Authentification de l'administrateur de salle d'attente du contrôleur de réseau local sans fil via un serveur RADIUS

Contenu

Introduction

Ce document explique les étapes de configuration impliquées pour authentifier un administrateur de lobby du contrôleur LAN Sans fil (WLC) avec un serveur de RAYON.

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, tel que le Cisco Secure ACS
- La connaissance des utilisateurs d'invité dans le WLC

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.

Informations générales

Un administrateur de lobby, également connu sous le nom d'ambassadeur de lobby d'un WLC, peut créer et gérer des comptes utilisateurs d'invité sur le contrôleur LAN Sans fil (WLC). L'ambassadeur de lobby a limité des privilèges de configuration et peut accéder à seulement les pages Web utilisées pour gérer les comptes d'invité. L'ambassadeur de lobby peut spécifier la durée que les comptes utilisateurs d'invité demeurent actifs. Après que le temps spécifié s'écoule, les comptes utilisateurs d'invité expirent automatiquement.

Référez-vous au guide de déploiement : Accès invité de Cisco utilisant le contrôleur LAN Sans fil de Cisco pour plus d'informations sur des utilisateurs d'invité.

Afin de créer un compte utilisateur d'invité sur le WLC, vous devez ouvrir une session au contrôleur en tant qu'administrateur de lobby. Ce document explique comment un utilisateur est authentifié dans le WLC comme un administrateur de lobby basé sur les attributs est retourné par le serveur de RAYON.

Remarque: L'administrateur de lobby que l'authentification peut également être exécutée a basé sur le compte administrateur de lobby configuré localement sur le WLC. Référez-vous à créer un Ambassadeur de lobby expliquent les informations de la façon créer un compte administrateur de lobby localement sur un contrôleur.

Configurez

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

Configurations

Ce document utilise les configurations suivantes :

- L'adresse IP d'interface de gestion de WLC est 10.77.244.212/27.
- L'adresse IP du serveur de RAYON est 10.77.244.197/27.
- La clé secrète partagée qui est utilisée sur le Point d'accès (AP) et le serveur de RAYON est cisco123.
- Le nom d'utilisateur et mot de passe de l'administrateur de lobby configuré dans le serveur de RAYON sont deux lobbyadmin.

Dans l'exemple de configuration dans ce document, n'importe quel utilisateur se connectant dans le contrôleur avec le nom d'utilisateur et mot de passe comme lobbyadmin est assigné le rôle d'un administrateur de lobby.

Configuration WLC

Avant que vous commenciez la configuration nécessaire WLC, assurez-vous que votre contrôleur exécute la version 4.0.206.0 ou plus tard. C'est dû à l'ID de bogue Cisco CSCsg89868 (clients enregistrés seulement) dans lequel l'interface web du contrôleur affiche les pages Web fausses pour l'utilisateur de LobbyAdmin quand le nom d'utilisateur est enregistré dans une base de données de RAYON. Le LobbyAdmin est présenté avec l'interface inaltérable au lieu de l'interface de LobbyAdmin.

Cette bogue a été résolue dans la version 4.0.206.0 WLC. , Assurez-vous par conséquent que votre version de contrôleur est 4.0.206.0 ou plus tard. Référez-vous à la mise à niveau de logiciel Sans fil du contrôleur LAN (WLC) pour des instructions sur la façon dont améliorer votre contrôleur à la version appropriée.

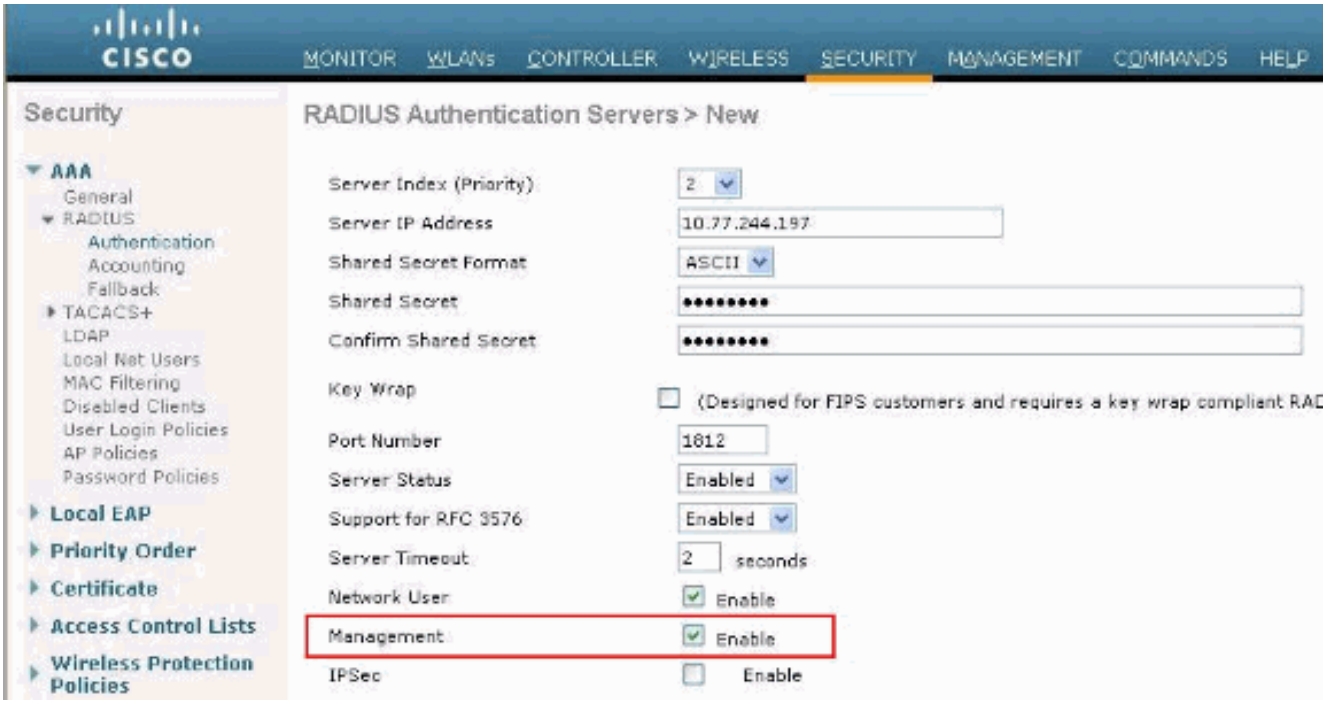
Afin d'exécuter l'authentification de Gestion de contrôleur avec le serveur de RAYON, assurez-vous que l'indicateur d'Admin-auth-par l'intermédiaire-**RAYON** est activé sur le contrôleur. Ceci peut être vérifié de la sortie de commande de **show radius summary**.

La première étape est de configurer les informations du serveur de RAYON sur le contrôleur et d'établir l'accessibilité de la couche 3 entre le contrôleur et le serveur de RAYON.

Configurez les informations du serveur de RAYON sur le contrôleur

Terminez-vous ces étapes afin de configurer le WLC avec des détails au sujet de l'ACS :

1. Du GUI WLC, choisissez l'**onglet Sécurité** et configurez l'adresse IP et le secret partagé du serveur ACS.Ceci a partagé secret doit être identique sur l'ACS pour que le WLC communique avec l'ACS.**Remarque:** Le secret partagé par ACS distingue les majuscules et minuscules. , Veillez par conséquent à écrire les informations secrètes partagées correctement.Cette figure affiche un exemple
   :



2. Cochez la case de **Gestion** afin de permettre à l'ACS pour gérer les utilisateurs WLC suivant les indications de la figure dans l'étape 1. Cliquez ensuite sur **Apply**.
3. Vérifiez l'accessibilité de la couche 3 entre le contrôleur et le serveur configuré de RAYON avec l'aide de la **commande ping**. Cette option de ping est également disponible à la page configurée de serveur de RAYON dans le GUI WLC dans l'onglet d'**authentification de Security>RADIUS**.Ce diagramme affiche une réponse ping réussie du serveur de RAYON. Par conséquent, l'accessibilité de la couche 3 est disponible entre le contrôleur et le serveur de
RAYON.

Configuration du serveur RADIUS

Terminez-vous les étapes dans ces sections afin de configurer le serveur de RAYON :

1. Ajoutez le WLC en tant que client d'AAA au serveur de RAYON
2. Configurez l'attribut de type de service approprié IETF de RAYON pour un administrateur de lobby

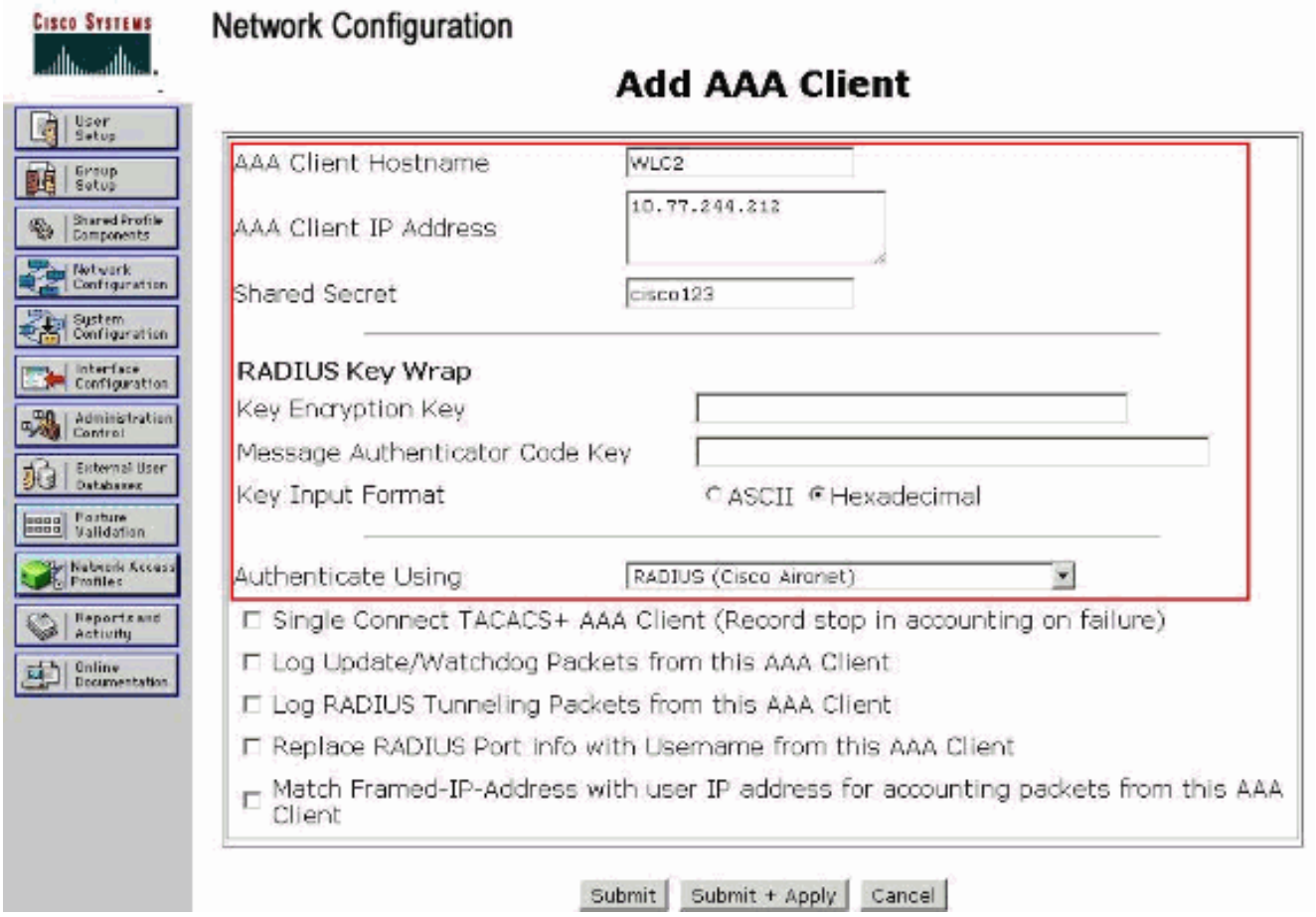
Ajoutez le WLC en tant que client d'AAA au serveur de RAYON

Terminez-vous ces étapes afin d'ajouter le WLC en tant que client d'AAA dans le serveur de

RAYON. Comme cité précédemment, ce document utilise l'ACS en tant que serveur de RAYON. Vous pouvez utiliser n'importe quel serveur de RAYON pour cette configuration.

Terminez-vous ces étapes afin d'ajouter le WLC en tant que client d'AAA dans l'ACS :

1. Du GUI ACS, choisissez l'onglet de **configuration réseau**.
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. Voyez le diagramme d'exemple sous l'étape 5.
4. De l'authentifier utilisant le menu déroulant, choisissez le **RAYON (Cisco Aironet)**.
5. Cliquez sur Submit **+ reprise** afin de sauvegarder la configuration.

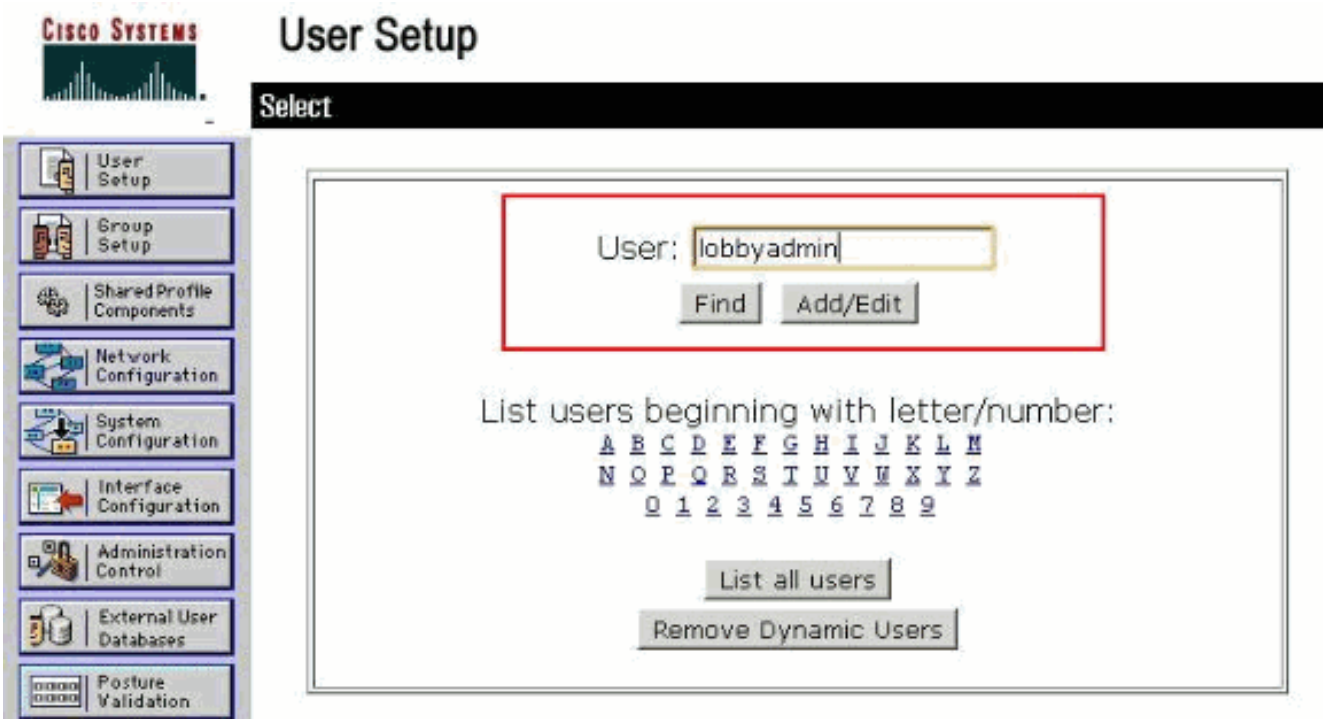


Configurez l'attribut de type de service approprié IETF de RAYON pour un administrateur de lobby

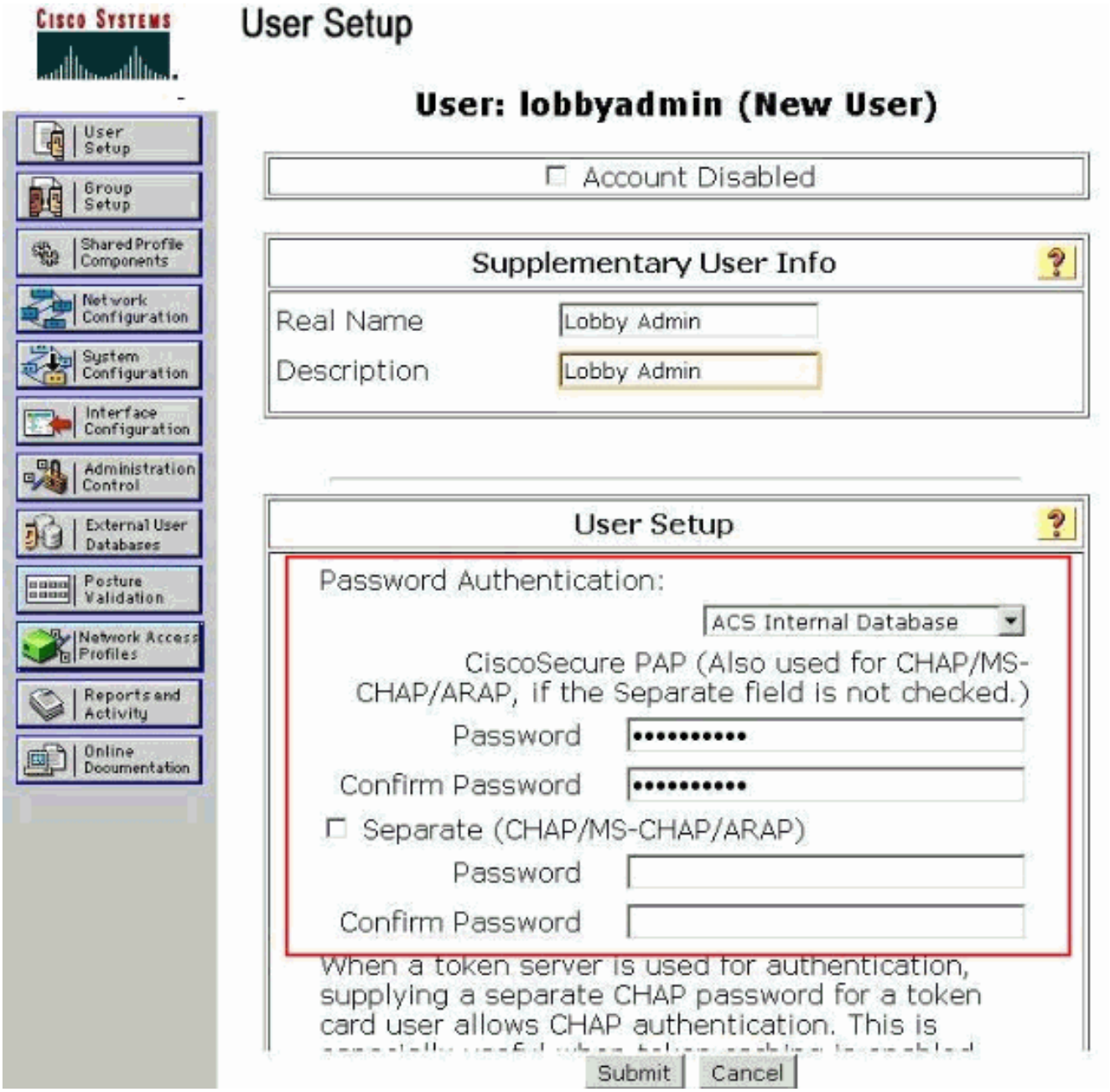
Afin d'authentifier un utilisateur de Gestion d'un contrôleur en tant qu'administrateur de lobby par l'intermédiaire du serveur de RAYON, vous devez ajouter l'utilisateur à la base de données de RAYON avec l'attribut de type de service de RAYON IETF réglé au **rappel administratif**. Cet attribut assigne à l'utilisateur spécifique le rôle d'un administrateur de lobby sur un contrôleur.

Ce document affiche le lobbyadmin d'utilisateur d'exemple en tant qu'administrateur de lobby. Afin de configurer cet utilisateur, terminez-vous ces étapes sur l'ACS :

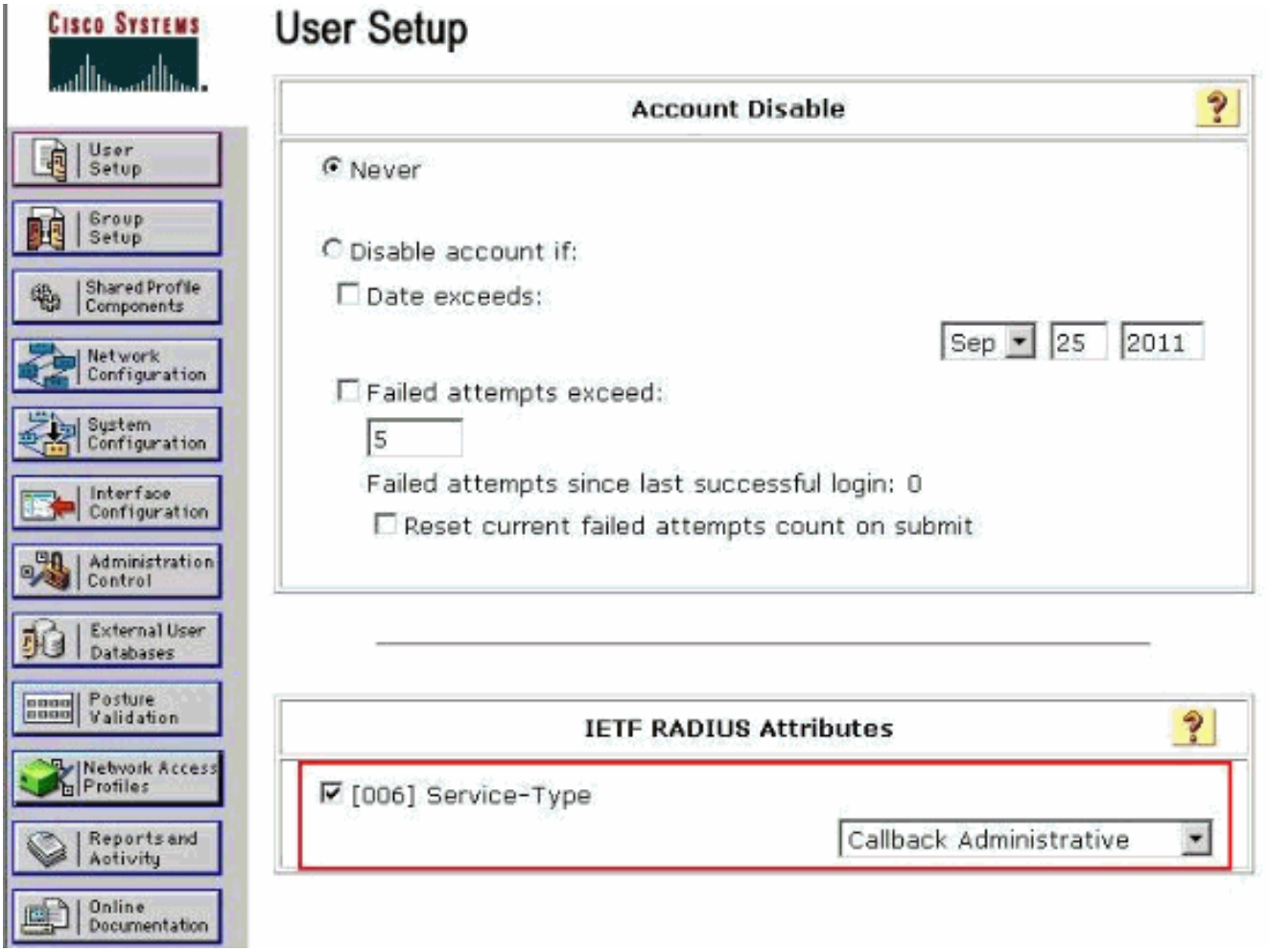
1. Du GUI ACS, choisissez l'onglet d'**installation utilisateur**.
2. Écrivez le nom d'utilisateur à ajouter à l'ACS comme cette fenêtre d'exemple affiche :



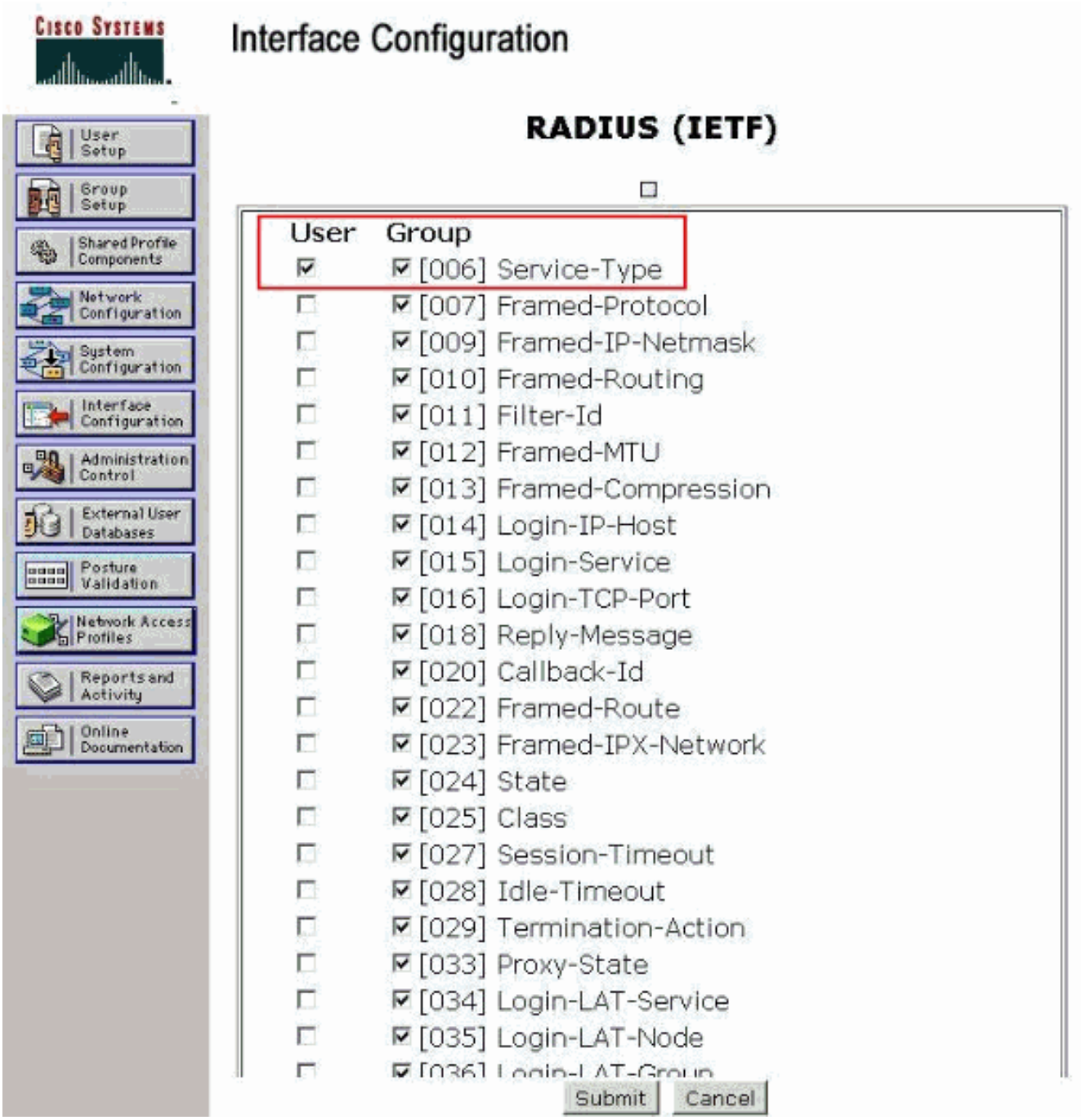
3. Cliquez sur Add**/éditez** afin d'aller à l'utilisateur éditent la page.
4. Sur l'utilisateur éditez la page, fournissez les coordonnées de nom réel, de description et de mot de passe de cet utilisateur.Dans cet exemple, le nom d'utilisateur et mot de passe utilisé sont deux
   lobbyadmin.



5. Faites descendre l'écran à l'IETF RADIUS Attributes plaçant et cochez la case d'**attribut de type de service**.
6. Choisissez le **rappel administratif du** menu déroulant de type de service et cliquez sur Submit.C'est l'attribut qui assigne à cet utilisateur le rôle d'un administrateur de lobby.



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 :Du GUI ACS, choisissez l'**Interface Configuration > RADIUS (IETF)** afin d'activer des attributs IETF dans la fenêtre de configuration utilisateur.Ceci vous amène à la page Settings du RAYON (IETF).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, cochez 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 d'utilisateurs pour des informations détaillées sur la façon configurer et gérer des groupes.

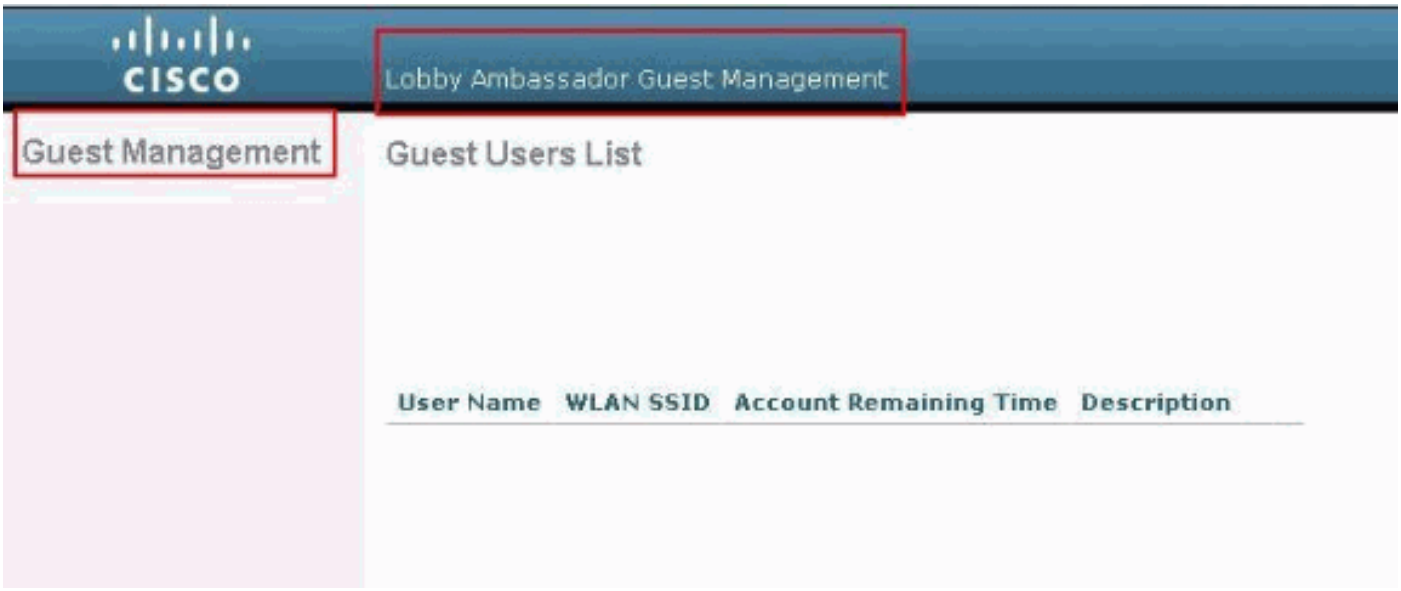
Vérifiez

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Afin de vérifier que votre configuration fonctionne correctement, accédez au WLC par le mode GUI (HTTP/HTTPS).

Remarque: Un ambassadeur de lobby ne peut pas accéder à l'interface CLI de contrôleur et peut donc créer des comptes utilisateurs d'invité seulement du GUI de contrôleur.

Quand l'invite d'ouverture de connexion apparaît, écrivez le nom d'utilisateur et mot de passe comme configuré sur l'ACS. Si vous avez les configurations correctes, vous êtes authentifié avec succès dans le WLC comme **administrateur de lobby**. Cet exemple affiche comment le GUI d'un administrateur de lobby s'occupe de l'authentification réussie :



Remarque: Vous pouvez voir qu'un administrateur de lobby n'a aucune autre option indépendamment de la gestion des utilisateurs d'invité.

Afin de le vérifier du mode CLI, telnet dans le contrôleur en tant qu'administrateur lecture/écriture. Émettez le **debug aaa toute la** commande d'**enable au** contrôleur CLI.

```
(Cisco Controller) >debug aaa all enable (Cisco Controller) > *aaaQueueReader: Aug 26
18:07:35.072: ReProcessAuthentication previous proto 28, next proto 20001 *aaaQueueReader: Aug
26 18:07:35.072: AuthenticationRequest: 0x3081f7dc *aaaQueueReader: Aug 26 18:07:35.072:
Callback.....0x10756dd0 *aaaQueueReader: Aug 26 18:07:35.072:
protocolType.....0x00020001 *aaaQueueReader: Aug 26 18:07:35.072:
proxyState.....00:00:00:40: 00:00-00:00 *aaaQueueReader: Aug 26
18:07:35.072: Packet contains 5 AVPs (not shown) *aaaQueueReader: Aug 26 18:07:35.072:
apfVapRadiusInfoGet: WLAN(0) dynamic int attributes srcAddr: 0x0, gw:0x0, mask:0x0, vlan:0,
dpPort:0, srcPort:0 *aaaQueueReader: Aug 26 18:07:35.073: 00:00:00:40:00:00 Successful
transmission of Authentication Packet (id 39) to 10.77.244.212:1812, proxy state
00:00:00:40:00:00-00:01 *aaaQueueReader: Aug 26 18:07:35.073: 00000000: 01 27 00 47 00 00 00 00
00 00 00 00 00 00 00 00 .'.G..... *aaaQueueReader: Aug 26 18:07:35.073: 00000010: 00 00
00 00 01 0c 6c 6f 62 62 79 61 64 6d 69 6e ......lobbyadmin *aaaQueueReader: Aug 26 18:07:35.073:
00000020: 02 12 5f 5b 5c 12 c5 c8 52 d3 3f 4f 4f 8e 9d 38 .._[\...R.?OO..8 *aaaQueueReader: Aug
26 18:07:35.073: 00000030: 42 91 06 06 00 00 00 07 04 06 0a 4e b1 1a 20 09 B.....N....
*aaaQueueReader: Aug 26 18:07:35.073: 00000040: 57 4c 43 34 34 30 30 WLC4400
*radiusTransportThread: Aug 26 18:07:35.080: 00000000: 02 27 00 40 7e 04 6d 533d ed 79 9c b6 99
d1 f8 .'.@~.mS=.y..... *radiusTransportThread: Aug 26 18:07:35.080: 00000010: d0 5a 8f 4f 08 06
ff ffff ff 06 06 00 00 00 0b .Z.O..... *radiusTransportThread: Aug 26 18:07:35.080:
00000020: 19 20 43 41 43 53 3a 302f 61 65 32 36 2f 61 34 ..CACS:0/ae26/a4
*radiusTransportThread: Aug 26 18:07:35.080: 00000030: 65 62 31 31 61 2f 6c 6f62 62 79 61 64 6d
69 6e eb11a/lobbyadmin *radiusTransportThread: Aug 26 18:07:35.080: ****Enter
processIncomingMessages: response code=2 *radiusTransportThread: Aug 26 18:07:35.080: ****Enter
processRadiusResponse: response code=2 *radiusTransportThread: Aug 26 18:07:35.080:
00:00:00:40:00:00 Access-Accept received from RADIUS server 10.77.244.212 for mobile
00:00:00:40:00:00 receiveId = 0 *radiusTransportThread: Aug 26 18:07:35.080:
AuthorizationResponse: 0x13c73d50 *radiusTransportThread: Aug 26 18:07:35.080:
structureSize.....118 *radiusTransportThread: Aug 26 18:07:35.080:
```

```
resultCode.....................0 *radiusTransportThread: Aug 26 18:07:35.080:
protocolUsed.....................0x00000001 *radiusTransportThread: Aug 26
18:07:35.080: proxyState.....00:00:00:40:00:00-00:00
*radiusTransportThread: Aug 26 18:07:35.080: Packet contains 3 AVPs: *radiusTransportThread: Aug
26 18:07:35.080: AVP[01] Framed-IP-Address.....0xffffffff (-1) (4 bytes)
*radiusTransportThread: Aug 26 18:07:35.080: AVP[02] Service-
Type.....0x0000000b (11) (4 bytes) *radiusTransportThread: Aug 26
18:07:35.080: AVP[03] Class..... CACS:0/ae26/a4eb11a/lobbyadmin
(30 bytes) *emWeb: Aug 26 18:07:35.084: Authentication succeeded for lobbyadmin
```

Dans les informations mises en valeur dans cette sortie, vous pouvez voir que l'attribut de type de service 11 (rappel administratif) est passé sur le contrôleur du serveur ACS et de l'utilisateur est ouvert une session en tant qu'administrateur de lobby.

Ces commandes pourraient être d'aide supplémentaire :

- **enable de détails de debug aaa**
- **enable d'événements de debug aaa**
- **debug aaa packets enable**

Remarque: Référez-vous aux informations importantes sur les commandes de débogage avant d'utiliser les commandes de **débogage**.

Dépannez

Quand vous ouvrez une session à un contrôleur avec des privilèges d'ambassadeur de lobby, vous ne pouvez pas créer un compte utilisateur d'invité avec « une valeur de durée de vie de **0"**, qui est un compte qui n'expire jamais. Dans ces situations, vous recevez la `valeur de vie ne pouvez pas être 0` messages d'erreur.

C'est dû à l'ID de bogue Cisco CSCsf32392 (clients enregistrés seulement), qui est trouvé principalement avec la version 4.0 WLC. Cette bogue a été résolue dans la version 4.1 WLC.

Informations connexes

- Exemple de configuration de l'authentification du serveur RADIUS des utilisateurs de gestion sur le contrôleur
- Configuration de TACACS+ pour un réseau sans fil unifié Cisco
- Guide de configuration Sans fil de contrôleur LAN de Cisco, version 4.0 - Gérer des comptes d'utilisateur
- Exemple de configuration de listes de contrôle d'accès sur un contrôleur de réseau local sans fil
- Contrôleur de réseau local sans fil (WLC) - Forum Aux Questions
- Listes de contrôle d'accès sur les contrôleurs de réseau local sans fil : Règles, limitations et exemples
- Exemple de configuration d'authentification Web externe avec des contrôleurs de réseau local sans fil
- Exemple de configuration de l'authentification Web sur un contrôleur de réseau local sans fil
- Exemple de configuration d'un WLAN invité et d'un WLAN interne à l'aide de contrôleurs de réseau local sans fil (WLC)
- Support et documentation techniques - Cisco Systems