Authentification de serveur de RAYON des utilisateurs de Gestion sur l'exemple Sans fil de configuration du contrôleur LAN (WLC)

Contenu

Introduction

Ce document explique comment configurer un contrôleur de réseau local sans fil (WLC) et un serveur de contrôle d'accès (Cisco Secure ACS) de sorte que le serveur d'AAA puisse authentifier des utilisateurs gestionnairs sur le contrôleur. Le document explique également comment les différents utilisateurs gestionnaires peuvent recevoir différents privilèges en utilisant les attributs spécifiques du fournisseur (VSA) retournés du serveur Cisco Secure ACS RADIUS.

Conditions préalables

Conditions requises

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

- La connaissance de la façon configurer des paramètres de base sur WLCs
- La connaissance de la façon configurer un serveur de RAYON comme le Cisco Secure ACS

Composants utilisés

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

logiciel suivantes :

- Contrôleur LAN de radio de Cisco 4400 qui exécute la version 7.0.216.0
- Un Cisco Secure ACS qui exécute la version de logiciel 4.1 et est utilisé en tant que serveur de RAYON dans cette configuration.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

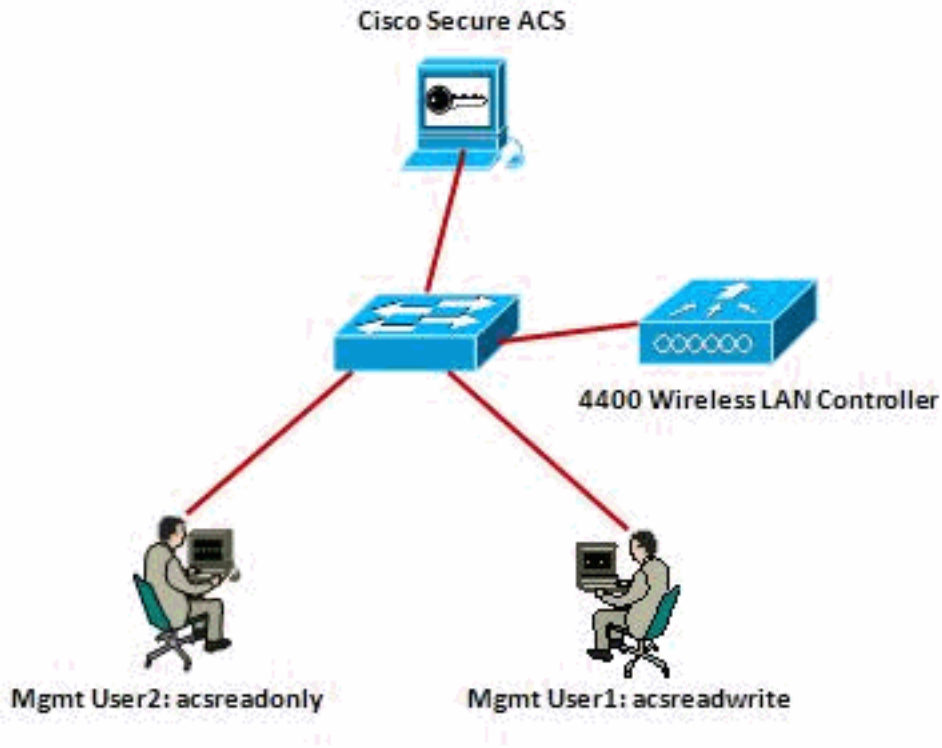
Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Configurez

Dans cette section, vous êtes présenté avec les informations sur la façon dont configurer le WLC et l'ACS pour le but décrit dans ce document.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Cet exemple de configuration utilise ces paramètres :

- Adresse IP du Cisco Secure ACS — 172.16.1.1/255.255.0.0

- Adresse IP d'interface de gestion du contrôleur — 172.16.1.30/255.255.0.0
- Clé secrète partagée qui est utilisée sur le Point d'accès (AP) et le serveur de RAYON — asdf1234
- Ce sont les qualifications des deux utilisateurs que cet exemple configure sur l'ACS :Nom d'utilisateur - acsreadwriteMot de passe - acsreadwriteNom d'utilisateur - acsreadonlyMot de passe - acsreadonly

Vous devez configurer le WLC et le Cisco Secure ACS Cisco Secure :

- Tout utilisateur qui se connecte dans le WLC avec le nom d'utilisateur et mot de passe pendant que l'**acsreadwrite** est donné le plein accès administratif au WLC.
- N'importe quel utilisateur qui se connecte dans le WLC avec le nom d'utilisateur et mot de passe comme **acsreadonly** est donné l'accès en lecture seule au WLC.

Configurations

Ce document utilise les configurations suivantes :

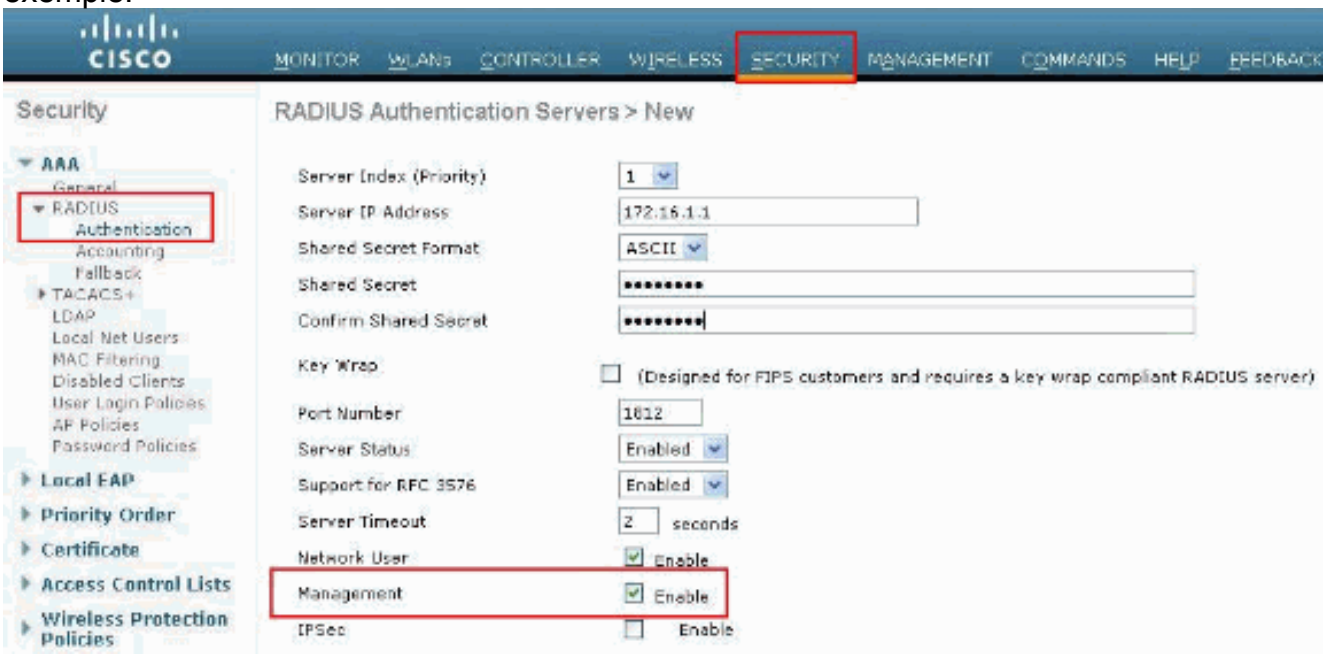
- Configuration WLC
- Configuration de Cisco Secure ACS

Configuration WLC

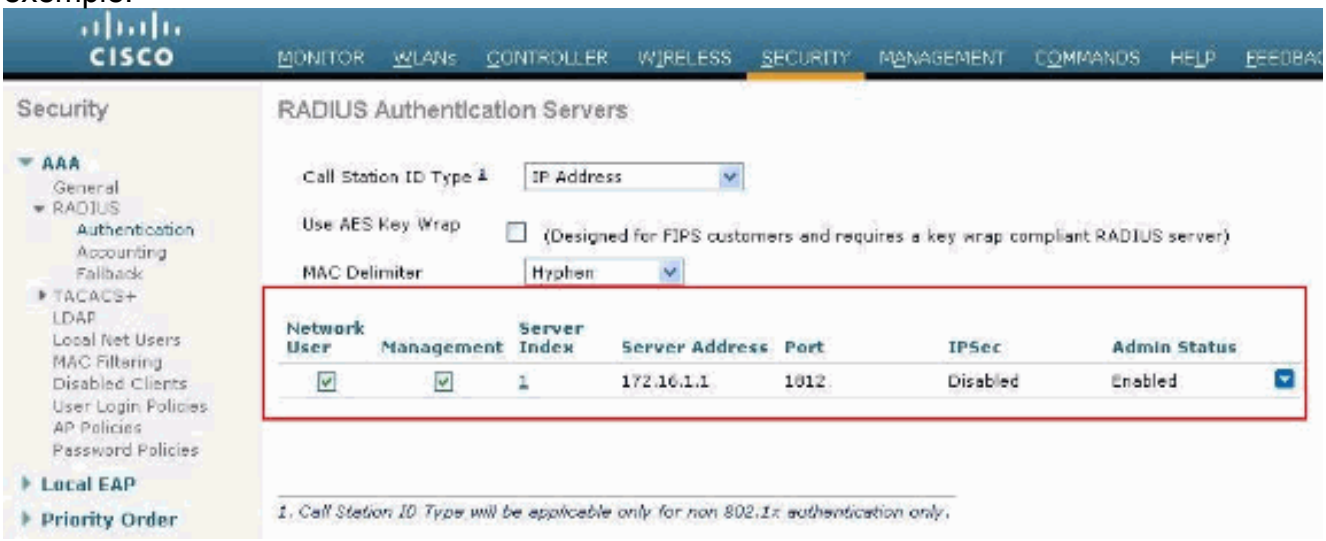
Configurez le WLC pour recevoir la Gestion par le serveur de Cisco Secure ACS

Terminez-vous ces étapes afin de configurer le WLC de sorte qu'il puisse communiquer avec le serveur de RAYON.

1. Du GUI WLC, cliquez sur Security. Du menu du côté gauche, cliquez sur le **RAYON > l'authentification**. La page de **serveurs d'authentification RADIUS** paraît. Pour ajouter un nouveau serveur de RAYON, cliquez sur New. Dans le **RADIUS Authentication Servers > New page**, entrez les paramètres spécifiques au serveur de RAYON. Voici un exemple.



2. Vérifiez la case d'option de **Gestion** afin de permettre au serveur de RAYON pour authentifier les utilisateurs qui ouvrent une session l'au WLC.**Remarque:** Assurez-vous que le secret partagé configuré à cette page s'assortit avec le secret partagé configuré sur le serveur de RAYON. Seulement alors le WLC peut communiquer avec le serveur de RAYON.
3. Vérifiez si le WLC est configuré pour être géré par Cisco Secure ACS. Afin de faire ceci, cliquez sur Security du GUI WLC. La fenêtre résultante GUI ressemble à cet exemple.



Vous pouvez voir que la case de **Gestion** est activée pour le serveur 172.16.1.1 de RAYON. Ceci illustre qu'on permet à ACS pour authentifier les utilisateurs de Gestion sur le WLC.

Configuration de Cisco Secure ACS

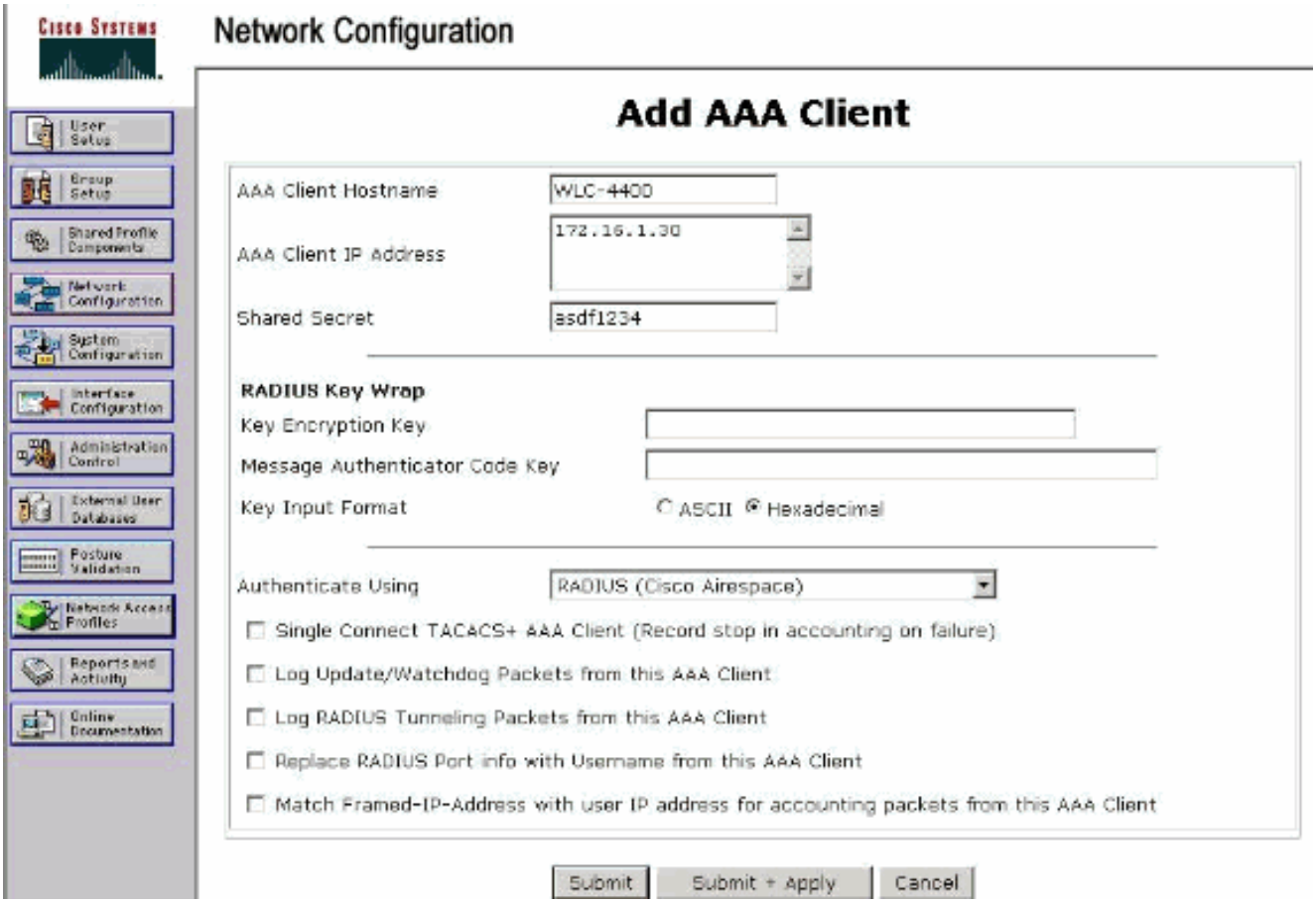
Terminez-vous les étapes dans ces sections afin de configurer l'ACS :

1. Ajoutez le WLC en tant que client d'AAA au serveur de RAYON.
2. Configurez les utilisateurs et leurs attributs appropriés IETF de RAYON.
3. Configurez un utilisateur avec l'accès en lecture-écriture.
4. Configurez un utilisateur avec l'accès en lecture seule.

Ajoutez le WLC en tant que client d'AAA au serveur de RAYON

Terminez-vous ces étapes afin d'ajouter le WLC en tant que client d'AAA dans le Cisco Secure ACS.

1. Dans l'interface graphique ACS, cliquez sur **Network Configuration**.
2. Sous des clients d'AAA, cliquez sur Add l'**entrée**.
3. Dans la fenêtre de **client d'AAA d'ajouter**, introduisez le nom d'hôte WLC, l'adresse IP du WLC, et une clé secrète partagée.Dans cet exemple, ce sont les configurations :L'adresse Internet de client d'AAA est WLC-4400172.16.1.30/16 est l'adresse IP de client d'AAA, qui, est dans ce cas le WLC.La clé secrète partagée est "asdf1234".



Ceci clé secrète partagée doit être identique que la clé secrète partagée que vous configurez sur le WLC.

4. De l'authentifier utilisant le menu déroulant, choisissez le **RAYON (Cisco Airespace)**.
5. Cliquez sur Submit **+ reprise** afin de sauvegarder la configuration.

Configurez les utilisateurs et leurs attributs appropriés IETF de RAYON

Afin d'authentifier un utilisateur par l'intermédiaire d'un serveur de RAYON, pour la procédure de connexion de contrôleur et la Gestion, vous devez ajouter l'utilisateur à la base de données de RAYON avec le *type de service d'*attribut RADIUS IETF réglé à la valeur appropriée selon les privilèges de l'utilisateur.

- Afin de placer des privilèges lecture/écriture pour l'utilisateur, placez l'attribut de *type de service à* **administratif**.
- Afin de placer des privilèges en lecture seule pour l'utilisateur, placez la Nas-**demande d'**attribut de *type de service*.

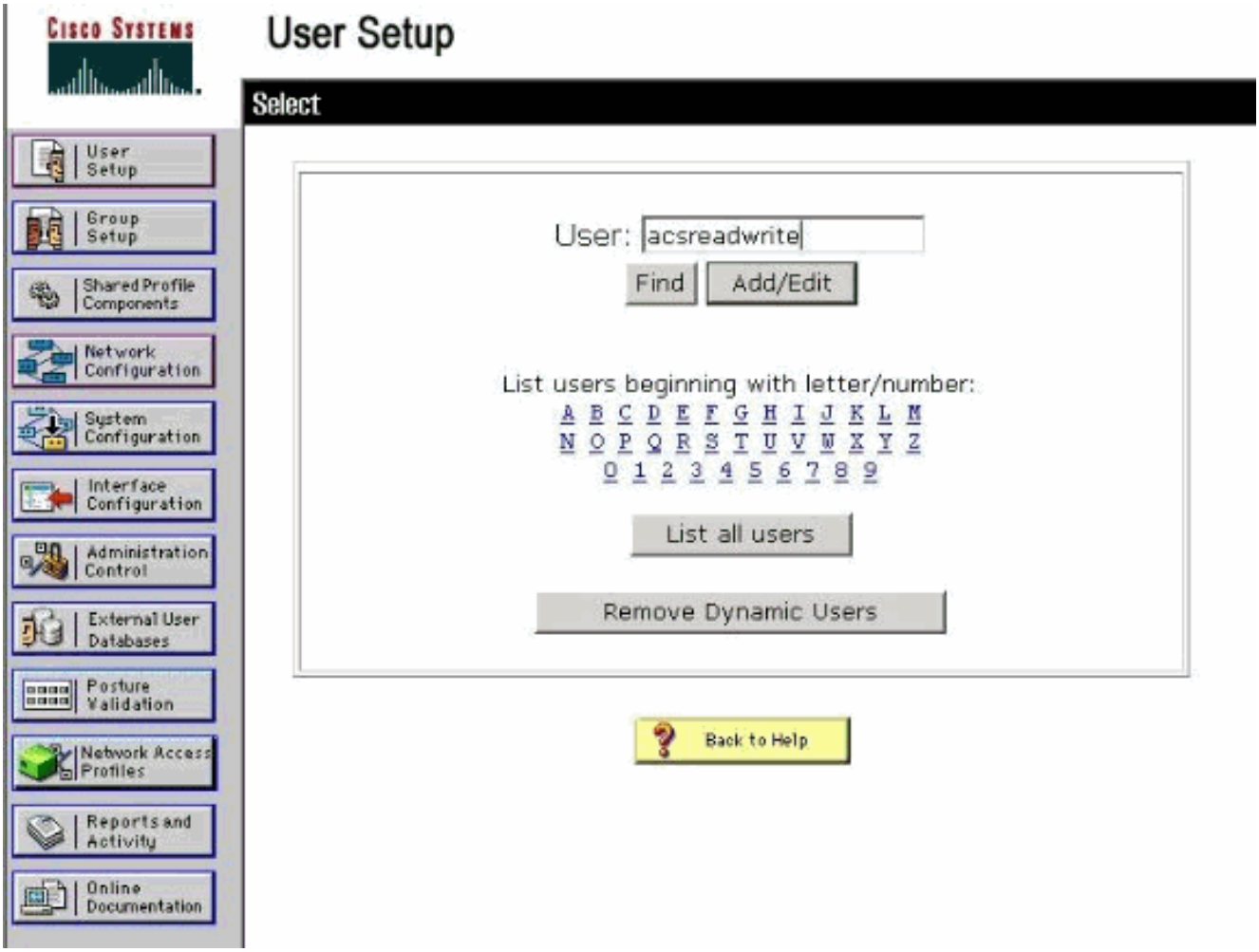
Configurez un utilisateur avec l'accès en lecture-écriture

Le premier exemple affiche la configuration d'un utilisateur avec l'accès complet au WLC. Quand les essais de cet utilisateur à ouvrir une session au contrôleur, le serveur de RAYON authentifie et fournit à cet utilisateur le plein accès administratif.

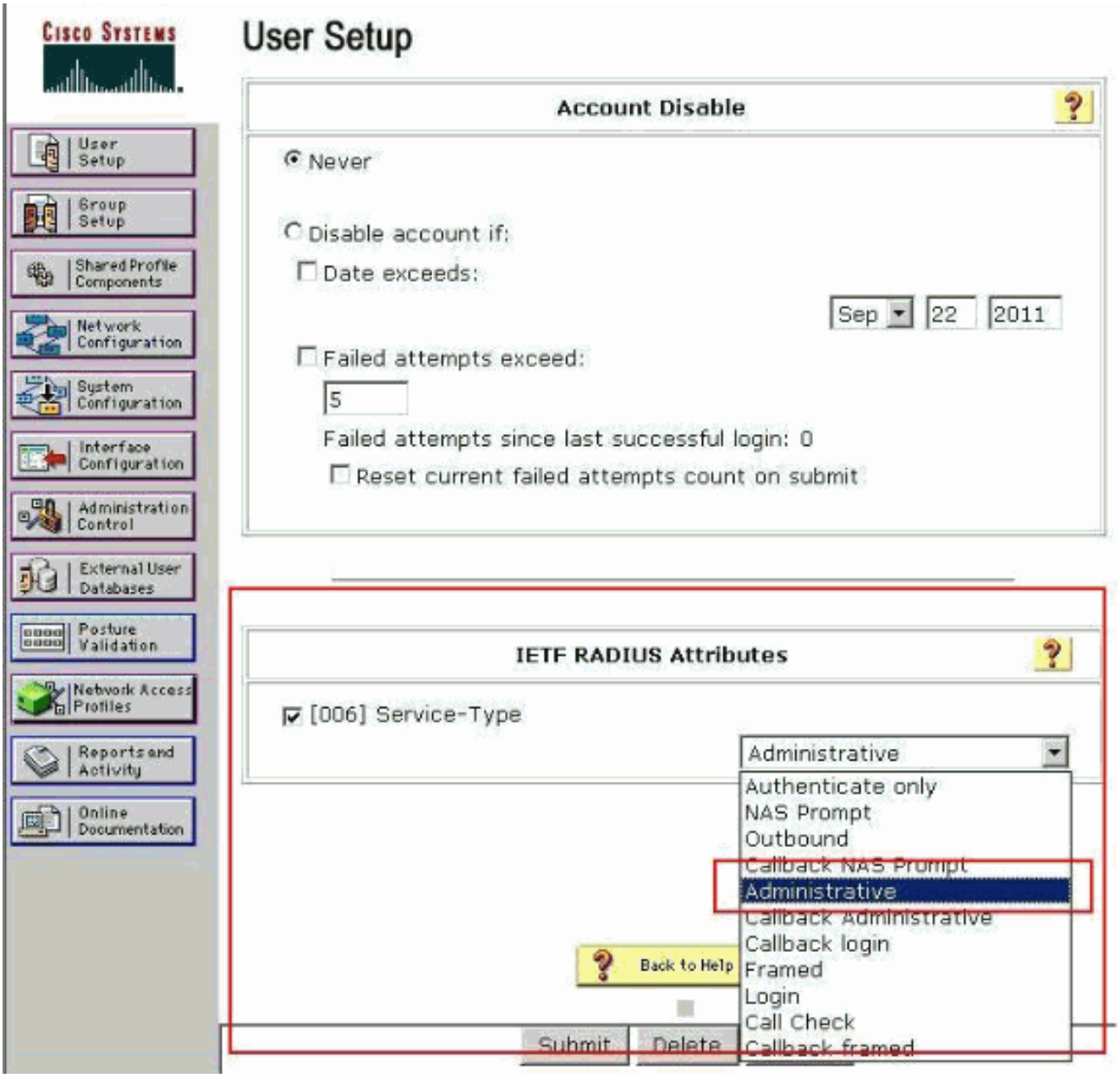
Dans cet exemple, le nom d'utilisateur et mot de passe est **acsreadwrite**.

Terminez-vous ces étapes sur le Cisco Secure ACS.

1. Dans l'interface graphique ACS, cliquez sur **User Setup**.
2. Tapez le nom d'utilisateur à ajouter à l'ACS comme cette fenêtre d'exemple affiche.

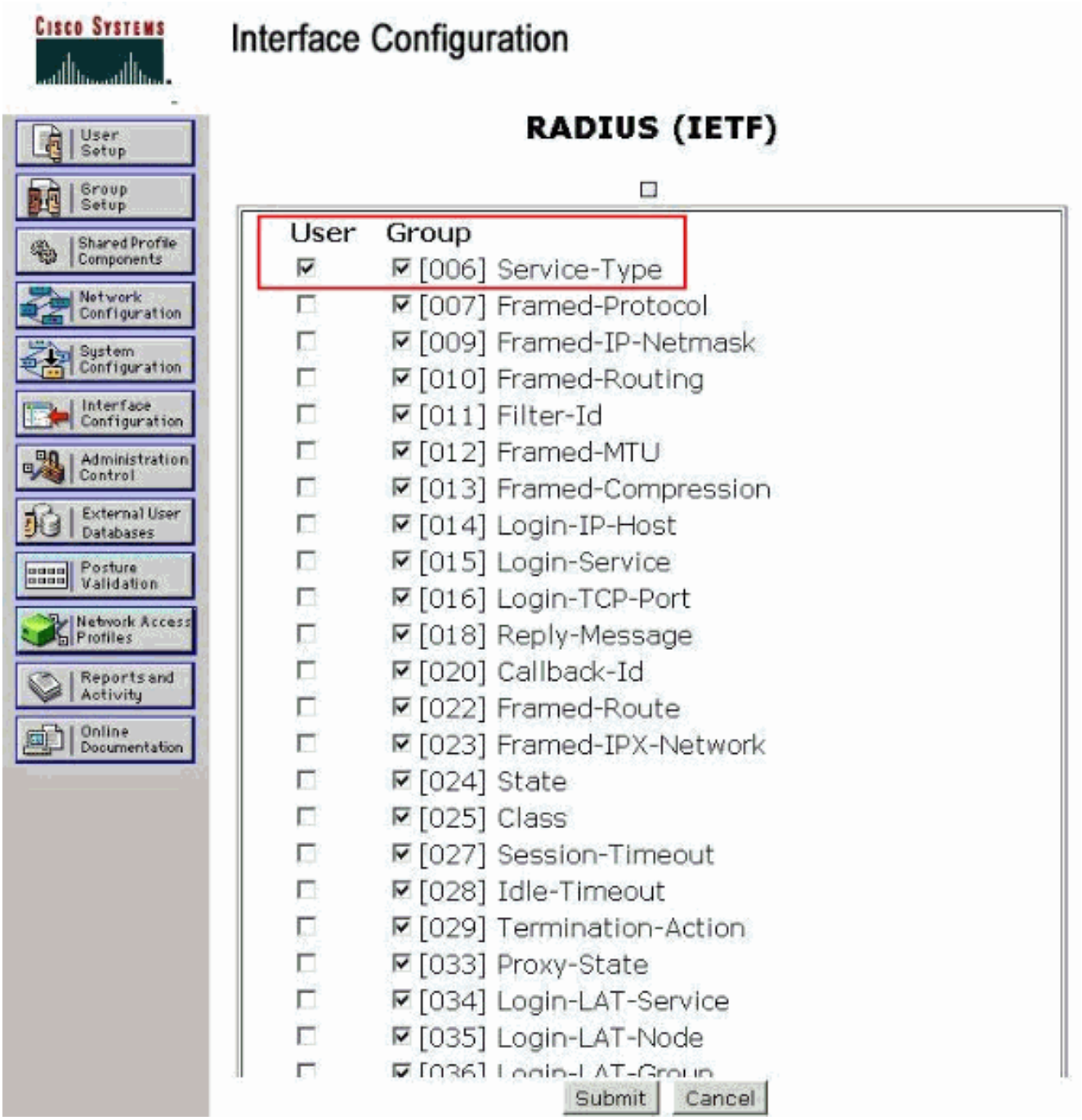


3. Cliquez sur Add**/éditez** afin d'aller à l'utilisateur éditent la page.
4. Dans l'utilisateur éditez la page, fournissez les coordonnées de nom réel, de description et de mot de passe de cet utilisateur.
5. Faites descendre l'écran à l'IETF RADIUS Attributes plaçant et à l'**attribut de type de service de** contrôle.
6. Puisque, dans cet exemple, l'acsreadwrite d'utilisateur doit être donné l'accès complet, choisissez **administratif** pour le menu déroulant de type de service et cliquez sur Submit.Ceci s'assure que cet utilisateur particulier a l'accès en lecture-écriture au WLC.



Parfois, cet attribut de type de service n'est pas visible sous les paramètres utilisateurs. En pareil cas, terminez-vous ces étapes afin de le rendre visible.

1. Du GUI ACS, choisissez l'**Interface Configuration > RADIUS (IETF)** afin d'activer des attributs IETF dans la fenêtre de configuration utilisateur.Ceci vous porte à la page Settings du RAYON (IETF).
2. De la page Settings du RAYON (IETF), vous pouvez activer l'attribut IETF qui doit être visible sous des configurations d'utilisateur ou de groupe. Pour cette configuration, vérifiez le **type de service** pour la colonne d'utilisateur et cliquez sur Submit. Cette fenêtre affiche un exemple.



Remarque: Cet exemple spécifie l'authentification sur une base par utilisateur. Vous pouvez également exécuter l'authentification basée sur le groupe auquel un utilisateur particulier appartient. En pareil cas, activez la case de **groupe** de sorte que cet attribut soit visible sous des configurations de groupe.**Remarque:** En outre, si l'authentification est sur une base de groupe, vous devez affecter des utilisateurs à un groupe particulier et configurer le groupe plaçant des attributs IETF pour fournir des privilèges d'accès aux utilisateurs de ce groupe. Référez-vous à la Gestion de groupe pour des informations détaillées sur la façon configurer et gérer des groupes.

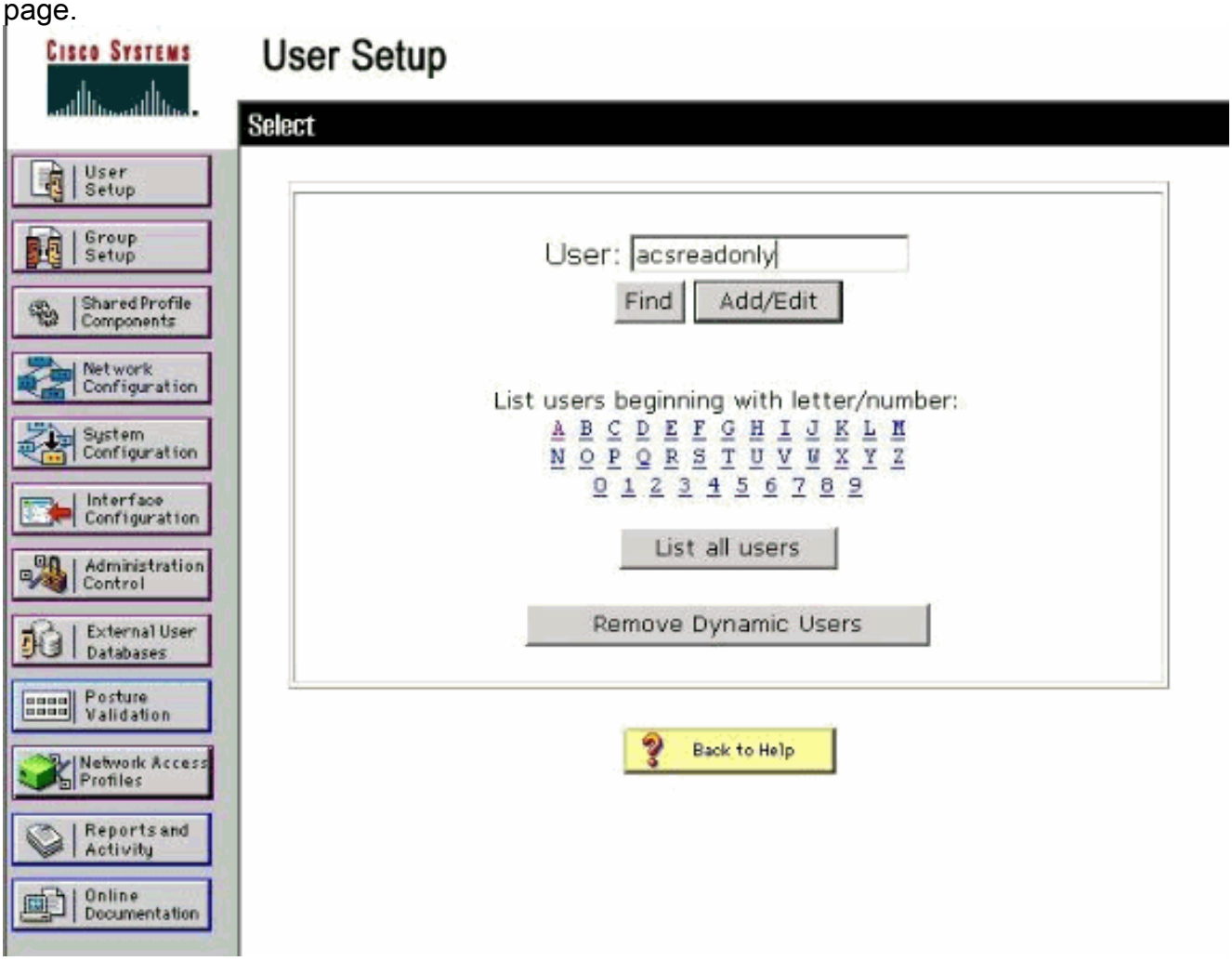
Configurez un utilisateur avec l'accès en lecture seule

Cet exemple affiche la configuration d'un utilisateur avec l'accès en lecture seule au WLC. Quand les essais de cet utilisateur à ouvrir une session au contrôleur, le serveur de RAYON authentifie et fournit à cet utilisateur l'accès en lecture seule.

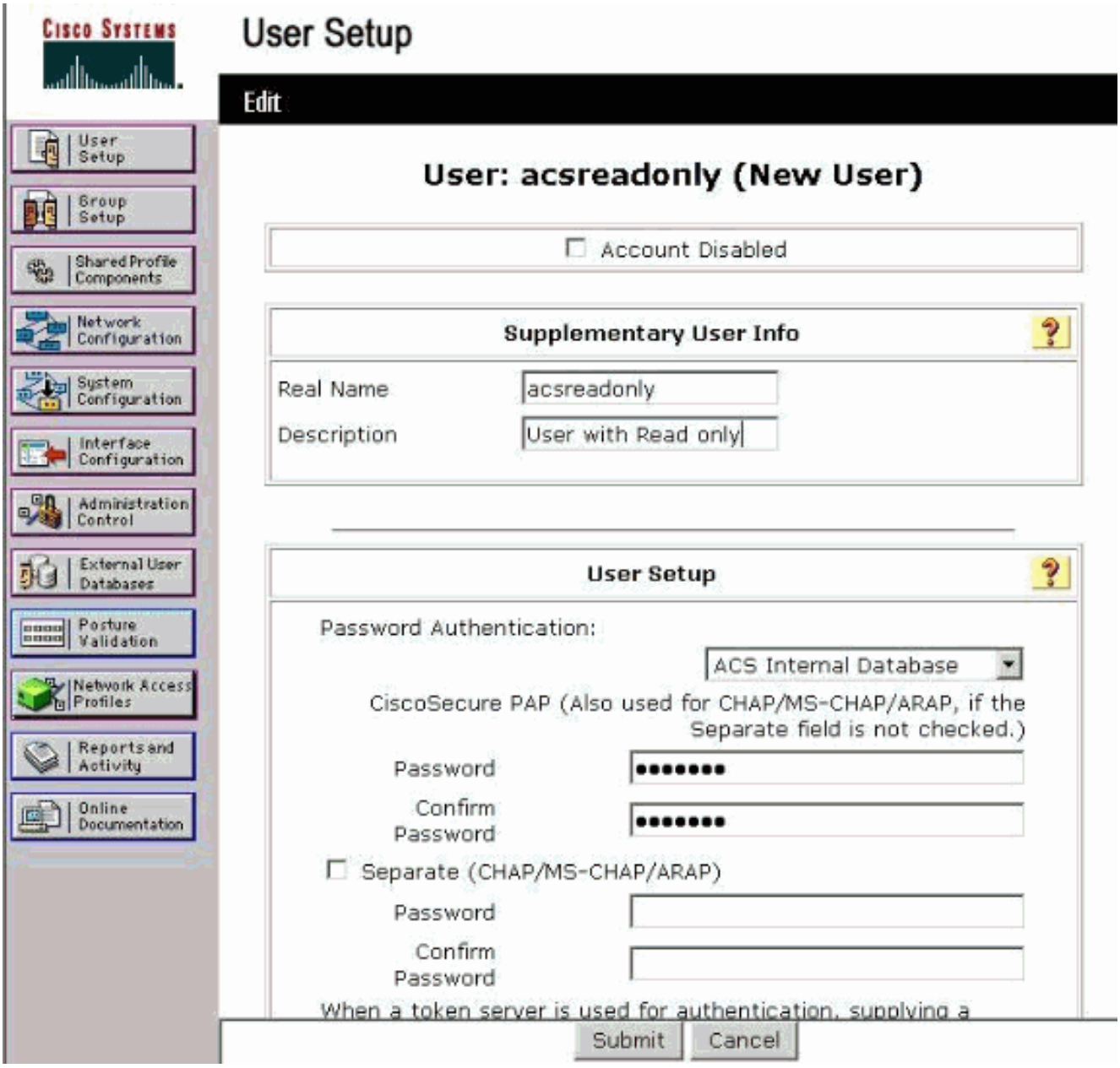
Dans cet exemple, le nom d'utilisateur et mot de passe est **acsreadonly**.

Terminez-vous ces étapes sur le Cisco Secure ACS :

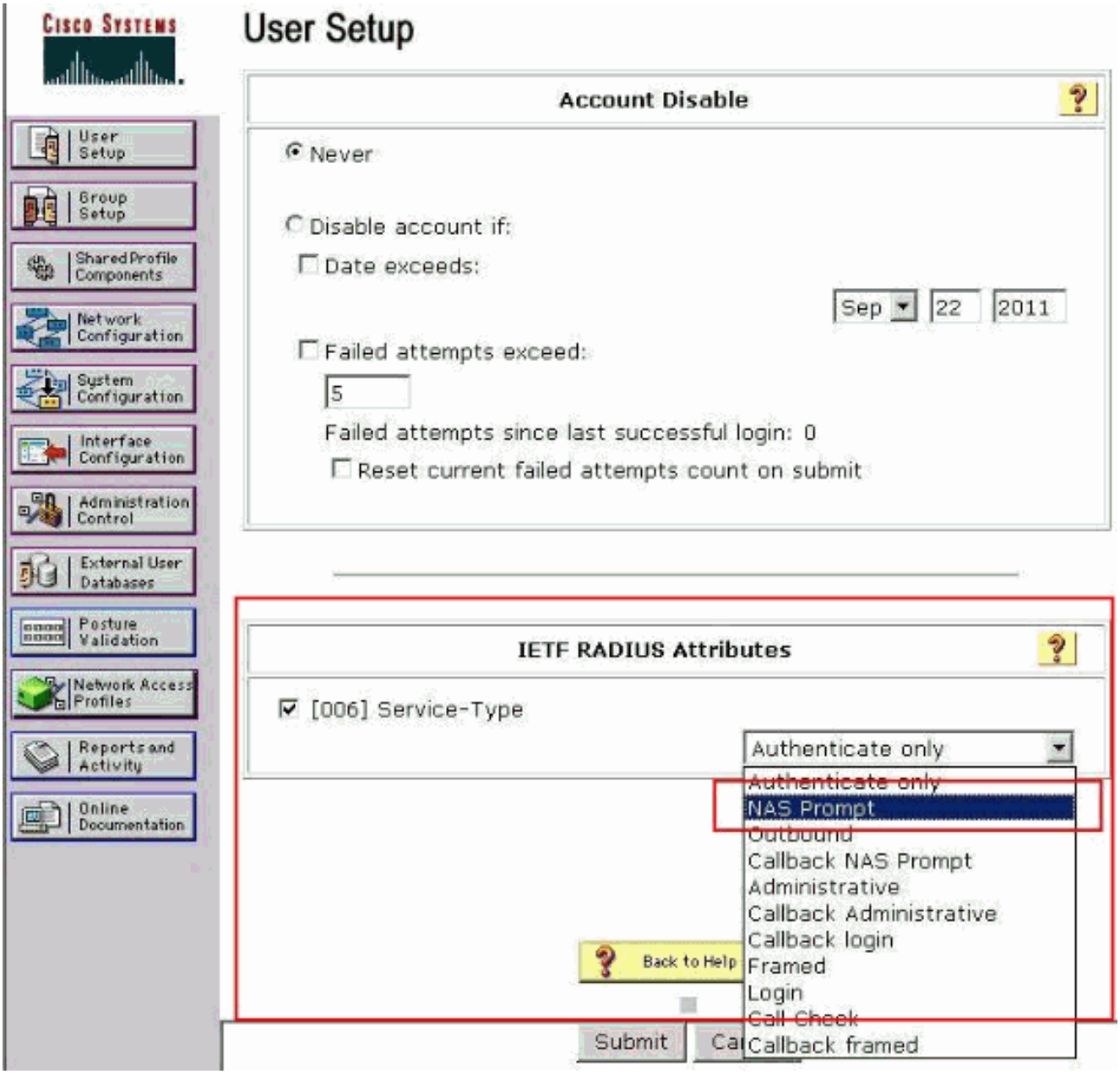
1. Dans l'interface graphique ACS, cliquez sur **User Setup**.
2. Tapez le nom d'utilisateur que vous voulez ajouter à l'ACS et cliquer sur Add**/éditez** afin d'aller à l'utilisateur éditent la
page.



3. Fournissez le nom réel, la description et le mot de passe de cet utilisateur. Cette fenêtre affiche un
exemple.

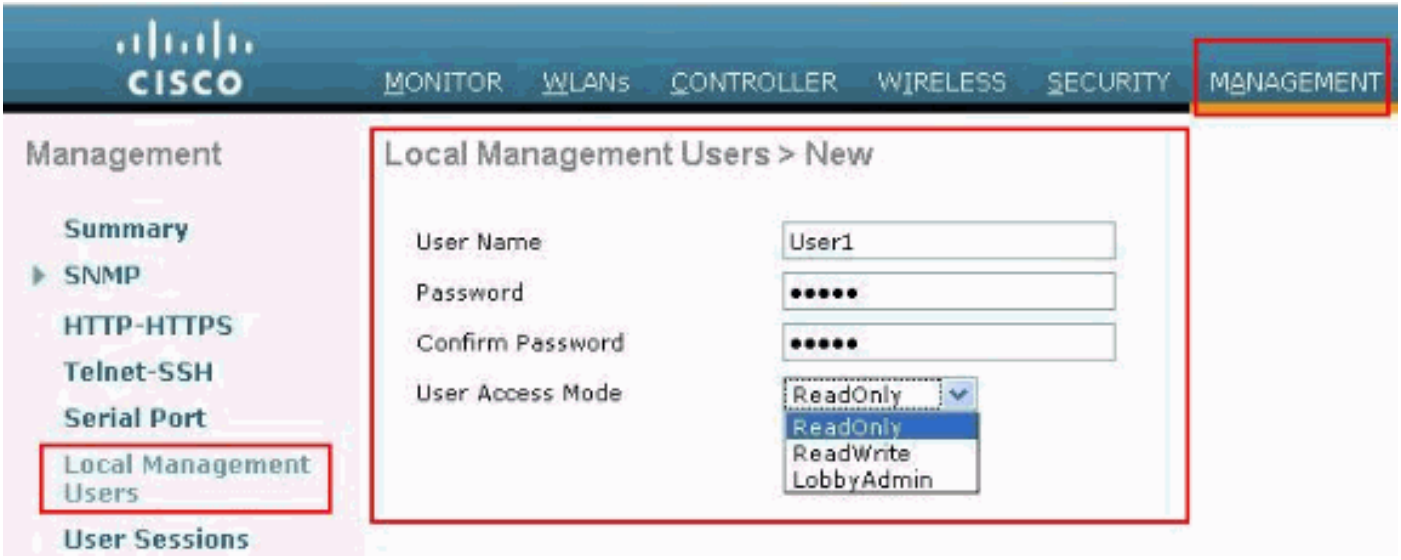


4. Faites descendre l'écran à l'IETF RADIUS Attributes plaçant et à l'**attribut de type de service de** contrôle.
5. Puisque, dans cet exemple, l'utilisateur doit acsreadonly avoir l'accès en lecture seule, choisissez la **demande de NAS du** menu déroulant de type de service et cliquez sur Submit.Ceci s'assure que cet utilisateur particulier a l'accès en lecture seule au WLC.



Gérez le WLC localement aussi bien que par le serveur de RAYON

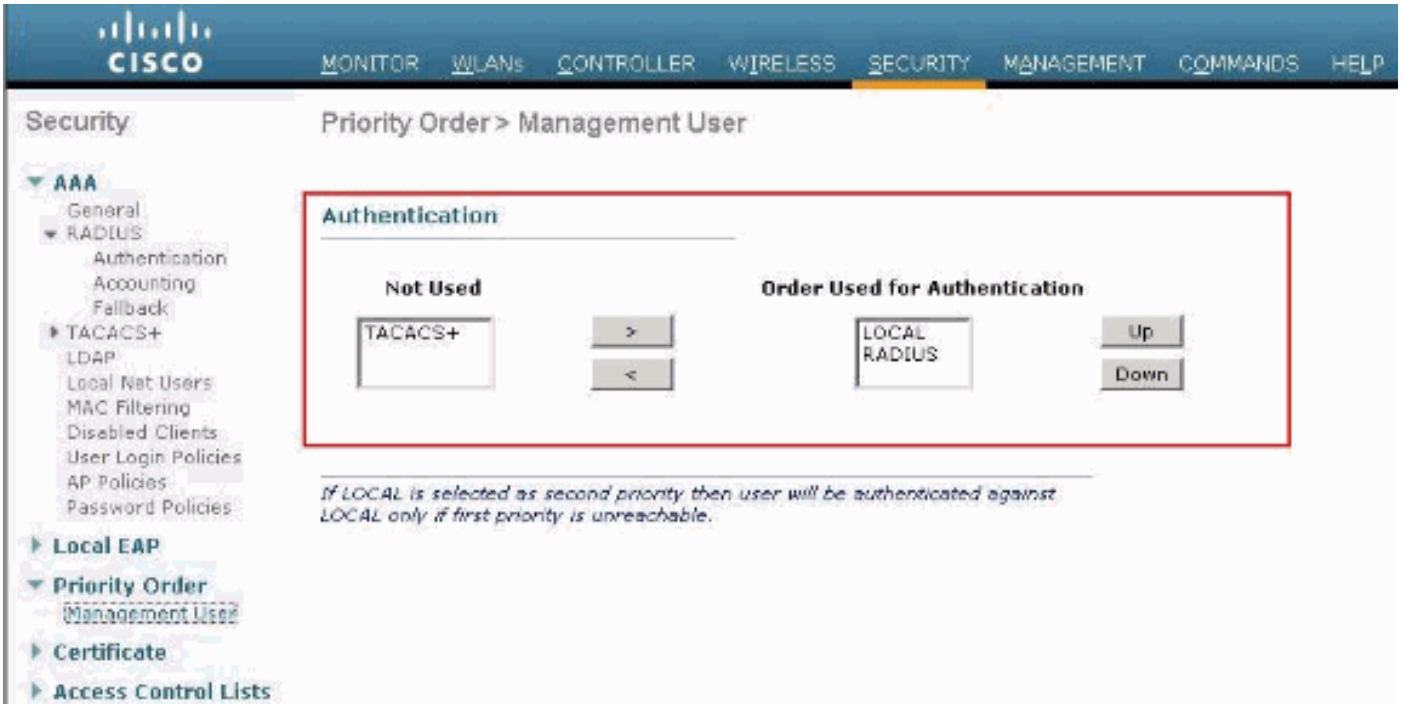
Vous pouvez également configurer les utilisateurs de Gestion localement sur le WLC. Ceci peut être fait du GUI de contrôleur, sous la **Gestion > les utilisateurs locaux de Gestion**.



Supposez que le WLC est configuré avec des utilisateurs de Gestion localement aussi bien que dans le serveur de RAYON avec la case de **Gestion** activée. Dans un tel scénario, par défaut, quand les essais d'un utilisateur à ouvrir une session au WLC, le WLC se comporte de cette manière :

1. Le WLC regarde d'abord les utilisateurs locaux de Gestion définis pour valider l'utilisateur. Si l'utilisateur existe dans sa liste locale, alors elle permet l'authentification pour cet utilisateur. Si cet utilisateur n'apparaît pas localement, alors il regarde au serveur de RAYON.
2. Si le même utilisateur existe localement aussi bien que dans le serveur de RAYON mais avec différents privilèges d'accès, alors le WLC authentifie l'utilisateur avec les privilèges spécifiés localement. En d'autres termes, la configuration locale sur le WLC a toujours la priorité une fois comparée au serveur de RAYON.

La commande de l'authentification pour des utilisateurs de Gestion peut être changée sur le WLC. Afin de faire ceci, de la page de **Sécurité** sur le WLC, **commande prioritaire de** clic **> utilisateur de Gestion**. De cette page vous pouvez spécifier la commande de l'authentification. Voici un exemple.



Remarque: Si des GENS DU PAYS sont sélectionnés en tant que deuxième priorité, alors

l'utilisateur sera authentifié suivre cette méthode seulement si la méthode définie comme première priorité (RAYON TACACS) est inaccessible.

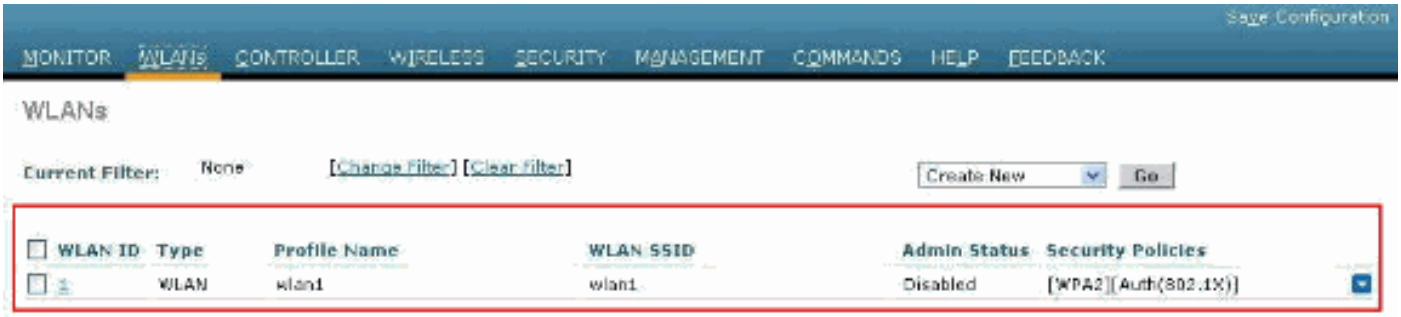
Vérifiez

Afin de vérifier si vos travaux de configuration correctement, accèdent au WLC par le mode CLI ou GUI (HTTP/HTTPS). Quand l'invite d'ouverture de connexion apparaît, tapez le nom d'utilisateur et mot de passe comme configuré sur le Cisco Secure ACS.

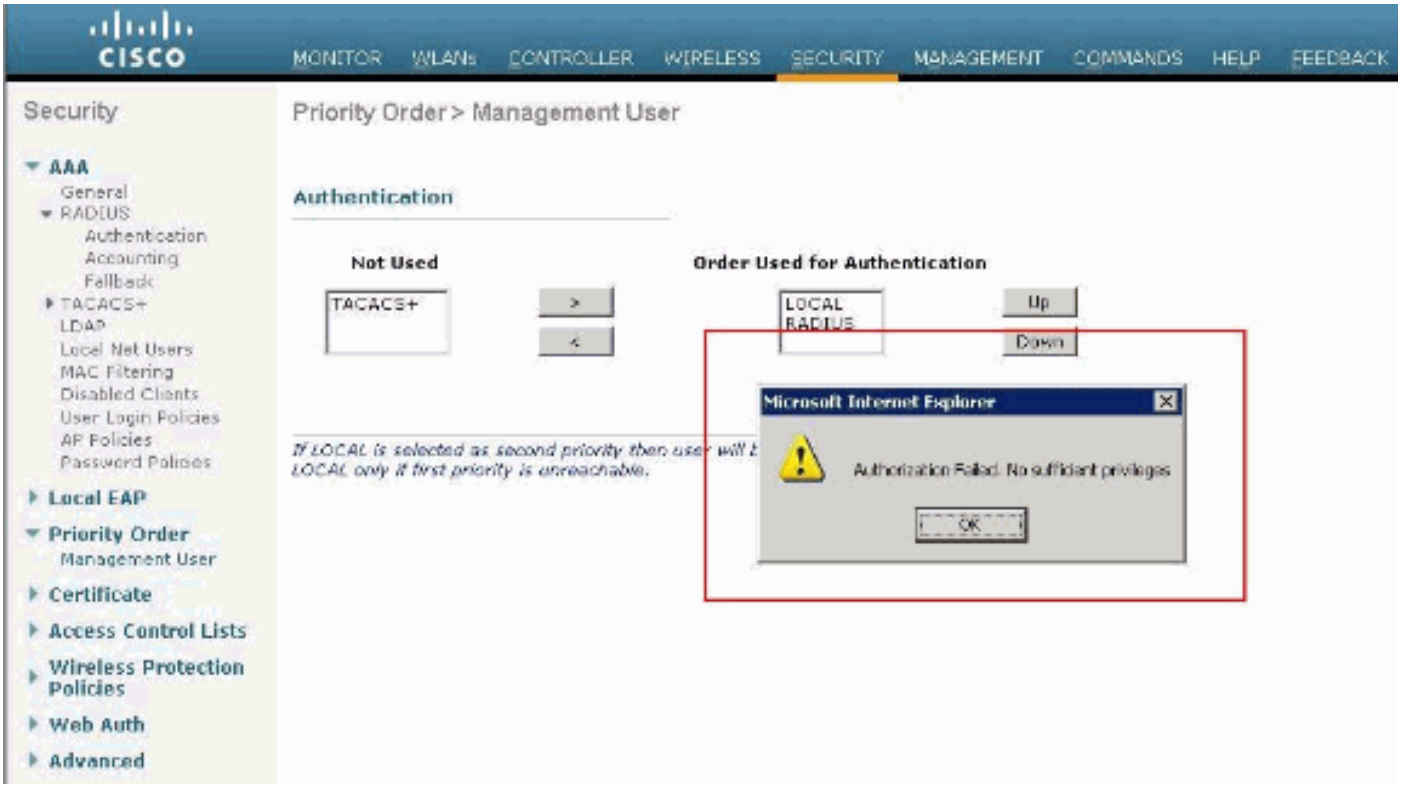
Si vous avez les configurations correctes, vous êtes authentifié avec succès dans le WLC.

Vous pouvez également s'assurer si l'utilisateur authentifié est équipé de restrictions d'accès comme spécifié par l'ACS. Afin de faire ainsi, accédez au GUI WLC par HTTP/HTTPS (assurez-vous que WLC est configuré pour permettre HTTP/HTTPS).

Un utilisateur avec le positionnement d'accès en lecture-écriture dans l'ACS a plusieurs privilèges configurables dans le WLC. Par exemple, un utilisateur lecture/écriture a le privilège de créer un nouveau WLAN sous la page WLAN du WLC. Cette fenêtre affiche un exemple.



Quand un utilisateur avec seulement des essais lus de provileges pour modifier la configuration sur le contrôleur, l'utilisateur voit ce message.



Ces restrictions d'accès peuvent également être vérifiées par le CLI du WLC. La sortie ci-dessous est un exemple.

```
(Cisco Controller) >? debug Manages system debug options. help Help linktest Perform a link test
to a specified MAC address. logout Exit this session. Any unsaved changes are lost. show Display
switch options and settings. (Cisco Controller) >config Incorrect usage. Use the '?' or <TAB>
key to list commands.
```

Comme cet exemple de sortie affiche, a **?** au contrôleur le CLI affiche une liste des commandes disponible pour l'utilisateur courant. Notez également que la commande de **config** n'est pas disponible dans cet exemple de sortie. Ceci illustre qu'un utilisateur en lecture seule n'a pas le privilège de ne faire aucune configuration sur le WLC. Considérant que, un utilisateur lecture/écriture a les privilèges de faire des configurations sur le contrôleur (GUI et mode CLI).

Remarque: Même après que vous authentifiez un utilisateur WLC par le serveur de RAYON, car vous parcourez de la page pour paginer, le serveur du HTTP [S] authentifie toujours entièrement le client chaque fois. La seule raison que vous n'êtes pas incité pour l'authentification à chaque page est que vos caches du navigateur et rejoue vos qualifications.

Dépannez

Il y a certaines circonstances quand un contrôleur authentifie des utilisateurs de Gestion par l'intermédiaire de l'ACS, les finitions d'authentification avec succès (Access-recevez), et vous ne voyez aucune erreur d'autorisation sur le contrôleur. *Mais, l'utilisateur est incité de nouveau pour l'authentification.*

En pareil cas, vous ne pouvez pas interpréter ce qui est erroné et par pourquoi l'utilisateur ne peut pas se connecter dans le WLC juste utilisant la commande d'**enable d'événements de debug aaa**. Au lieu de cela, le contrôleur affiche une autre demande pour l'authentification.

Un possible raison pour ceci est que l'ACS n'est pas configuré pour transmettre l'attribut de type de service pour cet utilisateur particulier ou pour le grouper quoique le nom d'utilisateur et mot de passe soient correctement configurés sur l'ACS.

La sortie de la commande d'**enable d'événements de debug aaa** n'indique pas qu'un utilisateur n'a pas les attributs priés (pour cet exemple, l'attribut de type de service) quoiqu'un Access-**recevoir** soit renvoyé du serveur d'AAA. Cette sortie de commande d'**enable d'événements de debug aaa d'**exemple affiche un exemple.

```
 (Cisco Controller) >debug aaa events enable Mon Aug 13 20:14:33 2011: AuthenticationRequest:
0xa449a8c Mon Aug 13 20:14:33 2011: Callback.....................................0x8250c40 Mon
Aug 13 20:14:33 2011: protocolType.....................................0x00020001 Mon Aug 13
20:14:33 2011: proxyState.....................1A:00:00:00:00:00-00:00 Mon Aug 13 20:14:33 2011:
Packet contains 5 AVPs (not shown) Mon Aug 13 20:14:33 2011: 1a:00:00:00:00:00 Successful
transmission of Authentication Packet (id 8) to 172.16.1.1:1812, proxy state 1a:00:00:00:00:00-
00:00 Mon Aug 13 20:14:33 2011: ****Enter processIncomingMessages: response code=2 Mon Aug 13
20:14:33 2011: ****Enter processRadiusResponse: response code=2 Mon Aug 13 20:14:33 2011:
1a:00:00:00:00:00 Access-Accept received from RADIUS server 172.16.1.1 for mobile
1a:00:00:00:00:00 receiveId = 0 Mon Aug 13 20:14:33 2011: AuthorizationResponse: 0x9802520 Mon
Aug 13 20:14:33 2011: structureSize.....................................28 Mon Aug 13 20:14:33 2011:
resultCode.....................................0 Mon Aug 13 20:14:33 2011:
protocolUsed.....................................0x00000001 Mon Aug 13 20:14:33 2011:
proxyState.....................1A:00:00:00:00:00-00:00 Mon Aug 13 20:14:33 2011: Packet
contains 0 AVPs:
```

Dans **debug aaa de** cet le premier exemple les **événements activent la** sortie de commande, vous

voient qu'Access-Recevoir est avec succès reçu du serveur de RAYON mais l'attribut de type de service n'est pas passé sur le WLC. C'est parce que l'utilisateur particulier n'est pas configuré avec cet attribut sur l'ACS.

Le Cisco Secure ACS doit être configuré pour renvoyer l'attribut de type de service après authentification de l'utilisateur. La valeur d'attribut de type de service doit être placée à **administratif** ou à la Nas-**demande** selon les privilèges des utilisateurs.

Cet deuxième exemple affiche la sortie de commande d'**enable d'événements de debug aaa** de nouveau. Cependant, cette fois l'attribut de type de service est placé à **administratif** sur l'ACS.

```
(Cisco Controller)>debug aaa events enable Mon Aug 13 20:17:02 2011: AuthenticationRequest:
0xa449f1c Mon Aug 13 20:17:02 2011: Callback.....................................0x8250c40 Mon
Aug 13 20:17:02 2011: protocolType.....................................0x00020001 Mon Aug 13
20:17:02 2011: proxyState.....................1D:00:00:00:00:00-00:00 Mon Aug 13 20:17:02
2011: Packet contains 5 AVPs (not shown) Mon Aug 13 20:17:02 2011: 1d:00:00:00:00:00 Successful
transmission of Authentication Packet (id 11) to 172.16.1.1:1812, proxy state 1d:00:00:00:00:00-
00:00 Mon Aug 13 20:17:02 2011: ****Enter processIncomingMessages: response code=2 Mon Aug 13
20:17:02 2011: ****Enter processRadiusResponse: response code=2 Mon Aug 13 20:17:02 2011:
1d:00:00:00:00:00 Access-Accept received from RADIUS server 172.16.1.1 for mobile
1d:00:00:00:00:00 receiveId = 0 Mon Aug 13 20:17:02 2011: AuthorizationResponse: 0x9802520 Mon
Aug 13 20:17:02 2011: structureSize.....100 Mon Aug 13 20:17:02 2011:
resultCode.....0 Mon Aug 13 20:17:02 2011:
protocolUsed.....0x00000001 Mon Aug 13 20:17:02 2011:
proxyState.....1D:00:00:00:00:00-00:00 Mon Aug 13 20:17:02 2011: Packet
contains 2 AVPs: Mon Aug 13 20:17:02 2011: AVP[01] Service-Type.....0x00000006 (6) (4
bytes) Mon Aug 13 20:17:02 2011: AVP[02] Class..... CISCOACS:000d1b9f/ac100128/acsserver (36
bytes)
```

Vous pouvez voir dans cet exemple de sortie que l'attribut de type de service est passé sur le WLC.

Informations connexes

- Configurant le contrôleur LAN Sans fil - Guide de configuration
- Exemple de configuration de réseaux VLAN sur des contrôleurs de réseau local sans fil
- Exemple de configuration d'une affectation de VLAN dynamique avec un serveur RADIUS et un contrôleur de réseau local sans fil
- Exemple de configuration de base d'un contrôleur LAN sans fil et d'un point d'accès léger
- Exemple de configuration de réseaux VLAN de groupe de points d'accès avec des contrôleurs de réseau local sans fil
- Support et documentation techniques - Cisco Systems