



Cisco Mobility Express

Guide de démarrage rapide

Septembre 2017

AireOS 8.5



Cisco Aironet 1815 Series



Cisco Aironet 1830/1850 Series



Cisco Aironet 1540/1560 Series



Cisco Aironet 2800/3800 Series

Sommaire

1	Introduction	3
1.1	Démarrage	4
2	Première installation de Mobility Express	4
3	Enregistrer des APs additionnels sur Mobility Express	16
4	Optionnel : haute disponibilité et redondance	18
5	Référence : convertir un AP en Mobility Express	18
6	Ressources additionnelles	20

1 Introduction

Cisco Mobility Express est le nouveau mode de déploiement simplifié pour configurer et gérer centralement jusqu'à 50 ou 100 points d'accès (Access Points, AP) Wi-Fi sans besoin d'un contrôleur (WLC, Wireless LAN Controller) dédié.

Les gammes d'APs 1540/1560/1800/2800/3800 supportent les fonctions de contrôleur, qui permettent de déployer facilement un réseau Wi-Fi pour des petites et moyennes entreprises (PME), des agences, ou toute autre scénario nécessitant jusqu'à 50 ou 100 APs, un temps d'installation réduit, une configuration rapide et un management simplifié.

Un AP 1540, 1560, 1800, 2800 ou 3800 agit en tant que contrôleur virtuel pour la configuration et la supervision de tous les réseaux Wi-Fi d'un déploiement Mobility Express : un AP portant ce rôle est dit l'AP maître (**Master AP**).

La liste complète des modèles d'APs supportant le rôle de Master AP est la suivante : 1542, 1562, 1815i, 1815w, 1832, 1852, 2802 et 3802.

Les APs des gammes 1540 et 1800 portant le rôle de Master AP supportent jusqu'à 50 APs enregistrés (en incluant l'AP embarqué dans le Master AP) ; les APs des gammes 1560, 2800 et 3800 portant le rôle de Master AP supportent jusqu'à 100 APs enregistrés (en incluant l'AP embarqué dans le Master AP). La limite du nombre d'APs enregistrés (50 ou 100) dépend à tout moment du modèle d'AP portant le rôle de Master AP.

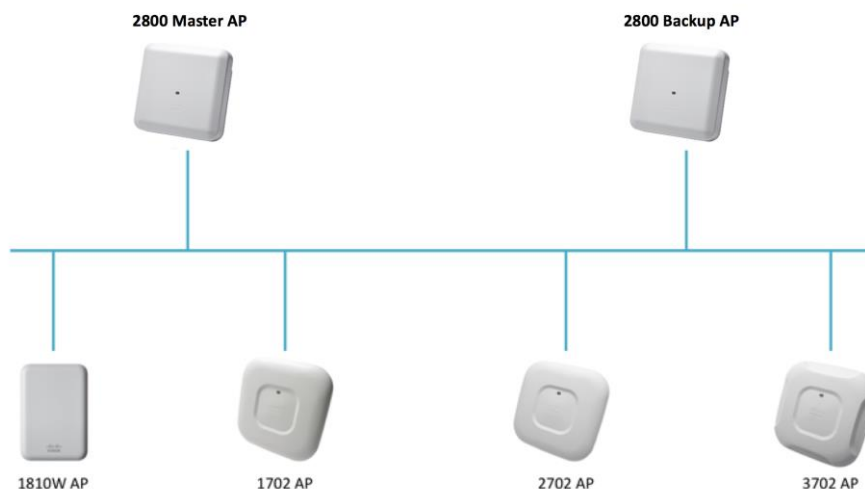
Note : l'AP 1810 ne supporte pas le rôle de Master AP, mais peut être enregistré à un déploiement Mobility Express comme tout autre AP standard.

Le Master AP est le point central de configuration et management pour tous les autres APs enregistrés au Master AP.

Un seul AP 1540/1560/1800/2800/3800 à la fois porte le rôle de Master AP à un instant donné dans le même sous-réseau ou VLAN. Dans le cas d'un Master AP déjà déployé, tout autre nouvel AP essaiera de rejoindre le Master AP et de se synchroniser en VRRP pour un éventuel backup (cf. aussi [Optionnel : haute disponibilité et redondance](#)). Dans le cas de plusieurs APs en train de démarrer pour la première fois, un processus d'élection du Master AP aura lieu, toujours à travers du VRRP, qui désignera un seul Master AP. Pour plus de détails sur cette procédure, n'hésitez pas à consulter le chapitre dédié dans le guide de déploiement officiel :

[Master AP Failover and Electing a new Master](#)

Les points d'accès d'autres gammes (700, 1600, 1700, 2600, 2700, 3600, 3700 et 1810) peuvent s'enregistrer à un Master AP de la gamme 1540/1560/1800/2800/3800, mais ces autres modèles ne supportent pas le rôle de Master AP eux-mêmes.



Pour toute tâche de configuration et supervision le Master AP communique avec les autres APs du même déploiement Mobility Express à travers un tunnel de contrôle basé sur le protocole standard CAPWAP (Control And Provisioning of Wireless Access Points, RFC 5415 et 5416).

Le flux de données des clients Wi-Fi est commuté localement, sur chaque port du switch où chaque AP est branché, sans remonter en central à travers le Master AP. Ce comportement est similaire à la commutation locale avec le mode Cisco FlexConnect quand on déploie un WLC dédié.

Le Master AP est également le point de contact pour toute autre ressource externe Cisco et non Cisco, comme par exemple Cisco Prime Infrastructure, Cisco Identity Services Engine (ISE) ou tout autre serveur RADIUS, Cisco Connected Mobile Experiences (CMX), de serveurs SYSLOG ou SNMP, etc. Les autres APs du déploiement Mobility Express ne requièrent pas une communication directe avec ces ressources externes.

1.1 Démarrage

Un AP 1540/1560/1800/2800/3800 peut être commandé avec le mode Mobility Express déjà activé dans son image préinstallée. La référence (SKU, stock keeping unit) à choisir lors de la commande est celle se terminant avec **K9C**, le **C** étant l'option **configurable**.

Par exemple, pour commander un AP 2802 avec antenne intégrées pour le domaine radio **-E** (ETSI, European Telecommunications Standards Institute), il faut choisir la référence **AIR-AP2802-I-E-K9C**.

Dans les options for Software, il faut vérifier que la référence **SW2802-MECPWP-K9** pour "Cisco 2800 Series Mobility Express software image" soit également sélectionnée. Cela devrait être en tout cas l'option par défaut pour les références K9C.

Si un nouvel AP configuré avec les paramètres d'usine se connecte à un réseau sans Master AP ou WLC, alors il dessert automatiquement un réseau Wi-Fi (SSID, Service Set Identifier) appelé **CiscoAirProvision** (cf. le chapitre suivant pour plus de détails).

Pour changer le mode opérationnel d'un AP 1540/1560/1800/2800/3800 de CAPWAP à Mobility Express, si précédemment enregistré à un autre WLC ou commandé avec une référence ne se terminant pas par **K9C** par exemple, veuillez-vous refaire à la [Référence : convertir un AP en Mobility Express](#) à la fin de ce guide.

2 Première installation de Mobility Express

Le premier équipement à déployer dans la solution Mobility Express est le Master AP. Une fois le Master AP opérationnel, vous pouvez éteindre votre réseau Wi-Fi en enregistrant automatiquement des APs additionnels.

Un AP 1540/1560/1800/2800/3800, avec la référence K9C ou converti de CAPWAP à Mobility Express, démarre avec les paramètres d'usine, prêt pour être configuré en tant que Master AP.

La procédure suivante décrit les phases et les recommandations pour déployer Mobility Express en 10 étapes.

Les exemples et les captures d'écrans de ce guide sont pris d'un AP 1832, mais les mêmes instructions s'appliquent à tout autre AP 1540/1560/1800/2800/3800 (sauf la série 1810, qui ne supporte pas le rôle de Master AP).

1. Avant de brancher le futur Master AP sur un switch on vous recommande de préconfigurer le port du switch en mode trunk.
Le Master AP, ou tout autre AP de la solution Mobility Express, obtient son adresse IP de management dans le VLAN natif du port trunk. Un port trunk vous permet également de commuter le flux de données des clients Wi-Fi sur d'autres VLANs du trunk, pour éventuellement séparer le trafic de management du flux de données des clients.

Si vous ne pouvez ou ne voulez pas configurer le port du switch en mode trunk et préférez le garder en mode *access*, le trafic de management sera commuté sur le VLAN d'accès, ainsi que le flux de données des clients Wi-Fi.

L'exemple suivant montre la configuration d'un port en mode trunk pour un switch Cisco :

```
interface GigabitEthernet0/3
  description --- MASTER_AP ---
  switchport trunk native vlan 10
  switchport trunk allowed vlan 10,20,30,40
  switchport mode trunk
  spanning-tree portfast trunk
```

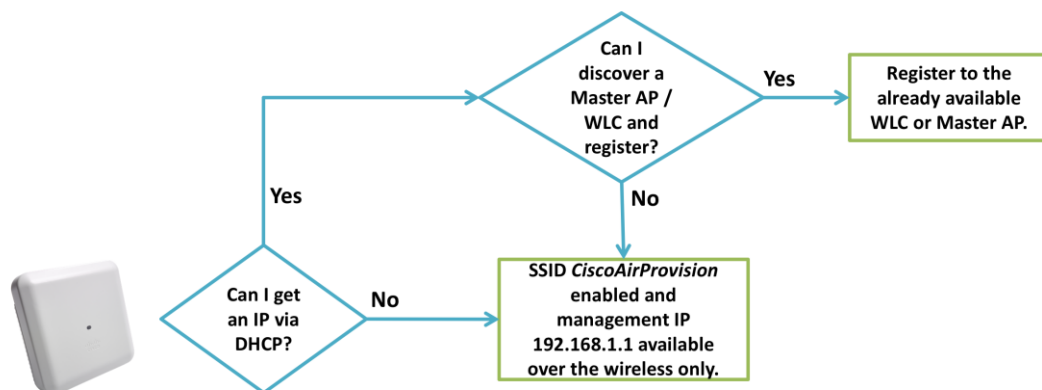
Dans cet exemple le trafic de management est commuté sur le VLAN natif 10 et tout autre flux de données des clients peut être commuté sur le VLAN natif 10 ou sur tout autre VLAN marqué permis dans le trunk (20, 30 ou 40).

2. Connectez maintenant le futur Master AP au port du switch et, si le switch ne supporte pas de PoE (Power over Ethernet) ou PoE+, alimentez-le à travers son alimentateur ou un *power injector*.

L'AP essaie d'obtenir une adresse IP par DHCP en premier. Si cette phase réussit, il essaie ensuite de découvrir un Master AP ou un WLC potentiellement déjà présent dans le même VLAN natif du port trunk.

Si aucun Master AP n'est disponible, l'AP s'autoproclame Master AP et commence à desservir le SSID *CiscoAirProvision*.

Si l'AP ne peut pas obtenir une IP par DHCP, il active l'interface graphique pour l'installation initiale sur l'IP de management 192.168.1.1 (disponible en Wi-Fi uniquement), puis il s'autoproclame Master AP et commence à desservir le SSID *CiscoAirProvision*.



3. Attendez que l'AP complète le processus de démarrage et connectez-vous au SSID *CiscoAirProvision* aussitôt qu'il sera desservi.

Le SSID *CiscoAirProvision* est sécurisé en WPA2 et son mot de passe est « **password** ».

Une fois le mot de passe rentré et la connexion au SSID *CiscoAirProvision* terminée, votre machine devrait obtenir une adresse IP dans le réseau 192.168.1.x/24 : parmi les phases de la première configuration, l'AP 2800 aura également activé un serveur DHCP interne.

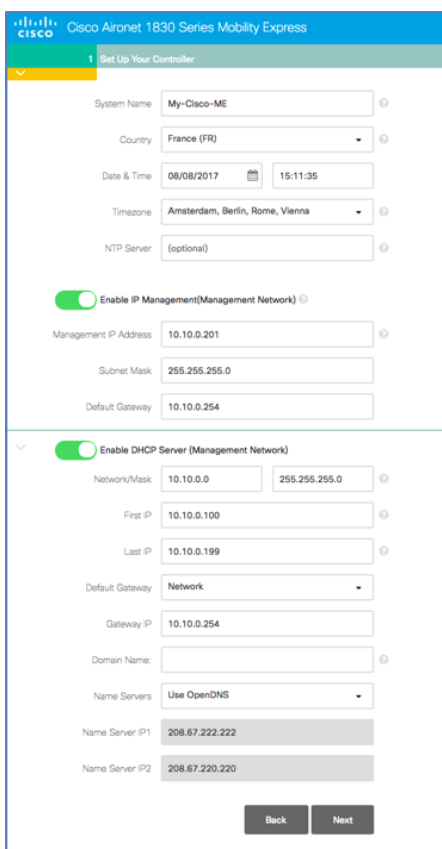
Vous pouvez maintenant lancer un navigateur et essayer d'ouvrir une page web. Vous serez automatiquement redirigé(e) vers l'URL <http://mobilityexpress.cisco/screens/day0-config.html>

Si vous n'êtes pas redirigé(e) automatiquement (parfois les navigateurs gardent des sites en cache ou n'acceptent pas des certificats non vérifiés), vous pouvez toujours ouvrir directement l'URL suivante : <http://192.168.1.1>

A partir de la version 8.5 est accessible également avec l'URL <http://mobilityexpress.cisco> (on recommande **Google Chrome** comme navigateur web pour de meilleures performances)



4. Configurez votre compte administrateur en spécifiant un identifiant de votre choix, normalement « admin », et en précisant votre mot de passe deux fois pour confirmation. Préférez un mot de passe non conventionnel, à sécurité avancée. Vous accéderez ensuite à la première section de configuration des propriétés du système du Master AP.



On vous demandera de configurer le nom du système et un serveur NTP (Network Time Protocol) optionnel. Vous pouvez également garder la date et l'heure automatiquement suggérées par le processus automatique d'installation : elles ont été prises directement du navigateur web depuis lequel vous êtes en train de configurer la solution Mobility Express.

L'adresse IP de management devrait être une IP dans le VLAN natif du port trunk où l'AP est branché, ou en alternative dans le VLAN d'accès dans le cas d'un port access (cf. 1er point). Il est recommandé de réserver cette IP dans le pool du serveur DHCP du VLAN de management, si présent, pour qu'aucun autre équipement essaie d'obtenir la même IP en causant de potentiels problèmes d'adresse dupliquée.

A partir de la version 8.3, Mobility Express supporte un serveur DHCP interne pour le réseau de management, grâce auquel les autres APs peuvent obtenir une adresse IP pour s'enregistrer au Master AP. Les serveurs DNS configurés dans le pool DHCP intègrent la solution [OpenDNS](#), mais peuvent également être configurés manuellement.

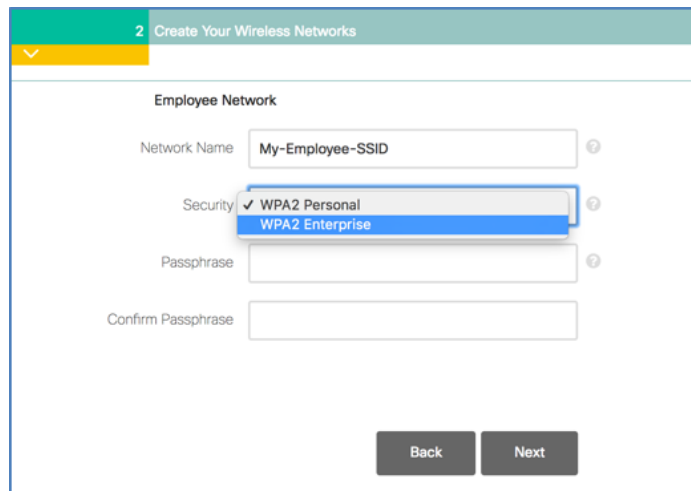
Note : un mix de pools DHCP internes dans Mobility Express et de pools d'un serveur DHCP externe n'est pas supporté pour le moment. Si vous configurez un pool DHCP interne pour le réseau de management, vous devez continuer à utiliser des pools DHCP internes pour vos SSIDs aussi (cf. prochaines étapes).

5. Une fois les propriétés du système paramétrées, cliquez sur le bouton **Next** et vous accédez à la page de configuration de votre premier SSID, ou WLAN (Wireless Local Area Network).

Choisissez d'abord le **Network Name**, qui sera le nom du SSID que vous verrez sur le Wi-Fi. Cela devrait être le SSID pour vos employés et son niveau de sécurité devrait être réglé pour du WPA2.

WPA2 Personal vous permet de choisir un mot de passe commun, que tous vos employés devront utiliser pour se connecter à ce SSID.

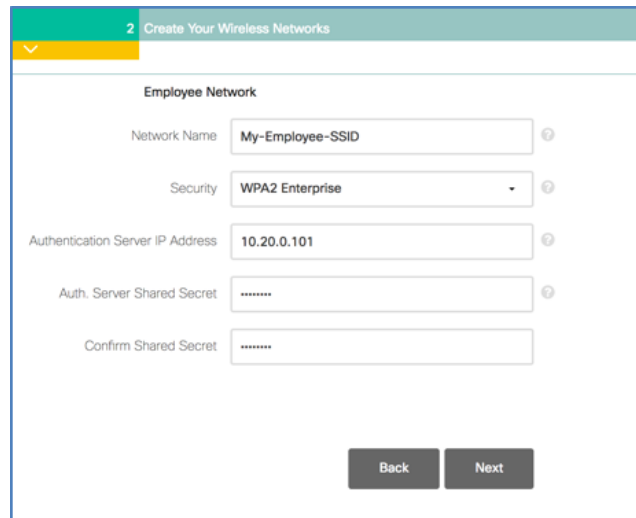
WPA2 Enterprise vous permet de préciser un serveur RADIUS externe pour authentifier vos employés en 802.1X avec leurs identifiants Active Directory, par exemple, ou par certificats, si ces méthodes sont supportées et configurées dans leurs machines et dans le serveur RADIUS. WPA2 Enterprise est la méthode de connexion la plus sécurisée.



The screenshot shows a web interface for configuring a wireless network. The title is "2 Create Your Wireless Networks". Below the title, there is a dropdown menu showing "Employee Network". The main form has the following fields:

- Network Name: My-Employee-SSID
- Security: WPA2 Personal (selected), WPA2 Enterprise
- Passphrase: (empty)
- Confirm Passphrase: (empty)

At the bottom of the form, there are two buttons: "Back" and "Next".



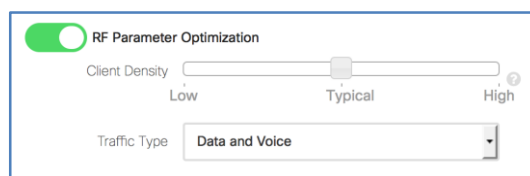
Depuis la version AireOS 8.5 la procédure initiale d'installation n'inclut plus la configuration d'un VLAN et d'un pool DHCP dédié pour le réseau employé : ce SSID sera associé par défaut au réseau de management, dans le VLAN natif du trunk ou dans le VLAN d'accès du port du switch.

Ces paramètres peuvent être modifiés dans une deuxième phase et un exemple est fourni au point 9.

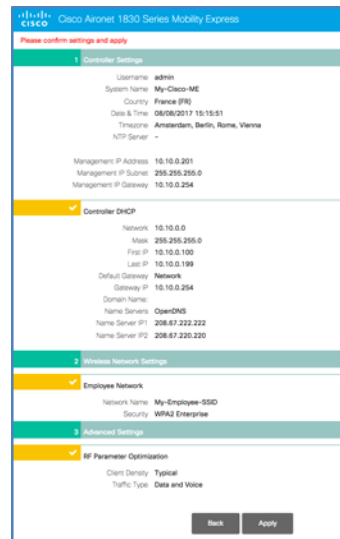
6. Cliquez sur **Next** pour continuer vers la troisième et dernière section. Ici vous pouvez optimiser les réglages radio selon votre environnement en activant les options **RF Parameter Optimization**.



Précisez le type d'usage de votre réseau Wi-Fi, en choisissant parmi différents niveaux de densité des clients (low, typical, high) et différents types de trafic prévus sur le réseau Wi-Fi (data, data and voice). Une faible densité (« Low ») optimisera le réseau pour la couverture, alors qu'une haute densité (« High ») l'optimisera pour la capacité à supporter plusieurs utilisateurs et terminaux. Des réglages utilisés souvent pour l'optimisation radio sont **Typical** pour la densité des clients et **Data and Voice** pour le type de trafic.



7. Pour terminer l'installation, cliquez sur **Next**, confirmez votre configuration, puis cliquez sur **Apply** et acceptez tout éventuel message de redémarrage. Le Master AP redémarrera avec la nouvelle configuration et commencera à desservir le SSID pour les employés configuré à l'étape 5. Le SSID *CiscoAirProvision* pour la configuration initiale ne sera plus desservi.

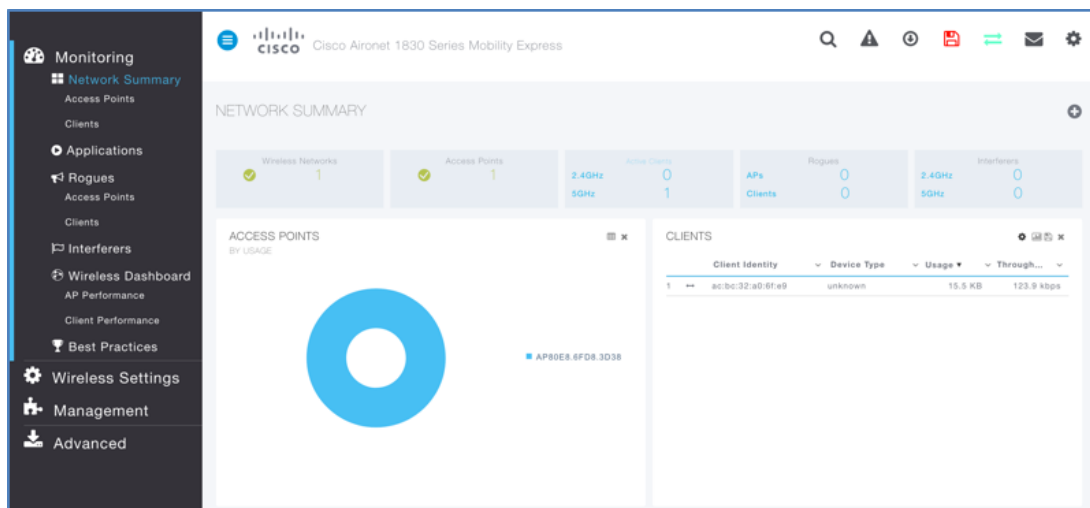


8. Cisco Mobility Express est maintenant opérationnel et vous devriez voir les SSID pour les employés configuré à l'étape 5. Pour vous connecter à l'interface graphique du Mobility Express, branchez votre machine sur le réseau filaire et ouvrez l'URL suivant dans votre navigateur : ***https://<Mobility-Express-Mgmt-IP>***

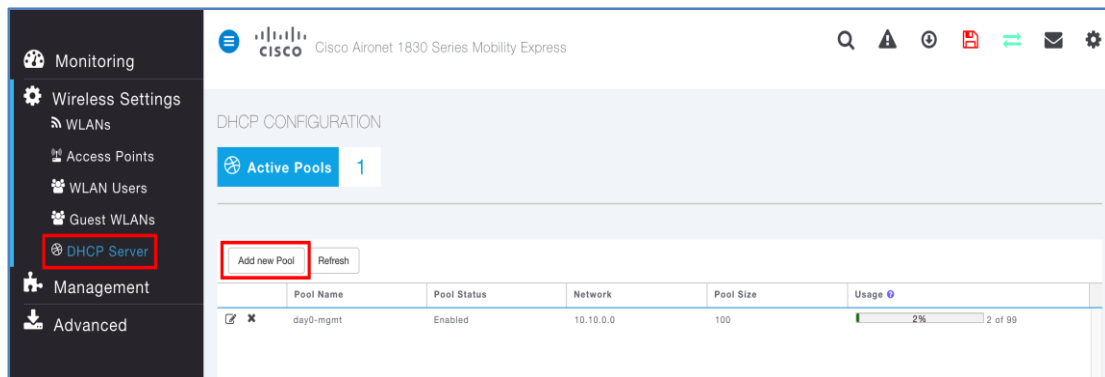
<Mobility-Express-Mgmt-IP> est l'adresse IP de management dans le VLAN natif du port trunk que vous avez configurée à l'étape 4.

En se connectant sur cette IP en HTTPS, il est attendu de recevoir une notification dans votre navigateur sur le certificat : veuillez l'ignorer et continuer vers la page de login.

La page de login vous demandera l'identifiant et mot de passe administrateur configurés à l'étape 3.

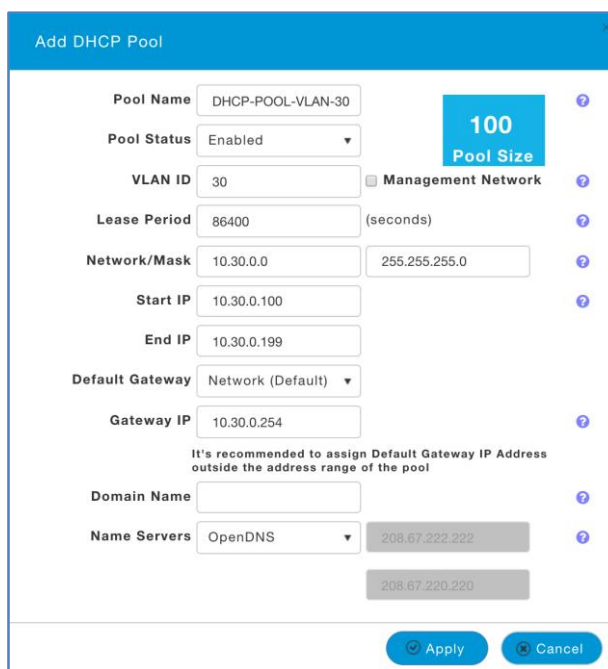


9. Vous pouvez maintenant naviguer vers la page ***Wireless Settings > DHCP Server*** et cliquer sur le bouton ***Add new Pool*** pour créer un nouveau pool DHCP en plus que celui généré par la procédure initiale de configuration dans le VLAN de management, appelé « *day0-mgmt* ».

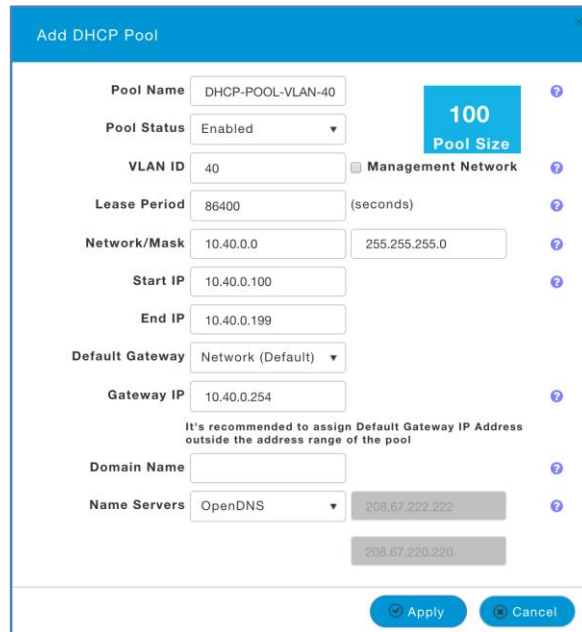


Dans l'exemple suivant, nous avons créé un nouveau pool DHCP dans le VLAN 30, où le SSID des employés sera commuté.

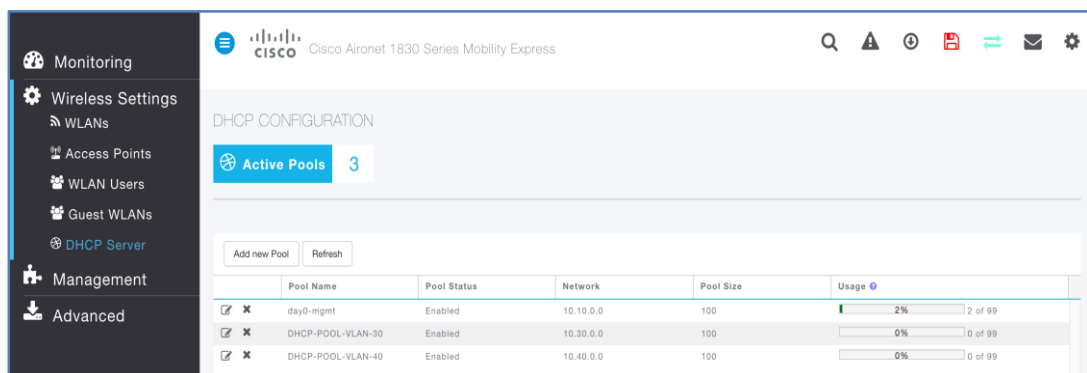
Note : un mix de pools DHCP internes dans Mobility Express et de pools d'un serveur DHCP externe n'est pas supporté pour le moment. Si vous configurez un pool DHCP interne pour le réseau de management, vous devez continuer à utiliser des pools DHCP internes pour vos SSIDs aussi (cf. prochaines étapes).



De la même manière, nous pouvons également créer un autre pool pour le réseau invité dans son VLAN dédié (VLAN 40 dans l'exemple), que l'on utilisera à l'étape 10 pour le SSID invité.

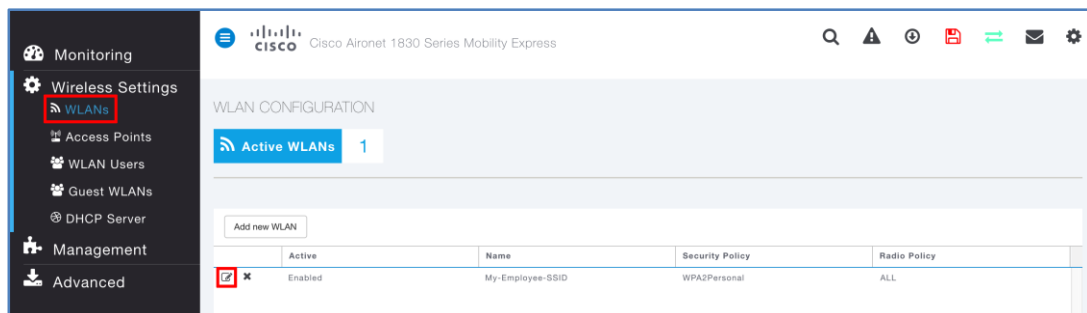


Les pools DHCP créés sont visibles dans la liste sous **Wireless Settings > DHCP Server**.



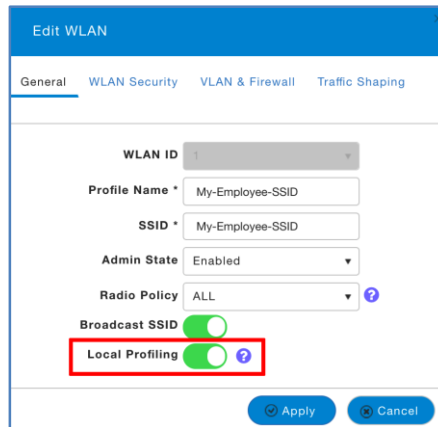
	Pool Name	Pool Status	Network	Pool Size	Usage
<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	day0-mgmt	Enabled	10.10.0.0	100	2% 2 of 99
<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	DHCP-POOL-VLAN-30	Enabled	10.30.0.0	100	0% 0 of 99
<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	DHCP-POOL-VLAN-40	Enabled	10.40.0.0	100	0% 0 of 99

Vous pouvez maintenant naviguer dans **Wireless Settings > WLANs** et cliquer sur l'icône pour modifier la configuration du réseau employé, juste à côté du SSID correspondant.



	Active	Name	Security Policy	Radio Policy
<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	Enabled	My-Employee-SSID	WPA2Personal	ALL

Parmi les paramètres recommandés, nous suggérons d'activer l'option **Local Profiling** dans l'onglet General, pour avoir plus de visibilité sur les profils des terminaux connectés à votre déploiement Mobility Express.



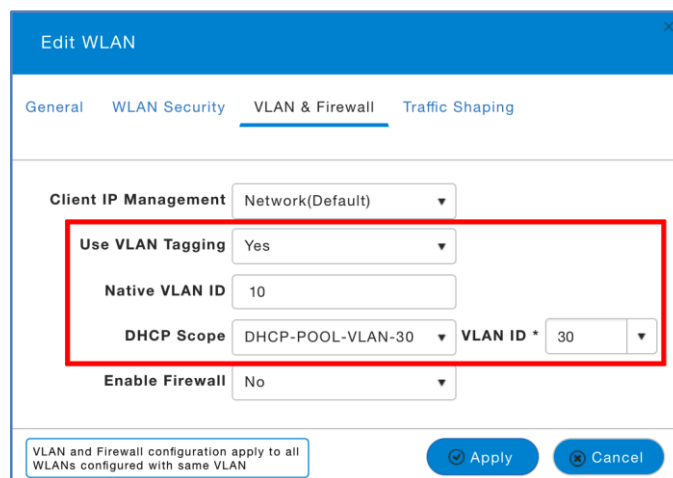
The screenshot shows the 'Edit WLAN' configuration window with the 'General' tab selected. The configuration includes:

- WLAN ID: 1
- Profile Name: My-Employee-SSID
- SSID: My-Employee-SSID
- Admin State: Enabled
- Radio Policy: ALL
- Broadcast SSID:
- Local Profiling: (highlighted with a red box)

 At the bottom, there are 'Apply' and 'Cancel' buttons.

Dans l'onglet **VLAN & Firewall** vous pouvez associer le pool DHCP que vous venez de créer au SSID employé.

Modifiez l'option **Use VLAN Tagging** en **Yes**, spécifiez un **Native VLAN ID** consistant avec la configuration du trunk du port du switch (VLAN 10 dans les exemples de ce guide) et sélectionnez dans le menu **DHCP Scope** le nom du pool DHCP créé précédemment. Le champ du **VLAN ID** correspondant sera automatiquement rempli avec la valeur configurée pour le pool DHCP.

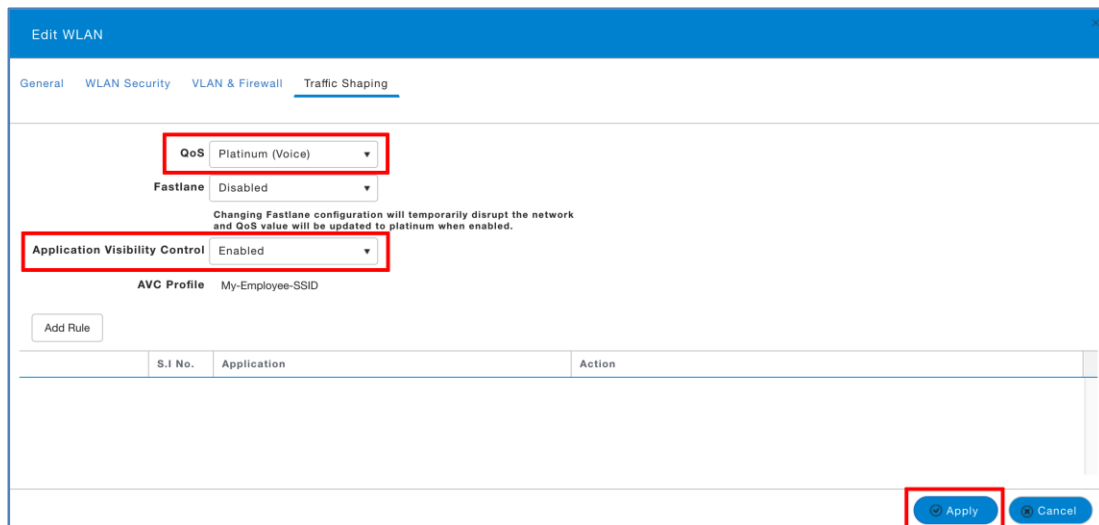


The screenshot shows the 'Edit WLAN' configuration window with the 'VLAN & Firewall' tab selected. The configuration includes:

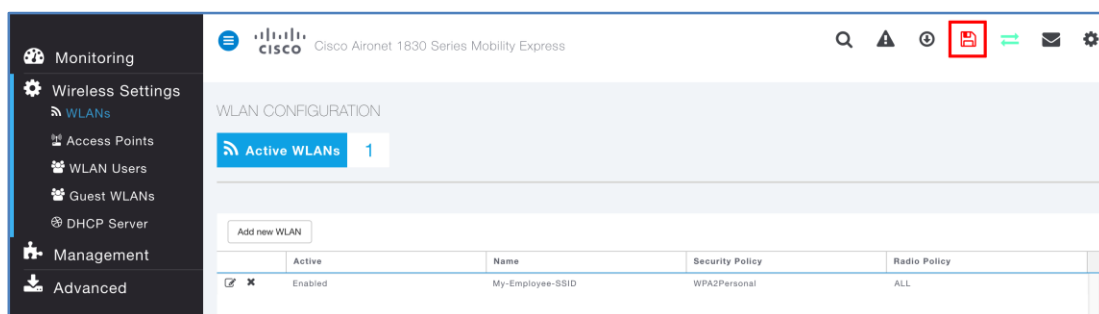
- Client IP Management: Network(Default)
- Use VLAN Tagging: Yes (highlighted with a red box)
- Native VLAN ID: 10 (highlighted with a red box)
- DHCP Scope: DHCP-POOL-VLAN-30 (highlighted with a red box)
- VLAN ID: 30 (highlighted with a red box)
- Enable Firewall: No

 At the bottom, there is a note: 'VLAN and Firewall configuration apply to all WLANs configured with same VLAN' and 'Apply' and 'Cancel' buttons.

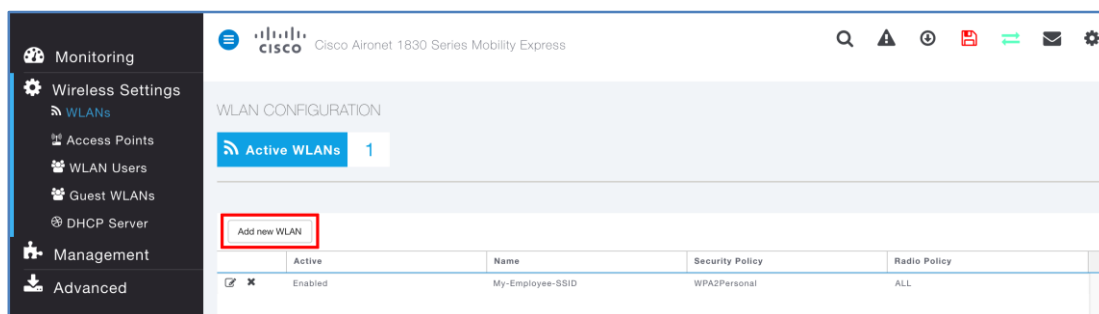
Une autre recommandation pour améliorer le niveau de visibilité et des statistiques de votre SSID serait d'activer la fonction **Application Visibility Control** dans l'onglet Traffic Shaping. Même si pas obligatoire, vous pouvez également changer le profil **QoS** avec **Platinum (Voice)** si vous souhaitez supporter des applications Voice over WLAN (VoWLAN).



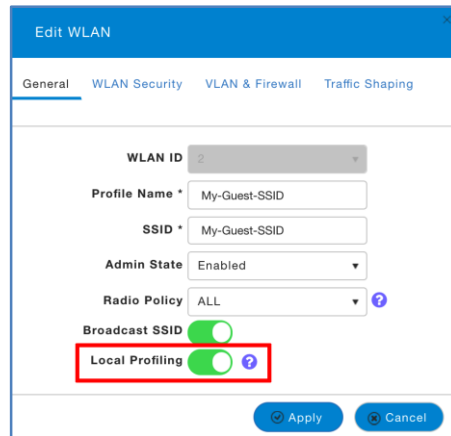
Après avoir complété ces étapes, veuillez cliquer sur le bouton **Apply** en bas à droite de la fenêtre, ainsi que sur l'icône pour sauvegarder la configuration en haut à droite de l'interface graphique de Mobility Express.



- Comme dernier point, vous pouvez aussi ajouter la configuration d'un réseau invité. Dans le menu **Wireless Settings > WLANs** cliquez sur le bouton **Add new WLAN** et spécifiez le nom de votre réseau invité.



Comme pour le SSID employé, nous recommandons d'activer l'option **Local Profiling** pour plus de visibilité sur les profils des terminaux connectés à votre réseau.



WLAN ID: 2

Profile Name: My-Guest-SSID

SSID: My-Guest-SSID

Admin State: Enabled

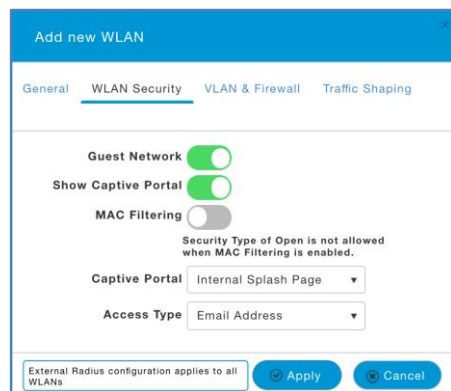
Radio Policy: ALL

Broadcast SSID:

Local Profiling:

Buttons: Apply, Cancel

Dans l'onglet **WLAN Security** activez l'option **Guest Network**. Pour une question de simplicité et si vous n'avez pas déployé un portail captive externe, vous pouvez garder l'option **Captive Portal** configurée avec **Internal Splash Page** et **Access Type** configuré avec **Email Address**. Les utilisateurs invités seront ainsi redirigés vers une page où ils pourront rentrer leur adresse mail avant d'avoir accès au réseau. Cette technique fournira une visibilité additionnelle grâce au fait que les adresses mail des visiteurs seront disponibles dans la liste des connexions des clients, dans l'interface de Mobility Express.



Guest Network:

Show Captive Portal:

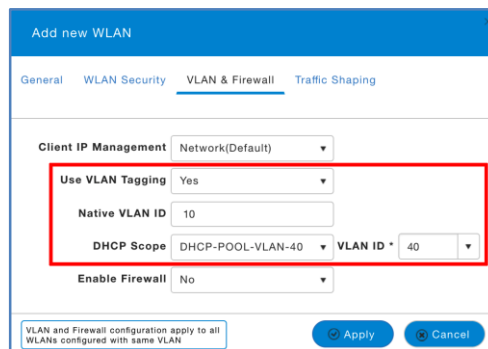
MAC Filtering:

Captive Portal: Internal Splash Page

Access Type: Email Address

Buttons: Apply, Cancel

Comme pour le SSID employé, dans l'onglet **VLAN & Firewall** vous pouvez modifier l'option **Use VLAN Tagging** en **Yes**, spécifier un **Native VLAN ID** consistant avec la configuration du trunk du port du switch (VLAN 10 dans les exemples de ce guide) et sélectionner dans le menu **DHCP Scope** le nom du pool DHCP créé précédemment. Le champ du **VLAN ID** correspondant sera automatiquement rempli avec la valeur configurée pour le pool DHCP.



Client IP Management: Network(Default)

Use VLAN Tagging: Yes

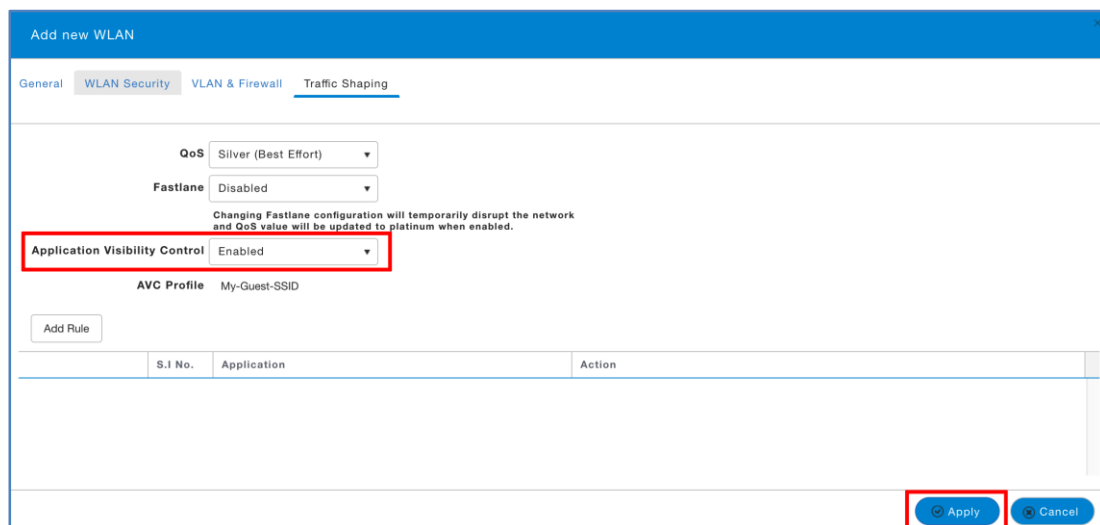
Native VLAN ID: 10

DHCP Scope: DHCP-POOL-VLAN-40 | VLAN ID: 40

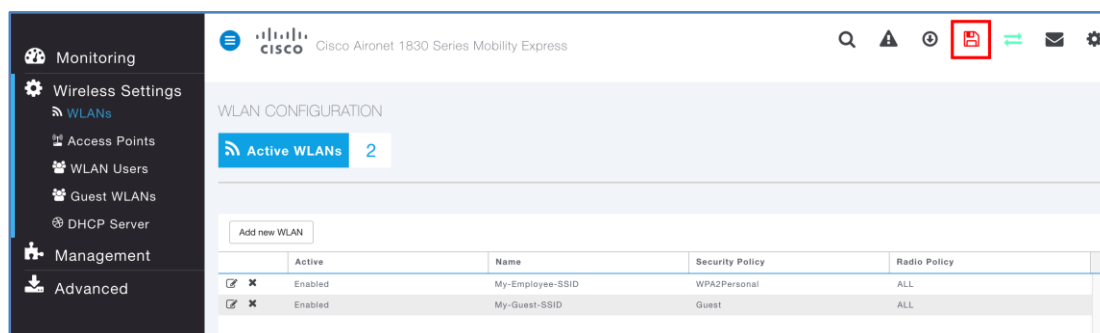
Enable Firewall: No

Buttons: Apply, Cancel

Une bonne pratique pour le SSID invité serait également d'activer la fonction **Application Visibility Control** dans l'onglet Traffic Shaping, pour bénéficier d'un niveau de visibilité applicative et de statistiques plus complètes.
 Pour les réseaux invité vous pouvez garder le profil **QoS** en **Silver (Best Effort)**.



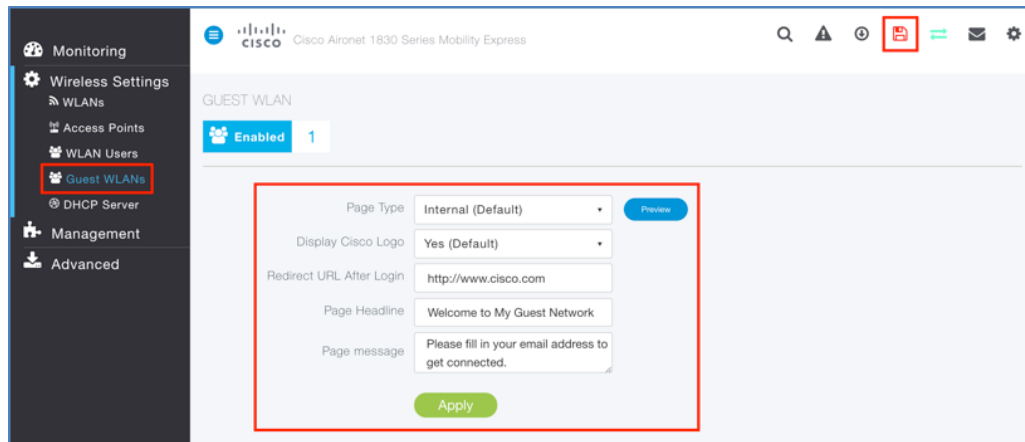
Après avoir complété ces étapes, veuillez cliquer sur le bouton **Apply** en bas à droite de la fenêtre, ainsi que sur l'icône pour sauvegarder la configuration en haut à droite de l'interface graphique de Mobility Express.



Vous pouvez également personnaliser le portail invité dans le menu **Wireless Settings > Guest WLANs**.

Par exemple, vous pouvez changer l'option **Display Cisco Logo**, saisir d'autres informations comme les **Page Headline** et **Page Message** pour guider vos visiteurs dans l'utilisation du portail et du réseau invité, ou encore télécharger votre portail personnalisé. Pour plus d'options sur la configuration et la personnalisation des réseaux invité, veuillez consulter les [Ressources additionnelles](#) à la fin de ce guide.
 Cliquez sur **Apply** pour confirmer toute modification.

Cliquez également sur **Save Configuration** en haut à droite de l'interface pour sauvegarder tous les derniers changements : votre solution Mobility Express est maintenant prêt pour le réseau de production. Félicitations !



3 Enregistrer des APs additionnels sur Mobility Express

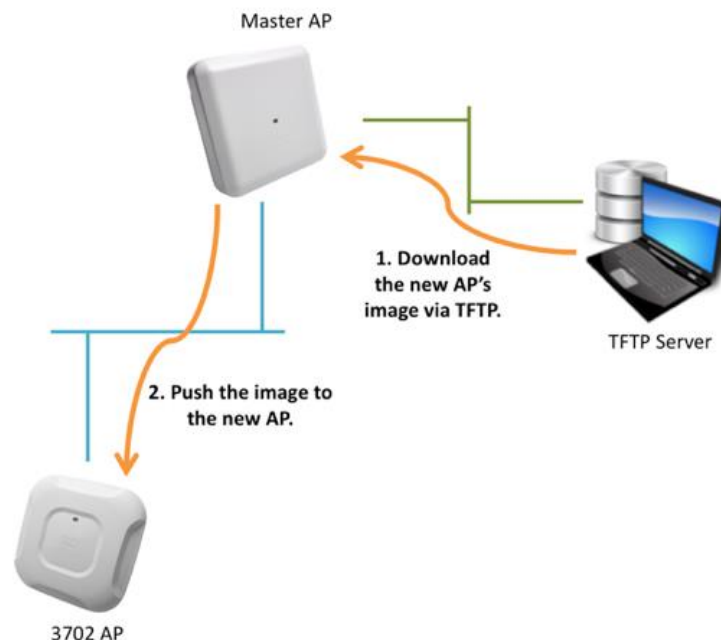
Des points d'accès (AP, Access Point) additionnels peuvent maintenant découvrir le Master AP du Cisco Mobility Express et s'y enregistrer.

Le processus de découverte est supporté à travers une requête broadcast sur le même réseau où l'AP obtient une adresse IP.

De nouveaux APs devront être connectés sur le même VLAN de management où vous avez connecté le Master AP (plus de détails dans les étapes suivantes).

La procédure suivante explique comment enregistrer de nouveaux APs.

1. Un nouvel AP s'enregistre au Master AP, s'il n'a pas déjà la même version de logiciel, doit télécharger la même version d'image que celle du Master AP.
Le Master AP ne stocke pas les images dans sa mémoire flash. Quand un nouvel AP doit mettre à jour son image, le Master AP télécharge d'abord l'image pour ce nouvel AP par TFTP et la provisionne ensuite au nouvel AP : ces deux tâches tournent en parallèle.



Pour cette raison la première étape pour enregistrer d'autres APs est de télécharger depuis Cisco.com le dossier contenant les images que le Master AP obtiendra par TFTP et poussera vers les autres APs du déploiement Mobility Express.

Par exemple, pour un AP 1830 dans le rôle de Master AP, téléchargez depuis Cisco.com le fichier *AIR-AP1830-K9-ME-8-5-103-0.zip* et stockez-le dans un serveur TFTP, par exemple Tftpd32, tournant dans une machine joignable depuis le Master AP.

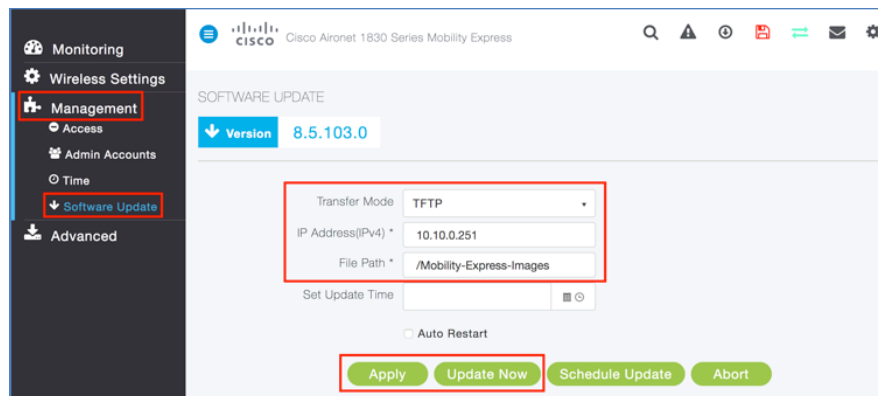
Ce fichier comprimé contient des images d'AP appelées *ap1g1*, *ap1g2*, *ap1g3*, etc. Décompressez le contenu de ce fichier dans un dossier, depuis lequel le Master AP pourra télécharger ces images par TFTP.

2. Accédez à l'interface de management du Mobility Express sur le Master AP et naviguez dans le menu **Management > Software Update**.

Dans ce menu, configurez l'adresse IP de la machine où le serveur TFTP évoqué dans l'étape précédent est en train de tourner.

Veuillez également préciser le parcours du dossier où vous avez décompressé les images Mobility Express pour d'autres APs.

Cliquez sur **Apply** pour appliquer ces paramètres et sur **Update Now** si vous souhaitez initier une mise à jour de Mobility Express (pour toute éventuelle nouvelle version).



Dans l'exemple de cette capture d'écran le serveur TFTP tourne sur un PC avec Tftpd32 installé et ayant l'adresse IP 10.10.0.251.

L'option *Current Directory* configurée dans Tftpd32 est un dossier générique (par exemple, le Bureau du PC) contenant le sous-dossier appelé *Mobility-Express-Images*, où le contenu du fichier *AIR-AP1830-K9-ME-8-5-103-0.zip* avait été décompressé.

Cela est la raison pour laquelle nous avons configuré */Mobility-Express-Images* dans l'option *File Path* du même exemple ci-dessus.

A partir de la version 8.3, si le Master AP peut joindre Cisco.com, vous pouvez également pousser les mises à jour directement de Cisco.com vers tous les APs 1800/2800/3800 du même déploiement Mobility Express dans l'option *Transfer Mode* (pour les gammes d'APs 1540/1560 vous devriez utiliser la version 8.5). Pour supporter les mises à jour depuis Cisco.com tout AP portant le rôle de Master AP doit être lié à un contrat de support SmartNet.

Tout autre modèle d'AP, si présent, devra toujours être mis à jour par TFTP.

3. Vous pouvez maintenant connecter des nouveaux APs dans le même VLAN de management que celui où vous avez configuré l'adresse IP de management du Master AP (cf. étape 4 du chapitre précédent). La requête broadcast permettra à un nouvel AP de découvrir automatiquement le Master AP dans le même VLAN.

En se basant sur l'exemple du port du switch pour le Master AP (cf. étape 1 du chapitre précédent), la configuration du port du switch pour un nouvel AP sera la suivante :

```
interface GigabitEthernet0/5
description --- 3702_AP ---
switchport trunk native vlan 10
switchport trunk allowed vlan 10,20,30,40
switchport mode trunk
spanning-tree portfast trunk
```

4. Une fois le TFTP et le port du switch configurés, vous pouvez connecter le nouvel AP. Après avoir démarré, l'AP essaie d'obtenir une adresse IP par DHCP, découvre le Master AP et télécharge la nouvelle image si besoin. Une fois l'enregistrement terminé, le nouvel AP télécharge automatiquement les paramètres de configuration depuis le Master AP et commencera à desservir les mêmes SSIDs configurés dans le chapitre précédent.

4 Optionnel : haute disponibilité et redondance

Le rôle de Master AP peut être repris à tout moment par un autre AP 1540/1560/1800/2800/3800 du même déploiement Mobility Express (sauf pour la série 1810), dans le cas où le Master AP d'origine ne serait plus joignable. Le Master AP et son backup ne doivent pas être du même modèle, mais on le recommande quand même pour plus de cohérence.

Les APs 1540/1560/1800/2800/3800 peuvent être enregistrés à un déploiement Mobility Express à travers la même procédure décrite dans le chapitre précédent, comme pour tout autre modèle d'AP supporté.

De nouveaux APs 1540/1560/1800/2800/3800 enregistrés détectent automatiquement le Master AP courant et se synchronise par VRRP (Virtual Router Redundancy Protocol). Ce protocole permet à tous les APs 1540/1560/1800/2800/3800 du même déploiement Mobility Express de détecter si le Master AP n'est plus joignable et de désigner automatiquement un nouveau Master AP parmi eux. Comme le VRRP est supporté uniquement entre des équipements dans le même réseau de niveau 2, il est essentiel que tous les APs du même déploiement Mobility Express soient connectés dans le même VLAN de management.

Pendant le processus d'élection d'un nouveau Master AP le flux de données des clients Wi-Fi déjà connectés sur les autres APs n'est pas affecté, car ce trafic est commuté localement derrière chaque AP et ne requiert pas une commutation centrale à travers le Master AP.

5 Référence : convertir un AP en Mobility Express

Un AP avec une image CAPWAP « classique » ou sans le mode Mobility Express activé peut toujours s'enregistrer à un Master AP.

Une image Mobility Express avec le mode Mobility Express activé permet à un AP de supporter le rôle de Master AP, en cas de redondance aussi : il est généralement recommandé d'avoir cette fonction disponible pour au moins une paire d'APs du déploiement.

Pour vérifier si votre AP 1540/1560/1800/2800/3800 est en train de tourner avec l'image et le mode Mobility Express, vous pouvez utiliser la commande « *show version* » en console/SSH/telnet, en mode *enable*.

L'identifiant et le mot de passe par défaut sont **Cisco / Cisco** et le password *enable* est également **Cisco**.

Si l'AP est déjà en version 8.5 et vous voyez la ligne suivante dans la commande « *show version* »

```
AP Image type      : MOBILITY EXPRESS IMAGE
```

cela signifie que l'AP peut être converti en mode Mobility Express avec une seule commande, si ce mode n'est pas déjà activé.

Si juste après la ligne précédente vous remarquez également la suivante

```
AP Configuration : MOBILITY EXPRESS CAPABLE
```

Le mode Mobility Express est déjà activé et l'AP peut porter le rôle de Master AP, ou le reprendre d'un autre AP du même déploiement en cas de redondance. Aucune autre action ne devrait être requise. Si avec la commande « *show version* » vous voyez le résultat suivant

```
AP Configuration : NOT MOBILITY EXPRESS CAPABLE
```

L'AP a déjà une image Mobility Express, mais n'est pas configuré pour supporter le rôle de Master AP. Pour activer le mode Mobility Express et le support du Master AP, vous pouvez utiliser la commande suivante en mode *enable* :

```
AP# ap-type mobility-express tftp
```

Si votre AP 1540/1560/1800/2800/3800 n'est pas en version 8.5 ou si avec la commande « *show version* » vous ne voyez aucune ligne indiquant qu'il s'agit d'une image Mobility Express, vous pouvez convertir l'image en version 8.5 et en mode Mobility Express en téléchargeant d'abord un des fichiers suivants (selon le modèle de votre AP) :

[AIR-AP1540-K9-ME-8-5-103-0.tar](#) (pour la gamme 1540)

[AIR-AP1560-K9-ME-8-5-103-0.tar](#) (pour la gamme 1560)

[AIR-AP1815-K9-ME-8-5-103-0.tar](#) (pour la gamme 1815)

[AIR-AP1830-K9-ME-8-5-103-0.tar](#) (pour la gamme 1830)

[AIR-AP1850-K9-ME-8-5-103-0.tar](#) (pour la gamme 1850)

[AIR-AP2800-K9-ME-8-5-103-0.tar](#) (pour la gamme 2800)

[AIR-AP3800-K9-ME-8-5-103-0.tar](#) (pour la gamme 3800)

Après avoir téléchargé l'image correspondante, vous pouvez convertir un AP CAPWAP « classique » en mode Mobility Express à travers la procédure suivante :

1. Sauvegardez le fichier .tar dans un serveur TFTP, comme [Tftpd32](#) pour Windows ou [TftpServer](#) pour Mac OS.
2. Connectez-vous à l'AP en console/SSH/telnet et tapez la commande suivante en mode *enable* :

```
AP# ap-type mobility-express tftp://<TFTP IP>/<path to the .tar file>
```

Dans certains cas, certaines versions plus anciennes du firmware des APs pourraient requérir les passages suivants pour la mise à jour, au lieu que la commande susmentionnée :

- i. Connectez-vous à l'AP en console/SSH/telnet et tapez la commande suivante en mode *enable* :

```
AP# archive download-sw /reload tftp://<TFTP IP>/<path to the .tar file>
```

- ii. Attendez que l'AP redémarre et tapez la commande suivante pour activer les fonctions Mobility Express aussi :

```
AP# ap-type mobility-express tftp
```

Attendez que l'AP redémarre avec le mode Mobility Express activé et prêt à supporter le rôle de Master AP.

6 Ressources additionnelles

La liste suivante de références devrait vous fournir des informations additionnelles pour les paramètres plus avancés d'un déploiement Mobility Express, ses options de personnalisation et des exemples d'intégration avec d'autres solutions.

- [Cisco Mobility Express Deployment Guide](#)
- [Configuration Details for Guest Networks and CMX Cloud Portals](#)
- [Configuration Details for Creating a Customized Bundle for the Internal Guest Portal](#)
- [Integration with Cisco CMX Cloud for Presence Analytics Services](#)
- [Integration with Cisco Prime Infrastructure](#)
- [Cisco Mobility Express Configuration and User Guide](#)
- [Cisco CMX Cloud Documentation](#)
- [Cisco OpenDNS Umbrella Solution for Cloud-Based Threat Protection](#)
- [Cisco Aironet Access Points](#)

Disclaimer

Les indications comprises dans ce document sont fournies à titre indicatif. Elles sont fondées sur des références issues de la documentation disponible, et d'essais effectués sur les équipements concernés dans le cadre de simples démonstrations. Des erreurs et des omissions ne sont pas exclues. Aucune garantie expresse ou tacite ne peut être donnée quant à l'utilisation de ces exemples en condition de production et d'exploitation réseau réelle.