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 nécessaires pour authentifier un administrateur du hall d'entrée du contrôleur LAN sans fil (WLC) avec un serveur RADIUS.

Conditions préalables

Conditions requises

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

- Connaissance de la configuration des paramètres de base sur les WLC
- Connaissance de la configuration d'un serveur RADIUS, tel que Cisco Secure ACS
- Connaissance des utilisateurs invités dans le WLC

Components Used

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

- Contrôleur LAN sans fil Cisco 4400 qui exécute la version 7.0.216.0

- Cisco Secure ACS qui exécute le logiciel version 4.1 et est utilisé comme serveur RADIUS dans cette configuration.

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

Un administrateur de hall, également appelé ambassadeur de hall d'entrée d'un WLC, peut créer et gérer des comptes d'utilisateurs invités sur le contrôleur de réseau local sans fil (WLC). L'ambassadeur du hall d'entrée dispose de privilèges de configuration limités et ne peut accéder qu'aux pages Web utilisées pour gérer les comptes d'invité. L'ambassadeur du hall d'entrée peut spécifier la durée pendant laquelle les comptes d'utilisateurs invités restent actifs. Après l'expiration du délai spécifié, les comptes d'utilisateur invité expirent automatiquement.

Reportez-vous au Guide de déploiement : Accès invité Cisco à l'aide du contrôleur de réseau local sans fil Cisco pour plus d'informations sur les utilisateurs invités.

Afin de créer un compte d'utilisateur invité sur le WLC, vous devez vous connecter au contrôleur en tant qu'administrateur de hall d'entrée. Ce document explique comment un utilisateur est authentifié dans le WLC en tant qu'administrateur de hall d'entrée en fonction des attributs retournés par le serveur RADIUS.

Remarque : L'authentification de l'administrateur du hall d'entrée peut également être effectuée en fonction du compte administrateur du hall configuré localement sur le WLC. Reportez-vous à Création d'un compte Lobby Ambassador pour plus d'informations sur la création d'un compte administrateur de hall localement sur un contrôleur.

Configuration

Dans cette section, vous trouverez les informations sur la façon de configurer le WLC et Cisco Secure ACS pour l'objectif décrit dans ce document.

Configurations

Ce document utilise les configurations suivantes :

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

Dans l'exemple de configuration de ce document, tout utilisateur se connectant au contrôleur avec un nom d'utilisateur et un mot de passe comme lobbyadmin se voit attribuer le rôle

d'administrateur de hall.

Configuration WLC

Avant de démarrer la configuration WLC nécessaire, assurez-vous que votre contrôleur exécute la version 4.0.206.0 ou ultérieure. Ceci est dû au bogue Cisco ID CSCsg89868 (clients enregistrés uniquement) dans lequel l'interface Web du contrôleur affiche des pages Web incorrectes pour l'utilisateur LobbyAdmin lorsque le nom d'utilisateur est stocké dans une base de données RADIUS. LobbyAdmin est présenté avec l'interface ReadOnly au lieu de l'interface LobbyAdmin.

Ce bogue a été résolu dans WLC version 4.0.206.0. Par conséquent, assurez-vous que votre version de contrôleur est 4.0.206.0 ou ultérieure. Référez-vous à Mise à niveau logicielle du contrôleur de réseau local sans fil (WLC) pour obtenir des instructions sur la mise à niveau de votre contrôleur vers la version appropriée.

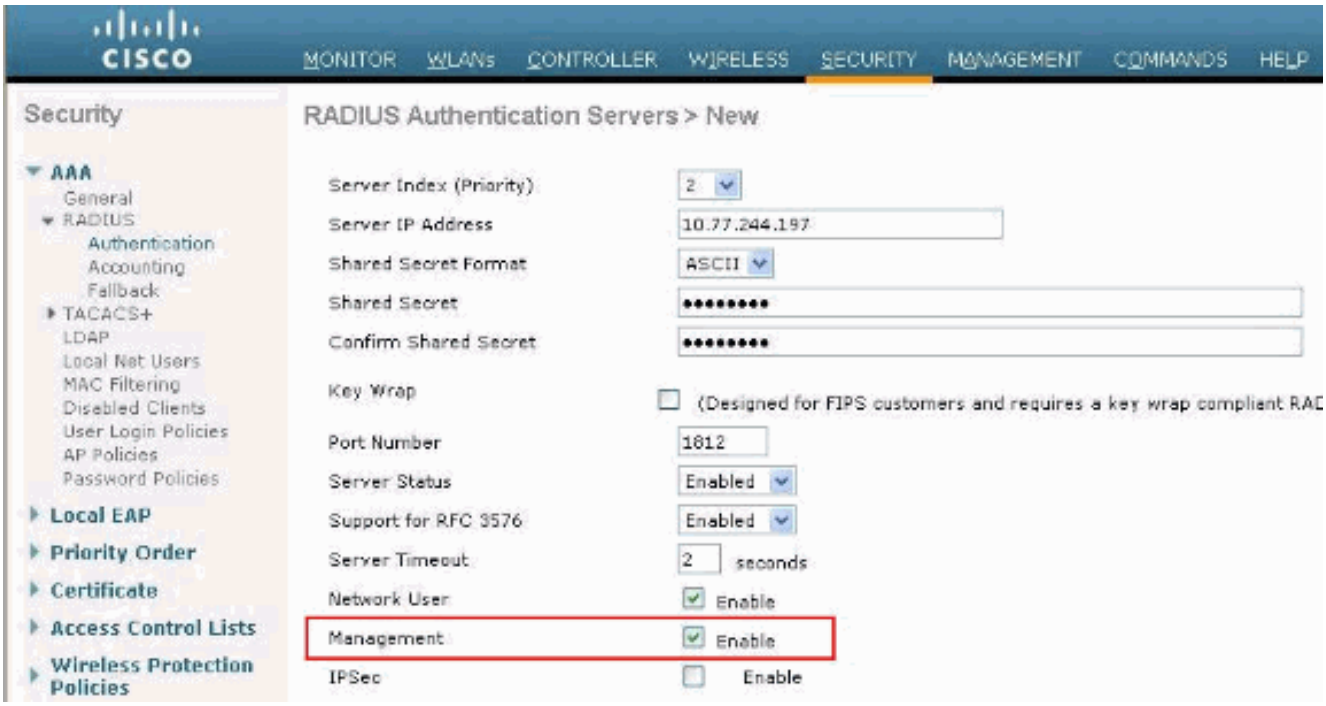
Afin d'exécuter l'authentification de gestion du contrôleur avec le serveur RADIUS, assurez-vous que l'indicateur **Admin-auth-via-RADIUS** est activé sur le contrôleur. Ceci peut être vérifié à partir de la sortie de commande **show radius summary**.

La première étape consiste à configurer les informations du serveur RADIUS sur le contrôleur et à établir l'accessibilité de couche 3 entre le contrôleur et le serveur RADIUS.

Configurer les informations du serveur RADIUS sur le contrôleur

Complétez ces étapes afin de configurer le WLC avec des détails sur l'ACS :

1. Dans l'interface graphique du WLC, sélectionnez l'onglet **Sécurité** et configurez l'adresse IP et le secret partagé du serveur ACS.Ce secret partagé doit être le même sur l'ACS pour que le WLC puisse communiquer avec l'ACS.**Remarque :** Le secret partagé ACS est sensible à la casse. Par conséquent, assurez-vous de saisir correctement les informations secrètes partagées.Cette figure illustre un exemple
:



2. Cochez la case **Gestion** afin de permettre à ACS de gérer les utilisateurs du WLC comme

indiqué dans la figure de l'étape 1. Cliquez ensuite sur **Apply**.

3. Vérifiez l'accessibilité de la couche 3 entre le contrôleur et le serveur RADIUS configuré à l'aide de la commande **ping**. Cette option ping est également disponible sur la page du serveur RADIUS configuré dans l'interface graphique du WLC dans l'onglet **Security>RADIUS Authentication**.Ce schéma montre une réponse ping réussie du serveur RADIUS. Par conséquent, l'accessibilité de couche 3 est disponible entre le contrôleur et le serveur
RADIUS.

Configuration du serveur RADIUS

Complétez les étapes de ces sections afin de configurer le serveur RADIUS :

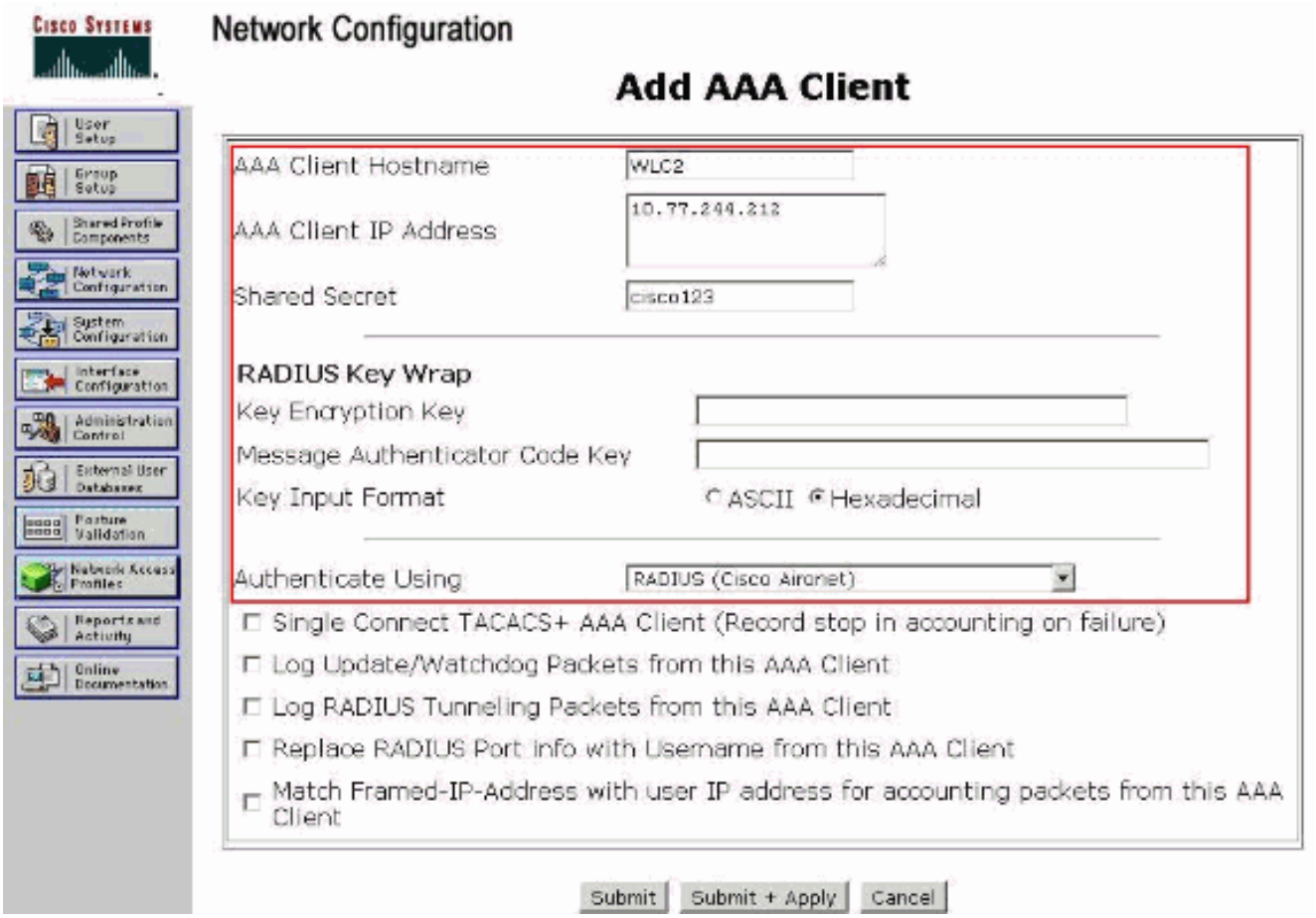
1. Ajouter le WLC en tant que client AAA au serveur RADIUS
2. Configurer l'attribut de type de service RADIUS IETF approprié pour un administrateur de hall d'entrée

Ajouter le WLC en tant que client AAA au serveur RADIUS

Complétez ces étapes afin d'ajouter le WLC en tant que client AAA dans le serveur RADIUS. Comme mentionné précédemment, ce document utilise ACS comme serveur RADIUS. Vous pouvez utiliser n'importe quel serveur RADIUS pour cette configuration.

Complétez ces étapes afin d'ajouter le WLC en tant que client AAA dans ACS :

1. Dans l'interface utilisateur graphique ACS, sélectionnez l'onglet **Configuration réseau**.
2. Sous Clients AAA, cliquez sur **Ajouter une entrée**.
3. Dans la fenêtre Add AAA Client, saisissez le nom d'hôte du WLC, l'adresse IP du WLC et une clé secrète partagée. Reportez-vous à l'exemple de diagramme de l'étape 5.
4. Dans le menu déroulant Authentifier à l'aide, sélectionnez **RADIUS (Cisco Aironet)**.
5. Cliquez sur **Soumettre + Redémarrer** afin d'enregistrer la
configuration.

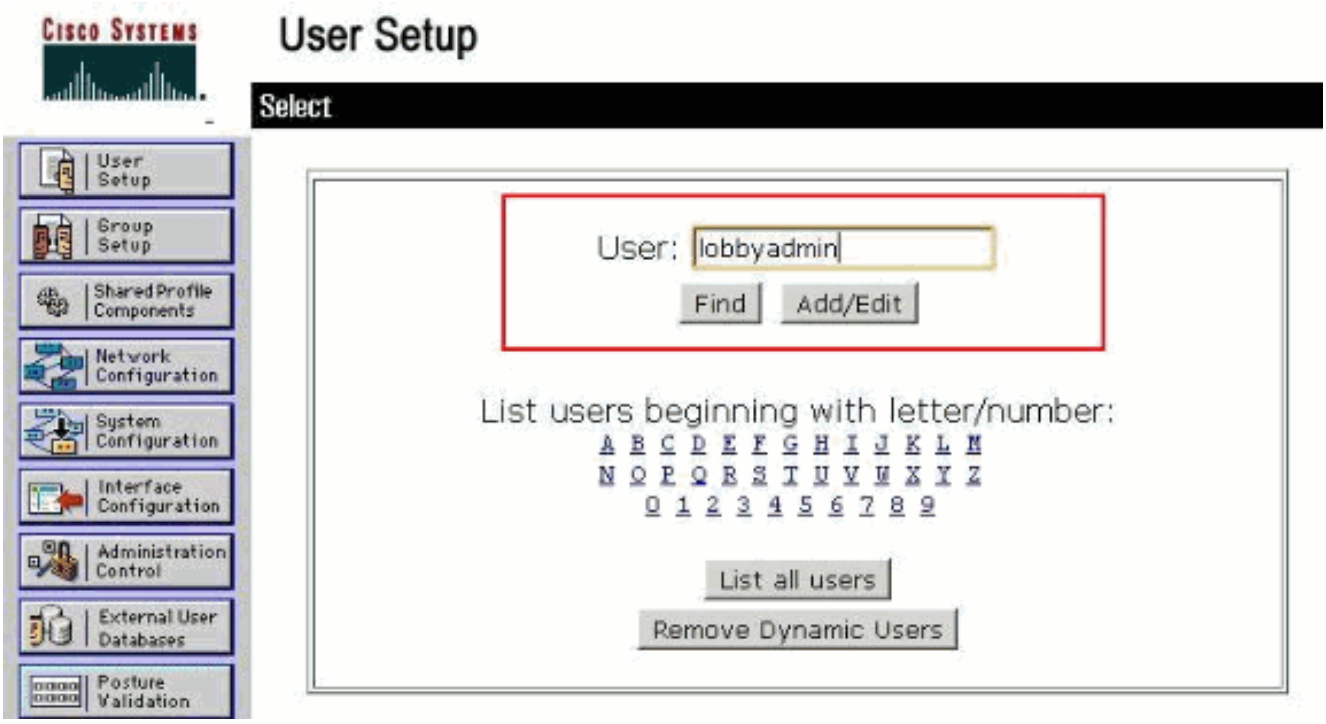


Configurer l'attribut de type de service RADIUS IETF approprié pour un administrateur de hall d'entrée

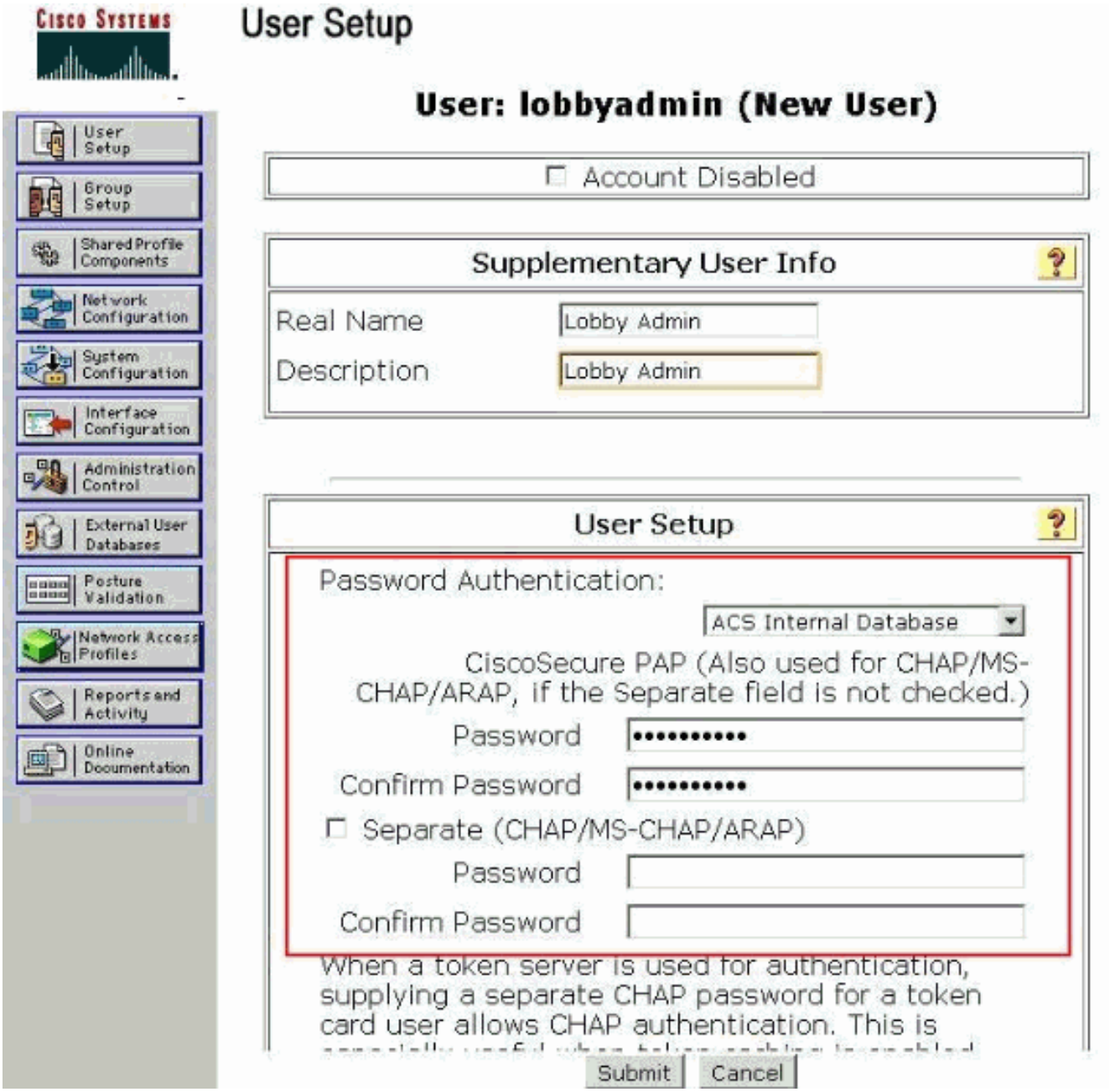
Afin d'authentifier un utilisateur de gestion d'un contrôleur en tant qu'administrateur de hall via le serveur RADIUS, vous devez ajouter l'utilisateur à la base de données RADIUS avec l'attribut de type de service RADIUS IETF défini sur **Callback Administrative**. Cet attribut attribue à l'utilisateur spécifique le rôle d'administrateur de hall d'entrée sur un contrôleur.

Ce document montre l'exemple d'utilisateur lobbyadmin en tant qu'administrateur de hall. Afin de configurer cet utilisateur, procédez comme suit sur ACS :

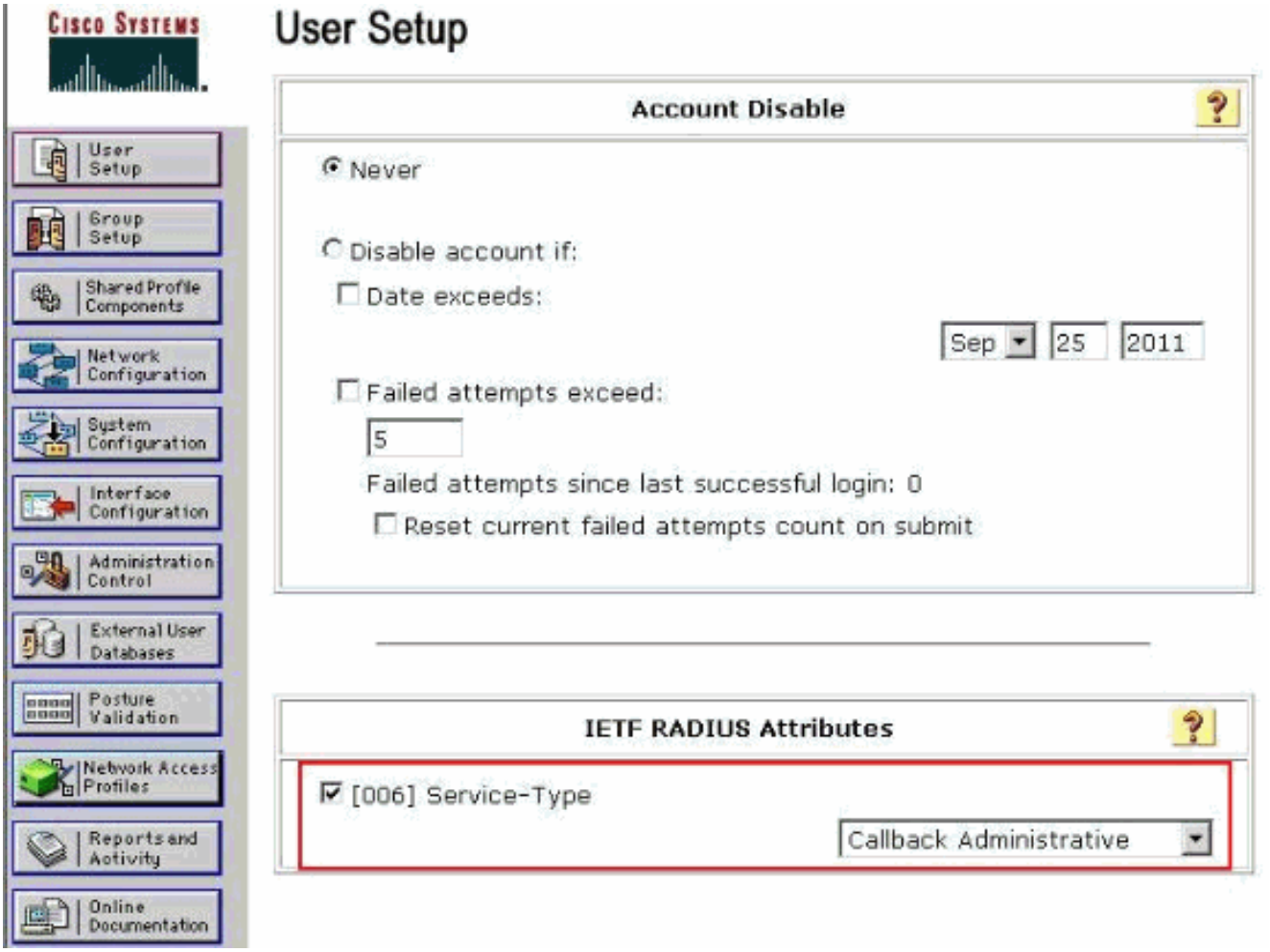
1. Dans l'interface utilisateur graphique ACS, sélectionnez l'onglet **User Setup**.
2. Entrez le nom d'utilisateur à ajouter à ACS comme le montre cet exemple de fenêtre :



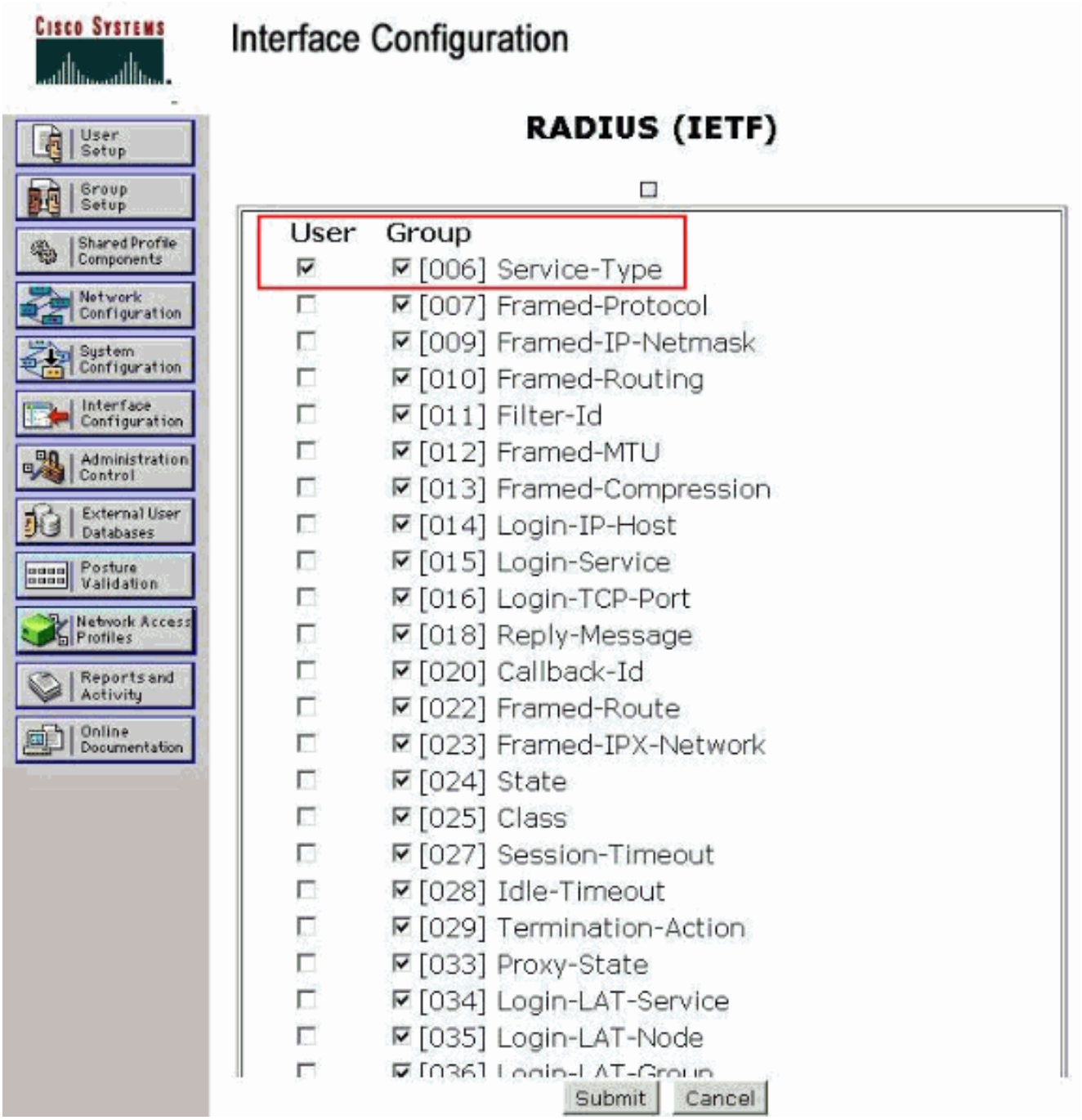
3. Cliquez sur **Ajouter/Modifier** afin d'accéder à la page Modifier l'utilisateur.
4. Sur la page User Edit, indiquez le nom réel, la description et le mot de passe de cet utilisateur.Dans cet exemple, le nom d'utilisateur et le mot de passe utilisés sont lobbyadmin.



5. Faites défiler jusqu'au paramètre IETF RADIUS Attributes et cochez la case **Service-Type Attribute**.
6. Choisissez **Callback Administrative** dans le menu déroulant Service-Type et cliquez sur **Submit**.Cet attribut attribue à cet utilisateur le rôle d'administrateur de hall d'entrée.



Parfois, cet attribut Service-Type n'est pas visible sous les paramètres utilisateur. Dans ce cas, procédez comme suit afin de le rendre visible :Dans l'interface graphique ACS, sélectionnez **Interface Configuration > RADIUS (IETF)** afin d'activer les attributs IETF dans la fenêtre User Configuration.Cela vous amène à la page Paramètres RADIUS (IETF).Dans la page Paramètres RADIUS (IETF), vous pouvez activer l'attribut IETF qui doit être visible sous les paramètres utilisateur ou groupe. Pour cette configuration, cochez **Service-Type** pour la colonne User et cliquez sur **Submit**.Cette fenêtre présente un exemple
:



Remarque : Cet exemple spécifie l'authentification par utilisateur. Vous pouvez également effectuer l'authentification en fonction du groupe auquel appartient un utilisateur particulier. Dans de tels cas, cochez la case **Groupe** pour que cet attribut soit visible sous Paramètres de groupe.**Remarque :** En outre, si l'authentification est basée sur un groupe, vous devez affecter des utilisateurs à un groupe particulier et configurer les attributs IETF du paramètre de groupe pour fournir des privilèges d'accès aux utilisateurs de ce groupe. Référez-vous à Gestion des groupes d'utilisateurs pour des informations détaillées sur la façon de configurer et de gérer les groupes.

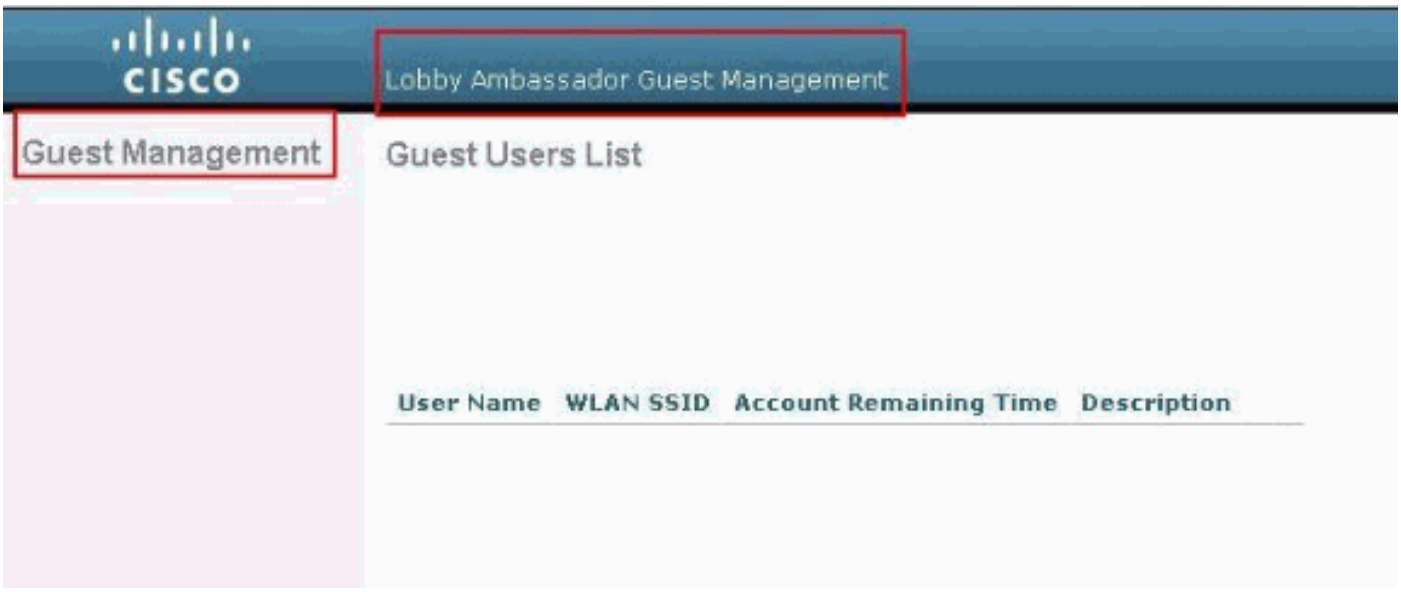
Vérification

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

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

Remarque : Un ambassadeur du hall d'entrée ne peut pas accéder à l'interface de ligne de commande du contrôleur et peut donc créer des comptes d'utilisateurs invités uniquement à partir de l'interface utilisateur graphique du contrôleur.

Lorsque l'invite de connexion apparaît, saisissez le nom d'utilisateur et le mot de passe configurés sur l'ACS. Si les configurations sont correctes, vous êtes authentifié avec succès dans le WLC en tant qu'**administrateur de hall d'entrée**. Cet exemple montre comment l'interface utilisateur graphique d'un administrateur de hall d'entrée gère l'authentification réussie :



Remarque : Vous pouvez voir qu'un administrateur de hall d'entrée n'a pas d'autre option que la gestion des utilisateurs invités.

Afin de le vérifier à partir du mode CLI, établissez une connexion Telnet avec le contrôleur en tant qu'administrateur en lecture-écriture. Émettez la commande **debug aaa all enable** au niveau de l'interface de ligne de commande du contrôleur.

```
(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 en surbrillance de cette sortie, vous pouvez voir que l'attribut de type de service 11 (Callback Administrative) est transmis au contrôleur à partir du serveur ACS et que l'utilisateur est connecté en tant qu'administrateur de hall d'entrée.

Ces commandes peuvent être utiles :

- **debug aaa details enable**
- **debug aaa events enable**
- **debug aaa packets enable**

Remarque : Consulter les renseignements importants sur les commandes de débogage avant d'utiliser les commandes de **débogage**.

Dépannage

Lorsque vous connectez à un contrôleur disposant des privilèges d'ambassadeur du hall d'entrée, vous ne pouvez pas créer un compte d'utilisateur invité avec une valeur de durée de vie "**0**« , qui est un compte qui n'expire jamais. Dans ces situations, vous recevez le message d'erreur `Lifetime not be 0`.

Ceci est dû au bogue Cisco ID CSCsf32392 (clients enregistrés uniquement) , qui se trouve

principalement avec WLC version 4.0. Ce bogue a été résolu dans WLC version 4.1.

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 du contrôleur de réseau local sans fil Cisco, version 4.0 - Gérer des comptes utilisateurs
- 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