Configurer CWA avec des points d'accès FlexConnect sur un WLC avec ISE

Table des matières

Introduction

Ce document décrit comment configurer l'authentification Web centrale avec les points d'accès FlexConnect sur un contrôleur LAN sans fil (WLC) avec Identity Services Engine (ISE) en mode de commutation locale.

Remarque importante : actuellement, l'authentification locale sur les FlexAP n'est pas prise en charge pour ce scénario.

Autres documents de cette série

- Exemple de configuration de l'authentification Web centralisée avec un commutateur et Identity Services Engine
- Authentification Web centralisée (CWA, pour Central Web Authentification) sur le WLC et exemple de configuration ISE

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco Identity Services Engine (ISE), version 1.2.1
- Logiciel du contrôleur LAN sans fil, version 7.4.100.0

Configurer

Il existe plusieurs méthodes pour configurer l'authentification Web centrale sur le contrôleur de réseau local sans fil (WLC). La première méthode est l'authentification Web locale dans laquelle le WLC redirige le trafic HTTP vers un serveur interne ou externe où l'utilisateur est invité à s'authentifier. Le WLC récupère ensuite les informations d'identification (renvoyées via une requête HTTP GET dans le cas d'un serveur externe) et effectue une authentification RADIUS. Dans le cas d'un utilisateur invité, un serveur externe (tel qu'Identity Service Engine (ISE) ou NAC Guest Server (NGS)) est requis car le portail fournit des fonctionnalités telles que l'enregistrement des périphériques et l'auto-approvisionnement. Ce processus comprend les étapes suivantes :

1. L'utilisateur s'associe au SSID d'authentification Web.
2. L'utilisateur ouvre son navigateur.
3. Le WLC redirige vers le portail invité (par exemple ISE ou NGS) dès qu'une URL est entrée.
4. L'utilisateur s'authentifie sur le portail.
5. Le portail invité redirige vers le WLC avec les informations d'identification entrées.
6. Le WLC authentifie l'utilisateur invité via RADIUS.
7. Le WLC redirige vers l'URL d'origine.

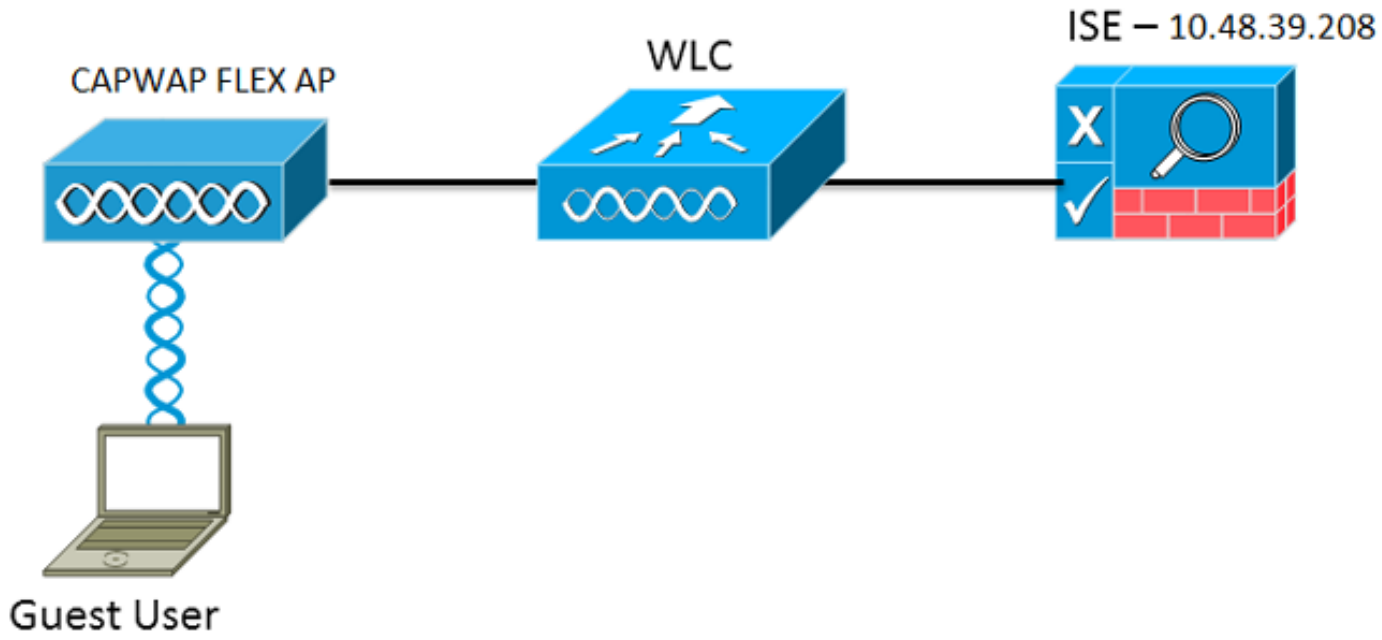
Ce processus inclut beaucoup de redirection. La nouvelle approche consiste à utiliser l'authentification Web centrale qui fonctionne avec ISE (versions ultérieures à 1.1) et WLC (versions ultérieures à 7.2). Ce processus comprend les étapes suivantes :

1. L'utilisateur s'associe au SSID d'authentification Web.
2. L'utilisateur ouvre son navigateur.
3. Le WLC redirige vers le portail invité.
4. L'utilisateur s'authentifie sur le portail.
5. L'ISE envoie une modification d'autorisation RADIUS (CoA - Port UDP 1700) pour indiquer au contrôleur que l'utilisateur est valide et finit par transmettre les attributs RADIUS tels que la liste de contrôle d'accès (ACL).
6. L'utilisateur est invité à réessayer l'URL d'origine.

Cette section décrit les étapes nécessaires pour configurer l'authentification Web centrale sur WLC et ISE.

Diagramme du réseau

Cette configuration utilise la configuration de réseau suivante :

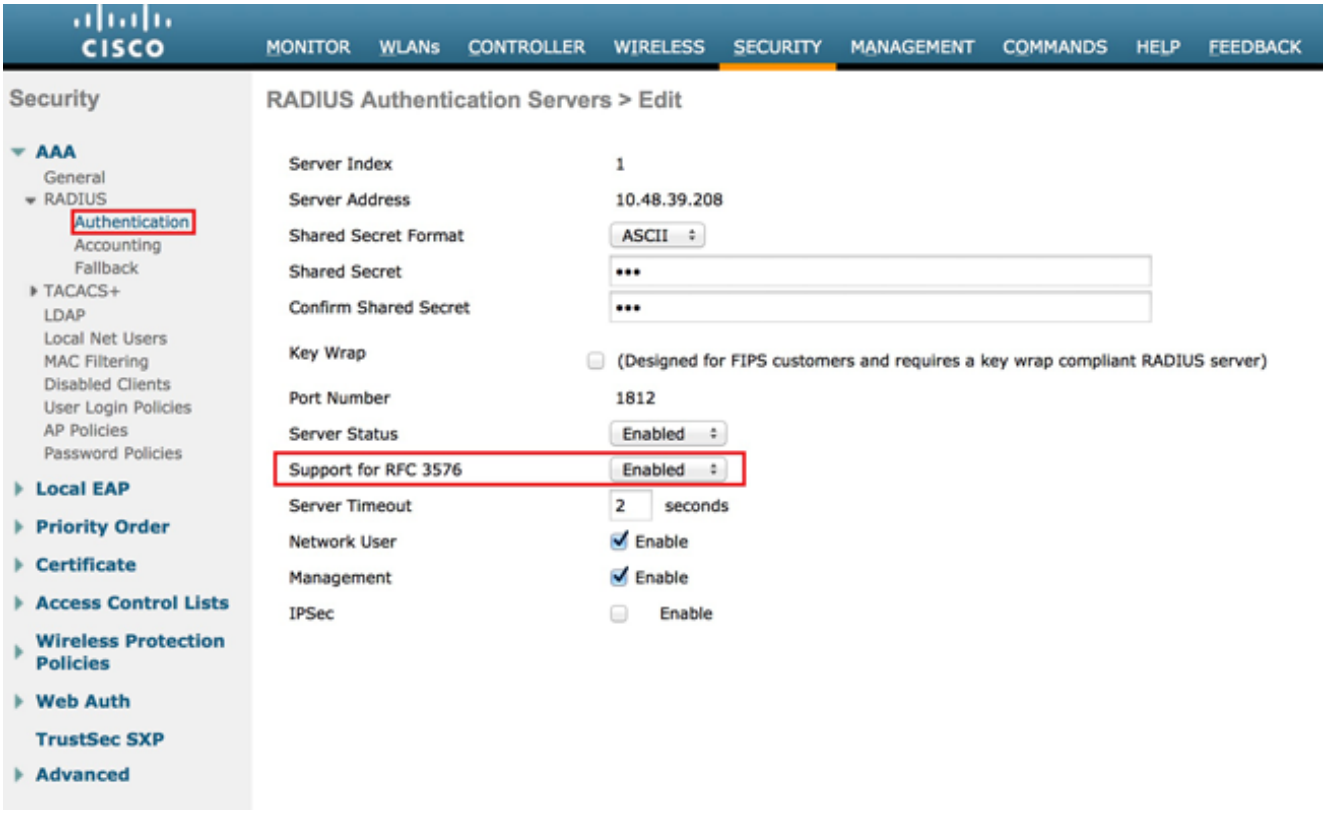


Configuration WLC

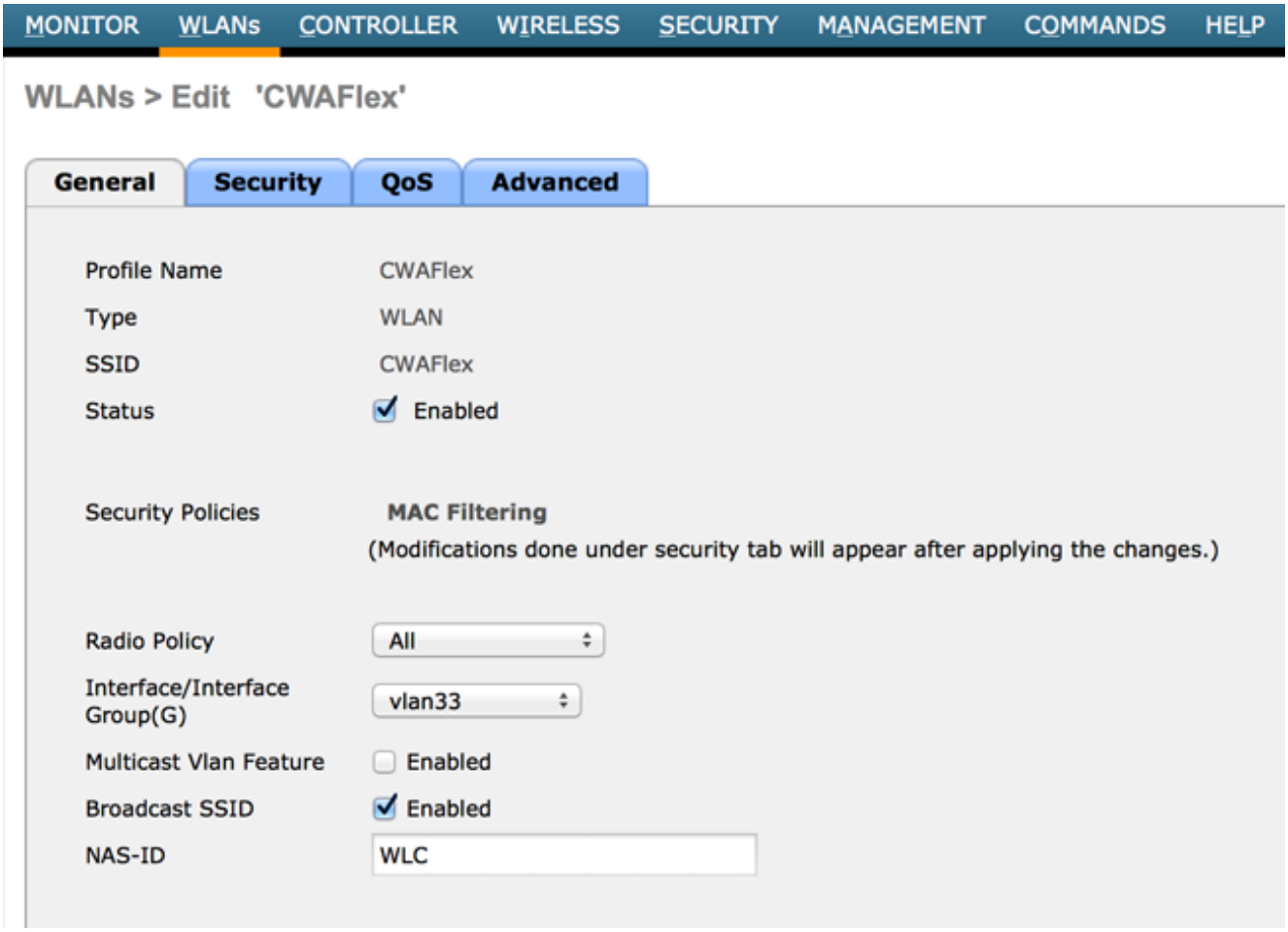
La configuration du WLC est assez simple. Un « truc ? » est utilisé (comme sur les commutateurs) pour obtenir l'URL d'authentification dynamique de l'ISE. (Comme il utilise CoA, une session doit être créée car l'ID de session fait partie de l'URL.) Le SSID est configuré pour utiliser le filtrage MAC, et l'ISE est configuré pour renvoyer un message d'acceptation d'accès même si l'adresse MAC est introuvable afin qu'il envoie l'URL de redirection pour tous les utilisateurs.

En outre, le contrôle d'admission au réseau (NAC) RADIUS et le remplacement AAA doivent être activés. Le contrôle d'accès réseau RADIUS permet à l'ISE d'envoyer une requête CoA qui indique que l'utilisateur est désormais authentifié et peut accéder au réseau. Il est également utilisé pour l'évaluation de posture dans laquelle l'ISE modifie le profil utilisateur en fonction du résultat de posture.

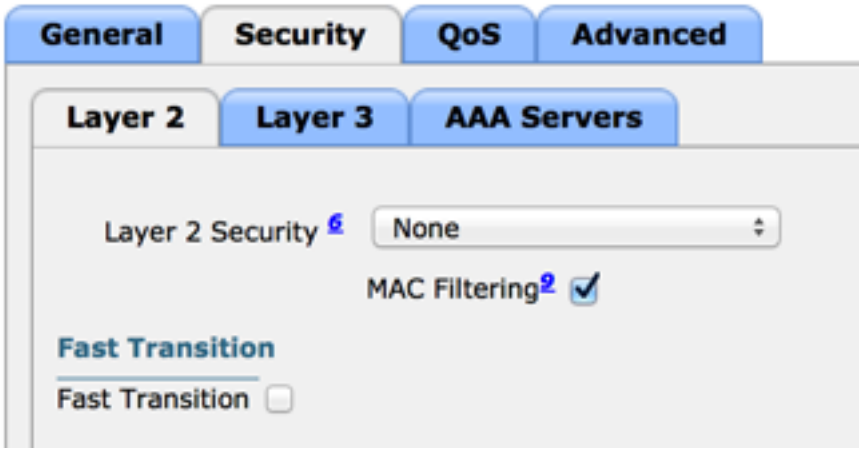
1. Assurez-vous que le protocole RFC3576 (CoA) est activé sur le serveur RADIUS, qui est le paramètre par défaut.



2. Créez un nouveau WLAN. Cet exemple crée un nouveau WLAN nommé *CWAFlex* et l'attribue à vlan33. (Notez qu'il n'aura pas beaucoup d'effet puisque le point d'accès est en mode de commutation locale.)

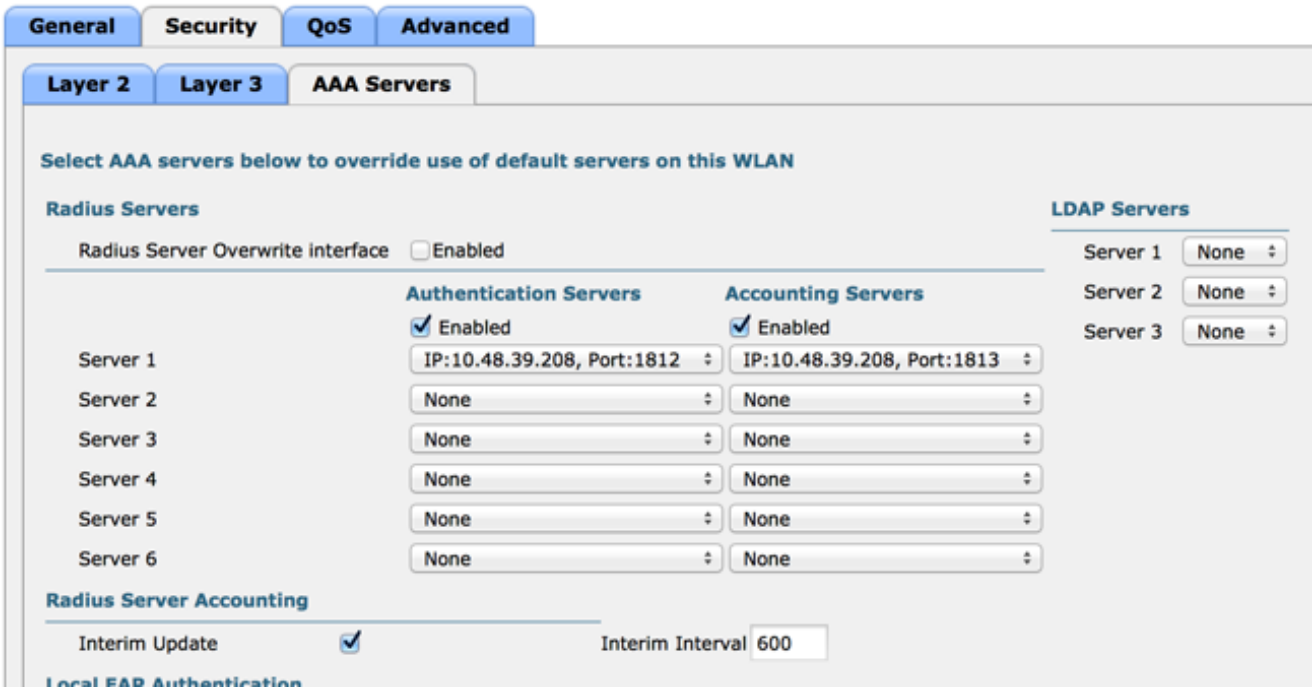


3. Dans l'onglet Security, activez MAC Filtering as Layer 2 Security.

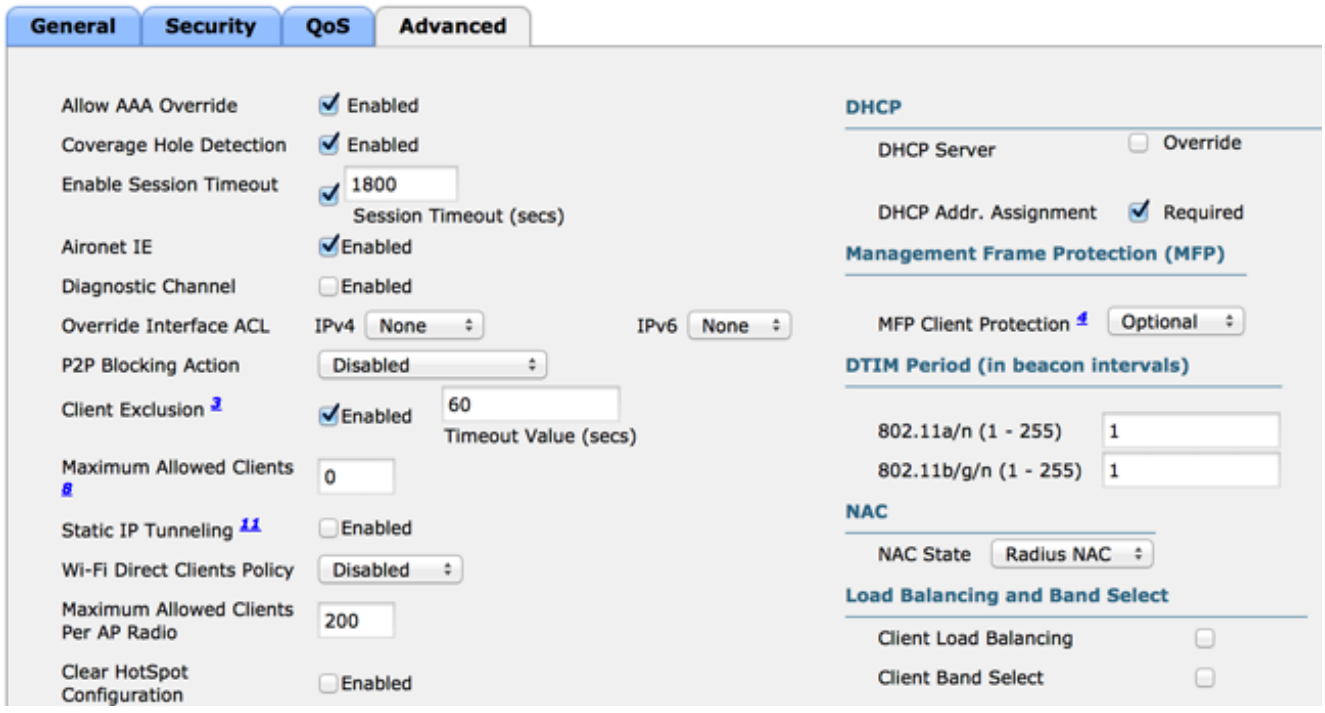


4. Dans l'onglet Couche 3, vérifiez que la sécurité est désactivée. (Si l'authentification Web est activée sur la couche 3, l'authentification Web locale est activée, et non l'authentification Web centrale.)

5. Dans l'onglet AAA Servers, sélectionnez le serveur ISE en tant que serveur radius pour le WLAN. Vous pouvez éventuellement le sélectionner pour la comptabilité afin d'obtenir des informations plus détaillées sur ISE.



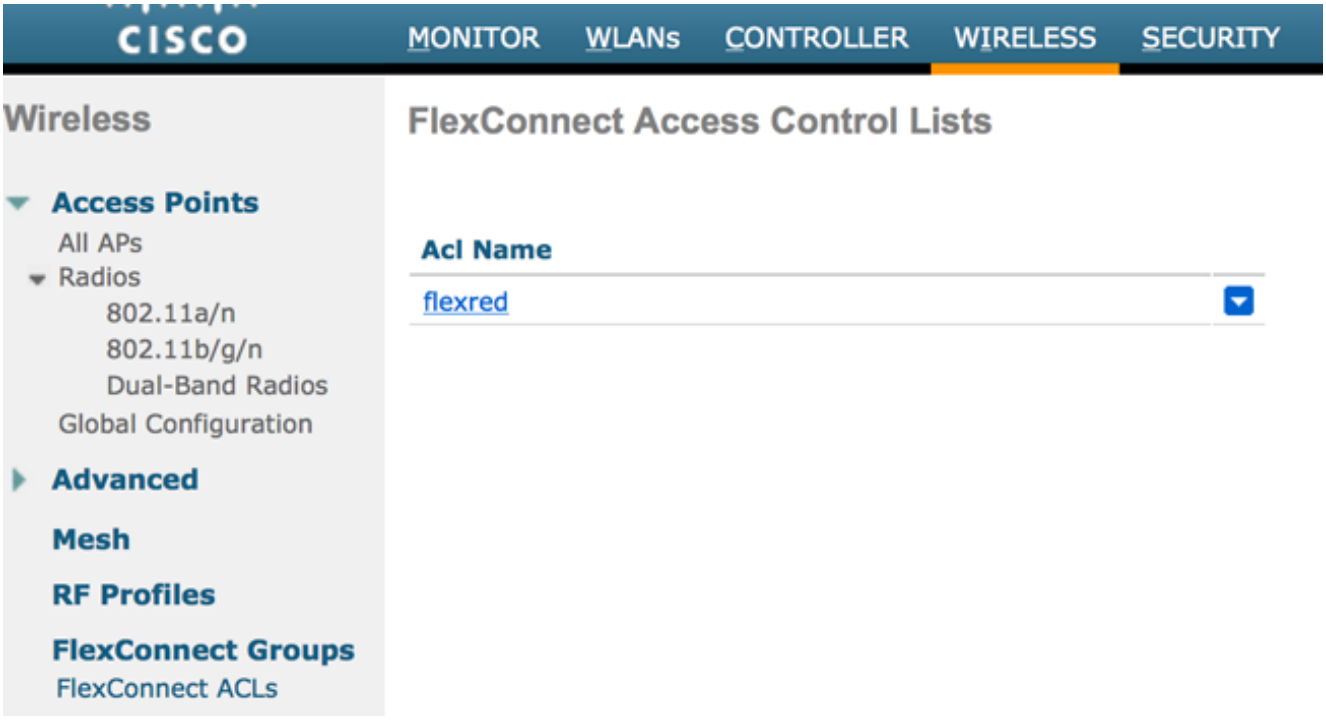
6. Sous l'onglet Avancé, vérifiez que l'option Autoriser le remplacement AAA est cochée et que l'option NAC Rayon est sélectionnée pour l'état NAC.



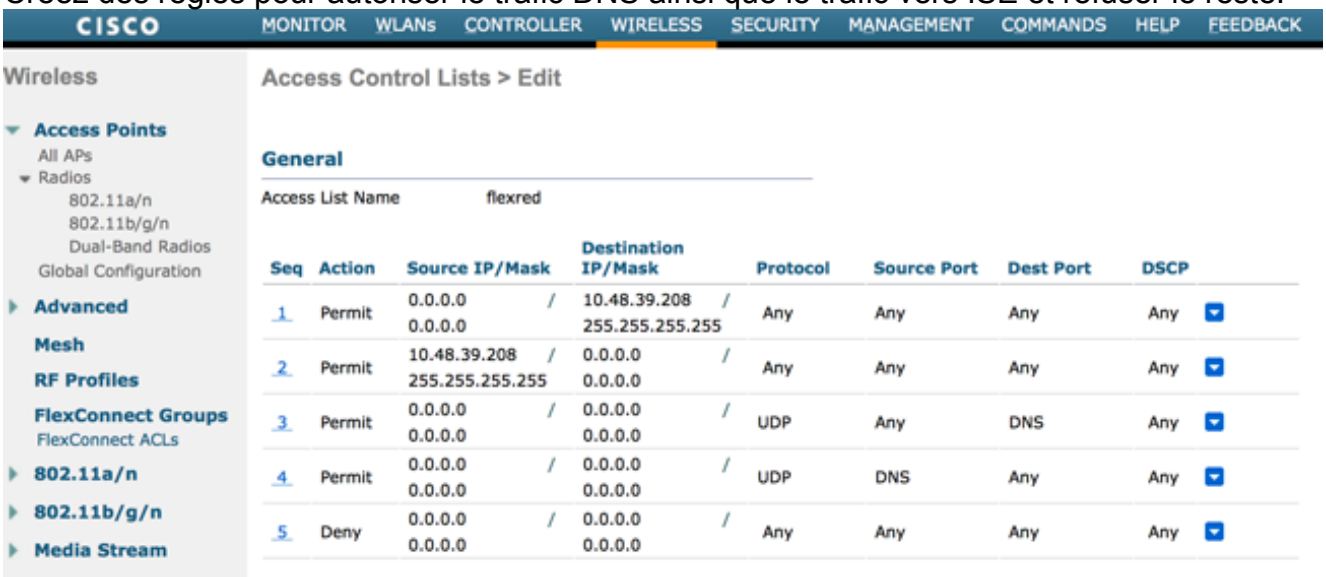
7. Créez une liste de contrôle d’accès redirigée.

   Cette liste de contrôle d'accès est référencée dans le message Access-Accept de l'ISE et définit le trafic qui doit être redirigé (refusé par la liste de contrôle d'accès) ainsi que le trafic qui ne doit pas être redirigé (autorisé par la liste de contrôle d'accès). Fondamentalement, le DNS et le trafic vers/depuis l'ISE doivent être autorisés. **Remarque** : un problème avec les points d'accès FlexConnect est que vous devez créer une liste de contrôle d'accès FlexConnect distincte de votre liste de contrôle d'accès normale. Ce problème est documenté dans le bogue Cisco CSCue68065 et est corrigé dans la version 7.5. Dans WLC 7.5 et versions ultérieures, seule une ACL FlexACL est requise, et aucune ACL standard

n'est requise. Le WLC s'attend à ce que l'ACL de redirection retournée par ISE soit une ACL normale. Toutefois, pour garantir son fonctionnement, vous devez appliquer la même liste de contrôle d'accès que la liste FlexConnect.
Cet exemple montre comment créer une liste de contrôle d'accès FlexConnect nommée *flexred* :

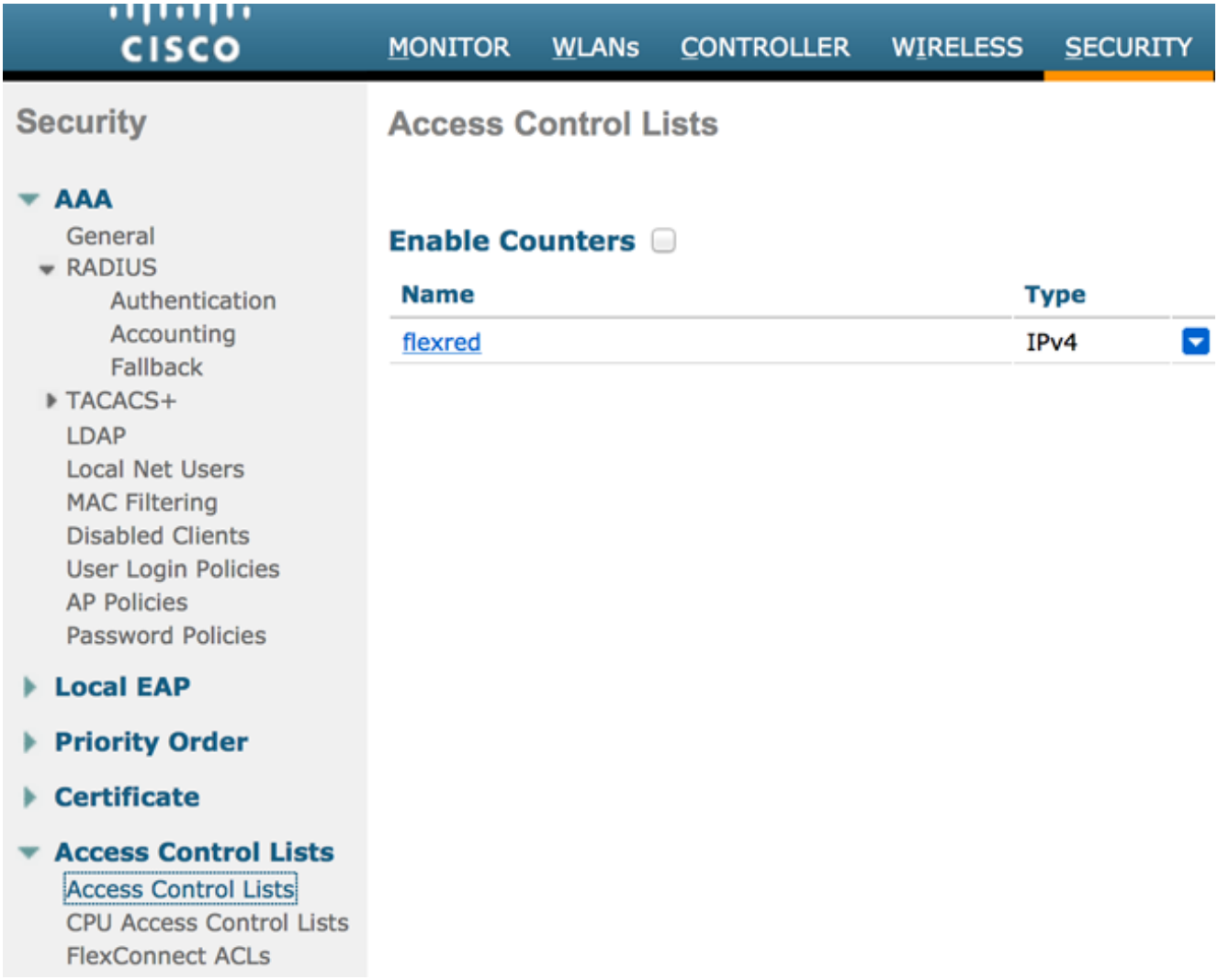


Créez des règles pour autoriser le trafic DNS ainsi que le trafic vers ISE et refuser le reste.



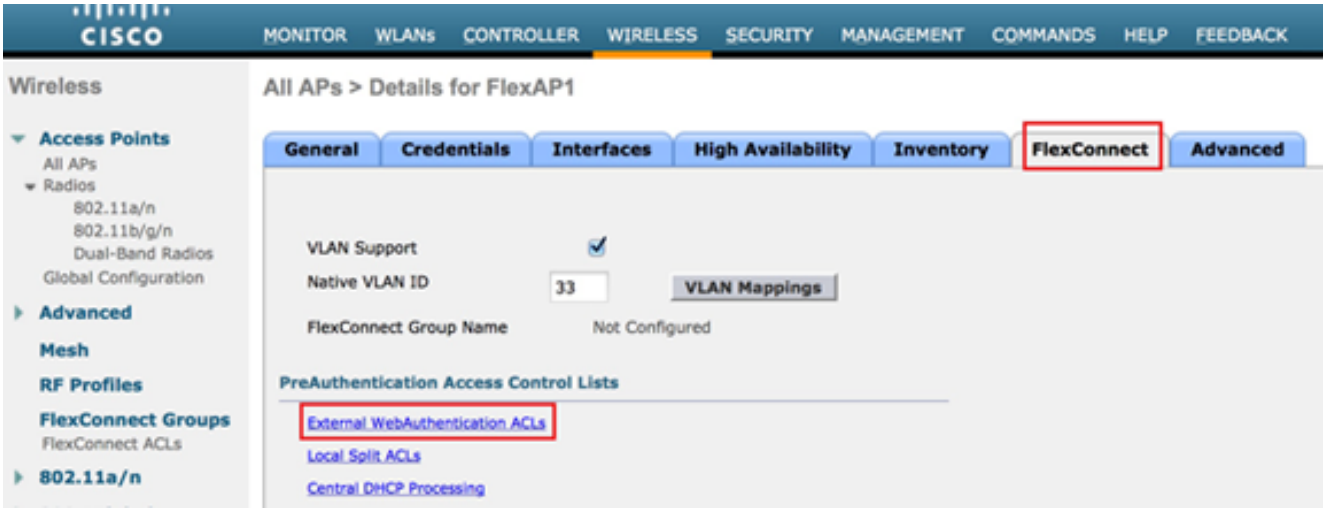
Si vous souhaitez une sécurité maximale, vous ne pouvez autoriser que le port 8443 vers ISE. (En cas de positionnement, vous devez ajouter des ports de positionnement standard, tels que 8905, 8906, 8909, 8910.)

(Uniquement sur les codes antérieurs à la version 7.5 en raison de CSCue68065) Choisissez **Security > Access Control Lists** pour créer une liste de contrôle d'accès identique portant le même nom.



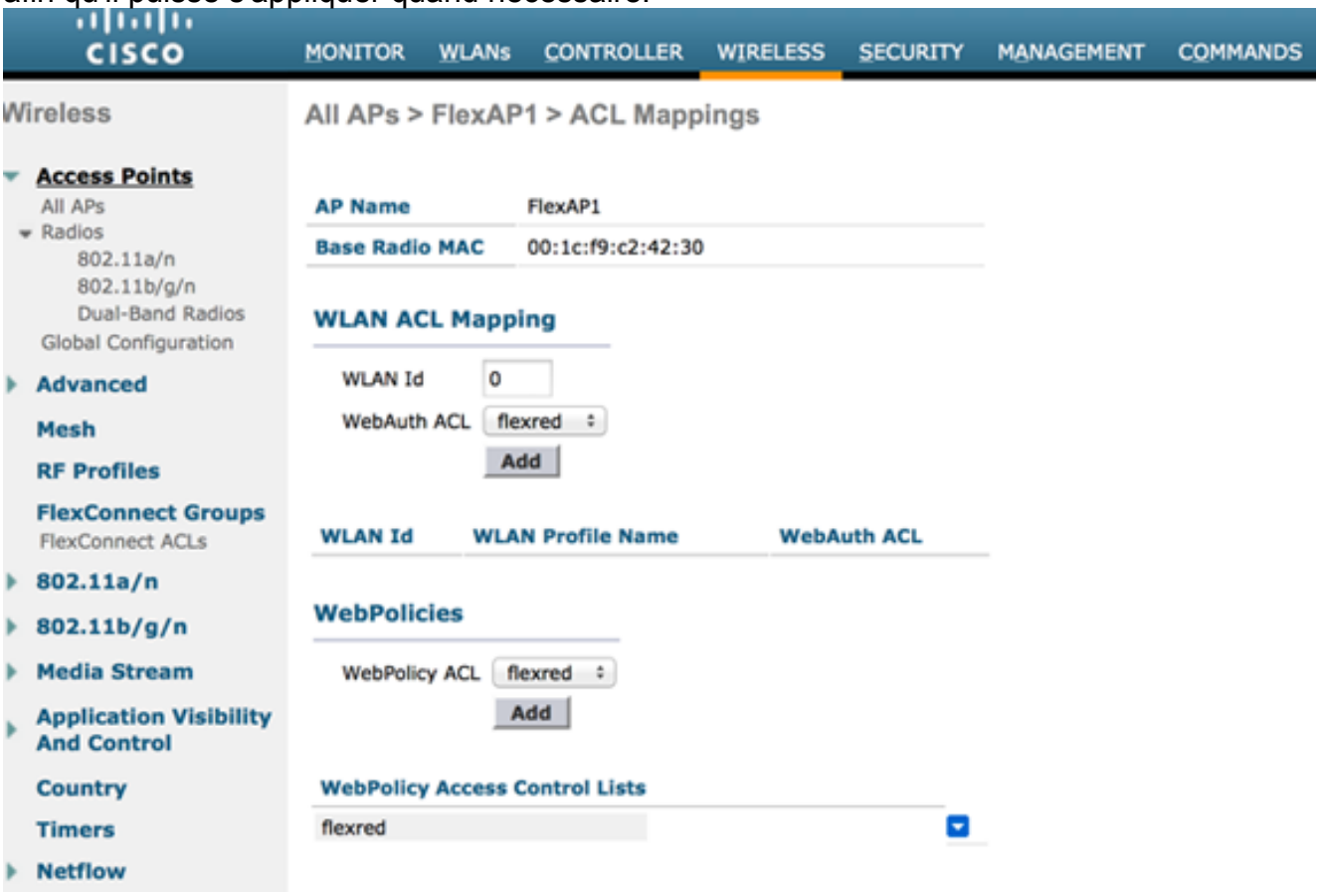
Préparez le point d'accès FlexConnect spécifique. Notez que pour un déploiement plus important, vous utiliserez généralement des groupes FlexConnect et n'exécuterez pas ces éléments sur une base par point d'accès pour des raisons d'évolutivité.

Cliquez sur **Wireless**, puis sélectionnez le point d'accès spécifique.Cliquez sur l'onglet **FlexConnect**, puis sur **External Webauthentication ACLs**. (Avant la version 7.4, cette option était appelée *stratégies Web*.)



Ajoutez la liste de contrôle d'accès (nommée *flexred* dans cet exemple) à la zone des

stratégies Web. La liste de contrôle d'accès est ainsi pré-poussée vers le point d'accès. Il n'est pas encore appliqué, mais le contenu de la liste de contrôle d'accès est donné à l'AP afin qu'il puisse s'appliquer quand nécessaire.



La configuration du WLC est maintenant terminée.

Configuration ISE

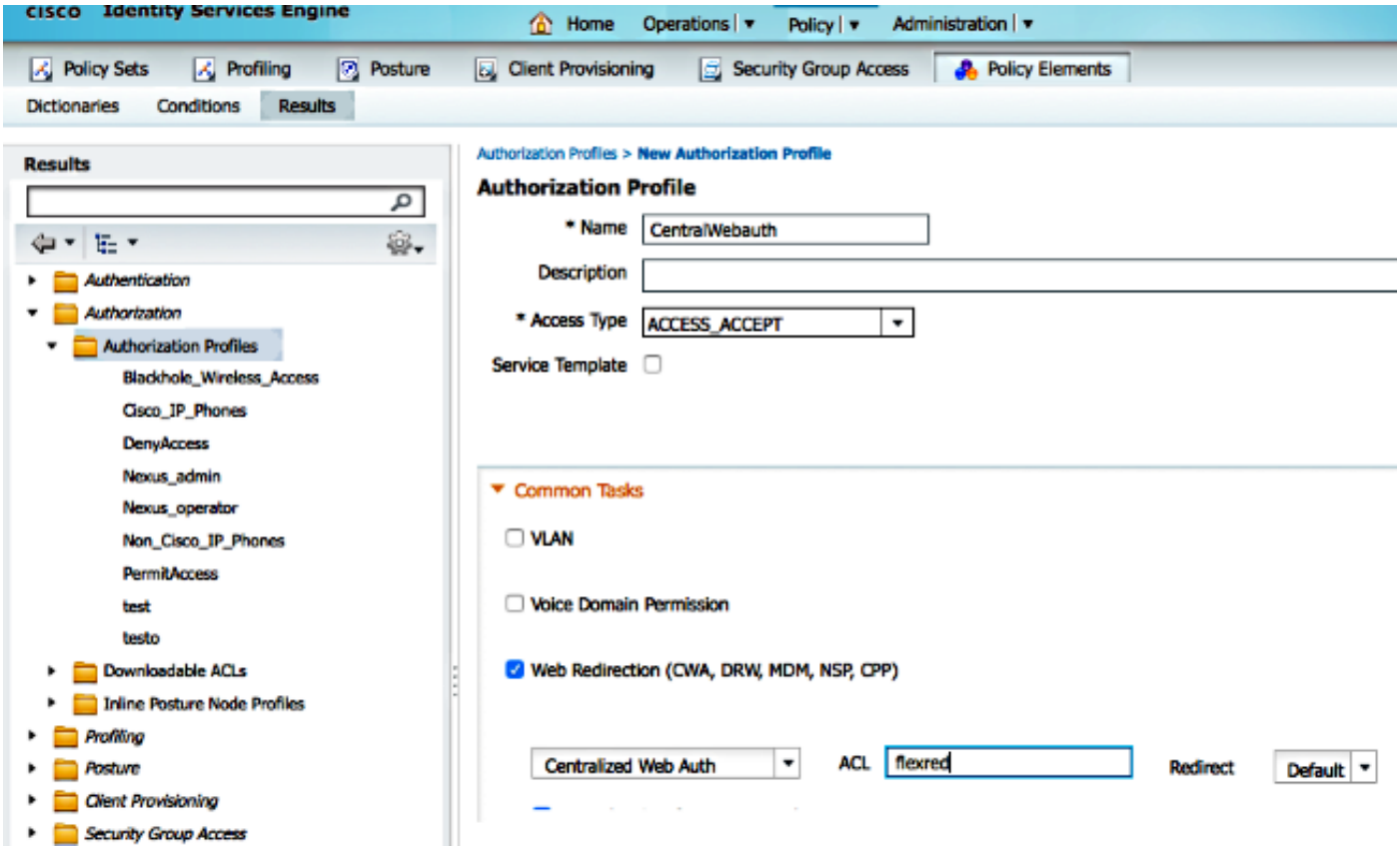
Créer le profil d'autorisation

Complétez ces étapes afin de créer le profil d'autorisation :

1. Cliquez sur **Policy**, puis sur **Policy Elements**.
2. Cliquez sur **Résultats**.
3. Développez **Autorisation**, puis cliquez sur **Profil d'autorisation**.
4. Cliquez sur le bouton **Add** afin de créer un nouveau profil d'autorisation pour l'authentification Web centrale.
5. Dans le champ **Nom**, entrez un nom pour le profil. Cet exemple utilise *CentralWebauth*.
6. Sélectionnez **ACCESS_ACCEPT** dans la liste déroulante Type d'accès.
7. Cochez la case **Web Authentication** et choisissez **Centralized Web Auth** dans la liste déroulante.
8. Dans le champ ACL, entrez le nom de l'ACL sur le WLC qui définit le trafic qui sera redirigé. Cet exemple utilise *flexred*.

9. Choisissez **Default** dans la liste déroulante Redirect.

L'attribut Redirect définit si l'ISE voit le portail Web par défaut ou un portail Web personnalisé créé par l'administrateur ISE. Par exemple, la liste de contrôle d'accès *flexible* dans cet exemple déclenche une redirection sur le trafic HTTP du client vers n'importe où.



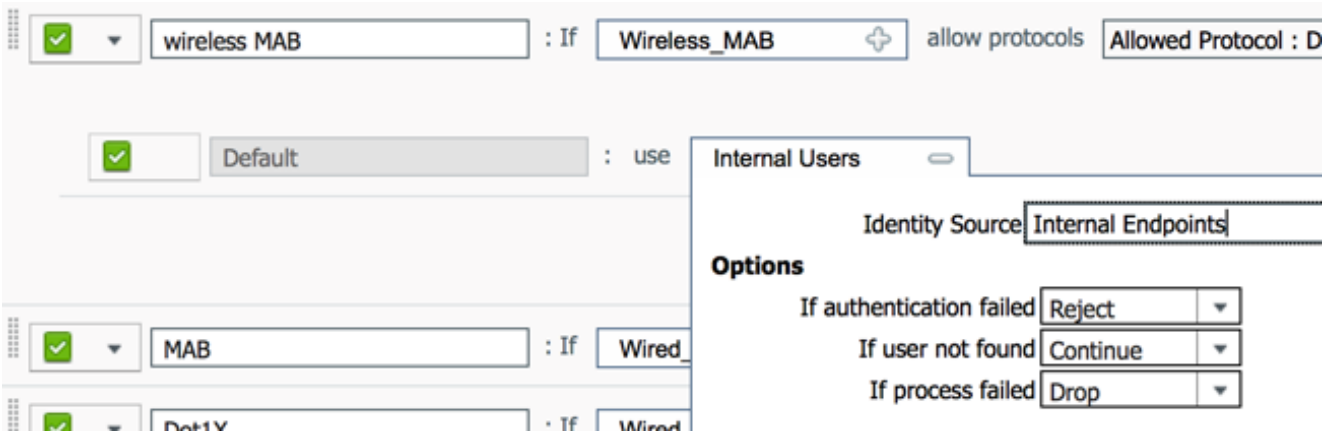
Créer une règle d'authentification

Complétez ces étapes afin d'utiliser le profil d'authentification pour créer la règle d'authentification :

1. Dans le menu Policy, cliquez sur **Authentication**. Cette image montre un exemple de configuration de la règle de stratégie d'authentification. Dans cet exemple, une règle est configurée qui se déclenche lorsque le filtrage MAC est détecté.

2. Entrez un nom pour votre règle d'authentification. Cet exemple utilise *Wireless Mab*.
3. Sélectionnez l'icône plus (**+**) dans le champ Condition If.
4. Sélectionnez **Condition composée**, puis **Wireless_MAB**.
5. Sélectionnez « Default network access » comme protocole autorisé.
6. Cliquez sur la flèche située à côté de **et ...** afin de développer davantage la règle.
7. Cliquez sur l'icône **+** dans le champ Identity Source, et choisissez **Internal endpoints**.

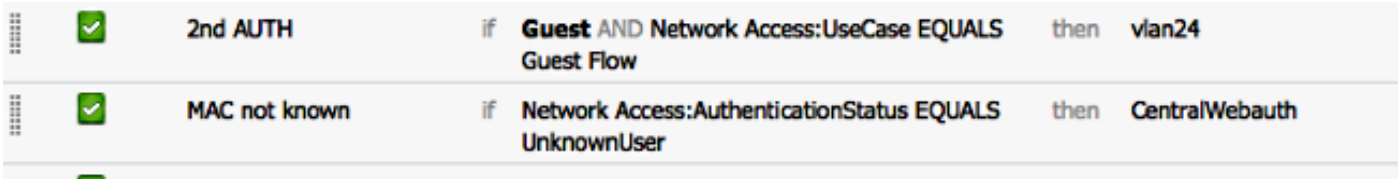
8. Choisissez **Continue** dans la liste déroulante If user not found.



Cette option permet à un périphérique d'être authentifié (via webauth) même si son adresse MAC n'est pas connue. Les clients Dot1x peuvent toujours s'authentifier avec leurs informations d'identification et ne doivent pas être concernés par cette configuration.

Créer une règle d'autorisation

Il existe désormais plusieurs règles à configurer dans la stratégie d'autorisation. Lorsque le PC est associé, il passe par le filtrage MAC ; il est supposé que l'adresse MAC n'est pas connue, de sorte que l'authentification Web et la liste de contrôle d'accès sont renvoyées. Cette règle *MAC inconnue* est illustrée dans l'image ci-dessous et est configurée dans cette section.



Complétez ces étapes afin de créer la règle d'autorisation :

1. Créez une nouvelle règle et entrez un nom. Cet exemple utilise *MAC inconnu*.
2. Cliquez sur l'icône plus (**+**) dans le champ de condition et choisissez de créer une condition.
3. Développez la liste déroulante **expression**.
4. Choisissez **Network access**, et développez-le.
5. Cliquez sur **AuthenticationStatus**, puis choisissez l'opérateur **Equals**.
6. Sélectionnez **UnknownUser** dans le champ de droite.
7. Sur la page Autorisation générale, choisissez **CentralWebauth** (profil d'autorisation) dans le champ à droite du mot **alors**.Cette étape permet à l'ISE de continuer même si l'utilisateur (ou l'adresse MAC) n'est pas connu.La page de connexion s'affiche désormais pour les utilisateurs inconnus. Cependant, une fois qu'ils ont entré leurs informations d'identification, une demande d'authentification leur est présentée à nouveau sur l'ISE ; par conséquent, une autre règle doit être configurée avec une condition qui est remplie si l'utilisateur est un utilisateur invité. Dans cet exemple, *Si UseridentityGroup est égal à Guest* est utilisé, et il est supposé que tous les invités appartiennent à ce groupe.
8. Cliquez sur le bouton Actions situé à la fin de la règle *MAC inconnu*, et choisissez d'insérer

une nouvelle règle ci-dessus.**Remarque :** il est très important que cette nouvelle règle précède la règle *MAC non connue*.

9. Entrez **2nd AUTH** dans le champ du nom.
10. Sélectionnez un groupe d'identité comme condition. Cet exemple a choisi **Invité**.
11. Dans le champ Condition, cliquez sur l'icône plus (**+**) et choisissez de créer une condition.
12. Choisissez **Network Access**, puis cliquez sur **UseCase**.
13. Sélectionnez **Égal** comme opérateur.
14. Choisissez **GuestFlow** comme opérande approprié. Cela signifie que vous attraperez les utilisateurs qui viennent de se connecter à la page Web et qui reviendront après une modification d'autorisation (la partie flux invité de la règle) et seulement s'ils appartiennent au groupe d'identité invité.
15. Sur la page d'autorisation, cliquez sur l'icône plus (**+**) (située à côté de *alors*) afin de choisir un résultat pour votre règle.

    Dans cet exemple, un profil préconfiguré (vlan34) est attribué ; cette configuration n'est pas affichée dans ce document.

    Vous pouvez choisir une option **Permit Access** ou créer un profil personnalisé afin de renvoyer le VLAN ou les attributs que vous aimez.

Remarque importante : dans la version 1.3 d'ISE, selon le type d'authentification Web, l'exemple d'utilisation « Guest Flow » peut ne plus être rencontré. La seule condition possible serait alors que la règle d'autorisation contienne le groupe d'utilisateurs invité.

Activer le renouvellement IP (facultatif)

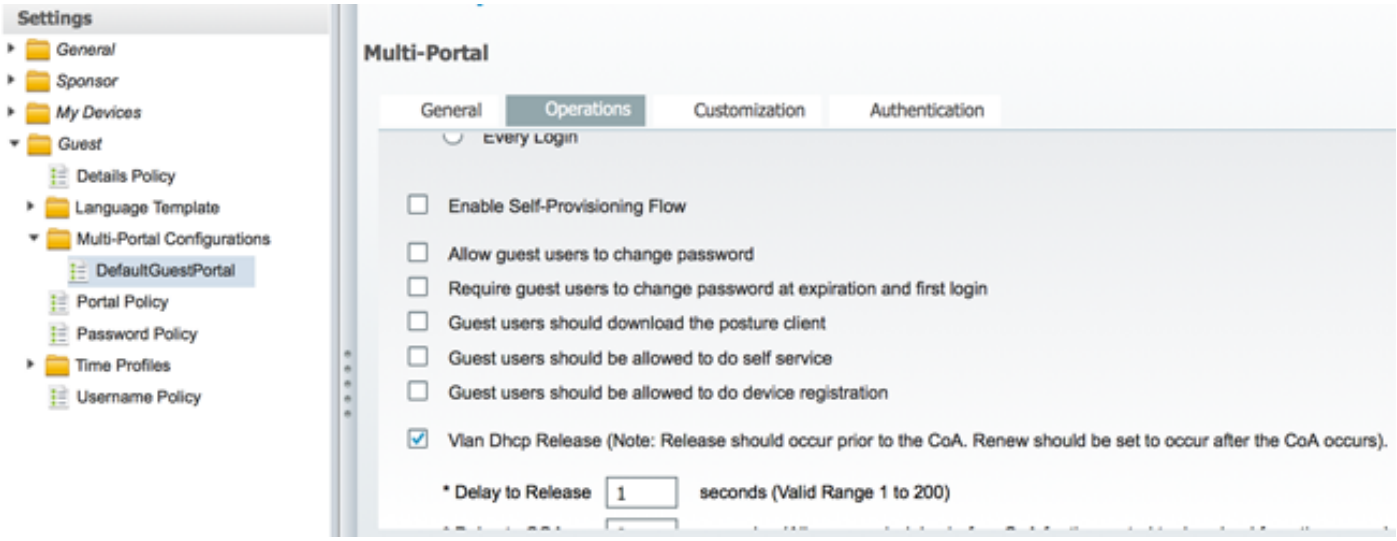
Si vous attribuez un VLAN, la dernière étape consiste pour l'ordinateur client à renouveler son adresse IP. Cette étape est réalisée par le portail invité pour les clients Windows. Si vous n'avez pas défini un VLAN pour la *2ème* règle *AUTH* plus tôt, vous pouvez ignorer cette étape.

Notez que sur les AP FlexConnect, le VLAN doit préexister sur l'AP lui-même. Par conséquent, si ce n'est pas le cas, vous pouvez créer un mappage VLAN-ACL sur l'AP lui-même ou sur le groupe flexible où vous n'appliquez aucune ACL pour le nouveau VLAN que vous voulez créer. Cela crée en fait un VLAN (sans ACL).

Si vous avez attribué un VLAN, procédez comme suit afin d'activer le renouvellement IP :

1. Cliquez sur **Administration**, puis sur **Guest Management**.
2. Cliquez sur **Paramètres**.
3. Développez **Guest**, puis **Multi-Portal Configuration**.
4. Cliquez sur **DefaultGuestPortal** ou sur le nom d'un portail personnalisé que vous avez peut-être créé.

5. Cochez la case **Vlan DHCP Release**.**Remarque :** cette option ne fonctionne que pour les clients Windows.



Flux de trafic

Il peut sembler difficile de comprendre quel trafic est envoyé où dans ce scénario. Voici un bref commentaire :

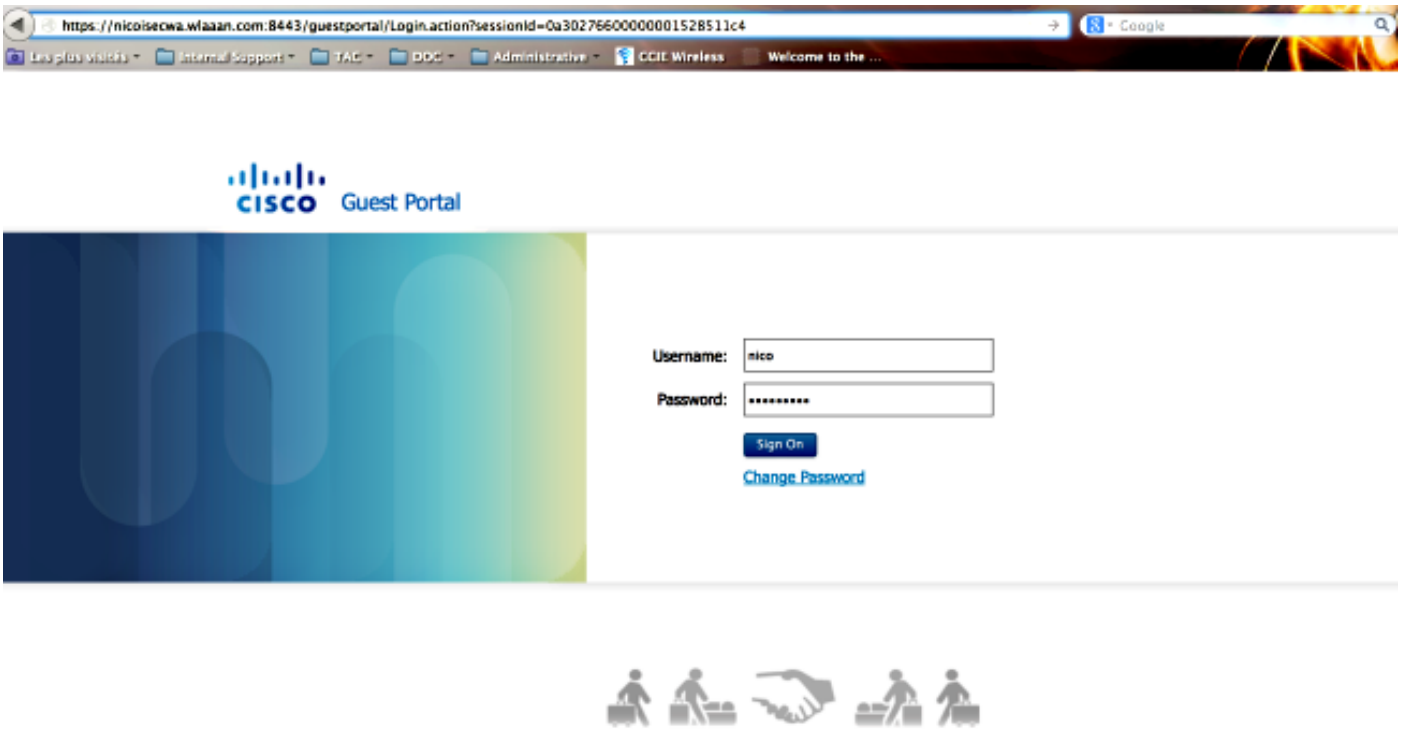
- Le client envoie une requête d'association par liaison radio pour le SSID.
- Le WLC gère l'authentification de filtrage MAC avec ISE (où il reçoit les attributs de redirection).
- Le client ne reçoit une réponse assoc qu'une fois le filtrage MAC terminé.
- Le client envoie une requête DHCP, ce qui est **LOCAL** commuté par le point d'accès afin d'obtenir une adresse IP du site distant.
- Dans l'état Central_webauth, le trafic marqué pour deny sur la liste de contrôle d'accès de redirection (donc HTTP généralement) est **CENTRALEMENT** commuté. Ainsi, ce n'est pas l'AP qui fait la redirection mais le WLC ; par exemple, quand le client demande un site Web, l'AP envoie ceci au WLC encapsulé dans CAPWAP et le WLC usurpe cette adresse IP de site Web et redirige vers ISE.
- Le client est redirigé vers l'URL de redirection ISE. C'est **LOCAL** de nouveau commuté (parce qu'il appuie sur permit sur l'ACL de redirection flex).
- Une fois à l'état EXÉCUTÉ, le trafic est commuté localement.

Vérifier

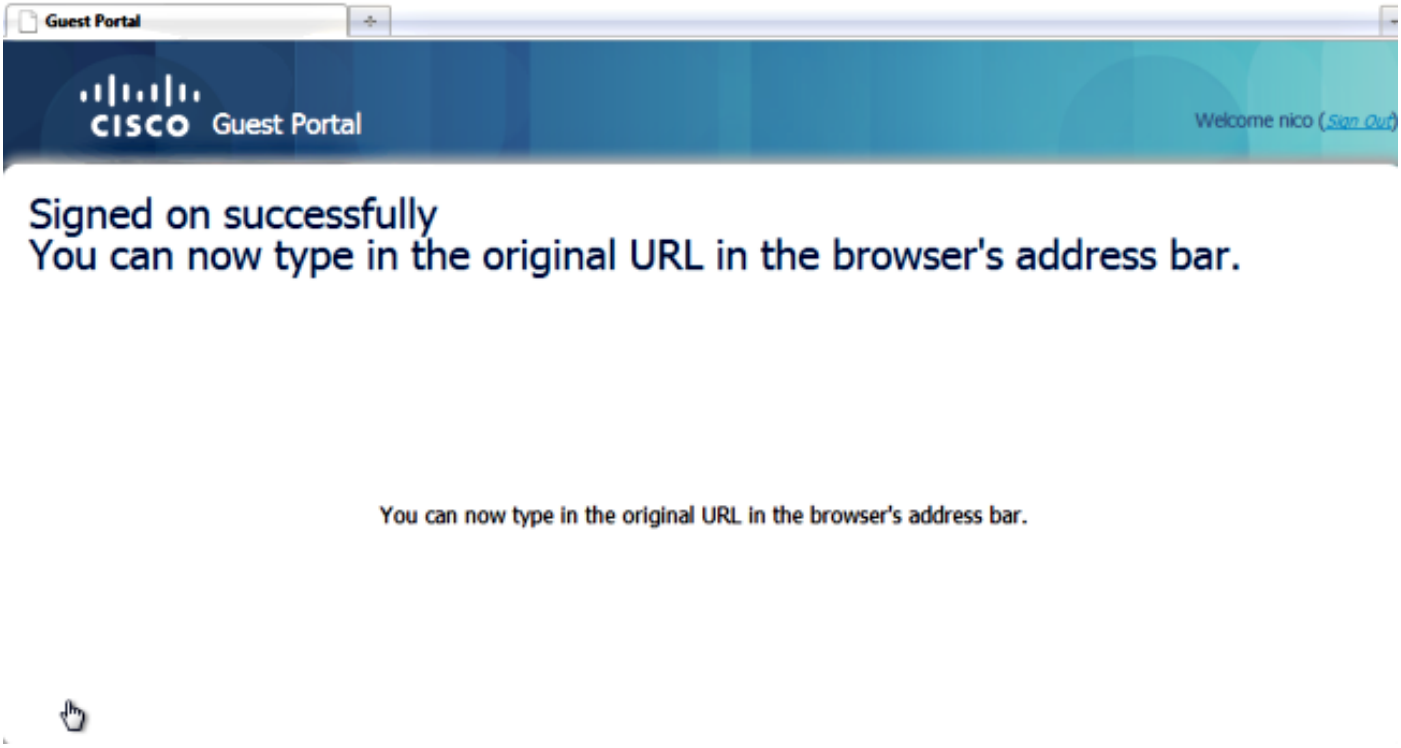
Une fois que l'utilisateur est associé au SSID, l'autorisation s'affiche dans la page ISE.

De bas en haut, vous pouvez voir l'authentification de filtrage d'adresse MAC qui renvoie les attributs CWA. Ensuite, vous accédez au portail avec le nom d'utilisateur. L'ISE envoie alors un CoA au WLC et la dernière authentification est une authentification de filtrage MAC de couche 2 du côté du WLC, mais ISE se souvient du client et du nom d'utilisateur et applique le VLAN nécessaire que nous avons configuré dans cet exemple.

Lorsqu'une adresse est ouverte sur le client, le navigateur est redirigé vers l'ISE. Assurez-vous que le système de noms de domaine (DNS) est correctement configuré.



L'accès au réseau est accordé une fois que l'utilisateur a accepté les stratégies.



Sur le contrôleur, l'état du Gestionnaire de stratégies et l'état du NAC RADIUS passe de *POSTURE_REQD* à *RUN*.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.