

# Profilage des applications

## Objectif

Cet article illustre les étapes de configuration du profilage d'application sur CBW145AC. Il passe également en revue les avantages et un petit contexte pour les débutants.

Si vous ne connaissez pas les termes de ce document, consultez [Cisco Business : Glossaire des nouveaux termes](#).

## Périphériques pertinents | Version du logiciel

- 140AC ([fiche technique](#)) | 10.0.1.0 ([Télécharger la dernière version](#))
- 141ACM ([fiche technique](#)) | 10.0.1.0 ([Télécharger la dernière version](#))
- 142ACM ([fiche technique](#)) | 10.0.1.0 ([Télécharger la dernière version](#))
- 143ACM ([fiche technique](#)) | 10.0.1.0 ([Télécharger la dernière version](#))
- 240AC ([fiche technique](#)) | 10.0.1.0 ([Télécharger la dernière version](#))

## Que devez-vous savoir sur le profilage des applications ?

Le profilage est un sous-ensemble de fonctionnalités qui permettent d'appliquer une politique d'organisation. Il permet à l'administrateur de faire correspondre et de hiérarchiser les types de trafic. Comme les règles prennent des décisions sur la façon de classer ou de supprimer le trafic. Le système Cisco Business Mesh Wireless comporte un profilage des applications et des clients. L'accès à un réseau en tant qu'utilisateur commence par de nombreux échanges d'informations, parmi lesquels le type de trafic. La stratégie interrompt le flux de trafic pour diriger le chemin, tout comme un diagramme de flux. D'autres types de fonctionnalités de stratégie incluent l'accès invité, les listes de contrôle d'accès et la qualité de service. Chacune de ces caractéristiques a ses propres avantages et inconvénients.

## Que dois-je savoir sur le profilage d'application CBW ?

De nombreuses solutions de maillage sans fil peuvent omettre des fonctionnalités telles que le profilage des applications. Si la bande passante était illimitée, cette fonctionnalité aurait moins de cas d'utilisation. Dans le monde réel, il se peut que nous devions composer les paramètres relatifs au traitement des types de trafic. La série CBW permet un contrôle complet sur de nombreux types d'applications courants. Par exemple, la gestion du débit pour la diffusion en continu par des services tels que Netflix.

## Configuration du profilage d'application

Cette section vous propose des conseils pour les débutants.

### Connexion

Connectez-vous à l'interface utilisateur Web du point d'accès principal. Pour ce faire, ouvrez un navigateur Web et saisissez <https://ciscobusiness.cisco.com>. Vous pouvez recevoir un avertissement avant de continuer. Entrez vos informations d'identification. Vous pouvez également

accéder au point d'accès principal en entrant [https://\[adresse IP\]](https://[adresse IP]) (du point d'accès principal) dans un navigateur Web.

## Conseils

Si vous avez des questions sur un champ de l'interface utilisateur, recherchez une info-bulle qui ressemble à ceci : 

## Trouver l'icône Développer le menu principal pose problème ?

Accédez au menu situé à gauche de l'écran. Si le bouton de menu ne s'affiche pas, cliquez sur cette icône pour ouvrir le menu de la barre latérale. 

## Application Cisco Business

Ces périphériques disposent d'applications complémentaires qui partagent certaines fonctions de gestion avec l'interface utilisateur Web. Toutes les fonctionnalités de l'interface utilisateur Web ne seront pas disponibles dans l'application.

[Télécharger l'application iOS](#) [Télécharger l'application Android](#)

## Forum aux questions

Si vous avez encore des questions sans réponse, vous pouvez consulter notre foire aux questions . [Forum aux questions](#)

### Étape 1

Connectez-vous à votre point d'accès principal.

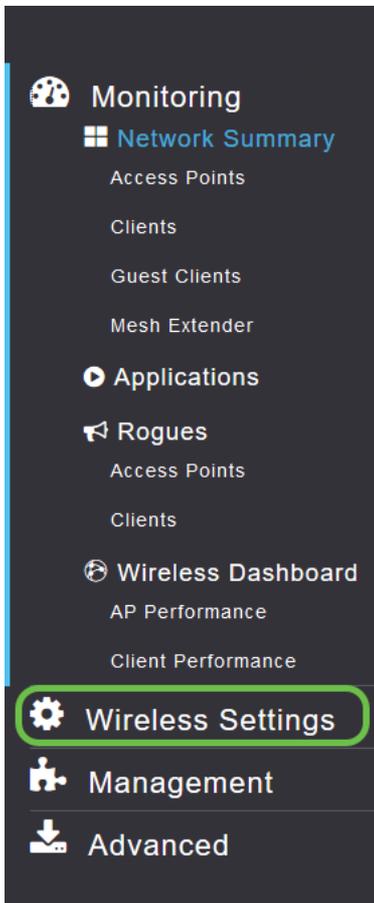
### Étape 2

Naviguez jusqu'au menu situé à gauche de l'écran, si vous ne voyez pas le bouton de menu

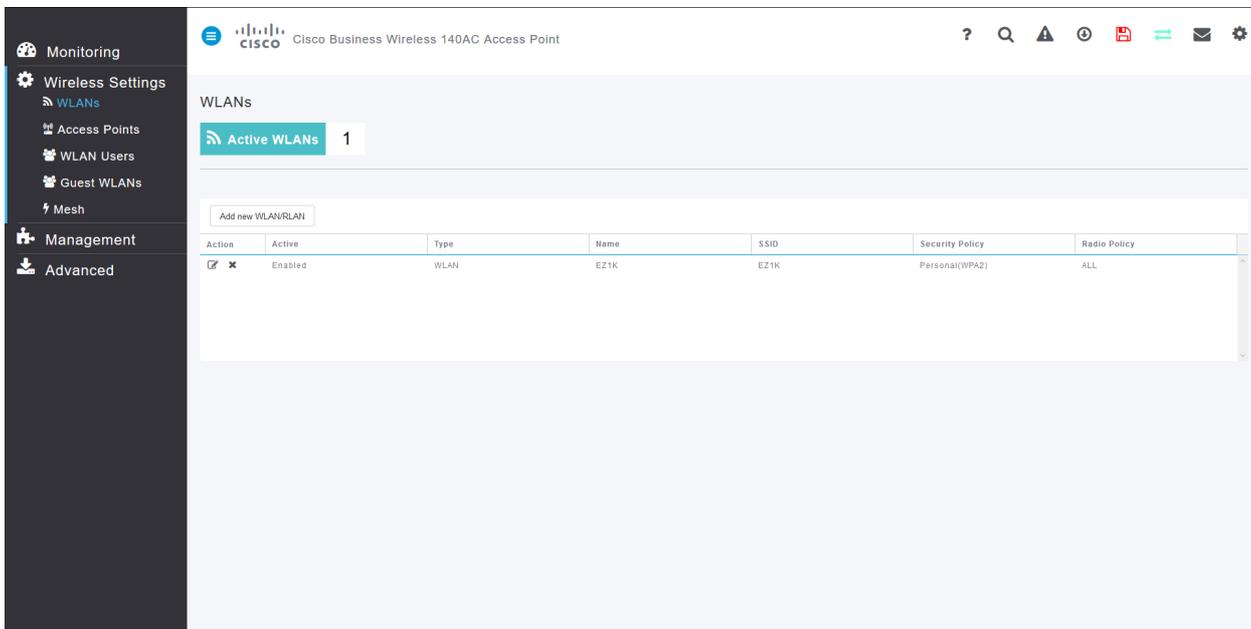


### Étape 3

Le menu Surveillance se charge par défaut lors de la connexion au périphérique. Vous devez plutôt cliquer sur **Wireless Settings (Paramètres sans fil)**.



Les informations ci-dessous sont similaires à celles que vous verrez lorsque vous cliquez sur le lien Wireless Settings (Paramètres sans fil) :



#### Étape 4

Cliquez sur l'icône Edit située à gauche du réseau local sans fil sur lequel vous souhaitez activer l'application.

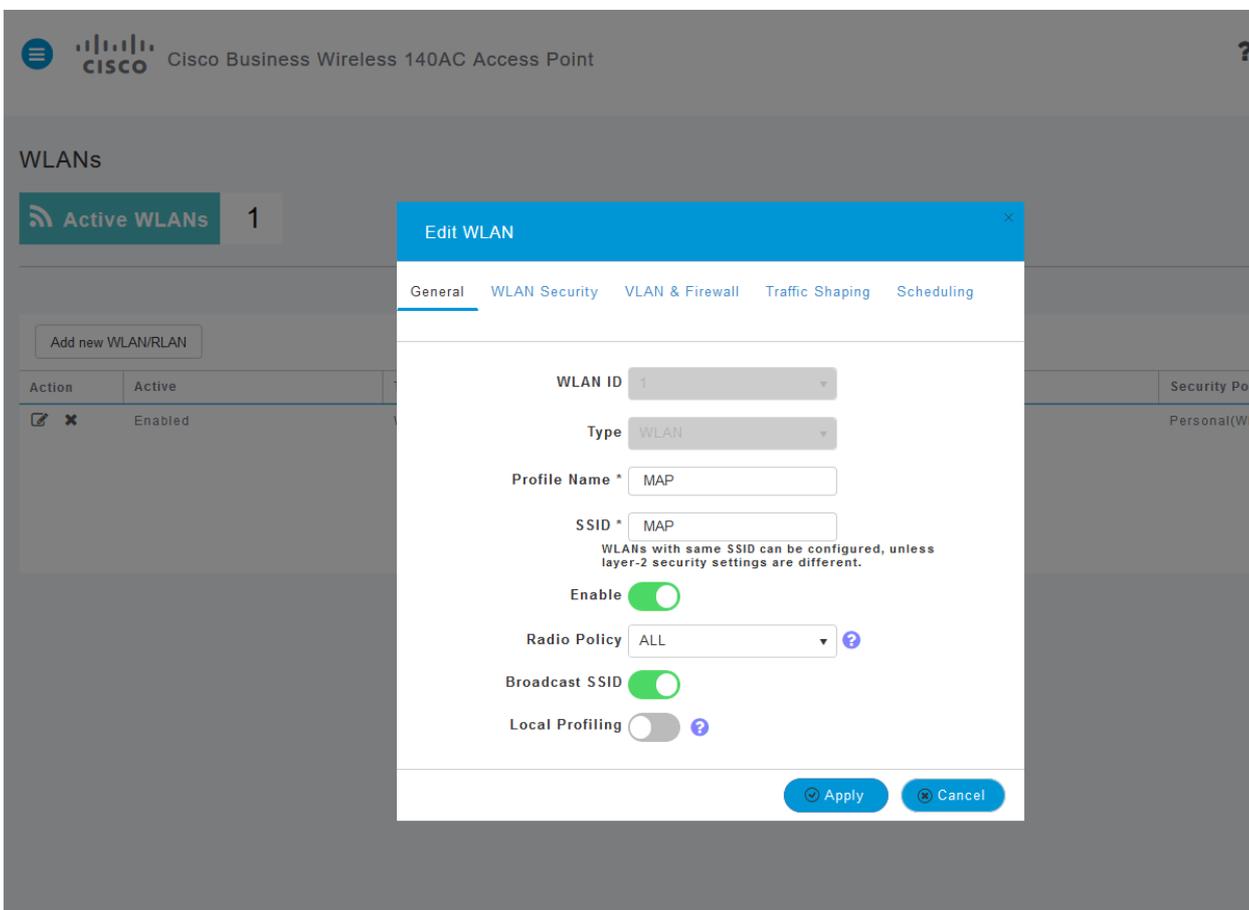
## WLANs

 Active WLANs 1

Add new WLAN/RLAN

Action	Active	Type	N.
 	Enabled	WLAN	E.

Si votre périphérique a été récemment configuré, votre page *Edit WLAN* peut apparaître comme suit :



WLANs

 Active WLANs 1

Add new WLAN/RLAN

Action	Active	Type	N.
 	Enabled	WLAN	E.

### Edit WLAN

General | WLAN Security | VLAN & Firewall | Traffic Shaping | Scheduling

WLAN ID: 1

Type: WLAN

Profile Name \*: MAP

SSID \*: MAP

WLANs with same SSID can be configured, unless layer-2 security settings are different.

Enable:

Radio Policy: ALL

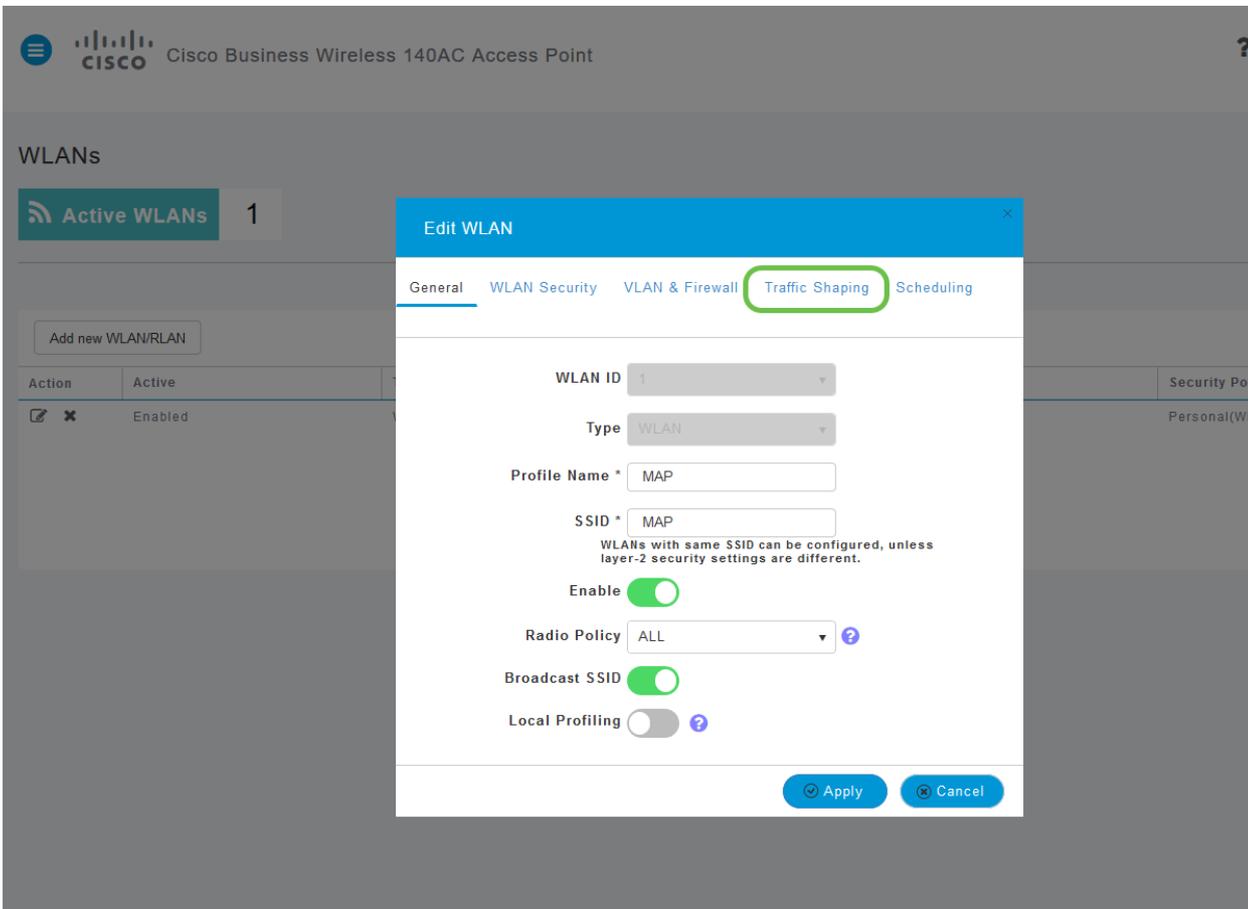
Broadcast SSID:

Local Profiling:

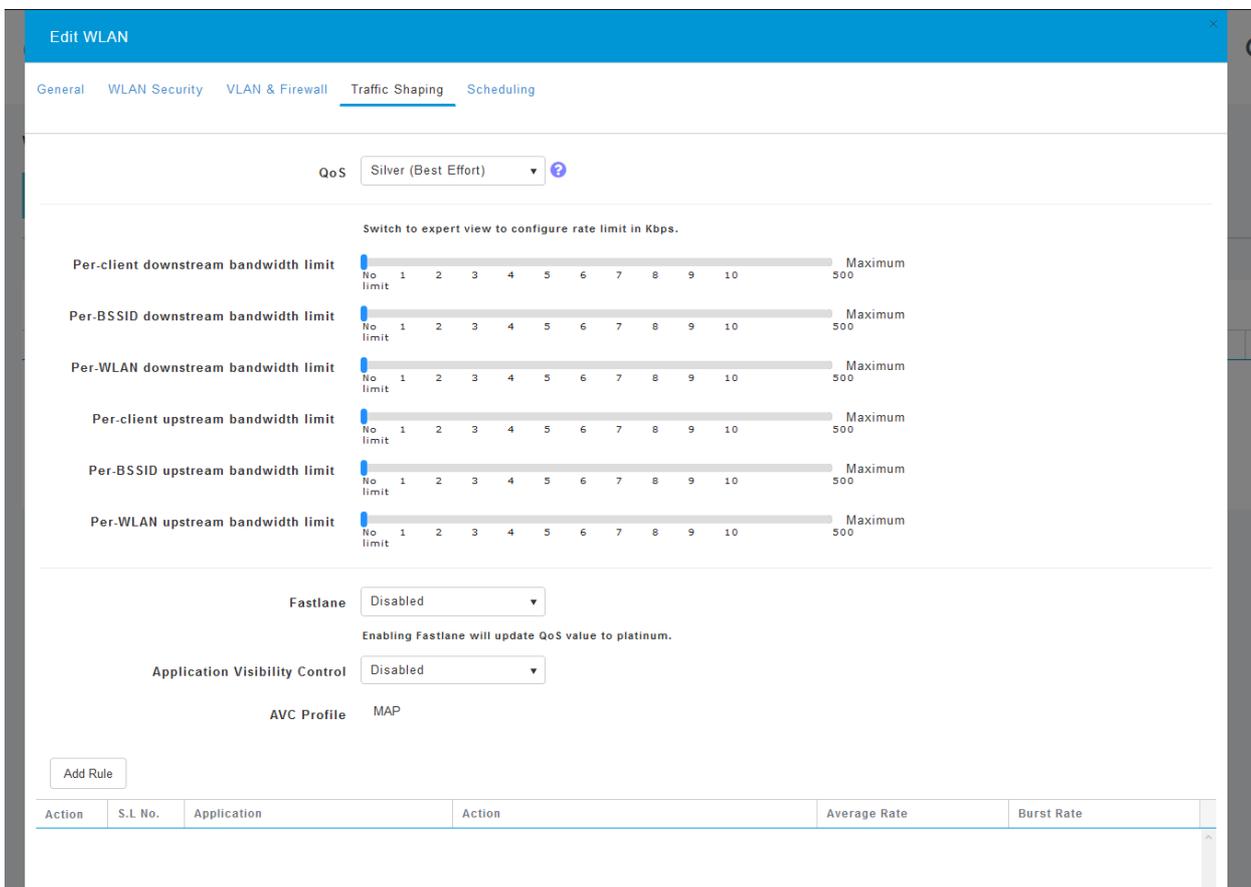
Apply Cancel

## Étape 5

Accédez à l'onglet **Formatage du trafic** en cliquant dessus.



Votre écran peut apparaître comme suit :



Étape 6

Vers le bas de la page, vous trouverez la fonction *Contrôle de visibilité des applications*. Ceci est désactivé par défaut. Cliquez sur la liste déroulante et sélectionnez **Enabled**.

Per-WLAN upstream bandwidth limit 

Fastlane    
 Enabling Fastlane will update QoS value to platinum.

Application Visibility Control  **1**

AVC Profile  **2**

Action	S.L No.	Application	Action	Average Rate
--------	---------	-------------	--------	--------------

## Étape 7

Cliquez sur le bouton **Apply (Appliquer)**.

Application Visibility Control

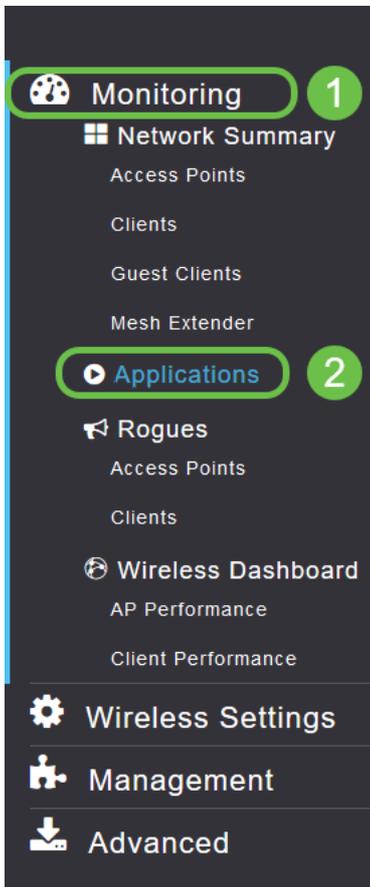
AVC Profile

Action	S.L No.	Application	Action	Average Rate	Burst Rate
--------	---------	-------------	--------	--------------	------------

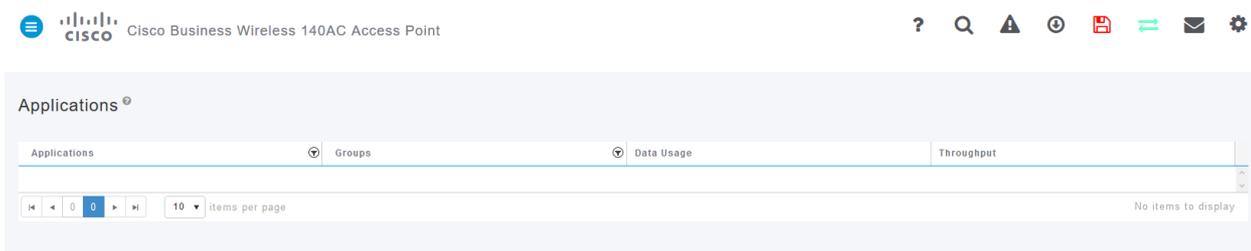
Ce paramètre doit être activé sinon la fonctionnalité ne fonctionnera pas.

## Étape 8

Après avoir cliqué sur Appliquer, **cliquez sur le bouton Annuler** pour fermer le sous-menu WLAN. Puis **cliquez sur le menu Surveillance** dans la barre de menus de gauche. Une fois que vous êtes en mesure de le faire, cliquez sur l'élément de menu Application.



Si vous n'avez eu aucun trafic vers une source quelconque, votre page sera vide comme suit :



Cette page affiche les informations suivantes :

Application : inclut de nombreux types différents

Groupes : indique le type de groupe d'applications pour faciliter le tri

Utilisation des données - Quantité de données utilisées par ce service dans son ensemble

Débit : quantité de bande passante utilisée par l'application

Vous pouvez cliquer sur les onglets pour trier de la plus grande à la plus petite, ce qui permet d'identifier les plus grands consommateurs de ressources réseau.

Cette fonctionnalité est très puissante pour gérer vos ressources WLAN de manière granulaire. Voici quelques-uns des groupes et types d'applications les plus courants. Il est probable que votre liste en contienne beaucoup plus. Y compris les éléments suivants :

## Groupes et exemples

Navigation

EX : Spécifique au client, SSL

Courriel

EX : Outlook, Secure-pop3

Voix et vidéo

EX : WebEx, Cisco Spark,

Outils d'entreprise et de productivité

EX : Microsoft Office 365,

Sauvegarde et stockage

EX : Windows-Azure,

Internet grand public

iCloud, Google Drive

Réseaux sociaux

EX : Twitter, Facebook

Software Updates

EX : Google-Play, IOS

Messagerie instantanée

EX : Raccrochements, messages

Voici à quoi ressemblera la page lorsqu'elle sera remplie :

Cisco Business Wireless 145AC Access Point

Applications

Applications	Groups	Data Usage	Throughput
ssl	browsing	2.6 MB	1.1 Mbps
outlook-web-service	email	819.4 KB	233.1 kbps
cisco-spark	voice-and-video	735.6 KB	0.0 bps
secure-pop3	email	453.1 KB	0.0 bps
ms-office-365	business-and-productivity-tools	238.2 KB	75.1 kbps
webex-meeting	voice-and-video	132.3 KB	0.0 bps
samsung	browsing	79.4 KB	0.0 bps
windows-azure	backup-and-storage	74.0 KB	5.7 kbps
twitter	social-networking	48.6 KB	0.0 bps
icloud	consumer-internet	47.3 KB	0.0 bps

10 items per page 1 - 10 of 28 items

Chaque en-tête de table est cliquable pour le tri, particulièrement utile pour les champs *Utilisation des données* et *Débit*.

## Étape 9

Cliquez sur la ligne correspondant au type de trafic que vous souhaitez gérer.

Cisco Business Wireless 145AC Access Point

Applications

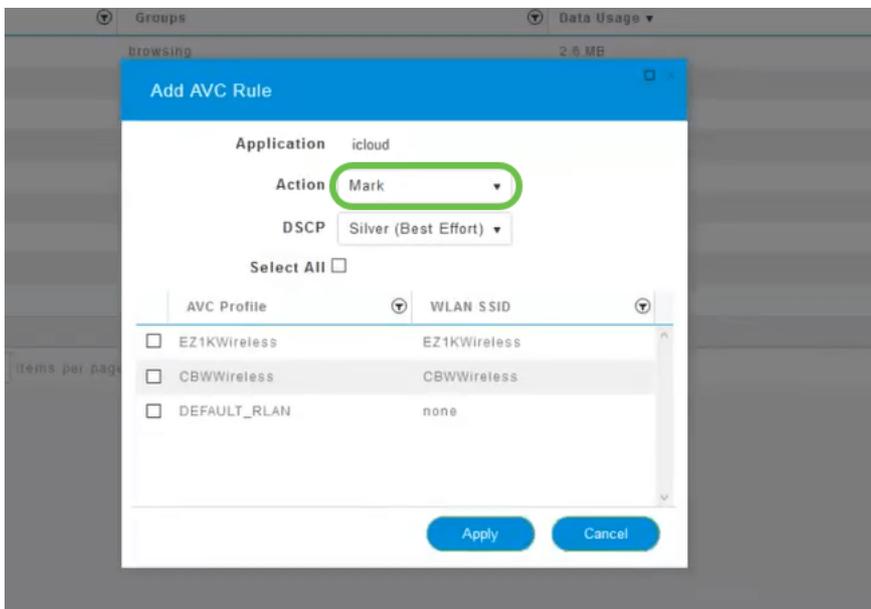
Applications	Groups	Data Usage	Throughput
ssl	browsing	2.6 MB	1.1 Mbps
outlook-web-service	email	819.4 KB	233.1 kbps
cisco-spark	voice-and-video	735.6 KB	0.0 bps
secure-pop3	email	453.1 KB	0.0 bps
ms-office-365	business-and-productivity-tools	238.2 KB	75.1 kbps
webex-meeting	voice-and-video	132.3 KB	0.0 bps
samsung	browsing	79.4 KB	0.0 bps
windows-azure	backup-and-storage	74.0 KB	5.7 kbps
twitter	social-networking	48.6 KB	0.0 bps
icloud	consumer-internet	47.3 KB	0.0 bps

10 items per page 1 - 10 of 28 items

Dans les captures d'écran, nous sommes passés à un périphérique qui a du trafic à gérer.

## Étape 10

Cliquez sur la liste déroulante Action pour sélectionner la manière dont vous traiterez ce type de trafic.



Pour les besoins de cet article, nous laissons cette option à Mark.

Mesures à prendre en matière de trafic

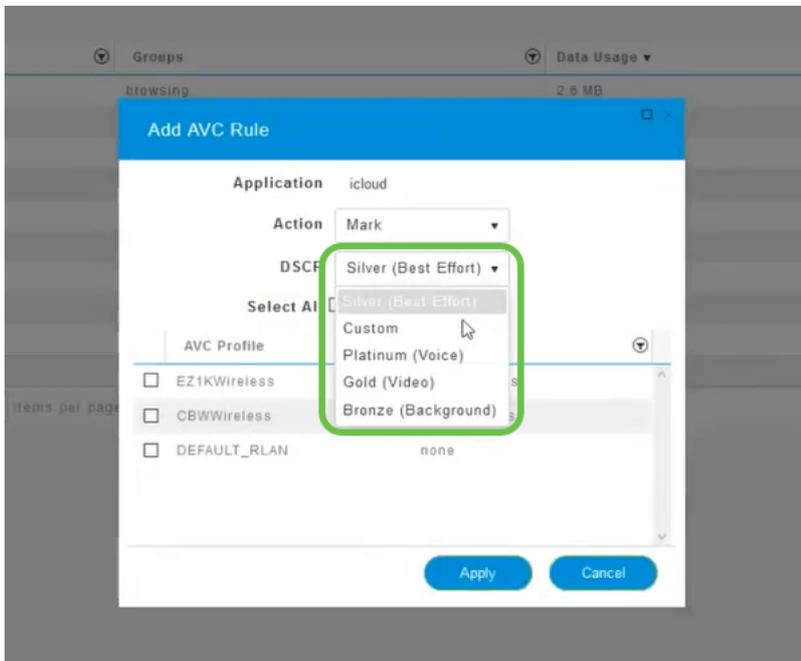
Marquer : place le type de trafic dans l'un des 3 niveaux DSCP (Differentiated Services Code Point), qui détermine le nombre de ressources disponibles pour le type d'application.

Déposer - Ne faites rien d'autre que rejeter le trafic

Limite de débit : permet de définir le taux moyen et le taux de rafale en Kbits/s.

## Étape 11

Cliquez maintenant sur la liste déroulante du champ DSCP pour sélectionner l'une des options suivantes.



Vous trouverez ci-dessous les options DSCP du trafic à marquer. Ces options passent d'une diminution des ressources à une augmentation des ressources disponibles pour le type de trafic que vous modifiez.

Bronze (arrière-plan) - Moins

Argent (au mieux)

Gold (vidéo)

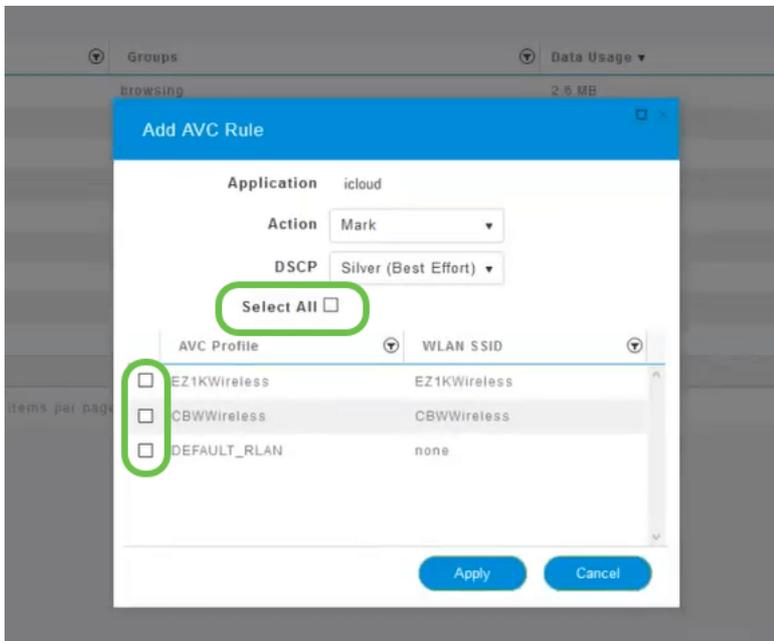
Platinum (voix) Plus

Personnalisé - Ensemble d'utilisateurs

En tant que convention Web, le trafic a migré vers la navigation SSL, ce qui vous empêche de voir ce qui se trouve à l'intérieur des paquets lorsqu'ils se déplacent de votre réseau vers le WAN. Ainsi, une grande majorité du trafic web pariera avec SSL. La définition du trafic SSL pour une priorité inférieure peut affecter votre navigation.

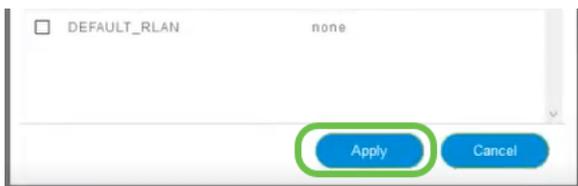
## Étape 12

Sélectionnez maintenant le **SSID individuel** que vous souhaitez exécuter. Vous pouvez également cliquer sur **Sélectionner tout**.



## Étape 13

Cliquez maintenant sur le bouton Appliquer pour commencer cette stratégie.



Arrondi en définissant deux cas d'utilisation de base :

Les invités/utilisateurs diffusent une grande quantité de trafic, empêchant ainsi le trafic critique de passer. Vous pouvez soit augmenter la priorité de la voix, soit diminuer la priorité du trafic Netflix pour améliorer les choses.

Le téléchargement de mises à jour logicielles de grande taille pendant les heures de bureau peut être déclassé ou limité.

## Conclusion

Vous l'avez fait. Le profilage des applications est un outil très puissant qui peut être activé en activant également le profilage des clients.

Si vous souhaitez en savoir plus sur les réseaux maillés sans fil, consultez l'un des articles suivants :

[Forum aux questions RADIUS](#) [Mise à niveau du micrologiciel RLAN](#) [Profilage des applications](#) [Profilage client](#) [Outils PA principaux](#) [Umbrella](#) [Utilisateurs WLAN](#) [Journalisation](#) [Modélisation du trafic](#) [Rogues](#) [Interféreurs](#) [Gestion de la configuration](#) [Mode de maillage de configuration de port](#) [Bienvenue dans CBW](#) [Mesh Networking](#) [Réseau invité à l'aide de l'authentification par e-mail et de la comptabilité RADIUS](#) [Dépannage](#) [Utilisation d'un routeur Draytek avec CBW](#)