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 de services Sans fil de RÉSEAU LOCAL (WLSM) comme WDS et au moins un autre comme infrastructure AP. 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 destine pour établir une base dont vous peut configurer l'itinérance sécurisée rapide ou introduire une engine Sans fil de solutions LAN (WLSE) dans le réseau, ainsi vous pouvez utiliser les caractéristiques.

Conditions préalables

Conditions requises

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

- Ayez la connaissance complète des réseaux LAN sans fil et des problèmes de sécurité de radio.
- Ayez la connaissance des méthodes en cours de Sécurité de Protocole EAP (Extensible Authentication Protocol).

Composants utilisés

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

- Aps avec le logiciel de Cisco IOS®
- Version du logiciel Cisco IOS 12.3(2)JA2 ou plus tard
- Module de services Sans fil réseau local de 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 commencé par une configuration (par défaut) effacée et une adresse IP sur l'interface BVI1, ainsi l'unité est accessible du GUI de logiciel de Cisco IOS ou de l'interface de ligne de commande (CLI). Si vous travaillez dans un réseau vivant, assurez-vous que vous comprenez l'impact potentiel de n'importe quelle 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

Le WDS est une nouvelle caractéristique pour des aps dans le logiciel de Cisco IOS et la base de la gamme Catalyst 6500 WLSM. Le WDS est une principale fonction qui active d'autres caractéristiques comme ces derniers :

- Jeûnent l'itinérance sécurisée
- Interaction WLSE
- Gestion par radio

Vous devez établir des relations entre les aps qui participent au WDS et au WLSM, avant que toutes les autres caractéristiques basées sur WDS fonctionnent. Un des buts du WDS est d'éliminer le besoin du serveur d'authentification de valider des identifiants utilisateurs et de réduire la durée requise pour des authentifications client.

Afin d'utiliser le WDS, vous devez indiquer un AP ou le WLSM comme WDS. UN WDS AP doit employer un nom d'utilisateur et le mot de passe WDS pour établir des relations avec un serveur d'authentification. Le serveur d'authentification peut être un serveur RADIUS externe ou la caractéristique locale de serveur de RADIUS dans le WDS AP. Le WLSM doit avoir des relations avec le serveur d'authentification, quoique WLSM n'ait pas besoin d'authentifier au serveur.

D'autres aps, appelés l'infrastructure aps, communiquent avec le WDS. Avant que l'enregistrement se produise, l'infrastructure aps doit s'authentifier au WDS. Un groupe de serveurs d'infrastructure sur le WDS définit cette authentification d'infrastructure.

Un ou plusieurs groupes de client-serveur sur le WDS définissent l'authentification client.

Quand les tentatives d'un client de s'associer à une infrastructure AP, l'infrastructure AP passe les qualifications de l'utilisateur au WDS pour la validation. Si le WDS voit les qualifications pour la première fois, le WDS se tourne vers le serveur d'authentification pour valider les qualifications. Le WDS cache alors les qualifications, afin d'éliminer la nécessité de retourner au serveur

d'authentification quand le même utilisateur tente l'authentification de nouveau. Les exemples de la ré-authentification incluent :

- Nouvelle saisie
- Errer
- Quand l'utilisateur met en marche le périphérique de client

N'importe quel protocole d'authentification EAP basé sur RADIUS peut être percé un tunnel par le WDS de ce type :

- EAP léger (LEAP)
- EAP protégé (PEAP)
- EAP-Transport Layer Security (EAP-TLS)
- Authentification Eap-flexible par le Tunnellisation sécurisé (EAP-FAST)

L'authentification d'adresse MAC peut également percer un tunnel à un serveur d'authentification externe ou contre des gens du pays de liste à un WDS AP. Le WLSM ne prend en charge pas l'authentification d'adresse MAC.

Le WDS et l'infrastructure aps communiquent au-dessus d'un protocole de Multidiffusion appelé le Control Protocol de contexte WLAN (WLCCP). Ces messages multicasts ne peuvent pas être conduits, ainsi un WDS et l'infrastructure associée aps doivent être dans le même IP de sous-réseau et sur le même segment de RÉSEAU LOCAL. Le TCP et le Protocole UDP (User Datagram Protocol) entre le WDS et WLSE, WLCCP utilisations sur le port 2887. Quand le WDS et les WLSE sont sur des différents sous-réseaux, un protocole comme le Traduction d'adresses de réseau (NAT) ne peut pas traduire les paquets.

AP configuré comme périphérique WDS prend en charge jusqu'à 60 aps participants. Un Integrated Services Router (ISR) configuré comme périphériques WDS prend en charge jusqu'à 100 aps participants. Et un commutateur WLSM-équipé prend en charge jusqu'à 600 aps participants et jusqu'à 240 Groupes de mobilité. AP simple prend en charge jusqu'à 16 Groupes de mobilité.

Remarque: Cisco recommande que l'infrastructure aps exécutent la même version de l'IOS que le périphérique WDS. Si vous utilisez une version plus ancienne d'IOS, les aps pourraient pour authentifier au périphérique WDS. En outre, Cisco recommande que vous utilisiez la dernière version de l'IOS. Vous pouvez trouver la dernière version de l'IOS dans la page Sans fil de téléchargements.

Rôle du périphérique WDS

Le périphérique WDS effectue plusieurs tâches sur votre RÉSEAU LOCAL Sans fil :

- Annonce sa capacité WDS et participe à élire le meilleur périphérique WDS pour votre RÉSEAU LOCAL Sans fil. Quand vous configurez votre RÉSEAU LOCAL Sans fil pour le WDS, vous installez un périphérique en tant que le candidat principal WDS et un ou plusieurs périphériques supplémentaires en tant que candidats de sauvegarde WDS. Si le périphérique principal WDS va off-line, un des périphériques de la sauvegarde WDS prend son endroit.
- Authentifie tous les aps dans le sous-réseau et établit un canal de communication protégée avec chacun d'eux.
- Collecte les données par radio des aps dans le sous-réseau, agrège les données, et en avant elles au périphérique WLSE sur votre réseau.

- Agit en tant qu'intercommunication pour tous les périphériques du client 802.1x-authenticated associés aux aps participants.
- Enregistre tout le client que les périphériques dans le sous-réseau qui utilisent l'introduction dynamique, établit des clés de session pour elles, et cache leurs qualifications de Sécurité. Quand un client erre à un autre AP, le périphérique WDS en avant les qualifications de la Sécurité du client à nouvel AP.

Rôle des Points d'accès utilisant le périphérique WDS

Les aps sur votre RÉSEAU LOCAL Sans fil interagissent avec le périphérique WDS dans ces activités :

- Découvrez et dépistez les annonces de périphérique et de relais WDS du courant WDS au RÉSEAU LOCAL Sans fil.
- Authentifiez avec le périphérique WDS et établissez un canal de communication protégée au périphérique WDS.
- Enregistrez les périphériques associés de client avec le périphérique WDS.
- Données par radio d'état au périphérique WDS.

Configuration

Le WDS présente la configuration d'une mode commandée et modulaire. Constructions de chaque concept sur le concept qui précède. Le WDS omet d'autres éléments de configuration tels que des mots de passe, l'Accès à distance, et des configurations par radio pour la clarté et le foyer sur la principale matière.

Cette section présente les informations nécessaires pour configurer les caractéristiques décrites dans ce document.

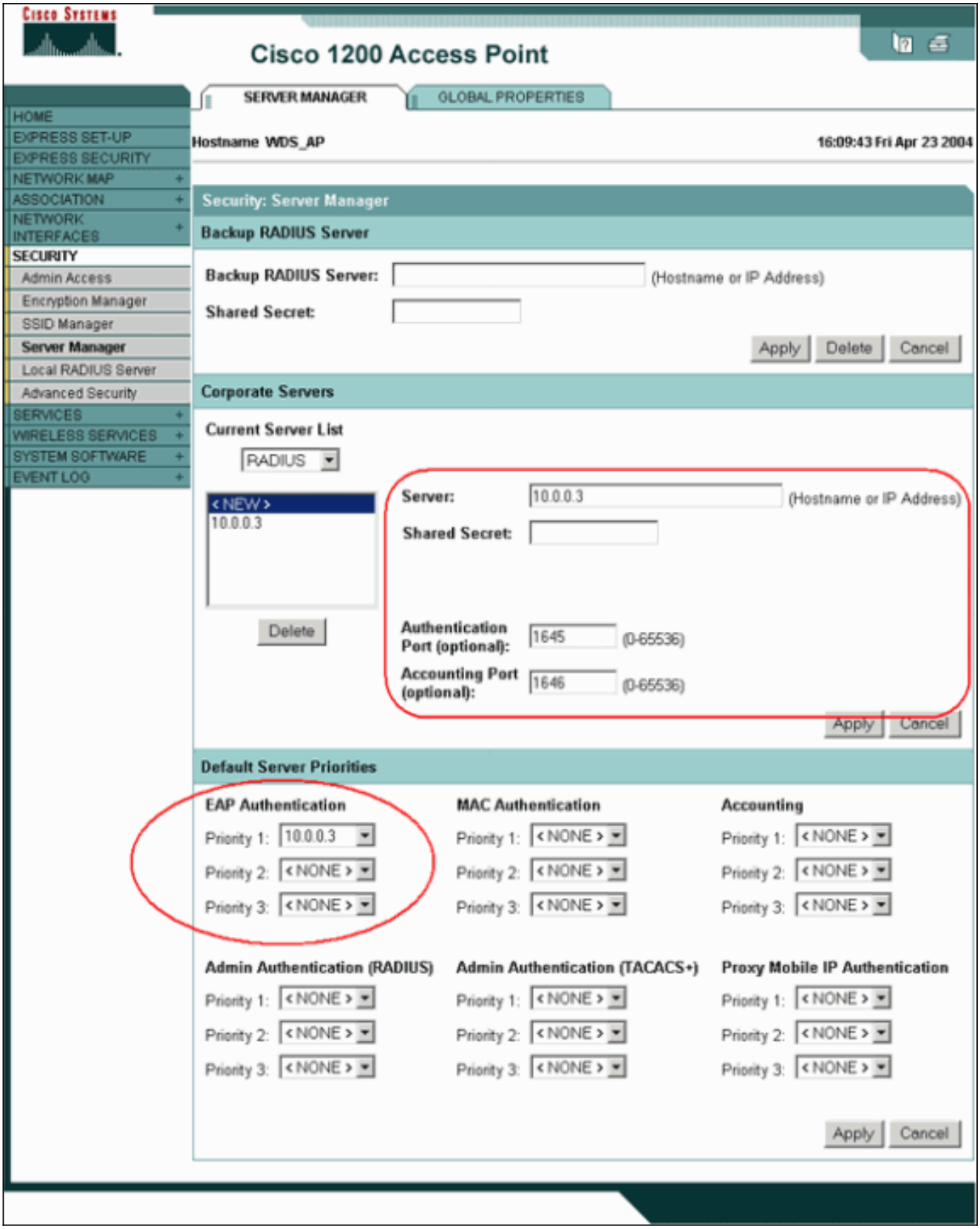
Remarque: Utilisez l'outil Command Lookup Tool (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Indiquez AP comme WDS

La première étape est d'indiquer AP comme WDS. Le WDS AP est le seul qui communique avec le serveur d'authentification.

Terminez-vous ces étapes afin d'indiquer AP comme WDS :

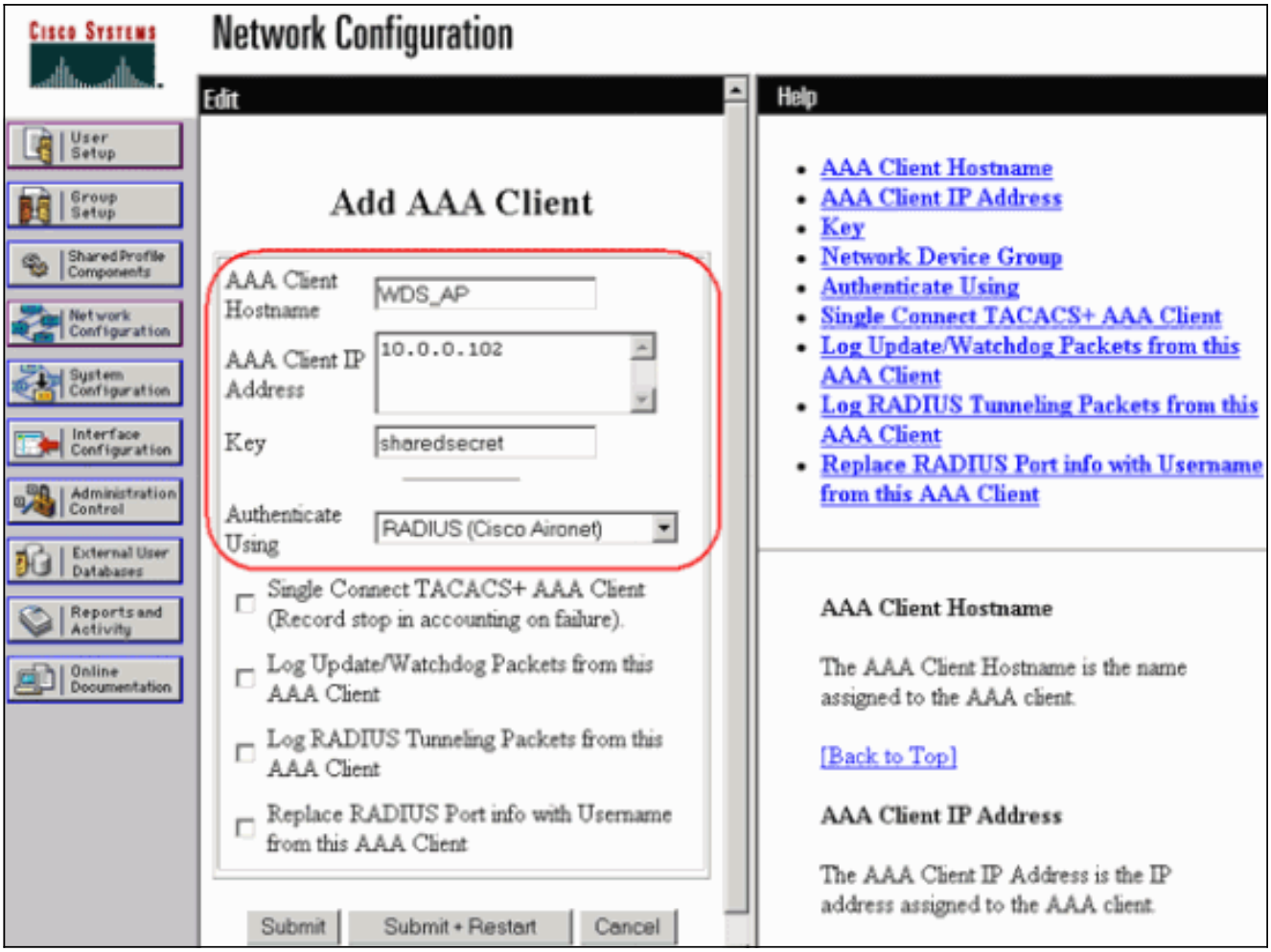
1. Afin de configurer le serveur d'authentification sur le WDS AP, choisissez le **Security > Server Manager** pour aller à l'onglet de gestionnaire du serveur :Sous les serveurs entreprise, tapez l'adresse IP du serveur d'authentification dans le champ de serveur.Spécifiez le secret partagé et les ports.Sous le Default Server Priorities, placez le champ prioritaire 1 à cette adresse IP du serveur sous le type approprié d'authentification.



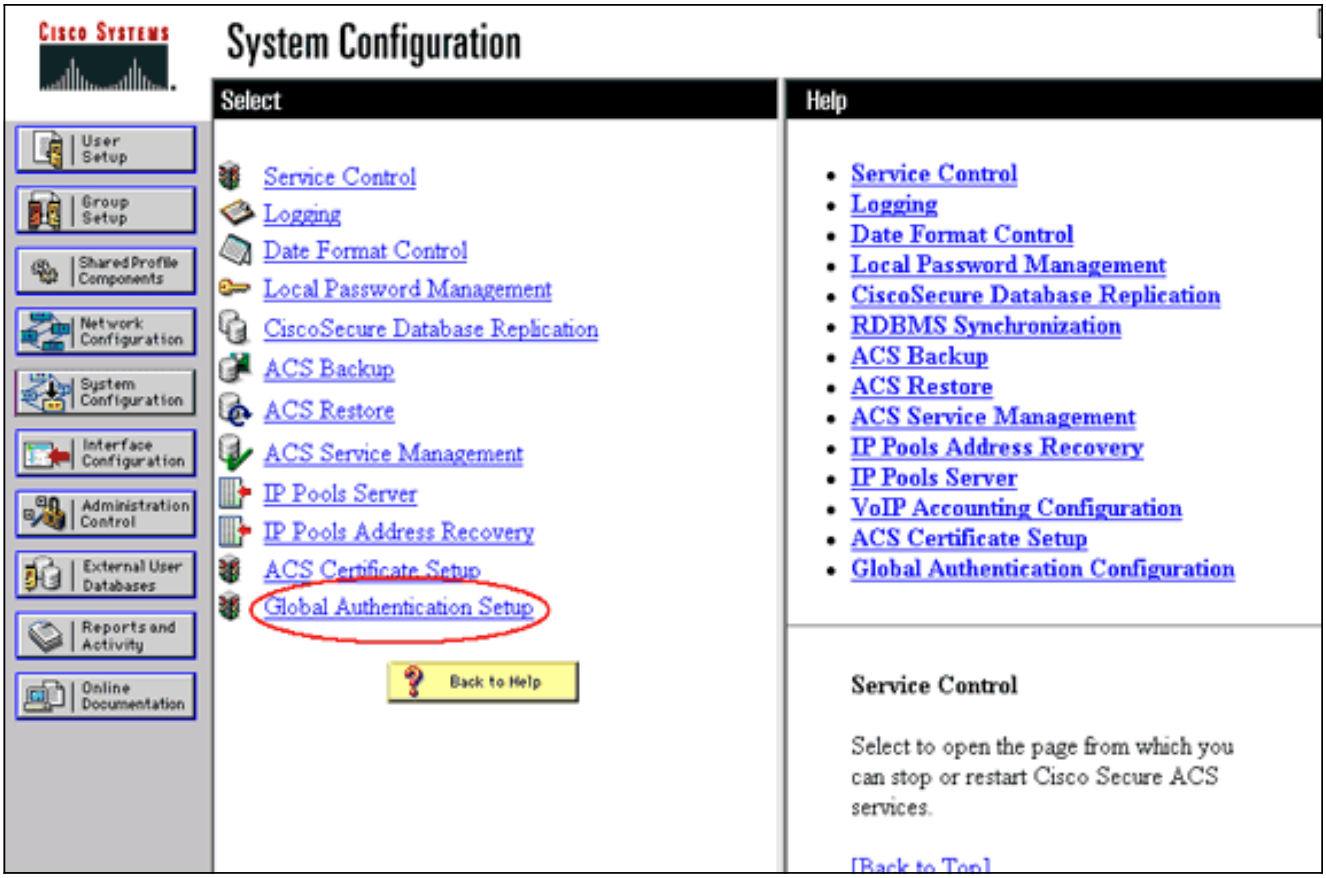
Alternativement, émettez ces commandes du CLI :

2. L'étape suivante est de configurer le WDS AP dans le serveur d'authentification en tant que client d'Authentification, autorisation et comptabilité (AAA). Pour ceci, vous devez ajouter le WDS AP en tant que client d'AAA. Procédez comme suit :**Remarque:** Ce document utilise le serveur de Cisco Secure ACS en tant que serveur d'authentification.Dans le Cisco Secure Access Control Server (ACS), ceci se produit à la page de configuration réseau où vous définissez ces attributs pour le WDS AP :NomAdresse IPSecret partagéMéthode d'authentificationRADIUS Cisco AironetInternet Engineering Task Force de RADIUS [IETF]Cliquez sur **soumettent** en fonction.Pour d'autres serveurs d'authentification de non-

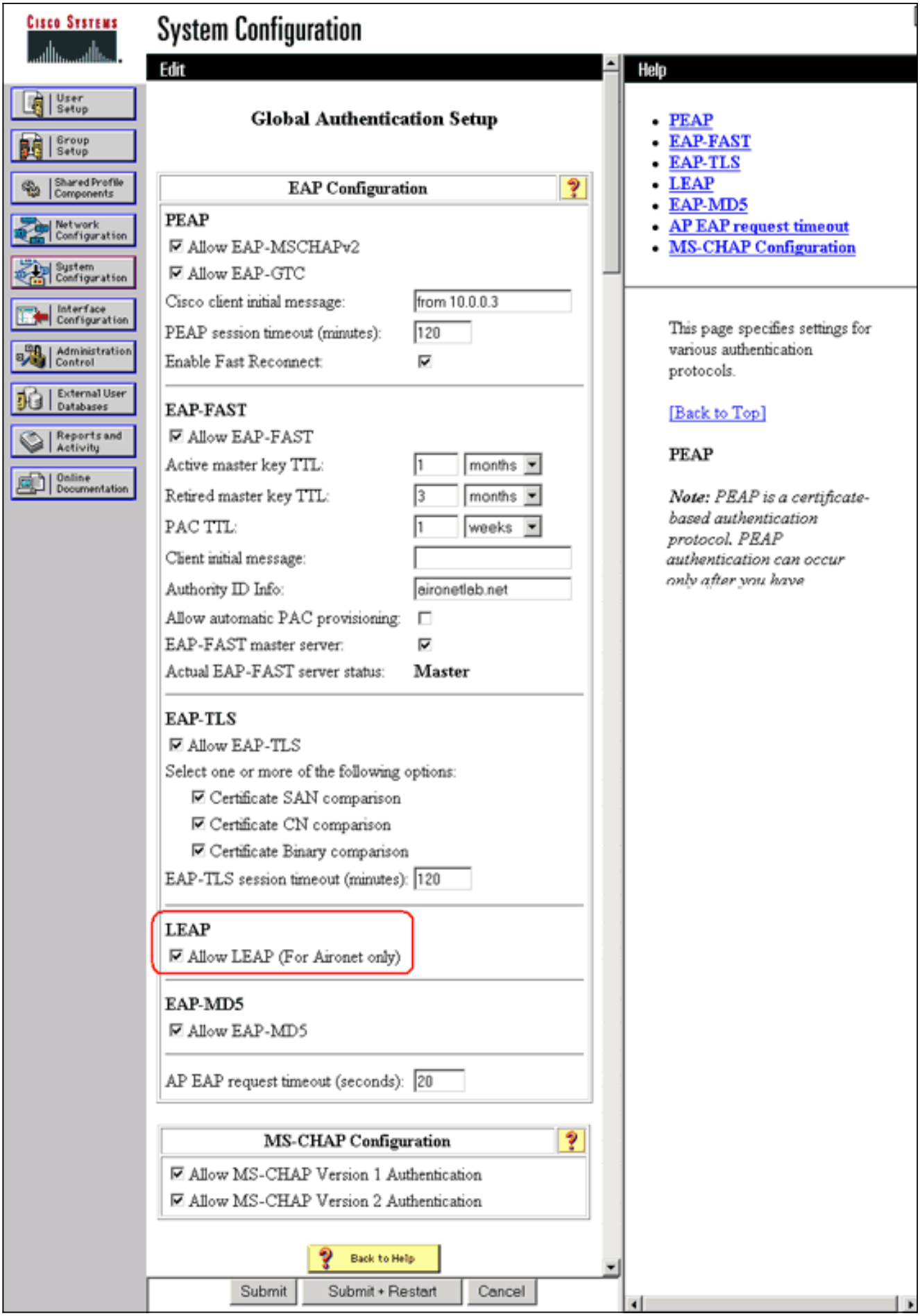
ACS, référez-vous à la documentation du fabricant.



En outre, dans le Cisco Secure ACS, assurez-vous que vous configurez ACS pour exécuter l'authentification de LEAP sur la configuration système - page globale d'installation d'authentification. D'abord, la **configuration système de** clic, cliquent sur alors l'**installation globale d'authentification**.

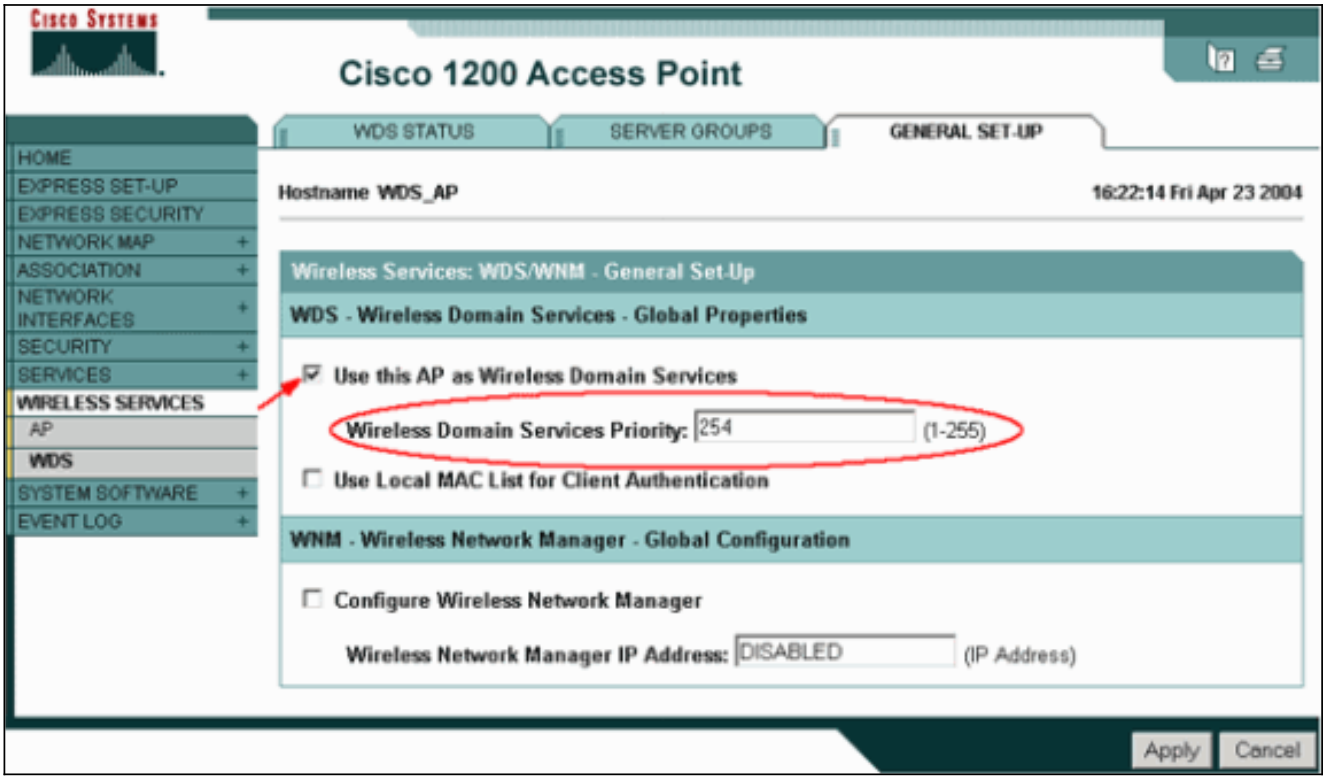


Faites descendre l'écran la page à la configuration de LEAP. Quand vous cochez la case, ACS authentifie le
LEAP.



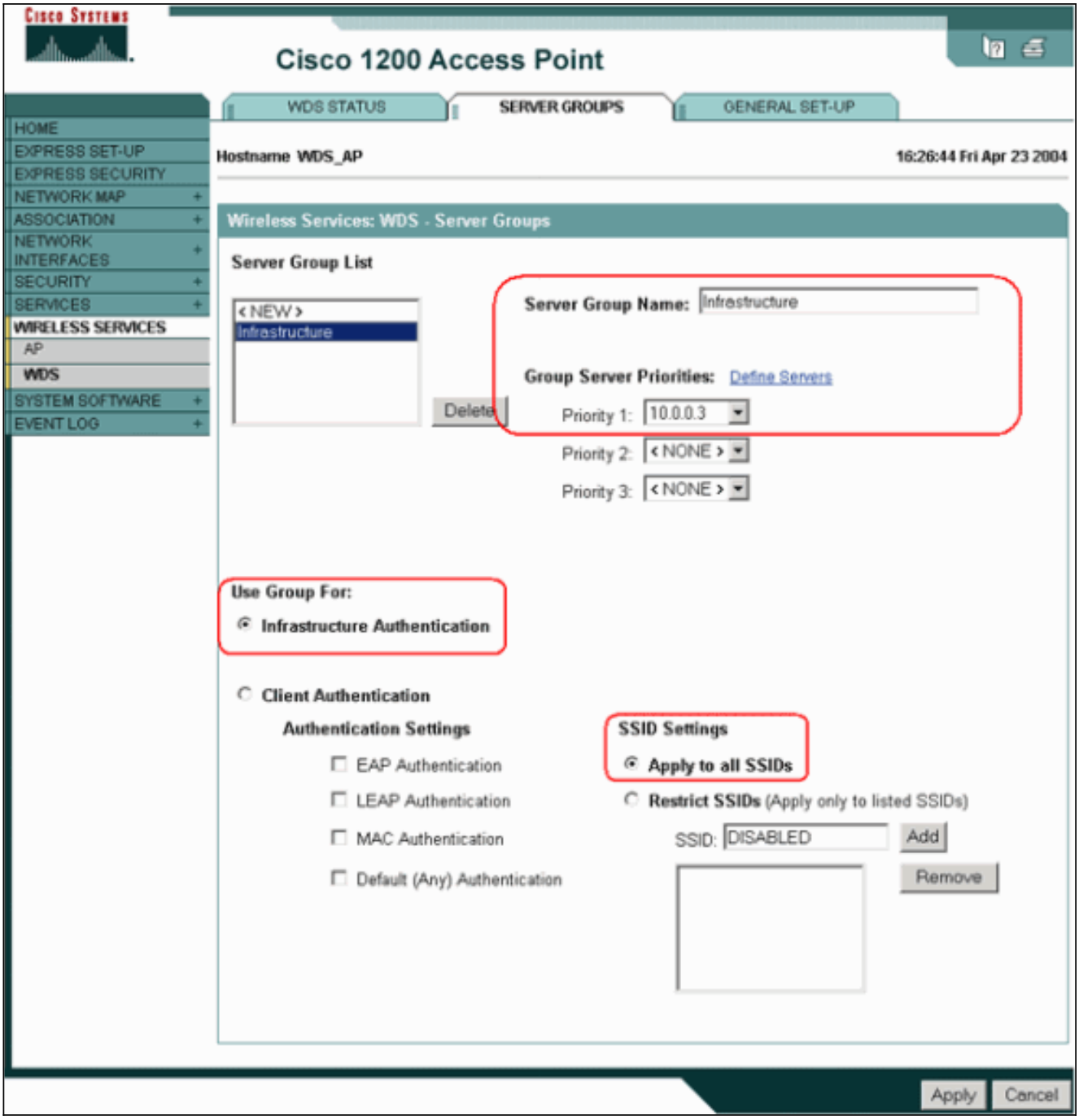
3. Afin de configurer les setttings WDS sur le WDS AP, choisir des **Services sans fil > le WDS** sur le WDS AP, et cliquer sur en fonction la **configuration générale** tableau exécutez ces étapes :Sous des services de domaine de WDS-radio - Properties global, **utilisation de**

contrôle **cet AP en tant que services de domaine Sans fil**.Placez la valeur pour le champ de priorité Sans fil de services de domaine à une valeur approximativement de **254**, parce que c'est le premier. Vous pouvez configurer un ou plusieurs aps ou Commutateurs comme candidats pour fournir le WDS. Le périphérique avec le plus prioritaire fournit le WDS.



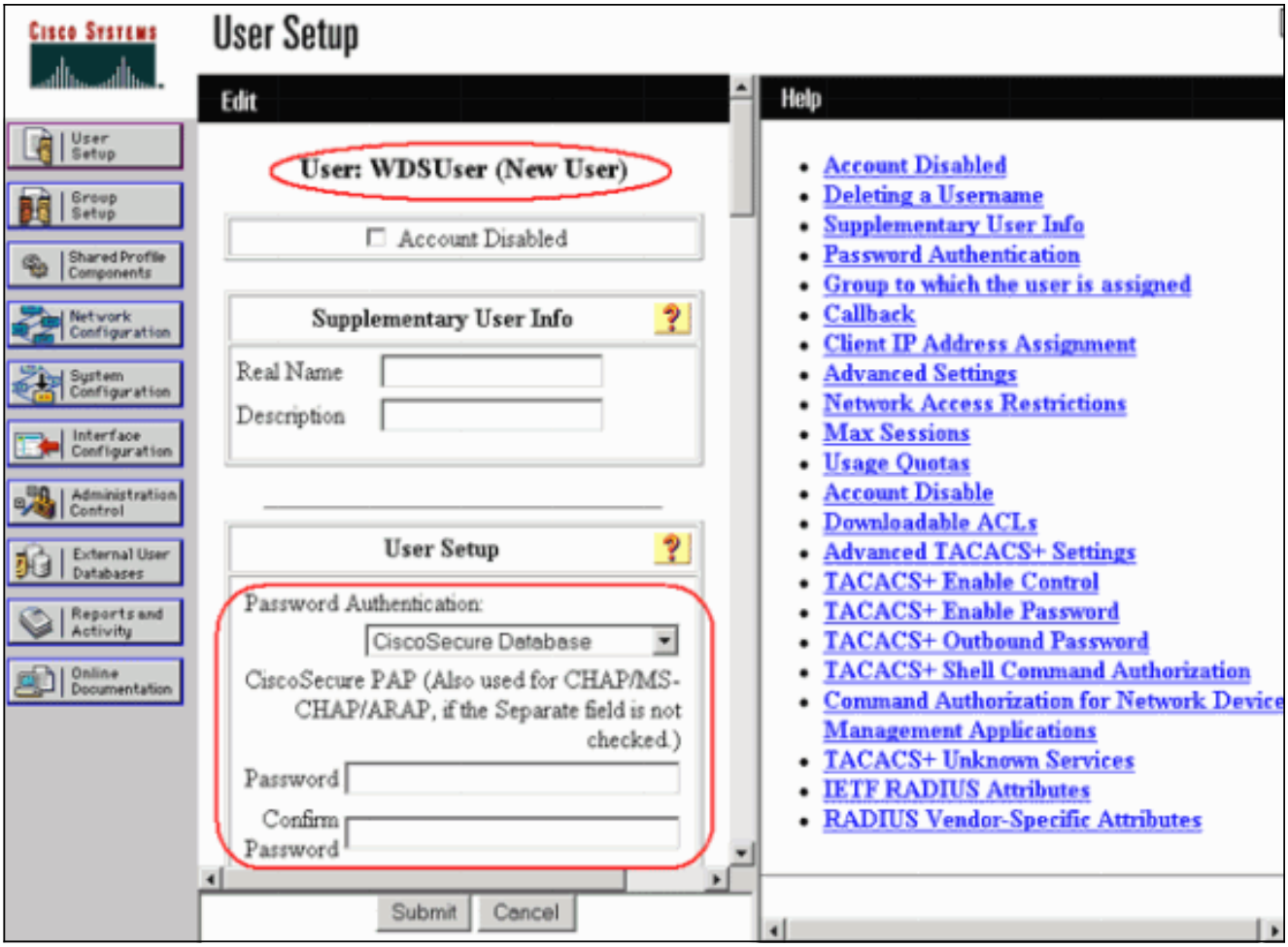
Alternativement, émettez ces commandes du CLI :

4. Choisissez les **Services sans fil > le WDS**, et allez aux **groupes de serveurs l'**onglet :Définissez un nom de groupe de serveurs qui authentifie les autres aps, un groupe d'infrastructure.Fixez la priorité 1 au serveur précédemment configuré d'authentification.Cliquez sur le **groupe d'utilisation pour :** Case d'option d'**authentification d'infrastructure**.Appliquez les configurations aux identifiants appropriés d'ensemble de services
(SSID).



Alternativement, émettez ces commandes du CLI :

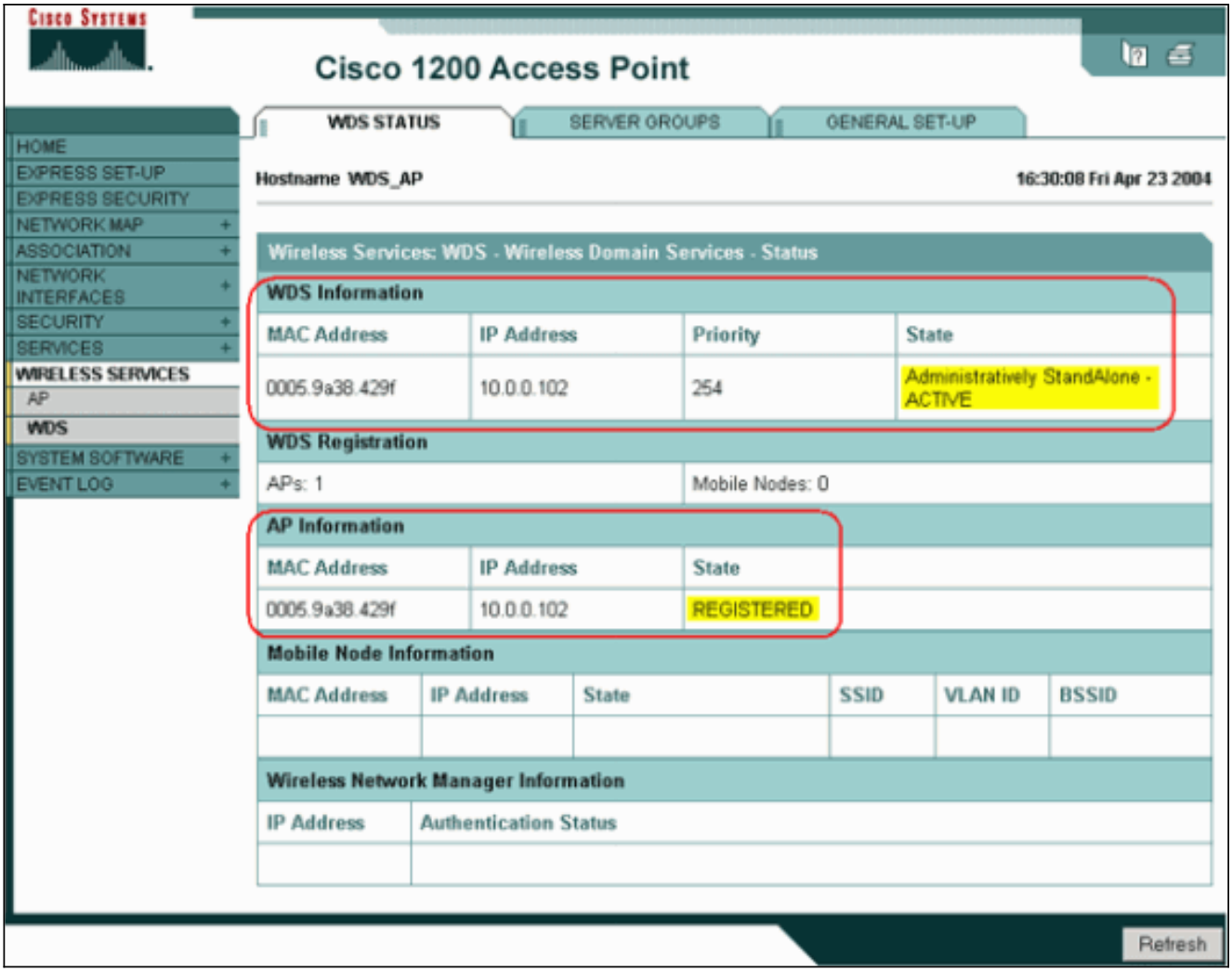
5. Configurez le nom d'utilisateur et le mot de passe WDS en tant qu'utilisateur dans votre serveur d'authentification.Dans le Cisco Secure ACS, ceci se produit à la page d'installation utilisateur, où vous définissez le nom d'utilisateur et le mot de passe WDS. Pour d'autres serveurs d'authentification de non-ACS, référez-vous à la documentation du fabricant.**Remarque:** Ne mettez pas l'utilisateur WDS dans un groupe qui est assigné beaucoup de droits et de privilèges — le WDS exige seulement l'authentification limitée.



6. Choisissez les **Services sans fil > l'AP**, et cliquez sur l'**enable** pour le participer à l'option d'infrastructure de CYGNE. Tapez alors le nom d'utilisateur et mot de passe WDS.Vous devez définir un nom d'utilisateur et le mot de passe WDS sur le serveur d'authentification pour tous les périphériques que vous indiquez des membres du WDS.

Alternativement, émettez ces commandes du CLI :

7. Choisissez les **Services sans fil > le WDS**. Sur l'onglet d'état WDS AP WDS, contrôle si le WDS AP apparaît dans la région de l'information WDS, dans l'état active. AP doit également apparaître dans la région de l'information AP, avec l'état comme ENREGISTRÉ.Si AP ne semble pas ENREGISTRÉ ou ACTIF, vérifiez le serveur d'authentification pour toutes les erreurs ou tentatives d'authentification défaillante.Quand AP s'enregistre convenablement, ajoutez une infrastructure AP pour utiliser les services du WDS.



Alternativement, émettez ces commandes du CLI :**Remarque:** Vous ne pouvez pas tester des associations de client parce que l'authentification client n'a pas des dispositions encore.

Indiquez un WLSM comme WDS

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

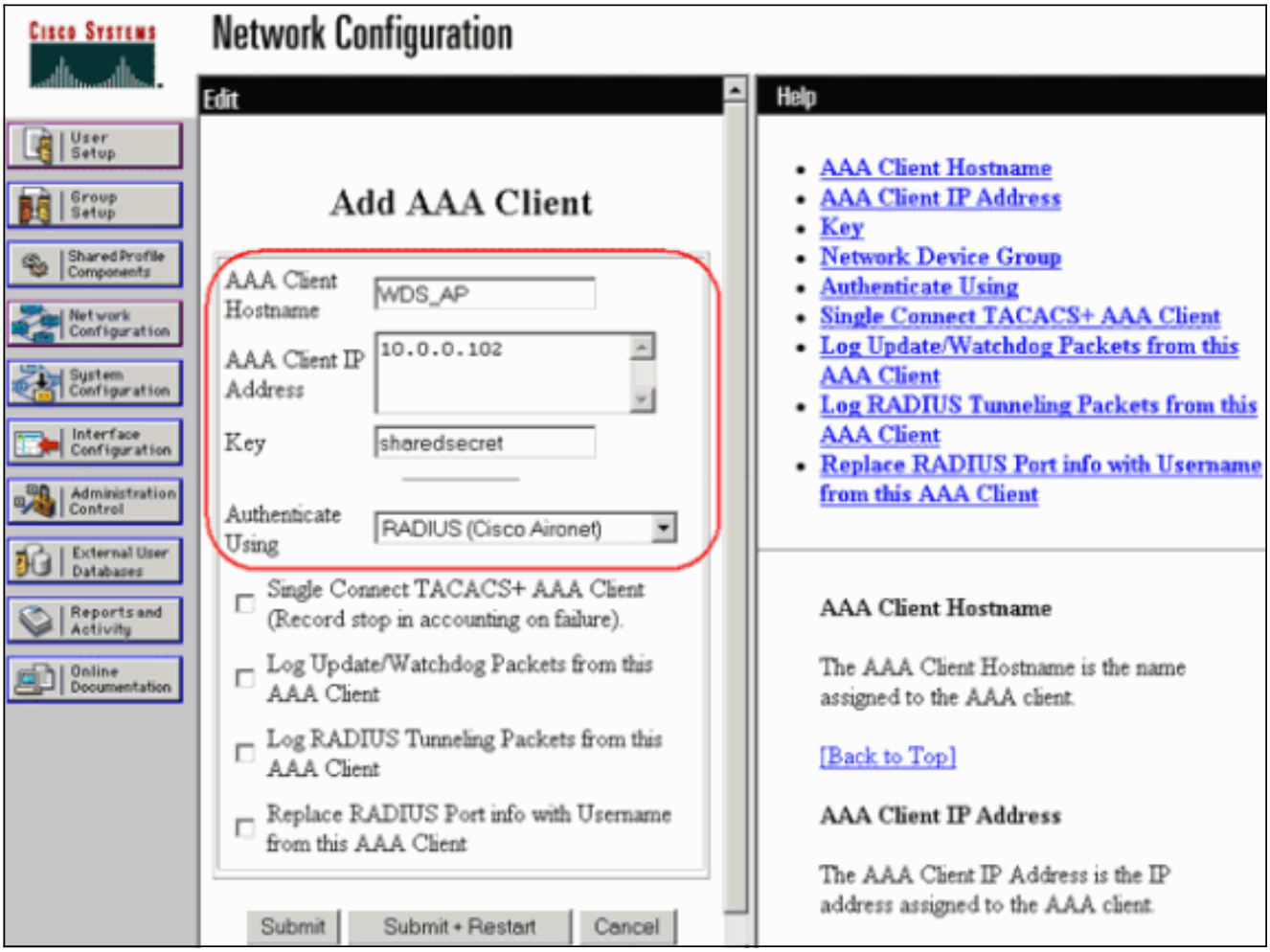
Remarque: Émettez ces commandes à l'invite de commande d'`enable du` WLSM, pas de l'engine 720 de superviseur. Afin d'obtenir à l'invite de commande du WLSM, émettez ces commandes à une invite de commande d'`enable` dans l'engine 720 de superviseur :

```
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#
```

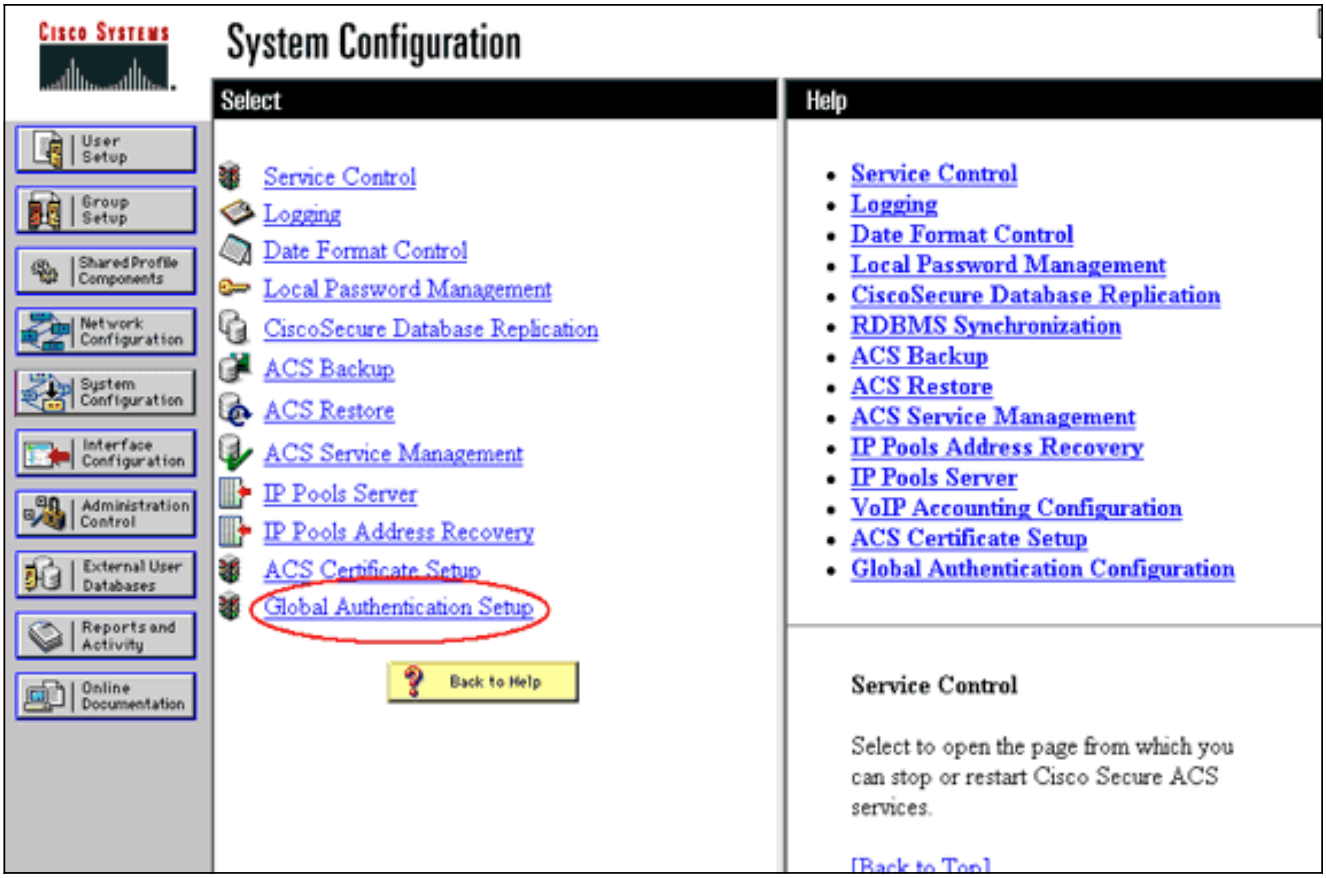
Remarque: Afin de dépanner et mettre à jour votre WLSM plus facilement, configurez l'Accès à distance de telnet au WLSM. Référez-vous à configurer l'Accès à distance de telnet.

Afin d'indiquer un WLSM comme WDS :

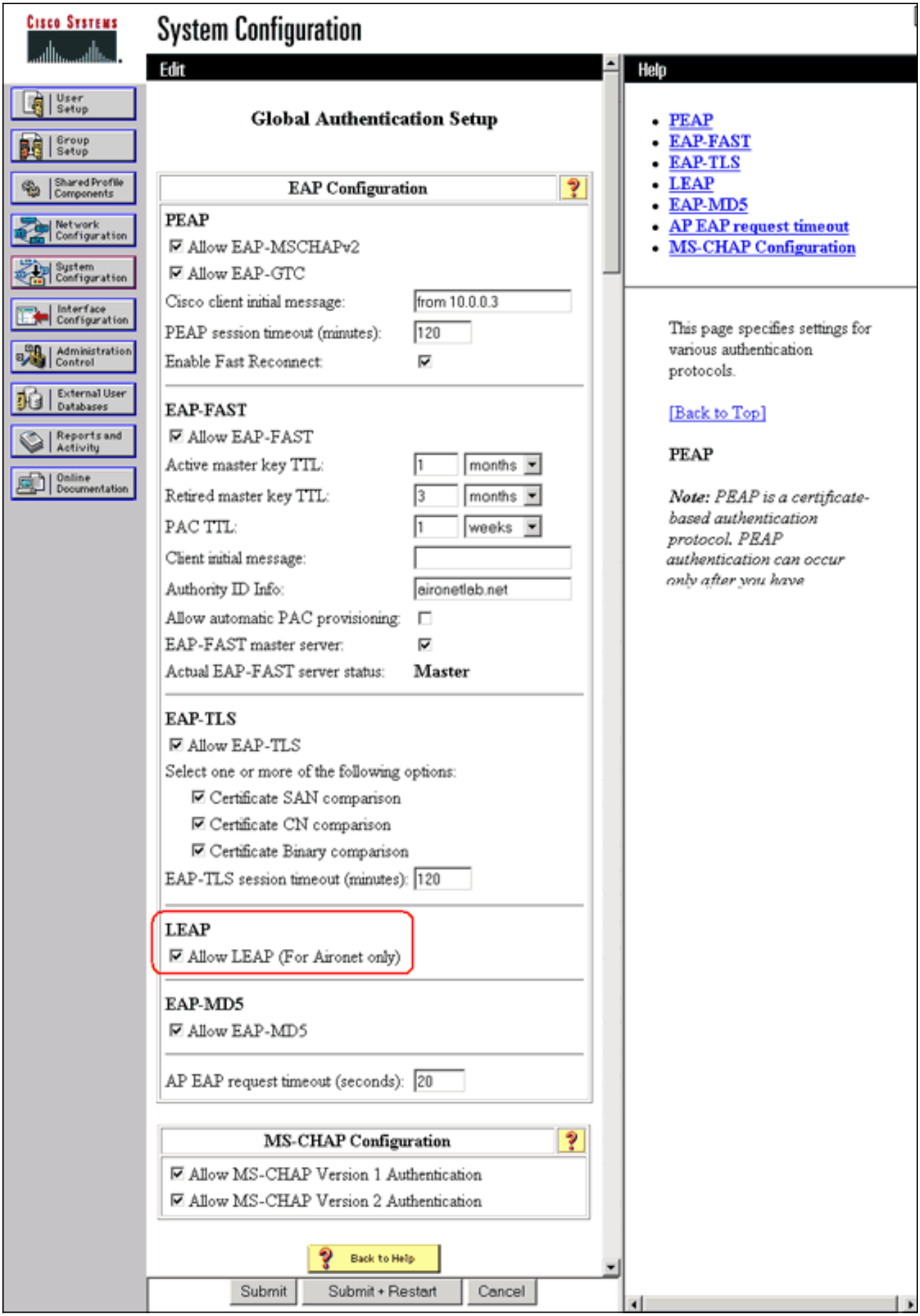
1. Du CLI du WLSM, émettez ces commandes, et établissez des relations avec le serveur d'authentification :**Remarque:** Il n'y a aucun contrôle prioritaire dans le WLSM. Si le réseau contient de plusieurs modules WLSM, WLSM emploie la configuration de Redondance afin de déterminer le module primaire.
2. Configurez le WLSM dans le serveur d'authentification en tant que client d'AAA.Dans le Cisco Secure ACS, ceci se produit à la page de configuration réseau où vous définissez ces attributs pour le WLSM :NomAdresse IPSecret partagéMéthode d'authentificationRADIUS Cisco AironetIETF DE RADIUSPour d'autres serveurs d'authentification de non-ACS, référez-vous à la documentation du fabricant.



En outre, dans le Cisco Secure ACS, configurez ACS pour exécuter l'authentification de LEAP sur la configuration système - page globale d'installation d'authentification. D'abord, la **configuration système de** clic, cliquent sur alors l'**installation globale d'authentification**.



Faites descendre l'écran la page à la configuration de LEAP. Quand vous cochez la case, ACS authentifie le
LEAP.



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

de client-serveur) et le quel EAP tape l'utilisation de ces clients.**Remarque:** Cette étape élimine le besoin de procédé de méthode d'authentification client de définir.

5. Définissez un seul VLAN entre l'engine 720 et le WLSM de superviseur afin de permettre au WLSM pour communiquer avec les entités extérieures comme des aps et des serveurs d'authentification. Ce VLAN est inutilisé n'importe où ailleurs ou pour n'importe quel autre but sur le réseau. Créez le VLAN sur l'engine 720 de superviseur d'abord, puis émettez ces commandes :Sur le Supervisor Engine 720 :Sur le WLSM :
6. Vérifiez la fonction du WLSM avec ces commandes :Sur le WLSM :Sur le Supervisor Engine 720 :

Indiquez AP comme périphérique d'infrastructure

Ensuite, vous devez indiquer au moins une infrastructure AP et associer AP au WDS. L'associé de clients à l'infrastructure aps. L'infrastructure aps invitent le WDS AP ou WLSM à exécuter l'authentification pour eux.

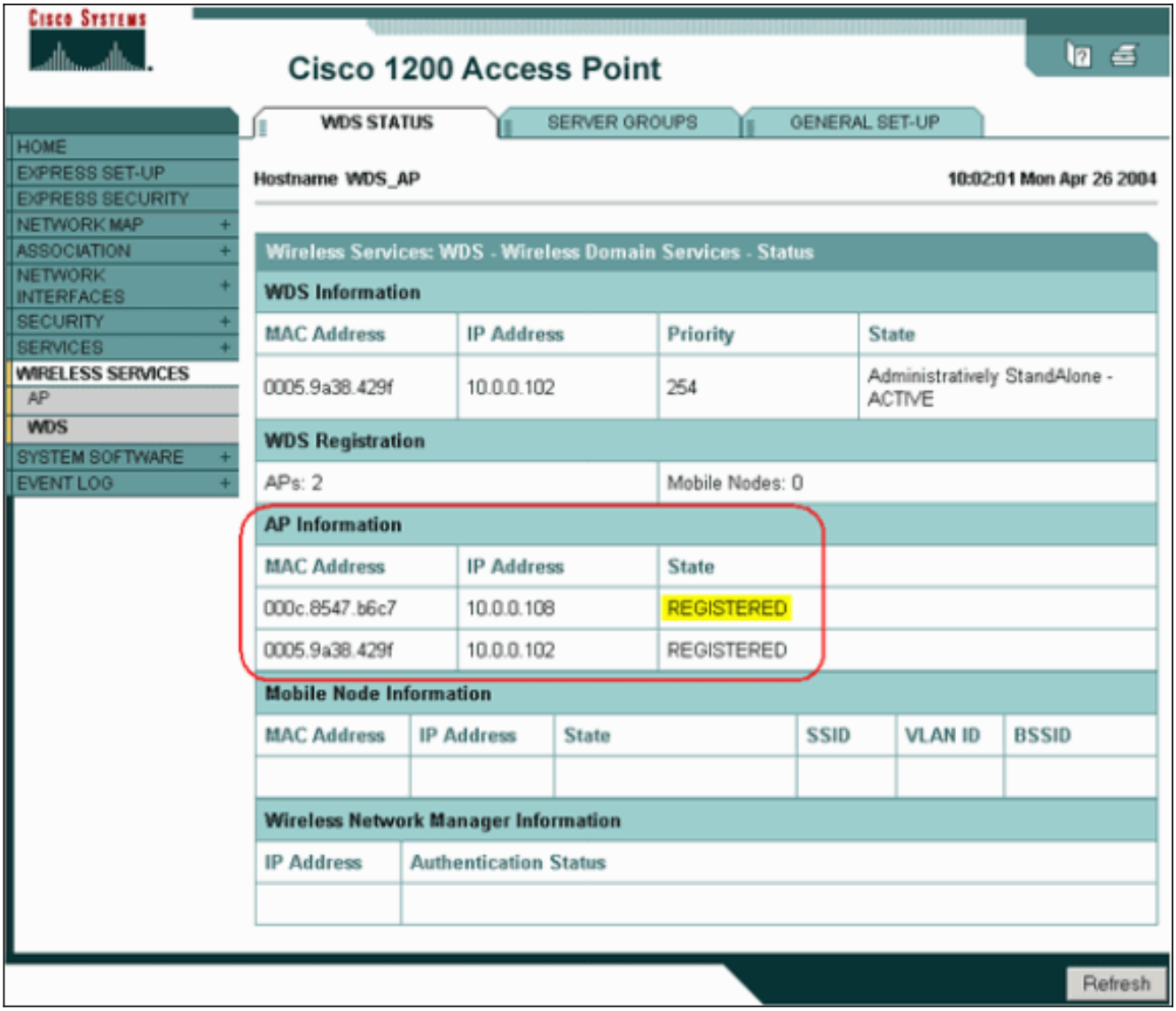
Terminez-vous ces étapes afin d'ajouter une infrastructure AP qui utilise les services du WDS :

Remarque: Cette configuration s'applique seulement à l'infrastructure aps et pas le WDS AP.

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

Alternativement, émettez ces commandes du CLI :

2. Choisissez les **Services sans fil > le WDS**. Sur l'onglet d'état WDS AP WDS, la nouvelle infrastructure AP apparaît dans la région de l'information WDS, avec l'état aussi ACTIF, et dans la région de l'information AP, avec l'état qu'ENREGISTRÉE.Si AP ne semble pas ACTIF et/ou ENREGISTRÉ, vérifiez le serveur d'authentification pour toutes les erreurs ou tentatives d'authentification défaillante.Après qu'AP semble ACTIF et/ou ENREGISTRÉ, ajoutez une méthode d'authentification client au WDS.



Alternativement, émettez cette commande du CLI :Alternativement, émettez cette commande du WLSM :Puis, émettez cette commande sur l'infrastructure AP :**Remarque:** Vous ne pouvez pas tester des associations de client parce que l'authentification client n'a pas des dispositions encore.

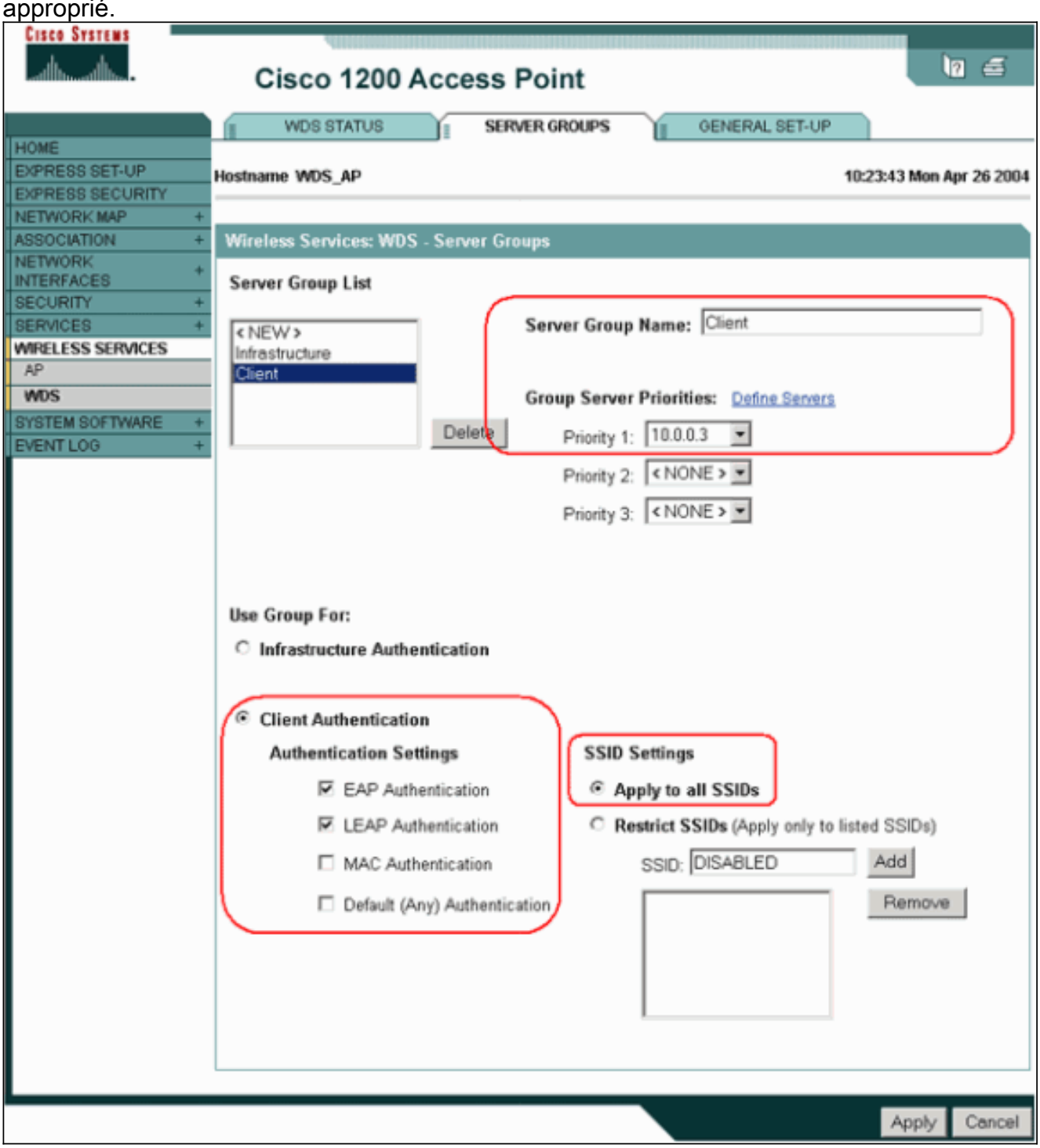
Définissez la méthode d'authentification client

En conclusion, définissez une méthode d'authentification client.

Terminez-vous ces étapes afin d'ajouter une méthode d'authentification client :

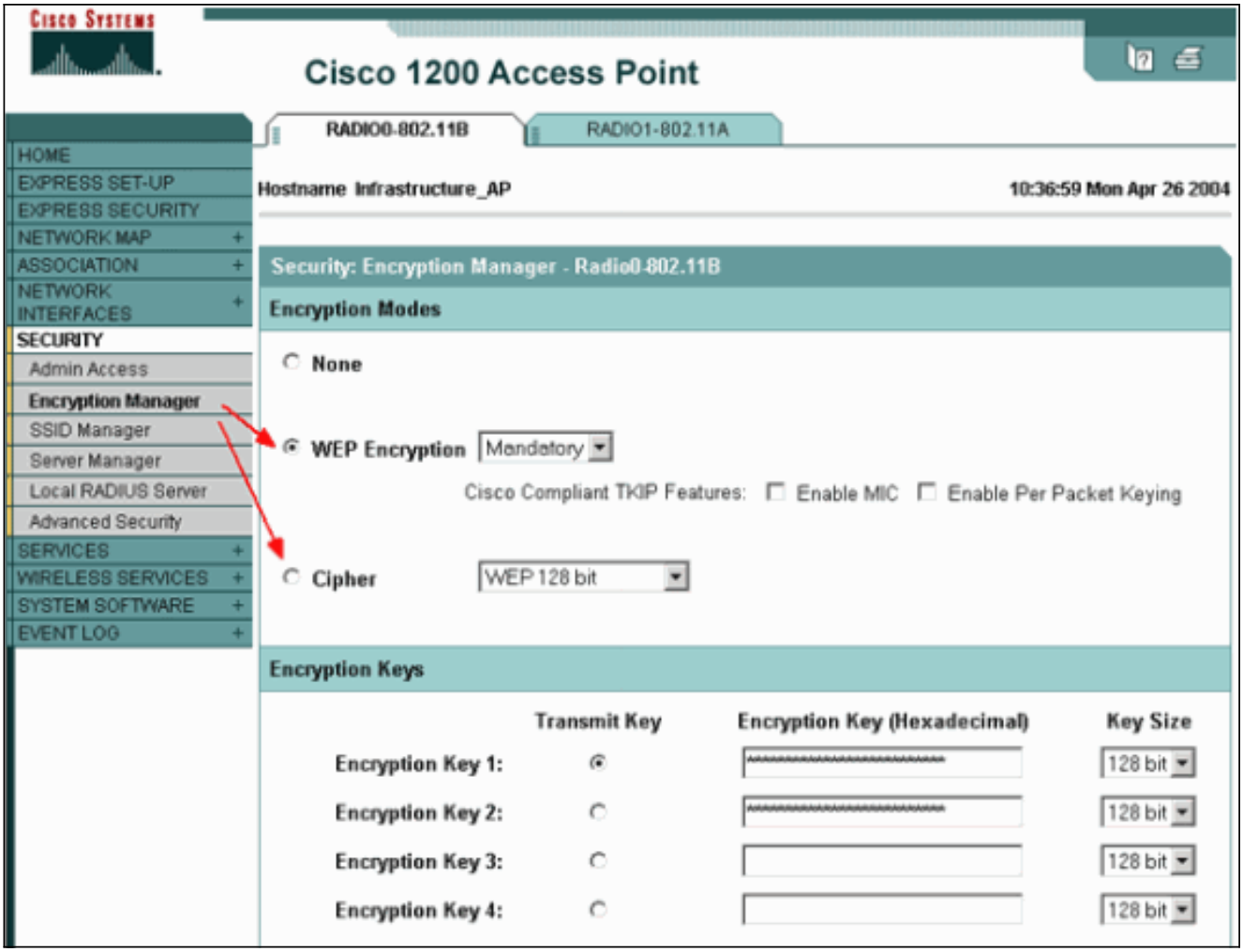
1. Choisissez les **Services sans fil > le WDS**. Exécutez ces étapes sur l'onglet de groupes de serveurs WDS AP :Définissez un groupe de serveurs qui authentifie des clients (un groupe

de clients).Fixez la priorité 1 au serveur précédemment configuré d'authentification.Placez le type applicable d'authentification (LEAP, EAP, MAC, et ainsi de suite).Appliquez les configurations au SSID
approprié.

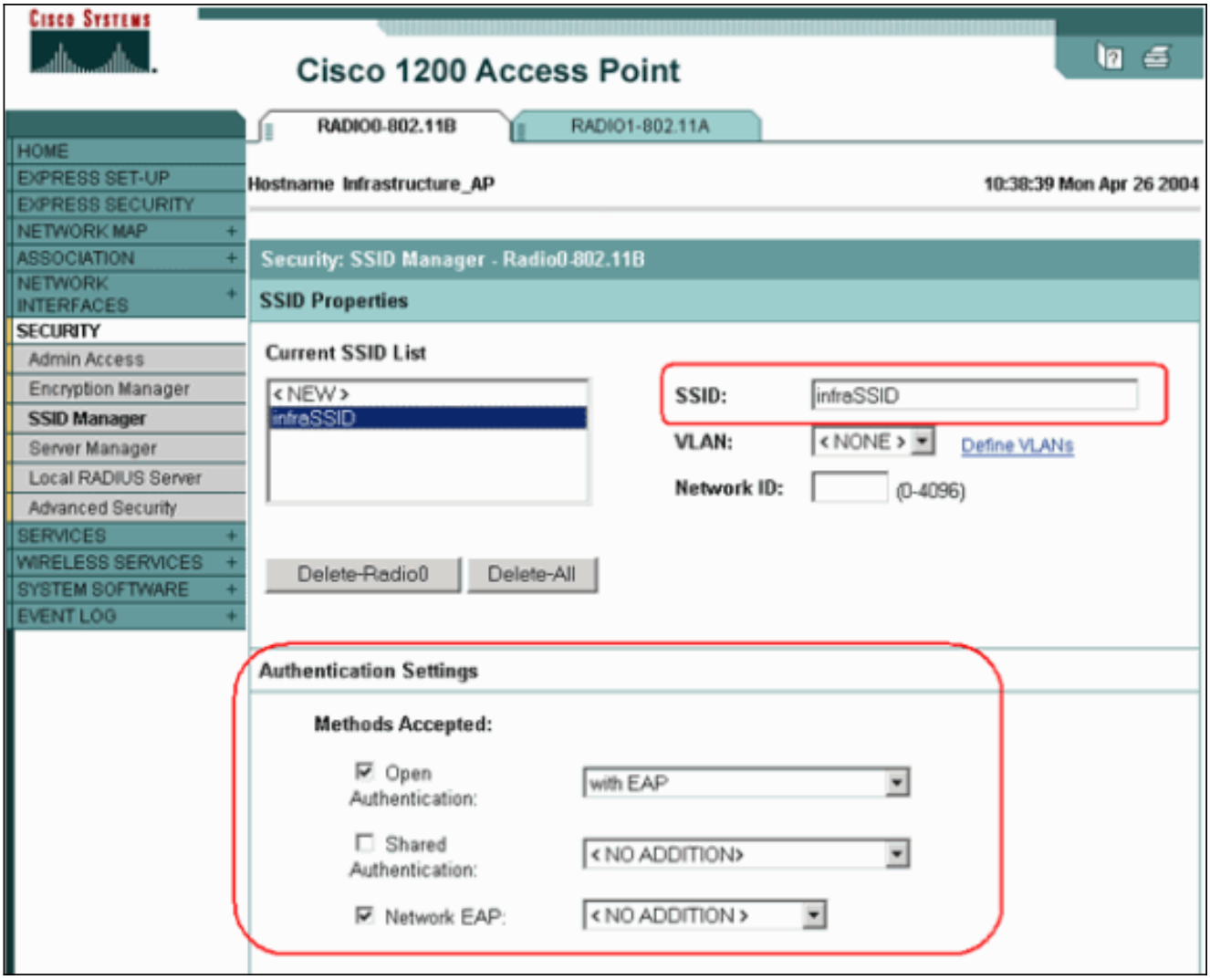


Alternativement, émettez ces commandes du CLI :**Remarque:** L'exemple WDS AP est dédié et ne reçoit pas des associations de client.**Remarque:** Ne configurez pas sur l'infrastructure aps pour des groupes de serveurs parce que l'infrastructure aps font suivre à toutes les demandes le WDS d'être traité.

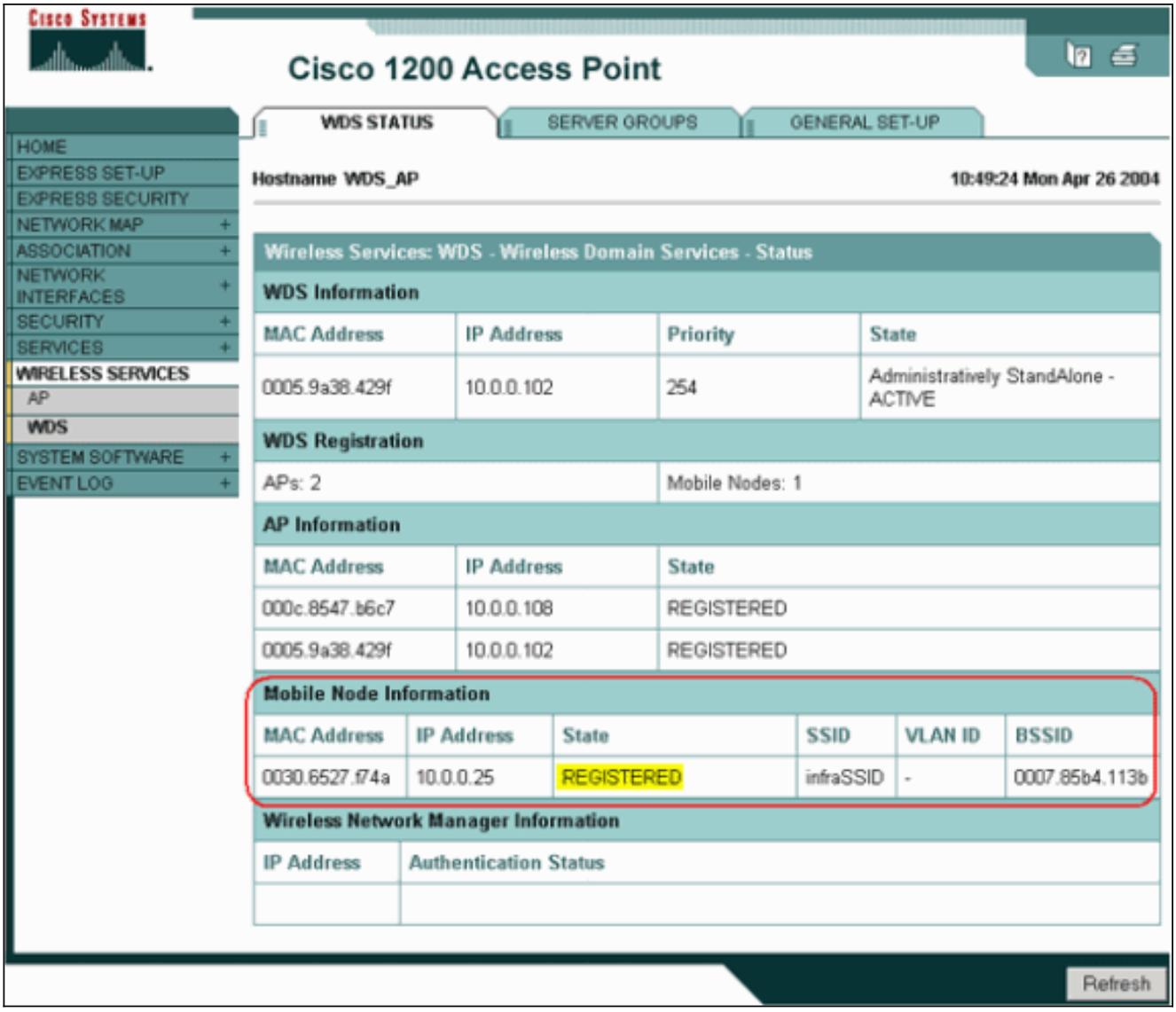
2. Sur l'infrastructure AP ou aps :Sous la commande de menu de **Security > Encryption Manager**, le **cryptage WEP** ou le **chiffrement de** clic, selon les exigences du protocole d'authentification vous
utilisez.



Àla commande de menu de **Security > SSID Manager**, méthodes d'authentification choisies selon les exigences du protocole d'authentification que vous utilisez.



3. Vous pouvez maintenant avec succès tester si les clients authentifient à l'infrastructure aps. AP du WDS dans l'onglet d'état WDS (aux **Services sans fil > à la** commande de menu **WDS**) indique que le client apparaît dans la région mobile de l'information de noeud et a un état ENREGISTRÉ.Si le client n'apparaît pas, vérifiez le serveur d'authentification pour toutes les erreurs ou tentatives d'authentification défaillante par les clients.



Alternativement, émettez ces commandes du CLI :**Remarque:** Si vous avez besoin de debug authentication, assurez-vous que vous mettez au point sur le WDS AP, parce que le WDS AP est le périphérique qui communique avec le serveur d'authentification.

Vérifier

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

Dépanner

Cette section présente les informations que vous pouvez utiliser pour dépanner votre configuration. Cette liste affiche certaines des questions communes liées à la commande WDS afin de clarifier plus loin l'utilité de ces commandes :

- **Question : Sur le WDS AP, quelles sont les configurations recommandées pour ces éléments ?radius-server timeoutradius-server deadtimeTemps de Holdoff de panne du contrôle d'intégrité des messages de Protocole TKIP (Temporal Key Integrity Protocol) (MIC)Temps de Holdoff de clientIntervalle de réauthentification d'EAP ou de MACDélai d'attente de client d'EAP (facultatif)Réponse :** On lui suggère que vous gardiez la configuration avec des valeurs par défaut concernant ces configurations spéciales, et les utilise seulement quand il y a un

problème concernant la synchronisation.Ce sont les configurations recommandées pour le WDS AP :**Radius-server timeout de** débronchement. C'est le nombre de secondes des attentes AP une réponse à une demande RADIUS avant qu'il renvoie la demande. Le par défaut est de 5 secondes.**Radius-server deadtime de** débronchement. RADIUS est ignoré par des demandes supplémentaires de la durée des minutes à moins que tous les serveurs soient marqués complètement.Le temps de Holdoff de panne TKIP MIC est activé par défaut à 60 secondes. Si vous activez le temps de holdoff, vous pouvez écrire l'intervalle en quelques secondes. Si AP détecte deux pannes MIC dans 60 secondes, il bloque tous les clients TKIP sur cette interface pour le délai prévu de holdoff spécifié ici.Le temps de Holdoff de client devrait être désactivé par défaut. Si vous activez le holdoff, écrivez le nombre de secondes qu'AP devrait attendre après qu'un échec d'authentification avant une demande d'authentification ultérieure soit traité.L'intervalle de réauthentification d'EAP ou de MAC est désactivé par défaut. Si vous activez la réauthentification, vous pouvez spécifier l'intervalle ou recevoir l'intervalle donné par le serveur d'authentification. Si vous choisissez de spécifier l'intervalle, écrivez l'intervalle en quelques secondes qu'AP attend avant qu'il force un client authentifié à authentifier à nouveau.Le délai d'attente de client d'EAP (facultatif) est de 120 secondes par défaut. Écrivez la durée qu'AP devrait attendre des clients sans fil pour répondre aux demandes d'authentification EAP.

- **Question : En vue de le temps de holdoff TKIP, j'ai lu que ceci devrait être placé à 100 ms et à non 60 secondes. Je suppose qu'il est placé à une seconde du navigateur parce que c'est le nombre le plus peu élevé que vous pouvez choisi ?Réponse :** Il n'y a aucune recommandation spécifique de la placer à 100 ms à moins qu'il y ait une panne signalée où la seule solution est d'augmenter cette fois. Une seconde est la plus basse configuration.
- **Question : Ces deux commandes aident-elles l'authentification client de quelque façon et sont-elles nécessaires sur le WDS ou l'infrastructure AP ?sur-pour-procédure de connexion-auth de radius-server attribute 6support-multiple de radius-server attribute 6Réponse :** Ces commandes n'aident pas la procédure d'authentification et elles ne sont pas nécessaires sur le WDS ou l'AP.
- **Question : Sur l'infrastructure AP, je suppose que rien le gestionnaire du serveur et les configurations globales de Properties sont nécessaires parce qu'AP reçoit les informations du WDS. L'un de ces commandes de particularité sont-elles nécessaires pour l'infrastructure AP ?sur-pour-procédure de connexion-auth de radius-server attribute 6support-multiple de radius-server attribute 6radius-server timeoutradius-server deadtimeRéponse :** Il n'y a aucun besoin d'avoir le gestionnaire du serveur et le Properties global pour l'infrastructure aps. Le WDS prend soin de cette tâche et il n'y a aucun besoin d'avoir ces configurations :**sur-pour-procédure de connexion-auth de radius-server attribute 6support-multiple de radius-server attribute 6radius-server timeoutradius-server deadtime**La configuration du **format %h de radius-server attribute 32 include-in-access-req** demeure à côté de par défaut et est exigée.

AP est un périphérique de la couche 2. Par conséquent, AP ne prend en charge pas la mobilité de la couche 3 quand AP est configuré pour agir en tant que périphérique WDS. Vous pouvez réaliser la mobilité de la couche 3 seulement quand vous configurez le WLSM comme périphérique WDS. Référez-vous à la section d'*architecture de mobilité de la couche 3 du* Module de services Sans fil réseau local de gamme Cisco Catalyst 6500 : Pour en savoir plus de Livre Blanc.

Par conséquent, quand vous configurez AP comme périphérique WDS, n'utilisez pas la commande de **mobility network-id**. Cette commande s'applique pour poser 3 mobilité et vous devez avoir un WLSM pendant que votre périphérique WDS afin de configurer correctement la mobilité de la couche 3. Si vous utilisez la commande de **mobility network-id** inexactement, vous

pouvez voir certains de ces symptômes :

- Les clients sans fil ne peuvent pas s'associer à l'AP.
- Les clients sans fil peuvent s'associer à AP, mais ne reçoivent pas une adresse IP du serveur DHCP.
- Un téléphone Sans fil n'est pas authentifié quand vous avez une Voix au-dessus de déploiement WLAN.
- L'authentification EAP ne se produit pas. **Le mobility network-id** étant configuré, les essais AP pour construire un tunnel d'Encapsulation de routage générique (GRE) pour expédier des paquets d'EAP. Si aucun tunnel n'est établi, les paquets ne vont pas n'importe où.
- AP configuré comme périphérique WDS ne fonctionne pas comme prévu, et la configuration WDS ne fonctionne pas.**Remarque:** Vous ne pouvez pas configurer Cisco Aironet 1300 AP/Bridge comme maître WDS. Les 1300 AP/Bridge ne prennent en charge pas cette fonctionnalité. Les 1300 AP/Bridge peuvent participer à un réseau WDS pendant qu'un périphérique d'infrastructure en lequel quelque autre AP 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: Référez-vous aux informations importantes sur les commandes de débogage avant d'utiliser les commandes de **débogage**.

- **l'authentificateur de debug dot11 aaa** prouve **entièrement aux** diverses négociations qu'un client intervient pendant que le client s'associe et authentifie par le 802.1x ou le processus d'EAP. Ce débogage a été introduit dans le logiciel Cisco IOS Version 12.2(15)JA. Ce **dot1x tout de debug dot11 aaa d'**obsoletes de commande dans cela et des versions ultérieures.
- **debug aaa authentication** — Affiche la procédure d'authentification d'un point de vue générique d'AAA.
- **debug wlccp ap** — Affiche que les négociations WLCCP impliquées comme AP joint un WDS.
- **debug wlccp packet** — Affiche les informations détaillées au sujet des négociations WLCCP.
- **mettez au point le LEAP-client de wlccp** — Affiche les détails pendant qu'un périphérique d'infrastructure joint un WDS.

Informations connexes

- En configurant le WDS, jeûnez itinérance sécurisée, et Gestion de radio
- Note de configuration Sans fil en Module de services réseau local de gamme Catalyst 6500
- Configuration des suites de chiffre et de WEP
- Configuration des types d'authentification
- Page de support technique sur LAN sans fil
- Support et documentation techniques - Cisco Systems