

Configuration de services de domaine sans fil

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Conventions](#)

[Services de domaine Sans fil](#)

[Rôle du périphérique WDS](#)

[Rôle des Points d'accès utilisant le périphérique WDS](#)

[Configuration](#)

[Indiquez AP comme WDS](#)

[Indiquez un WLSM comme WDS](#)

[Indiquez AP comme périphérique d'infrastructure](#)

[Définissez la méthode d'authentification client](#)

[Vérifier](#)

[Dépanner](#)

[Dépannage des commandes](#)

[Informations connexes](#)

[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.

The screenshot shows the Cisco 1200 Access Point configuration page. The left sidebar contains navigation options like HOME, EXPRESS SET-UP, SECURITY, SERVICES, etc. The main content area is divided into several sections:

- SERVER MANAGER / GLOBAL PROPERTIES:** Hostname WDS_AP, Date: 16:09:43 Fri Apr 23 2004.
- Security: Server Manager:** Backup RADIUS Server configuration with fields for Backup RADIUS Server (Hostname or IP Address) and Shared Secret. Buttons: Apply, Delete, Cancel.
- Corporate Servers:** Current Server List (RADIUS) showing a list with '< NEW >' and '10.0.0.3'. A red box highlights the configuration for the selected server:
 - Server: 10.0.0.3 (Hostname or IP Address)
 - Shared Secret: [Empty]
 - Authentication Port (optional): 1645 (0-65536)
 - Accounting Port (optional): 1646 (0-65536)
 Buttons: Apply, Cancel.
- Default Server Priorities:** A table of priority settings for various authentication methods. A red circle highlights the EAP Authentication section:

Authentication Method	Priority 1	Priority 2	Priority 3
EAP Authentication	10.0.0.3	< NONE >	< NONE >
MAC Authentication	< NONE >	< NONE >	< NONE >
Accounting	< NONE >	< NONE >	< NONE >
Admin Authentication (RADIUS)	< NONE >	< NONE >	< NONE >
Admin Authentication (TACACS+)	< NONE >	< NONE >	< NONE >
Proxy Mobile IP Authentication	< NONE >	< NONE >	< NONE >

 Buttons: Apply, Cancel.

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 : Nom Adresse IP Secret partagé Méthode d'authentification RADIUS Cisco Aironet Internet Engineering Task Force de RADIUS [IETF] Cliquez sur **soumettre** en fonction. Pour d'autres serveurs d'authentification de non-

ACS, référez-vous à la documentation du fabricant.

Network Configuration

Add AAA Client

AAA Client Hostname: WDS_AP

AAA Client IP Address: 10.0.0.102

Key: sharedsecret

Authenticate Using: RADIUS (Cisco Aironet)

- 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

Buttons: Submit, Submit + Restart, Cancel

Help

- [AAA Client Hostname](#)
- [AAA Client IP Address](#)
- [Key](#)
- [Network Device Group](#)
- [Authenticate Using](#)
- [Single Connect TACACS+ AAA Client](#)
- [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](#)

AAA Client Hostname

The AAA Client Hostname is the name assigned to the AAA client.

[\[Back to Top\]](#)

AAA Client IP Address

The AAA Client IP Address is the IP address assigned to the AAA client.

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](#), cliquez sur alors l'[installation globale d'authentification](#).

CISCO SYSTEMS **System Configuration**

Select	Help
<ul style="list-style-type: none"> User Setup Group Setup Shared Profile Components Network Configuration System Configuration Interface Configuration Administration Control External User Databases Reports and Activity Online Documentation 	<ul style="list-style-type: none"> Service Control Logging Date Format Control Local Password Management CiscoSecure Database Replication ACS Backup ACS Restore ACS Service Management IP Pools Server IP Pools Address Recovery ACS Certificate Setup Global Authentication Setup <p style="text-align: center;"> Back to Help</p>
	<ul style="list-style-type: none"> • Service Control • Logging • Date Format Control • Local Password Management • CiscoSecure Database Replication • RDBMS Synchronization • ACS Backup • ACS Restore • ACS Service Management • IP Pools Address Recovery • IP Pools Server • VoIP Accounting Configuration • ACS Certificate Setup • Global Authentication Configuration <hr/> <p>Service Control</p> <p>Select to open the page from which you can stop or restart Cisco Secure ACS services.</p> <p>[Back to Top]</p>

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

CISCO SYSTEMS **System Configuration**

Edit **Help**

Global Authentication Setup

EAP Configuration ?

PEAP

Allow EAP-MSCHAPv2

Allow EAP-GTC

Cisco client initial message:

PEAP session timeout (minutes):

Enable Fast Reconnect:

EAP-FAST

Allow EAP-FAST

Active master key TTL:

Retired master key TTL:

PAC TTL:

Client initial message:

Authority ID Info:

Allow automatic PAC provisioning:

EAP-FAST master server:

Actual EAP-FAST server status: **Master**

EAP-TLS

Allow EAP-TLS

Select one or more of the following options:

Certificate SAN comparison

Certificate CN comparison

Certificate Binary comparison

EAP-TLS session timeout (minutes):

LEAP

Allow LEAP (For Aironet only)

EAP-MD5

Allow EAP-MD5

AP EAP request timeout (seconds):

MS-CHAP Configuration ?

Allow MS-CHAP Version 1 Authentication

Allow MS-CHAP Version 2 Authentication

[? Back to Help](#)

Help

- [PEAP](#)
- [EAP-FAST](#)
- [EAP-TLS](#)
- [LEAP](#)
- [EAP-MD5](#)
- [AP EAP request timeout](#)
- [MS-CHAP Configuration](#)

This page specifies settings for various authentication protocols.

[\[Back to Top\]](#)

PEAP

Note: PEAP is a certificate-based authentication protocol. PEAP authentication can occur only after you have

3. Afin de configurer les settings 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 - Propriétés 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).

Cisco 1200 Access Point

WDS STATUS | SERVER GROUPS | GENERAL SET-UP

Hostname WDS_AP 16:26:44 Fri Apr 23 2004

Wireless Services: WDS - Server Groups

Server Group List

< NEW >
Infrastructure

Delete

Server Group Name: Infrastructure

Group Server Priorities: [Define Servers](#)

Priority 1: 10.0.0.3
Priority 2: < NONE >
Priority 3: < NONE >

Use Group For:

Infrastructure Authentication

Client Authentication

Authentication Settings

EAP Authentication
 LEAP Authentication
 MAC Authentication
 Default (Any) Authentication

SSID Settings

Apply to all SSIDs

Restrict SSIDs (Apply only to listed SSIDs)

SSID: DISABLED Add Remove

Apply Cancel

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.

User Setup

User: WDSUser (New User)

Account Disabled

Supplementary User Info

Real Name

Description

User Setup

Password Authentication:

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

Password

Confirm Password

Help

- [Account Disabled](#)
- [Deleting a Username](#)
- [Supplementary User Info](#)
- [Password Authentication](#)
- [Group to which the user is assigned](#)
- [Callback](#)
- [Client IP Address Assignment](#)
- [Advanced Settings](#)
- [Network Access Restrictions](#)
- [Max Sessions](#)
- [Usage Quotas](#)
- [Account Disable](#)
- [Downloadable ACLs](#)
- [Advanced TACACS+ Settings](#)
- [TACACS+ Enable Control](#)
- [TACACS+ Enable Password](#)
- [TACACS+ Outbound Password](#)
- [TACACS+ Shell Command Authorization](#)
- [Command Authorization for Network Device Management Applications](#)
- [TACACS+ Unknown Services](#)
- [IETF RADIUS Attributes](#)
- [RADIUS Vendor-Specific Attributes](#)

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.

Cisco Systems Cisco 1200 Access Point

Hostname WDS_AP 16:00:29 Fri Apr 23 2004

HOME
EXPRESS SET-UP
EXPRESS SECURITY
NETWORK MAP +
ASSOCIATION +
NETWORK INTERFACES +
SECURITY +
SERVICES +
WIRELESS SERVICES
AP
WDS
SYSTEM SOFTWARE +
EVENT LOG +

Wireless Services: AP

Participate in SWAN Infrastructure: Enable Disable

WDS Discovery: Auto Discovery
 Specified Discovery: (IP Address)

Username:
Password:
Confirm Password:

L3 Mobility Service via IP/GRE Tunnel: Enable Disable

Apply Cancel

Alternativement, émettez ces commandes du CLI :

7. Choisissez les **Services sans fil > le WDS**. Sur l'onglet d'état WDS AP WDS, contrôlez 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 défectueuses. Quand AP s'enregistre convenablement, ajoutez une infrastructure AP pour utiliser les services du WDS.

Cisco 1200 Access Point

WDS STATUS | SERVER GROUPS | GENERAL SET-UP

Hostname WDS_AP 16:30:08 Fri Apr 23 2004

Wireless Services: WDS - Wireless Domain Services - Status

WDS Information			
MAC Address	IP Address	Priority	State
0005.9a38.429f	10.0.0.102	254	Administratively StandAlone - ACTIVE

WDS Registration

APs: 1 Mobile Nodes: 0

AP Information		
MAC Address	IP Address	State
0005.9a38.429f	10.0.0.102	REGISTERED

Mobile Node Information					
MAC Address	IP Address	State	SSID	VLAN ID	BSSID

Wireless Network Manager Information	
IP Address	Authentication Status

Refresh

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 : Nom Adresse IP Secret partagé Méthode d'authentification RADIUS Cisco Aironet IETF DE RADIUS. Pour d'autres serveurs d'authentification de non-ACS, référez-vous à la documentation du fabricant.

The screenshot shows the 'Add AAA Client' configuration page in Cisco Secure ACS. The page is titled 'Network Configuration' and has a left-hand navigation menu with options like 'User Setup', 'Group Setup', 'Shared Profile Components', 'Network Configuration', 'System Configuration', 'Interface Configuration', 'Administration Control', 'External User Databases', 'Reports and Activity', and 'Online Documentation'. The main content area is titled 'Add AAA Client' and contains the following fields and options:

- AAA Client Hostname:
- AAA Client IP Address:
- Key:
- Authenticate Using:

Below these fields are four unchecked 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 form are three buttons: 'Submit', 'Submit + Restart', and 'Cancel'. On the right side, there is a 'Help' section with a list of links: 'AAA Client Hostname', 'AAA Client IP Address', 'Key', 'Network Device Group', 'Authenticate Using', 'Single Connect TACACS+ AAA Client', 'Log Update/Watchdog Packets from this AAA Client', 'Log RADIUS Tunneling Packets from this AAA Client', and 'Replace RADIUS Port info with Username from this AAA Client'. Below the links, there are two sections of help text: 'AAA Client Hostname' (The AAA Client Hostname is the name assigned to the AAA client.) and 'AAA Client IP Address' (The AAA Client IP Address is the IP address assigned to the AAA client.). A '[Back to Top]' link is also present.

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**.

CISCO SYSTEMS **System Configuration**

Select	Help
<ul style="list-style-type: none"> User Setup Group Setup Shared Profile Components Network Configuration System Configuration Interface Configuration Administration Control External User Databases Reports and Activity Online Documentation 	<ul style="list-style-type: none"> Service Control Logging Date Format Control Local Password Management CiscoSecure Database Replication ACS Backup ACS Restore ACS Service Management IP Pools Server IP Pools Address Recovery ACS Certificate Setup Global Authentication Setup <p style="text-align: center;"> Back to Help</p>
	<ul style="list-style-type: none"> • Service Control • Logging • Date Format Control • Local Password Management • CiscoSecure Database Replication • RDBMS Synchronization • ACS Backup • ACS Restore • ACS Service Management • IP Pools Address Recovery • IP Pools Server • VoIP Accounting Configuration • ACS Certificate Setup • Global Authentication Configuration <hr/> <p>Service Control</p> <p>Select to open the page from which you can stop or restart Cisco Secure ACS services.</p> <p>[Back to Top]</p>

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

CISCO SYSTEMS **System Configuration**

Edit

Global Authentication Setup

EAP Configuration

PEAP

Allow EAP-MSCHAPv2

Allow EAP-GTC

Cisco client initial message:

PEAP session timeout (minutes):

Enable Fast Reconnect:

EAP-FAST

Allow EAP-FAST

Active master key TTL:

Retired master key TTL:

PAC TTL:

Client initial message:

Authority ID Info:

Allow automatic PAC provisioning:

EAP-FAST master server:

Actual EAP-FAST server status: **Master**

EAP-TLS

Allow EAP-TLS

Select one or more of the following options:

Certificate SAN comparison

Certificate CN comparison

Certificate Binary comparison

EAP-TLS session timeout (minutes):

LEAP

Allow LEAP (For Aironet only)

EAP-MD5

Allow EAP-MD5

AP EAP request timeout (seconds):

MS-CHAP Configuration

Allow MS-CHAP Version 1 Authentication

Allow MS-CHAP Version 2 Authentication

[Back to Help](#)

Help

- [PEAP](#)
- [EAP-FAST](#)
- [EAP-TLS](#)
- [LEAP](#)
- [EAP-MD5](#)
- [AP EAP request timeout](#)
- [MS-CHAP Configuration](#)

This page specifies settings for various authentication protocols.

[\[Back to Top\]](#)

PEAP

Note: PEAP is a certificate-based authentication protocol. PEAP authentication can occur only after you have

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.

The screenshot shows the Cisco 1200 Access Point configuration page. The left sidebar contains a navigation menu with options like HOME, EXPRESS SET-UP, EXPRESS SECURITY, NETWORK MAP, ASSOCIATION, NETWORK INTERFACES, SECURITY, SERVICES, WIRELESS SERVICES, AP, WDS, SYSTEM SOFTWARE, and EVENT LOG. The main content area is titled 'Cisco 1200 Access Point' and shows the configuration for 'Wireless Services: AP'. The hostname is 'Infrastructure_AP' and the time is '10:00:26 Mon Apr 26 2004'. Under 'Participate in SWAN Infrastructure', the 'Enable' radio button is selected. Below this, 'WDS Discovery' is set to 'Auto Discovery', and 'Specified Discovery' is set to 'DISABLED' (IP Address). A red box highlights the 'Username' field containing 'infrastructureap', and the 'Password' and 'Confirm Password' fields. At the bottom, 'L3 Mobility Service via IP/GRE Tunnel' is set to 'Disable'. The 'Apply' and 'Cancel' buttons are visible at the bottom right.

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 défailante. Après qu'AP semble ACTIF et/ou ENREGISTRÉ, ajoutez une méthode d'authentification client au WDS.

Cisco 1200 Access Point

WDS STATUS | SERVER GROUPS | GENERAL SET-UP

Hostname WDS_AP 10:02:01 Mon Apr 26 2004

Wireless Services: WDS - Wireless Domain Services - Status

WDS Information

MAC Address	IP Address	Priority	State
0005.9a38.429f	10.0.0.102	254	Administratively StandAlone - ACTIVE

WDS Registration

APs: 2 Mobile Nodes: 0

AP Information

MAC Address	IP Address	State
000c.8547.b6c7	10.0.0.108	REGISTERED
0005.9a38.429f	10.0.0.102	REGISTERED

Mobile Node Information

MAC Address	IP Address	State	SSID	VLAN ID	BSSID
-------------	------------	-------	------	---------	-------

Wireless Network Manager Information

IP Address	Authentication Status
------------	-----------------------

Refresh

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.

The screenshot shows the Cisco 1200 Access Point configuration page for WDS Server Groups. The page is titled "Cisco 1200 Access Point" and has tabs for "WDS STATUS", "SERVER GROUPS", and "GENERAL SET-UP". The hostname is "WDS_AP" and the date is "10:23:43 Mon Apr 26 2004".

The "Wireless Services: WDS - Server Groups" section contains a "Server Group List" with a table:

< NEW >
Infrastructure
Client

Below the list is a "Delete" button. To the right, the "Server Group Name" is "Client". The "Group Server Priorities" are: Priority 1: 10.0.0.3, Priority 2: < NONE >, Priority 3: < NONE >.

The "Use Group For:" section has two radio buttons: "Infrastructure Authentication" (unselected) and "Client Authentication" (selected). Under "Client Authentication", the "Authentication Settings" are: EAP Authentication (checked), LEAP Authentication (checked), MAC Authentication (unchecked), and Default (Any) Authentication (unchecked). The "SSID Settings" are: "Apply to all SSIDs" (selected) and "Restrict SSIDs (Apply only to listed SSIDs)" (unselected). Under "Restrict SSIDs", there is a text input field with "DISABLED" and "Add" and "Remove" buttons.

At the bottom right, there are "Apply" and "Cancel" buttons.

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.

CISCO SYSTEMS

Cisco 1200 Access Point

RADIO0-802.11B RADIO1-802.11A

Hostname: Infrastructure_AP 10:36:59 Mon Apr 26 2004

HOME
EXPRESS SET-UP
EXPRESS SECURITY
NETWORK MAP +
ASSOCIATION +
NETWORK INTERFACES +
SECURITY
Admin Access
Encryption Manager
SSID Manager
Server Manager
Local RADIUS Server
Advanced Security
SERVICES +
WIRELESS SERVICES +
SYSTEM SOFTWARE +
EVENT LOG +

Security: Encryption Manager - Radio0-802.11B

Encryption Modes

None

WEP Encryption Mandatory

Cisco Compliant TKIP Features: Enable MIC Enable Per Packet Keying

Cipher WEP 128 bit

Encryption Keys

	Transmit Key	Encryption Key (Hexadecimal)	Key Size
Encryption Key 1:	<input checked="" type="radio"/>	<input type="text"/>	128 bit
Encryption Key 2:	<input type="radio"/>	<input type="text"/>	128 bit
Encryption Key 3:	<input type="radio"/>	<input type="text"/>	128 bit
Encryption Key 4:	<input type="radio"/>	<input type="text"/>	128 bit

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

The screenshot displays the Cisco 1200 Access Point configuration interface. The top navigation bar includes the Cisco Systems logo and the title 'Cisco 1200 Access Point'. Below this, there are tabs for 'RADIO0-802.11B' and 'RADIO1-802.11A'. The main content area is divided into several sections: 'HOME', 'EXPRESS SET-UP', 'EXPRESS SECURITY', 'NETWORK MAP', 'ASSOCIATION', 'NETWORK INTERFACES', 'SECURITY', 'Admin Access', 'Encryption Manager', 'SSID Manager', 'Server Manager', 'Local RADIUS Server', 'Advanced Security', 'SERVICES', 'WIRELESS SERVICES', 'SYSTEM SOFTWARE', and 'EVENT LOG'. The 'SSID Manager' section is active, showing 'Security: SSID Manager - Radio0-802.11B'. The 'SSID Properties' section includes a 'Current SSID List' with a table containing one entry: 'infraSSID'. To the right of the list are input fields for 'SSID:' (set to 'infraSSID'), 'VLAN:' (set to '< NONE >'), and 'Network ID:' (set to '(0-4096)'). Below the list are 'Delete-Radio0' and 'Delete-All' buttons. The 'Authentication Settings' section is highlighted with a red box and contains 'Methods Accepted:' with three options: 'Open Authentication' (checked, set to 'with EAP'), 'Shared Authentication' (unchecked, set to '< NO ADDITION >'), and 'Network EAP' (checked, set to '< NO ADDITION >').

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 défectueuse par les clients.

Cisco 1200 Access Point

WDS STATUS | SERVER GROUPS | GENERAL SET-UP

Hostname WDS_AP | 10:49:24 Mon Apr 26 2004

Wireless Services: WDS - Wireless Domain Services - Status

WDS Information

MAC Address	IP Address	Priority	State
0005.9a38.429f	10.0.0.102	254	Administratively StandAlone - ACTIVE

WDS Registration

APs: 2 | Mobile Nodes: 1

AP Information

MAC Address	IP Address	State
000c.8547.b6c7	10.0.0.108	REGISTERED
0005.9a38.429f	10.0.0.102	REGISTERED

Mobile Node Information

MAC Address	IP Address	State	SSID	VLAN ID	BSSID
0030.6527.f74a	10.0.0.25	REGISTERED	infraSSID	-	0007.85b4.113b

Wireless Network Manager Information

IP Address	Authentication Status

Refresh

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 utilisez seulement quand il y a un

problème concernant la synchronisation. Ce sont les configurations recommandées pour le WDS AP : **Radius-server timeout de débranchement**. 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 débranchement**. 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 6
Réponse : 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 deadtime
Réponse : 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](#)