Configurer l'authentification Web externe avec les WLC

Table des matières

Introduction

Ce document explique comment employer un serveur Web externe afin d'installer un contrôleur de réseau local sans fil (WLC) pour l'authentification Web.

Conditions préalables

Exigences

Assurez-vous que vous répondez à ces exigences avant d'essayer cette configuration :

- Connaissance de base de la configuration des points d'accès légers (LAP) et des WLC Cisco
- Connaissances de base du protocole LWAPP (Lightweight Access Point Protocol) et du protocole CAPWAP (Control and Provisioning of Wireless Access Points)
- Connaissances sur la configuration d'un serveur Web externe

- Connaissances sur la configuration des serveurs DHCP et DNS

Composants utilisés

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

- WLC Cisco 4400 exécutant la version de microprogramme 7.0.116.0
- LAP de la gamme Cisco 1131AG
- Adaptateur client sans fil Cisco 802.11a/b/g exécutant la version de microprogramme 3.6
- Serveur Web externe qui héberge la page de connexion d'authentification Web
- Serveurs DNS et DHCP pour la résolution d'adresses et l'allocation d'adresses IP aux clients sans fil

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Informations générales

L'authentification Web est une fonctionnalité de sécurité de troisième couche faisant en sorte que le contrôleur empêche le trafic IP (à l'exception des paquets liés au protocole DHCP et au DNS) provenant d'un client particulier jusqu'à ce que le client ait fourni un nom d'utilisateur et un mot de passe valides. L'authentification Web est une méthode d'authentification simple qui ne nécessite pas d'utilitaire demandeur ou client.

L'authentification Web peut se faire par les moyens suivants :

- Fenêtre de connexion par défaut sur le WLC
- Version modifiée de la fenêtre de connexion par défaut sur le WLC
- Fenêtre de connexion personnalisée, que vous configurez sur un serveur Web externe (authentification Web externe)
- Fenêtre de connexion personnalisée que vous téléchargez vers le contrôleur

Ce document fournit un exemple de configuration pour expliquer comment configurer le WLC pour utiliser un script de connexion à partir d'un serveur Web externe.

Processus d'authentification Web externe

Avec l'authentification Web externe, la page de connexion utilisée pour l'authentification Web est stockée sur un serveur Web externe. Voici la séquence d'événements lorsqu'un client sans fil tente d'accéder à un réseau WLAN sur lequel l'authentification Web externe est activée :

1. Le client (utilisateur final) se connecte au WLAN, ouvre un navigateur Web et saisit une URL, telle que www.cisco.com.

2. Le client envoie une requête DNS à un serveur DNS afin de convertir www.cisco.com en adresse IP.
3. Le WLC transfère la requête au serveur DNS qui, à son tour, résout www.cisco.com en adresse IP et envoie une réponse DNS. Le contrôleur transfère la réponse au client.
4. Le client tente d'établir une connexion TCP avec l'adresse IP www.cisco.com en envoyant le paquet SYN TCP à l'adresse IP www.cisco.com.
5. Le WLC a configuré des règles pour le client, donc peut agir en tant que serveur mandataire pour www.cisco.com. Il renvoie un paquet TCP SYN-ACK au client, avec l'adresse IP de www.cisco.com comme source. Le client renvoie un paquet TCP ACK afin de se terminer la connexion TCP en trois temps. Une fois cela terminé, la connexion TCP est entièrement établie.
6. Le client envoie un paquet HTTP GET destiné à www.google.com. Le WLC intercepte ce paquet, l'envoie pour le traitement de redirection. La passerelle d'application HTTP prépare un corps en HTML et le renvoie comme réponse au HTTP GET demandé par le client. Ce HTML incite le client à se rendre à l'URL de page Web par défaut du WLC, par exemple : http://<Virtual-Server-IP>/login.html.
7. Le client démarre alors la connexion HTTPS à l'URL de redirection qui l'envoie à l'adresse 1.1.1.1. Il s'agit de l'adresse IP virtuelle du contrôleur. Le client doit valider le certificat du serveur ou l'ignorer pour activer le tunnel SSL.
8. Comme l'authentification Web externe est activée, le WLC redirige le client vers le serveur Web externe.
9. L'URL de connexion d'authentification Web externe est ajoutée avec des paramètres tels que l'adresse AP_Mac_Address, l'URL client (www.cisco.com) et l'URL action_URL dont le client a besoin pour contacter le serveur Web du contrôleur.**Remarque :** l'action_URL indique au serveur Web que le nom d'utilisateur et le mot de passe sont stockés sur le contrôleur. Les informations d'identification doivent être renvoyées au contrôleur afin d'être authentifiées.
10. L'URL du serveur Web externe dirige l'utilisateur vers une page de connexion.
11. La page de connexion prend les informations d'identification de l'utilisateur et renvoie la demande à l'action_URL, par exemple http://1.1.1.1/login.html, du serveur Web du WLC.
12. Le serveur Web WLC envoie le nom d'utilisateur et le mot de passe pour l'authentification.
13. Le WLC initie la requête du serveur RADIUS ou utilise la base de données locale sur le WLC et authentifie l'utilisateur.
14. Si l'authentification réussit, le serveur Web du WLC transfère l'utilisateur à l'URL de redirection configurée ou à l'URL avec laquelle le client a commencé, telle que www.cisco.com.
15. Si l'authentification échoue, le serveur Web du WLC redirige l'utilisateur vers l'URL de connexion du client.

Remarque : afin de configurer l'authentification Web externe pour utiliser des ports autres que HTTP et HTTPS, émettez cette commande :

```
(Cisco Controller) >config network web-auth-port

<port>          Configures an additional port to be redirected for web authentication.
```

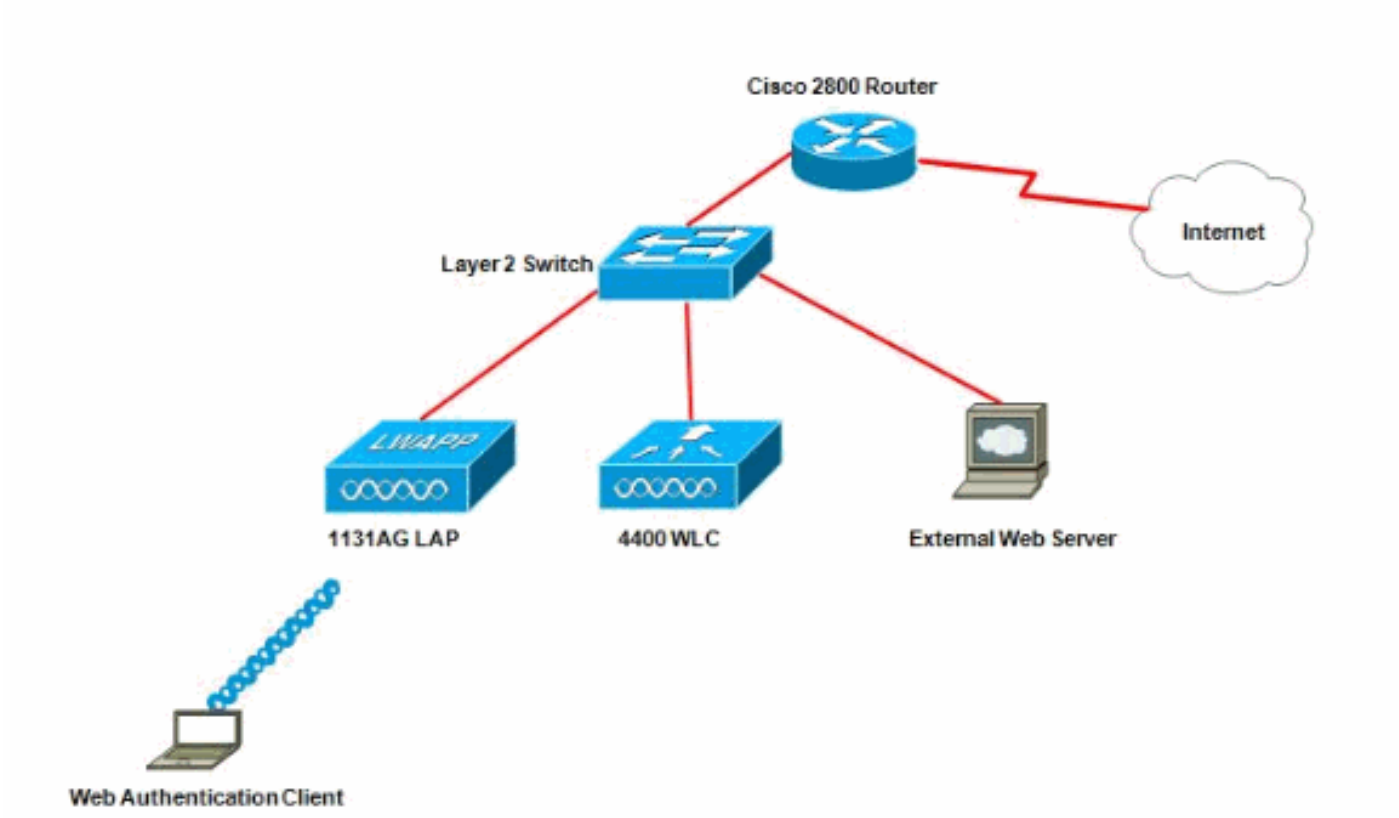
Configuration du réseau

L'exemple de configuration utilise cette configuration. Un LAP est enregistré auprès du WLC. Vous devez configurer un **invité** WLAN pour les utilisateurs invités et activer l'authentification Web pour

les utilisateurs. Vous devez également vous assurer que le contrôleur redirige l'utilisateur vers l'URL du serveur Web externe (pour l'authentification Web externe). Le serveur Web externe héberge la page de connexion Web utilisée pour l'authentification.

Les informations d'identification de l'utilisateur doivent être validées par rapport à la base de données locale gérée sur le contrôleur. Une fois l'authentification réussie, les utilisateurs doivent être autorisés à accéder à l'invité WLAN. Le contrôleur et les autres périphériques doivent être configurés pour cette configuration.

Remarque : vous pouvez utiliser une version personnalisée du script de connexion, qui sera utilisée pour l'authentification Web. Vous pouvez télécharger un exemple de script d'authentification Web à partir de la page Téléchargements de logiciels Cisco. Par exemple, pour les contrôleurs 4400, accédez à **Products > Wireless > Wireless LAN Controller > Standalone Controllers > Cisco 4400 Series Wireless LAN Controllers > Cisco 4404 Wireless LAN Controller > Software on Chassis > Wireless Lan Controller Web Authentication Bundle-1.0.1** et téléchargez le fichier **webauth_bundle.zip**.



Remarque : le bundle d'authentification Web personnalisé peut contenir jusqu'à 30 caractères pour les noms de fichiers. Assurez-vous qu'aucun nom de fichier dans le bundle ne dépasse 30 caractères.

Remarque : ce document suppose que les serveurs DHCP, DNS et Web externes sont configurés. Reportez-vous à la documentation tierce appropriée pour obtenir des informations sur la configuration du serveur DHCP, DNS et Web externe.

Configurer

Avant de configurer le WLC pour l'authentification Web externe, vous devez configurer le WLC pour le fonctionnement de base et enregistrer les LAP sur le WLC. Ce document suppose que WLC est configuré pour les opérations de base et que les LAP sont enregistrés au WLC. Référez-

vous à Enregistrement d'un point d'accès léger (LAP) à un contrôleur de réseau local sans fil (WLC) si vous êtes un nouvel utilisateur essayant de configurer le WLC pour un fonctionnement de base avec les LAP.

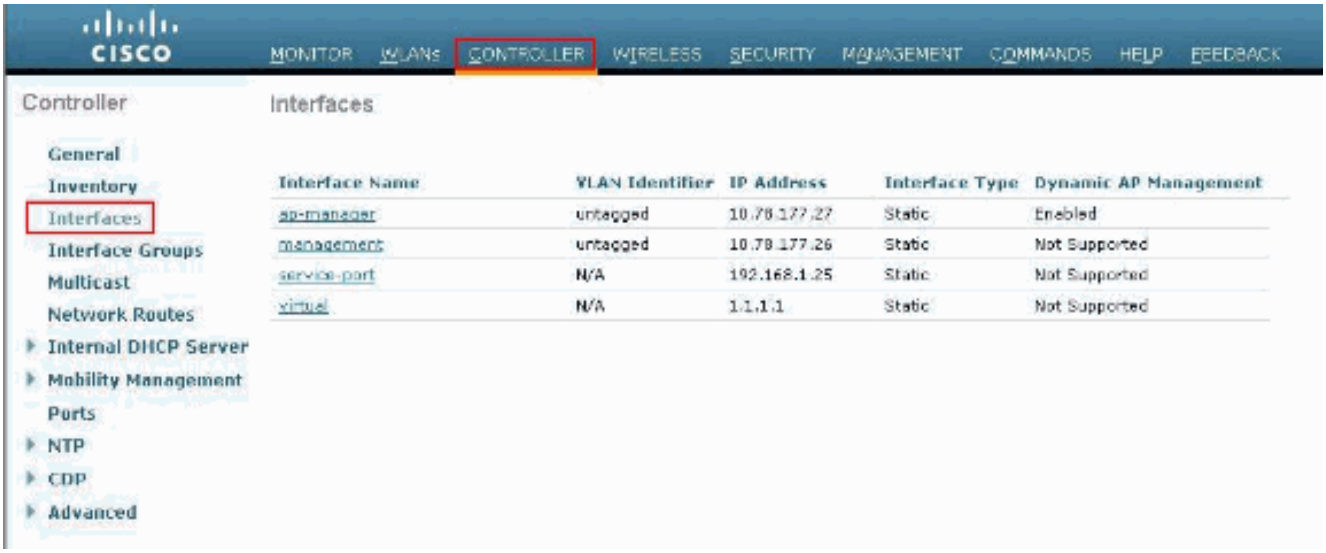
Complétez ces étapes afin de configurer les LAP et le WLC pour cette configuration :

1. Créer une interface dynamique pour les utilisateurs invités
2. Créer une ACL de préauthentification
3. Créer une base de données locale sur le WLC pour les utilisateurs invités
4. Configurer le WLC pour l'authentification Web externe
5. Configurer le WLAN pour les utilisateurs invités

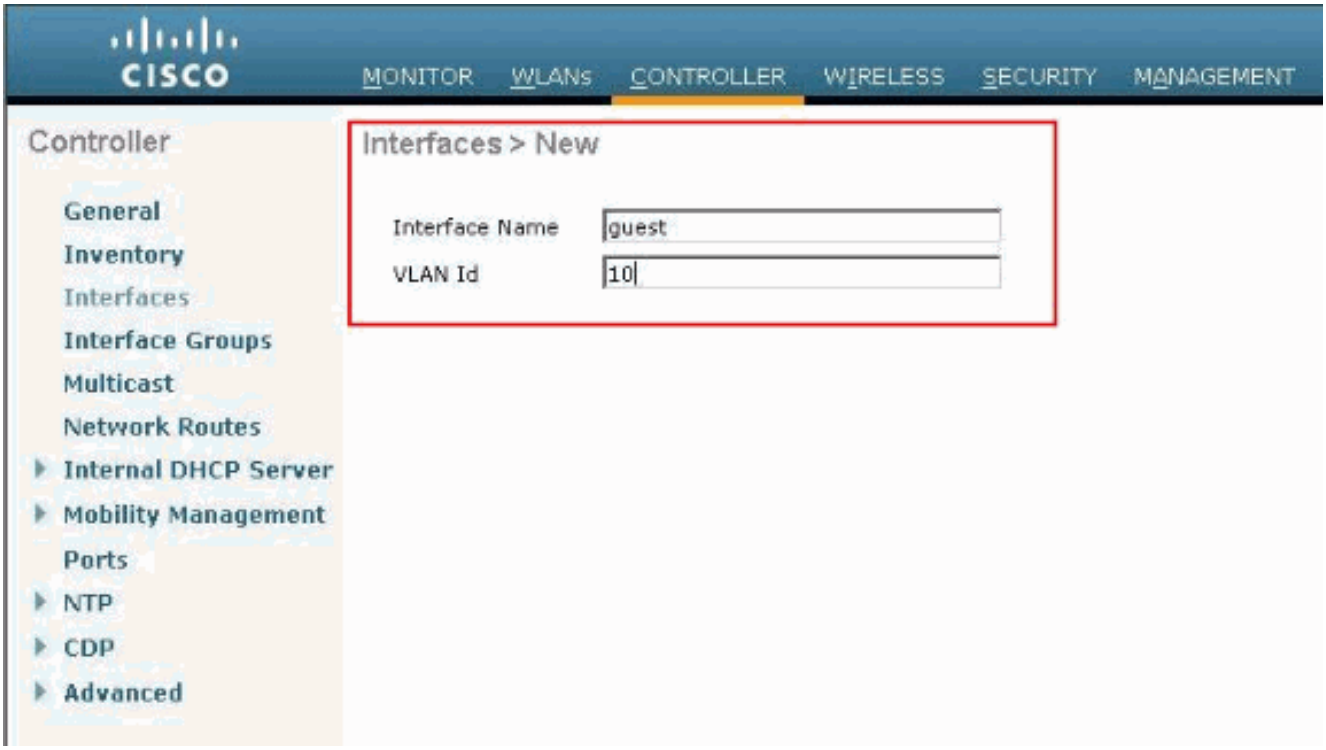
Créer une interface dynamique pour les utilisateurs invités

Complétez ces étapes afin de créer une interface dynamique pour les utilisateurs invités :

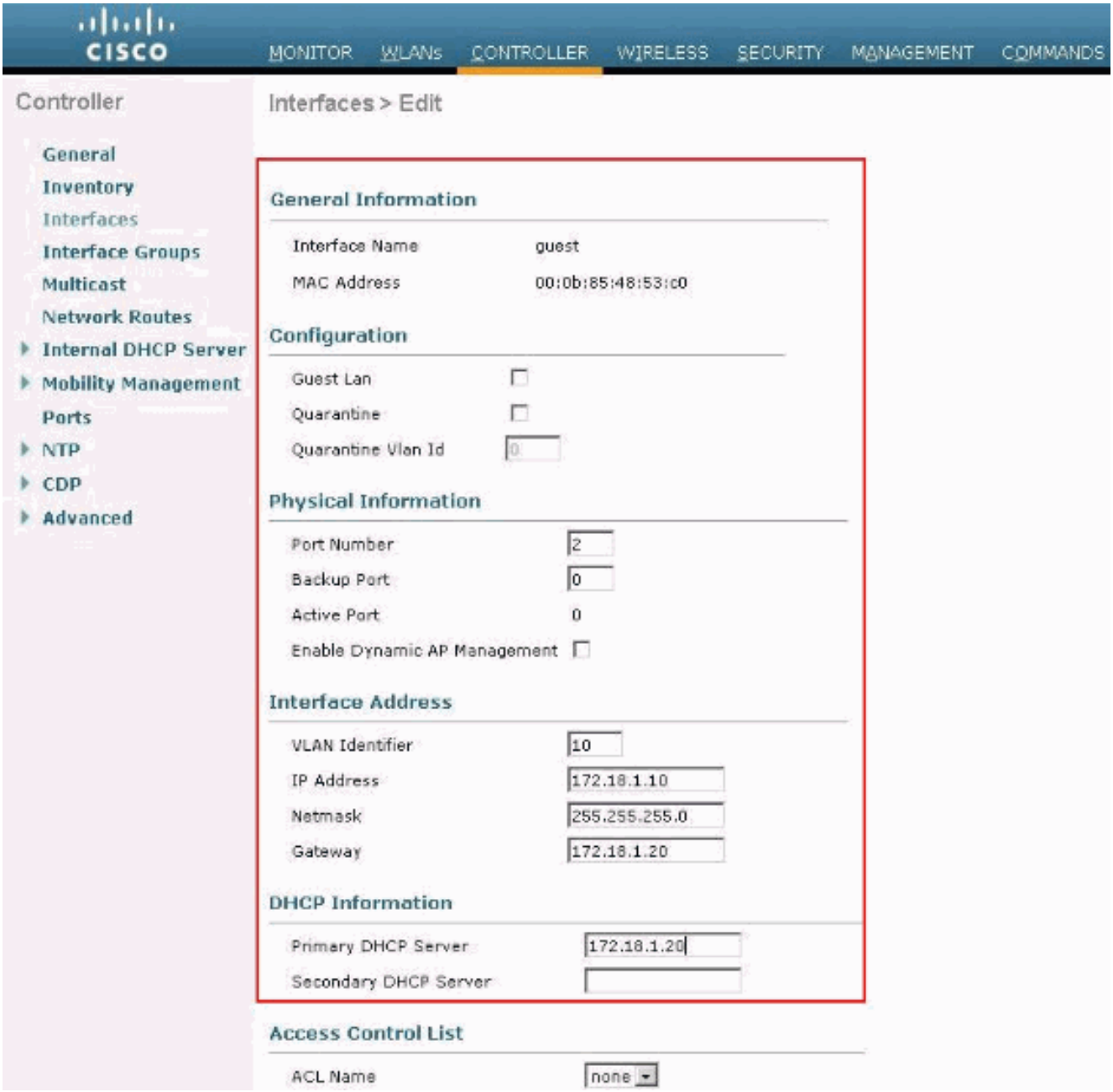
1. Àpartir de l'interface graphique utilisateur du WLC, choisir **Controller > Interfaces** [contrôleur > interfaces].La fenêtre Interfaces apparaît. Cette fenêtre liste les interfaces qui sont configurées sur le contrôleur. Les interfaces par défaut sont comprises, soit l'interface de gestion, l'interface de gestionnaire du point d'accès, l'interface virtuelle, l'interface du port de service et les interfaces dynamiques définies par l'utilisateur.



2. Afin de créer une nouvelle interface dynamique, cliquez sur **New.**
3. Dans la fenêtre Interfaces > New [interfaces > nouveau], entrer le nom de l'interface et l'identifiant du réseau VLAN. Cliquer ensuite sur **Apply** [appliquer].Dans cet exemple, l'interface dynamique est nommée **guest** et l'ID de VLAN est attribué à **10**.



4. Dans la fenêtre Interfaces > Edit [interfaces > modifier], pour l'interface dynamique, saisir l'adresse IP, le masque de sous-réseau et la passerelle par défaut. Attribuez-la à un port physique sur le WLC et entrez l'adresse IP sur le serveur DHCP. Cliquez ensuite sur Apply.



Créer une ACL de préauthentification

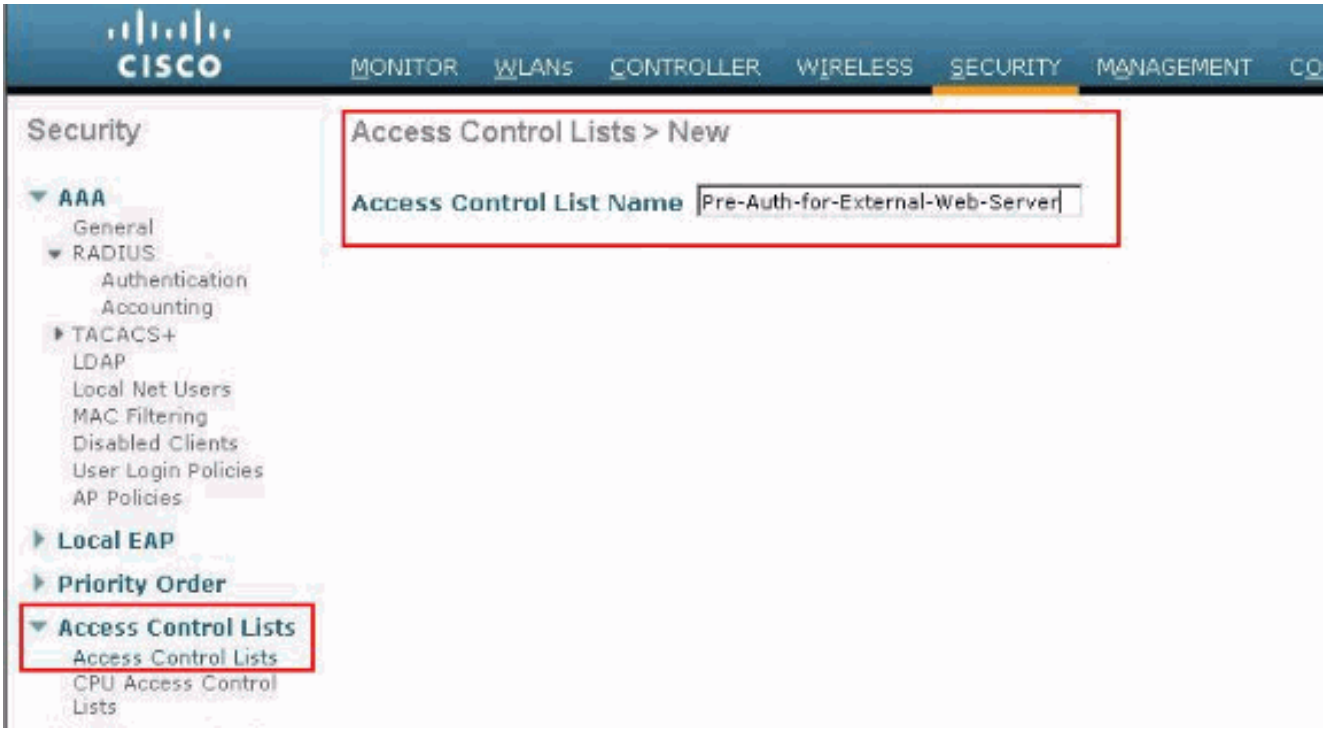
Lorsque vous utilisez un serveur Web externe pour l'authentification Web, certaines plates-formes WLC ont besoin d'une liste de contrôle d'accès de pré-authentification pour le serveur Web externe (le contrôleur de la gamme Cisco 5500, un contrôleur de la gamme Cisco 2100, la gamme Cisco 2000 et le module de réseau du contrôleur). Pour les autres plates-formes WLC, la liste de contrôle d'accès de pré-authentification n'est pas obligatoire.

Cependant, il est recommandé de configurer une liste de contrôle d'accès de préauthentification pour le serveur Web externe lors de l'utilisation de l'authentification Web externe.

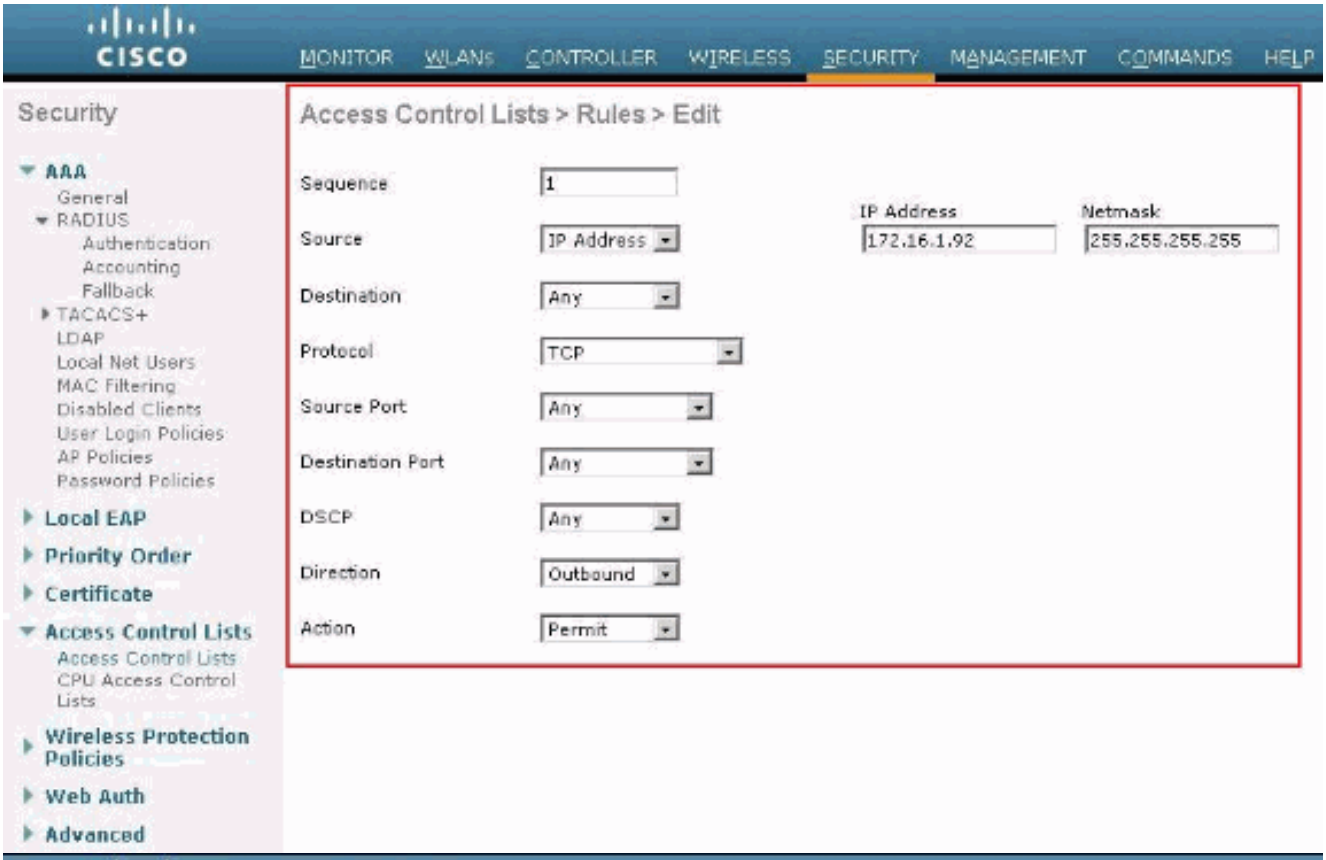
Complétez ces étapes afin de configurer la liste de contrôle d'accès de pré-authentification pour le WLAN :

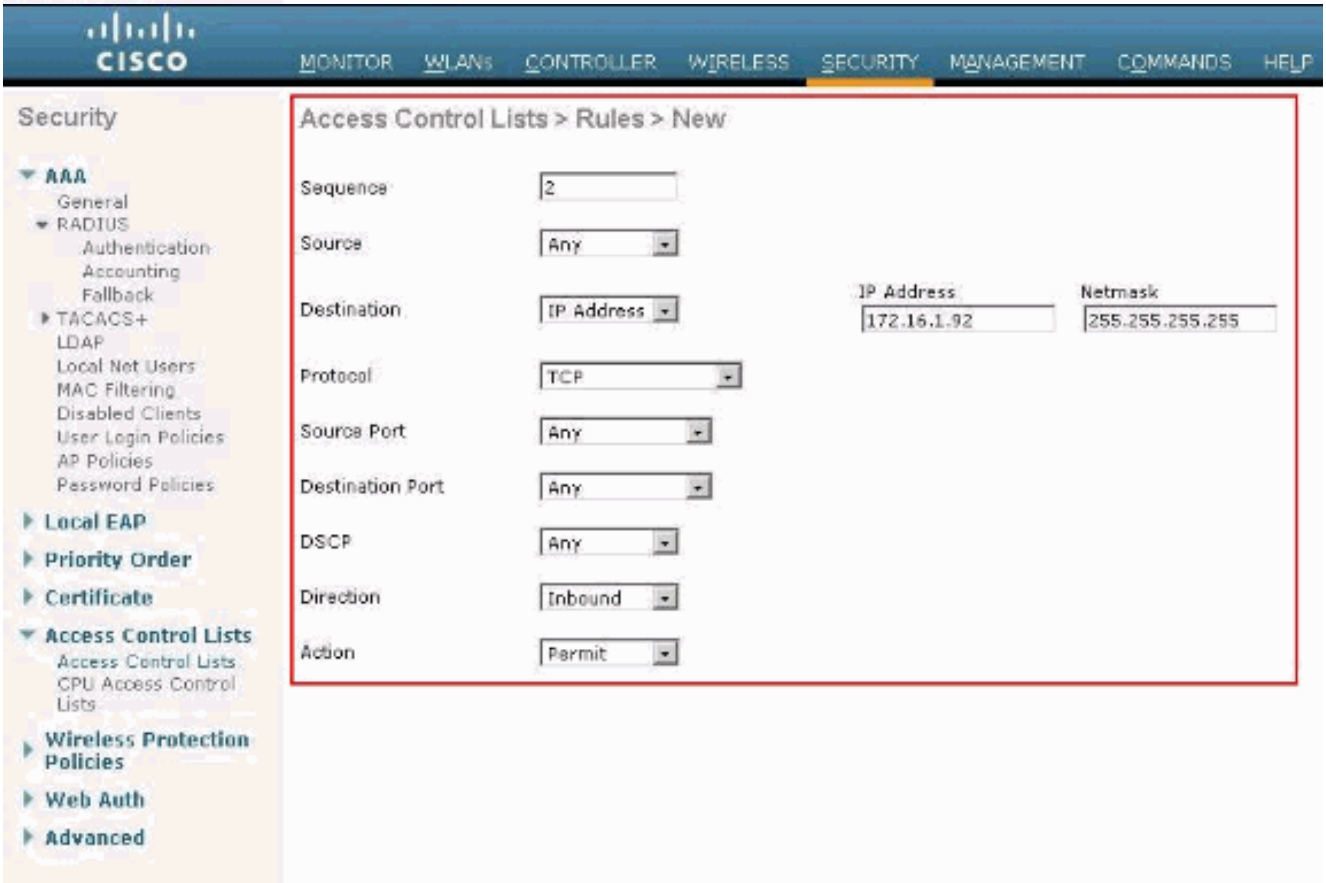
1. Dans l'interface graphique du WLC, choisissez **Security > Access Control Lists**.Cette fenêtre vous permet d'afficher les listes de contrôle d'accès actuelles similaires aux listes de contrôle d'accès de pare-feu standard.

2. Cliquez sur **New** afin de créer une nouvelle ACL.
3. Entrez le nom de la liste de contrôle d'accès et cliquez sur **Apply**.Dans cet exemple, la liste de contrôle d'accès est nommée **Pre-Auth-for-External-Web-Server**.

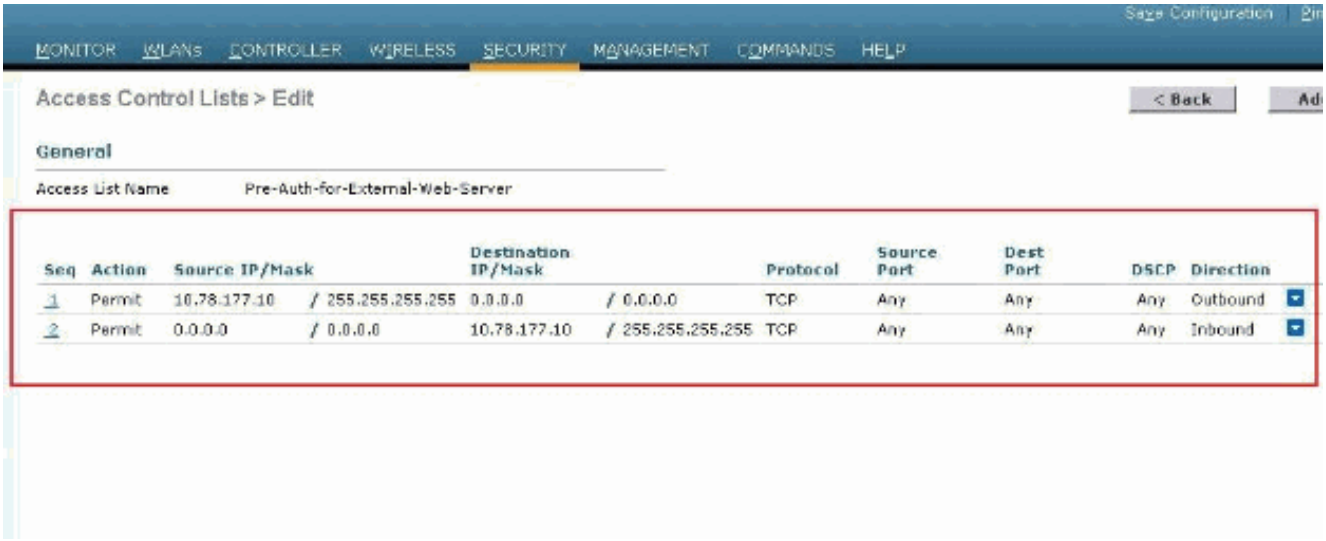


4. Pour la nouvelle liste de contrôle d'accès créée, cliquez sur **Edit**.La fenêtre ACL > Edit s'affiche. Cette fenêtre permet à l'utilisateur de définir de nouvelles règles ou de modifier les règles existantes de la liste de contrôle d'accès.
5. Cliquez sur **Ajouter une nouvelle règle**.
6. Définissez une règle de liste de contrôle d'accès qui autorise l'accès des clients au serveur Web externe.Dans cet exemple, 172.16.1.92 est l'adresse IP du serveur Web externe.





7. Cliquez sur **Apply** afin de valider les modifications.

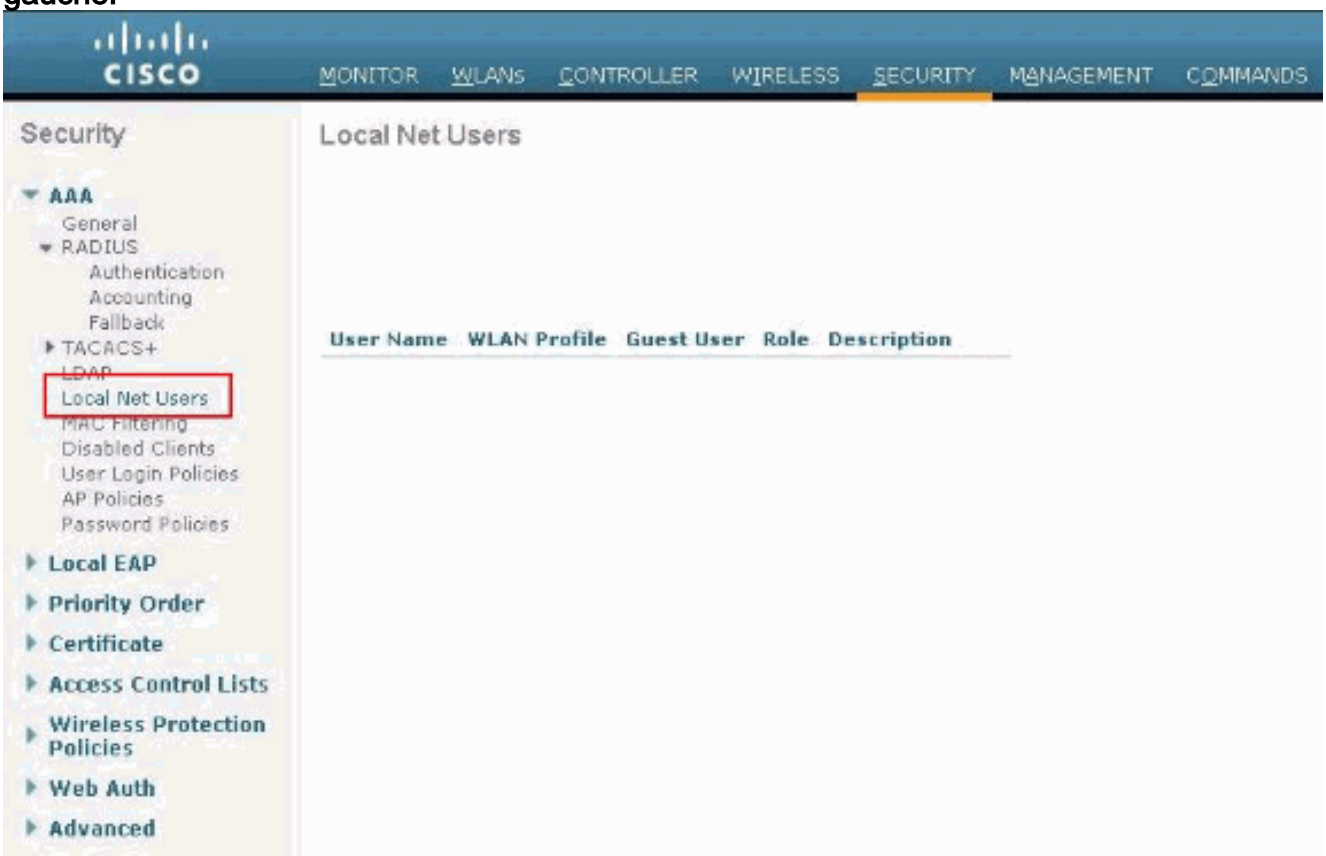


Créer une base de données locale sur le WLC pour les utilisateurs invités

La base de données utilisateur des utilisateurs invités peut être stockée dans la base de données locale du contrôleur de réseau local sans fil ou peut être stockée à l'extérieur du contrôleur.

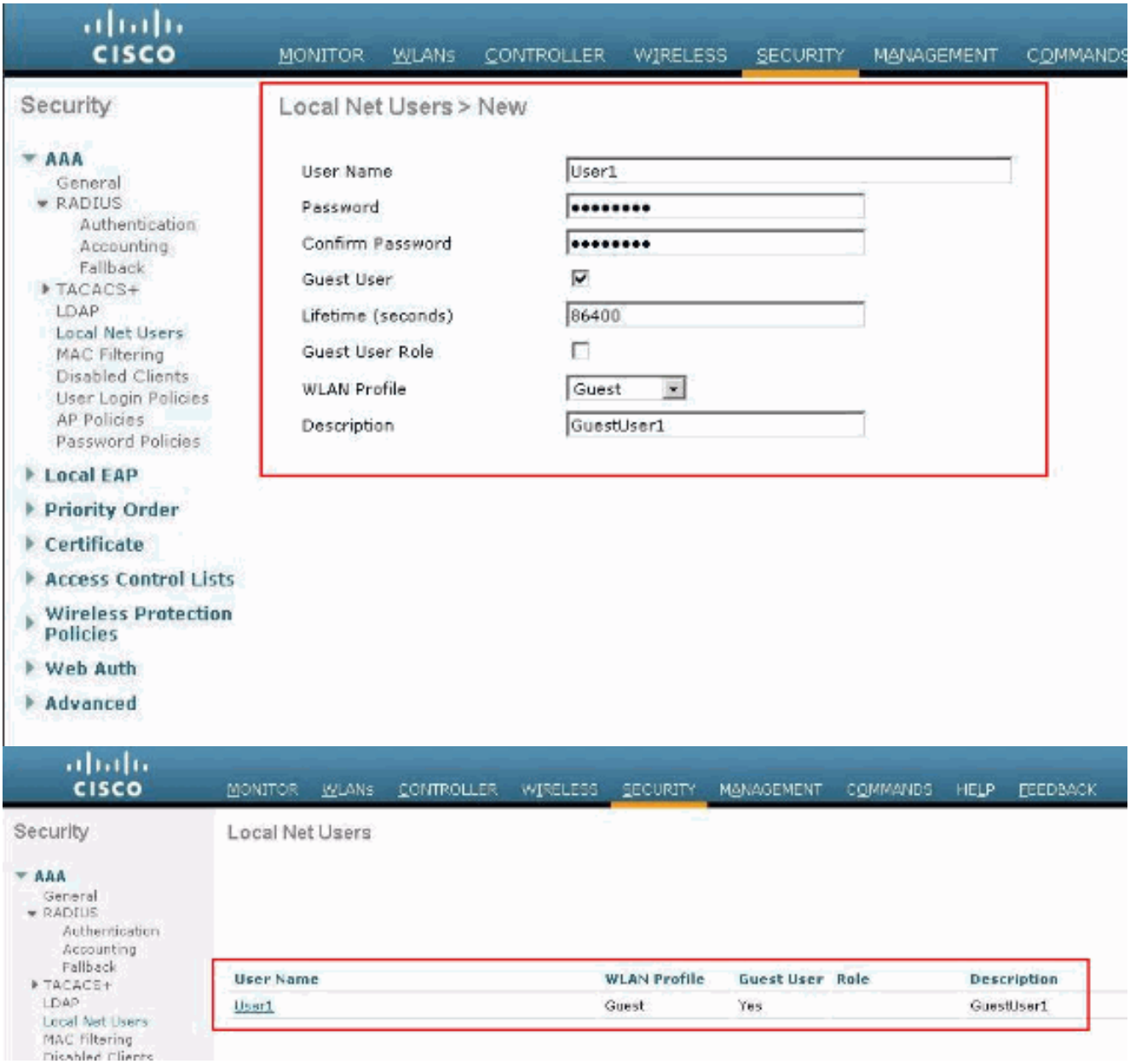
Dans ce document, la base de données locale sur le contrôleur est utilisée pour authentifier les utilisateurs. Vous devez créer un utilisateur du réseau local et définir un mot de passe pour la connexion du client d'authentification Web. Complétez ces étapes afin de créer la base de données utilisateur sur le WLC :

1. Àpartir de l'interface GUI du WLC, sélectionnez **Sécurité**.
2. Cliquez sur **Utilisateurs du réseau local dans le menuAAA à gauche.**



3. Cliquez sur Nouveau afin de créer un utilisateur.Une nouvelle fenêtre s'affiche pour demander les informations de nom d'utilisateur et de mot de passe.

4. Entrez un nom d'utilisateur et un mot de passe afin de créer un nouvel utilisateur, puis confirmez le mot de passe que vous voulez utiliser.Cet exemple crée l'utilisateur nommé **Utilisateur1**.
5. Ajoutez une description, le cas échéant.Cet exemple se sert de l'**utilisateur invité 1**.
6. Cliquez sur Apply pour sauvegarder la nouvelle configuration utilisateur.



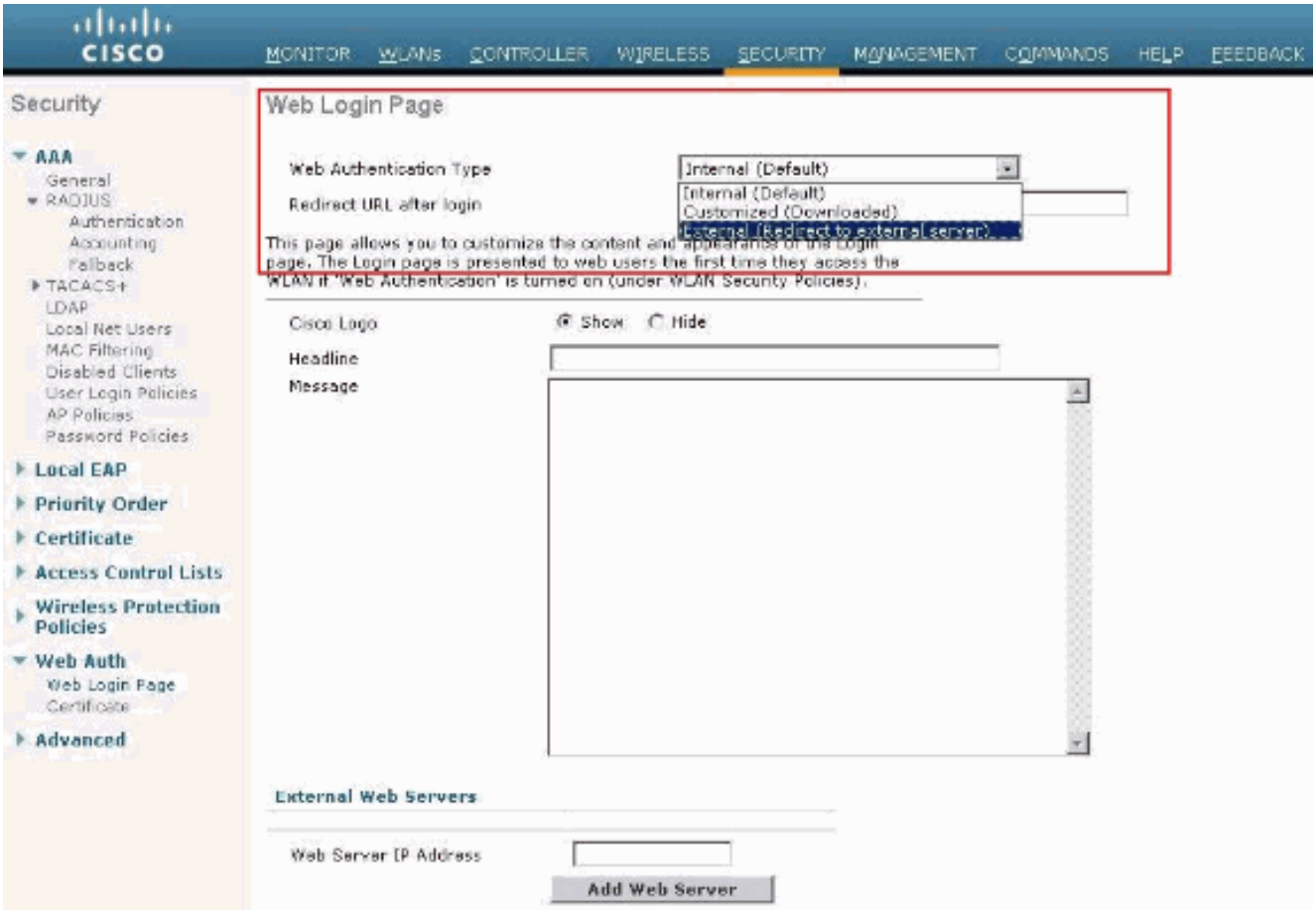
7. Répétez les étapes 3 à 6 pour ajouter plus d'utilisateurs à la base de données.

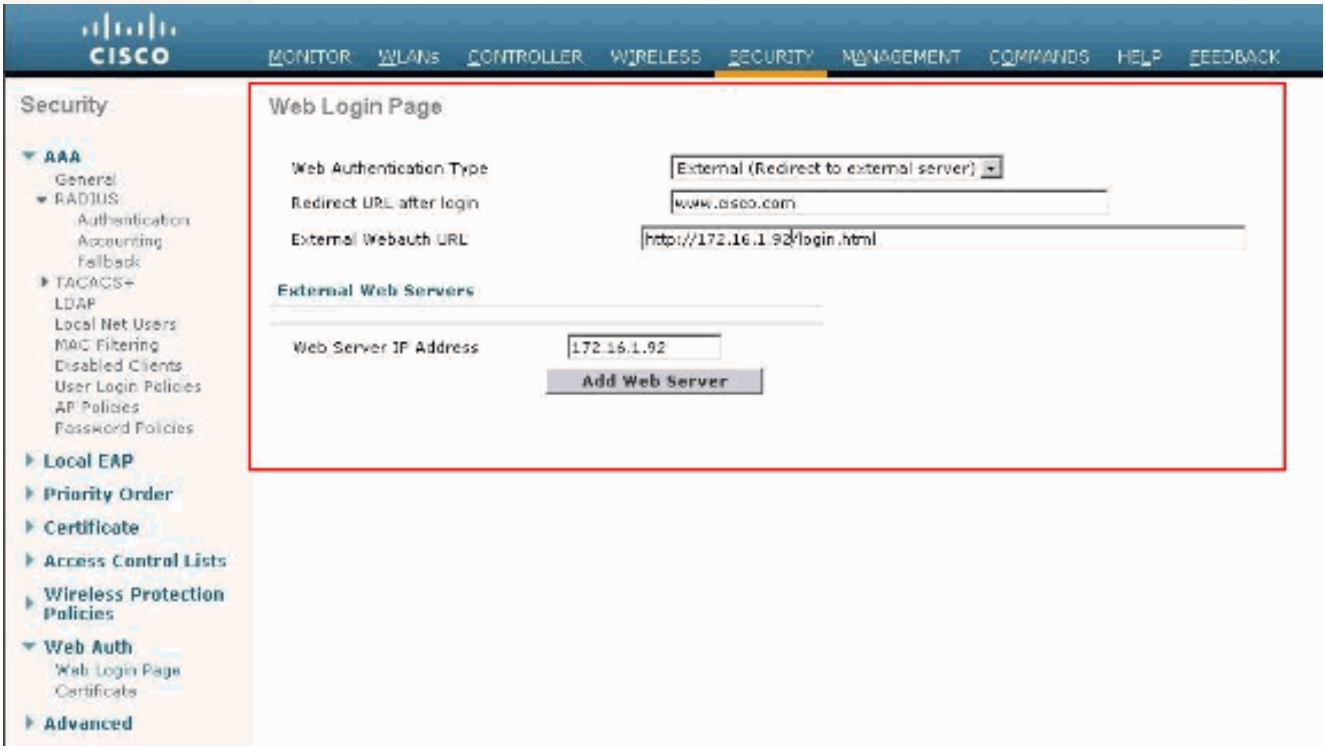
Configurer le WLC pour l'authentification Web externe

L'étape suivante consiste à configurer le WLC pour l'authentification Web externe. Procédez comme suit :

1. Àpartir de l'interface GUI de contrôleur, sélectionnez**Sécurité > Authentification Web > Page de connexion Web afin d'accéder à la page de connexion.**
2. Dans la liste déroulante Web Authentication Type, sélectionnez **External (Redirect to external server)**.
3. Dans la section **Serveur Web externe**, ajoutez le nouveau serveur Web externe.
4. Dans le champ **Redirect URL after login**, saisissez l'URL de la page vers laquelle l'utilisateur

final sera redirigé une fois l'authentification réussie. Dans le champ **External Web Auth URL**, entrez l'URL où la page de connexion est stockée sur le serveur Web externe.



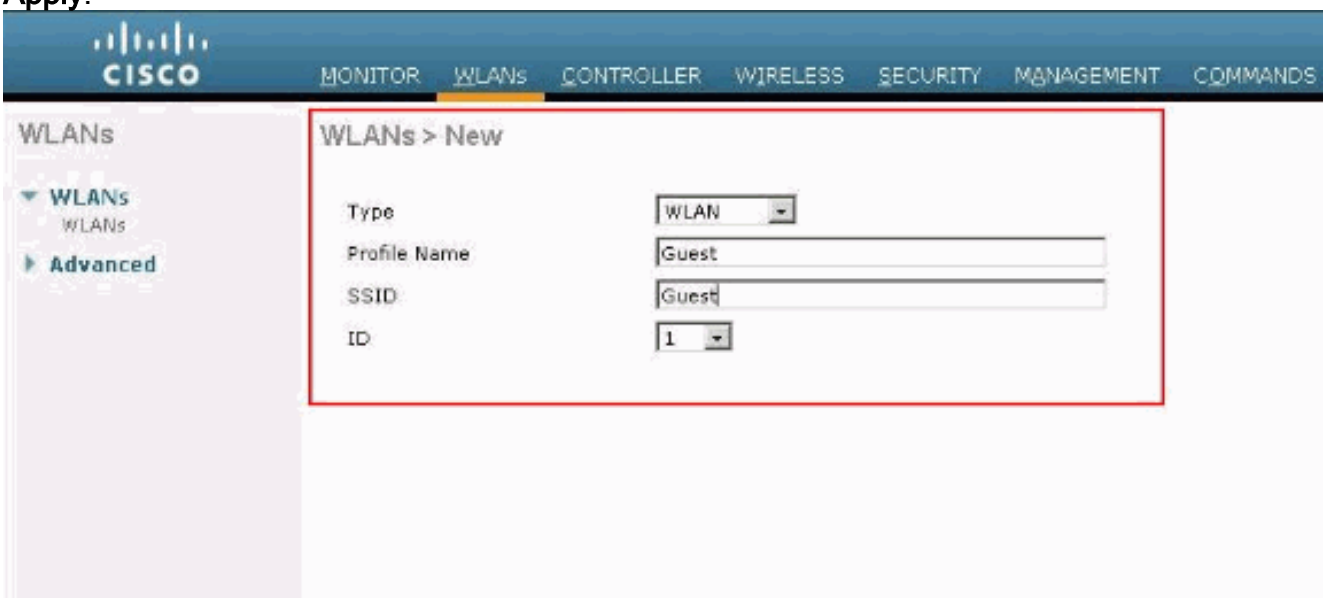


Remarque : dans les versions 5.0 et ultérieures du WLC, la page de déconnexion pour l'authentification Web peut également être personnalisée. Référez-vous à la section Attribuer une connexion , Échec de connexion et Déconnexion par WLAN du *Guide de configuration du contrôleur de réseau local sans fil, 5.2* pour plus d'informations sur la façon de le configurer.

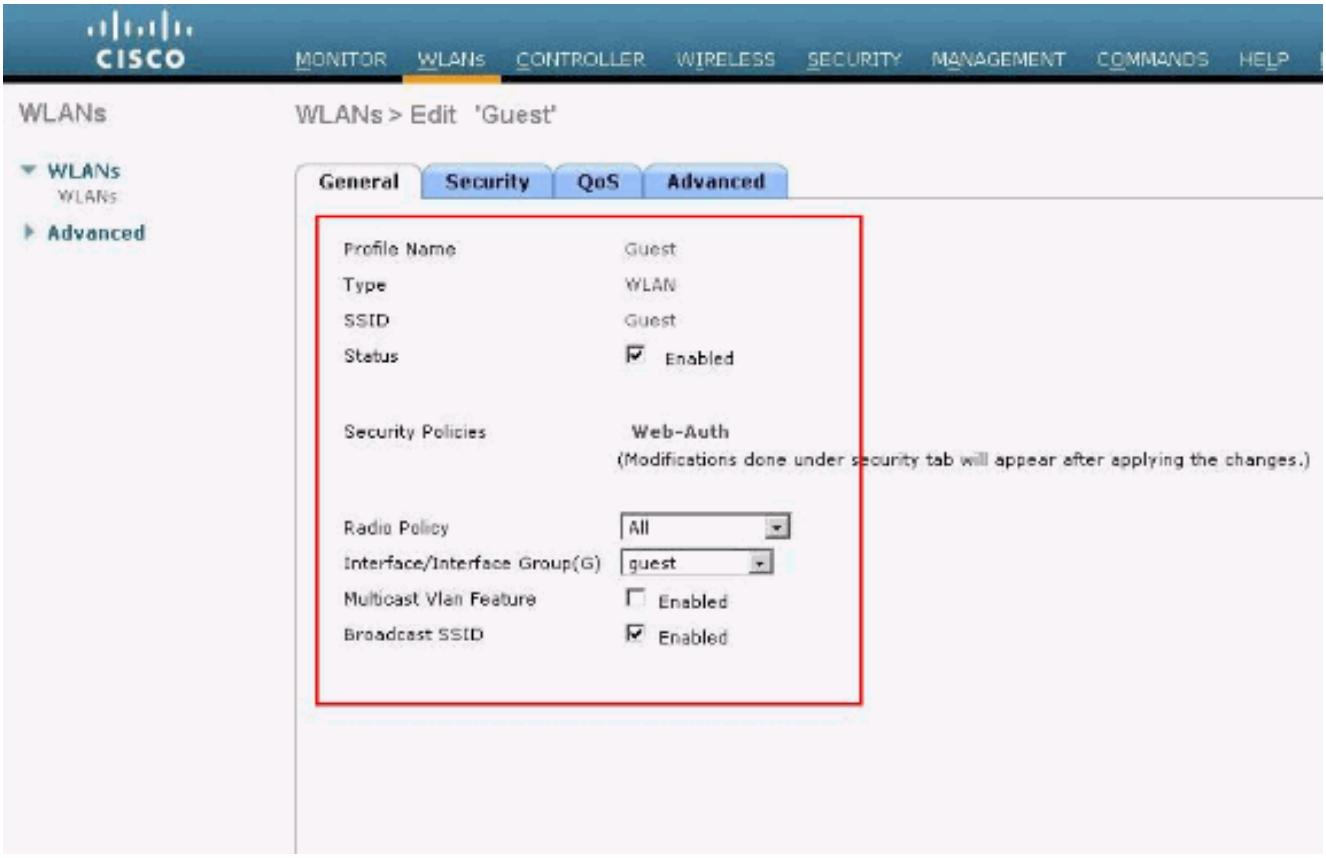
Configurer le WLAN pour les utilisateurs invités

La dernière étape consiste à créer des réseaux locaux sans fil pour les utilisateurs invités. Procédez comme suit :

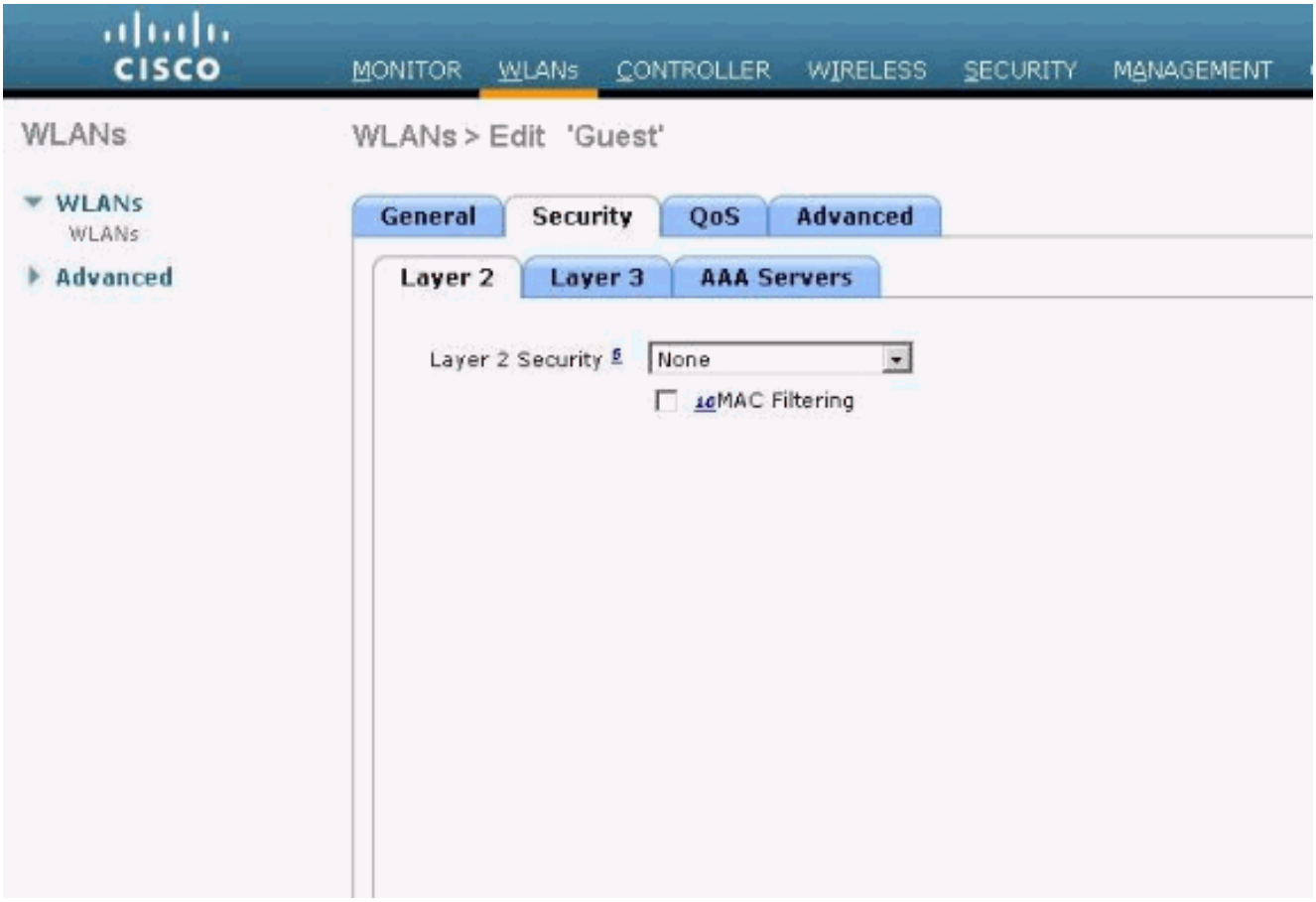
1. Cliquez sur **WLANs depuis l'interface utilisateur graphique (GUI) du contrôleur afin de créer un WLAN.**La fenêtre de WLAN s'affiche. Cette fenêtre répertorie les WLAN configurés sur le contrôleur.
2. Cliquez sur **New pour configurer un nouveau WLAN.**Dans l'exemple-ci, le WLAN est désigné **invité** et son identifiant est 1.
3. Cliquez sur
   Apply.



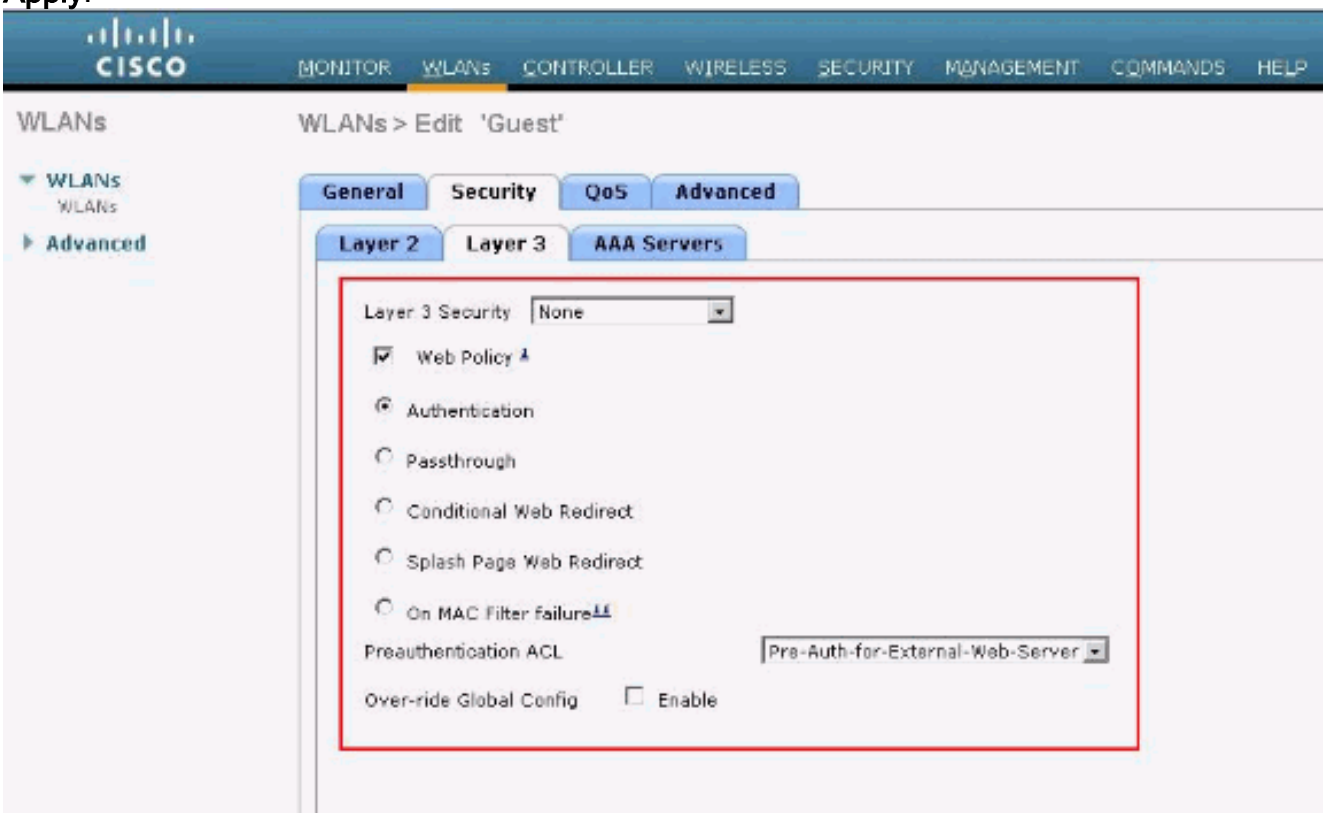
4. Dans la fenêtre WLAN > Edit, définissez les paramètres spécifiques au WLAN.Pour le WLAN invité, dans l'onglet General, sélectionnez l'interface appropriée dans le champ Interface Name.Cet exemple mappe l'**invité de l'**interface dynamique qui a été précédemment créé à l'invité
   WLAN.



Accédez à l'onglet Sécurité. Sous Layer 2 Security, **None** est sélectionné dans cet exemple.**Remarque : l'**authentification Web n'est pas prise en charge avec l'authentification 802.1x. Cela signifie que vous ne pouvez pas choisir 802.1x ou un WPA/WPA2 avec 802.1x comme sécurité de couche 2 lorsque vous utilisez l'authentification Web.L'authentification Web est prise en charge avec tous les autres paramètres de sécurité de couche 2.



Dans le champ Layer 3 Security, cochez la case **Web Policy** et choisissez l'option **Authentication**.Cette option est sélectionnée car l'authentification Web est utilisée pour authentifier les clients invités sans fil.Sélectionnez la liste de contrôle d'accès de préauthentification appropriée dans le menu déroulant.Dans cet exemple, la liste de contrôle d'accès de préauthentification créée précédemment est utilisée.Cliquez sur **Apply**.

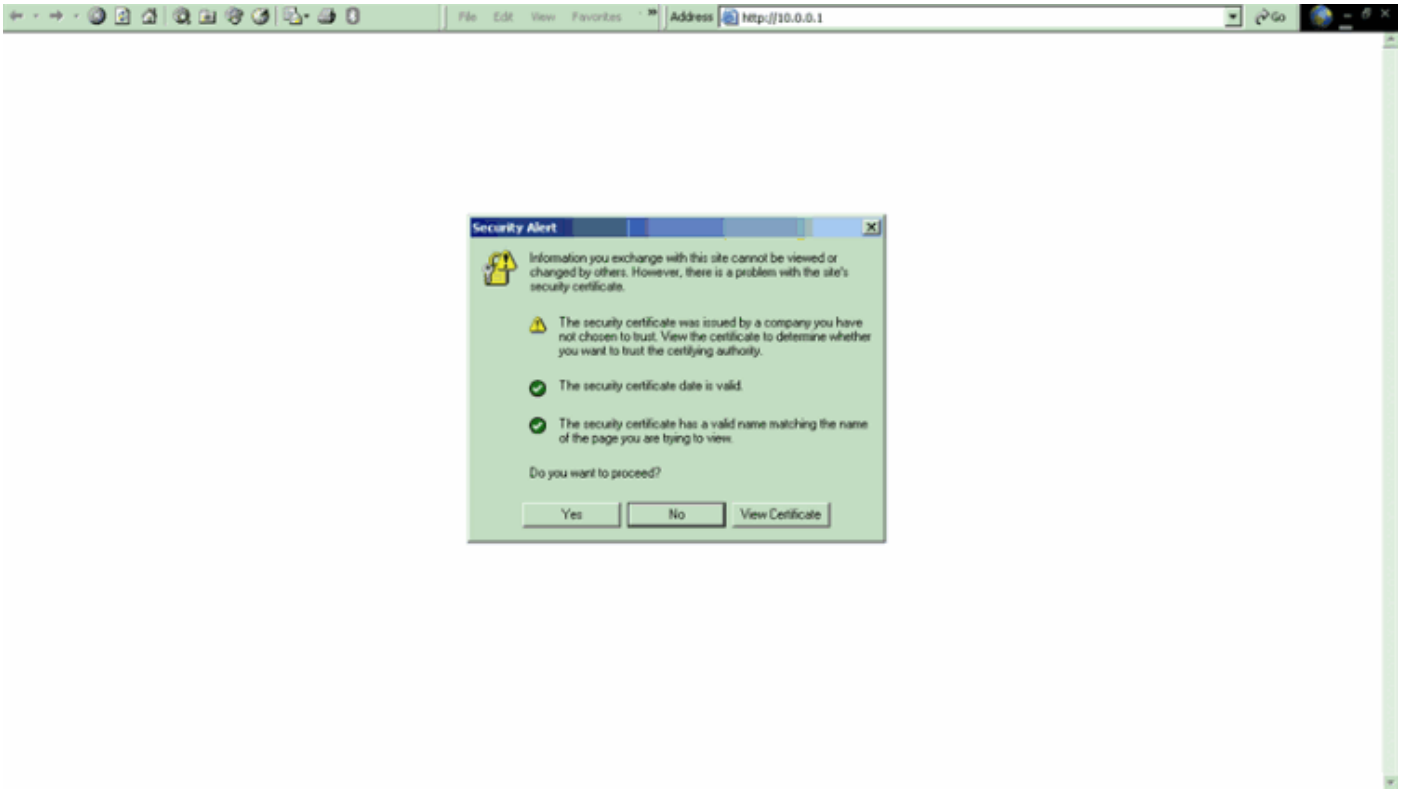


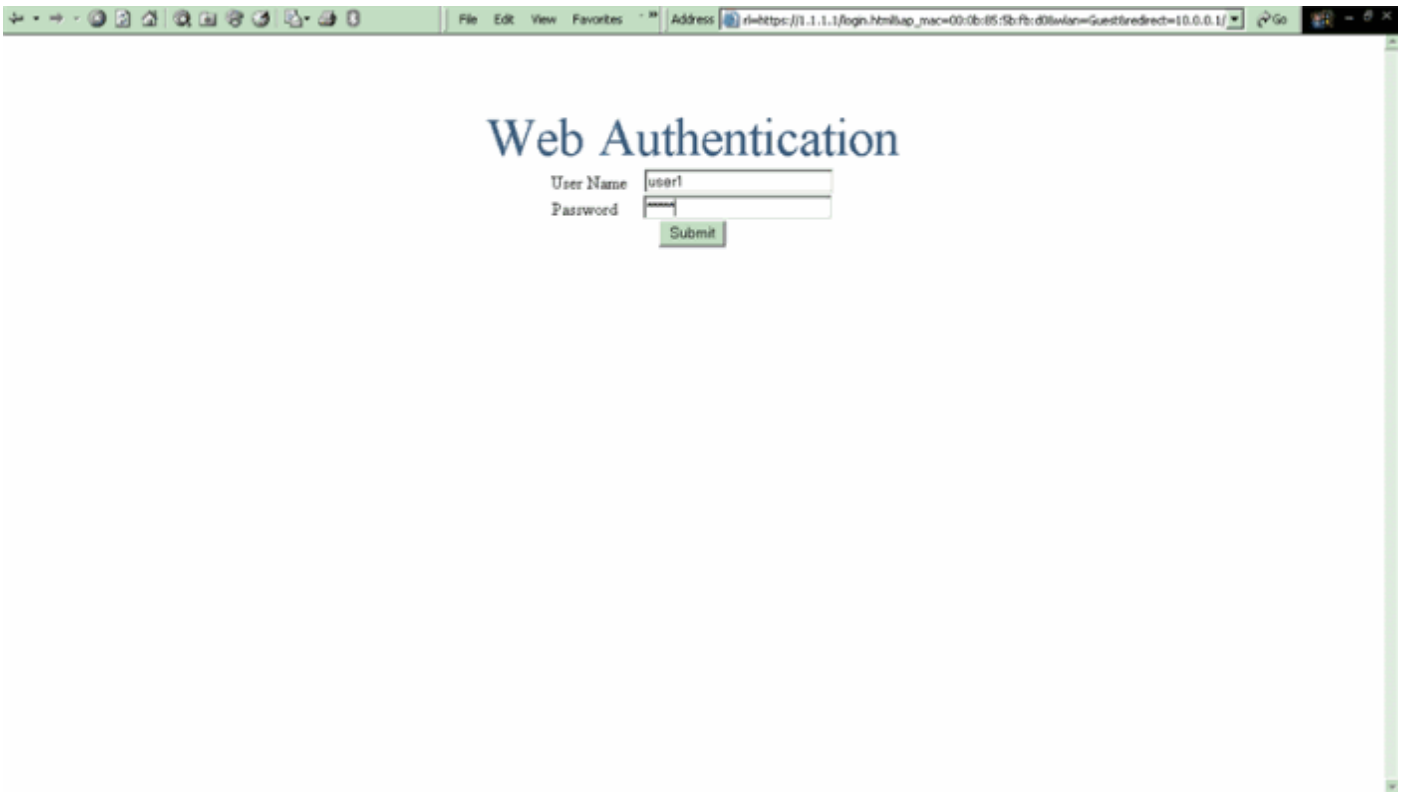
Vérifier

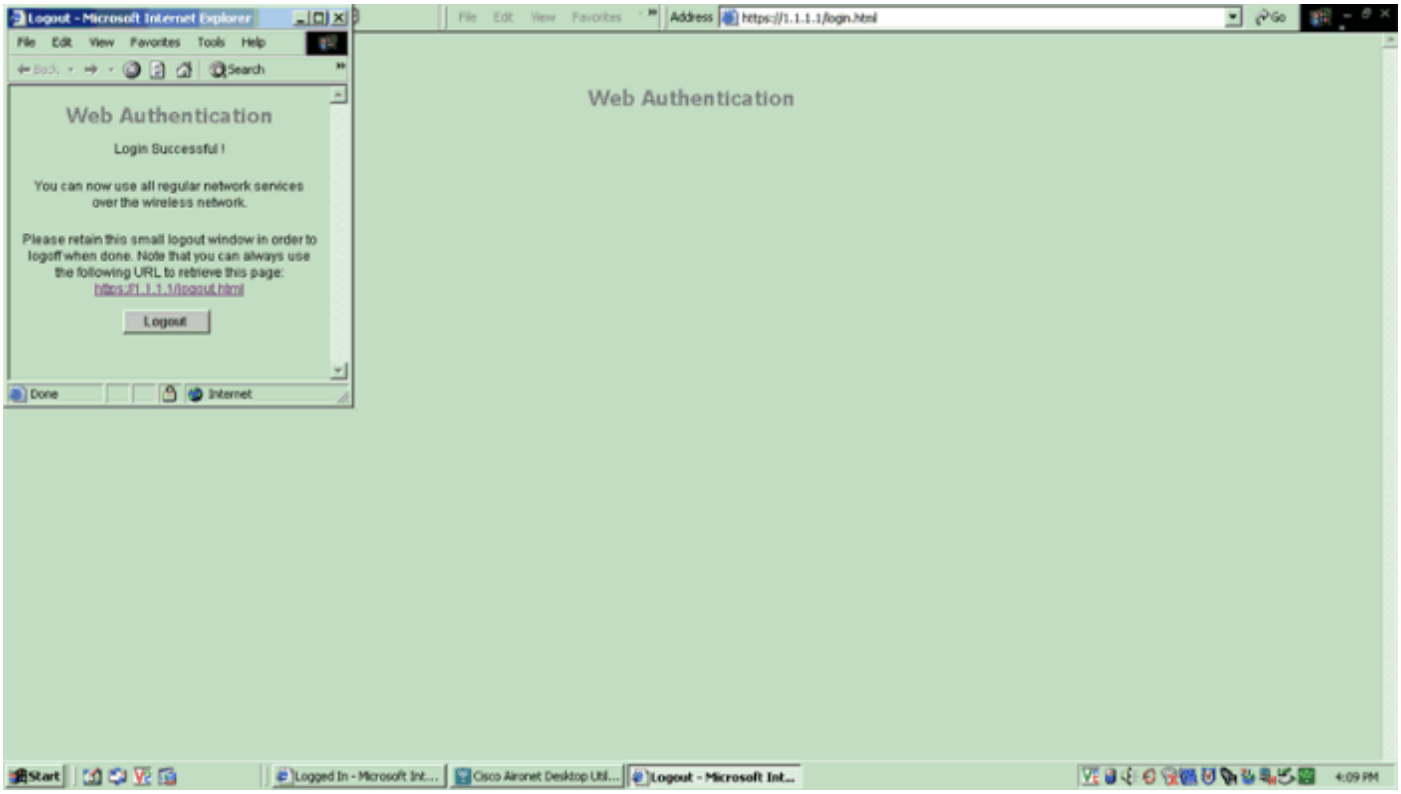
Le client sans fil apparaît et l'utilisateur saisit l'URL, par exemple www.cisco.com, dans le navigateur Web. Comme l'utilisateur n'a pas été authentifié, le WLC redirige l'utilisateur vers l'URL de connexion Web externe.

L'utilisateur est invité à saisir ses informations d'identification. Une fois que l'utilisateur envoie le nom d'utilisateur et le mot de passe, la page de connexion prend les informations d'identification de l'utilisateur et, lors de l'envoi, renvoie la demande à l'exemple action_URL, http://1.1.1.1/login.html, du serveur Web WLC. Il s'agit d'un paramètre d'entrée pour l'URL de redirection du client, où 1.1.1.1 est l'adresse d'interface virtuelle sur le commutateur.

Le WLC authentifie l'utilisateur par rapport à la base de données locale configurée sur le WLC. Une fois l'authentification réussie, le serveur Web du WLC transfère l'utilisateur à l'URL de redirection configurée ou à l'URL avec laquelle le client a commencé, telle que www.cisco.com.


File Edit View Favorites
Address http://10.0.0.1
Security Alert
Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.
The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.
The security certificate date is valid.
The security certificate has a valid name matching the name of the page you are trying to view.
Do you want to proceed?
Yes
No
View Certificate


File Edit View Favorites
Address rl=https://1.1.1.1/login.html&ap_mac=00:0b:85:5b:fb:d0&wlan=Guest&redirect=10.0.0.1/
Web Authentication
User Name user1
Password
Submit



Dépannage

Utilisez ces commandes debug afin de dépanner votre configuration.

- debug mac addr <adresse MAC du client xx:xx:xx:xx:xx:xx>
- debug aaa all enable
- debug pem state enable
- debug pem events enable
- debug dhcp message enable
- debug dhcp packet enable
- debug pm ssh-appgw enable
- debug pm ssh-tcp enable

Utilisez cette section pour dépanner votre configuration.

Les clients redirigés vers un serveur d'authentification Web externe reçoivent un avertissement de certificat

Problème : lorsque les clients sont redirigés vers le serveur d'authentification Web externe de Cisco, ils reçoivent un avertissement de certificat. Il existe un certificat valide sur le serveur et si vous vous connectez directement au serveur d'authentification Web externe, l'avertissement de certificat n'est pas reçu. Est-ce parce que l'adresse IP virtuelle (1.1.1.1) du WLC est présentée au client au lieu de l'adresse IP réelle du serveur d'authentification Web externe qui est associé au certificat ?

Solution : Oui. Que vous effectuiez ou non une authentification Web locale ou externe, vous continuez à accéder au serveur Web interne sur le contrôleur. Lorsque vous redirigez vers un serveur Web externe, vous recevez toujours l'avertissement de certificat du contrôleur, sauf si vous avez un certificat valide sur le contrôleur lui-même. Si la redirection est envoyée à https, vous recevez l'avertissement de certificat du contrôleur et du serveur Web externe, sauf si les

deux ont un certificat valide.

Afin de vous débarrasser de tous les avertissements de certificat, vous devez avoir un certificat de niveau racine émis et téléchargé sur votre contrôleur. Le certificat est émis pour un nom d'hôte et vous placez ce nom d'hôte dans la zone Nom d'hôte DNS sous l'interface virtuelle sur le contrôleur. Vous devez également ajouter le nom d'hôte à votre serveur DNS local et le pointer vers l'adresse IP virtuelle (1.1.1.1) du WLC.

Référez-vous à Génération de demande de signature de certificat (CSR) pour un certificat tiers sur un contrôleur WLAN (WLC) pour plus d'informations.

Erreur : "la page ne peut pas être affichée"

Problème : Une fois le contrôleur mis à niveau vers 4.2.61.0, le message d'erreur « page cannot be display » s'affiche lorsque vous utilisez une page Web téléchargée pour l'authentification Web. Cela a bien fonctionné avant la mise à niveau. La page Web interne par défaut se charge sans problème .

Solution : à partir de la version 4.2 et ultérieure du WLC, une nouvelle fonctionnalité est introduite dans laquelle vous pouvez avoir plusieurs pages de connexion personnalisées pour l'authentification Web.

Pour que la page Web se charge correctement, il ne suffit pas de définir le type d'authentification Web comme **personnalisé** globalement dans la **page Security > Web Auth > Web login**. Il doit également être configuré sur un WLAN particulier . Pour ce faire, suivez ces étapes :

1. Connectez-vous à l'interface utilisateur graphique du WLC.
2. Cliquez sur l'onglet **WLANs**, et accédez au profil du WLAN configuré pour l'authentification Web.
3. Sur la page WLAN > Edit, cliquez sur l'onglet **Security**. Ensuite, choisissez **Layer 3.**
4. Sur cette page, choisissez **None** comme niveau de sécurité de la couche 3.
5. Cochez la case **Web Policy** et choisissez l'option **Authentication**.
6. Cochez la case Override Global Config **Enable**, choisissez **Customized (Downloaded)** comme type d'authentification Web et sélectionnez la page de connexion souhaitée dans le menu déroulant de la page de **connexion**. Cliquez sur **Apply**.

Informations connexes

- Exemple de configuration de l'authentification Web sur un contrôleur de réseau local sans fil
- Vidéo : Authentification Web sur les contrôleurs LAN sans fil (WLC) Cisco
- Exemple de configuration de réseaux VLAN sur des contrôleurs de réseau local sans fil
- Exemple de configuration de base d'un contrôleur LAN sans fil et d'un point d'accès léger
- Assistance et documentation techniques - Cisco Systems

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.

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.