Configuration de services de domaine sans fil

Contenu

Introduction

Ce document présente le concept du Wireless Domain Services (WDS). Le document décrit également comment configurer un point d'accès (AP) ou le module WLSM (Wireless LAN Services Module) comme WDS et au moins un autre comme point d'accès d'infrastructure. La procédure dans ce document vous guide à un WDS qui est fonctionnel et permet à des clients de s'associer au WDS AP ou à une infrastructure AP. Ce document vise à établir une base à partir de laquelle vous pouvez configurer Fast Secure Roaming ou introduire un Wireless LAN Solutions Engine (WLSE) dans le réseau, afin que vous puissiez utiliser les fonctionnalités.

Conditions préalables

Conditions requises

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

- Connaître parfaitement les réseaux LAN sans fil et les problèmes de sécurité sans fil.
- Connaître les méthodes de sécurité actuelles du protocole EAP (Extensible Authentication Protocol).

Components Used

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

- Points d'accès avec le logiciel Cisco IOS®
- Logiciel Cisco IOS Version 12.3(2)JA2 ou ultérieure
- Module de services LAN sans fil de la gamme Catalyst 6500

Les informations présentées dans ce document ont été créées à partir de périphériques dans un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut) et une adresse IP sur l'interface BVI1, de sorte que l'unité est accessible à partir de l'interface utilisateur graphique du logiciel Cisco IOS ou de l'interface de ligne de commande (CLI). Si vous travaillez sur un réseau en direct, assurez-vous de bien comprendre l'impact 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.

Services de domaine sans fil

WDS est une nouvelle fonctionnalité pour les points d'accès dans le logiciel Cisco IOS et la base du WLSM de la gamme Catalyst 6500. WDS est une fonction centrale qui permet d'autres fonctionnalités telles que :

- Itinérance rapide et sécurisée
- interaction WLSE
- Gestion de la radio

Vous devez établir des relations entre les points d'accès qui participent au WDS et au WLSM, avant que d'autres fonctionnalités basées sur WDS ne fonctionnent. L'un des objectifs de WDS est d'éliminer la nécessité pour le serveur d'authentification de valider les informations d'identification de l'utilisateur et de réduire le temps requis pour les authentifications du client.

Pour utiliser WDS, vous devez désigner un point d'accès ou le WLSM comme WDS. Un point d'accès WDS doit utiliser un nom d'utilisateur et un mot de passe WDS pour établir une relation avec un serveur d'authentification. Le serveur d'authentification peut être un serveur RADIUS externe ou la fonctionnalité Serveur RADIUS local dans l'AP WDS. Le WLSM doit avoir une relation avec le serveur d'authentification, même si le WLSM n'a pas besoin de s'authentifier auprès du serveur.

D'autres points d'accès, appelés points d'accès d'infrastructure, communiquent avec le WDS. Avant l'enregistrement, les points d'accès d'infrastructure doivent s'authentifier auprès du WDS. Un groupe de serveurs d'infrastructure sur le WDS définit cette authentification d'infrastructure.

Un ou plusieurs groupes de serveurs clients sur le WDS définissent l'authentification du client.

Lorsqu'un client tente de s'associer à un AP d'infrastructure, le AP d'infrastructure transmet les informations d'identification de l'utilisateur au WDS pour validation. Si WDS voit les informations d'identification pour la première fois, WDS se tourne vers le serveur d'authentification pour valider

les informations d'identification. Le WDS met alors en cache les informations d'identification, afin d'éliminer la nécessité de revenir au serveur d'authentification lorsque le même utilisateur tente à nouveau l'authentification. Exemples de réauthentification :

- Nouvelle frappe
- Itinérance
- Lorsque l'utilisateur démarre le périphérique client

Tout protocole d'authentification EAP basé sur RADIUS peut être tunnelisé via WDS tel que :

- EAP léger (LEAP)
- Protected EAP (PEAP)
- EAP-Transport Layer Security (EAP-TLS)
- Authentification EAP-Flexible via la tunnellisation sécurisée (EAP-FAST)

L'authentification d'adresse MAC peut également passer en tunnel vers un serveur d'authentification externe ou une liste locale vers un point d'accès WDS. Le WLSM ne prend pas en charge l'authentification des adresses MAC.

Le WDS et les AP d'infrastructure communiquent via un protocole de multidiffusion appelé WLCCP (WLAN Context Control Protocol). Ces messages de multidiffusion ne peuvent pas être routés, de sorte qu'un WDS et les AP d'infrastructure associés doivent se trouver dans le même sous-réseau IP et sur le même segment de réseau local. Entre le WDS et le WLSE, le WLCCP utilise le protocole TCP et le protocole UDP (User Datagram Protocol) sur le port 2887. Lorsque le WDS et le WLSE se trouvent sur des sous-réseaux différents, un protocole comme la traduction d'adresses de réseau (NAT) ne peut pas traduire les paquets.

Un point d'accès configuré comme périphérique WDS prend en charge jusqu'à 60 points d'accès participants. Un routeur de services intégrés (ISR) configuré en tant que périphériques WDS prend en charge jusqu'à 100 points d'accès participants. De plus, un commutateur WLSM prend en charge jusqu'à 600 points d'accès participants et jusqu'à 240 groupes de mobilité. Un point d'accès unique prend en charge jusqu'à 16 groupes de mobilité.

Remarque : Cisco recommande que les AP d'infrastructure exécutent la même version d'IOS que le périphérique WDS. Si vous utilisez une version antérieure d'IOS, les points d'accès peuvent ne pas s'authentifier sur le périphérique WDS. En outre, Cisco vous recommande d'utiliser la dernière version de l'IOS. Vous pouvez trouver la dernière version d'IOS dans la page Téléchargements sans fil.

Rôle du périphérique WDS

Le périphérique WDS effectue plusieurs tâches sur votre réseau local sans fil :

- Annonce sa fonctionnalité WDS et participe à l'élection du meilleur périphérique WDS pour votre LAN sans fil. Lorsque vous configurez votre réseau local sans fil pour WDS, vous configurez un périphérique comme candidat WDS principal et un ou plusieurs périphériques supplémentaires comme candidats WDS de secours. Si le périphérique WDS principal est hors ligne, l'un des périphériques WDS de sauvegarde prend sa place.
- Authentifie tous les points d'accès du sous-réseau et établit un canal de communication sécurisé avec chacun d'eux.
- Collecte les données radio des points d'accès du sous-réseau, agrège les données et les transmet au périphérique WLSE de votre réseau.

- Agit en tant que transfert pour tous les périphériques clients authentifiés 802.1x associés aux points d'accès participants.
- Inscrit tous les périphériques clients du sous-réseau qui utilisent la clé dynamique, établit les clés de session pour eux et met en cache leurs informations d'identification de sécurité. Lorsqu'un client se déplace vers un autre point d'accès, le périphérique WDS transfère les informations d'identification de sécurité du client au nouveau point d'accès.

Rôle des points d'accès à l'aide du périphérique WDS

Les points d'accès de votre réseau local sans fil interagissent avec le périphérique WDS dans ces activités :

- Découvrir et suivre le périphérique WDS actuel et relayer les annonces WDS vers le LAN sans fil.
- Authentifier avec le périphérique WDS et établir un canal de communication sécurisé vers le périphérique WDS.
- Enregistrez les périphériques clients associés au périphérique WDS.
- Signalez les données radio au périphérique WDS.

Configuration

WDS présente la configuration de manière ordonnée et modulaire. Chaque concept repose sur le concept qui précède. Le WDS omet d'autres éléments de configuration tels que les mots de passe, l'accès à distance et les paramètres radio pour plus de clarté et se concentrer sur l'objet principal.

Cette section présente les informations nécessaires à la configuration des fonctionnalités décrites dans ce document.

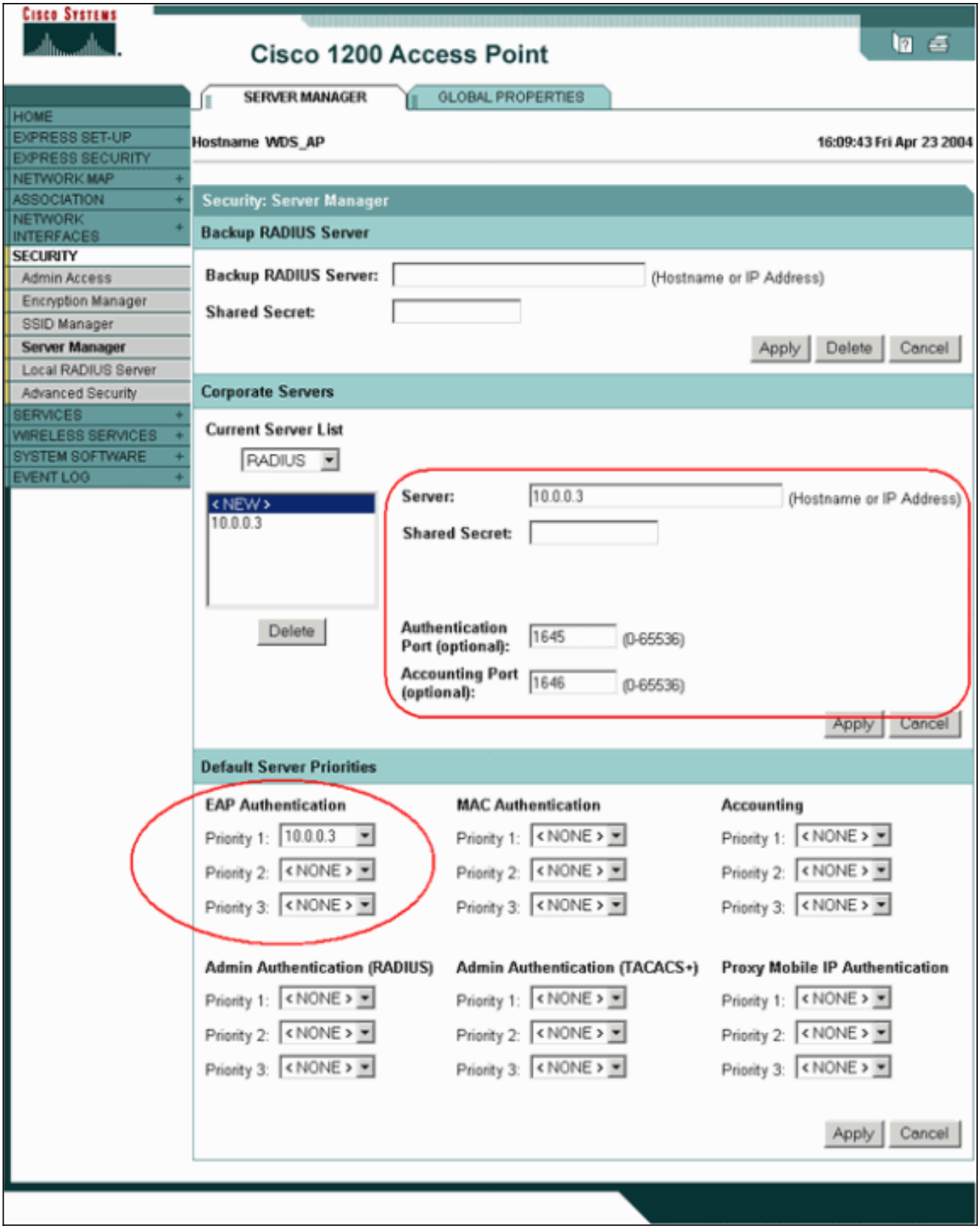
Remarque : utilisez l'outil de recherche de commandes (clients enregistrés uniquement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Désigner un point d'accès en tant que WDS

La première étape consiste à désigner un point d'accès comme WDS. Le point d'accès WDS est le seul qui communique avec le serveur d'authentification.

Complétez ces étapes afin de désigner un point d'accès comme WDS :

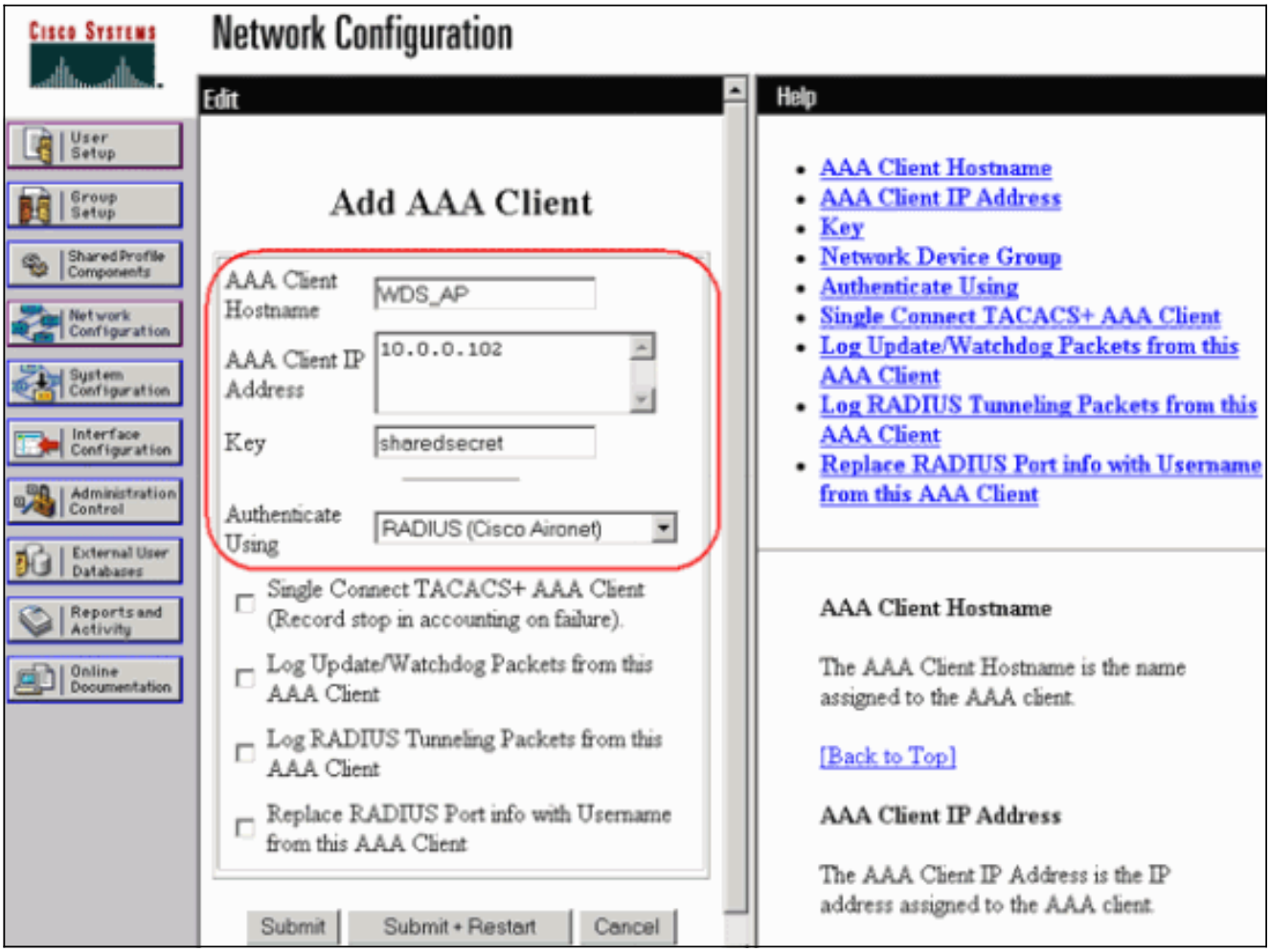
1. Afin de configurer le serveur d'authentification sur l'AP WDS, choisissez **Security > Server Manager** pour accéder à l'onglet Server Manager :Sous Serveurs d'entreprise, tapez l'adresse IP du serveur d'authentification dans le champ Serveur.Spécifiez le secret partagé et les ports.Sous Priorités du serveur par défaut, définissez le champ Priorité 1 sur l'adresse IP du serveur sous le type d'authentification approprié.



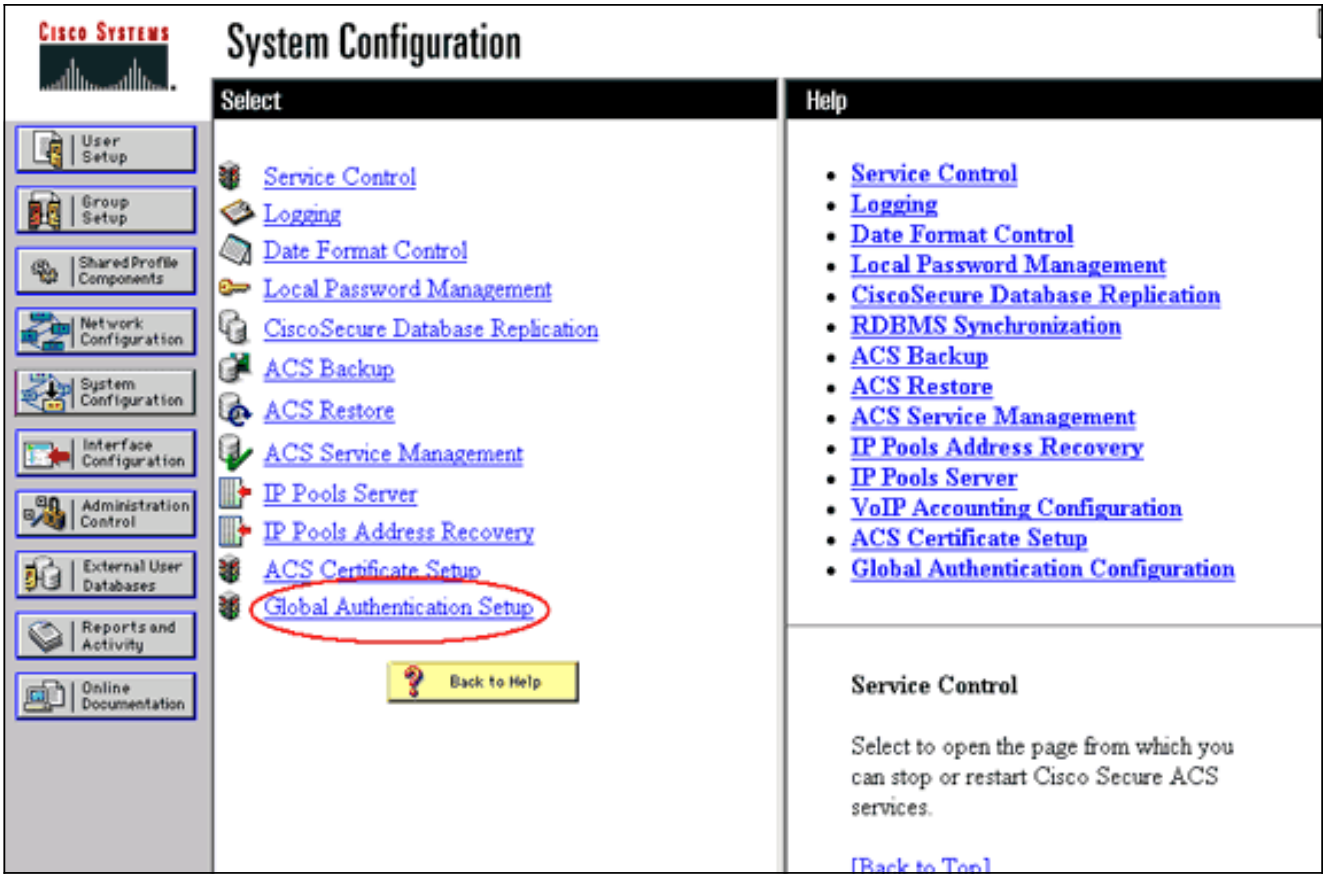
Vous pouvez également émettre ces commandes à partir de l'interface de ligne de commande :

2. L'étape suivante consiste à configurer l'AP WDS dans le serveur d'authentification en tant que client AAA (Authentication, Authorization, and Accounting). Pour cela, vous devez ajouter l'AP WDS en tant que client AAA. Procédez comme suit :**Remarque :** ce document utilise le serveur Cisco Secure ACS comme serveur d'authentification.Dans Cisco Secure Access Control Server (ACS), ceci se produit sur la page Network Configuration où vous définissez ces attributs pour l'AP WDS :Name (nom)Adresse IPSecret partagéMéthode d'authentificationRADIUS Cisco AironetGroupe de travail technique sur l'Internet RADIUS

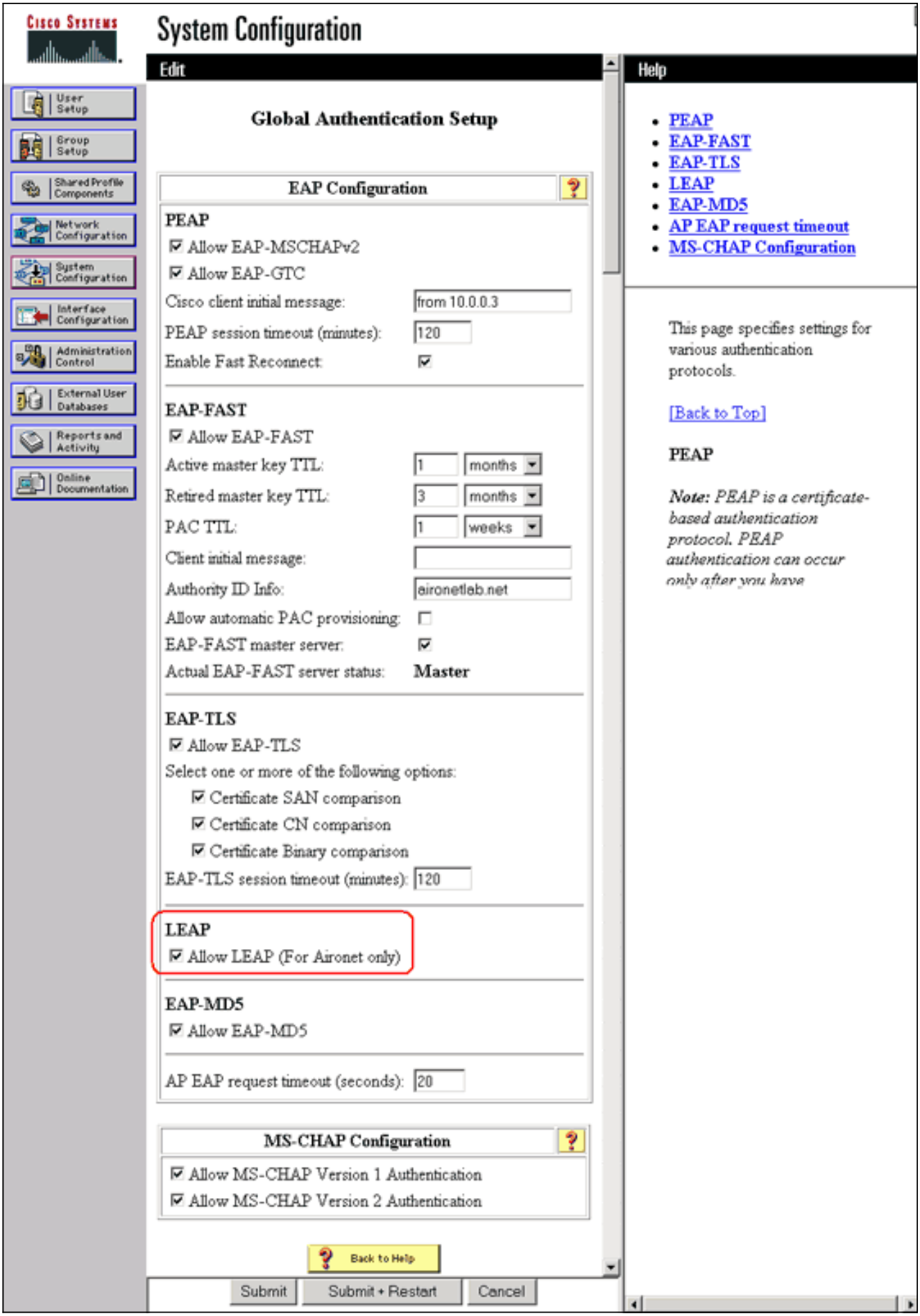
[IETF]Cliquez sur **Soumettre**.Pour les autres serveurs d'authentification non ACS, reportez-vous à la documentation du
fabricant.



En outre, dans Cisco Secure ACS, assurez-vous que vous configurez ACS pour exécuter l'authentification LEAP sur la page Configuration du système - Configuration de l'authentification globale. Tout d'abord, cliquez sur **Configuration du système**, puis sur **Configuration de l'authentification
globale**.

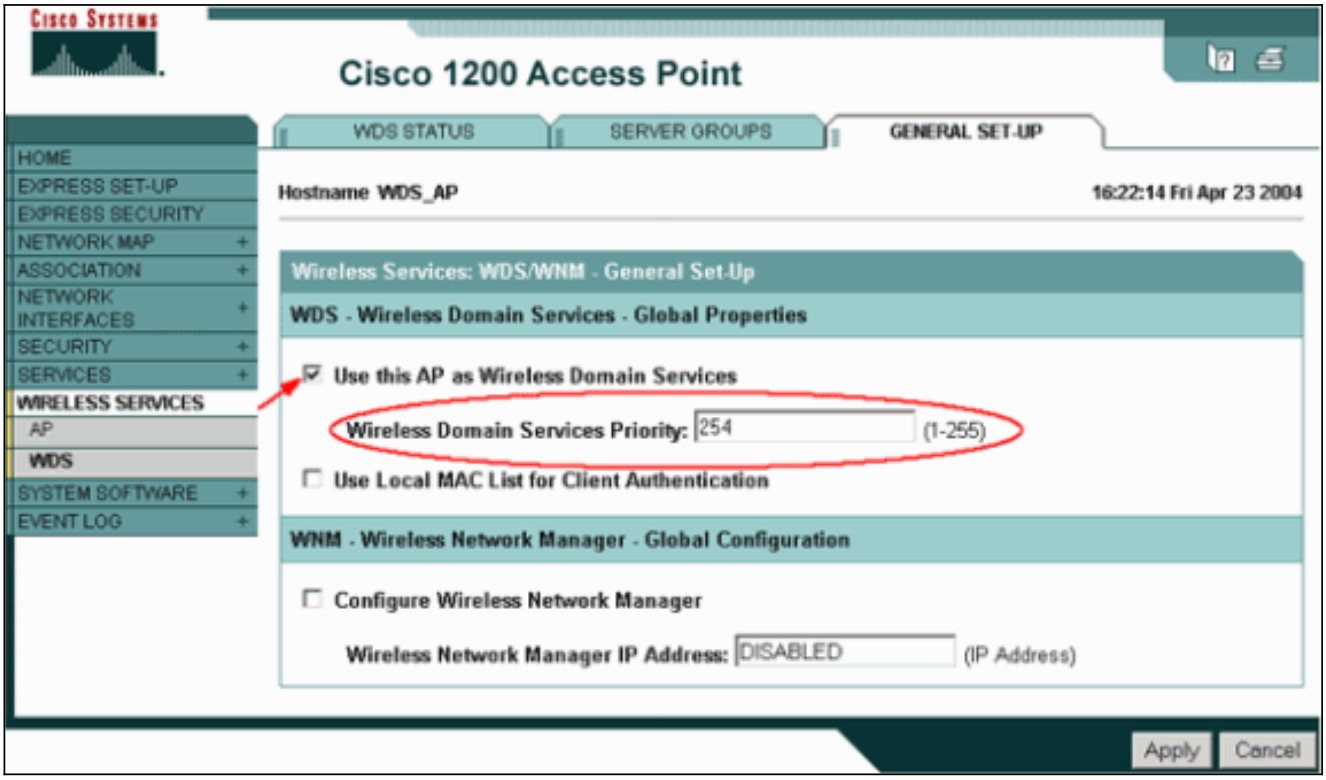


Faites défiler la page vers le bas jusqu'au paramètre LEAP. Lorsque vous cochez cette case, ACS authentifie
LEAP.



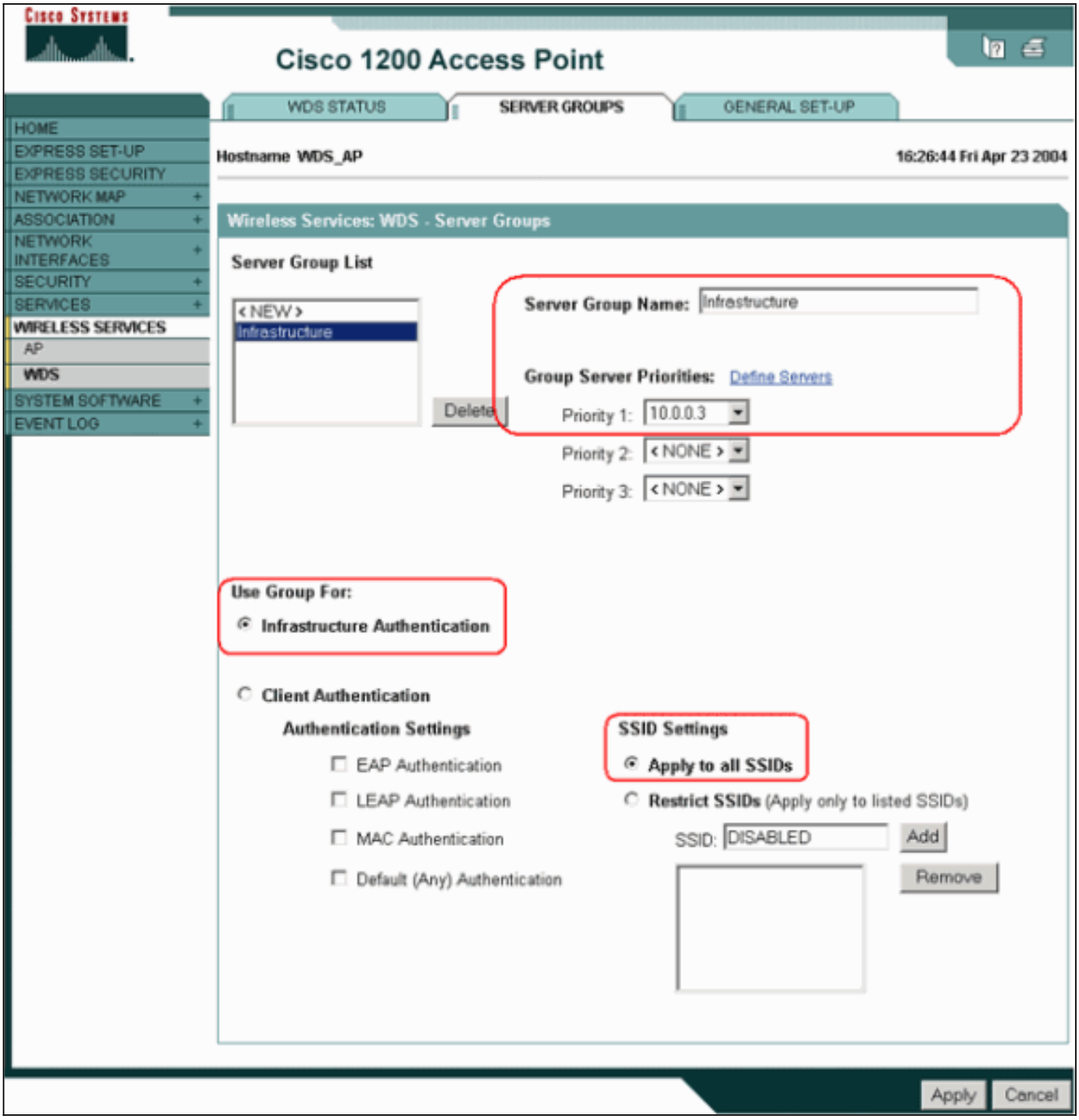
3. Afin de configurer les paramètres WDS sur l'AP WDS, choisissez **Wireless Services > WDS** sur l'AP WDS, puis cliquez sur l'onglet **General Set-Up**. Effectuez les étapes suivantes :Sous WDS-Wireless Domain Services - Global Properties, cochez la case **Use this AP as Wireless**

Domain Services.Définissez la valeur du champ Wireless Domain Services Priority sur environ **254**, car il s'agit du premier. Vous pouvez configurer un ou plusieurs points d'accès ou commutateurs comme candidats pour fournir WDS. Le périphérique ayant la priorité la plus élevée fournit
WDS.



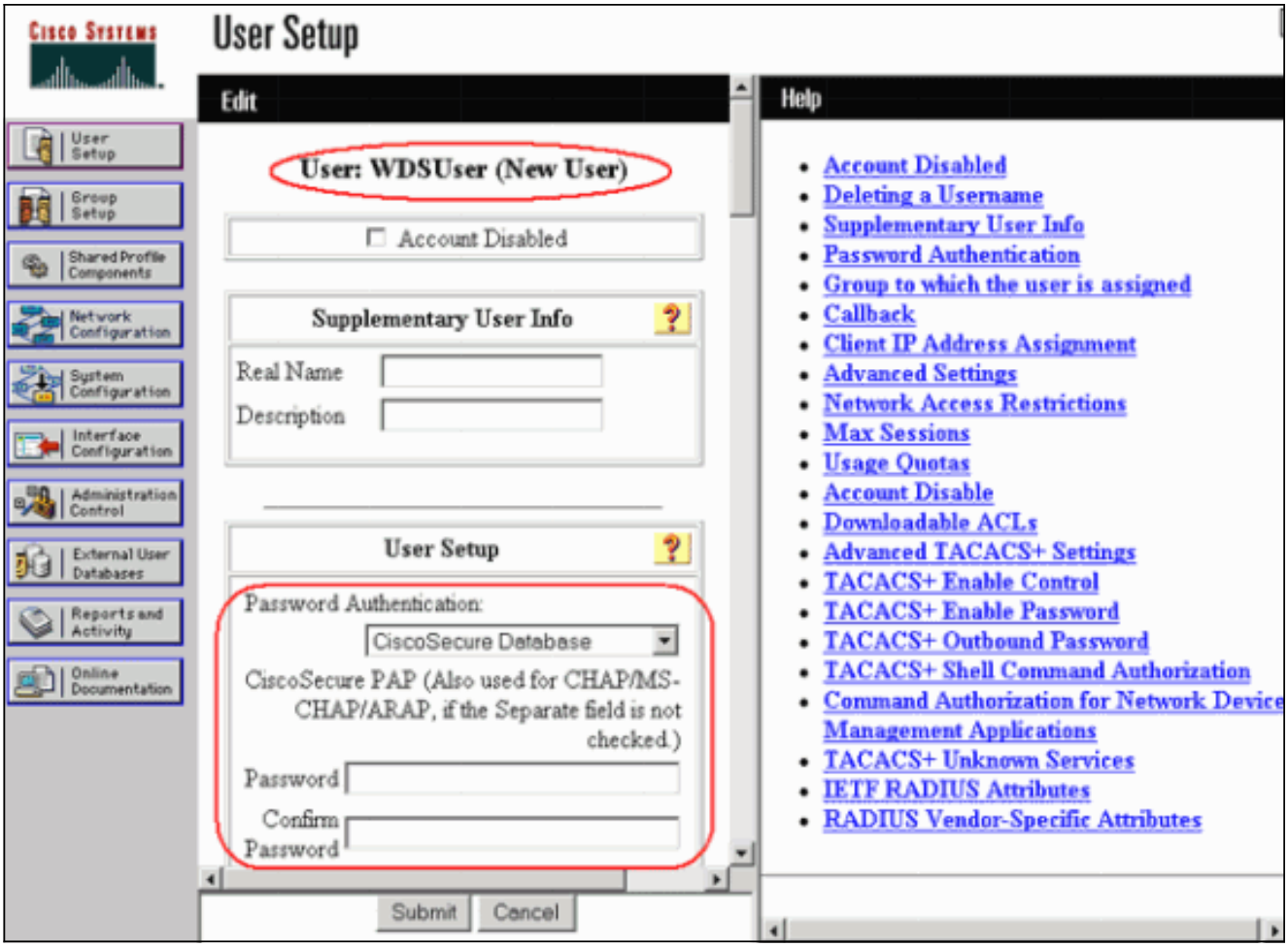
Vous pouvez également émettre ces commandes à partir de l'interface de ligne de commande :

4. Choisissez **Wireless Services > WDS**, puis accédez à l'onglet **Server Groups** :Définissez un nom de groupe de serveurs qui authentifie les autres points d'accès, un groupe d'infrastructure.Définissez la priorité 1 sur le serveur d'authentification précédemment configuré.Cliquez sur le **groupe Utiliser pour :** Bouton radio **Infrastructure Authentication**.Appliquez les paramètres aux SSID (Service Set Identifiers) appropriés.



Vous pouvez également émettre ces commandes à partir de l'interface de ligne de commande :

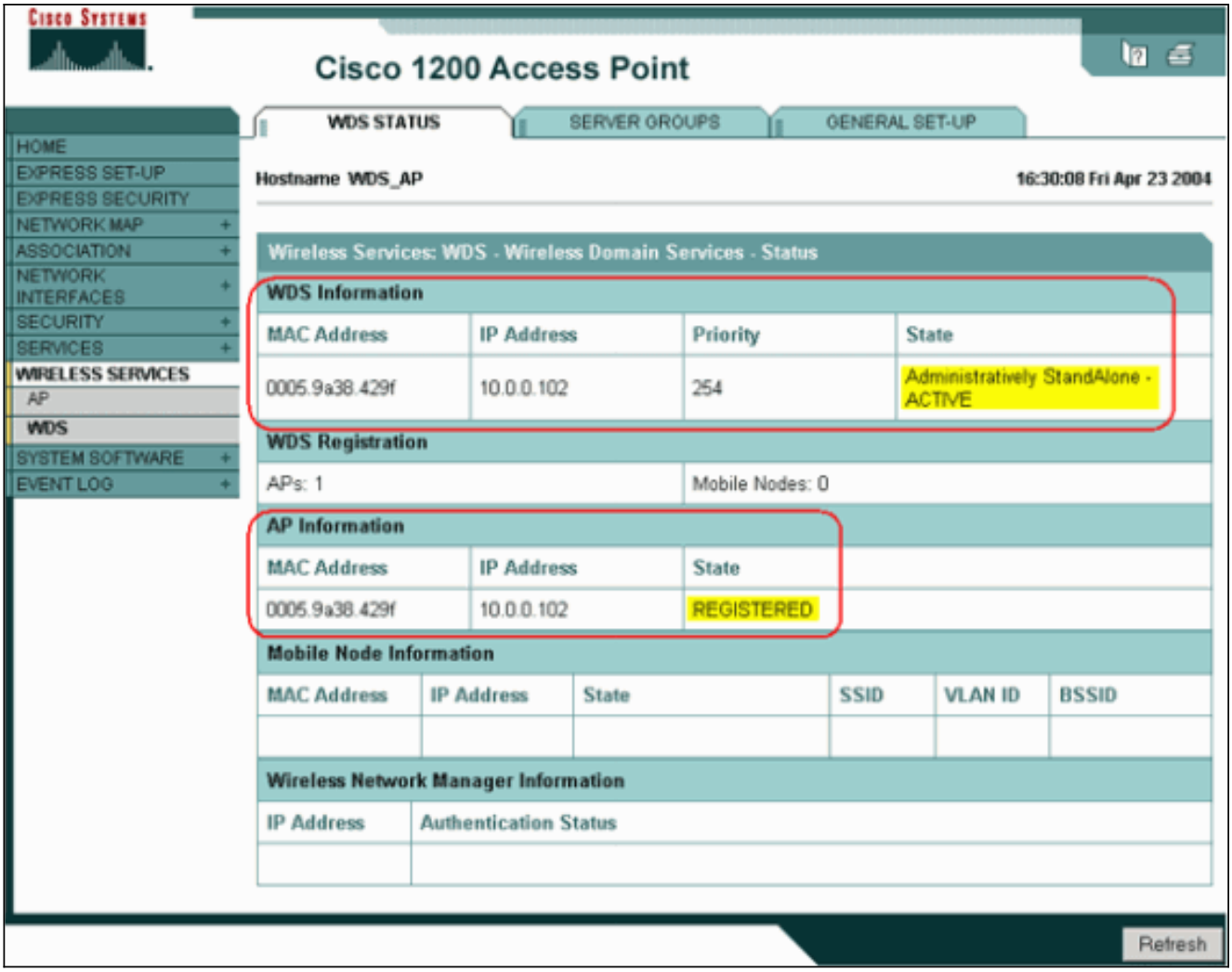
5. Configurez le nom d'utilisateur et le mot de passe WDS en tant qu'utilisateur dans votre serveur d'authentification.Dans Cisco Secure ACS, cela se produit sur la page User Setup, où vous définissez le nom d'utilisateur et le mot de passe WDS. Pour les autres serveurs d'authentification non ACS, reportez-vous à la documentation du fabricant.**Remarque :** Ne placez pas l'utilisateur WDS dans un groupe auquel sont attribués de nombreux droits et privilèges : WDS ne nécessite qu'une authentification limitée.



6. Choisissez **Wireless Services > AP**, puis cliquez sur **Enable** pour l'option Participate in SWAN infrastructure. Tapez ensuite le nom d'utilisateur et le mot de passe WDS.Vous devez définir un nom d'utilisateur et un mot de passe WDS sur le serveur d'authentification pour tous les périphériques que vous désignez membres du
WDS.

Vous pouvez également émettre ces commandes à partir de l'interface de ligne de commande :

7. Choisissez **Wireless Services > WDS**. Dans l'onglet WDS AP Status, vérifiez si le WDS AP apparaît dans la zone WDS Information, dans l'état ACTIVE. Le point d'accès doit également apparaître dans la zone Informations du point d'accès, avec l'état REGISTERED.Si le point d'accès n'apparaît pas ENREGISTRÉ ou ACTIF, recherchez des erreurs ou des tentatives d'authentification échouées sur le serveur d'authentification.Lorsque le point d'accès s'enregistre correctement, ajoutez un point d'accès d'infrastructure pour utiliser les services du
WDS.



Vous pouvez également émettre ces commandes à partir de l'interface de ligne de commande :**Remarque :** Vous ne pouvez pas tester les associations de clients car l'authentification de client n'a pas encore de dispositions.

Désigner un WLSM comme WDS

Cette section explique comment configurer un WLSM en tant que WDS. Le WDS est le seul périphérique qui communique avec le serveur d'authentification.

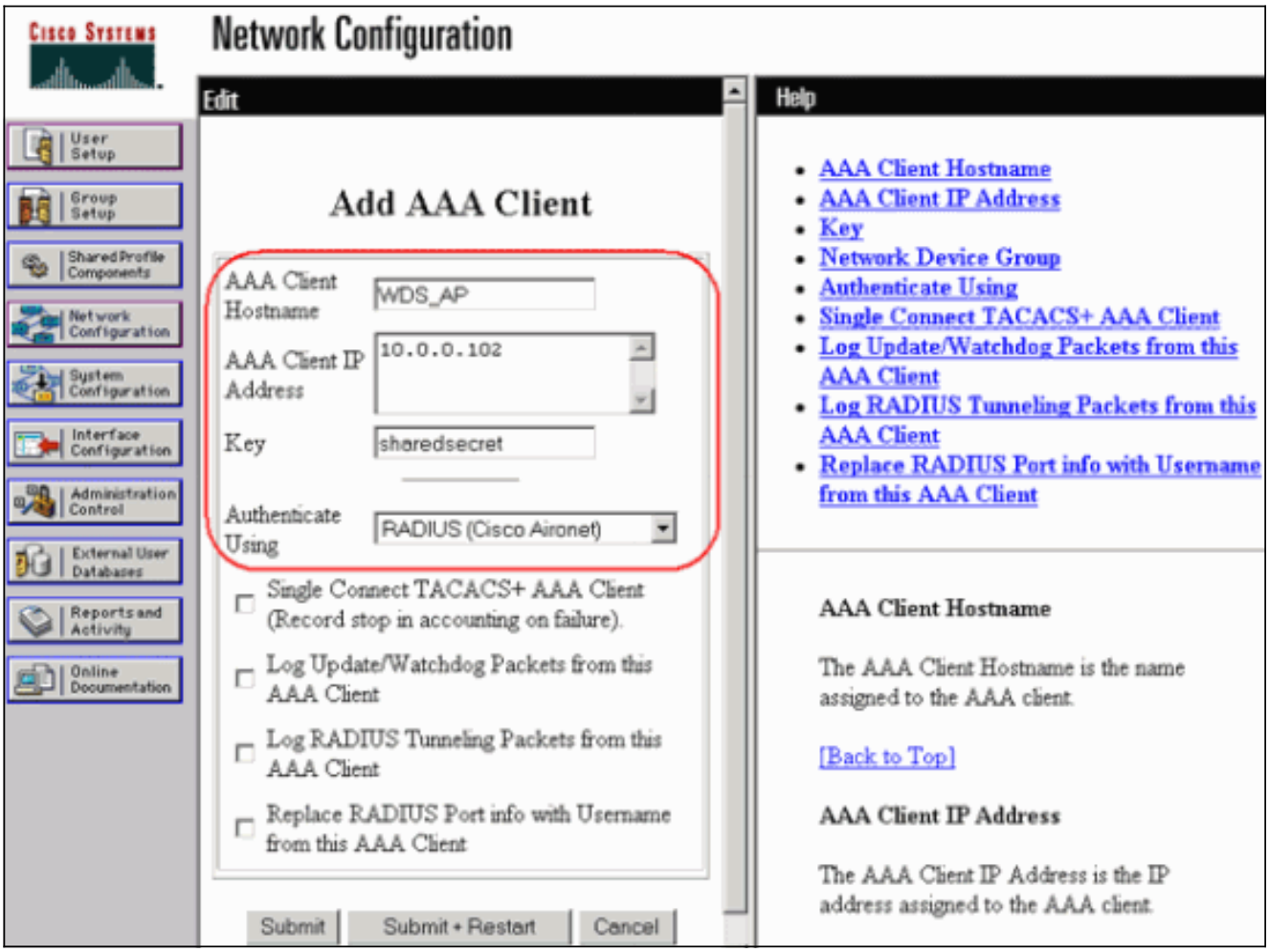
Remarque : Émettez ces commandes à l'invite de commandes `enable` du WLSM, et non du Supervisor Engine 720. Afin d'accéder à l'invite de commandes du WLSM, émettez ces commandes à une invite de commandes `enable` dans le Supervisor Engine 720 :

```
c6506#session slot x proc 1
!--- In this command, x is the slot number where the
WLSM resides. The default escape character is Ctrl-^,
then x. You can also type 'exit' at the remote prompt to
end the session Trying 127.0.0.51 ... Open User Access
Verification Username: <username> Password: <password>
wlan>enable
Password: <enable password>
wlan#
```

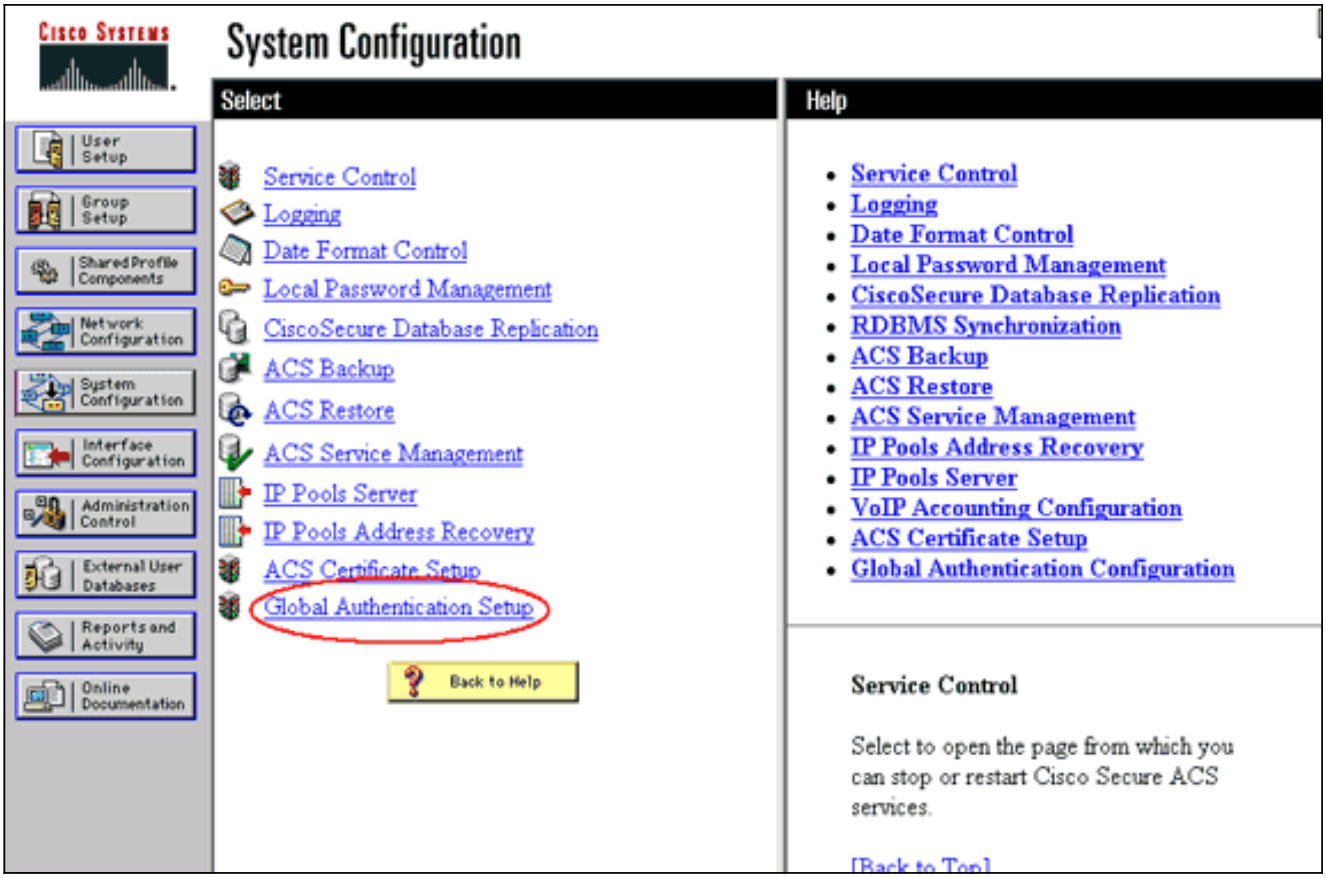
Remarque : afin de dépanner et de gérer votre WLSM plus facilement, configurez l'accès distant Telnet au WLSM. Reportez-vous à Configuration de l'accès distant Telnet.

Afin de désigner un WLSM comme WDS :

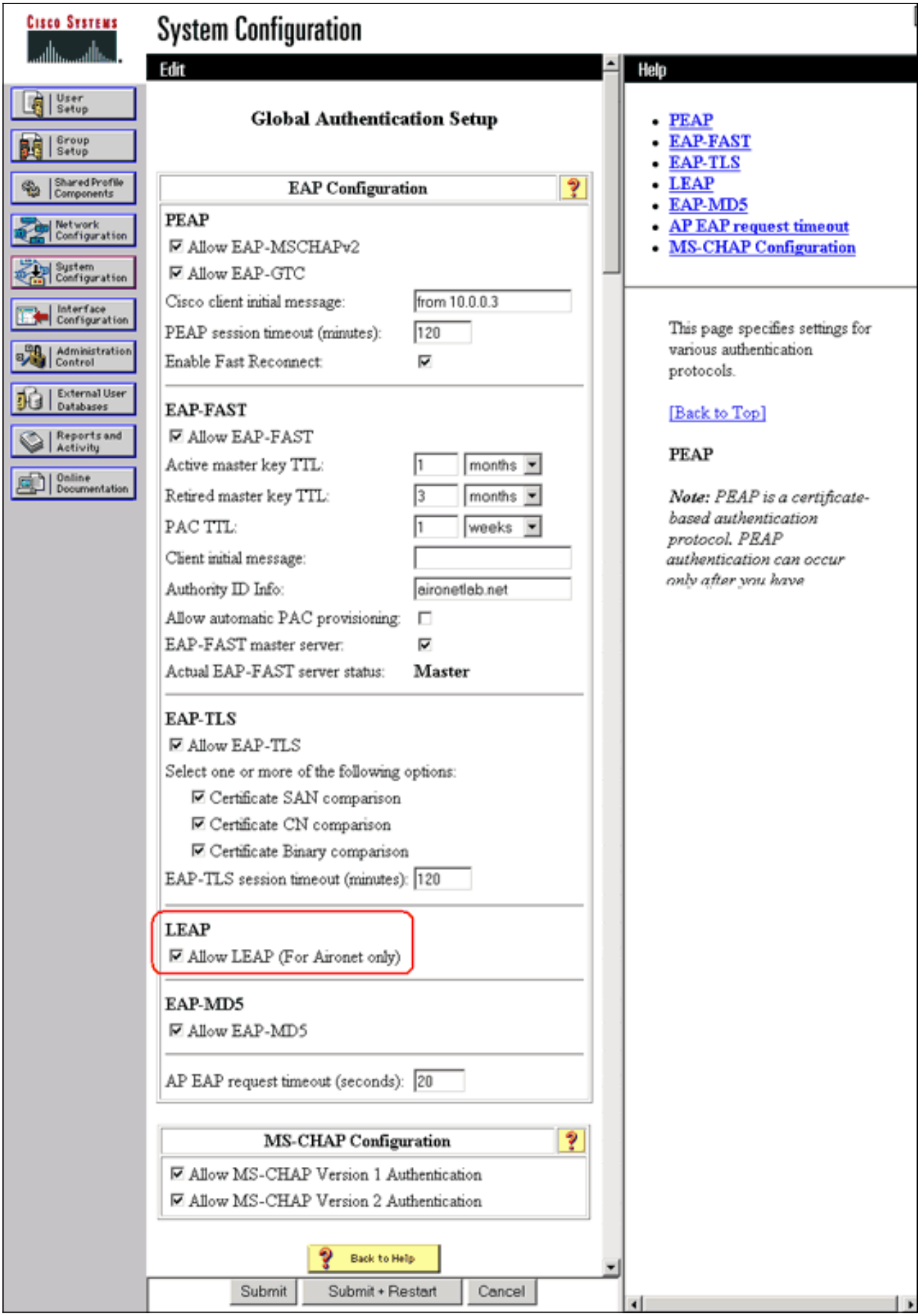
1. Àpartir de l'interface de ligne de commande du WLSM, émettez ces commandes et établissez une relation avec le serveur d'authentification :**Remarque :** Il n'existe aucun contrôle de priorité dans le WLSM. Si le réseau contient plusieurs modules WLSM, WLSM utilise la configuration de redondance afin de déterminer le module principal.
2. Configurez le WLSM dans le serveur d'authentification en tant que client AAA.Dans Cisco Secure ACS, ceci se produit sur la page Configuration du réseau où vous définissez ces attributs pour le WLSM :Name (nom)Adresse IPSecret partagéMéthode d'authentificationRADIUS Cisco AironetIETF RADIUSPour les autres serveurs d'authentification non ACS, reportez-vous à la documentation du fabricant.



En outre, dans Cisco Secure ACS, configurez ACS pour exécuter l'authentification LEAP sur la page Configuration du système - Configuration de l'authentification globale. Tout d'abord, cliquez sur **Configuration du système**, puis sur **Configuration de l'authentification globale**.



Faites défiler la page vers le bas jusqu'au paramètre LEAP. Lorsque vous cochez cette case, ACS authentifie
LEAP.



3. Sur le WLSM, définissez une méthode qui authentifie les autres AP (un groupe de serveurs d'infrastructure).
4. Sur le WLSM, définissez une méthode qui authentifie les périphériques clients (un groupe de

serveurs clients) et les types EAP que ces clients utilisent.**Remarque :** Cette étape élimine la nécessité du processus Définir la méthode d'authentification du client.

5. Définissez un VLAN unique entre le Supervisor Engine 720 et le WLSM afin de permettre au WLSM de communiquer avec des entités externes telles que les AP et les serveurs d'authentification. Ce VLAN est inutilisé partout ailleurs ou à toute autre fin sur le réseau. Créez d'abord le VLAN sur le Supervisor Engine 720, puis exécutez les commandes suivantes :Sur le Supervisor Engine 720 :Sur le WLSM :
6. Vérifiez la fonction du WLSM à l'aide des commandes suivantes :Sur le WLSM :Sur le Supervisor Engine 720 :

Désigner un point d'accès en tant que périphérique d'infrastructure

Ensuite, vous devez désigner au moins un point d'accès d'infrastructure et associer le point d'accès au WDS. Les clients s'associent aux points d'accès d'infrastructure. Les points d'accès d'infrastructure demandent au point d'accès WDS ou au WLSM d'effectuer l'authentification pour eux.

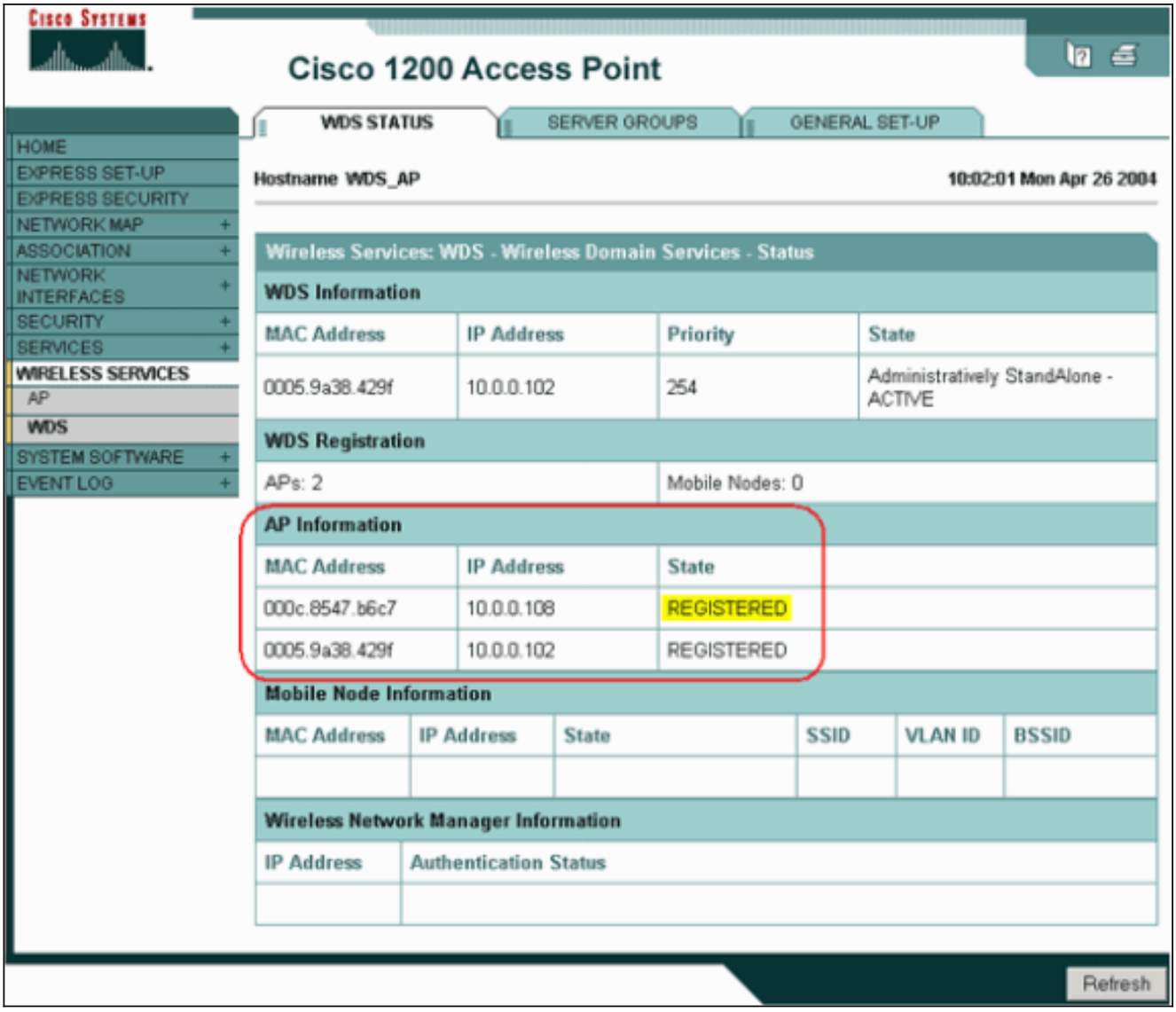
Complétez ces étapes afin d'ajouter un point d'accès d'infrastructure qui utilise les services du WDS :

Remarque : Cette configuration s'applique uniquement aux points d'accès d'infrastructure et non au point d'accès WDS.

1. Choisissez **Wireless Services > AP**. Sur le point d'accès de l'infrastructure, sélectionnez **Activer** pour l'option Services sans fil. Tapez ensuite le nom d'utilisateur et le mot de passe WDS.Vous devez définir un nom d'utilisateur et un mot de passe WDS sur le serveur d'authentification pour tous les périphériques qui doivent être membres du WDS.

Vous pouvez également émettre ces commandes à partir de l'interface de ligne de commande :

2. Choisissez **Wireless Services > WDS**. Dans l'onglet WDS AP Status, le nouveau point d'accès d'infrastructure apparaît dans la zone WDS Information, avec l'état ACTIVE, et dans la zone AP Information, avec l'état REGISTERED.Si le point d'accès n'apparaît pas ACTIVE et/ou REGISTERED, recherchez des erreurs ou des tentatives d'authentification échouées sur le serveur d'authentification.Une fois que le point d'accès apparaît ACTIVE et/ou REGISTERED, ajoutez une méthode d'authentification client au WDS.



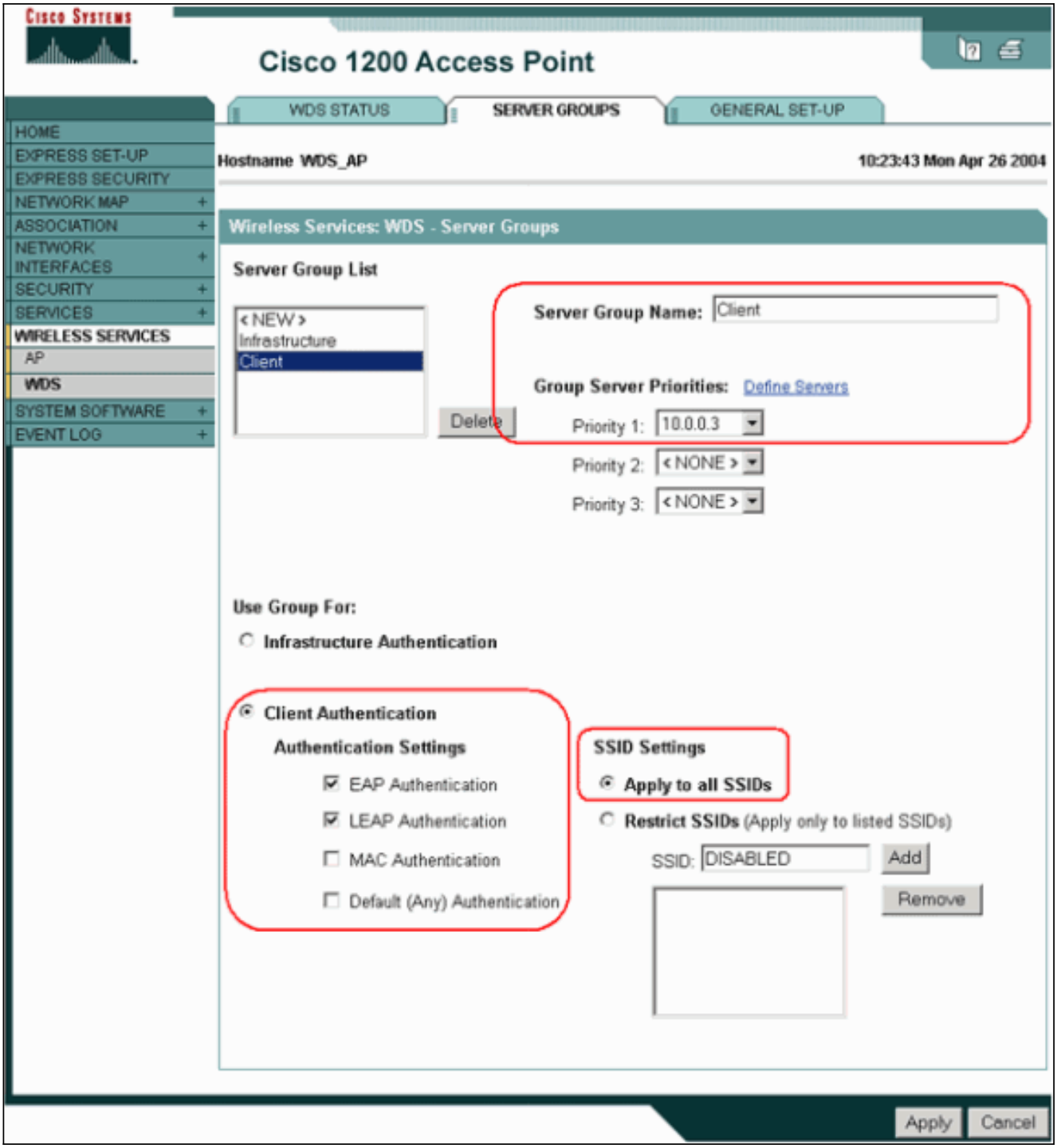
Vous pouvez également émettre cette commande à partir de l'interface de ligne de commande :Vous pouvez également émettre cette commande à partir du WLSM :Ensuite, émettez cette commande sur l'AP d'infrastructure :**Remarque :** Vous ne pouvez pas tester les associations de clients car l'authentification de client n'a pas encore de dispositions.

Définir la méthode d'authentification du client

Enfin, définissez une méthode d'authentification du client.

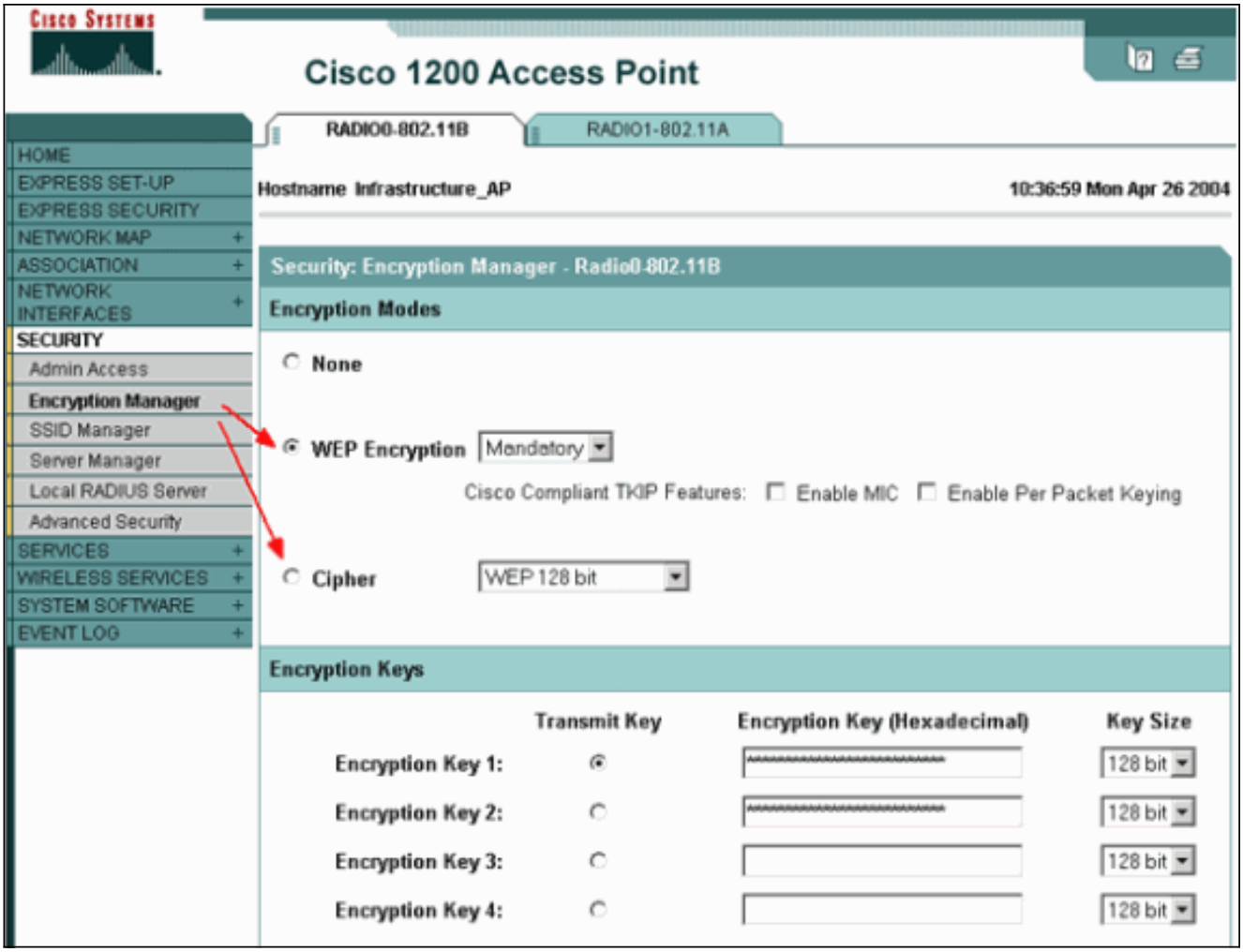
Complétez ces étapes afin d'ajouter une méthode d'authentification client :

1. Choisissez **Wireless Services > WDS**. Effectuez ces étapes dans l'onglet WDS AP Server Groups :Définissez un groupe de serveurs qui authentifie les clients (un groupe de clients).Définissez la priorité 1 sur le serveur d'authentification précédemment configuré.Définissez le type d'authentification applicable (LEAP, EAP, MAC, etc.).Appliquez les paramètres aux SSID
appropriés.

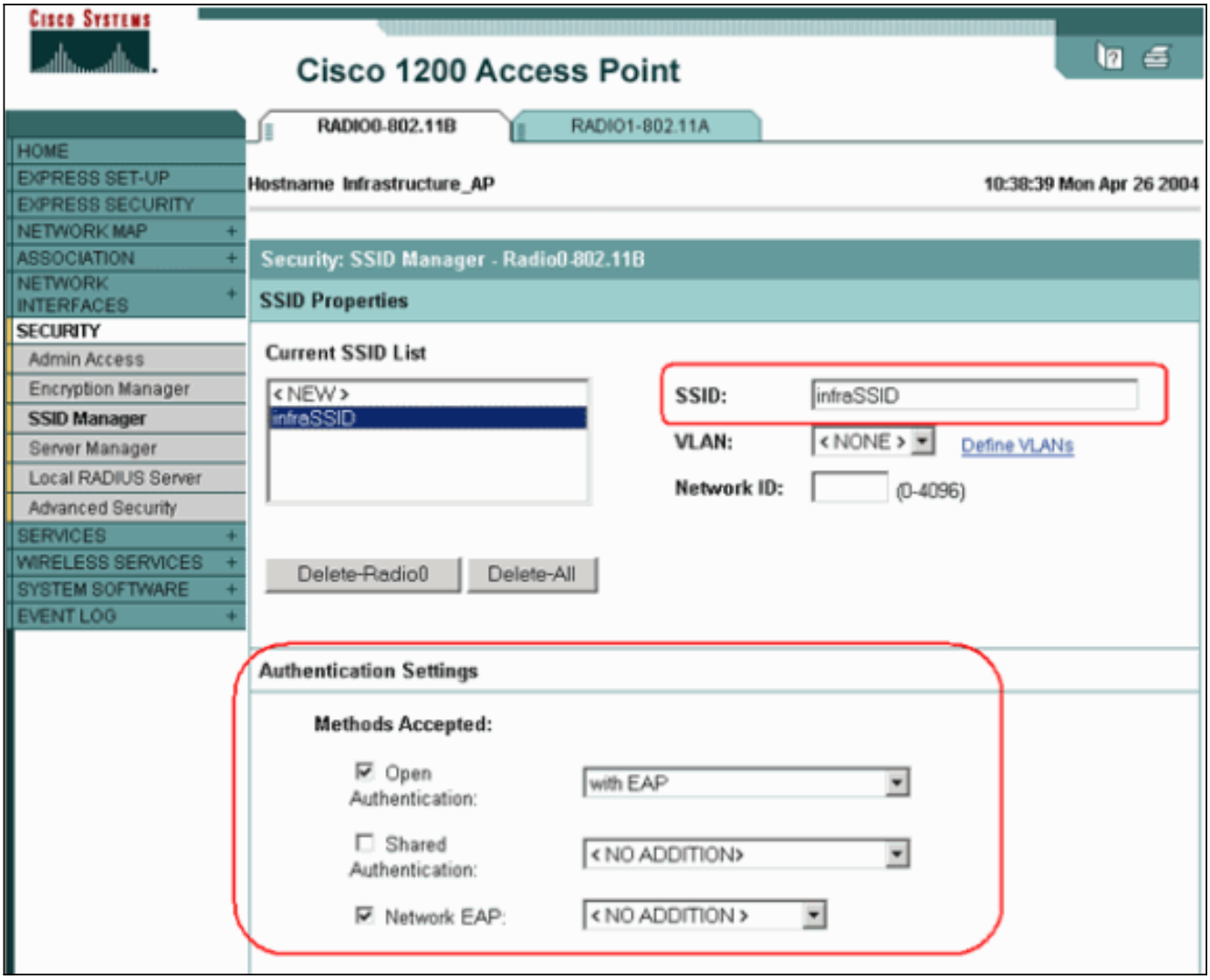


Vous pouvez également émettre ces commandes à partir de l'interface de ligne de commande :**Remarque :** L'exemple de point d'accès WDS est dédié et n'accepte pas les associations de clients.**Remarque :** Ne configurez pas les points d'accès d'infrastructure pour les groupes de serveurs, car les points d'accès d'infrastructure transmettent toutes les demandes au WDS à traiter.

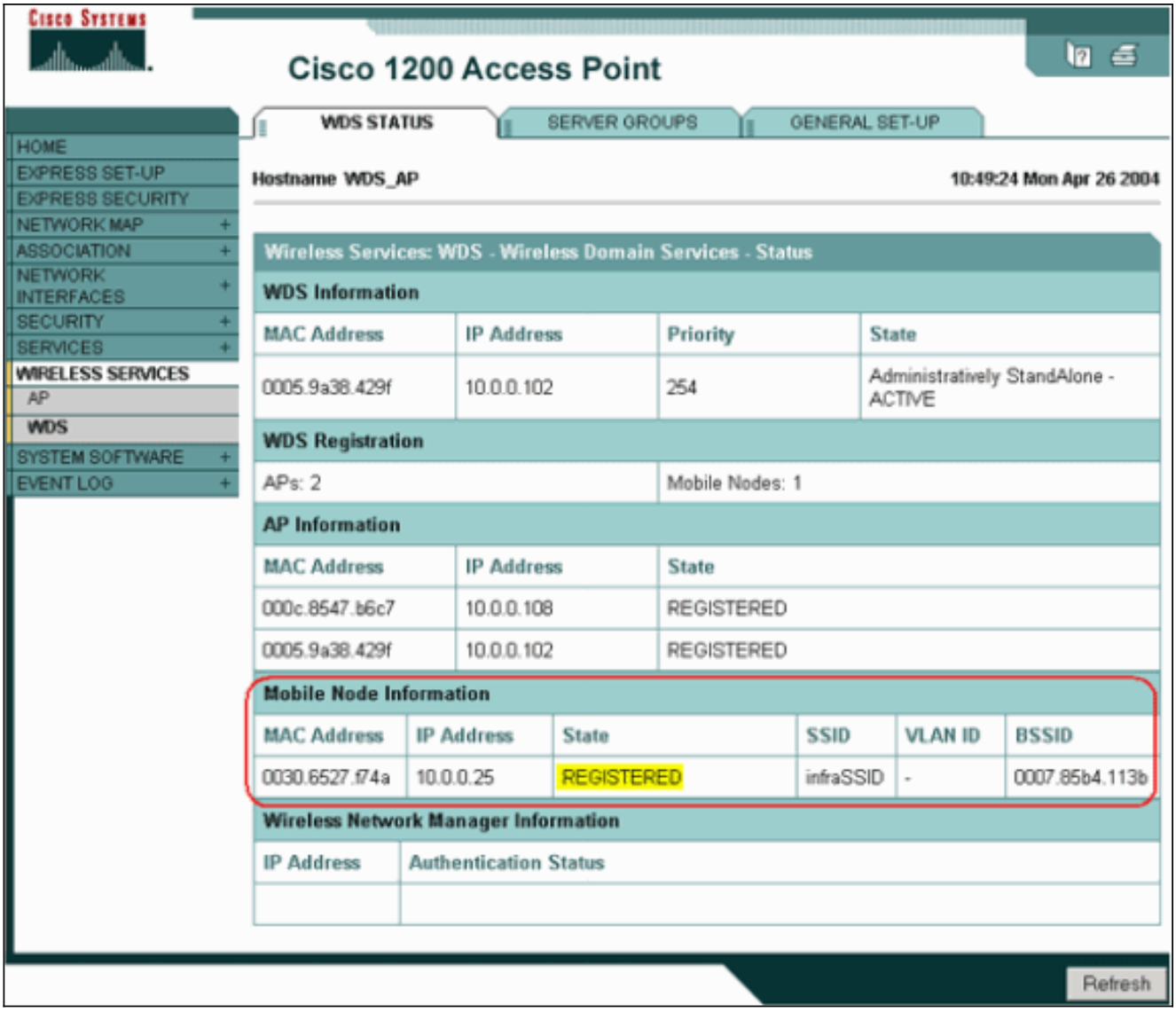
2. Sur le ou les AP d'infrastructure :Sous l'élément de menu **Security > Encryption Manager**, cliquez sur **WEP Encryption** ou **Cipher**, selon les besoins du protocole d'authentification que vous
utilisez.



Sous l'élément de menu **Security > SSID Manager**, sélectionnez les méthodes d'authentification requises par le protocole d'authentification que vous utilisez.



3. Vous pouvez maintenant vérifier si les clients s'authentifient auprès des points d'accès d'infrastructure. L'AP du WDS dans l'onglet État du WDS (sous l'élément de menu **Wireless Services > WDS**) indique que le client apparaît dans la zone Informations du noeud mobile et a un état REGISTERED (ENREGISTRÉ).Si le client n'apparaît pas, recherchez des erreurs ou des tentatives d'authentification échouées par les clients sur le serveur d'authentification.



Vous pouvez également émettre ces commandes à partir de l'interface de ligne de commande :**Remarque :** Si vous devez déboguer l'authentification, assurez-vous que vous déboguez sur l'AP WDS, car l'AP WDS est le périphérique qui communique avec le serveur d'authentification.

Vérification

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannage

Cette section présente les informations que vous pouvez utiliser pour dépanner votre configuration. Cette liste présente quelques-unes des questions courantes liées à la commande WDS afin de clarifier l'utilité de ces commandes :

- **Question : Sur le point d'accès WDS, quels sont les paramètres recommandés pour ces éléments ?radius-server timeoutradius-server interminableTemporal Key Integrity Protocol (TKIP) Message Integrity Check (MIC) Failure Holdoff TimeDurée d'attente du clientIntervalle de réauthentification EAP ou MACDélai d'attente du client EAP (facultatif)Réponse :** Il est conseillé de conserver la configuration avec les paramètres par défaut concernant ces

paramètres spéciaux, et de ne les utiliser que lorsqu'il y a un problème de synchronisation.Voici les paramètres recommandés pour l'AP WDS :Désactivez **radius-server timeout**. Il s'agit du nombre de secondes pendant lesquelles un point d'accès attend une réponse à une requête RADIUS avant de renvoyer la requête. 5 secondes sont établies par défaut.Désactivez **radius-server interminable**. Le RADIUS est ignoré par des requêtes supplémentaires pendant la durée des minutes, sauf si tous les serveurs sont marqués comme morts.La durée d'attente des échecs MIC TKIP est activée par défaut à 60 secondes. Si vous activez le temps d'attente, vous pouvez entrer l'intervalle en secondes. Si le point d'accès détecte deux défaillances MIC dans les 60 secondes, il bloque tous les clients TKIP sur cette interface pendant la période de retenue spécifiée ici.Par défaut, la durée d'attente du client doit être désactivée. Si vous activez la mise hors service, entrez le nombre de secondes pendant lesquelles le point d'accès doit attendre après une défaillance d'authentification avant de traiter une demande d'authentification ultérieure.L'intervalle de réauthentification EAP ou MAC est désactivé par défaut. Si vous activez la réauthentification, vous pouvez spécifier l'intervalle ou accepter l'intervalle donné par le serveur d'authentification. Si vous choisissez de spécifier l'intervalle, entrez l'intervalle en secondes que le point d'accès attend avant de forcer un client authentifié à se réauthentifier.Le délai d'attente du client EAP (facultatif) est de 120 secondes par défaut. Saisissez le délai pendant lequel le point d'accès doit attendre que les clients sans fil répondent aux demandes d'authentification EAP.

- **Question : En ce qui concerne le temps de retenue TKIP, j'ai lu que ce délai devrait être fixé à 100 ms et non à 60 secondes. Je suppose qu'il est réglé sur une seconde à partir du navigateur, car c'est le nombre le plus bas que vous pouvez sélectionner ?Réponse :** Il n'y a pas de recommandation spécifique de le régler à 100 ms à moins qu'il y ait un échec signalé où la seule solution est d'augmenter cette fois. Une seconde est la valeur la plus basse.
- **Question : Ces deux commandes aident-elles l'authentification des clients de quelque manière que ce soit et sont-elles nécessaires sur le WDS ou le point d'accès d'infrastructure ?radius-server attribute 6 on-for-login-authradius-server attribute 6 support-multipleRéponse :** Ces commandes n'aident pas le processus d'authentification et elles ne sont pas nécessaires sur le WDS ou le point d'accès.
- **Question : Sur le point d'accès d'infrastructure, je suppose qu'aucun des paramètres du Gestionnaire de serveur et des propriétés globales n'est nécessaire car le point d'accès reçoit des informations du WDS. L'une de ces commandes spécifiques est-elle nécessaire pour le point d'accès de l'infrastructure ?radius-server attribute 6 on-for-login-authradius-server attribute 6 support-multipleradius-server timeoutradius-server interminableRéponse :** Il n'est pas nécessaire d'avoir Gestionnaire de serveur et Propriétés globales pour les AP d'infrastructure. Le WDS s'occupe de cette tâche et il n'est pas nécessaire d'avoir ces paramètres :**radius-server attribute 6 on-for-login-authradius-server attribute 6 support-multipleradius-server timeoutradius-server interminable**Le paramètre **radius-server attribute 32 include-in-access-req format %h** reste par défaut et est obligatoire.

Un point d'accès est un périphérique de couche 2. Par conséquent, le point d'accès ne prend pas en charge la mobilité de couche 3 lorsque le point d'accès est configuré pour agir comme un périphérique WDS. Vous ne pouvez atteindre la mobilité de couche 3 que lorsque vous configurez le WLSM en tant que périphérique WDS. Reportez-vous à la section *Architecture de mobilité de couche 3* du module de services LAN sans fil de la gamme Cisco Catalyst 6500 : Livre blanc pour plus d'informations.

Par conséquent, lorsque vous configurez un point d'accès en tant que périphérique WDS, n'utilisez pas la commande **mobile network-id**. Cette commande s'applique à la mobilité de couche

3 et vous devez disposer d'un WLSM comme périphérique WDS pour configurer correctement la mobilité de couche 3. Si vous utilisez la commande **mobile network-id** de manière incorrecte, vous pouvez voir certains des symptômes suivants :

- Les clients sans fil ne peuvent pas s'associer à l'AP.
- Les clients sans fil peuvent s'associer au point d'accès, mais ne reçoivent pas d'adresse IP du serveur DHCP.
- Un téléphone sans fil n'est pas authentifié lorsque vous disposez d'un déploiement voix sur WLAN.
- L'authentification EAP ne se produit pas. Avec l'**ID réseau de mobilité** configuré, le point d'accès tente de créer un tunnel GRE (Generic Routing Encapsulation) pour transférer les paquets EAP. Si aucun tunnel n'est établi, les paquets ne vont nulle part.
- Un point d'accès configuré en tant que périphérique WDS ne fonctionne pas comme prévu et la configuration WDS ne fonctionne pas.**Remarque :** Vous ne pouvez pas configurer le point d'accès/pont Cisco Aironet 1300 en tant que maître WDS. Le point d'accès/pont 1300 ne prend pas en charge cette fonctionnalité. Le point d'accès/pont 1300 peut participer à un réseau WDS en tant que périphérique d'infrastructure dans lequel un autre point d'accès ou WLSM est configuré comme maître WDS.

Dépannage des commandes

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes show. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show .**

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

- **debug dot11 aaa authenticator all** - Affiche les différentes négociations qu'un client passe pendant que le client s'associe et s'authentifie au cours du processus 802.1x ou EAP. Ce débogage a été introduit dans le logiciel Cisco IOS Version 12.2(15)JA. Cette commande rend obsolète **debug dot11 aaa dot1x** dans cette version et les versions ultérieures.
- **debug aaa authentication** - Affiche le processus d'authentification du point de vue AAA générique.
- **debug wlcp ap** - Affiche les négociations WLCCP impliquées lorsqu'un point d'accès rejoint un WDS.
- **debug wlcp packet** - Affiche les informations détaillées sur les négociations WLCCP.
- **debug wlcp leap-client** - Affiche les détails lorsqu'un périphérique d'infrastructure rejoint un WDS.

Informations connexes

- Configuration de WDS, de l'itinérance sécurisée rapide et de la gestion radio
- Note de configuration du module de services LAN sans fil de la gamme Catalyst 6500
- Configuration des suites de chiffre et de WEP
- Configuration des types d'authentification
- Pages d'assistance LAN sans fil
- Support et documentation techniques - Cisco Systems