

Configurer un WLC et un ACS pour authentifier les utilisateurs de gestion

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Conventions](#)

[Informations générales](#)

[Configurer](#)

[Diagramme du réseau](#)

[Configurations](#)

[Configuration WLC](#)

[Configurer le WLC pour accepter la gestion via le serveur Cisco Secure ACS](#)

[Configuration de Cisco Secure ACS](#)

[Ajouter le WLC en tant que client AAA au serveur RADIUS](#)

[Configurer les utilisateurs et leurs attributs IETF RADIUS appropriés](#)

[Configurer un utilisateur avec un accès en lecture-écriture](#)

[Configurer un utilisateur avec un accès en lecture seule](#)

[Gérer le WLC localement ainsi que par le biais du serveur RADIUS](#)

[Vérifier](#)

[Dépannage](#)

[Informations connexes](#)

Introduction

Ce document décrit comment configurer un WLC et un Cisco Secure ACS afin que le serveur AAA puisse authentifier les utilisateurs de gestion sur le contrôleur.

Conditions préalables

Exigences

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

Composants utilisés

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 la version logicielle 4.1 et qui 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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Conventions

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

Informations générales

Ce document explique comment configurer un contrôleur LAN sans fil (WLC) et un serveur de contrôle d'accès (Cisco Secure ACS) de sorte que le serveur d'authentification, d'autorisation et de comptabilité (AAA) puisse authentifier les utilisateurs de gestion sur le contrôleur. Le document explique également comment différents utilisateurs de gestion peuvent recevoir différents privilèges avec des attributs spécifiques au fournisseur (VSA) retournés à partir du serveur RADIUS Cisco Secure ACS.

Configurer

Dans cette section, vous êtes présenté avec les informations sur la façon de configurer le WLC et l'ACS à la fin décrite dans ce document.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :

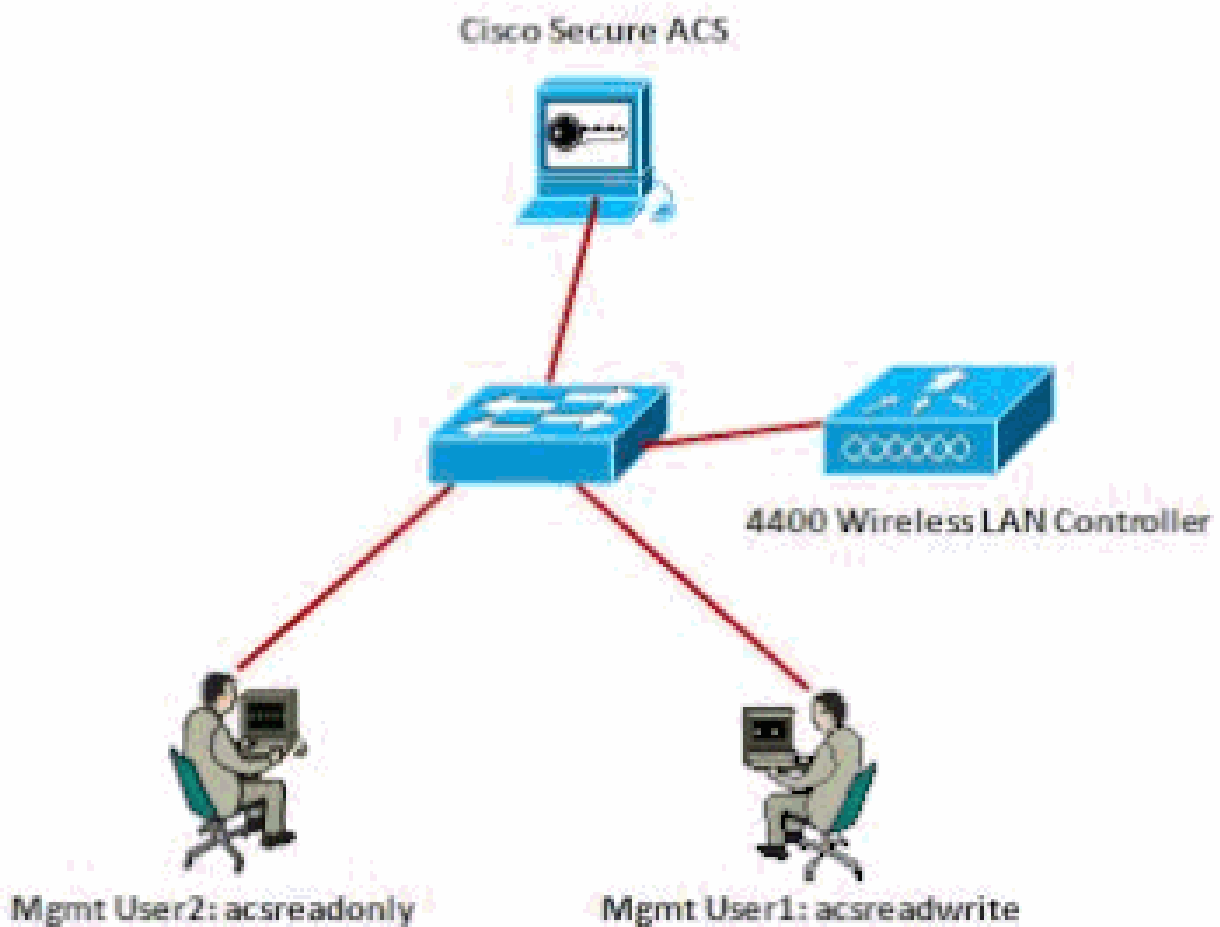


Diagramme du réseau

Cet exemple de configuration utilise les paramètres suivants :

- Adresse IP de Cisco Secure ACS : 172.16.1.1/255.255.0.0
- Adresse IP de l'interface de gestion du contrôleur : 172.16.1.30/255.255.0.0
- Clé secrète partagée utilisée sur le point d'accès et le serveur RADIUS : asdf1234
- Voici les informations d'identification des deux utilisateurs que cet exemple configure sur ACS :
 1. Nom d'utilisateur - acsreadwrite
Mot de passe - acsreadwrite
 2. Nom d'utilisateur - acsreadonly
Mot de passe - acsreadonly

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

- Tout utilisateur qui se connecte au WLC avec le nom d'utilisateur et le mot de passe asacsreadwrite bénéficie d'un accès administratif complet au WLC.
- Tout utilisateur qui se connecte au WLC avec le nom d'utilisateur et le mot de passe comme acsreadonly a un accès en lecture seule au WLC.

Configurations

Ce document utilise les configurations suivantes :

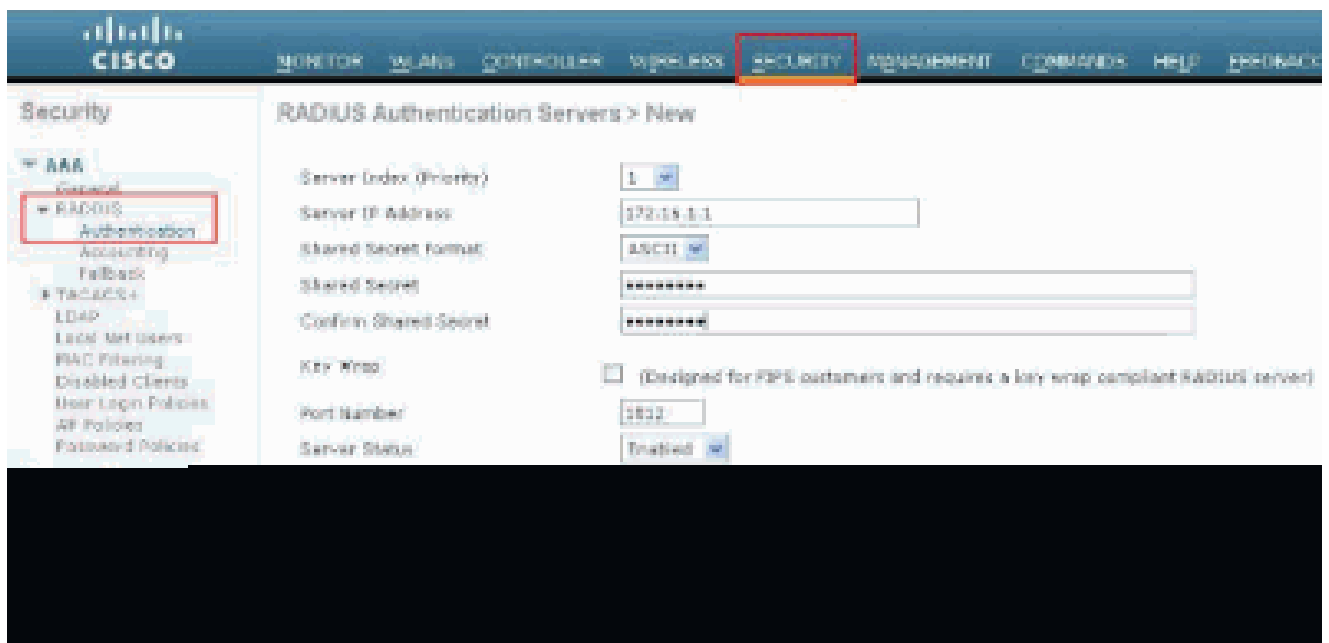
- [Configuration WLC](#)
- [Configuration de Cisco Secure ACS](#)

Configuration WLC

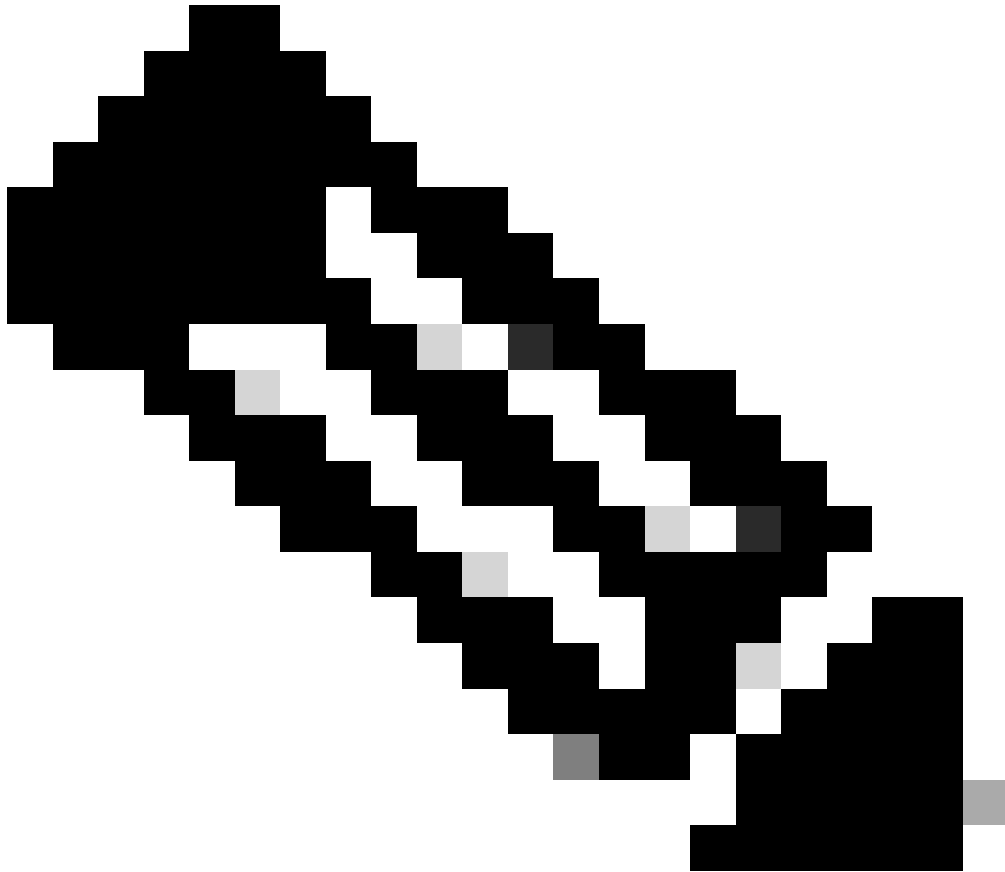
Configurer le WLC pour accepter la gestion via le serveur Cisco Secure ACS

Complétez ces étapes afin de configurer le WLC de sorte qu'il communique avec le serveur RADIUS :

1. Dans l'interface graphique utilisateur du WLC, cliquez sur Security. Dans le menu de gauche, cliquez sur RADIUS > Authentication. La page RADIUS Authentication serverspage s'affiche. Pour ajouter un nouveau serveur RADIUS, cliquez sur New. Dans la page RADIUS Authentication Servers > New, entrez les paramètres spécifiques au serveur RADIUS. Voici un exemple.

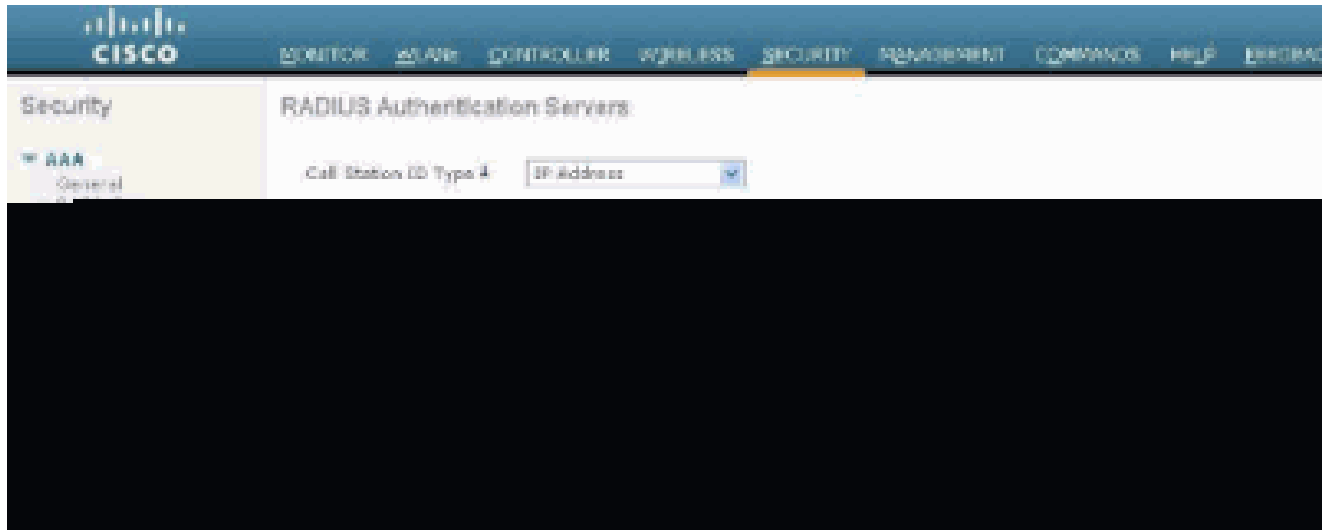


2. Cochez la case d'option Management afin de permettre au serveur RADIUS d'authentifier les utilisateurs qui se connectent au WLC.



Remarque : assurez-vous que le secret partagé configuré sur cette page correspond au secret partagé configuré sur le serveur RADIUS. C'est seulement alors que le WLC peut communiquer avec le serveur RADIUS.

-
3. Vérifiez si le WLC est configuré pour être géré par Cisco Secure ACS. Pour ce faire, cliquez sur Security depuis l'interface graphique du WLC. La fenêtre GUI résultante ressemble à cet exemple.



Vous pouvez voir que la case à cocher Gestion est activée pour le serveur RADIUS 172.16.1.1. Ceci illustre que ACS est autorisé à authentifier les utilisateurs de gestion sur le WLC.

Configuration de Cisco Secure ACS

Complétez les étapes dans ces sections afin de configurer l'ACS :

1. [Ajouter le WLC en tant que client AAA au serveur RADIUS](#)
2. [Configurer les utilisateurs et leurs attributs IETF RADIUS appropriés](#)
3. [Configurer un utilisateur avec un accès en lecture-écriture](#)
4. [Configurer un utilisateur avec un accès en lecture seule](#)

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 Cisco Secure ACS :

1. Dans l'interface graphique ACS, cliquez sur Network Configuration.
2. Sous Clients AAA, cliquez sur Ajouter une entrée.
3. Dans la fenêtre Add AAA Client, entrez le nom d'hôte du WLC, l'adresse IP du WLC et une clé secrète partagée.

Dans cet exemple, voici les paramètres :

- Le nom d'hôte du client AAA est WLC-4400.
- 172.16.1.30/16 est l'adresse IP du client AAA, qui, dans ce cas, est le WLC.
- La clé secrète partagée est asdf1234.

Network Configuration

Add AAA Client

AAA Client Hostname:

AAA Client IP Address:

Shared Secret:

RADIUS Key Wrap

Key Encryption Key:

Message Authenticator Code Key:

Key Input Format: ASCII Hexadecimal

Authenticate Using:

Single Connect TACACS+ AAA Client (Record stop in accounting on failure)

Log Update/Watchdog Packets from this AAA Client

Log RADIUS Tunneling Packets from this AAA Client

Replace RADIUS Port info with Username from this AAA Client

Match Framed-IP-Address with user IP address for accounting packets from this AAA Client

Fenêtre Ajouter un client AAA

Cette clé secrète partagée doit être la même que la clé secrète partagée que vous configurez sur le WLC.

4. Dans le menu déroulant Authenticate Using, sélectionnez RADIUS (Cisco Airespace).
5. Cliquez sur Submit + Restart afin d'enregistrer la configuration.

Configurer les utilisateurs et leurs attributs IETF RADIUS appropriés

Afin d'authentifier un utilisateur via un serveur RADIUS, pour la connexion et la gestion du contrôleur, vous devez ajouter l'utilisateur à la base de données RADIUS avec l'attribut IETF RADIUS Service-Type défini à la valeur appropriée basée sur les privilèges utilisateur.

- Afin de définir des privilèges de lecture-écriture pour l'utilisateur, définissez l'attribut Service-Type sur Administrative.
- Afin de définir des privilèges en lecture seule pour l'utilisateur, définissez l'attribut Service-Type sur NAS-Prompt.

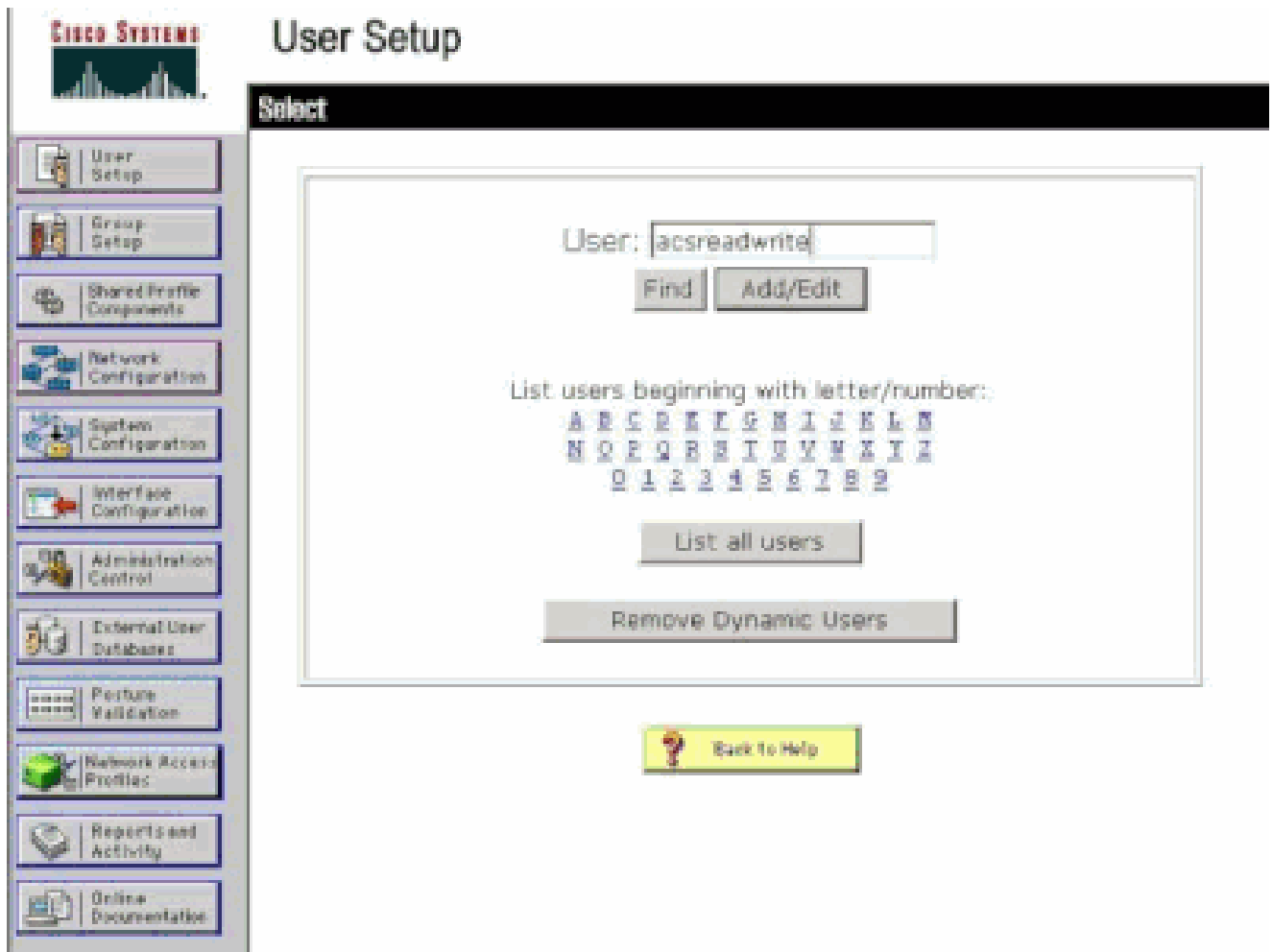
Configurer un utilisateur avec un accès en lecture-écriture

Le premier exemple montre la configuration d'un utilisateur avec un accès complet au WLC. Lorsque cet utilisateur tente de se connecter au contrôleur, le serveur RADIUS s'authentifie et fournit à cet utilisateur un accès administratif complet.

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

Complétez 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 le montre cet exemple de fenêtre.



Fenêtre Configuration utilisateur

3. Cliquez sur Add/Edit afin d'accéder à la page User Edit.
4. Dans la page User Edit, indiquez le nom réel, la description et le mot de passe de cet utilisateur.
5. Faites défiler jusqu'au paramètre IETF RADIUS Attributes et cochez Service-Type Attribute.
6. Puisque, dans cet exemple, l'utilisateur acsreadwrite doit avoir un accès complet, choisissez Administrative pour le menu déroulant Service-Type et cliquez sur Submit.

Cela garantit que cet utilisateur particulier a un accès en lecture-écriture au WLC.

Paramètres des attributs ETF RADIUS

Parfois, cet attribut Service-Type n'est pas visible sous les paramètres utilisateur. Dans ce cas, suivez ces étapes afin de le rendre visible.

1. Dans l'interface graphique ACS, naviguez vers Interface Configuration > RADIUS (IETF) afin d'activer les attributs IETF dans la fenêtre User Configuration.

La page RADIUS (IETF) Settings s'affiche.

2. Dans la page RADIUS (IETF) Settings, vous pouvez activer l'attribut IETF qui doit être visible sous les paramètres de l'utilisateur ou du groupe. Pour cette configuration, cochez Service-Type pour la colonne User et cliquez sur Submit. Cette fenêtre présente un exemple.

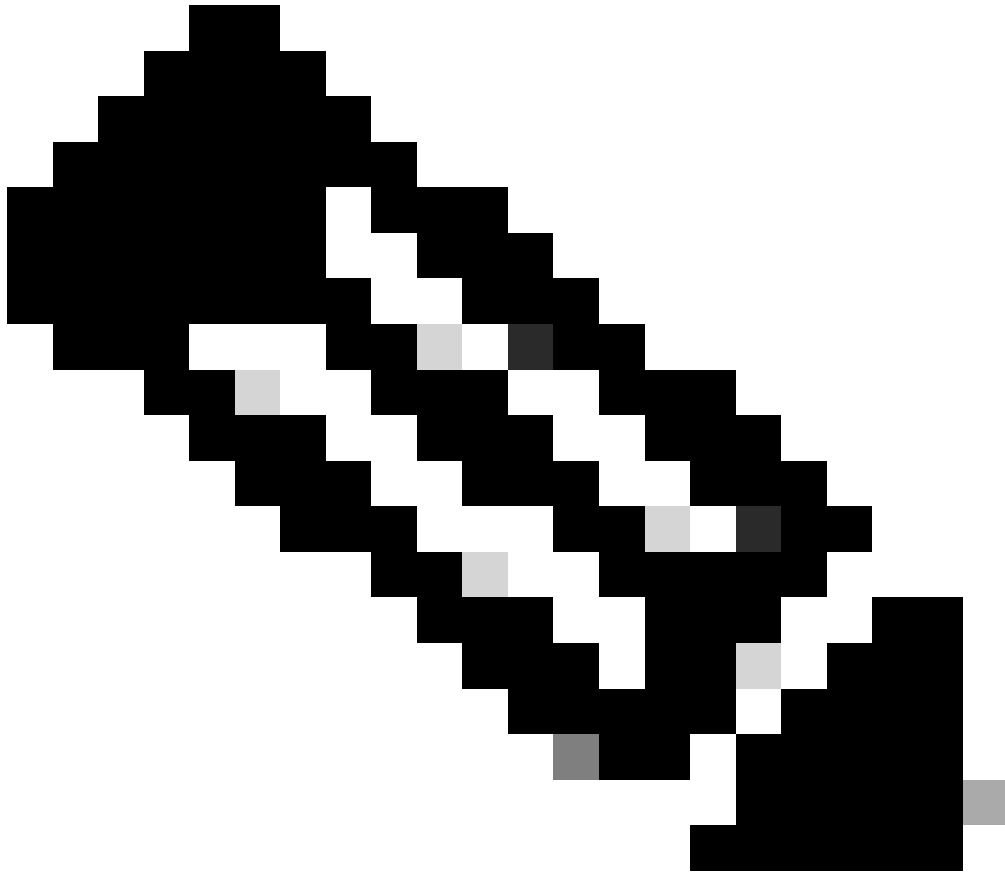


Interface Configuration

RADIUS (IETF)

- User Setup
- Group Setup
- Shared Profile Components
- Network Configuration
- System Configuration
- Interface Configuration
- Administration Control
- External User Database
- Posture Validation
- Network Access Profiles
- Reports and Activity
- Online Documentation

User	Group
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> [006] Service-Type
<input type="checkbox"/>	<input checked="" type="checkbox"/> [007] Framed-Protocol
<input type="checkbox"/>	<input checked="" type="checkbox"/> [009] Framed-IP-Netmask
<input type="checkbox"/>	<input checked="" type="checkbox"/> [010] Framed-Routing
<input type="checkbox"/>	<input checked="" type="checkbox"/> [011] Filter-Id
<input type="checkbox"/>	<input checked="" type="checkbox"/> [012] Framed-MTU
<input type="checkbox"/>	<input checked="" type="checkbox"/> [013] Framed-Compression
<input type="checkbox"/>	<input checked="" type="checkbox"/> [014] Login-IP-Host
<input type="checkbox"/>	<input checked="" type="checkbox"/> [015] Login-Service
<input type="checkbox"/>	<input checked="" type="checkbox"/> [016] Login-TCP-Port
<input type="checkbox"/>	<input checked="" type="checkbox"/> [018] Reply-Message
<input type="checkbox"/>	<input checked="" type="checkbox"/> [020] Callback-Id
<input type="checkbox"/>	<input checked="" type="checkbox"/> [022] Framed-Route
<input type="checkbox"/>	<input checked="" type="checkbox"/> [023] Framed-IPX-Network
<input type="checkbox"/>	<input checked="" type="checkbox"/> [024] State
<input type="checkbox"/>	<input checked="" type="checkbox"/> [025] Class
<input type="checkbox"/>	<input checked="" type="checkbox"/> [027] Session-Timeout
<input type="checkbox"/>	<input checked="" type="checkbox"/> [028] Idle-Timeout



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

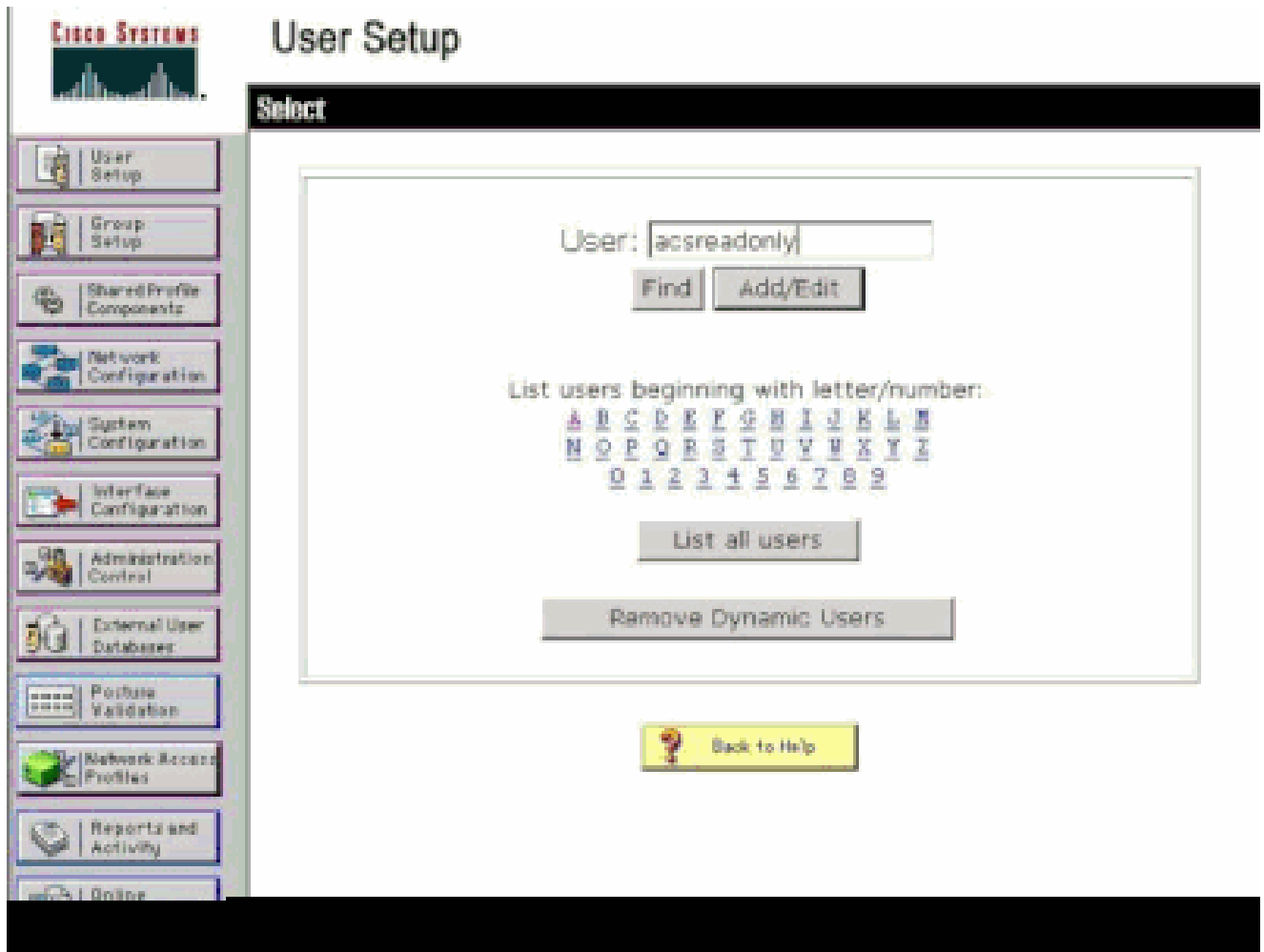
Configurer un utilisateur avec un accès en lecture seule

Cet exemple montre la configuration d'un utilisateur avec un accès en lecture seule au WLC. Lorsque cet utilisateur tente de se connecter au contrôleur, le serveur RADIUS s'authentifie et fournit à cet utilisateur un accès en lecture seule.

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


Complétez 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 souhaitez ajouter à l'ACS et cliquez sur Add/Edit afin d'accéder à la page User Edit.



Ajouter un nom d'utilisateur

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



User Setup

Edit

User: acsreadonly (New User)

Account Disabled

Supplementary User Info

Real Name:

Description:

User Setup

Password Authentication:

CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)

Password:

Confirm Password:

Separate (CHAP/MS-CHAP/ARAP)

Password:

Confirm Password:

When a token server is used for authentication, supplying a

Fournissez le nom réel, la description et le mot de passe de l'utilisateur ajouté

4. Faites défiler jusqu'au paramètre IETF RADIUS Attributes et cochez Service-Type Attribute.
5. Comme, dans cet exemple, l'utilisateur acsreadonly doit avoir un accès en lecture seule, choisissez NAS Prompt dans le menu déroulant Service-Type et cliquez sur Submit.

Cela garantit que cet utilisateur particulier a un accès en lecture seule au WLC.

Cisco Systems

User Setup

Account Disable

Never

Disable account if:

Date exceeds: Sep 22 2011

Failed attempts exceed:

Failed attempts since last successful login: 0

Reset current failed attempts count on submit:

IETF RADIUS Attributes

[006] Service-Type

Authenticate only

Authenticate only

NAS Prompt

Outbound

Callback NAS Prompt

Administrative

Callback Administrative

Callback login

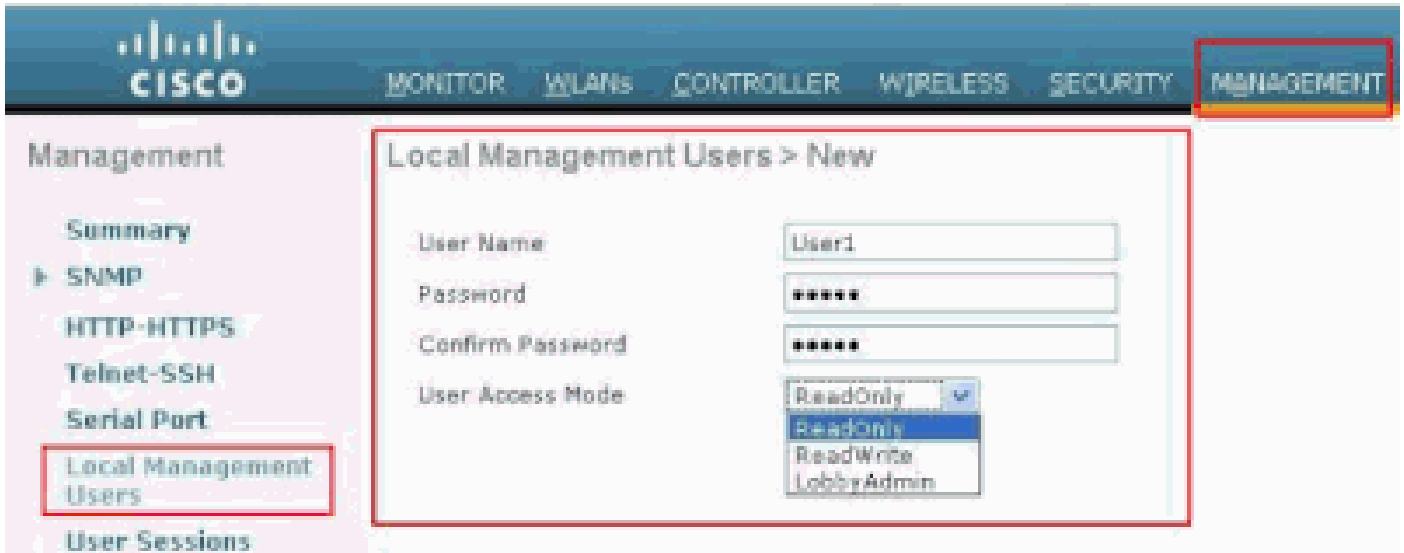
Framed

Back to Help

Vérifier l'attribut Service-Type

Gérer le WLC localement ainsi que par le biais du serveur RADIUS

Vous pouvez également configurer les utilisateurs de gestion localement sur le WLC. Vous pouvez le faire à partir de l'interface graphique du contrôleur, sous Management > Local Management Users.



Configurer les utilisateurs de gestion localement sur le WLC

Supposons que le WLC est configuré avec des utilisateurs de gestion à la fois localement et dans le serveur RADIUS avec la case à cocher Management activée. Dans un tel scénario, par défaut, quand un utilisateur tente de se connecter au WLC, le WLC se comporte de cette manière :

1. Le WLC examine d'abord les utilisateurs de gestion locaux définis pour valider l'utilisateur. Si l'utilisateur figure dans sa liste locale, il autorise l'authentification pour cet utilisateur. Si cet utilisateur n'apparaît pas localement, il recherche le serveur RADIUS.
2. Si le même utilisateur existe à la fois localement, ainsi que dans le serveur RADIUS, mais avec des privilèges d'accès différents, alors le WLC authentifie l'utilisateur avec les privilèges spécifiés localement. En d'autres termes, la configuration locale sur le WLC est toujours prioritaire par rapport au serveur RADIUS.

L'ordre d'authentification des utilisateurs de gestion peut être modifié sur le WLC. Pour ce faire, à partir de la page Security sur le WLC, cliquez sur Priority Order > Management User. Dans cette page, vous pouvez spécifier l'ordre d'authentification. Voici un exemple.

CISCO [MONITOR](#) [WLAN](#) [CONTROLLER](#) [WIRELESS](#) **[SECURITY](#)** [MANAGEMENT](#) [COMMANDS](#) [HELP](#)

Security: **Priority Order > Management User**

AAA

- General
- RADIUS**
 - Authentication
 - Accounting
 - Fallback
- TACACS+**
- LDAP
 - Local Net Users
 - MAC Filtering
 - Disabled Clients
 - User Logs Policies
 - AP Policies
 - Password Policies
- Local ERP**
- Priority Order**
 - Management User**
- Certificate**
- Access Control Lists**

Authentication:

Not Used

TACACS+

>

<

Order Used for Authentication

LOCAL RADIUS

Up

Down

If LOCAL is selected as second priority, then user will be authenticated against LOCAL only if first priority is unreachable.

Ordre de priorité > Sélection de l'utilisateur Management



Remarque : si LOCAL est sélectionné comme deuxième priorité, l'utilisateur est authentifié avec cette méthode uniquement si la méthode définie comme première priorité (RADIUS/ TACACS) est inaccessible.

Vérifier

Afin de vérifier si votre configuration fonctionne correctement, accédez au WLC via l'interface de ligne de commande ou le mode GUI (HTTP/HTTPS). Lorsque l'invite de connexion apparaît, tapez le nom d'utilisateur et le mot de passe configurés sur Cisco Secure ACS.

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

Vous pouvez également vous assurer que l'utilisateur authentifié dispose des restrictions d'accès spécifiées par l'ACS. Pour ce faire, accédez à l'interface graphique utilisateur du WLC via HTTP/HTTPS (assurez-vous que le WLC est configuré pour autoriser HTTP/HTTPS).

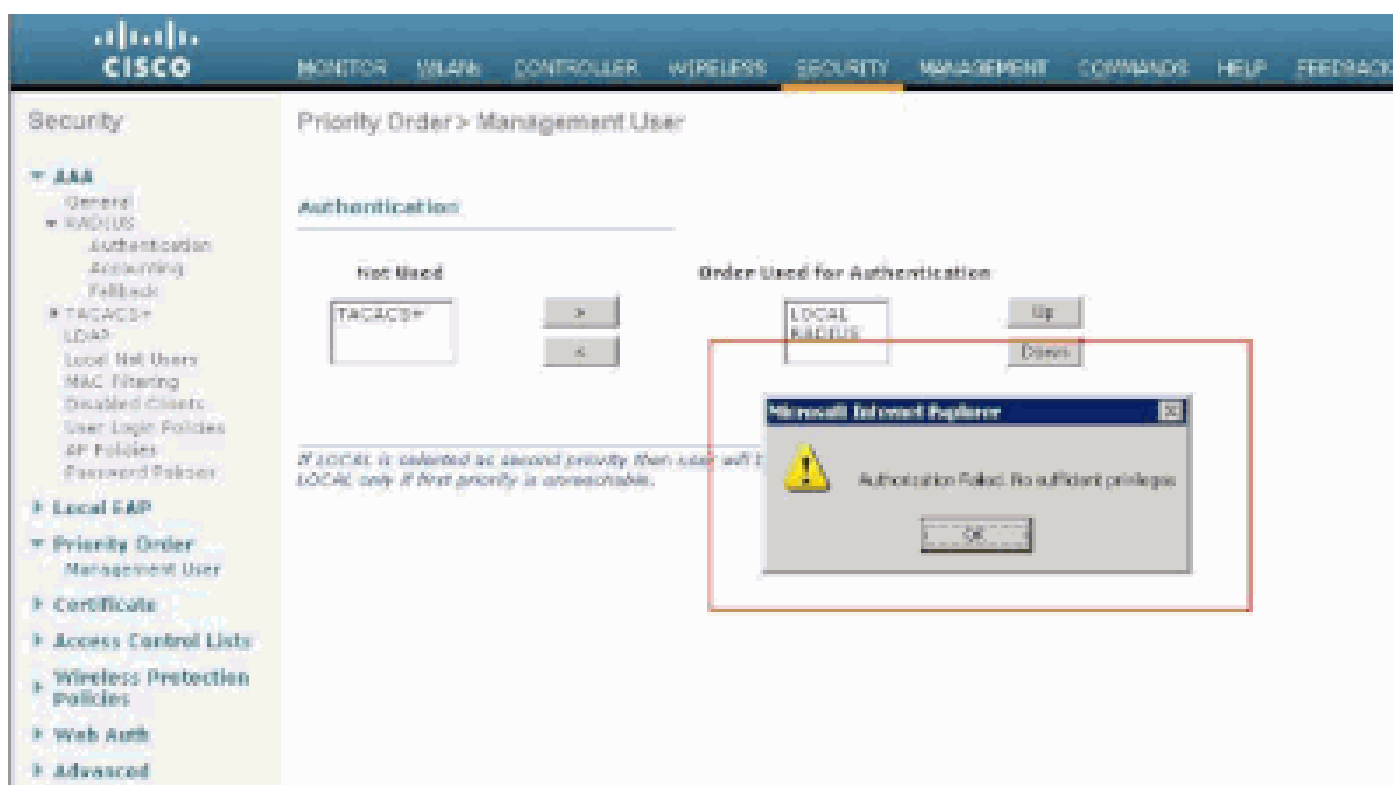
Un utilisateur avec un accès en lecture-écriture défini dans l'ACS a plusieurs privilèges

configurables dans le WLC. Par exemple, un utilisateur en lecture-écriture a le privilège de créer un nouveau WLAN sous la page WLANs du WLC. Cette fenêtre présente un exemple.



Privilèges configurables dans le WLC

Lorsqu'un utilisateur avec des privilèges de lecture seule tente de modifier la configuration sur le contrôleur, l'utilisateur voit ce message.



Impossible de modifier le contrôleur avec un accès en lecture seule

Ces restrictions d'accès peuvent également être vérifiées via l'interface de ligne de commande du WLC. La sortie ci-dessous est un exemple.

```
<#root>
```

```
(Cisco Controller) >
```

```
?
```

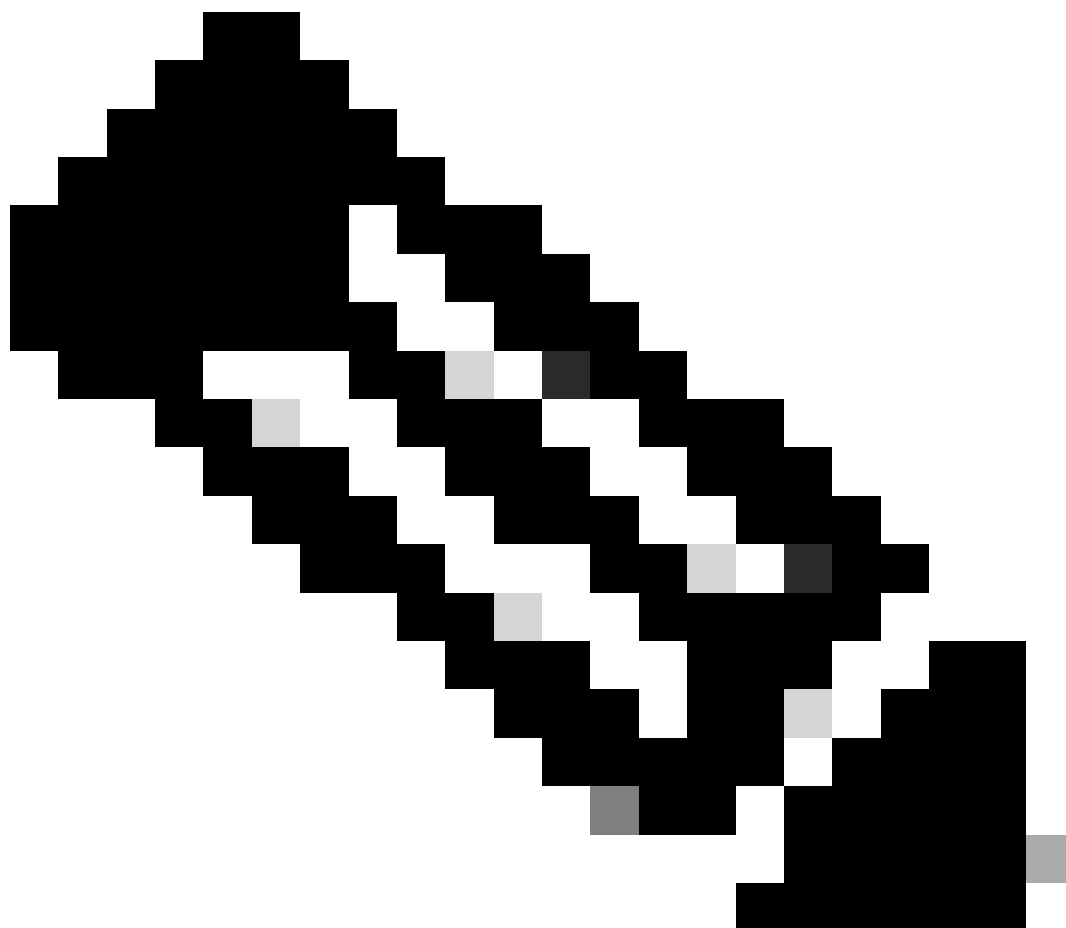
```
debug          Manages system debug options.
help           Help
linktest       Perform a link test to a specified MAC address.
```

```
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 le montre cet exemple de résultat, un?au niveau de l'interface de ligne de commande du contrôleur affiche une liste des commandes disponibles pour l'utilisateur actuel. Notez également que la **config** commande n'est pas disponible dans cet exemple de résultat. Ceci montre qu'un utilisateur en lecture seule n'a pas le privilège d'effectuer des configurations sur le WLC. Par contre, un utilisateur en lecture-écriture a les privilèges nécessaires pour effectuer des configurations sur le contrôleur (mode GUI et mode CLI).



Remarque : même après avoir authentifié un utilisateur WLC via le serveur RADIUS, lorsque vous naviguez de page en page, le serveur HTTP[S] authentifie toujours complètement le client à chaque fois. La seule raison pour laquelle vous n'êtes pas invité à vous authentifier sur chaque page est que votre navigateur met en cache et rejoue vos informations d'identification.

Dépannage

Dans certaines circonstances, lorsqu'un contrôleur authentifie des utilisateurs de gestion via l'ACS, l'authentification se termine avec succès (acceptation d'accès) et vous ne voyez aucune erreur d'autorisation sur le contrôleur. Cependant, l'utilisateur est de nouveau invité à s'authentifier.

Dans de tels cas, vous ne pouvez pas interpréter ce qui est mal et pourquoi l'utilisateur ne peut pas se connecter au WLC avec seulement la **debug aaa events enable** commande. Au lieu de cela, le contrôleur affiche une autre invite d'authentification.

L'une des raisons possibles est que l'ACS n'est pas configuré pour transmettre l'attribut Service-Type pour cet utilisateur ou ce groupe particulier même si le nom d'utilisateur et le mot de passe sont correctement configurés sur l'ACS.

Le résultat de la **debug aaa events enable** commande n'indique pas qu'un utilisateur ne possède pas les attributs requis (pour cet exemple, l'attribut Service-Type) même si un **access-accept** est renvoyé à partir du serveur AAA. Dans cet exemple, le résultat de la **debug aaa events enable** commande montre un exemple.

```
<#root>
```

```
(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
```

```
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 ce premier exemple de sortie de **debug aaa events enable** commande, vous voyez que Access-Accept est reçu avec succès du serveur RADIUS mais que l'attribut Service-Type n'est pas passé sur le WLC. Ceci est dû au fait que l'utilisateur particulier n'est pas configuré avec cet attribut sur l'ACS.

Cisco Secure ACS doit être configuré pour renvoyer l'attribut Service-Type après authentification de l'utilisateur. La valeur de l'attribut Service-Type doit être définie sur **Administrative** ou **NAS-Prompt** en fonction des privilèges utilisateur.

Ce deuxième exemple montre à nouveau le résultat de la **debug aaa events enable** commande. Cependant, cette fois, l'attribut Service-Type est défini sur **Administrative** sur ACS.

```
<#root>
```

```
(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
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 Successful transmission of
Authentication Packet (id 11) to 172.16.1.1:1812, proxy state
1d: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 Access-Accept received
from RADIUS server 172.16.1.1 for mobile 1d: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
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 précédent que l'attribut Service-Type est passé sur le WLC.

Informations connexes

- [Configuration du contrôleur LAN sans fil - Guide de configuration](#)
- [Configurer des VLAN sur des contrôleurs LAN sans fil](#)
- [Configurer un serveur RADIUS et un WLC pour l'attribution de VLAN dynamique](#)
- [Configurer le contrôleur LAN sans fil et le point d'accès allégé de base](#)
- [Configurer les VLAN du groupe AP avec des contrôleurs LAN sans fil](#)
- [Assistance technique de Cisco et téléchargements](#)

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.