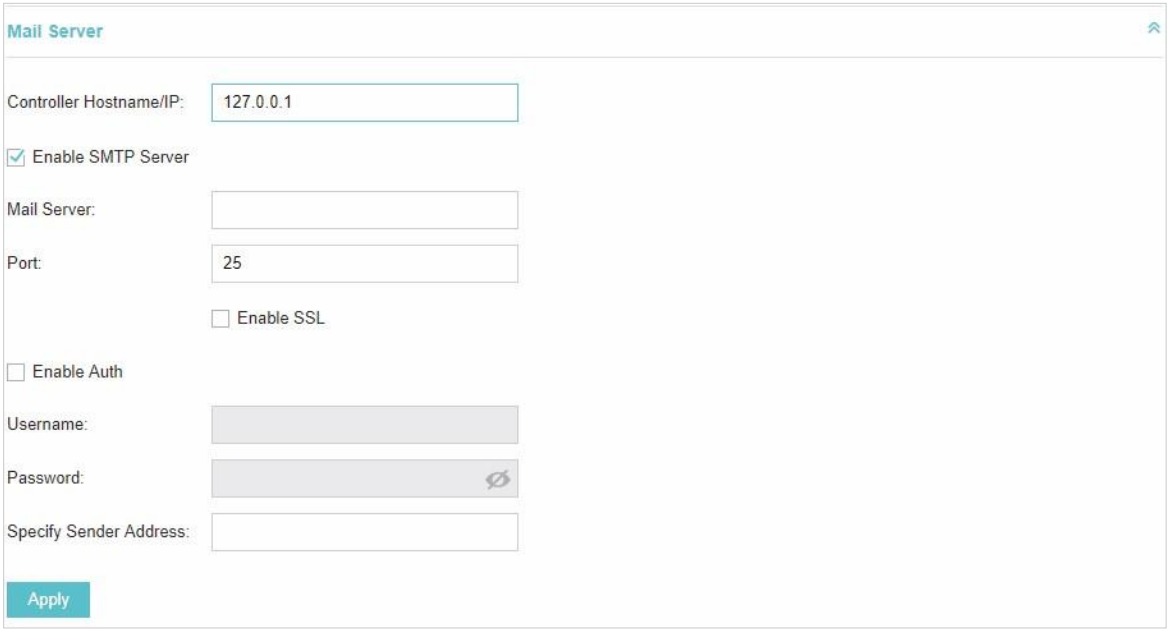


2. Entrez le nom d'hôte ou l'adresse IP de l'OC200. L'adresse IP par défaut de l'OC200 est 127.0.0.1.

   Vous pouvez le conserver ou personnaliser le nom d'hôte ou l'adresse IP qui peut être visité par l'hôte de gestion.

   Lorsque l'e-mail avec le lien de réinitialisation du mot de passe est envoyé, l'adresse OC200 ou IP sera spécifiée dans l'URL du contrôleur dans chaque message.

3. Cochez la case pour activer SMTP Server, puis l'écran suivant s'affiche .



4. Configurer les paramètres suivants.

Serveur de messagerie	Entrez l'adresse IP ou le domaine de SMTP Server.
Port	Le serveur SMTP utilise le port 25 comme valeur par défaut. Vous pouvez activer SSL (Security Socket Layer) pour améliorer les communications sécurisées sur Internet. Si SSL est activé, le numéro de port passera automatiquement à 465.
Activer Auth	Cochez la case pour activer l'authentification (Facultatif).
Nom d'utilisateur/Mot de passe	Si vous activez l'authentification, entrez le nom d'utilisateur et le mot de passe requis par le serveur de messagerie.
Spécifier l'expéditeur Adresse	Spécifiez l'adresse de messagerie de l'expéditeur. Entrez l'adresse e-mail qui apparaîtra comme l'expéditeur pour réinitialiser le mot de passe.

5. Cliquez sur Appliquer pour enregistrer la configuration.

Notes

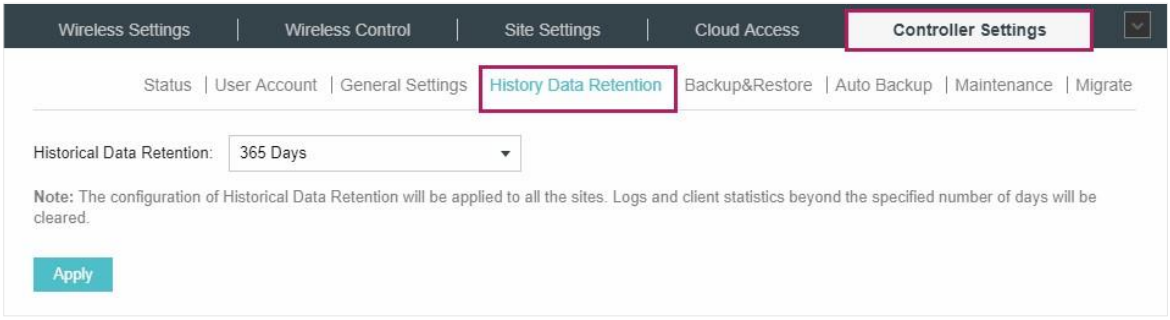
Spécifiez l'adresse de messagerie du compte en fonction du serveur de messagerie pour recevoir le message de réinitialisation du mot de passe.

6.4 Historique conservation des données

Historique La conservation des données permet aux utilisateurs de déterminer la conservation des journaux et des statistiques clients. Les journaux et les statistiques clients au-delà du nombre spécifié de jours seront effacés. Par exemple, avec 7 jours sélectionnés, seuls les journaux et les statistiques clients au cours des 7 derniers jours seront conservés, et les données au-delà de 7 jours seront effacées de l'OC200.

Procédez comme suit pour configurer la conservation des données historiques :

1. Accédez aux paramètres de l'historique du contrôleur > Historique de la conservation des données .



2. Sélectionnez la durée pendant les jours pendant lesquelles les données seront conservées dans la liste déroulante. Sept options sont fournies ***7 jours,30 jours,60 jours,90 jours,180 jours et 365 jours*.**

3. Cliquez sur Appliquer.

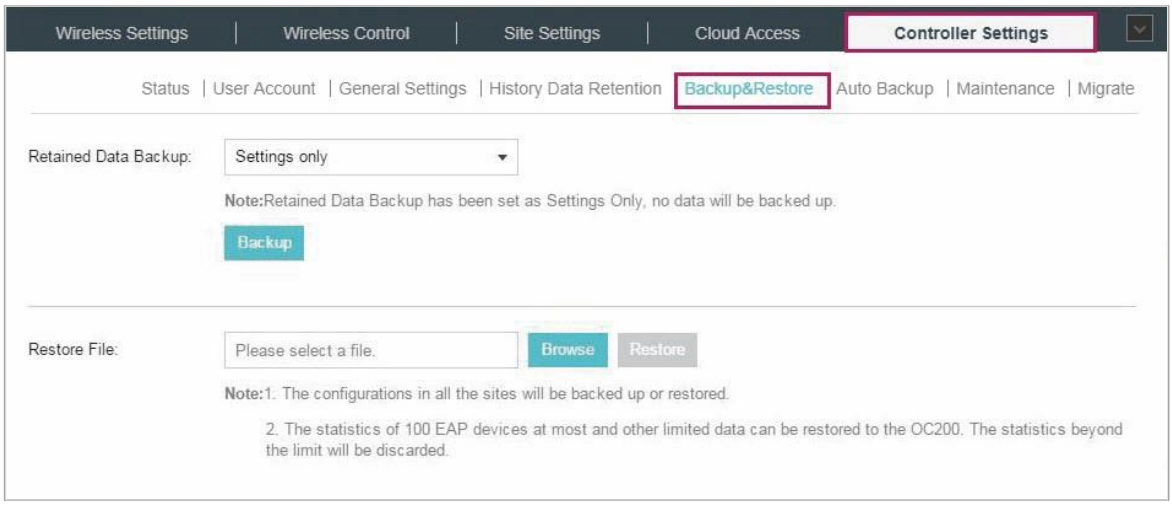
6.5 Sauvegarde et restauration

Vous pouvez enregistrer les configurations et données actuelles dans l'OC200 en tant que fichier de sauvegarde et, si nécessaire, restaurer les configurations à l'aide du fichier de sauvegarde. Nous vous recommandons de sauvegarder les paramètres avant de mettre à niveau l'appareil. Cette fonction n'est disponible que pour les utilisateurs connectés locaux.

Suivez les étapes ci-dessous pour sauvegarder et restaurer les configurations.

1. Accédez aux paramètres du contrôleur > Sauvegarde et restauration.

2. Sélectionnez la durée pendant les jours pendant lesquelles les données seront sauvegardées dans la liste déroulante Sauvegarde de données conservées .
   Par exemple, avec 7jours sélectionnés les données uniquement dans les 7 jours récents seront sauvegardées.



3. Cliquez sur Sauvegarde pour enregistrer le fichier de sauvegarde.

4. Si nécessaire, cliquez sur Parcourir pour localiser et choisissez le fichier de sauvegarde. Cliquez ensuite sur Restaurer pour restaurer les configurations.

Vous pouvez importer les fichiers de configuration du contrôleur logiciel Omada dans l'OC200 à l'aide de la fonction Restaurer. Notez que certains paramètres seront modifiés et que vous devez à nouveau configurer. Pour plus d'informations, reportez-vous à l'article : ***detailed***

Comment restaurer les fichiers de configuration d'Omada Software Controller dans OC200 ?

Notes

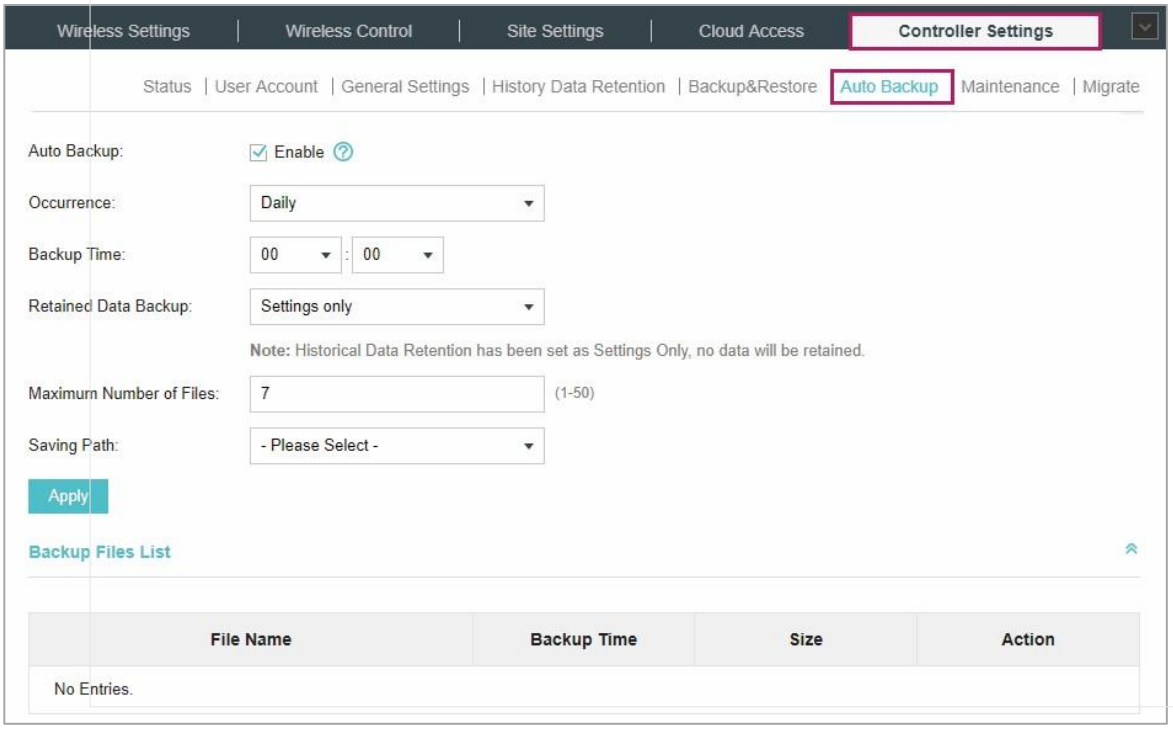
- Si vous ne souhaitez pas sauvegarder des données historiques, vous pouvez sélectionner Paramètres uniquement pour obtenir uniquement les paramètres enregistrés dans les fichiers de sauvegarde.
- Si vous ne souhaitez pas sauvegarder manuellement des données, vous pouvez activer la fonction Sauvegarde automatique. Veuillez-vous référer à Sauvegarde automatique.
- Lorsque vous restaurez les fichiers de sauvegarde dont la fonction sauvegarde automatique est activée, vous devez à nouveau configurer la sauvegarde automatique. Veuillez-vous référer à Sauvegarde automatique.

6.6 Sauvegarde automatique

Avec la sauvegarde automatique activée, les paramètres de OC200 seront programmés pour sauvegarder la configuration et les données automatiquement à l'heure spécifiée.

Suivez les étapes ci-dessous pour configurer la fonction Sauvegarde automatique.

1. Accédez aux paramètres du contrôleur > Sauvegarde automatique.



2. Cochez la case pour activer la fonction Sauvegarde automatique.

3. Sélectionnez la fréquence à laquelle effectuer la sauvegarde automatique dans l'occurrence. Vous pouvez choisir quotidien, hebdomadaire, mensuel ou annuel dans la liste déroulante. Définissez ensuite le moment approprié pour sauvegarder les fichiers dans l'heure de sauvegarde.

Lorsque, vous choisissez l'occurrence comme mensuel, veuillez choisir soigneusement la date de sauvegarde dans Sauvegarde

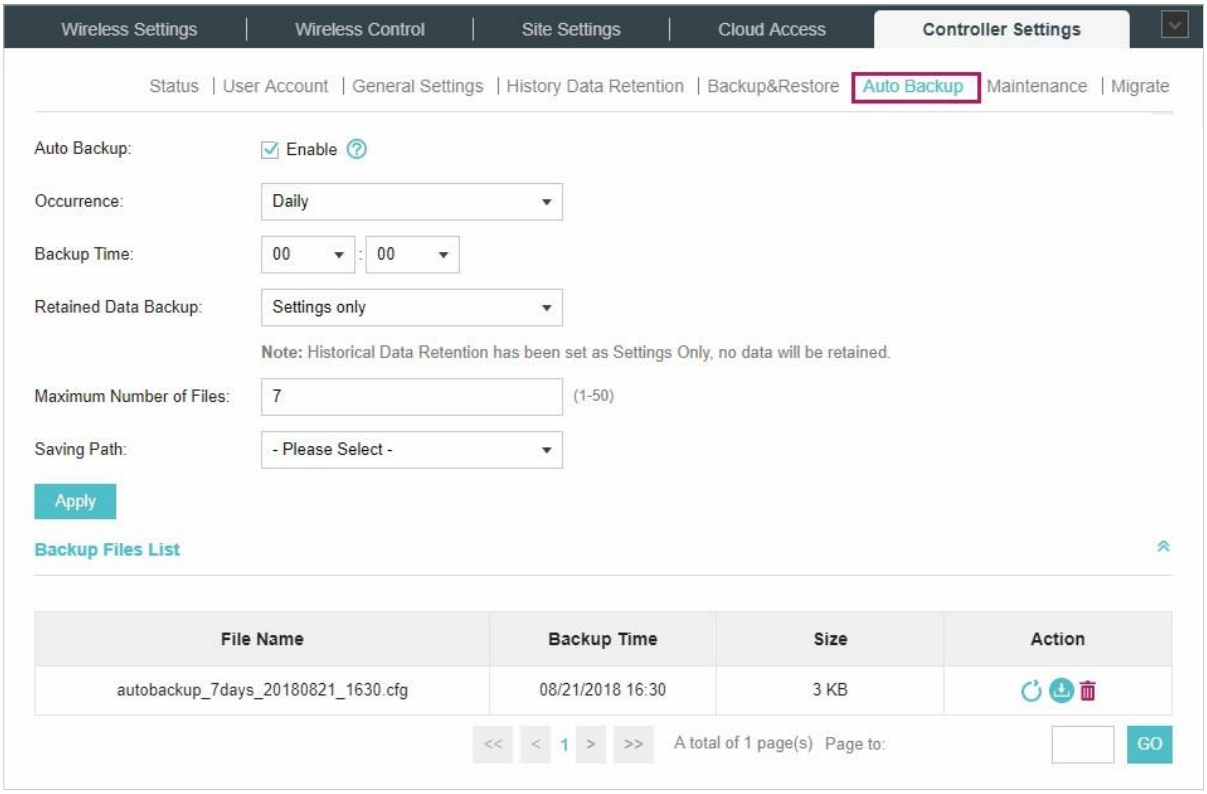
Heure. Par exemple,si vous choisissez de sauvegarder automatiquement les données le 31ème jour de chaque mois. Quand take il s'agit de Juin, qui est seulement 30 jours, la sauvegarde automatique ne prendra pas effet

4. Sélectionnez la durée pendant les jours pendant lesquelles les données seront sauvegardées dans la sauvegarde de données conservées. Par exemple, avec 7jours sélectionnés ,les données uniquement dans les 7 jours récents seront sauvegardées.

5. Spécifiez le nombre maximal de fichiers de sauvegarde à enregistrer dans le nombre maximal de fichiers. La valeur par défaut est 7.

6. Sélectionnez le chemin d'enregistrement des données. Choisissez le périphérique de **stockage USB externe**.

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



Vous pouvez exécuter l'opération correspondante aux fichiers de sauvegarde en cliquant sur une icône dans la colonne **Action**.

	Restauration des Configurations dans le fichier de sauvegarde.
	Téléchargez le fichier de sauvegarde.
	Supprimez le fichier de sauvegarde.

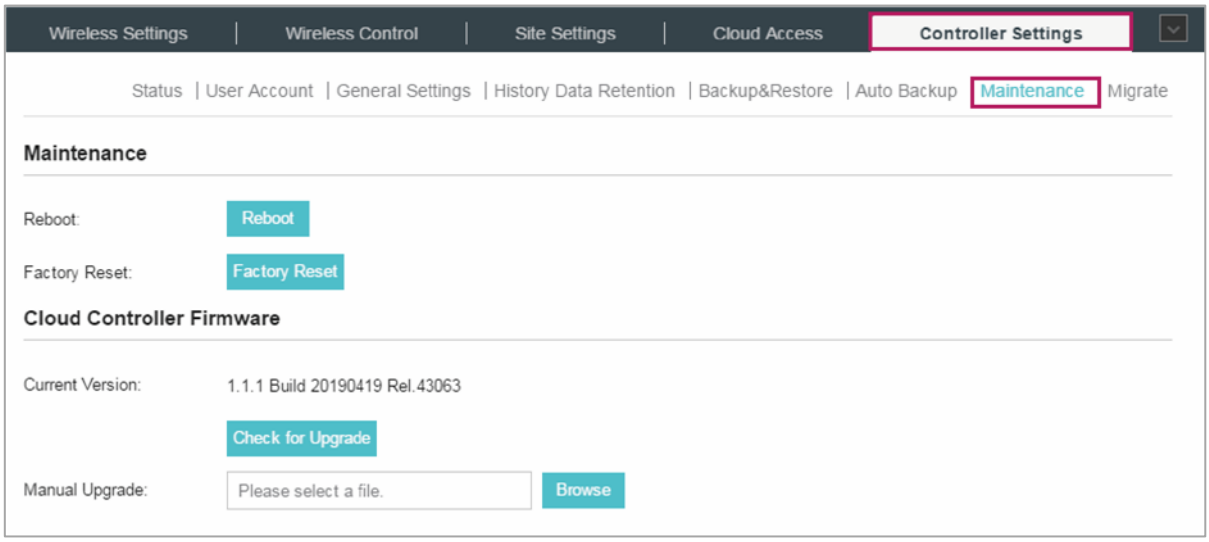
Notes

- Pour sauvegarder manuellement les données et restaurer les données dans l'OC200, configurez la fonction **Backup&Restore** . Veuillez-vous référer à Sauvegarde et restauration.
- Si vous ne souhaitez pas sauvegarder des données historiques, vous pouvez sélectionner Paramètres uniquement pour obtenir uniquement les paramètres enregistrés dans les fichiers de sauvegarde.
- Les fichiers de sauvegarde automatique seront stockés dans le périphérique **de stockage USB externe**. Cette fonction n'est disponible que lorsque OC200 est alimenté par un périphérique PoE.

6.7 Entretien

Dans la page Paramètres du contrôleur > Maintenance, vous pouvez redémarrer, reposer ou mettre à niveau le firmware de l'OC200.

Lorsque vous lancez l'OC200 via Cloud Access, vous pouvez vérifier le firmware et le mettre à niveau en ligne. Lorsque vous lancez l'OC200 localement, vous pouvez le mettre à niveau en ligne ou sélectionner manuellement un firmware pour le mettre à niveau.



La fonction Migrate permet aux utilisateurs de migrer les configurations et les données vers n'importe quel autre site ou OC200.

Pour migrer toutes les configurations et données de l'OC200 actuel vers tout autre OC200, reportez-vous à Migration du contrôleur « Migrate ».

Pour migrer les configurations et les données du site existant vers tout autre OC200, reportez-vous à Migrer le site « Migrate ».

6.8.1 Migration du contrôleur

Avec la fonction Migration du contrôleur, vous pouvez migrer vos configurations et données de l'OC200 actuel vers tout autre OC200 ayant la même version.

Le processus de migration des configurations et des données de l'OC200 actuel vers tout autre OC200 peut être résumé en trois étapes: Contrôleur d'exportation, Contrôleur de migration et Périphériques de migration.

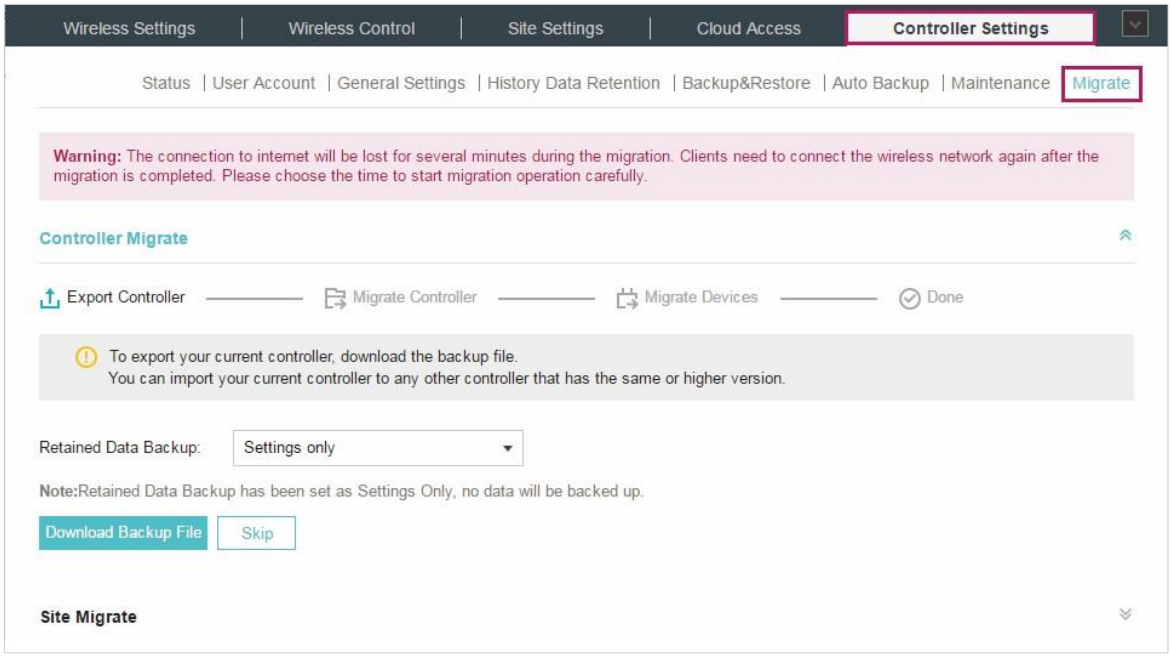
Suivez les étapes ci-dessous pour migrer votre OC200.

Notes

- 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 est terminée. Veuillez choisir le moment de commencer soigneusement l'opération de migration.
- Le contrôleur d'exportation et le contrôleur de migration ne sont disponibles que pour les utilisateurs enregistrés localement.

■ Contrôleur d'exportation

1. Accédez aux paramètres du contrôleur > Migrer > Migrer lecontrôleur.



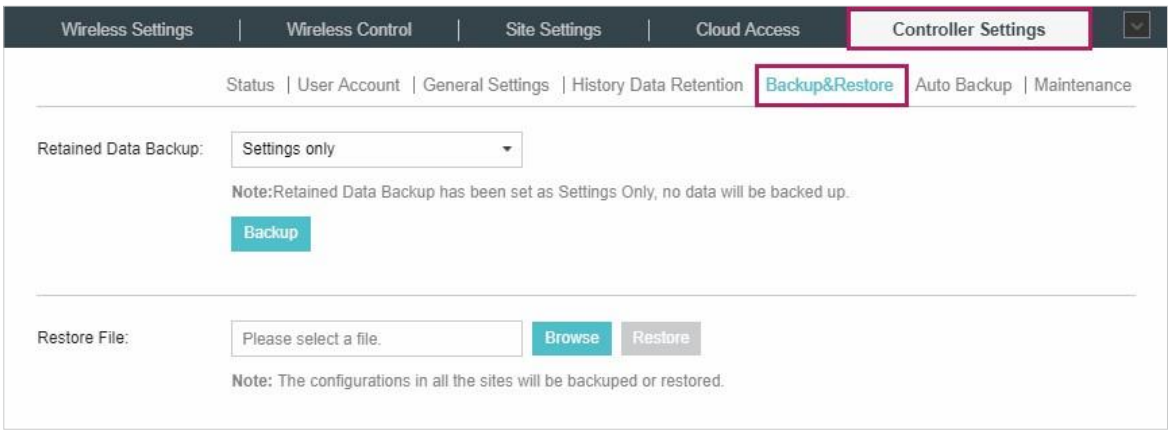
2. Sélectionnez la durée en jours où les données doivent être importées dans le deuxième contrôleur dans la liste déroulante Sauvegarde de données conservées . Par exemple, avec 7 jours sélectionnés, les données seulement au cours des 7 derniers jours seront importés dans le deuxième contrôleur.

3. Cliquez sur Télécharger le fichier de sauvegarde pour télécharger le fichier du contrôleur actuel.

   Si vous avez sauvegardé le fichier, cliquez sur Ignorer. ■ Contrôleur de migration

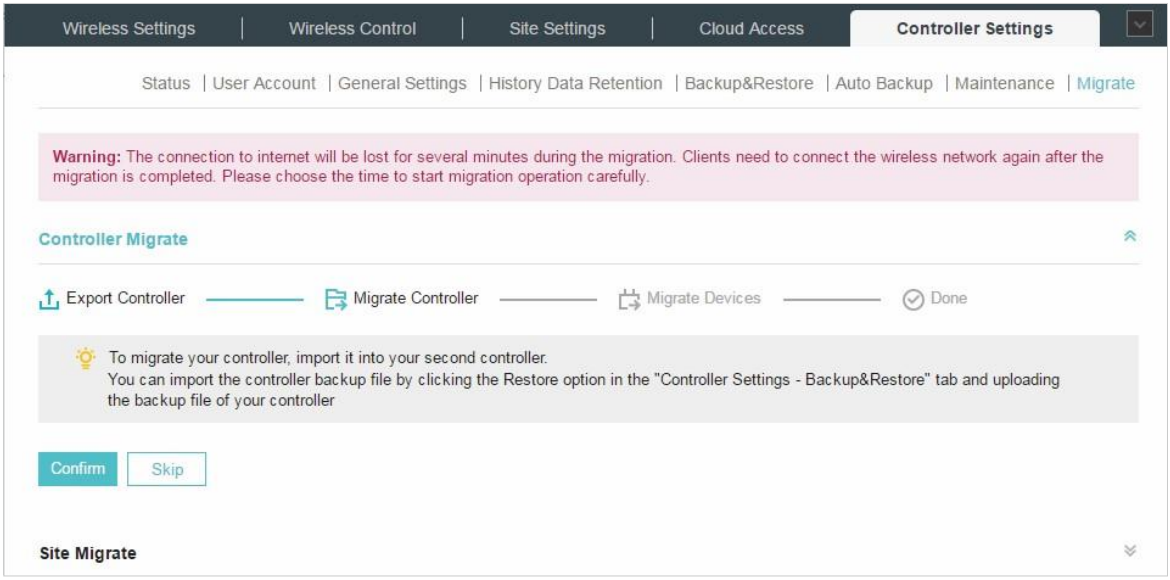
1. Démarrer et se connecter au deuxième OC200, accédez aux Paramètres du contrôleur > **Sauvegarde&Restauration** > Restaurer

   Fichier.



2. Cliquez sur Parcourir pour localiser et choisissez le fichier de votre contrôleur à importer. Cliquez ensuite sur Restaurer pour télécharger le fichier.

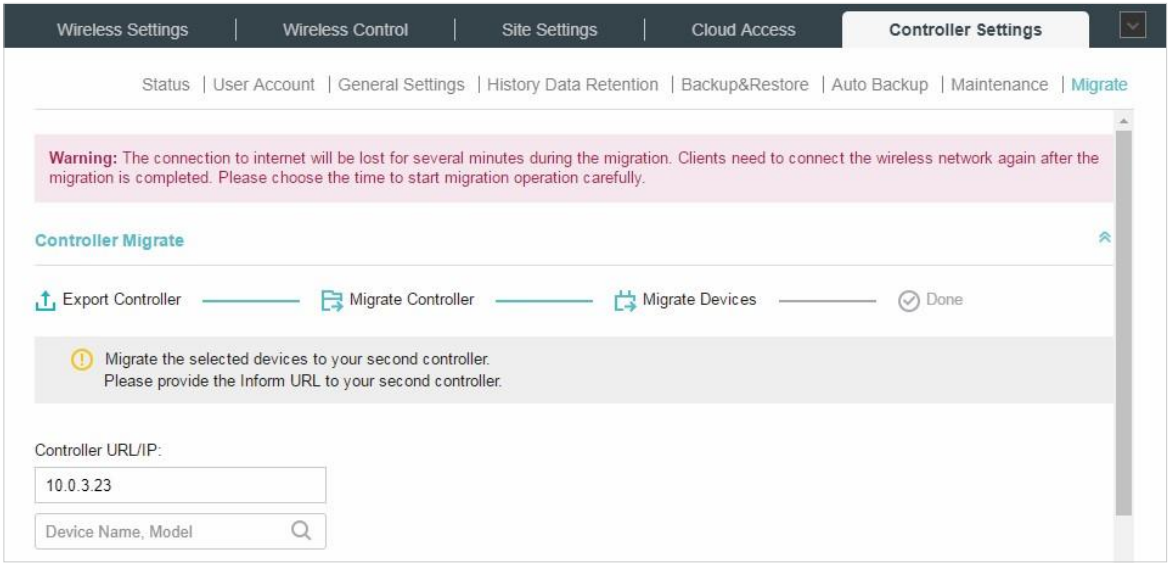
3. Une fois que le fichier a été restauré sur le deuxième contrôleur, retournez au contrôleur d'exportation et cliquez sur Confirmer.



■ Migrer les périphériques

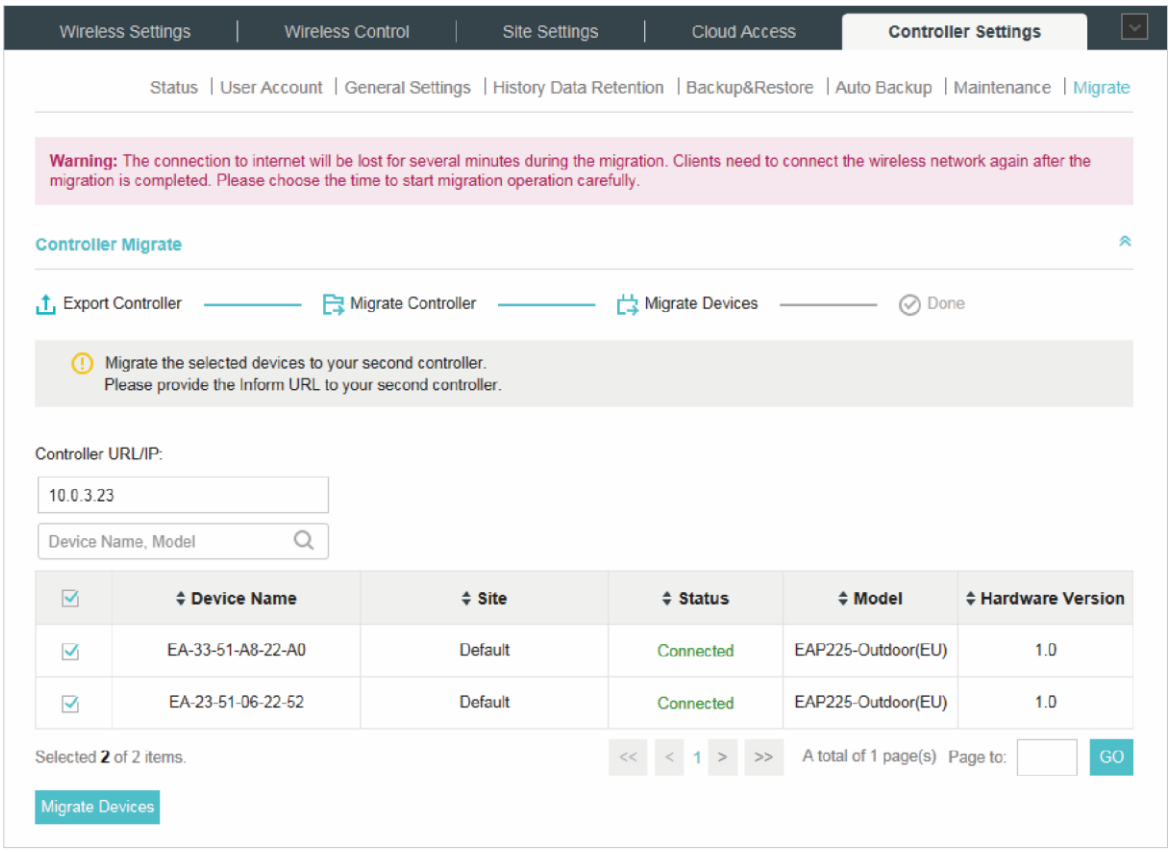
1. Cliquez sur Parcourir pour localiser et choisissez le fichier de votre contrôleur à be importer. Cliquez ensuite sur Restaurer pour télécharger le fichier.

2. Entrez l'adresse IP ou l'URL de votre deuxième contrôleur dans l'URL/IP du contrôleur déposée . Dans ce cas, l'adresse IP address du deuxième contrôleur est 10.0.3.23.



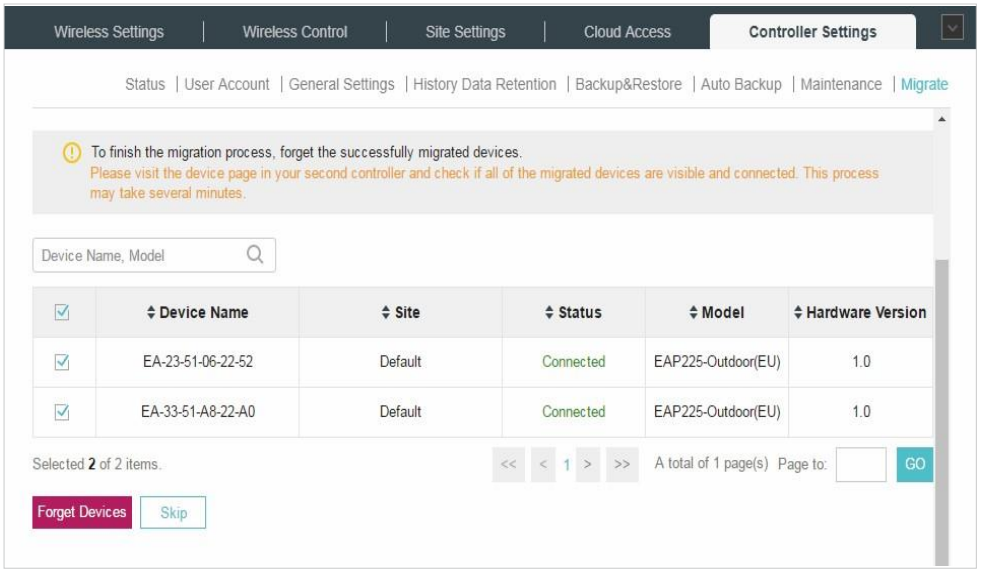
Notes : Assurez-vous d'entrer l'adresse IP correcte du deuxième contrôleur pour établir la communication entre les EAP et votre deuxième contrôleur. Dans le cas contraire, les EAP ne peuvent pas être adoptés par le deuxième contrôleur.

3. Sélectionnez les périphériques à migrer en cliquant sur les cases à côté de chaque appareil. Par défaut, tous les appareils sont sélectionnés.

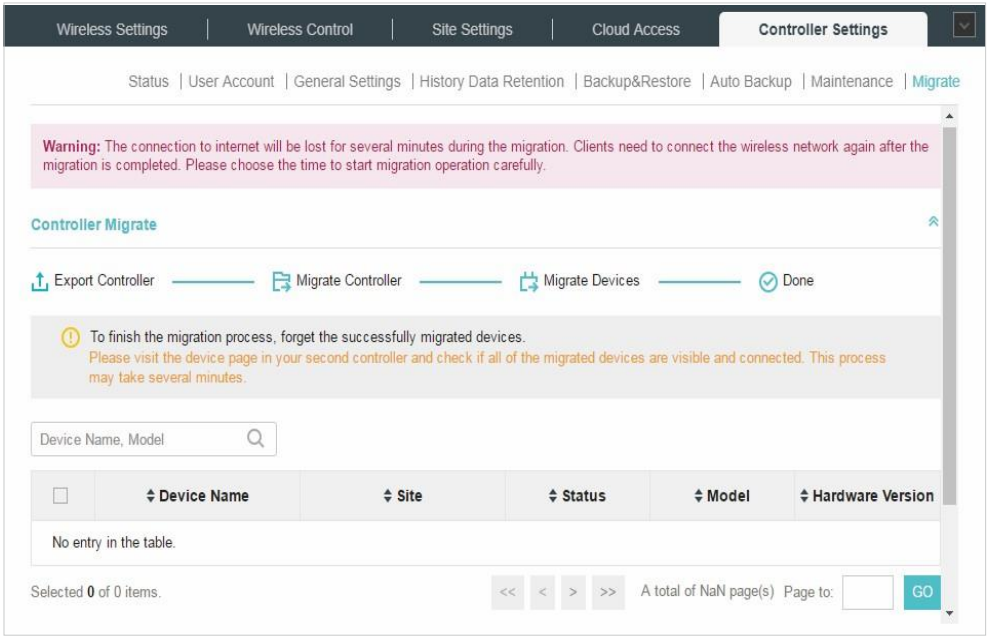


4. Cliquez sur Migrer des périphériques pour migrer les périphériques sélectionnés vers le deuxième contrôleur.

5. Vérifiez que tous les périphériques migrés sont visibles et connectés sur le deuxième contrôleur. Notez que cela peut prendre plusieurs minutes. Lorsque tous les périphériques migrés sont en état connecté dans la page Points d'accès du deuxième contrôleur, 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 deuxième contrôleur. Vous pouvez désinstaller le contrôleur précédent si nécessaire.



6.8.2 Migration du site

Avec la fonction Migrer de site, vous pouvez migrer vos configurations et données d'un site vers n'importe quel autre contrôleur ayant la même version.

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.

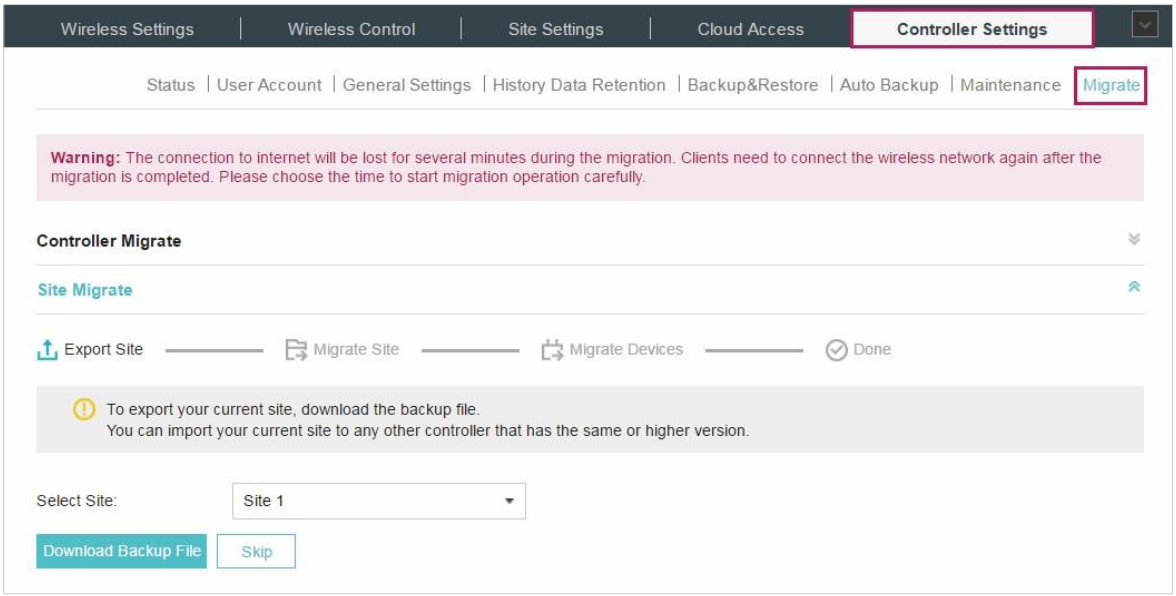
Suivez les étapes ci-dessous pour migrer un site vers un contrôleur.

Notes

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 est terminée. Veuillez choisir le moment de commencer soigneusement l'opération de migration.

■ Site d’exportation

1. Accédez aux paramètres du contrôleur > Migrer > Migrerle site.

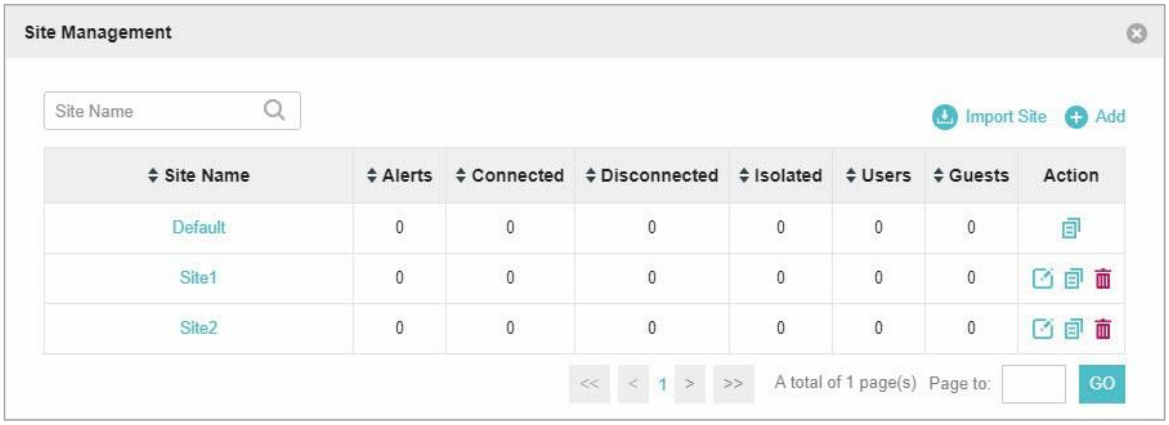


2. Sélectionnez le site à importer dans le deuxième contrôleur de la liste déroulante Sélectionner le site.

3. Cliquez sur Télécharger le fichier de sauvegarde pour télécharger le fichier du site actuel. Si vous avez sauvegardé le fichier, cliquez sur Ignorer.

■ Migrer le site

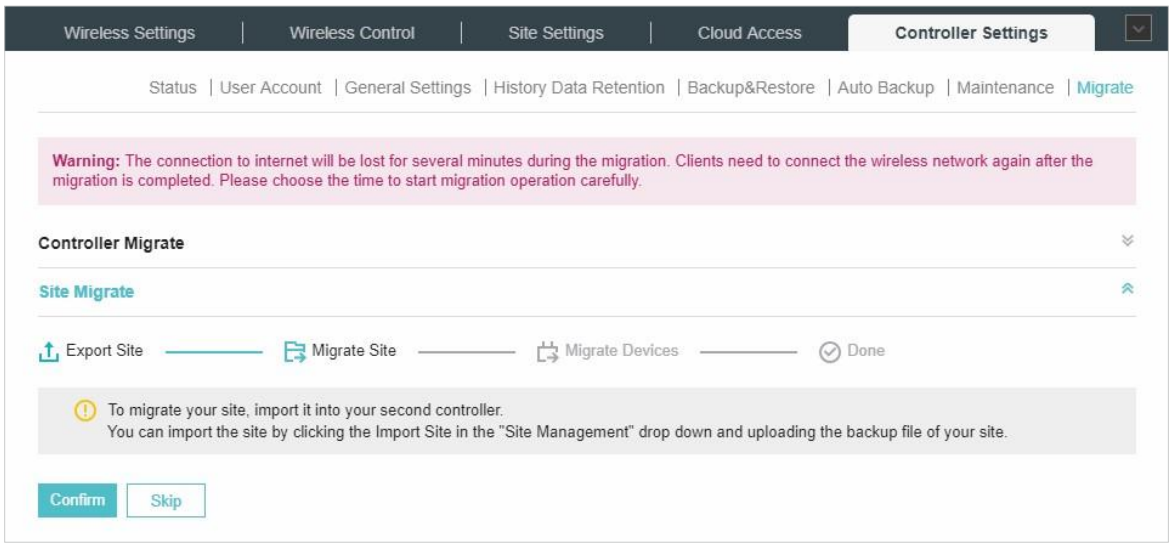
1 Sélectionnez Site Manager et se connecter sur le site voulu.



2. Import Site et entrez Onu nom Unique Verser le nouveau Site.

3. Cliquez sur Parcourir pour télécharger le fichier du site à importer, puis sur Importer pour importer le site.

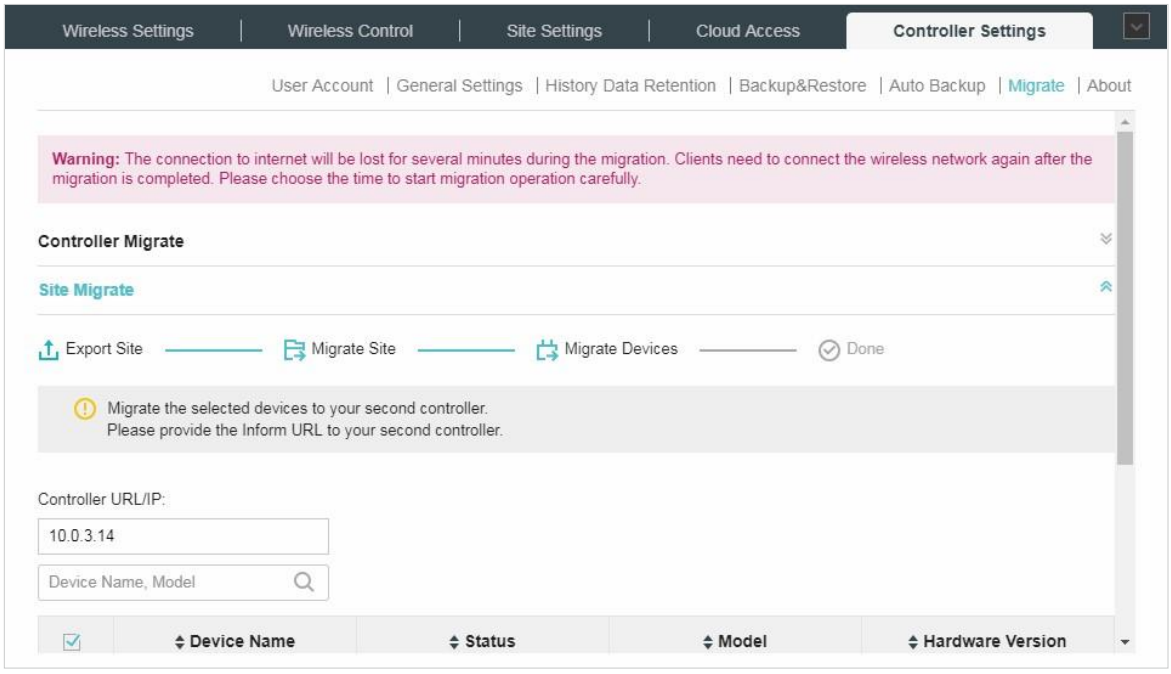
4. Une fois que le fichier a été importé sur le deuxième contrôleur, retournez au contrôleur d'exportation et cliquez sur Confirmer.



■ Migrer les périphériques

1. Entrez l'adresse IP ou l'URL de votre deuxième contrôleur dans l'URL/IP du contrôleur déposée.

   Dans ce cas, l'adresse IP du deuxième contrôleur est ***10.0.3.14***.

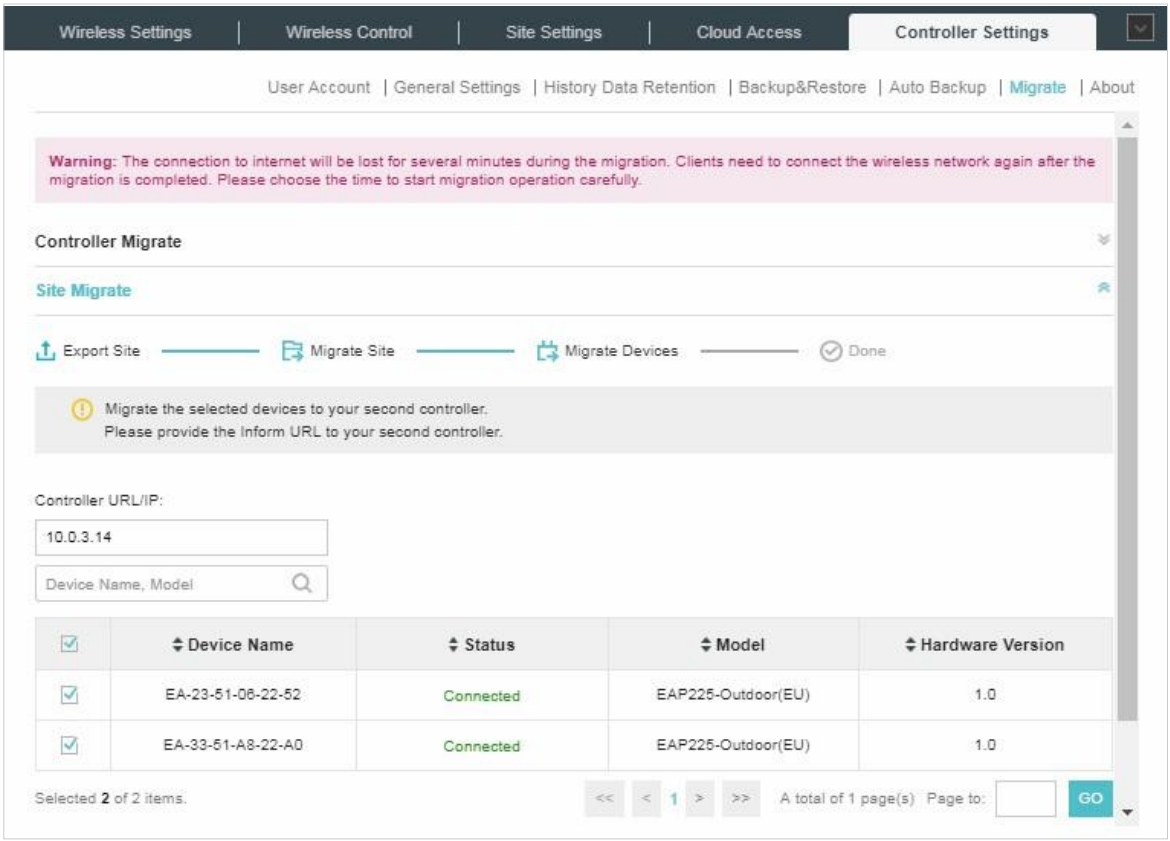


Notes :

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

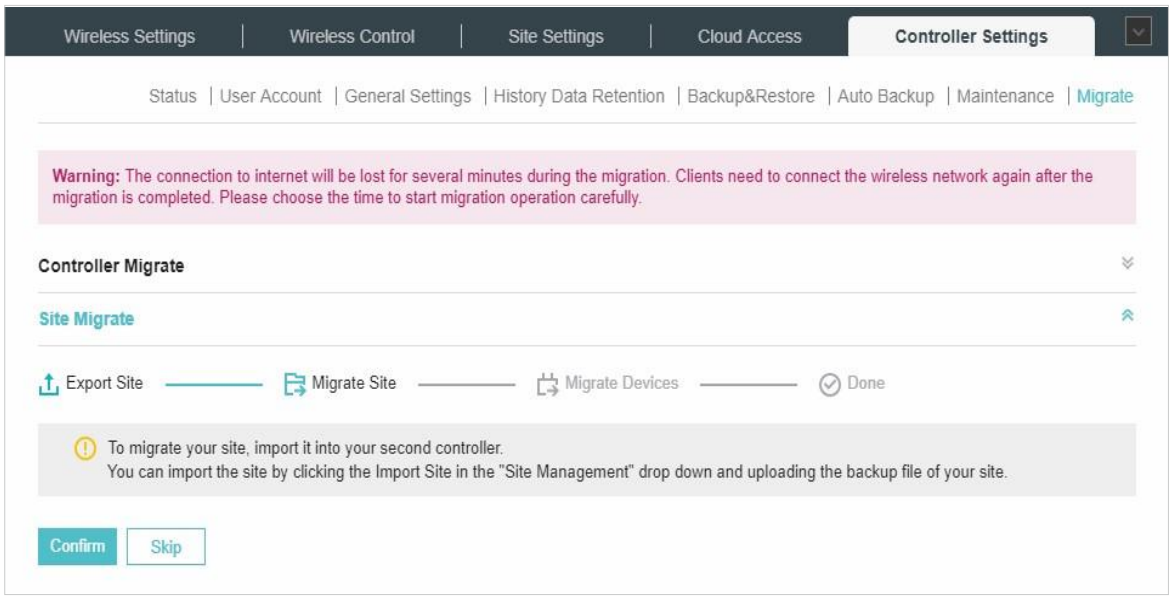
2. Sélectionnez les périphériques à migrer en cliquant sur les cases à côté de chaque appareil.

   Par défaut, tous les appareils sont sélectionnés.

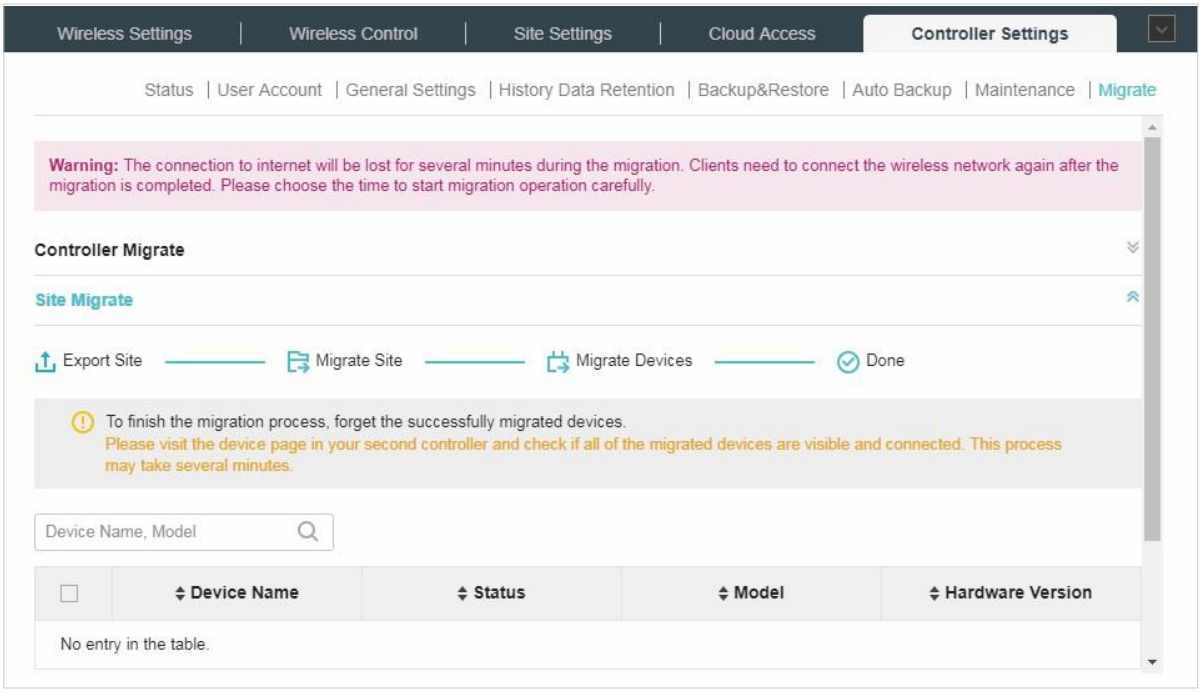


3. Cliquez sur Migrer des périphériques pour migrer les périphériques sélectionnés vers le deuxième contrôleur.

4. Vérifiez que tous les périphériques migrés sont visibles et connectés sur le deuxième contrôleur. Notez que cela peut prendre plusieurs minutes. Lorsque tous les périphériques migrés sont en état connecté dans la page Points d'accès du deuxième contrôleur, 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 deuxième contrôleur. Vous pouvez supprimer le site précédent si nécessaire.


Wireless Settings
Wireless Control
Site Settings
Cloud Access
Controller Settings
Status | User Account | General Settings | History Data Retention | Backup&Restore | Auto Backup | Maintenance | Migrate
Warning: The connection to internet will be lost for several minutes during the migration. Clients need to connect the wireless network again after the migration is completed. Please choose the time to start migration operation carefully.
Controller Migrate
Site Migrate
Export Site
Migrate Site
Migrate Devices
Done
To finish the migration process, forget the successfully migrated devices.
Please visit the device page in your second controller and check if all of the migrated devices are visible and connected. This process may take several minutes.
Device Name, Model
Device Name
Status
Model
Hardware Version
No entry in the table.

7 Exemple d’application

Une usine dispose d’un réseau sans fil avec trois EAP gérés par l’OC200. L’administrateur réseau veut :

■ Surveiller les EAP avec la carte.

■ Activer la fonction Portal pour attirer l’attention des clients sur les annonces du supermarché lorsque les clients tentent d’accéder accès au réseau. Les clients doivent utiliser un mot de passe simple pour passer l’authentification.

■ Permettre aux employés du restaurant d’accéder aux accès ressources du réseau sans authentification du portail.

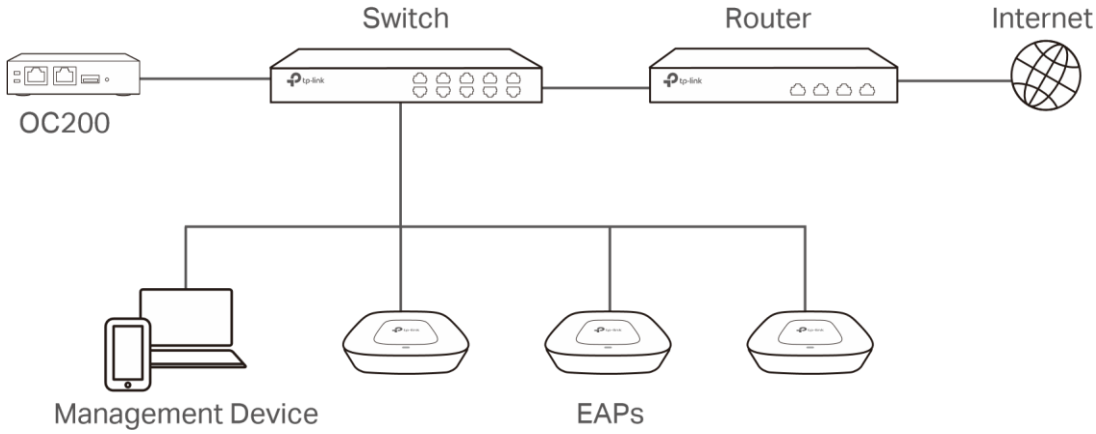
■ Planifier la radio pour fonctionner uniquement pendant le temps de travail (8h00 am à 22h00) afin de réduire la consommation d’énergie.

Suivez les étapes ci-dessous pour atteindre les exigences ci-dessus.

7.1 Configurations de base

Suivez les étapes ci-dessous pour effectuer la configuration de base.

1. Connectez les périphériques comme l'indique la topologie suivante.



2. Lancez l'OC200 et suivez les instructions pour compléter certaines configurations initiales.
3. Connectez-vous à l'interface de gestion d'OC200.
4. Adoptez les EAP en attente.

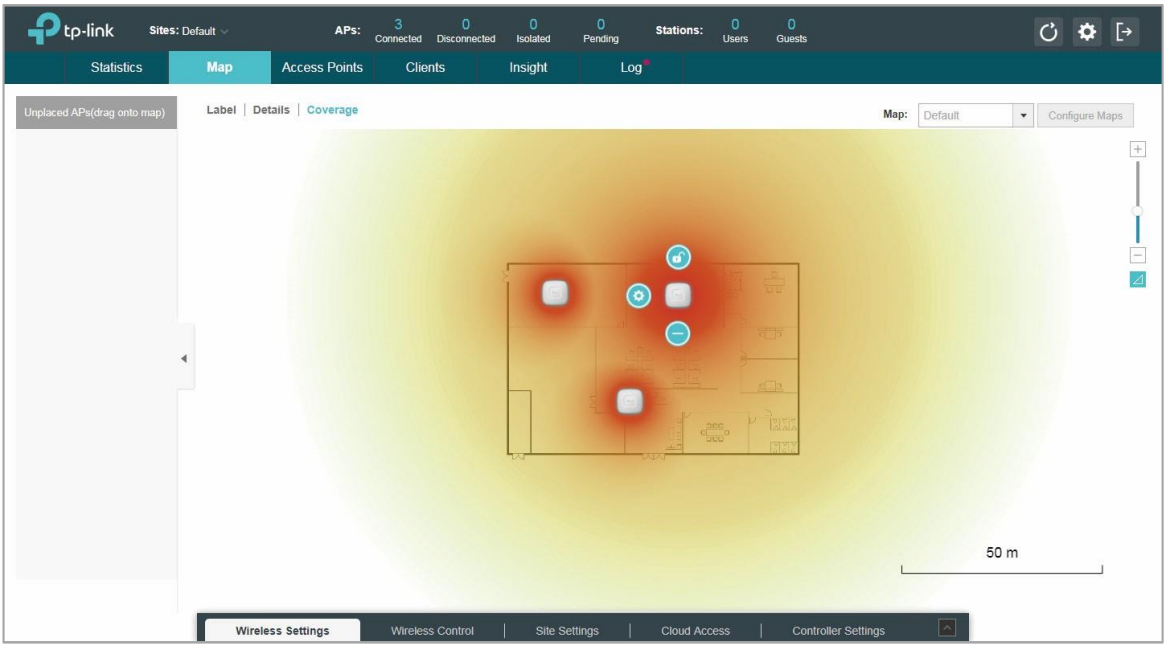
7.2 Paramètres avancés

Après la configuration de base, reportez-vous au contenu suivant pour répondre aux exigences de l'administrateur réseau .

7.2.1 Surveiller les EAP avec carte

Suivez les étapes ci-dessous pour créer une carte et surveiller les EAP avec la carte.

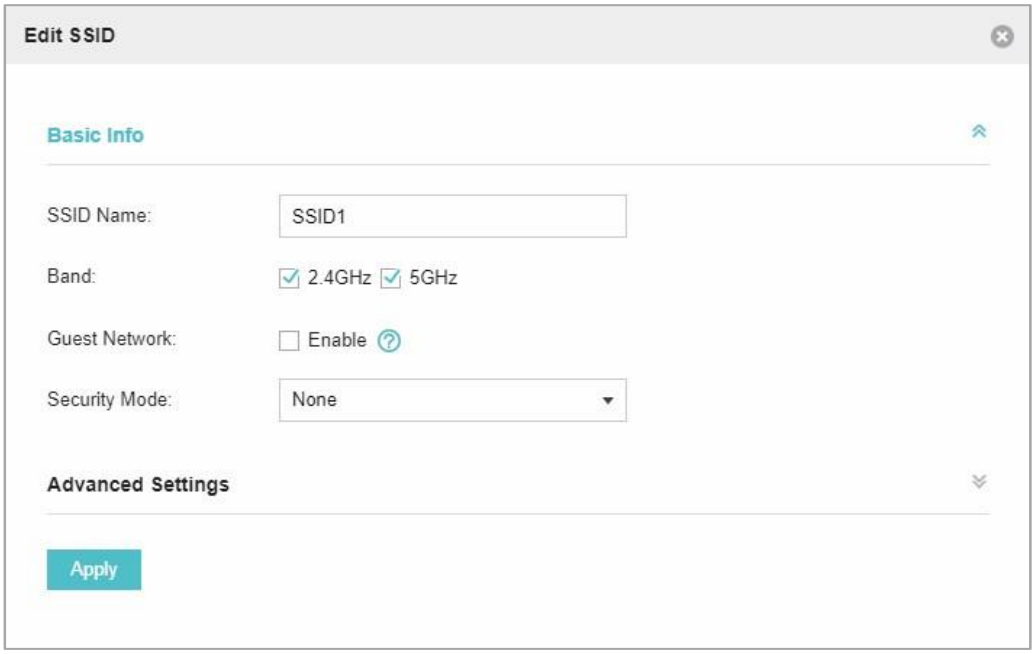
1. Accédez à la carte.
2. Importer une carte locale et définir l'échelle de la carte.
3. Faites glisser les EAP vers les emplacements appropriés sur la carte.
4. Cliquez sur Couverture et vous pouvez voir la représentation de la couverture sans fil des EAP.



7.2.2 Configurer l'authentification du portail

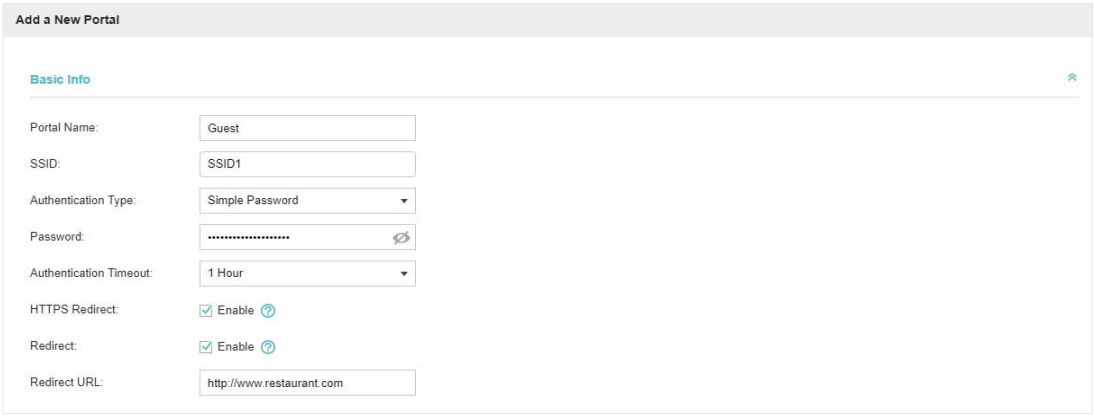
Suivez les étapes ci-dessous pour configurer la fonction Portal.

1. Accédez à Paramètres sans fil > Paramètres sans fil de base et modifiez le SSID que nous avons créé dans la configuration de base.



Pour faciliter la connexion des clients, modifiez le mode sécurité de WPA-PSK en Aucun. Les clients peuvent se connecter aux EAP sans mot de passe et être redirigés vers l'authentification du portail où le mot de passe correct sera requis.

2. Ouvrez la fenêtre de configuration globale et accédez à Contrôle sans fil > Portail. Cliquez sur La Add a New Portal fenêtre de configuration apparaît .
3. Dans la section Informations de base, remplissez les paramètres de base du portail.



1) Spécifiez un nom au portail.

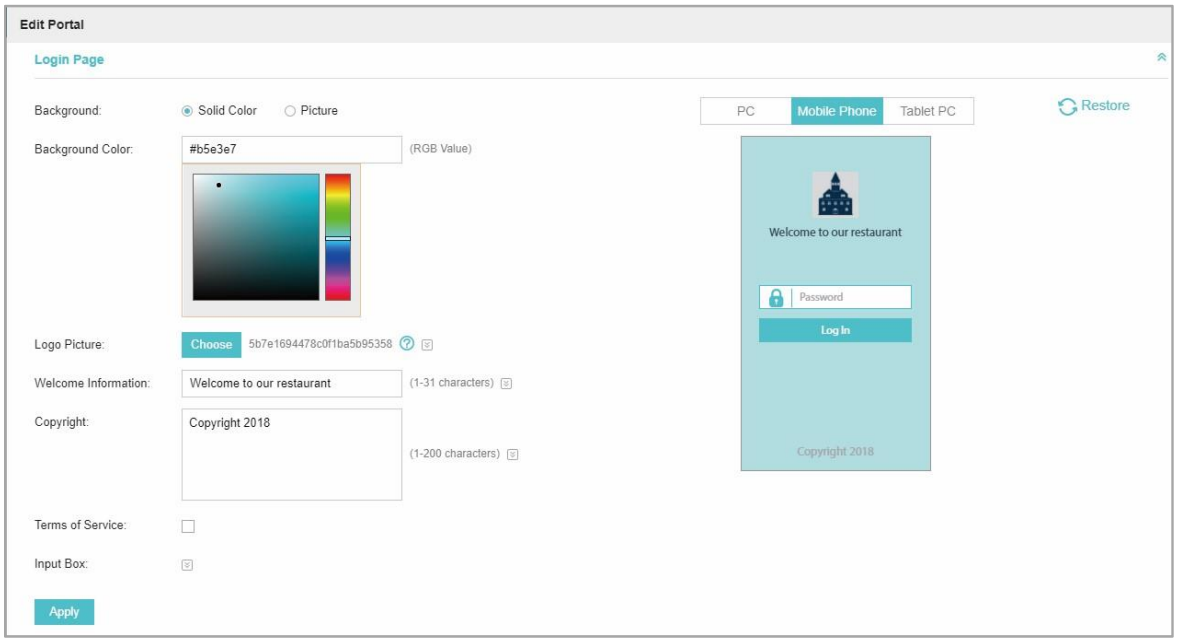
2) Sélectionnez un SSID pour le portail.

3) Sélectionnez le type d'authentification comme mot de passe simple. Spécifiez un mot de passe simple pour les invités.

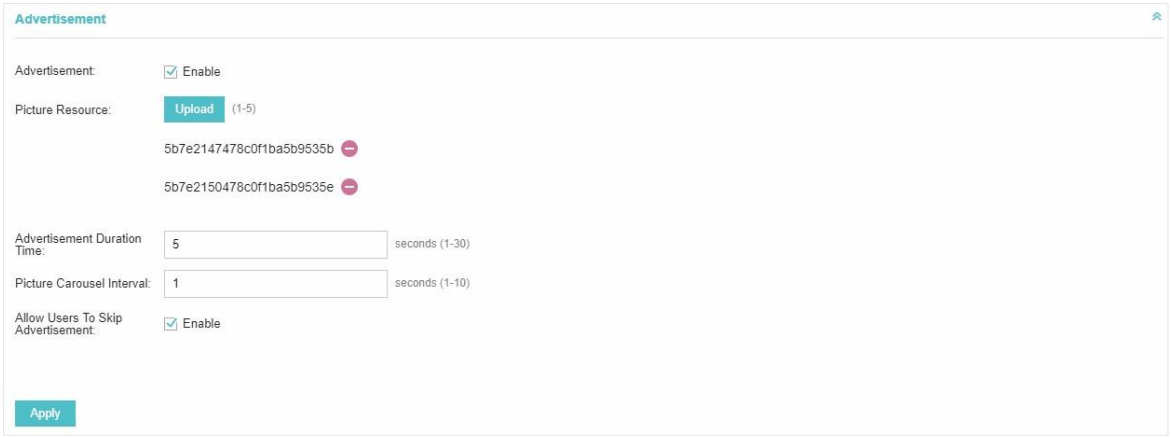
4) Sélectionnez le délai d'expiration d'authentification. Par exemple,1 heure convient aux clients du restaurant.

5) Permettre à la redirection de conduire les clients à la page d'accueil du restaurant après connexion réussie. Nous pouvons mettre quelques informations de promotion sur la page.

4. Dans la section Page de connexion, configurez la page de connexion.



5. Dans la section Publicité, téléchargez deux photos du restaurant et définissez les paramètres connexes .



6. Appliquer

7.2.3 Créer un SSID pour les employés

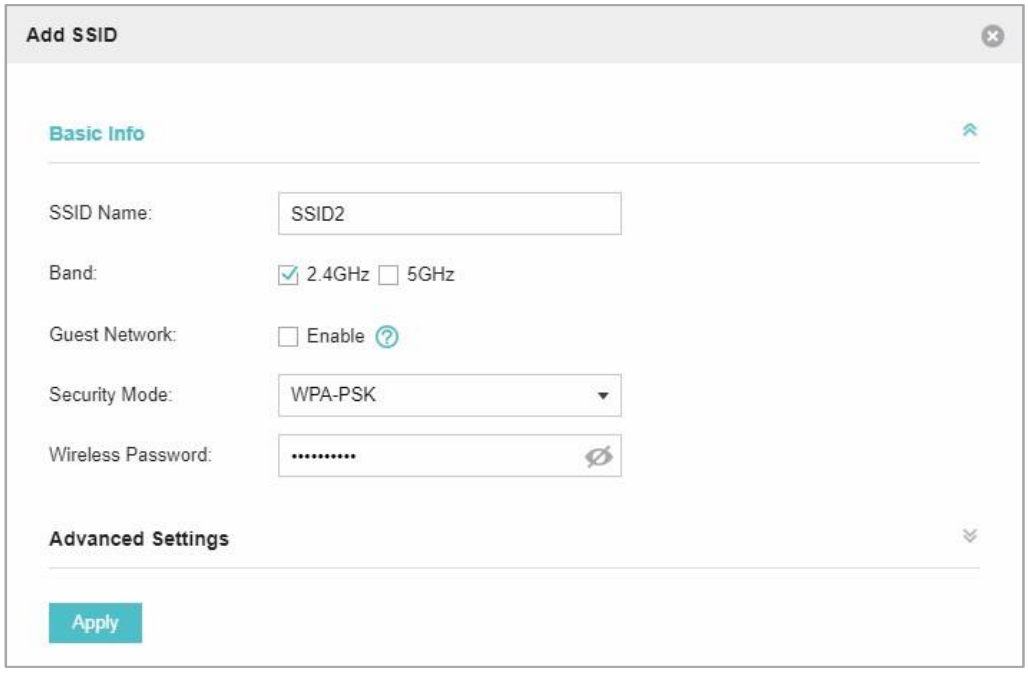
Nous avons créé un SSID dans la configuration de base pour les clients. Ici, nous devons créer un autre SSID pour les employés pour leur permettre d'accéder au accès réseau sans authentification du portail .

En outre, le nouveau SSID devrait être invisible pour les clients.

Suivez les étapes ci-dessous pour créer un SSID pour les employés.

1. Ouvrez la fenêtre de configuration globale et accédez aux paramètres sans fil > Paramètres sans fil de base.

2. Cliquez sur Ajouter pour ajouter un nouveau SSID.



Configurer les paramètres.

1) Désactiver la diffusion SSID pour masquer ce SSID aux clients.

2) Spécifiez le nom SSID, le mode de sécurité et le mot de passe sans fil. Laissez les employés entrer manuellement le nom et le mot de passe SSID et choisissez le mode de sécurité que vous définissez pour accéder au réseau.

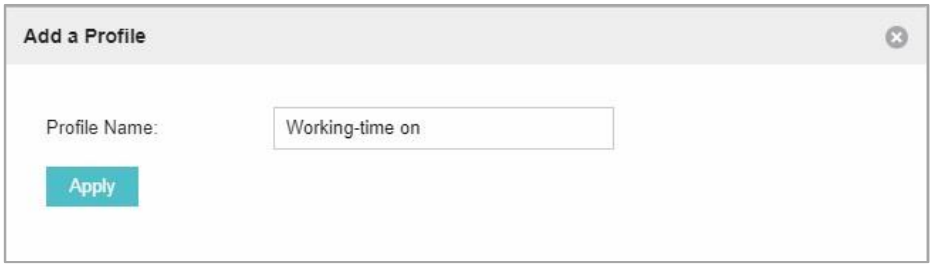
3) Cliquez sur Appliquer pour enregistrer la configuration.

7.2.4 Configurer le planificateur

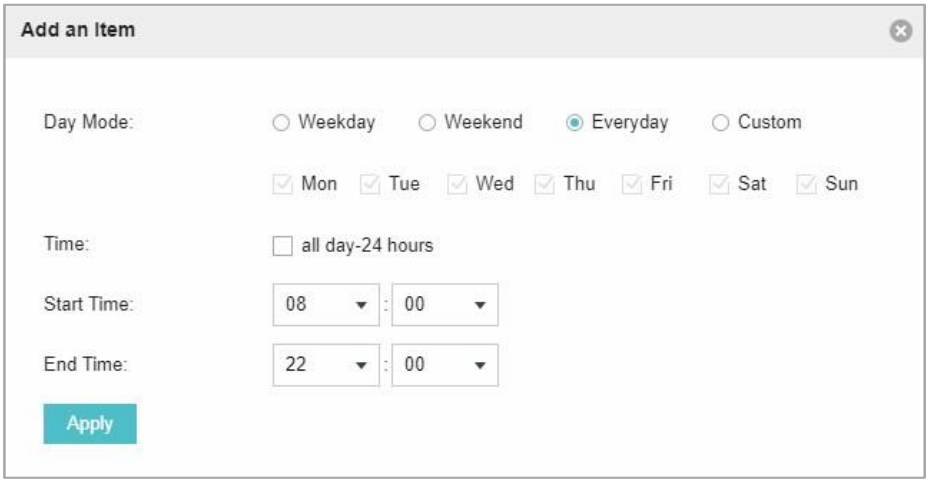
Suivez les étapes ci-dessous pour planifier la radio pour fonctionner uniquement pendant le temps de travail (de 8:00 à 22:00).

1. Ouvrez la fenêtre de configuration globale et accédez à Contrôle sans fil > Planificateur.

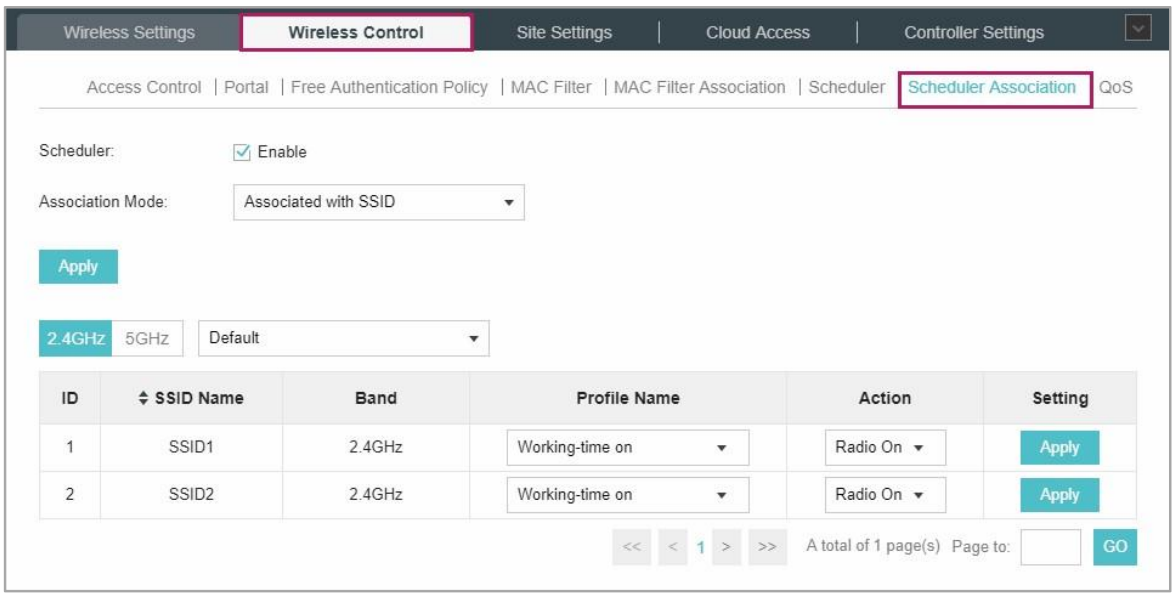
1) Ajouter un profil.



2) Ajouter un élément pour le profil. Les paramètres sont réglés comme indiqué sur l'écran suivant.



2. Accédez à l'onglet Association des planificateurs.



1) Activez la fonction et sélectionnez Associé au SSID. Cliquez sur Appliquer.

2) Dans la colonne Nom du profil des deux SSID, sélectionnez le profil que nous venons de créer.

3) Dans la colonne Action des deux SSID, sélectionnez Radio On.

4) Cliquez sur Appliquer dans la colonne Définition des deux SSID.

5) Sélectionnez 5GHz et effectuez les mêmes configurations que ci-dessus.

Annexe Omada APP

Omada app est une application mobile conçue pour les produits EAP de la série Omada. Il vous permet de surveiller et de gérer facilement votre réseau. L'application Omada peut être utilisée pour les modes Autonome et Controller.

Cette annexe présente comment utiliser l'application Omada pour gérer votre réseau et inclut les sections suivantes :

- Installez l'application Omada sur l'appareil mobile
- Gérer votre réseau en mode autonome
- Gérer votre réseau en mode Contrôleur

1 Installer l'application Omada sur l'appareil mobile

L'application Omada s'exécute sur des appareils iOS et Android, tels que les téléphones intelligents et les tablettes. Lancez l'Apple App Store (iOS) ou google play store (Android) et recherchez « TP-Link Omada » ou numérisez simplement le code QR pour télécharger et installer l'application.

Download on the App Store

GET IT ON Google Play

ou

Scan for Omada App

Download Omada App

2 Gérer votre réseau en mode autonome

Pour un réseau relativement petit qui dispose de quelques EAP (généralement moins de trois) et que seules les fonctions de base sont nécessaires, le mode autonome est recommandé. Vous pouvez utiliser un appareil mobile pour configurer chaque EAP individuellement pour les fonctionnalités de base sans configurer un contrôleur logiciel OC200 ou Omada. Notez que le EAP géré par l'OC200 ou le Contrôleur logiciel Omada est inaccessible en mode autonome.

Reportez-vous à la topologie ci-dessous, assurez-vous que les exigences suivantes ont été remplies :

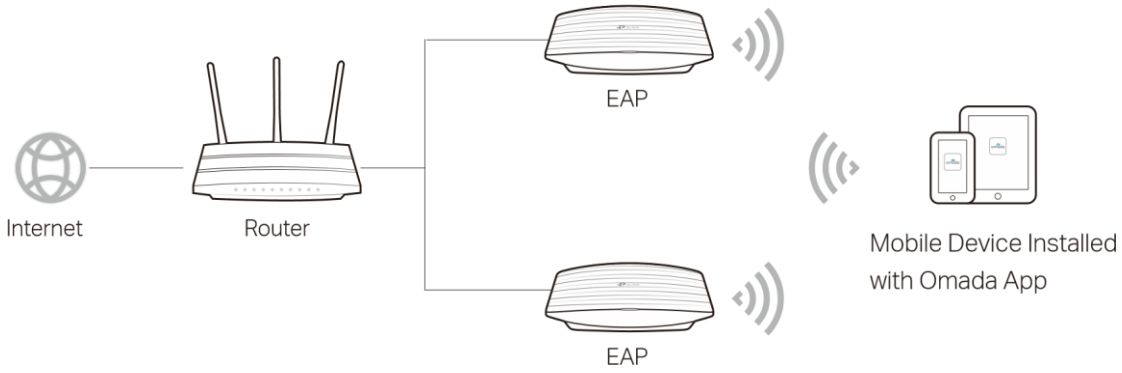
- les connexions Ethernet de votre EAP Omada au réseau local avec un serveur DHCP.
- La version du firmware prise en charge du EAP. EAP245, EAP225, EAP115, EAP110, EAP225-Outdoor, EAP110-Outdoor, EAP115-Wall et EAP225-Wall sont actuellement pris en charge. Pour vérifier les versions du firmware des EAP pris en charge, veuillez consulter :

  www.tp-link.com/omada_compatibility_list.

D'autres produits seront pris en charge par l'application Omada dans un proche avenir que les mises à jour du firmware sont libérés.

■ Un appareil compatible iOS ou Android avec l'application Omada.

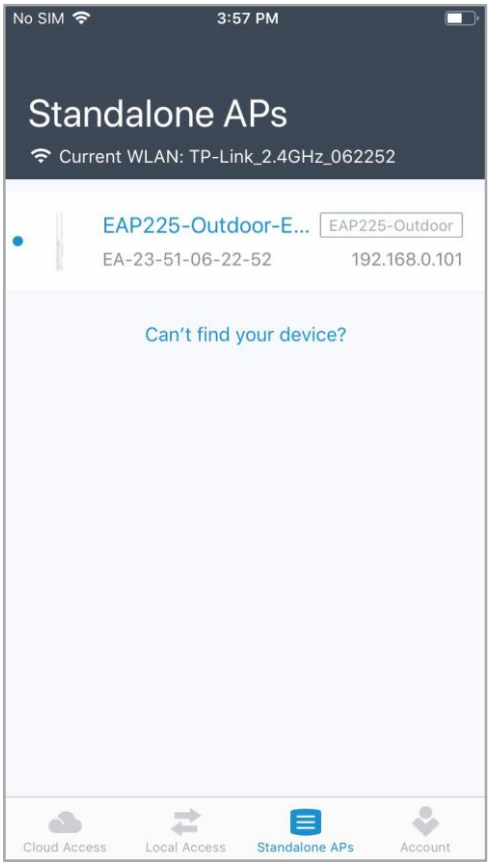
Connexion de votre EAP Omada au réseau local avec un serveur DHCP.



Suivez les étapes ci-dessous pour gérer votre réseau via l'application Omada en mode autonome. La page suivante est exemple avec la version iOS de l'application. La version Android est similaire.

1. Connectez votre appareil mobile au EAP à l'aide du SSID par défaut (format : TPLink 2.4GHz/5GHz_XXXXXX) imprimé sur l'étiquette.

2. Lancez l'application Omada, appuyez sur Ap autonomes et attendez que le EAP soit découvert automatiquement.



Conseils

Conseils

3. L'application Omada est conçue pour vous aider à configurer rapidement certains paramètres de base. Pour une configuration avancée, vous pouvez utiliser le mode

contrôleur. Et lorsque votre EAP est géré par le contrôleur, vous ne pouvez pas utiliser le mode autonome.

4. En mode autonome, un seul utilisateur est autorisé à se connecter à la page de gestion du EAP en même temps. Ainsi, la page Web de gestion du EAP ne peut pas être connecté à l'utilisation de l'application Omada et vice versa. En outre, un seul utilisateur peut se connecter à l'EAP via l'application Omada.

3 Gérer votre réseau en mode Contrôleur

Pour un réseau à grande échelle qui a des EAP de masse et des fonctions avancées sont nécessaires, le mode contrôleur est recommandé. Le mode contrôleur vous permet de configurer et de synchroniser automatiquement les paramètres sans fil unifiés à tous les EAP du réseau.

L'application Omada offre un moyen pratique d'accéder à l'OC200 et d'adopter des EAP. Avec la fonction Accès local et accès au cloud sur l'application Omada, vous pouvez gérer l'OC200 sur les sites locaux et distants.

Notes

L'OC200 doit être maintenu en cours d'exécution lors de l'utilisation de l'application Omada pour accéder à l'OC200.

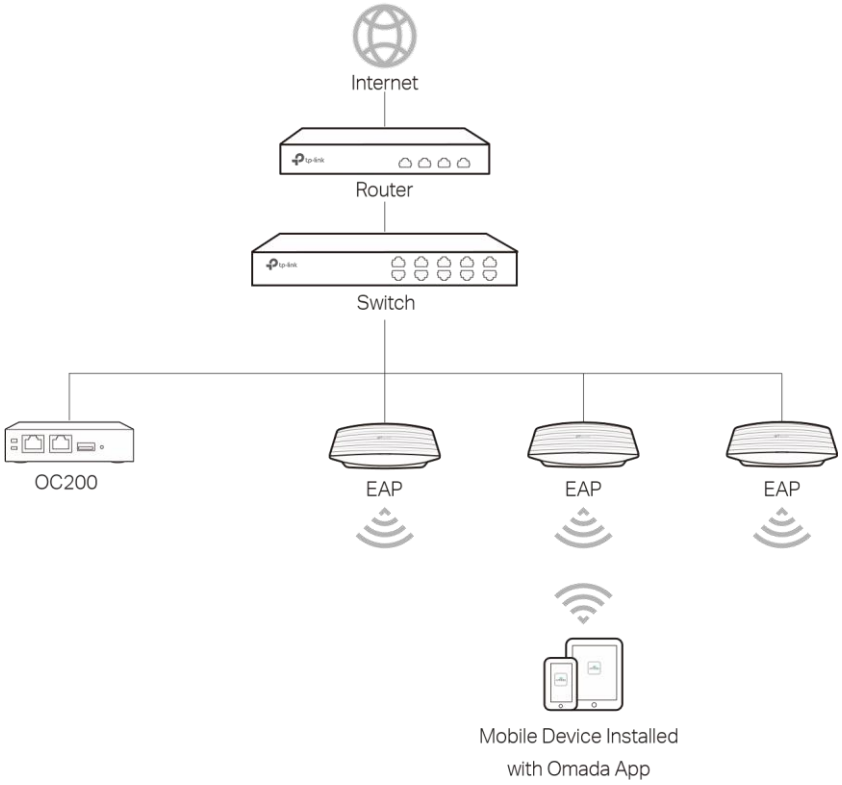
3.1 Gérer localement vos EAP à l'aide de l'application Omada

La fonction Accès local de l'application Omada est conçue pour accéder à l'OC200 qui se trouve dans le même sous-réseau avec vos appareils mobiles. Reportez-vous à la topologie ci-dessous, assurez-vous que les exigences suivantes ont été remplies :

■ Une connexion Ethernet entre votre EAP Omada et le réseau local avec un serveur DHCP.

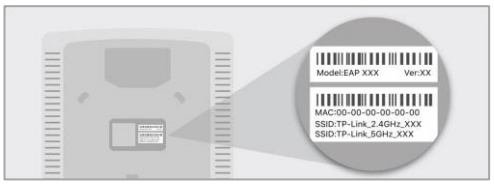
■ La version du contrôleur logiciel Omada est 3.0.2 ou plus.

■ Un appareil compatible iOS ou Android avec l'application Omada.

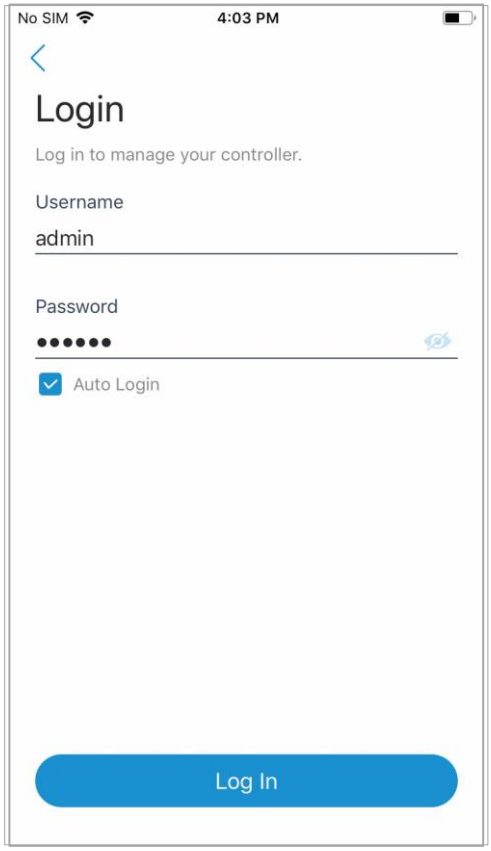


Suivez les étapes ci-dessous pour gérer votre réseau via l'application Omada en mode contrôleur localement. La page suivante est exemple avec la version iOS de l'application. La version Android est similaire.

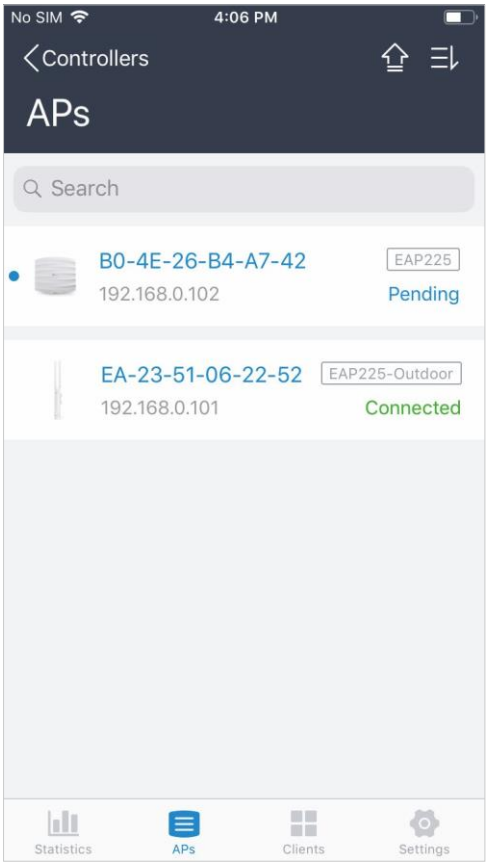
1. Connectez votre appareil mobile au EAP à l'aide du SSID par défaut (format : TP-Link 2.4GHz/5GHz_XXXXXX) imprimé sur l'étiquette en bas du produit. Notez que le EAP doit se faire dans le même sous-réseau que l'OC200.



1. Appuyez sur l'OC200, la page de connexion s'affiche. Entrez le nom d'utilisateur et le mot de passe de l'OC200, puis appuyez sur Connexion pour lancer l'OC200.



1. Sur l’écran AP, appuyez sur le EAP en attente d’adoption. Et vous pouvez utiliser les fonctions en bas pour naviguer dans différents écrans de l’OC200, y compris les statistiques sans fil, les informations des clients et les paramètres de base.



3.2 Gérez à distance vos EAP à l’aide de l’application Omada

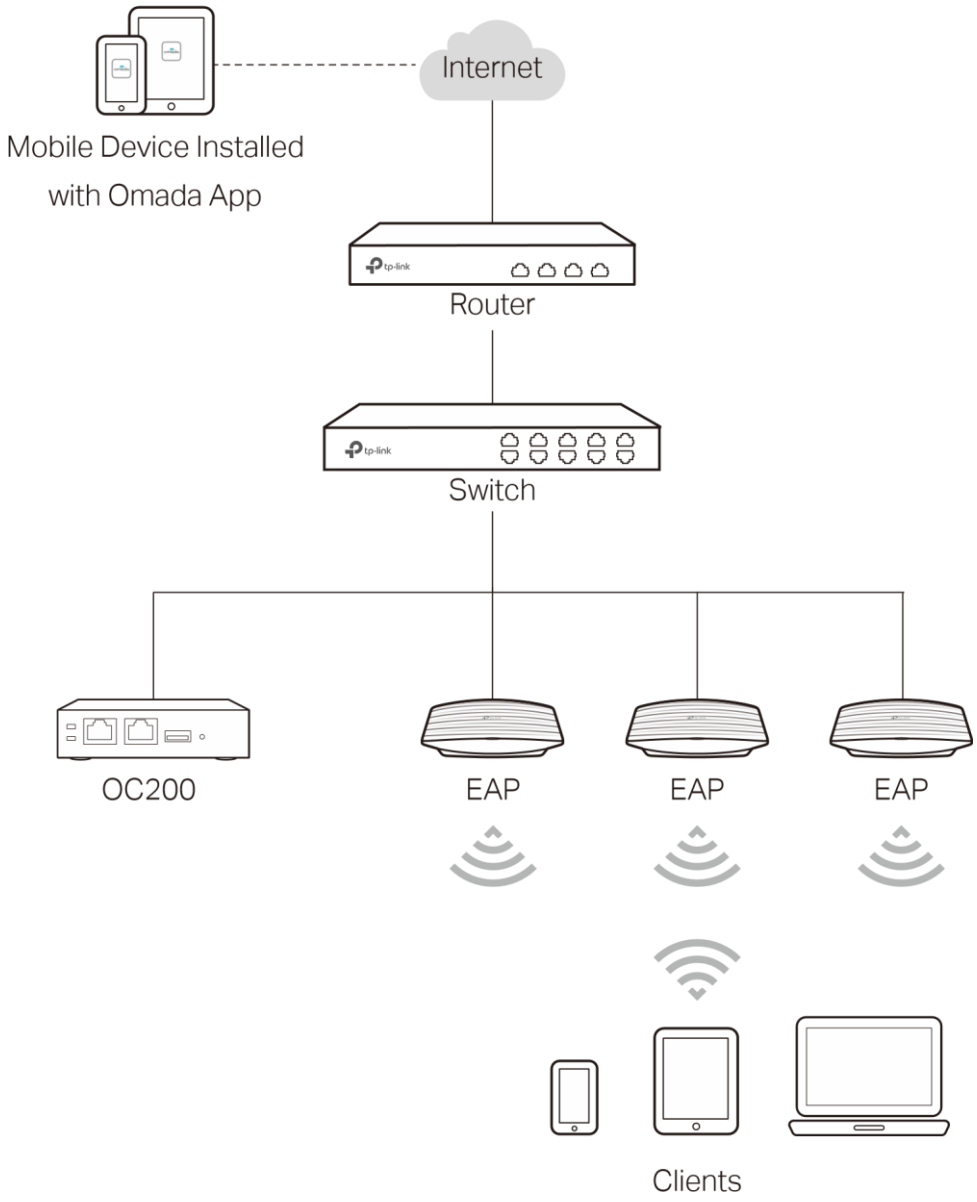
La fonction Cloud Access de l’application Omada est conçue pour accéder au service OC200 via Omada Cloud. Ainsi, vous pouvez configurer votre OC200 et gérer les EAP à tout moment, de n’importe où.

Reportez-vous à la topologie ci-dessous, assurez-vous que les exigences suivantes ont été remplies :

■ Votre OC200 et votre appareil mobile ont accès à Internet.

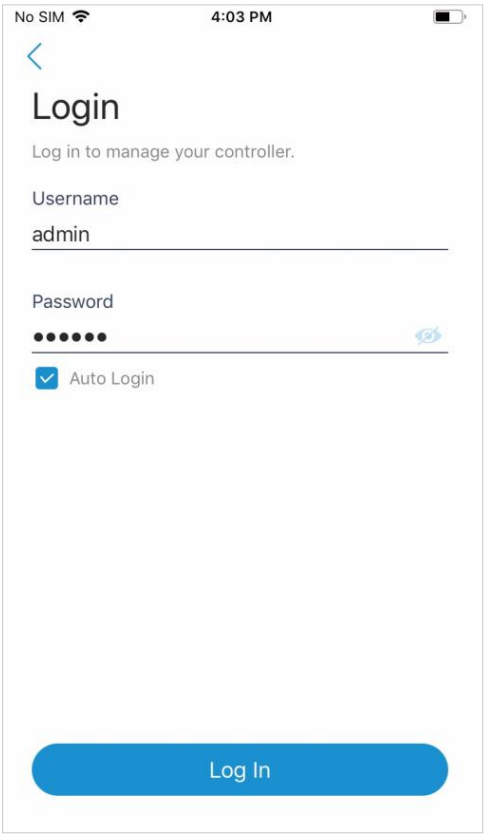
■ Un appareil compatible iOS ou Android avec l’application Omada.

■ L’accès au cloud est activé sur l’OC200. L’OC200 a été lié par un ID TP-Link. Pour plus de détails sur l’accès au cloud sur l’OC200, reportez-vous au service Cloud Omada.

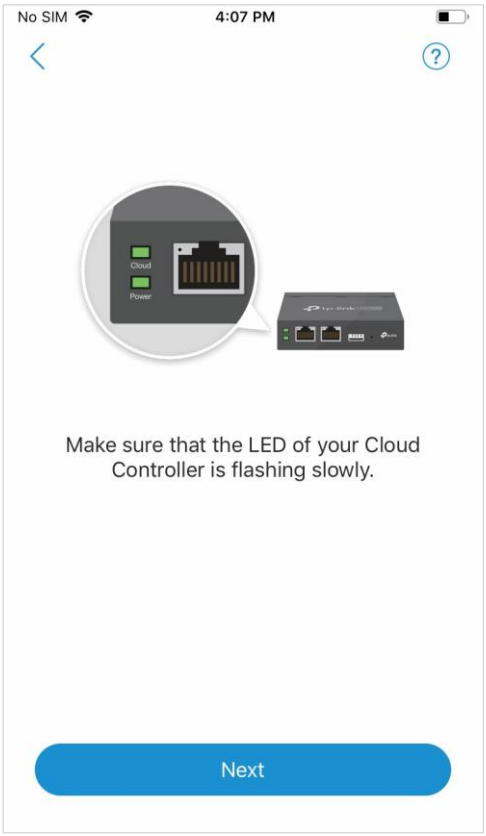


Suivez les étapes ci-dessous pour gérer votre réseau via l’application Omada en mode contrôleur à distance. La page suivante est exemple avec la version iOS de l’application. La version Android est similaire.

1. Lancez l’application Omada, accédez à Cloud Access et appuyez sur Aller pour vous connecter pour vous connecter à Omada Cloud avec votre ID TP-Link.



1. Dans la page Accès cloud, appuyez sur le bouton **+** dans le coin supérieur droit, la page suivante s'affiche. Puis appuyez sur Suivant.



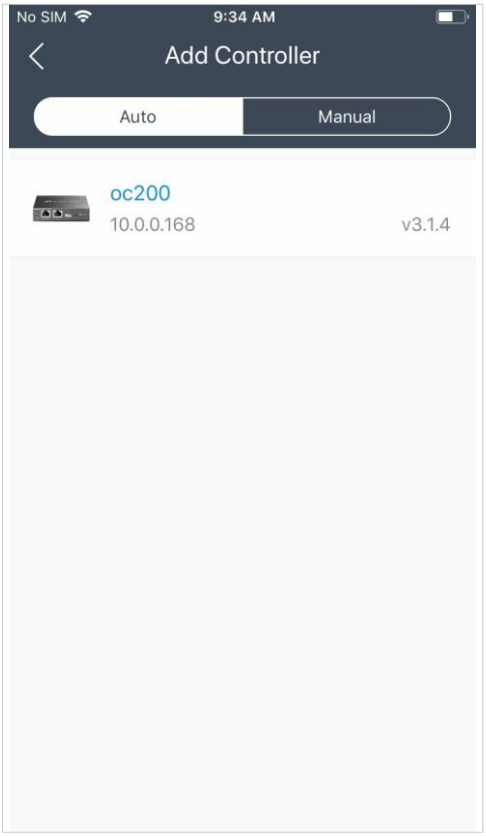
2 Numérisez le code QR qui est imprimé à l'arrière du contrôleur cloud ou entrez manuellement la clé du périphérique pour lier l'OC200 à votre ID TP-Link.

Conseils

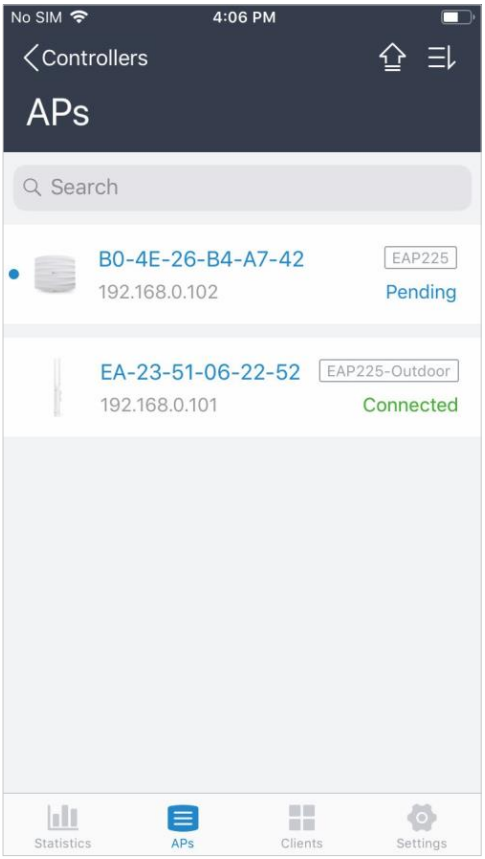
Vous pouvez également vous connecter à l'OC200 et lier l'ID TP-Link à l'OC200. Pour plus d'informations, reportez-vous au service Cloud d'Omada.

4. Tous les OC200 en ligne qui sont liés à votre ID TP-Link apparaîtront sur la page.

Robinetl'OC200 pour lancer et configurer le contrôleur.



3. Sur l'écran AP, appuyez sur le EAP en attente d'adoption. Et vous pouvez utiliser les fonctions en bas pour naviguer dans différents écrans du contrôleur Omada, y compris les statistiques sans fil, les informations des clients et les paramètres de base.



DROITS D’AUTEUR ET MARQUES DE COMMERCE

Les spécifications peuvent être modifiées sans préavis. tp-link 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.

DÉCLARATION DE LA FCC

Nom du produit **:**Omada Cloud Controller Numéro de

modèle**:** OC200

Partie responsable :

TP-Link USA Corporation, d/b/a TP-Link North America, Inc.

Adresse : 145 South State College Blvd. Suite 400, Brea, CA 92821

Site Web : https://www.tp-link.com/us/

Tél.: +1 626 333 0234

Fax: +1 909 527 6803

E-mail: sales.usa@tp-link.com

Cet équipement a été testé et jugé conforme aux limites d’un appareil numérique de classe B, conformément à la partie 15 des règles de la FCC. Ces limites sont conçues pour fournir une protection raisonnable contre les interférences nocives dans une installation résidentielle. Cet équipement génère, utilise et peut émettre de l’énergie par radiofréquence et, s’il n’est pas installé et utilisé conformément aux instructions, peut causer des interférences nocives aux communications radio. Toutefois, il n’y a aucune garantie que des interférences ne se produiront pas dans une installation particulière. Si cet équipement cause des interférences nuisibles à la réception de la radio ou de la télévision, qui peuvent être déterminées en éteignant et en allumant l’équipement, l’utilisateur est encouragé à essayer de corriger l’interférence par une ou plusieurs des mesures suivantes :

- Réorienter ou déplacer l’antenne de réception.
- Augmenter la séparation entre l’équipement et le récepteur.
- Connectez l’équipement à une prise sur un circuit différent de celui auquel le récepteur est connecté.

■ Consultez le concessionnaire ou un technicien expérimenté en radio/télévision pour obtenir de l'aide. Ce dispositif est conforme à la partie 15 des règles de la FCC. L'opération est soumise aux deux conditions suivantes :

1. Cet appareil peut ne pas causer d'interférences nocives.
2. Ce dispositif doit accepter toute interférence reçue, y compris toute interférence qui peut provoquer un fonctionnement indésirable.

Toute modification ou modification non expressément approuvée par la partie responsable de la conformité pourrait annuler le pouvoir de l'utilisateur d'exploiter l'équipement.

Avertissement de marque CE

Il s'agit d'un produit de classe B. Dans un environnement domestique, ce produit peut provoquer des interférences radio, auquel cas l'utilisateur peut être amené à prendre des mesures adéquates.

Déclaration de conformité de l'UE

TP-Link déclare par les présentes que le dispositif est conforme aux exigences essentielles et aux autres dispositions pertinentes des directives 2014/30/UE, 2014/35/UE, 2009/125/CE et 2011/65/UE.

La déclaration de conformité initiale de l'UE peut être trouvée à **ce** **https://www.tp-link.com/en/**

Canadian Comiliance Statement

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes :

1) L'appareil ne doit pas produire de brouillage ;
2) L'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

Industry Canada Statement

CAN ICES-3 (B)/NMB-3(B)

CC notice 注意!

依據 低功率電波輻射性電機管理辦法

第十二條 經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、

加大功率或變更原設計之特性或功能。第十四條 低功率射頻電機之使用不得影響飛航安全及干擾合法

通行；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。前項合法通信，指依電

信規定作業之無線電信。低功率射頻電機需忍受合法通信或工業、科學以及醫療用電波輻射性電機設

備之干擾。

BSMI Notice 安全諮詢及注意事項

- 請使用原裝電源供應器或只能按照本產品注明的電源類型使用本產品。
- 清潔本產品之前請先拔掉電源線。請勿使用液體、噴霧清潔劑或濕布進行清潔。
- 注意防潮，請勿將水或其他液體潑灑到本產品上。
- 插槽與開口供通風使用，以確保本產品的操作可靠並防止過熱，請勿堵塞或覆蓋開口。

■■ 請勿將本產品置放於靠近熱源的地方。除非有正常的通風，否則不可放在密閉位置中。 ■■

請不要私自打開機殼，不要嘗試自行維修本產品，請由授權的專業人士進行此項工作。

限用物質含有情況標示聲明書備考 2."-" 系指該

產品元件名稱	限用物質及其化學符號					
	Pb 鉛	Cd 鎘	Hg 汞	六價鉻 CrVI	多溴聯苯 PBB	多溴二苯醚 PBDE
PCB	○	○	○	○	○	○
外殼	○	○	○	○	○	○
備考 1."○"系指該項限用物質之百分比含量未超出百分比含量基準值。						

項限用物質為排除項目。

Продукт сертифіковано згідно с правилами системи УкрСЕПРО на відповідність вимогам нормативних документів та вимогам, що передбачені чинними законодавчими актами України.

EAC

Information sur la sécurité

- Tenez l'appareil éloigné de l'eau, du feu, de l'humidité ou des environnements chauds.
- N'essayez pas de démonter, réparer ou modifier l'appareil.
- N'utilisez pas de chargeur ou de câble USB endommagé pour charger l'appareil.

Veuillez lire et suivre les informations de sécurité ci-dessus lors de l'utilisation de l'appareil. Nous ne pouvons garantir qu'aucun accident ou dommage ne se produira en raison d'une mauvaise utilisation de l'appareil. Veuillez utiliser ce produit avec précaution et le faire fonctionner à vos propres risques.

Explication des symboles sur l'étiquette du produit

Symboles	Explication
	Alimentation Continu DC
	Utilisation à l’intérieur seulement.
	RECYCLAGE Ce produit porte le symbole de tri sélectif pour les déchets d'équipements électriques et électroniques (DEEE). Cela signifie que ce produit doit être manipulé conformément à la directive européenne 2012/19 / UE afin d'être recyclé ou démantelé afin de minimiser son impact sur l'environnement. L'utilisateur a le choix de donner son produit à un organisme de recyclage compétent ou au détaillant lorsqu'il achète un nouvel équipement électrique ou électronique.
	Pour tout élément complémentaire ou toute information technique relative au Triman, les documents de référence sont le Décret d'application no 2014-1577 du 23 décembre 2014 relatif à la signalétique commune des produits recyclables qui relèvent d'une consigne de tri, codifié aux articles R541-12-17 et R541-12-18 au Code de l’environnement et les recommandations du Guide d'utilisation détaillé développé par l'ADEME