

Configuration de TACACS+ pour un réseau sans fil unifié Cisco

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Conventions](#)

[Implémentation TACACS+ dans le contrôleur](#)

[Authentification](#)

[Autorisation](#)

[Comptabilité](#)

[Configuration TACACS+ dans le WLC](#)

[Ajoutez un serveur d'authentification TACACS+](#)

[Ajoutez un serveur d'autorisation TACACS+](#)

[Ajoutez un serveur de comptabilité TACACS+](#)

[Configurez la commande de l'authentification](#)

[Vérifiez la configuration](#)

[Configurez le serveur de Cisco Secure ACS](#)

[Configuration du réseau](#)

[Configuration d'interface](#)

[Utilisateur/Group Setup](#)

[Enregistrements des comptes dans le Cisco Secure ACS](#)

[Configuration TACACS+ dans le WCS](#)

[WCS utilisant les domaines virtuels](#)

[Configurez le Cisco Secure ACS pour utiliser WCS](#)

[Configuration du réseau](#)

[Configuration d'interface](#)

[Utilisateur/Group Setup](#)

[Debugs](#)

[Debugs de WLC pour role1=ALL](#)

[Debugs de WLC pour de plusieurs rôles](#)

[Debugs d'un WLC pour la panne d'autorisation](#)

[Informations connexes](#)

[Introduction](#)

Ce document fournit un exemple de configuration du Terminal Access Controller Access Control System Plus (TACACS+) dans un contrôleur LAN sans fil Cisco (WLC) et un système de contrôle

sans fil Cisco (WCS) pour un réseau sans fil unifié Cisco. Ce document fournit également quelques conseils de dépannage de base.

TACACS+ est un protocole de client/serveur qui fournit la Sécurité centralisée pour les utilisateurs qui tentent de gagner l'accès de Gestion à un routeur ou à un serveur d'accès à distance. TACACS+ fournit ces services d'AAA :

- Authentification des utilisateurs tentant d'ouvrir une session à l'équipement réseau
- Autorisation de déterminer ce que les utilisateurs de niveau d'accès devraient avoir
- La comptabilité pour maintenir toutes les modifications l'utilisateur fait

Référez-vous à [configurer TACACS+](#) pour plus d'informations sur des services d'AAA et la fonctionnalité TACACS+.

Référez-vous à la [comparaison TACACS+ et de RAYON](#) pour une comparaison de TACACS+ et de RAYON.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- La connaissance de la façon configurer WLCs et Point d'accès léger (recouvrements) pour le fonctionnement de base
- La connaissance du point d'accès léger Protocol (LWAPP) et des méthodes de sécurité sans fil
- RAYON de connaissance de base et TACACS+
- Connaissance de base de configuration de Cisco ACS

Composants utilisés

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

- Cisco Secure ACS pour la version 4.0 de Windows
- Contrôleur LAN Sans fil de Cisco qui exécute la version 4.1.171.0. La fonctionnalité TACACS+ sur WLCs est prise en charge sur version de logiciel 4.1.171.0 ou plus tard.
- Système de contrôle sans fil Cisco qui exécute la version 4.1.83.0. La fonctionnalité TACACS+ sur WCS est prise en charge sur version de logiciel 4.1.83.0 ou plus tard.

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](#).

Implémentation TACACS+ dans le contrôleur

Authentification

L'authentification peut être exécutée utilisant une base de données locale, un serveur de RAYON, ou TACACS+ qui utilise un nom d'utilisateur et un mot de passe. L'implémentation n'est pas entièrement modulaire. Des services d'authentification et d'autorisation sont attachés entre eux. Par exemple, si l'authentification est exécutée utilisant la base de données RADIUS/local, puis l'autorisation n'est pas exécutée avec TACACS+. Il utiliserait les autorisations associées pour l'utilisateur dans les gens du pays ou base de données de RAYON, telle qu'en lecture seule ou lecture/écriture, tandis que quand l'authentification est exécutée avec TACACS+, l'autorisation est attachée à TACACS+.

Dans les cas où de plusieurs bases de données sont configurées, un CLI est fourni pour dicter l'ordre dans lequel la base de données principale devrait être référée.

Autorisation

L'autorisation est tâche basée plutôt qu'une autorisation basée par commande réelle. Les tâches sont tracées aux divers onglets qui correspondent aux sept éléments de barre de menus qui sont actuellement sur le GUI de Web. Ce sont les éléments de barre de menus :

- MONITEUR
- WLANS
- CONTRÔLEUR
- RADIO
- SÉCURITÉ
- GESTION
- COMMANDE

La raison pour ce mappage est basée sur le fait que la plupart des clients emploient l'interface web pour configurer le contrôleur au lieu du CLI.

Un rôle supplémentaire pour la Gestion d'admin de lobby (LOBBY) est disponible pour les utilisateurs qui doivent avoir des privilèges d'admin de lobby seulement.

La tâche qu'un utilisateur est autorisé est configurée dans le serveur TACACS+ (ACS) utilisant les paires faites sur commande de l'Attribut-valeur (poids du commerce). L'utilisateur peut être autorisé pour un ou des tâches de multiple. L'autorisation minimum est MONITEUR seulement et le maximum est TOUT (autorisé à exécuter chacun des sept onglets). Si un utilisateur n'est pas autorisé pour une tâche particulière, on permet encore à l'utilisateur pour accéder à cette tâche en mode en lecture seule. Si l'authentification est activée et le serveur d'authentification devient inaccessible ou incapable d'autoriser, l'utilisateur ne peut pas ouvrir une session au contrôleur.

Remarque: Afin de l'authentification de Gestion de base par l'intermédiaire de TACACS+ à réussir, vous devez configurer des serveurs d'authentification et d'autorisation sur le WLC. La configuration de comptabilité est facultative.

Comptabilité

La comptabilité se produit toutes les fois qu'une action utilisateur-initiée par détail est exécutée

avec succès. Les attributs changés sont ouverts une session le serveur de comptabilité TACACS+ avec ces derniers :

- L'user-id de la personne qui a apporté la modification
- Le serveur distant d'où l'utilisateur est ouvert une session
- La date et le moment où la commande a été exécutée
- Niveau d'autorisation de l'utilisateur
- Une chaîne qui fournit des informations quant à quelle action a été exécutée et les valeurs fournies

Si le serveur de comptabilité devient inaccessible, l'utilisateur peut encore continuer la session.

Remarque: Des enregistrements des comptes ne sont pas générés de WCS dans la version de logiciel 4.1 ou plus tôt.

[Configuration TACACS+ dans le WLC](#)

La version logicielle 4.1.171.0 WLC et introduit plus tard nouveau CLIs et le GUI de Web change afin d'activer la fonctionnalité TACACS+ sur le WLC. Le CLIs introduit sont répertoriés dans cette section pour la référence. Les modifications correspondantes pour le GUI de Web sont ajoutées sous l'onglet Sécurité.

Ce document suppose que la configuration de base du WLC est déjà terminée.

Afin de configurer TACACS+ dans le contrôleur WLC, vous devez se terminer ces étapes :

1. [Ajoutez un serveur d'authentification TACACS+](#)
2. [Ajoutez un serveur d'autorisation TACACS+](#)
3. [Ajoutez un serveur de comptabilité TACACS+](#)
4. [Configurez la commande de l'authentification](#)

[Ajoutez un serveur d'authentification TACACS+](#)

Terminez-vous ces étapes afin d'ajouter un serveur d'authentification TACACS+ :

1. Utilisez le GUI, et allez à la **Sécurité > au TACACS+ > à l'authentification.**



2. Ajoutez l'adresse IP du serveur TACACS+ et introduisez la clé secrète partagée. S'il y a lieu, changez le port par défaut de TCP/49.

The screenshot shows the Cisco GUI for configuring a new TACACS+ Authentication Server. The left sidebar shows the navigation menu with 'TACACS+' expanded to 'Authentication'. The main area is titled 'TACACS+ Authentication Servers > New' and contains the following fields:

- Server Index (Priority): 1
- Server IP Address: 10.1.1.12
- Shared Secret Format: ASCII
- Shared Secret: cisco123
- Confirm Shared Secret: cisco123
- Port Number: 49
- Server Status: Enabled
- Retransmit Timeout: 2 seconds

3. Cliquez sur **Apply**. Vous pouvez accomplir ceci du CLI utilisant le **config tacacs auth** ajoutez la commande de **<secret> de <port> d'addr> d'Index> <IP de <Server [ASCII/hexa]>:(Cisco Controller) >**

```
config tacacs auth add 1 10.1.1.12 49 ascii cisco123
```

[Ajoutez un serveur d'autorisation TACACS+](#)

Terminez-vous ces étapes afin d'ajouter un serveur d'autorisation TACACS+ :

1. Du GUI, allez à la **Sécurité > au TACACS+ > à l'autorisation**.
2. Ajoutez l'adresse IP du serveur TACACS+ et introduisez la clé secrète partagée. S'il y a lieu, changez le port par défaut de TCP/49.

The screenshot shows the Cisco GUI for configuring a new TACACS+ Authorization Server. The left sidebar shows the navigation menu with 'TACACS+' expanded to 'Authorization'. The main area is titled 'TACACS+ Authorization Servers > New' and contains the following fields:

- Server Index (Priority): 1
- Server IP Address: 10.1.1.12
- Shared Secret Format: ASCII
- Shared Secret: cisco123
- Confirm Shared Secret: cisco123
- Port Number: 49
- Server Status: Enabled
- Retransmit Timeout: 2 seconds

3. Cliquez sur **Apply**. Vous pouvez accomplir ceci du CLI utilisant le **config tacacs athr** ajoutez la commande de **<secret> de <port> d'addr> d'Index> <IP de <Server [ASCII/hexa]>:(Cisco Controller) >**

```
config tacacs athr add 1 10.1.1.12 49 ascii cisco123
```

[Ajoutez un serveur de comptabilité TACACS+](#)

Terminez-vous ces étapes afin d'ajouter un serveur de comptabilité TACACS+ :

1. Utilisez le GUI, et allez à la **Sécurité > au TACACS+ > à la comptabilité.**
2. Ajoutez l'adresse IP du serveur et introduisez la clé secrète partagée. S'il y a lieu, changez le port par défaut de TCP/49.

3. Cliquez sur **Apply**. Vous pouvez accomplir ceci du CLI utilisant le **config tacacs acct** ajoutez la commande de **<secret> de <port> d'addr> d'Index> <IP de <Server [ASCII/hexa] : (Cisco Controller) >**

```
config tacacs acct add 1 10.1.1.12 49 ascii cisco123
```

[Configurez la commande de l'authentification](#)

Cette étape explique comment configurer la commande d'AAA de l'authentification quand il y a de plusieurs bases de données configurées. La commande de l'authentification peut être **locale et RAYON**, ou **gens du pays et TACACS**. La configuration par défaut de contrôleur pour la commande de l'authentification est *locale et RAYON*.

Terminez-vous ces étapes afin de configurer la commande de l'authentification :

1. Du GUI, allez à l'**utilisateur de Sécurité > de commande > de Gestion prioritaire.**
2. Sélectionnez l'authentification priority. Dans cet exemple, TACACS+ a été sélectionné.
3. Cliquez sur Apply pour que la sélection ait lieu.

Vous pouvez accomplir ceci du CLI utilisant la commande du **config aaa auth mgmt**

```
<server1> <server2>:(Cisco Controller) >config aaa auth mgmt tacacs local
```

[Vérifiez la configuration](#)

Cette section décrit les commandes utilisées pour vérifier la configuration TACACS+ sur le WLC. Ce sont quelques **commandes show** utiles qui aident à déterminer si la configuration est correcte :

- **show aaa auth** — Fournit des informations sur l'ordre de l'authentification.(Cisco Controller)

```
>show aaa auth Management authentication server order:  
1..... local  
2..... Tacacs
```
- **show tacacs summary** — Affiche un résumé des services et des statistiques TACACS+.(Cisco Controller)

```
>show tacacs summary Authentication Servers Idx Server Address Port State Tout -  
-----  
----- 1 10.1.1.12 49 Enabled 2 Authorization Servers Idx  
Server Address Port State Tout ---  
----- 1 10.1.1.12 49  
Enabled 2 Accounting Servers Idx Server Address Port State Tout ---  
-----  
----- 1 10.1.1.12 49 Enabled 2
```
- **stats authentiques de show tacacs** — Statistiques de serveur d'authentification des affichages TACACS+.(Cisco Controller)

```
>show tacacs auth statistics Authentication Servers: Server  
Index..... 1 Server  
Address..... 10.1.1.12 Msg Round Trip  
Time..... 0 (1/100 second) First  
Requests..... 7 Retry  
Requests..... 3 Accept  
Responses..... 3 Reject  
Responses..... 0 Error  
Responses..... 0 Restart  
Responses..... 0 Follow  
Responses..... 0 GetData  
Responses..... 0 Encrypt no secret  
Responses..... 0 Challenge Responses..... 0  
Malformed Msgs..... 0 Bad Authenticator  
Msgs..... 0 Timeout Requests..... 12  
Unknowntype Msgs..... 0 Other  
Drops..... 0
```
- **stats d'athr de show tacacs** — Statistiques de serveur d'autorisation des affichages TACACS+.(Cisco Controller)

```
>show tacacs athr statistics Authorization Servers: Server  
Index..... 1 Server  
Address..... 10.1.1.12 Msg Round Trip  
Time..... 0 (1/100 second) First  
Requests..... 3 Retry  
Requests..... 3 Received  
Responses..... 3 Authorization Success.....  
3 Authorization Failure..... 0 Challenge  
Responses..... 0 Malformed Msgs.....  
0 Bad Athenticator Msgs..... 0 Timeout  
Requests..... 0 Unknowntype  
Msgs..... 0 Other Drops..... 0
```
- **stats d'acct de show tacacs** — Statistiques de serveur de comptabilité des affichages TACACS+.(Cisco Controller)

```
>show tacacs acct statistics Accounting Servers: Server  
Index..... 1 Server  
Address..... 10.1.1.12 Msg Round Trip  
Time..... 0 (1/100 second) First  
Requests..... 133 Retry  
Requests..... 0 Accounting  
Response..... 0 Accounting Request Success..... 0  
Accounting Request Failure..... 0 Malformed  
Msgs..... 0 Bad Authenticator Msgs.....  
0 Timeout Requests..... 399 Unknowntype
```


Configurez le serveur de Cisco Secure ACS

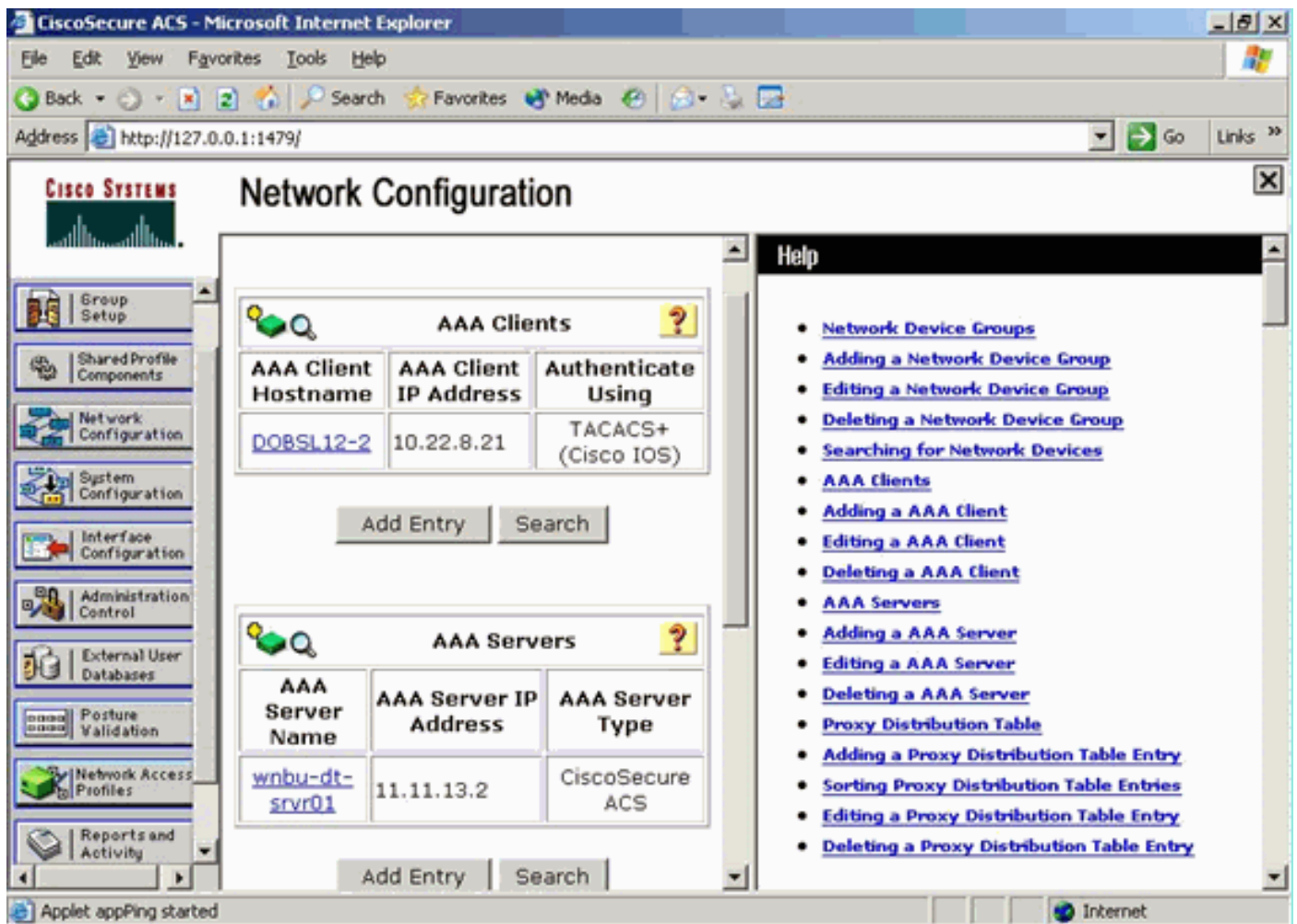
Cette section fournit les étapes impliquées dans le serveur ACS TACACS+ pour créer des services et des attributs personnalisés, et assigne les rôles aux utilisateurs ou aux groupes.

La création des utilisateurs et du groupe n'est pas expliquée dans cette section. On le suppose que les utilisateurs et les groupes sont créés comme nécessaires. Référez-vous au [guide utilisateur pour le Cisco Secure ACS pour les Windows Server 4.0](#) pour les informations sur la façon dont créer des utilisateurs et des groupes d'utilisateurs.

Configuration du réseau

Complétez cette étape :

Ajoutez l'adresse IP de Gestion de contrôleur comme client d'AAA avec le mécanisme d'authentification comme TACACS+ (Cisco IOS).



Configuration d'interface

Procédez comme suit :

1. Dans le menu de configuration d'interface, sélectionnez le lien **TACACS+ (Cisco IOS)**.

2. Activez les **nouveaux services**.
3. Vérifiez les cases d'**utilisateur** et de **groupe**.
4. Écrivez le **ciscowlc** pour le service et le **terrain communal** pour Protocol.
5. Activez les **caractéristiques avancées**

TACACS+.

Address <http://127.0.0.1:1767/> Go Links

CISCO SYSTEMS

Interface Configuration

TACACS+ Services

User	Group	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	PPP IP
<input type="checkbox"/>	<input type="checkbox"/>	PPP IPX
<input type="checkbox"/>	<input type="checkbox"/>	PPP Multilink
<input type="checkbox"/>	<input type="checkbox"/>	PPP Apple Talk
<input type="checkbox"/>	<input type="checkbox"/>	PPP VPDN
<input type="checkbox"/>	<input type="checkbox"/>	PPP LCP
<input type="checkbox"/>	<input type="checkbox"/>	ARAP
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Shell (exec)
<input type="checkbox"/>	<input type="checkbox"/>	PIX Shell (pixshell)
<input type="checkbox"/>	<input type="checkbox"/>	SLIP

New Services

		Service	Protocol
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	ciscowlc	common
<input type="checkbox"/>	<input type="checkbox"/>		
<input type="checkbox"/>	<input type="checkbox"/>		

Advanced Configuration Options

Advanced TACACS+ Features

Display a Time-of-Day access grid for every TACACS+ service where you can

Submit Cancel

6. Cliquez sur Submit afin d'appliquer les modifications.

Utilisateur/Group Setup

Procédez comme suit :

1. Sélectionnez un utilisateur/groupe précédemment créés.
2. Allez aux **configurations TACACS+**.
3. Cochez la case qui correspond au service de *ciscowlc* qui a été créé dans la section de configuration d'interface.
4. Cochez la case d'**attributs personnalisés**.



Group Setup

Jump To Access Restrictions

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

Shell Command Authorization Set

- None
 - Assign a Shell Command Authorization Set for any network device
 - Per Group Command Authorization
- Unmatched Cisco IOS commands
- Permit
 - Deny

Command:

Arguments:

Unlisted arguments

- Permit
- Deny

ciscowlc common

Custom attributes

Wireless-WCS HTTP

Custom attributes

IETF RADIUS Attributes

[006] Service-Type

Callback NAS Prompt

Submit

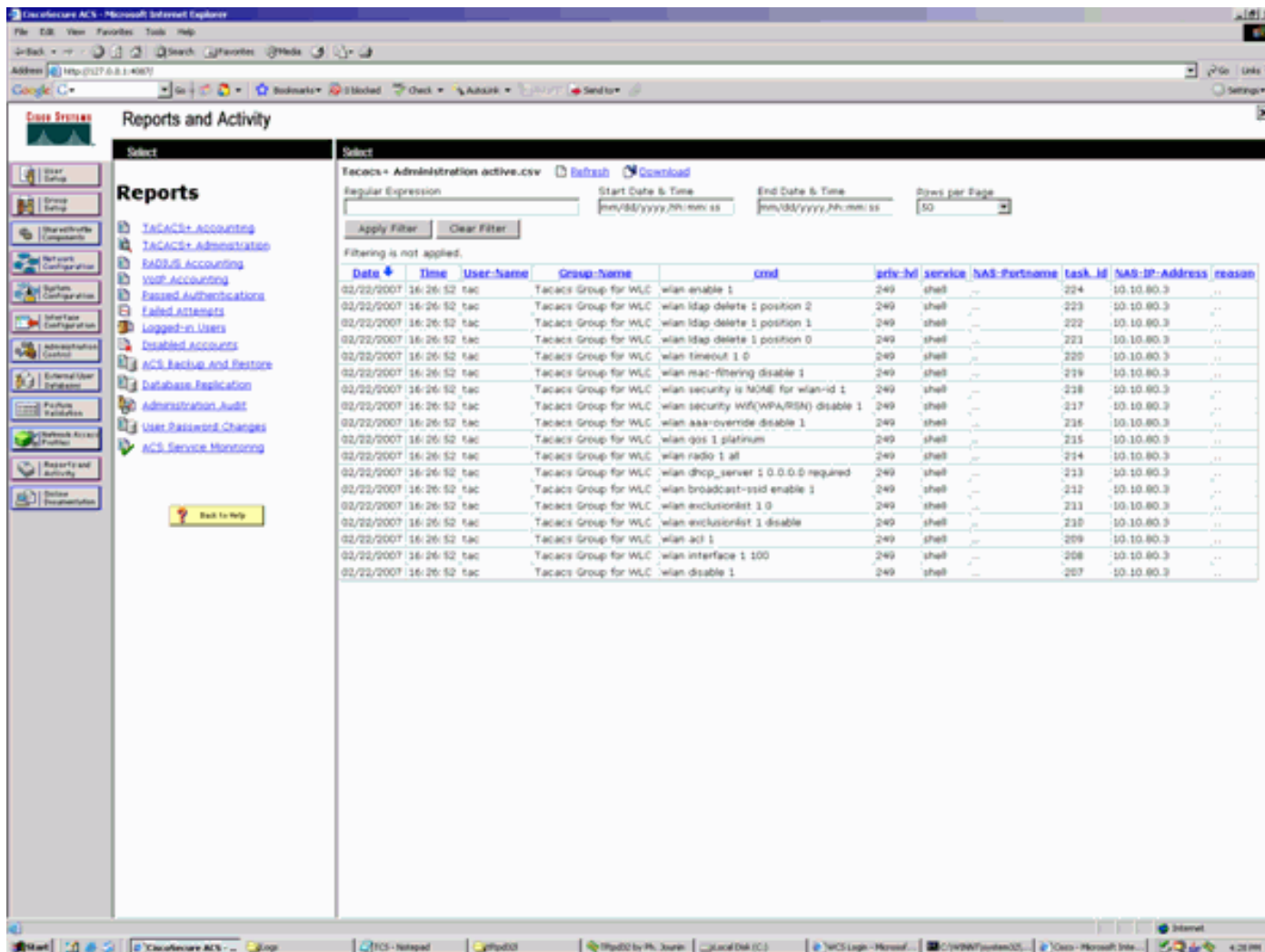
Submit + Restart

Cancel

- Dans la zone de texte au-dessous des attributs personnalisés, entrez dans ce texte si les besoins créés par l'utilisateur accèdent à seulement au WLAN, à la SÉCURITÉ et au CONTRÔLEUR : **role1=WLAN role2=SECURITY role3=CONTROLLER**. Si les besoins de l'utilisateur accèdent à seulement à l'onglet Sécurité, entrez dans ce texte : **role1=SECURITY**. Le rôle correspond aux sept éléments de barre de menus dans le GUI de Web de contrôleur. Les éléments de barre de menus sont MONITEUR, WLAN, CONTRÔLEUR, RADIO, SÉCURITÉ, GESTION et COMMANDE.
- Écrivez le rôle qui les besoins de l'utilisateur pour role1, role2 et ainsi de suite. Si les besoins de l'utilisateur tous les rôles, alors **TOUT le** mot clé sont utilisés. Pour le rôle d'admin de lobby, le **LOBBY de** mot clé devrait être utilisé.

Enregistrements des comptes dans le Cisco Secure ACS

Les enregistrements des comptes TACACS+ du WLC sont disponibles dans le Cisco Secure ACS dans la gestion TACACS+ des états et de l'activité :



The screenshot shows the Cisco Secure ACS interface. The main content area displays a table of TACACS+ Administration active.csv records. The table has columns for Date, Time, User-name, Group-name, cmd, priv-lvl, service, NAS-Portname, task_id, NAS-IP-Address, and reason. The records show various commands being executed by the 'tac' user from the 'Taccacs Group for WLC' group, such as 'wlan enable 1', 'wlan ldap delete 1 position 2', 'wlan mac-filtering disable 1', and 'wlan disable 1'.

Date	Time	User-name	Group-name	cmd	priv-lvl	service	NAS-Portname	task_id	NAS-IP-Address	reason
02/22/2007	16:26:52	tac	Taccacs Group for WLC	wlan enable 1	249	shell	...	224	10.10.80.3	...
02/22/2007	16:26:52	tac	Taccacs Group for WLC	wlan ldap delete 1 position 2	249	shell	...	223	10.10.80.3	...
02/22/2007	16:26:52	tac	Taccacs Group for WLC	wlan ldap delete 1 position 1	249	shell	...	222	10.10.80.3	...
02/22/2007	16:26:52	tac	Taccacs Group for WLC	wlan ldap delete 1 position 0	249	shell	...	221	10.10.80.3	...
02/22/2007	16:26:52	tac	Taccacs Group for WLC	wlan timeout 1 0	249	shell	...	220	10.10.80.3	...
02/22/2007	16:26:52	tac	Taccacs Group for WLC	wlan mac-filtering disable 1	249	shell	...	219	10.10.80.3	...
02/22/2007	16:26:52	tac	Taccacs Group for WLC	wlan security is NONE for wlan-id 1	249	shell	...	218	10.10.80.3	...
02/22/2007	16:26:52	tac	Taccacs Group for WLC	wlan security WPA(WPA/RSN) disable 1	249	shell	...	217	10.10.80.3	...
02/22/2007	16:26:52	tac	Taccacs Group for WLC	wlan aaa-overmode disable 1	249	shell	...	216	10.10.80.3	...
02/22/2007	16:26:52	tac	Taccacs Group for WLC	wlan qos 1 platinum	249	shell	...	215	10.10.80.3	...
02/22/2007	16:26:52	tac	Taccacs Group for WLC	wlan radio 1 all	249	shell	...	214	10.10.80.3	...
02/22/2007	16:26:52	tac	Taccacs Group for WLC	wlan dhcp_server 1 0.0.0.0 required	249	shell	...	213	10.10.80.3	...
02/22/2007	16:26:52	tac	Taccacs Group for WLC	wlan broadcast-ssid enable 1	249	shell	...	212	10.10.80.3	...
02/22/2007	16:26:52	tac	Taccacs Group for WLC	wlan exclusionlist 1 0	249	shell	...	211	10.10.80.3	...
02/22/2007	16:26:52	tac	Taccacs Group for WLC	wlan exclusionlist 1 disable	249	shell	...	210	10.10.80.3	...
02/22/2007	16:26:52	tac	Taccacs Group for WLC	wlan act 1	249	shell	...	209	10.10.80.3	...
02/22/2007	16:26:52	tac	Taccacs Group for WLC	wlan interface 1 100	249	shell	...	208	10.10.80.3	...
02/22/2007	16:26:52	tac	Taccacs Group for WLC	wlan disable 1	249	shell	...	207	10.10.80.3	...

Configuration TACACS+ dans le WCS

Procédez comme suit :

1. Du GUI, procédure de connexion au WCS avec le compte de racine.
2. Ajoutez le serveur TACACS+. Allez à la **gestion > à l'AAA > au TACACS+ > ajoutent le serveur TACACS+**.



3. Ajoutez les petits groupes de serveur TACACS+, tels que l'adresse IP, le numéro de port (49

est par défaut), et la clé secrète partagée.

The screenshot shows the Cisco WCS configuration interface for TACACS+. The left sidebar contains a navigation menu with options: AAA, Change Password, AAA Mode, Users, Groups, Active Sessions, TACACS+, and RADIUS. The main content area is titled 'TACACS+' and includes the following fields: Server Address (10.1.1.12), Port (49), Shared Secret Format (ASCII), Shared Secret (masked with asterisks), Confirm Shared Secret (masked with asterisks), Retransmit Timeout (5 seconds), Retries (1), and Authentication Type (PAP). There are 'Submit' and 'Cancel' buttons at the bottom.

4. Activez l'authentification TACACS+ pour la gestion dans le WCS. Allez à la **gestion > au mode d'AAA > d'AAA > TACACS+** choisi.

The screenshot shows the Cisco WCS configuration interface for AAA Mode Settings. The left sidebar is the same as in the previous screenshot. The main content area is titled 'AAA Mode Settings' and includes the following options: AAA Mode (radio buttons for Local, RADIUS, and TACACS+), and Fallback on Local (checkbox checked). There is an 'OK' button and a note: 'Install time super user is going to be always authenticated locally irrespective of the AAA Mode Settings.'

WCS utilisant les domaines virtuels

Le domaine virtuel est une nouvelle fonctionnalité introduite avec la version 5.1 WCS. Un domaine virtuel WCS se compose d'un ensemble de périphériques et de cartes et limite une vue standard aux informations concernant ces périphériques et cartes. Par un domaine virtuel, un administrateur peut s'assurer que les utilisateurs peuvent seulement visualiser les périphériques et les cartes dont ils sont responsables. En outre, en raison des filtres du domaine virtuel, les utilisateurs peuvent configurer, visualiser des alarmes, et générer des états pour seulement leur partie assignée du réseau. L'administrateur spécifie un ensemble de domaines virtuels permis pour chaque utilisateur. Seulement un de ces derniers peut être en activité pour cet utilisateur à la procédure de connexion. L'utilisateur peut changer le domaine virtuel en cours en sélectionnant un domaine virtuel permis différent du menu déroulant virtuel de domaine en haut de l'écran. Tout signale, des alarmes, et l'autre fonctionnalité sont maintenant filtrées par ce domaine virtuel.

S'il y a seulement un domaine virtuel défini (racine) dans le système et l'utilisateur n'a aucun domaine virtuel dans les attributs personnalisés met en place dans le serveur TACACS+/RADIUS, l'utilisateur est assigné le domaine virtuel de racine par défaut.

S'il y a plus d'un domaine virtuel, et l'utilisateur n'a aucun attribut spécifié, alors l'utilisateur est bloqué d'ouvrir une session. Afin de permettre à l'utilisateur pour ouvrir une session, les attributs personnalisés virtuels de domaine doivent être exportés au serveur Radius/TACACS+.

La fenêtre virtuelle d'attributs personnalisés de domaine te permet pour indiquer les données appropriées de Protocol-particularité pour chaque domaine virtuel. Le bouton d'exportation sur la barre latérale virtuelle de hiérarchie de domaine préformate les attributs du RAYON et TACACS+ du domaine virtuel. Vous pouvez copier et coller ces attributs dans le serveur ACS. Ceci te permet pour copier seulement les domaines virtuels applicables sur l'écran de serveur ACS et s'assure que les utilisateurs ont seulement accès à ces domaines virtuels.

Afin d'appliquer les attributs préformatés de RAYON et TACACS+ au serveur ACS, terminez-vous les étapes expliquées section dans de [domaine de RAYON et TACACS+ attributs virtuels](#).

[Configurez le Cisco Secure ACS pour utiliser WCS](#)

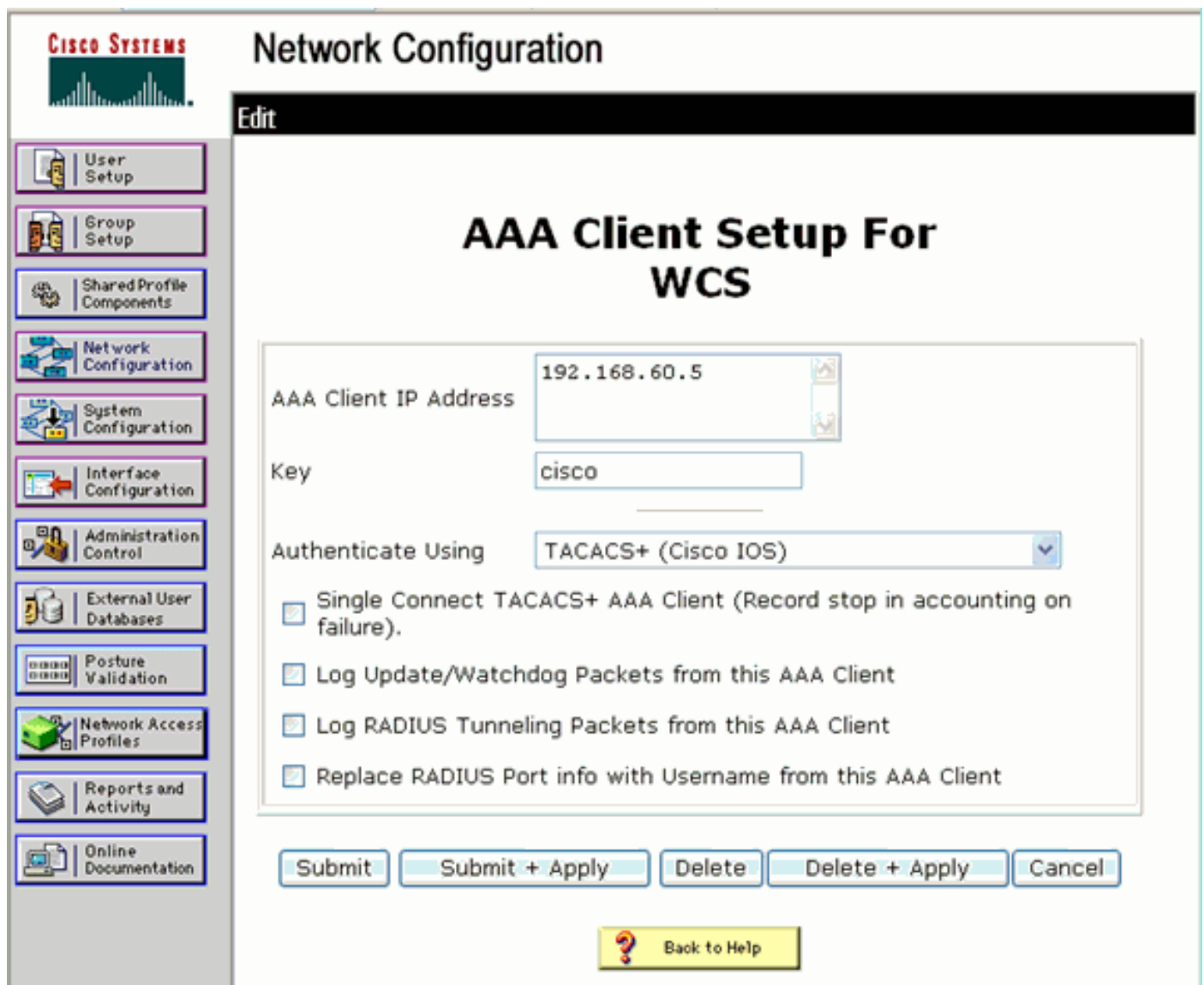
La section fournit les étapes impliquées dans le serveur ACS TACACS+ pour créer des services et des attributs personnalisés, et assigne les rôles aux utilisateurs ou aux groupes.

La création des utilisateurs et du groupe n'est pas expliquée dans cette section. On le suppose que les utilisateurs et les groupes sont créés comme nécessaires.

[Configuration du réseau](#)

Complétez cette étape :

Ajoutez l'adresse IP WCS comme client d'AAA avec le mécanisme d'authentification comme TACACS+ (Cisco IOS).



The screenshot displays the Cisco Secure ACS Network Configuration interface. The main title is "Network Configuration" with a sub-header "Edit". The central content area is titled "AAA Client Setup For WCS". The configuration fields are as follows:

- AAA Client IP Address: 192.168.60.5
- Key: cisco
- Authenticate Using: TACACS+ (Cisco IOS)

Below these fields are four checkboxes:

- 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

At the bottom of the configuration area are five buttons: "Submit", "Submit + Apply", "Delete", "Delete + Apply", and "Cancel". Below these buttons is a "Back to Help" button with a question mark icon.

The left sidebar contains the following navigation options:

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

[Configuration d'interface](#)

Procédez comme suit :

1. Dans le menu de configuration d'interface, sélectionnez le lien **TACACS+** (Cisco IOS).
2. Activez les **nouveaux services**.
3. Vérifiez les cases d'utilisateur et de **groupe**.
4. Entrez dans la **radio-WCS** pour le service et le **HTTP** pour Protocol. **Remarque:** Le HTTP doit être dans des CAPS.
5. Activez les **caractéristiques avancées TACACS+**.

CISCO SYSTEMS

Interface Configuration

<input type="checkbox"/>	<input checked="" type="checkbox"/>	PPP IP
<input type="checkbox"/>	<input type="checkbox"/>	PPP IPX
<input type="checkbox"/>	<input type="checkbox"/>	PPP Multilink
<input type="checkbox"/>	<input type="checkbox"/>	PPP Apple Talk
<input type="checkbox"/>	<input type="checkbox"/>	PPP VPDN
<input type="checkbox"/>	<input type="checkbox"/>	PPP LCP
<input type="checkbox"/>	<input type="checkbox"/>	ARAP
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Shell (exec)
<input type="checkbox"/>	<input type="checkbox"/>	PIX Shell (pixshell)
<input type="checkbox"/>	<input type="checkbox"/>	SLIP

New Services

		Service	Protocol
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	ciscowlc	common
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Wireless-WCS	HTTP
<input type="checkbox"/>	<input type="checkbox"/>		

Advanced Configuration Options

Advanced TACACS+ Features

6. Cliquez sur Submit afin d'appliquer les modifications.

[Utilisateur/Group Setup](#)

Procédez comme suit :

1. Dans le GUI WCS, naviguez vers la **gestion > l'AAA > les groupes** pour sélectionner les groupes d'utilisateurs préconfigurés l'un des, tels que des super utilisateurs dans le WCS.

Group Name	Members	Audit Trail	Export
Admin	...		Task List
ConfMnstrs	...		Task List
System Monitors	...		Task List
Users Assistant	...		Task List
LibbyAmbassador	libby		Task List
Monitor Libs	...		Task List
North Bound API	...		Task List
Subscribers	...		Task List
Root	root		Task List
User Defined 1	...		Task List
User Defined 2	...		Task List
User Defined 3	...		Task List
User Defined 4	...		Task List

2. Sélectionnez la liste des tâches pour les groupes d'utilisateurs et la pâte préconfigurés de copie à l'ACS.

Please cut and paste the appropriate protocol data below into the custom/vendor-specific attribute field in your AAA server.

TACACS+ Custom Attributes

```

role=root
task0=Users and Groups
task1=Audit Trails
task2=TACACS+ Servers
task3=RADIUS Servers
task4=Logging
task5=Logging
task6=Schedule Tasks and Data Collection
task7=User Preferences
task8=System Settings
task9=Diagnostic Information
task10=View Alerts and Events
task11=View Alerts and Events
task12=Email Notification
task13>Delete and Clear Alerts
task14=Push and Unpush Alerts
task15=Severity Configuration
task16=Configure Controllers
task17=Configure Templates
task18=Configure Config Groups
task19=Configure Access Points
task20=Configure Access Point Templates
task21=Configure Choke Points
task22=Monitor Controllers
task23=Monitor Controllers
task24=Monitor Access Points
task25=Monitor Access Points
task26=Monitor Clients
task27=Monitor Clients
task28=Monitor Tags

```

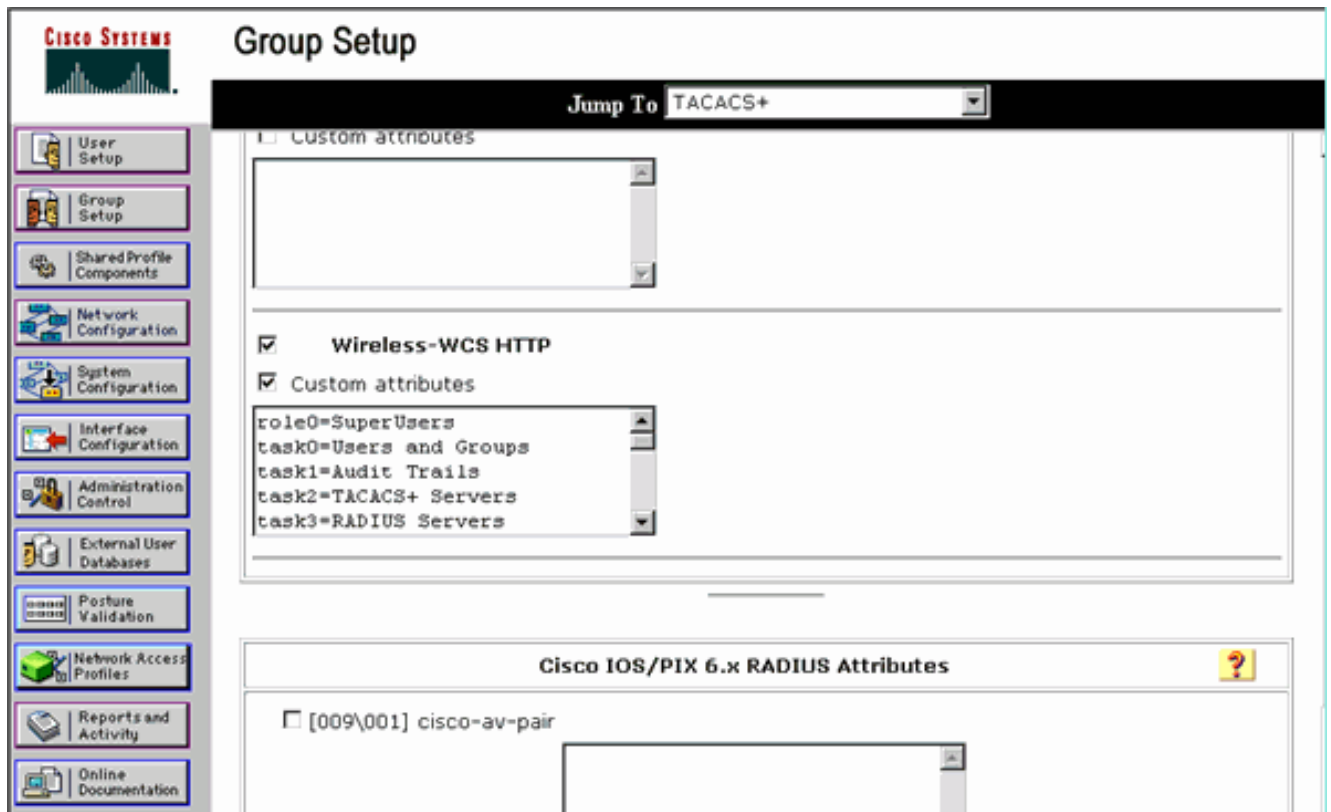
RADIUS Custom Attributes

```

Wireless-WCS-task0=Users and Groups
Wireless-WCS-task1=Audit Trails
Wireless-WCS-task2=TACACS+ Servers
Wireless-WCS-task3=RADIUS Servers
Wireless-WCS-task4=Logging
Wireless-WCS-task5=Logging
Wireless-WCS-task6=Schedule Tasks and Data Collection
Wireless-WCS-task7=User Preferences
Wireless-WCS-task8=System Settings
Wireless-WCS-task9=Diagnostic Information
Wireless-WCS-task10=View Alerts and Events
Wireless-WCS-task11=View Alerts and Events
Wireless-WCS-task12=Email Notification
Wireless-WCS-task13>Delete and Clear Alerts
Wireless-WCS-task14=Push and Unpush Alerts
Wireless-WCS-task15=Severity Configuration
Wireless-WCS-task16=Configure Controllers
Wireless-WCS-task17=Configure Templates
Wireless-WCS-task18=Configure Config Groups
Wireless-WCS-task19=Configure Access Points
Wireless-WCS-task20=Configure Access Point Templates
Wireless-WCS-task21=Configure Choke Points
Wireless-WCS-task22=Monitor Controllers
Wireless-WCS-task23=Monitor Controllers
Wireless-WCS-task24=Monitor Access Points
Wireless-WCS-task25=Monitor Access Points
Wireless-WCS-task26=Monitor Clients
Wireless-WCS-task27=Monitor Clients
Wireless-WCS-task28=Monitor Tags

```

3. Sélectionnez un utilisateur/groupe précédemment créés et allez aux configurations **TACACS+**.
4. Dans le GUI ACS, sélectionnez la case qui correspond au service de radio-WCS qui a été créé plus tôt.
5. Dans le GUI ACS, cochez la case d'**attributs personnalisés**.
6. Dans la zone de texte au-dessous des attributs personnalisés, écrivez ce rôle et chargez les informations copiées du WCS. Par exemple, écrivez la liste de tâches permises des super utilisateurs.



7. Puis, procédure de connexion au WCS avec le nom d'utilisateur/mot de passe de création récente dans l'ACS.

[Debugs](#)

[Debugs de WLC pour role1=ALL](#)

```
(Cisco Controller) >debug aaa tacacs enable (Cisco Controller) >Wed Feb 28 17:36:37 2007: Forwarding request to 10.1.1.12 port=49 Wed Feb 28 17:36:37 2007: tplus response: type=1 seq_no=2 session_id=5eaa857e length=16 encrypted=0 Wed Feb 28 17:36:37 2007: TPLUS_AUTHEN_STATUS_GETPASS Wed Feb 28 17:36:37 2007: auth_cont get_pass reply: pkt_length=22 Wed Feb 28 17:36:37 2007: processTplusAuthResponse: Continue auth transaction Wed Feb 28 17:36:37 2007: tplus response: type=1 seq_no=4 session_id=5eaa857e length=6 encrypted=0 Wed Feb 28 17:36:37 2007: tplus_make_author_request() from tplus_authen_passed returns rc=0 Wed Feb 28 17:36:37 2007: Forwarding request to 10.1.1.12 port=49 Wed Feb 28 17:36:37 2007: author response body: status=1 arg_cnt=1 msg_len=0 data_len=0 Wed Feb 28 17:36:37 2007: arg[0] = [9][role1=ALL] Wed Feb 28 17:36:37 2007: User has the following mgmtRole ffffffff8
```

[Debugs de WLC pour de plusieurs rôles](#)

```
(Cisco Controller) >debug aaa tacacs enable Wed Feb 28 17:59:33 2007: Forwarding request to 10.1.1.12 port=49 Wed Feb 28 17:59:34 2007: tplus response: type=1 seq_no=2 session_id=b561ad88 length=16 encrypted=0 Wed Feb 28 17:59:34 2007: TPLUS_AUTHEN_STATUS_GETPASS Wed Feb 28 17:59:34 2007: auth_cont get_pass reply: pkt_length=22 Wed Feb 28 17:59:34 2007: processTplusAuthResponse: Continue auth transaction Wed Feb 28 17:59:34 2007: tplus response: type=1 seq_no=4 session_id=b561ad88 length=6 encrypted=0 Wed Feb 28 17:59:34 2007: tplus_make_author_request() from tplus_authen_passed returns rc=0 Wed Feb 28 17:59:34 2007: Forwarding request to 10.1.1.12 port=49 Wed Feb 28 17:59:34 2007: author response body: status=1 arg_cnt=4 msg_len=0 data_len=0 Wed Feb 28 17:59:34 2007: arg[0] = [11][role1=WLAN] Wed Feb 28 17:59:34 2007: arg[1] = [16][role2=CONTROLLER] Wed Feb 28 17:59:34 2007: arg[2] = [14][role3=SECURITY] Wed Feb 28 17:59:34 2007: arg[3] = [14][role4=COMMANDS] Wed Feb 28 17:59:34 2007: User has the following mgmtRole 150
```

[Debugs d'un WLC pour la panne d'autorisation](#)

```
(Cisco Controller) >debug aaa tacacs enable Wed Feb 28 17:53:04 2007: Forwarding request to
10.1.1.12 port=49 Wed Feb 28 17:53:04 2007: tplus response: type=1 seq_no=2 session_id=89c553a1
length=16 encrypted=0 Wed Feb 28 17:53:04 2007: TPLUS_AUTHEN_STATUS_GETPASS Wed Feb 28 17:53:04
2007: auth_cont get_pass reply: pkt_length=22 Wed Feb 28 17:53:04 2007:
processTplusAuthResponse: Continue auth transaction Wed Feb 28 17:53:04 2007: tplus response:
type=1 seq_no=4 session_id=89c553a1 length=6 encrypted=0 Wed Feb 28 17:53:04 2007:
tplus_make_author_request() from tplus_authen_passed returns rc=0 Wed Feb 28 17:53:04 2007:
Forwarding request to 10.1.1.12 port=49 Wed Feb 28 17:53:04 2007: author response body:
status=16 arg_cnt=0 msg_len=0 data_len=0 Wed Feb 28 17:53:04 2007:User has the following
mgmtRole 0 Wed Feb 28 17:53:04 2007: Tplus authorization for tac failed status=16
```

[Informations connexes](#)

- [Exemple Sans fil du contrôleur LAN de Cisco \(WLC\) et de la configuration de Cisco ACS 5.x \(TACACS+\) pour l'authentification Web](#)
- [Configurer TACACS+](#)
- [Comment configurer l'authentification et l'autorisation TACACS pour des utilisateurs d'admin et de non-admin dans ACS 5.1](#)
- [Comparaison entre TACACS+ et RADIUS](#)
- [Support et documentation techniques - Cisco Systems](#)