Exemple de configuration d'un point d'accès des services de domaine sans fil en tant que serveur AAA

Contenu

Introduction

Ce document fournit une configuration d'échantillon pour configurer un Point d'accès (AP) à :

- Fournissez le Fonctions Wireless Domain Services (WDS).
- Exécutez le rôle d'un serveur d'Authentification, autorisation et comptabilité (AAA).

Vous pouvez utiliser ce genre d'installation quand vous n'avez pas un serveur RADIUS externe pour authentifier l'infrastructure aps et les périphériques de client qui participent au WDS.

Conditions préalables

Conditions requises

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

- Connaissance de base de WDS
- 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 :

- Gamme Cisco Aironet 1200 aps qui exécutent la version de logiciel 12.3(7)JA1 de Cisco IOS®

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.

Informations générales

Le WDS est une partie du réseau sans fil structuré par Cisco (CYGNE). Le WDS est une collection de Fonctions du logiciel Cisco IOS qui améliorent la mobilité Sans fil de client du RÉSEAU LOCAL (WLAN) et simplifient le déploiement et la Gestion WLAN.

Le WDS est la base pour beaucoup de caractéristiques telles que l'itinérance sécurisée rapide, pose la mobilité 3, et la Gestion de radio.

Référez-vous à configurer le WDS, l'itinérance sécurisée rapide, la Gestion par radio, et les services Sans fil de détection d'intrusion pour plus d'informations sur ces caractéristiques.

Un des buts principaux du WDS est de cacher les identifiants utilisateurs à la première authentification du client par le serveur d'authentification. Sur des essais ultérieurs, le WDS authentifie le client sur la base des informations en cache. Afin d'accomplir ceci :

- Un des aps doit être configuré comme WDS AP.
- D'autres aps doivent être configurés comme infrastructure aps qui communiquent au WDS AP.
- WDS AP doit établir des relations avec le serveur d'authentification en authentifiant à lui avec un nom d'utilisateur et mot de passe WDS.

Ce serveur d'authentification valide les qualifications de l'infrastructure aps et les clients quand ces périphériques authentifient pour la première fois. Le serveur d'authentification peut être un serveur RADIUS externe ou le serveur local de RADIUS sur le WDS AP.

Le WDS et l'infrastructure aps communiquent au-dessus d'un protocole de Multidiffusion appelé le Control Protocol Sans fil de contexte de RÉSEAU LOCAL (WLCCP). Ces messages multicasts ne peuvent pas être conduits. Par conséquent, un WDS et une infrastructure associée aps doivent être dans le même sous-réseau IP et sur le même segment de RÉSEAU LOCAL.

Ce document explique comment employer la caractéristique locale de serveur de RADIUS sur le WDS AP pour exécuter la validation des qualifications.

Configurer

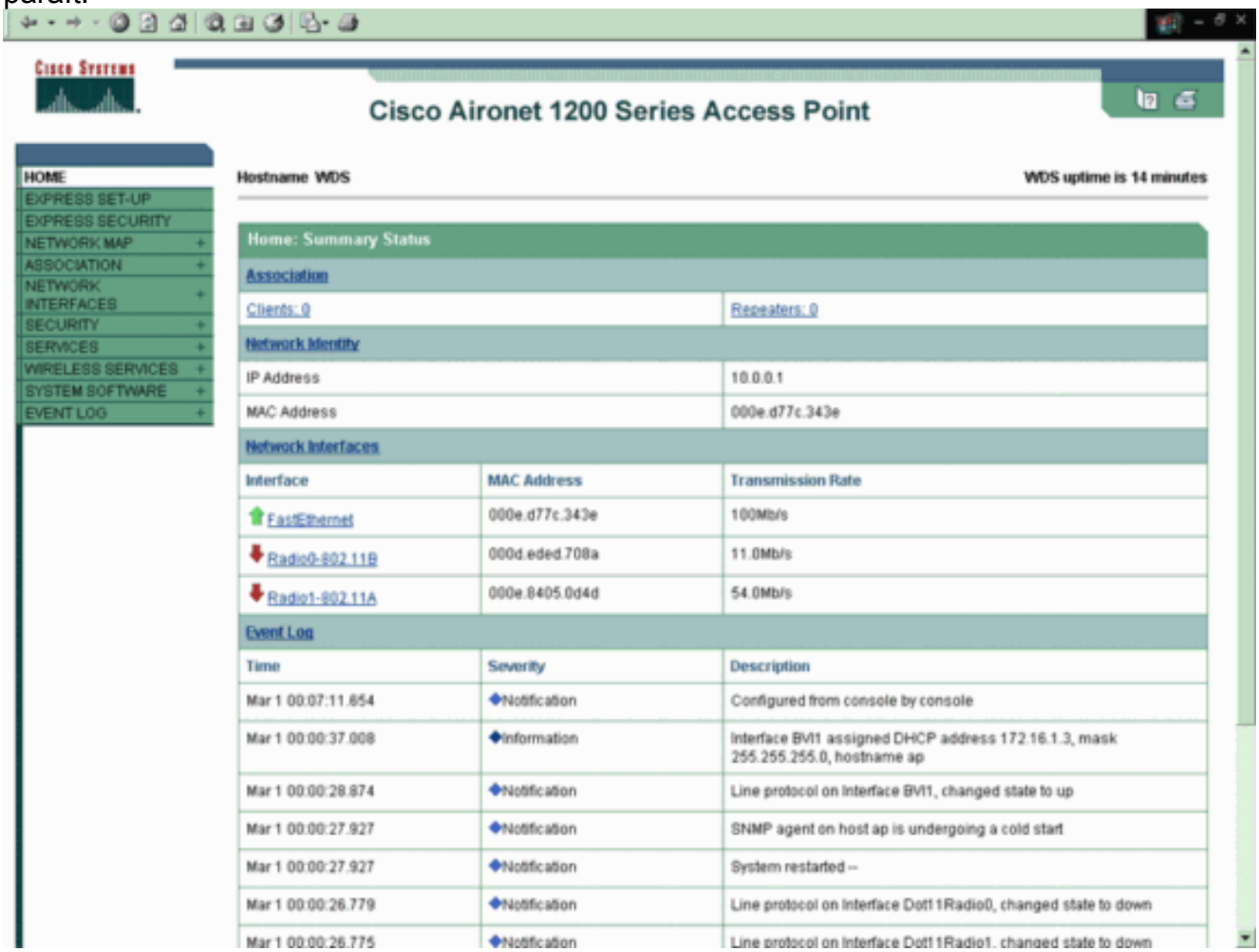
Configurez le WDS AP

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

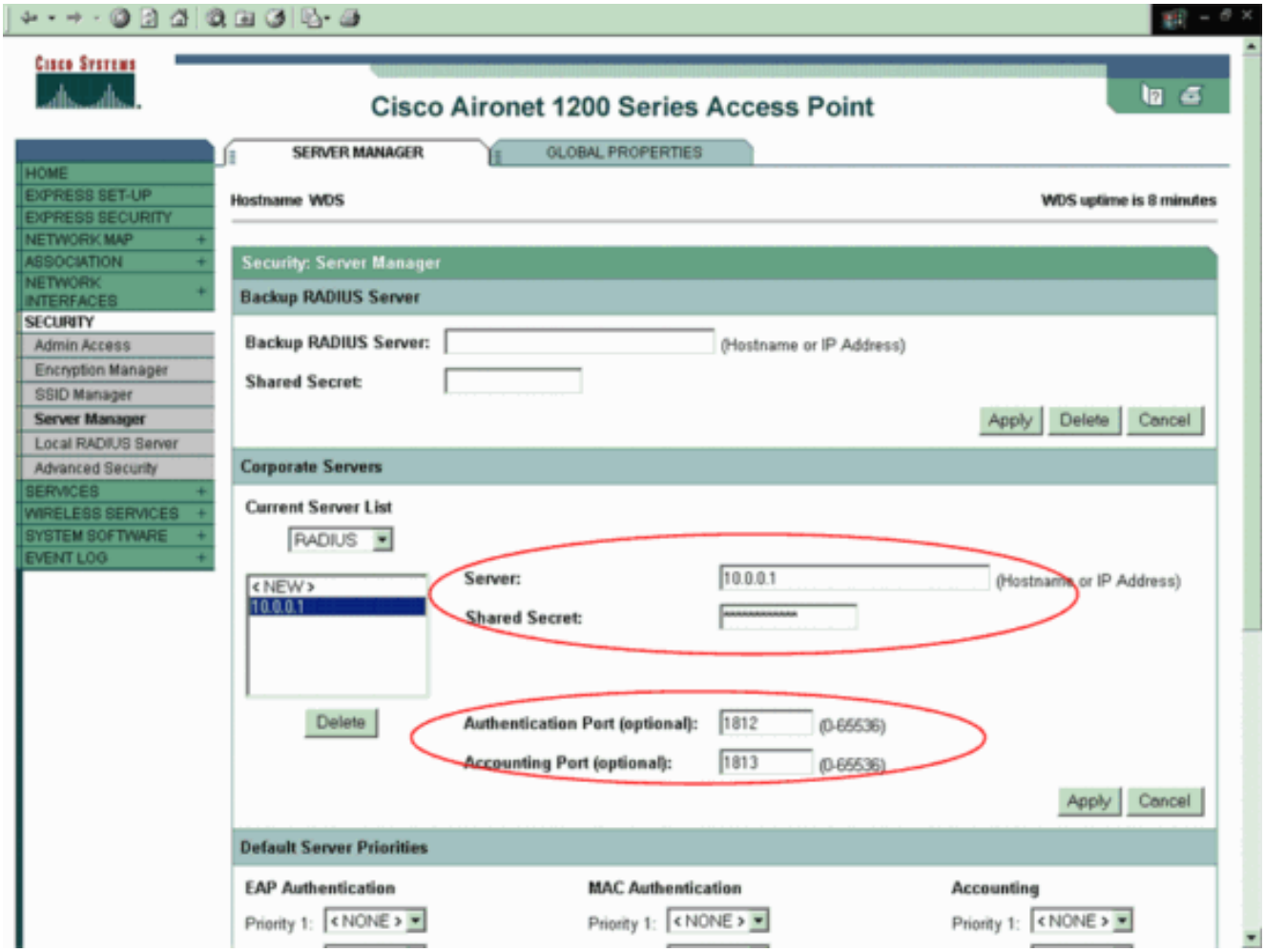
Afin de configurer AP pour servir de WDS AP avec la fonctionnalité de serveur d'AAA, vous devez d'abord activer la caractéristique locale de serveur de RADIUS sur AP.

Procédez comme suit :

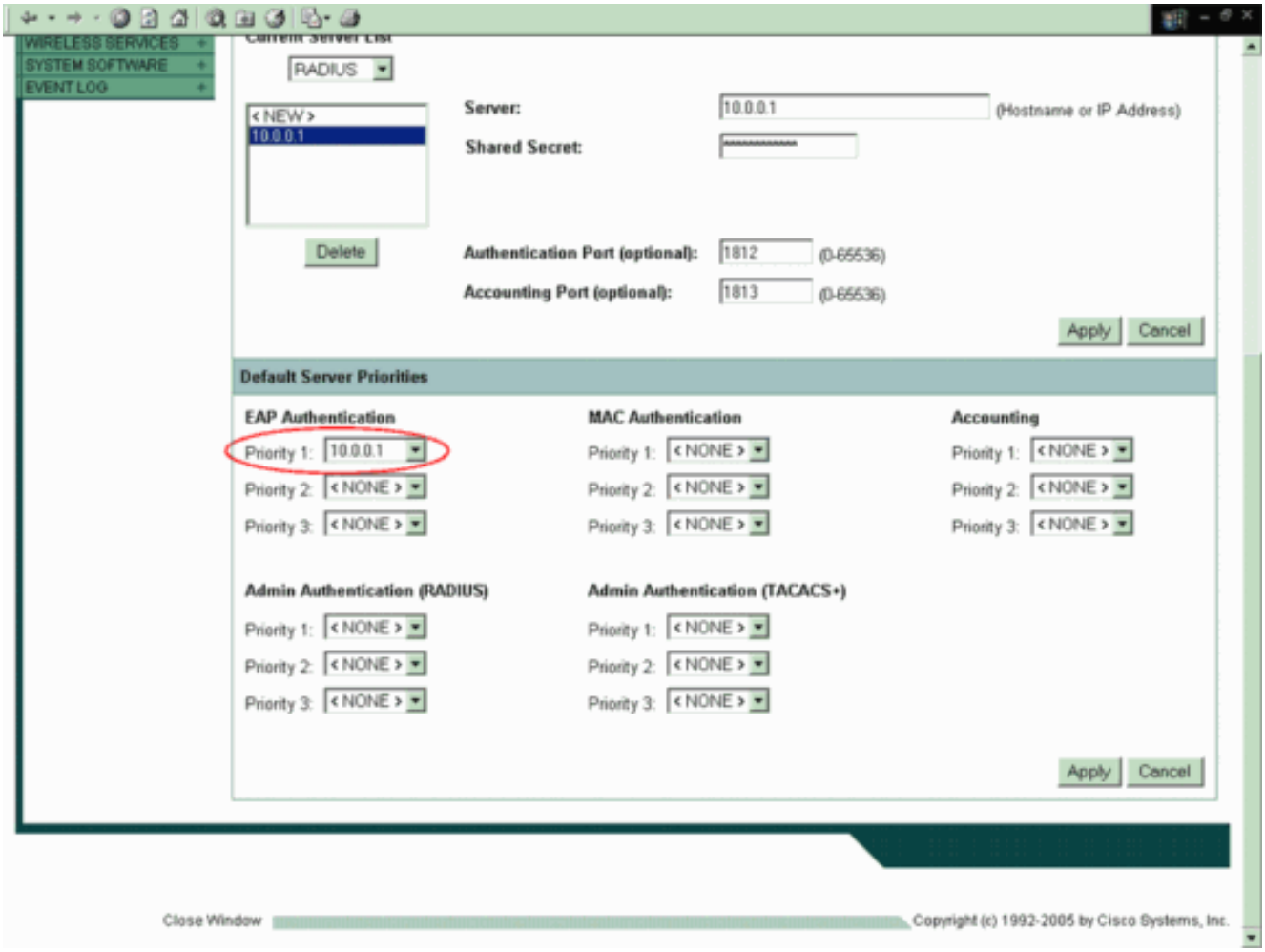
1. Procédure de connexion à AP par le GUI.La page d'état récapitulatif paraît.



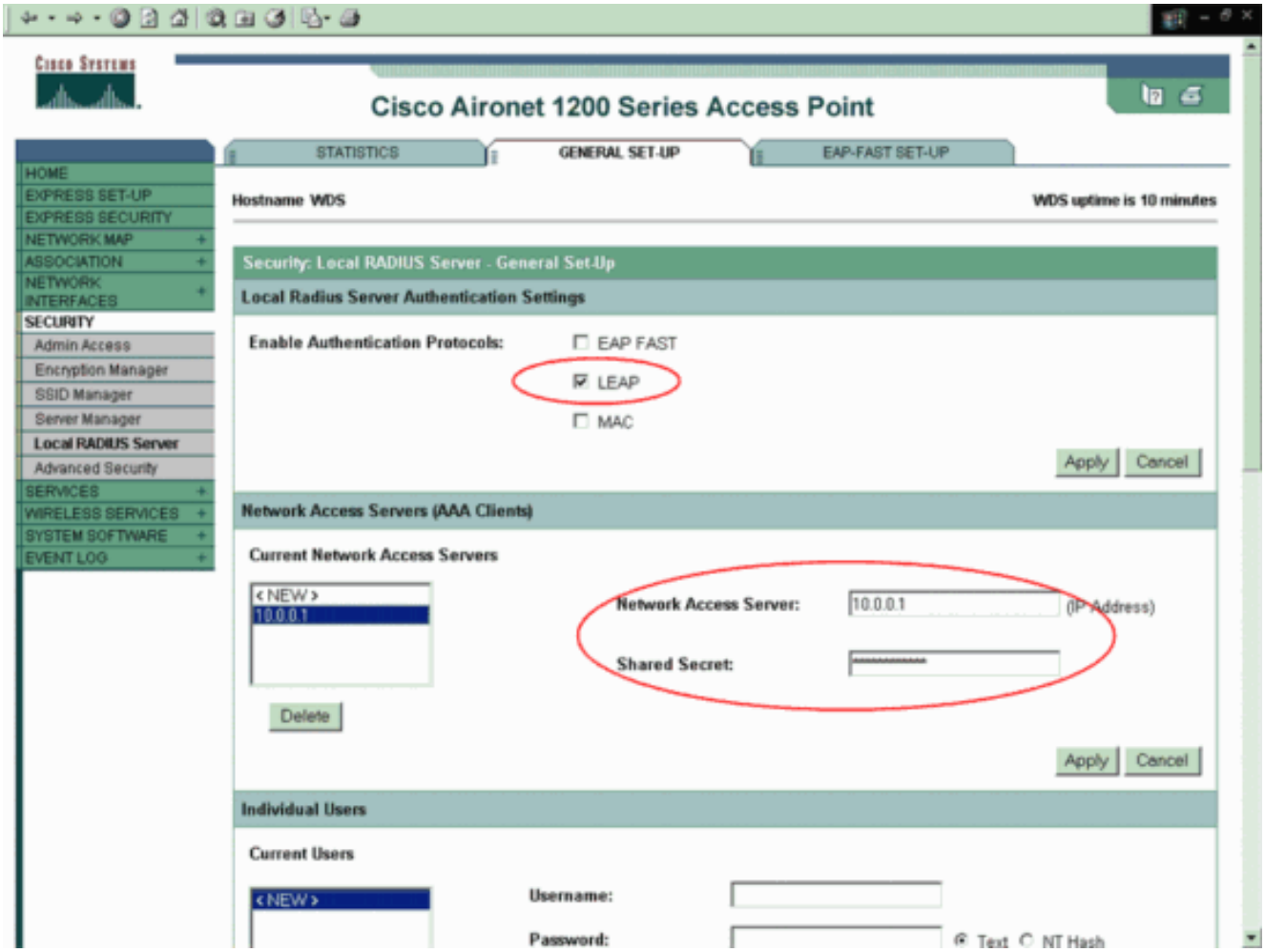
2. **Security > Server Manager** choisi du menu de côté gauche sur AP.
3. Écrivez l'adresse IP et le secret partagé d'AP qui agit en tant que serveur de RADIUS sous les serveurs entreprise.Écrivez dans ce cas l'adresse IP du WDS AP puisque le WDS AP va agir en tant que serveur de RADIUS. L'exemple utilise l'adresse IP 10.0.0.1. Puisque c'est un serveur local de RADIUS vous devez utiliser 1812 et 1813 en tant que comme indiqué dans cet exemple de l'authentification et de ports de traçabilité.
4. Cliquez sur **Apply**.



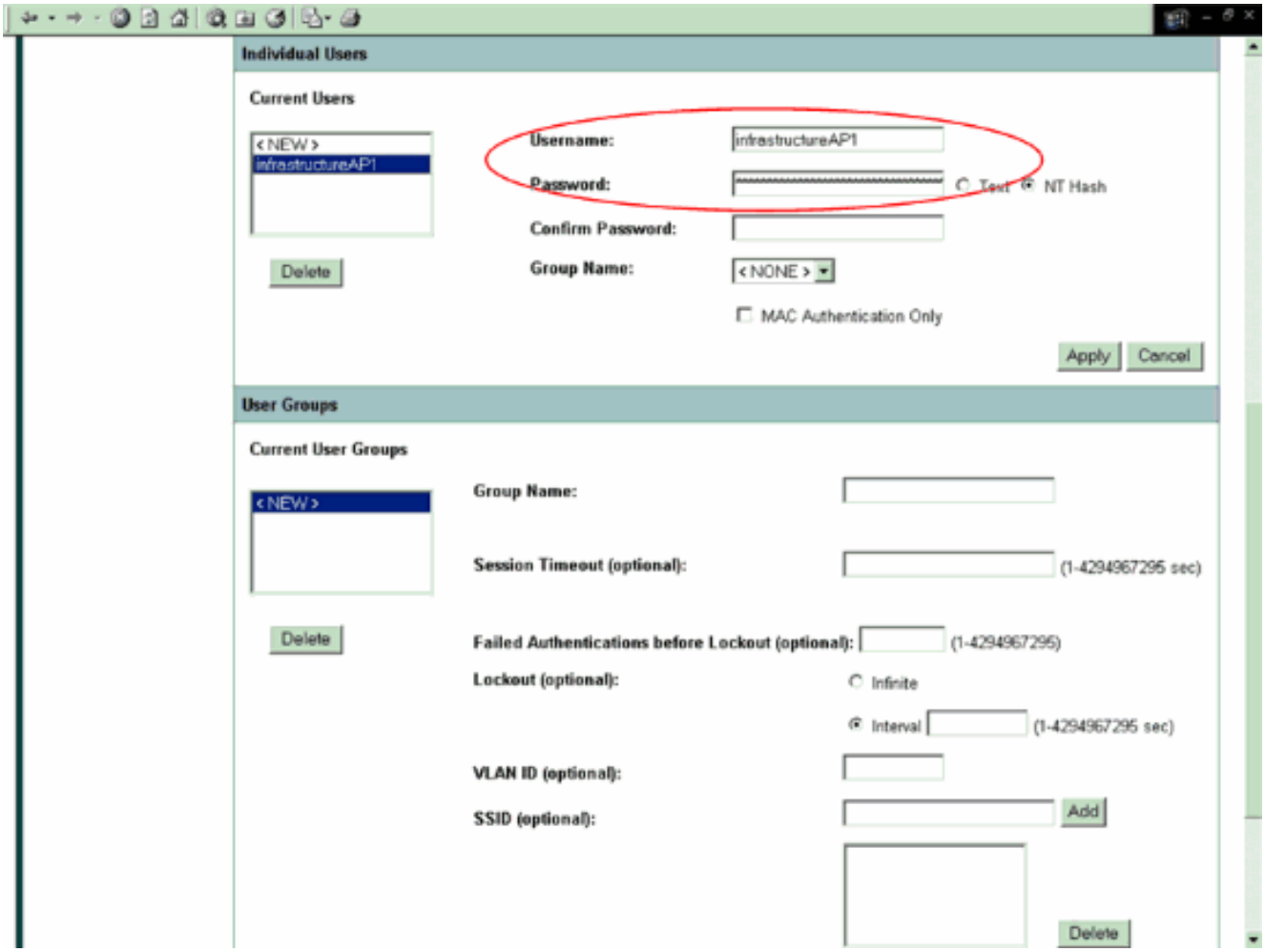
5. Sélectionnez l'adresse IP WDS aps comme Default Server Priorities de dessous **prioritaire 1** pour l'authentification EAP.Cliquez sur **Apply**.Ceci permet au serveur local de RADIUS pour être le premier choix pour authentifier l'infrastructure aps et les clients.



6. **Sécurité** choisie **> serveur de Radius de gens du pays du menu de côté gauche**.Cliquez sur la **configuration générale** afin de configurer des paramètres de serveur de RADIUS de gens du pays.Sélectionnez le **LEAP** sous des configurations d'authentification de serveur de Radius de gens du pays et cliquez sur Apply.Écrivez l'adresse IP du WDS AP et un mot de passe secret partagé sous des serveurs d'accès à distance. Cet exemple utilise le mot de passe secret partagé comme **test123**.Cliquez sur
Apply.



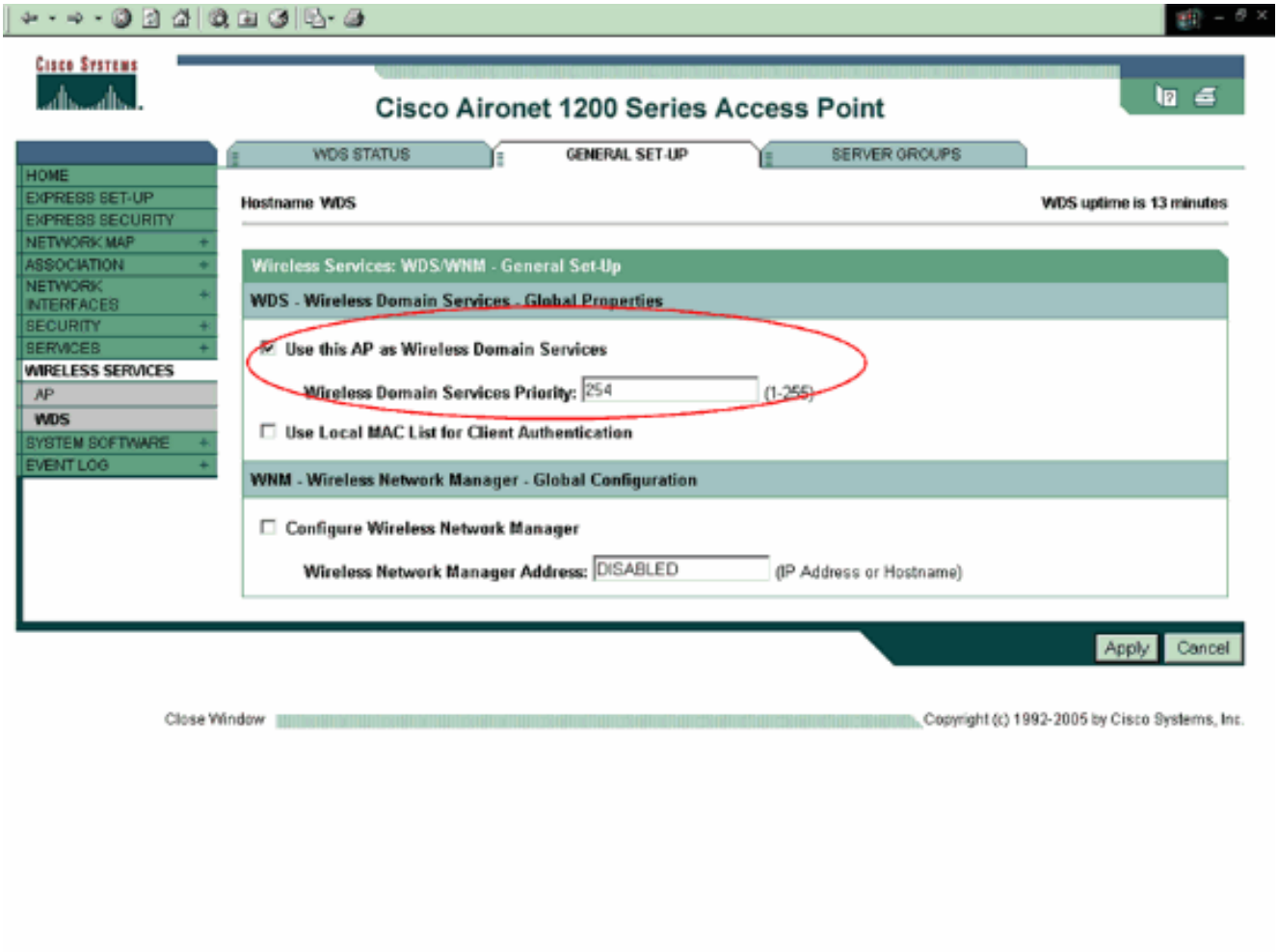
7. Écrivez le nom d'utilisateur et mot de passe de toute l'infrastructure aps et de clients qui communiquent avec le WDS AP sous des utilisateurs individuels.Cliquez sur **Apply**.Cet exemple inclut le nom d'utilisateur et mot de passe de l'infrastructure AP que vous configurez pour enregistrer avec le WDS AP. Cet exemple utilise le nom d'utilisateur comme **infrastructureAP1** et le mot de passe comme **Cisco**. Le même nom d'utilisateur et mot de passe doit être configuré sur le Point d'accès d'infrastructure.



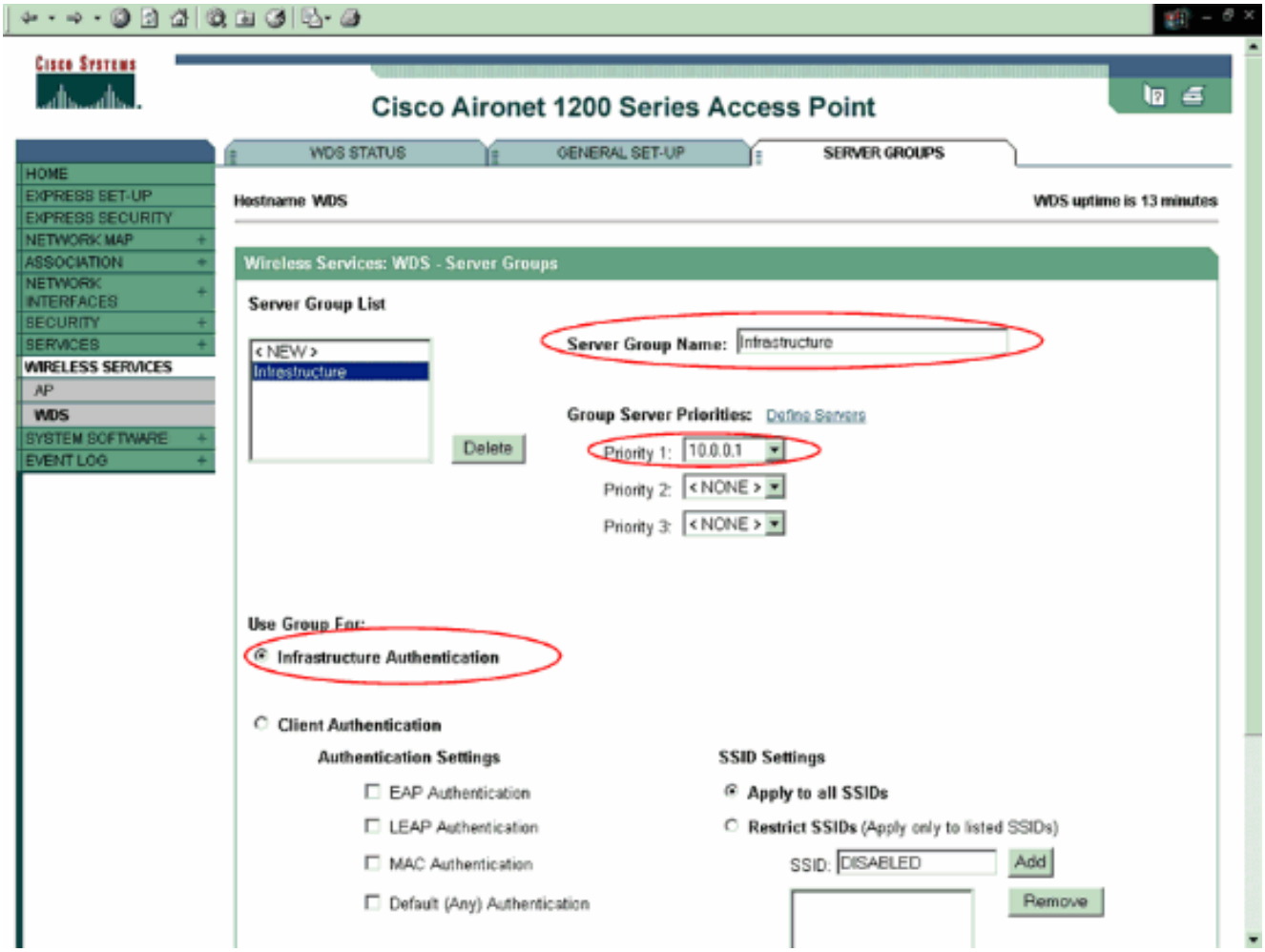
Après que vous configuriez la caractéristique locale de serveur de RADIUS sur AP, vous devez activer la fonctionnalité WDS sur AP.

Procédez comme suit :

1. **Services sans fil** choisis **> WDS du** menu de côté gauche sur AP.
2. **Configuration générale de**
   clic.



3. Vérifiez l'**utilisation cet AP comme des services de domaine Sans fil à la** page de configuration générale.Écrivez **254** dans le champ de priorité Sans fil de services de domaine. Cliquez sur **Apply**.
4. Authentification d'infrastructure d'enable.**Groupes de serveurs de** clic à la page WDS.Écrivez un nom dans la zone d'identification de groupe de serveurs pour authentifier l'infrastructure aps. Cet exemple utilise le nom de groupe de serveurs comme **infrastructure**.Sélectionnez l'adresse IP du serveur local de RADIUS de la liste déroulante prioritaires de serveur de groupe.Le WDS AP utilise ce serveur pour authentifier l'infrastructure aps.**Authentification** choisie d'**infrastructure** sous le groupe d'utilisation pour.Cliquez sur **Apply**.



Le WDS AP agit maintenant en tant que serveur d'AAA. Configurez un de l'infrastructure aps pour s'enregistrer avec le WDS AP.

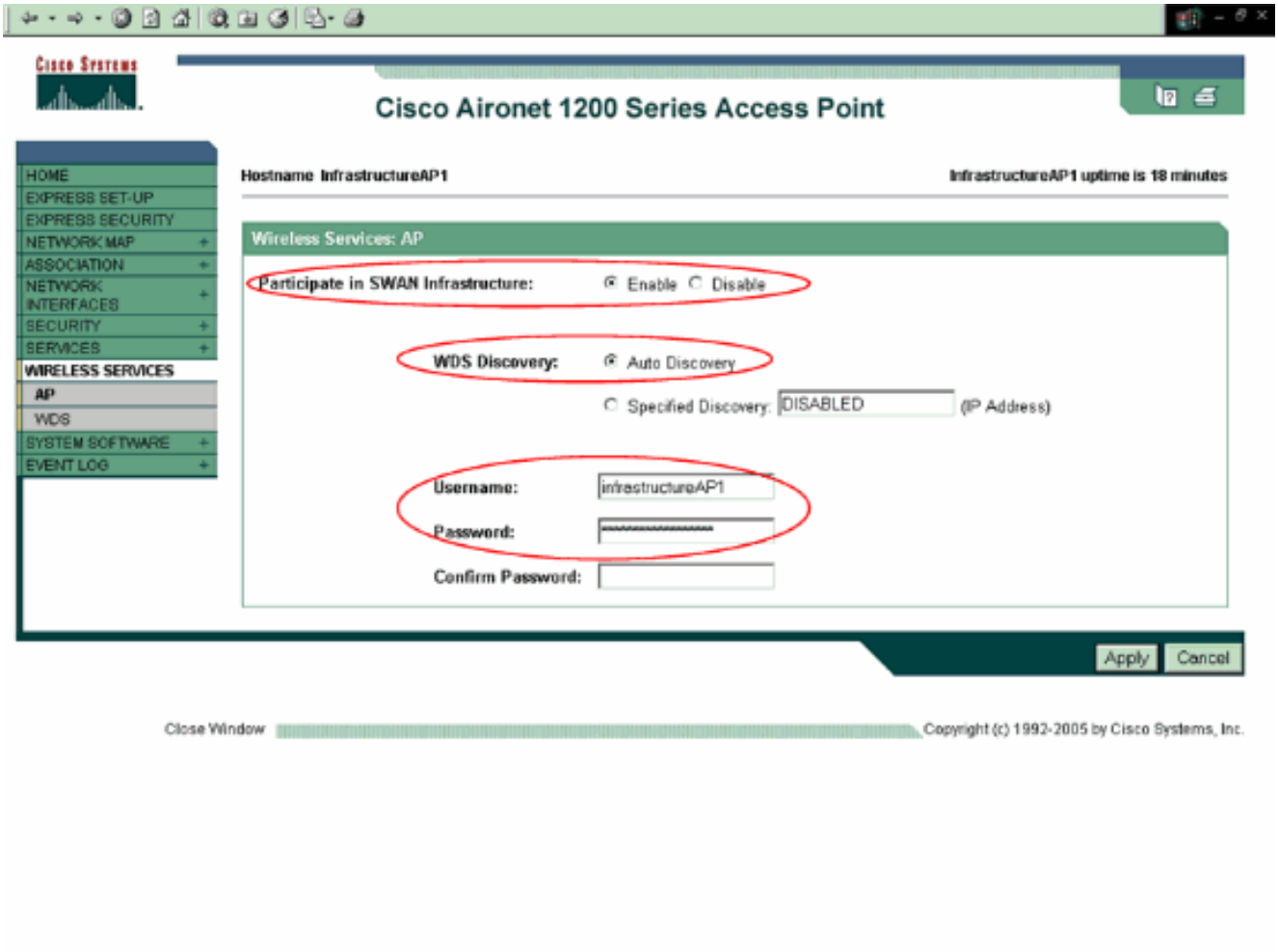
Remarque: Utilisez l'outil Command Lookup Tool (clients enregistrés seulement) pour trouver plus d'informations sur les commandes utilisées dans ce document.

Configurez l'infrastructure AP

Cette section explique la configuration exigée sur l'infrastructure AP pour s'enregistrer avec le WDS AP. L'associé de clients à l'infrastructure aps. L'infrastructure aps invitent le WDS AP à exécuter l'authentification pour eux.

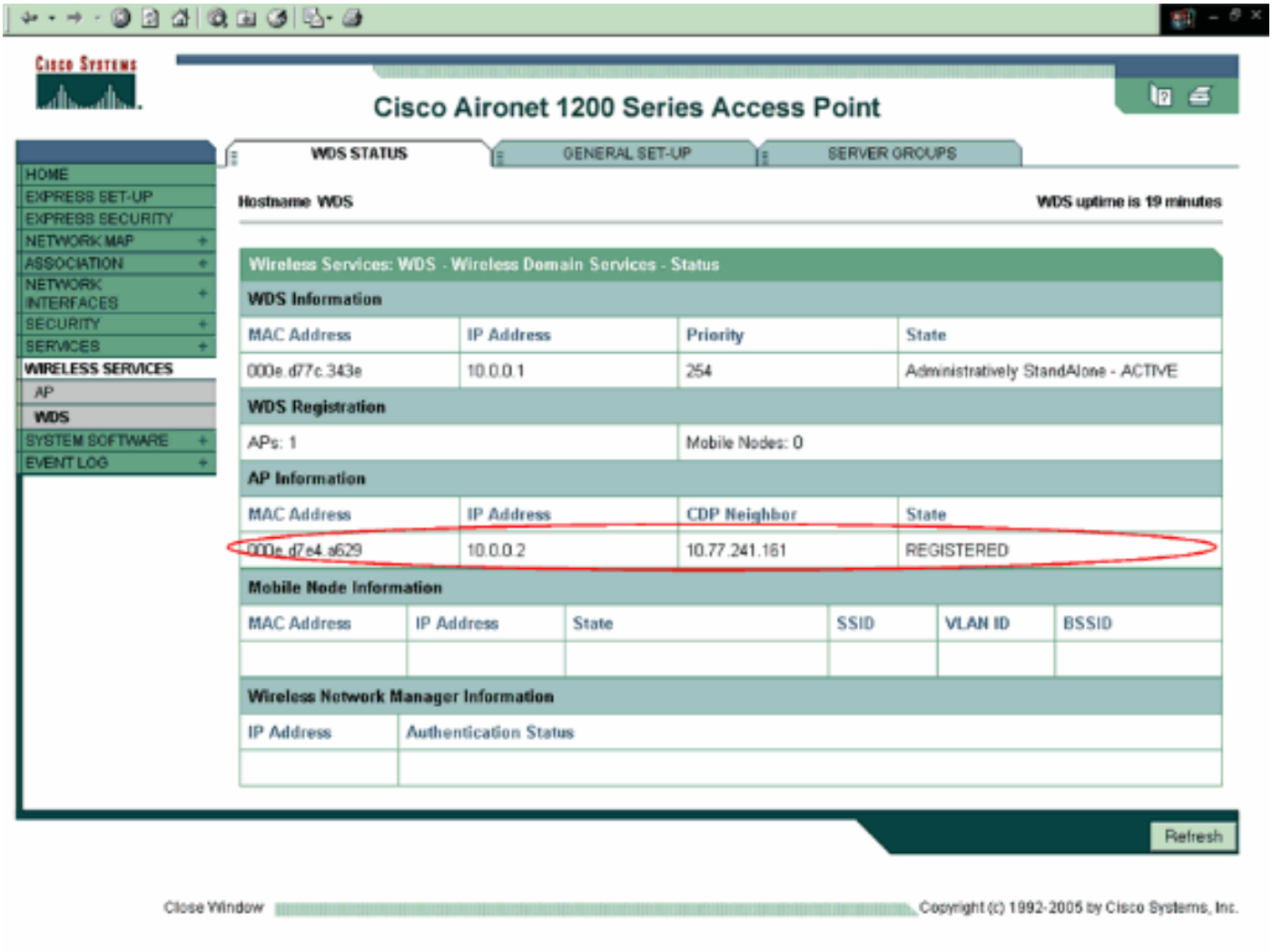
Terminez-vous ces étapes pour ajouter une infrastructure AP qui utilise les services du WDS :

1. **Services sans fil** choisis **> AP du** menu de côté gauche.
2. Sélectionnez l'**enable** participent dessous à l'infrastructure de CYGNE.
3. **Détection automatique** choisie sous la détection
   WDS.



4. Écrivez le nom d'utilisateur et mot de passe WDS dans les champs appropriés.Cliquez sur **Apply**.Le nom d'utilisateur et mot de passe doit exister sur le serveur local de RADIUS. Vous devez définir un nom d'utilisateur et mot de passe WDS sur le serveur d'authentification pour tous les périphériques qui sont d'être des membres du WDS.

L'infrastructure AP apparaît dans la région de l'information AP avec l'état comme ENREGISTRÉE une fois que vous configurez le WDS AP et l'infrastructure AP sur le WDS AP, onglet d'état WDS. C'est aux Services sans fil > à la commande de menu WDS.



Les configurations incorrectes d'authentification sur le WDS AP ou l'infrastructure AP peuvent faire ne pas apparaître AP comme ACTIVE et/ou SE SONT ENREGISTRÉES. Vérifiez les statistiques de serveur d'authentification pour toutes les erreurs ou tentatives d'authentification défaillante. **Security > Local Radius Server** choisi **> statistiques** pour des statistiques de serveur d'authentification.

Vous pouvez également employer le **show wlccp wds AP de** commande du CLI sur le WDS AP pour vérifier la configuration. Sur l'enregistrement réussi avec le WDS AP, la sortie après un enregistrement réussi avec le WDS AP ressemble à cet exemple :

```
WDS#show wlccp wds ap
  MAC-ADDR         IP-ADDR         STATE      LIFETIME    CDP-NEIGHBOR
  000e.d7e4.a629   10.0.0.2      REGISTERED    97          10.77.241.161
```

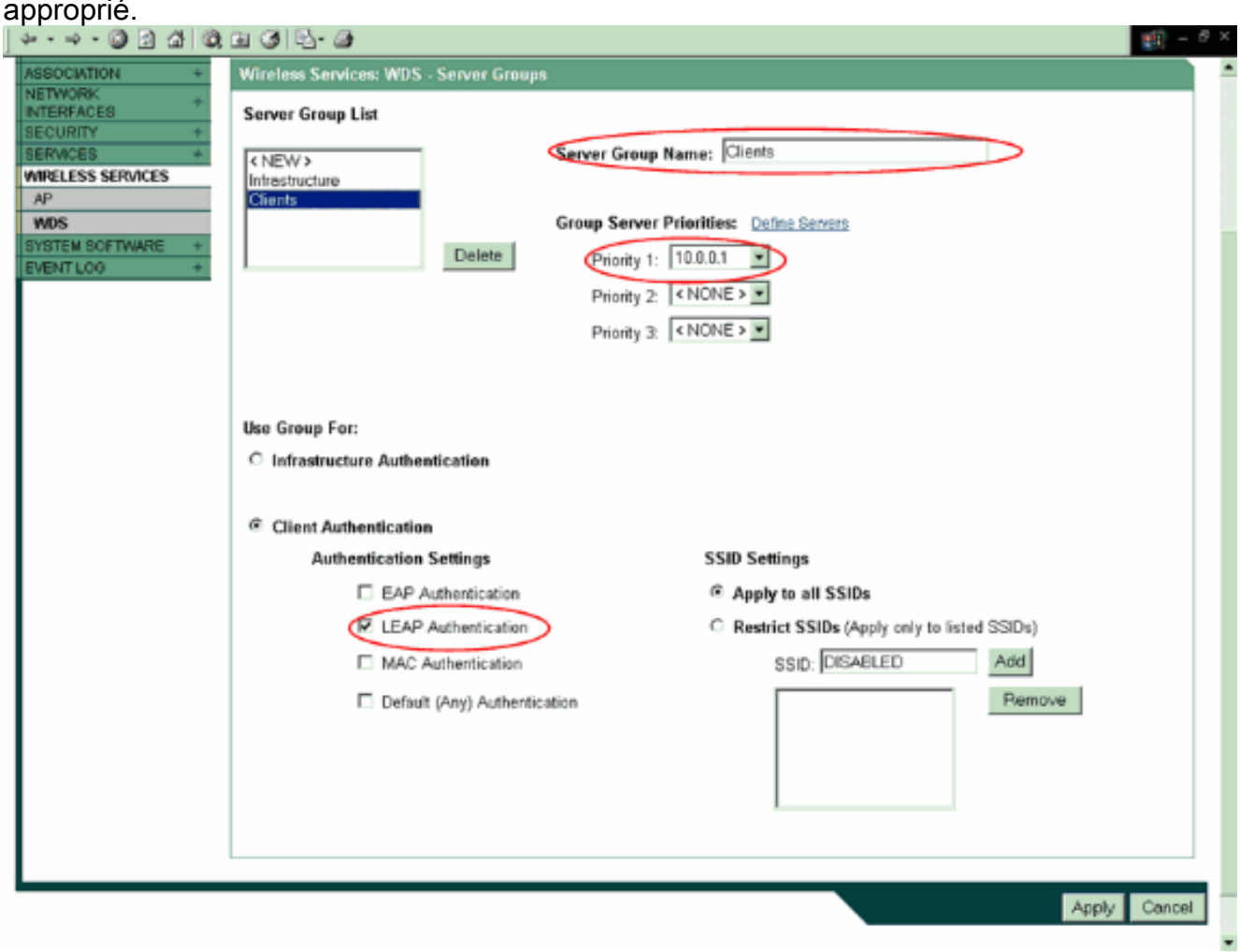
Configurez la méthode d'authentification client

Ajoutez une méthode d'authentification client au WDS.

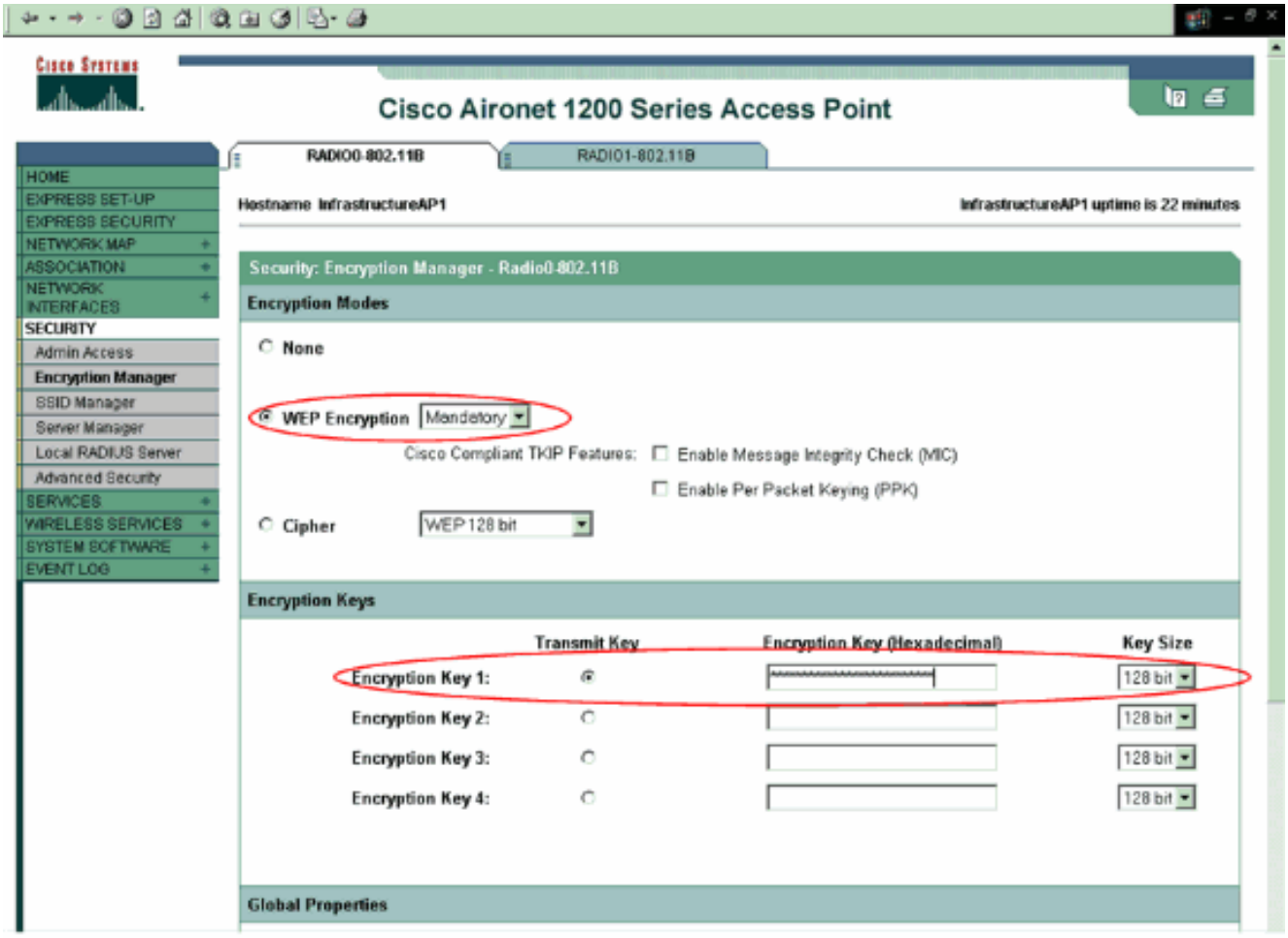
Procédez comme suit :

1. **Services sans fil** choisis **> WDS > groupes de serveurs** sur le WDS AP.Définissez un groupe de serveurs qui authentifie des clients (un groupe de clients).Ceci devrait être différent du groupe de serveurs précédemment configuré pour l'authentification d'infrastructure. Cet exemple utilise le nom de groupe de serveurs comme **clients**.Fixez la priorité 1 au serveur

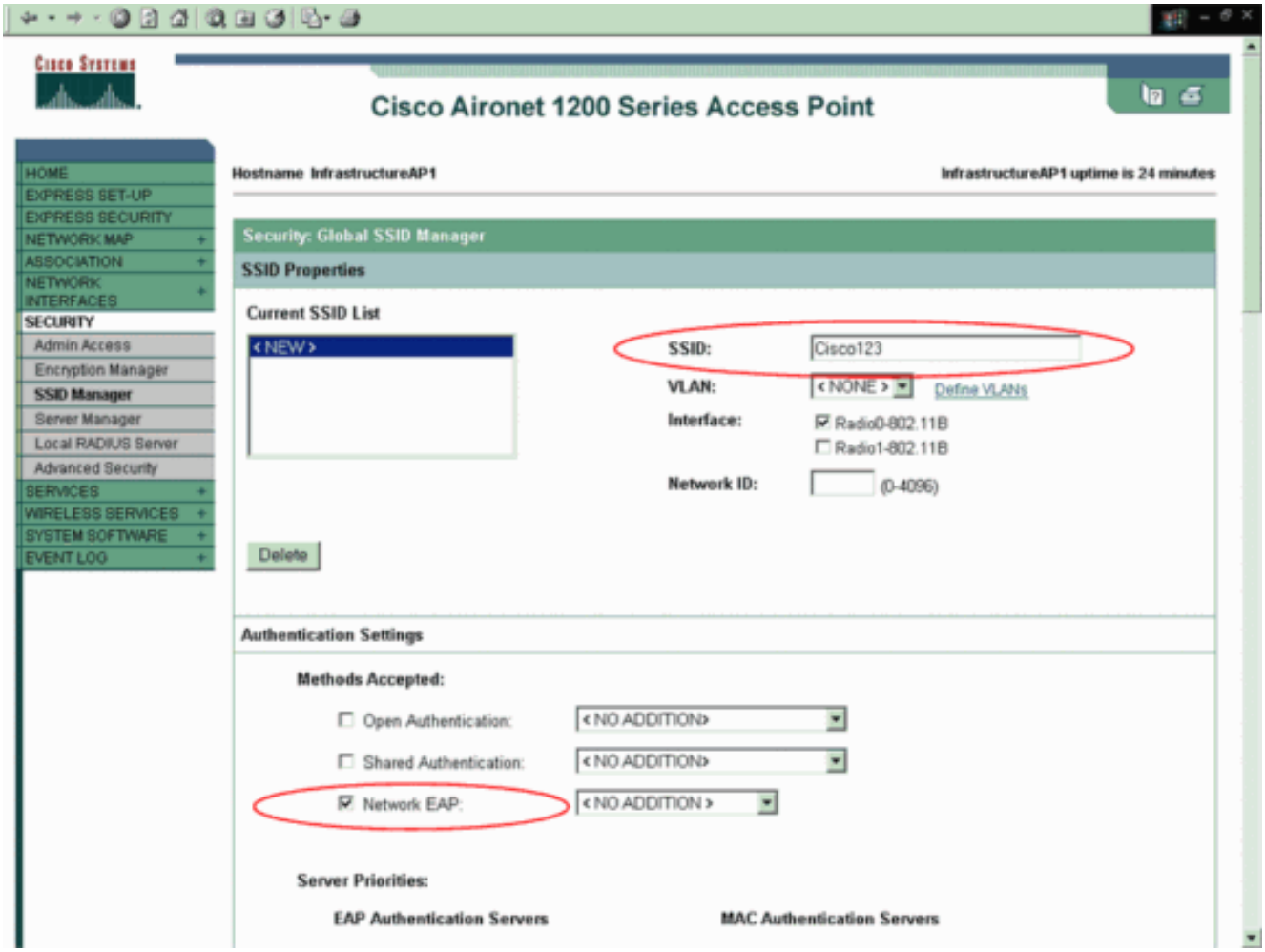
local de RADIUS.Sélectionnez le type d'authentification (LEAP, EAP, MAC, et ainsi de suite) pour l'utiliser pour l'authentification client.Cet exemple utilise l'authentification LEAP.Appliquez les configurations au SSID approprié.



2. Terminez-vous ces étapes sur l'infrastructure AP :**Le Security > Encryption Manager** et le **cryptage WEP** choisis de clic et choisissent **obligatoire du** menu déroulant. Sous des clés de chiffrement, introduisez la clé de chiffrement WEP 128-bit. Cet exemple utilise la clé de chiffrement comme **1234567890abcdef1234567890**.



Le Security > SSID Manager choisi et créent un nouveau SSID.Cet exemple utilise le SSID comme **Cisco123**. Ensuite, choisissez la méthode d'authentification.**EAP** choisi de **réseau** sur l'infrastructure
AP.



Testez que les clients authentifient avec succès et s'associent avec l'infrastructure aps. Le client passe en fonction ses qualifications à l'infrastructure AP quand elle est soulevée pour la première fois. L'infrastructure AP puis en avant les mêmes au WDS AP, qui valide les qualifications.

Remarque: Ce document n'explique pas comment configurer l'adaptateur de client. Référez-vous à l'Adaptateurs client LAN sans fil Cisco Aironet pour les informations sur la façon dont configurer l'adaptateur de client.

Vérifier

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

- **manganèse de show wlccp wds** - Utilisez cette commande du CLI sur le WDS AP de vérifier l'authentification client et l'association réussies avec le WDS AP.

```
WDS#show wlccp wds mn
  MAC-ADDR         IP-ADDR      Curr-AP          STATE
 0040.96a5.b5d4    10.0.0.15    000e.d7e4.a629  REGISTERED
```

Les commandes de débogage suivantes sont également utiles.

- **debug wlccp ap {manganèse | wds-détection | état}** - utilisez cette commande d'activer l'affichage des messages de débogage liés aux périphériques de client **(manganèse)**, au **processus de découverte WDS**, et à l'authentification de Point d'accès au Point d'accès WDS **(état)**.
- **debug wlccp packet** - Utilisez cette commande d'activer l'affichage des paquets à et du Point

d'accès WDS.
- **debug radius local-server** - Lance l'affichage des messages d'erreur liés aux authentifications client défectueuses à l'authentificateur local

Dépanner

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- Configuration de services de domaine sans fil
- Adaptateurs de client de Cisco Aironet
- Services de domaine sans fil - Forum Aux Questions
- Exemples et TechNotes de configuration WLAN
- Exemples et TechNotes de configuration de Gamme Cisco Aironet 1200
- Support et documentation techniques - Cisco Systems