WDS sur la version 15.2(4)JA de points d'accès autonome de Cisco avec l'exemple local de configuration du serveur RADIUS

Contenu

Introduction

Ce document décrit comment configurer le Fonctions Wireless Domain Services (WDS) sur un point d'accès autonome (AP) installé avec un serveur local de RAYON. Le document se concentre sur des configurations par le nouveau GUI, mais fournit également des configurations de l'interface de ligne de commande (CLI).

Conditions préalables

Conditions requises

Cisco recommande que vous ayez la connaissance de la configuration de base GUI et CLI sur des aps autonomes.

Composants utilisés

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

- Point d'accès de gamme de Cisco 3602e sur le logiciel autonome de ® IOS AP, release 15.2(4)JA1 ; ce périphérique agira en tant que WDS AP et serveur local de RAYON.
- Point d'accès de gamme de Cisco 2602i sur l'IOS Software autonome AP, release 15.2(4)JA1 ; ce périphérique agira en tant que client AP WDS.

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.

Configurez

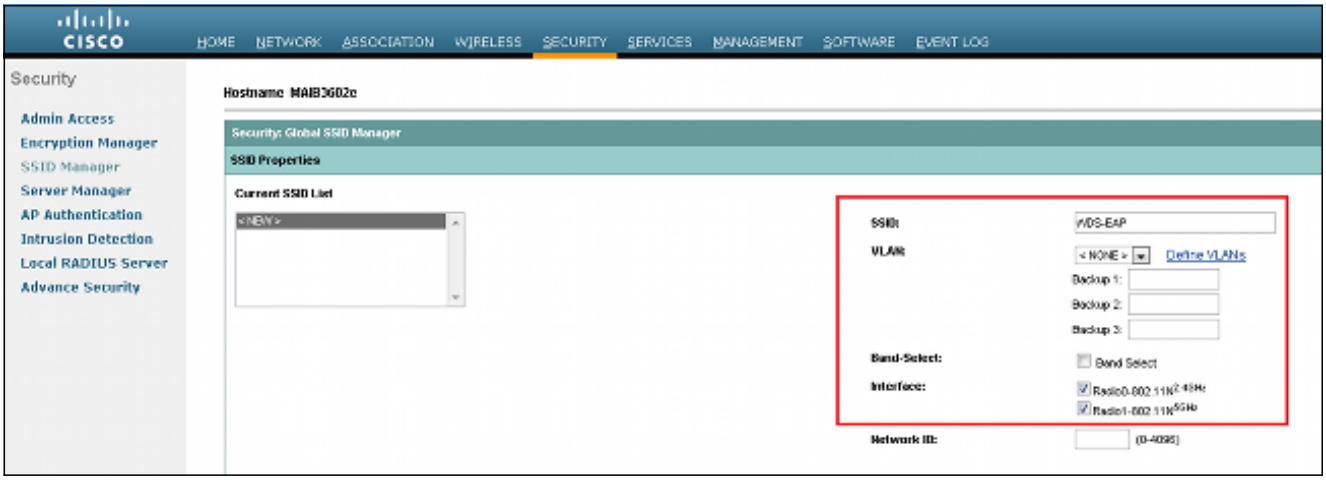
> Remarque: Utilisez l'Outil de recherche de commande (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Configurations GUI

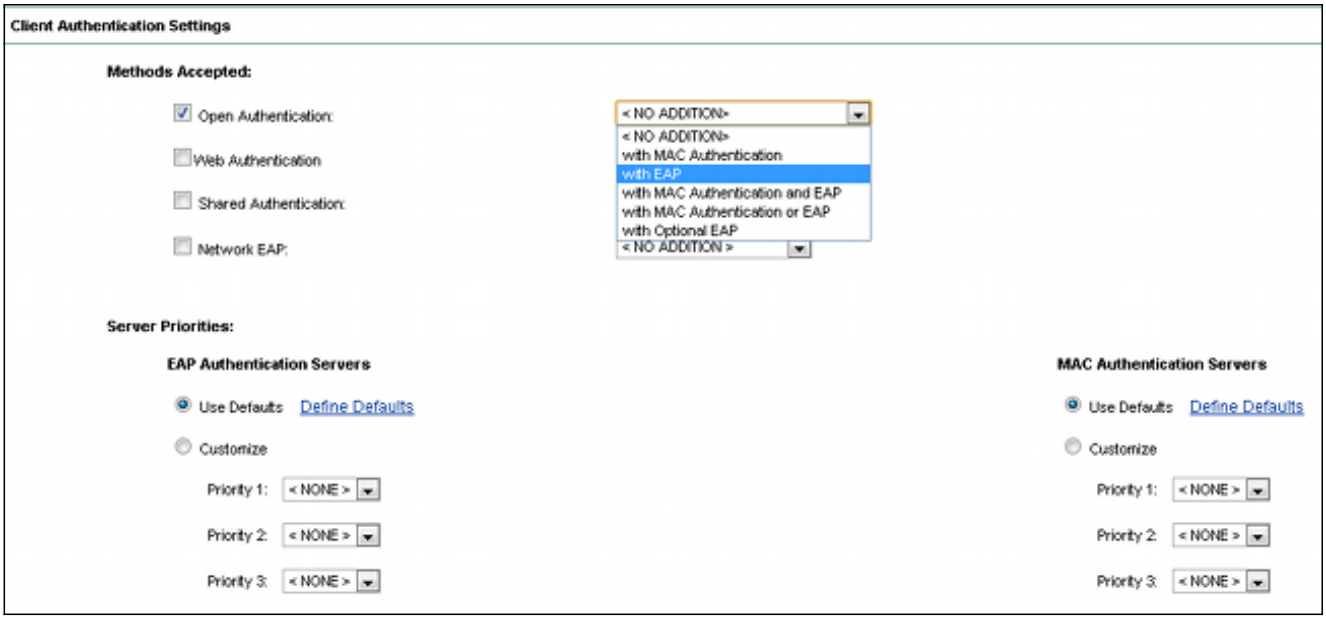
Créez le SSID

Cette procédure décrit comment créer un nouvel Identifiant SSID (Service Set Identifier).

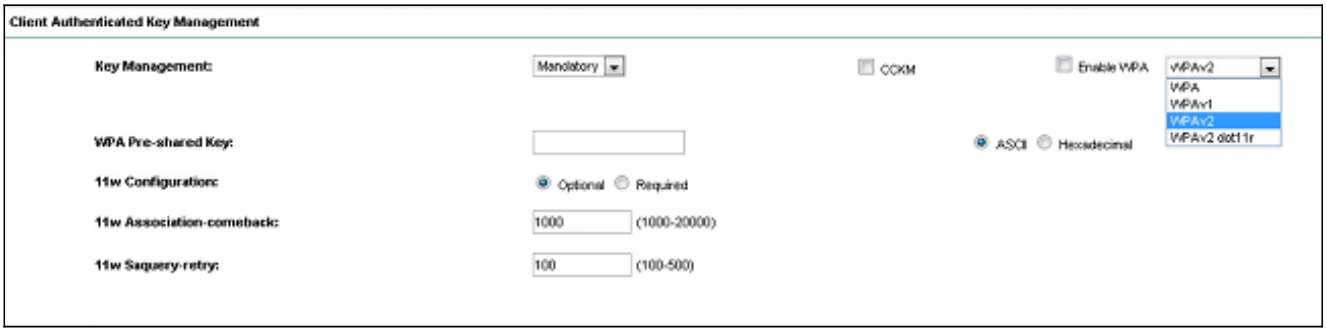
1. Naviguez vers le **Security > SSID Manager**, et cliquez sur New afin de créer un nouveau SSID.



2. Configurez le SSID pour l'authentification de Protocole EAP (Extensible Authentication Protocol).

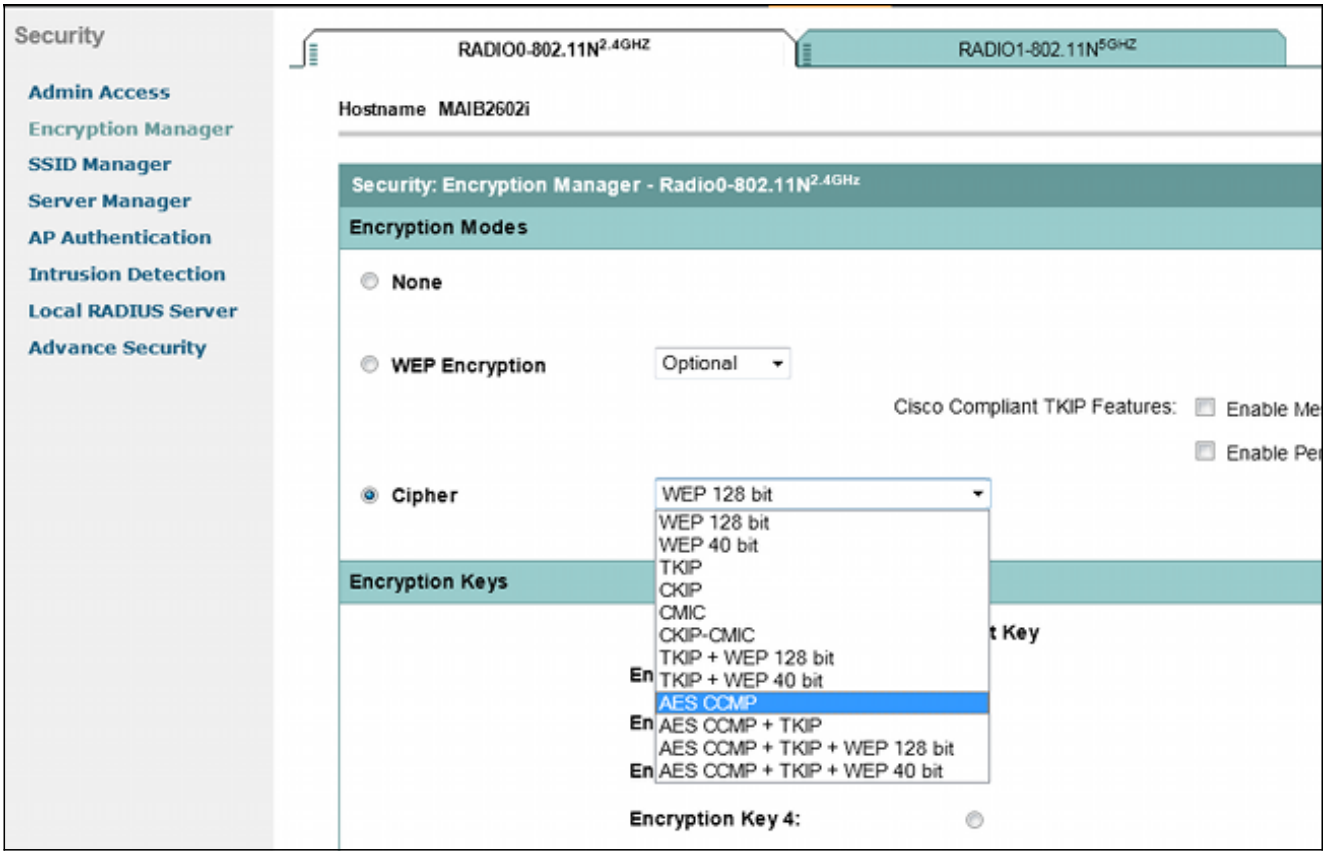


3. Placez le cryptage désiré de niveau. Dans cet exemple, accès protégé par Wi-Fi 2 (WPA2) d'utilisation.



4. Cliquez sur **Apply** afin de sauvegarder les paramètres.

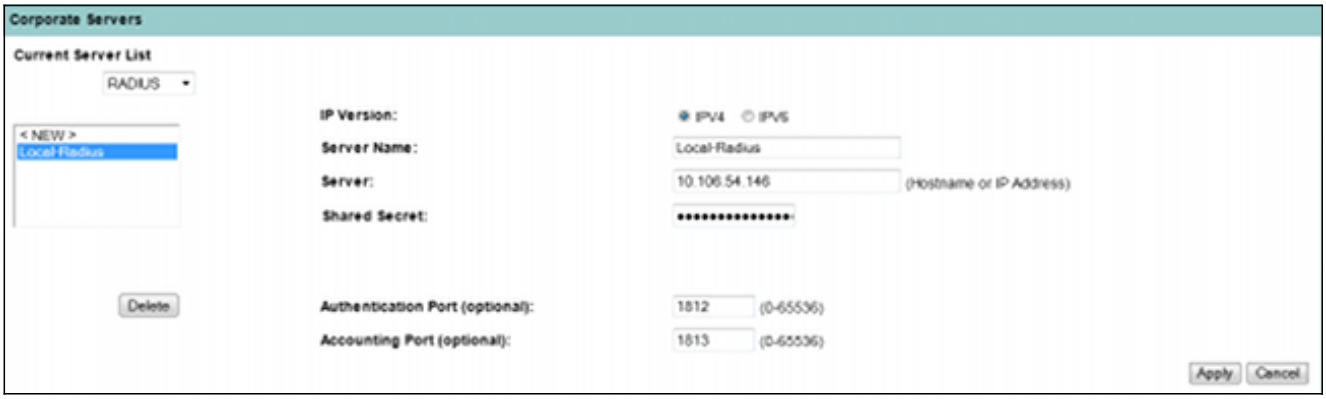
5. Naviguez vers le **Security > Encryption Manager**, et choisissez la méthode requise de chiffrement de cryptage.



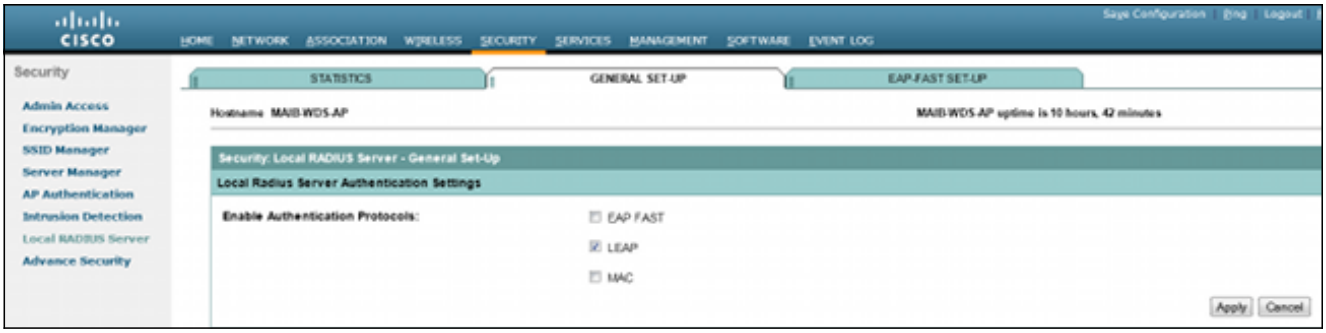
Configuration du serveur RADIUS locale sur WDS AP

Cette procédure décrit comment configurer le serveur local de RAYON sur le WDS AP :

1. Naviguez vers le **Security > Server Manager**, ajoutez l'IP de l'interface virtuelle de passerelle WDS AP (BVI) comme RAYON local, et ajoutez un secret partagé.



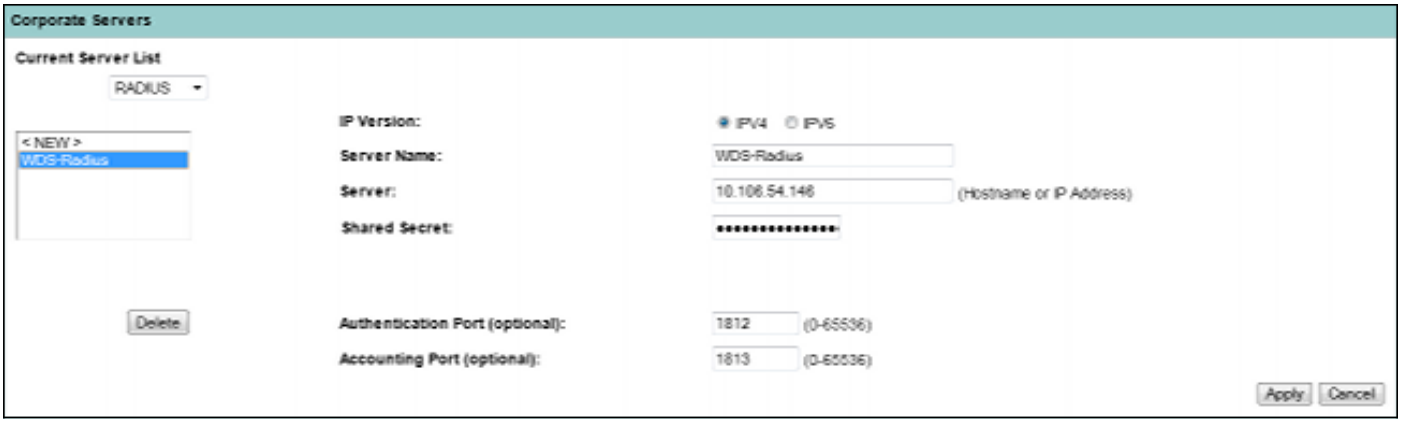
2. Naviguez vers le **Security > Local Radius Server** > la **configuration générale** tableau définissent les protocoles d'EAP que vous souhaitez utiliser. Dans cet exemple, authentification de Light Extensible Authentication Protocol d'enable (LEAP).



3. Vous pouvez également ajouter le serveur d'accès à distance (NAS) IPS et qualifications de nom d'utilisateur/mot de passe de client à la même page. La configuration d'un RAYON local sur un WDS AP est complète.

Configuration du serveur RADIUS locale sur le client AP WDS

Cette figure affiche comment configurer l'adresse IP du WDS AP en tant que serveur de RAYON :



Les deux aps sont maintenant configurés avec le SSID pour l'authentification de LEAP, et le serveur WDS agit en tant que RAYON local. Utilisez les mêmes étapes pour un RAYON externe ; seulement l'IP de serveur de RAYON changera.

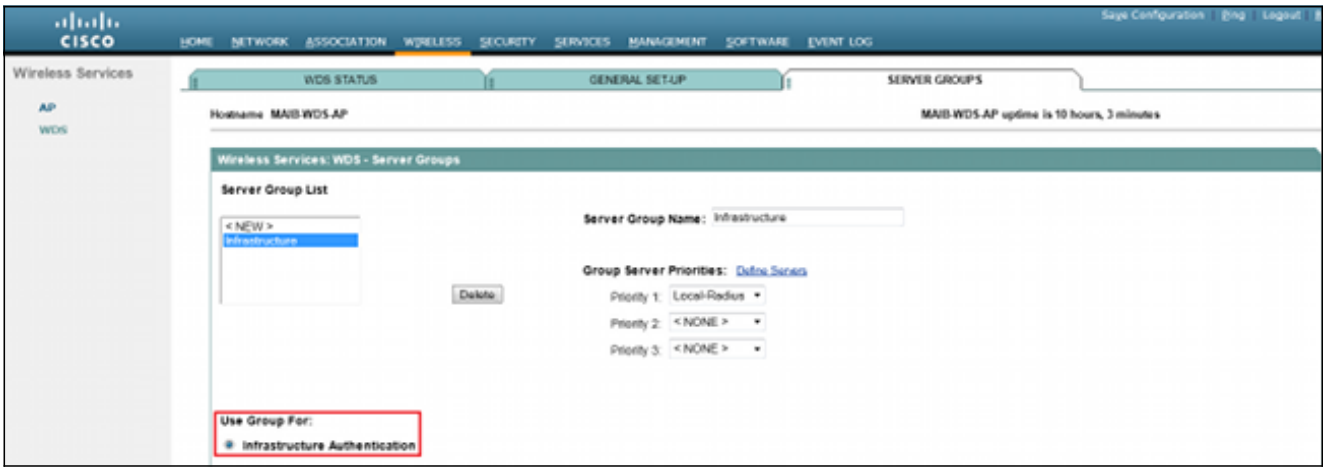
Enable WDS sur WDS AP

Cette procédure décrit comment activer le WDS sur le WDS AP :

1. Naviguez vers la **radio** > le **WDS** > l'onglet de **configuration générale**, et activez l'**utilisation de** case **cet AP en tant que services de domaine Sans fil**. Ceci active le service WDS sur AP.

2. Dans un réseau avec le multiple WDS aps, employez l'option Sans fil prioritaire de services de domaine afin de définir le WDS primaire et la sauvegarde WDS. La valeur s'étend de 1-255, où 255 est le plus prioritaire.

3. Naviguez vers l'onglet de **groupes de serveurs à la** même page. Créez une liste de groupe de serveurs d'infrastructure, à laquelle tout le client WDS des aps authentifiera. Vous pouvez utiliser le serveur local de RAYON sur le WDS AP à cet effet. Puisqu'on l'a déjà ajouté, il apparaît dans la liste déroulante.



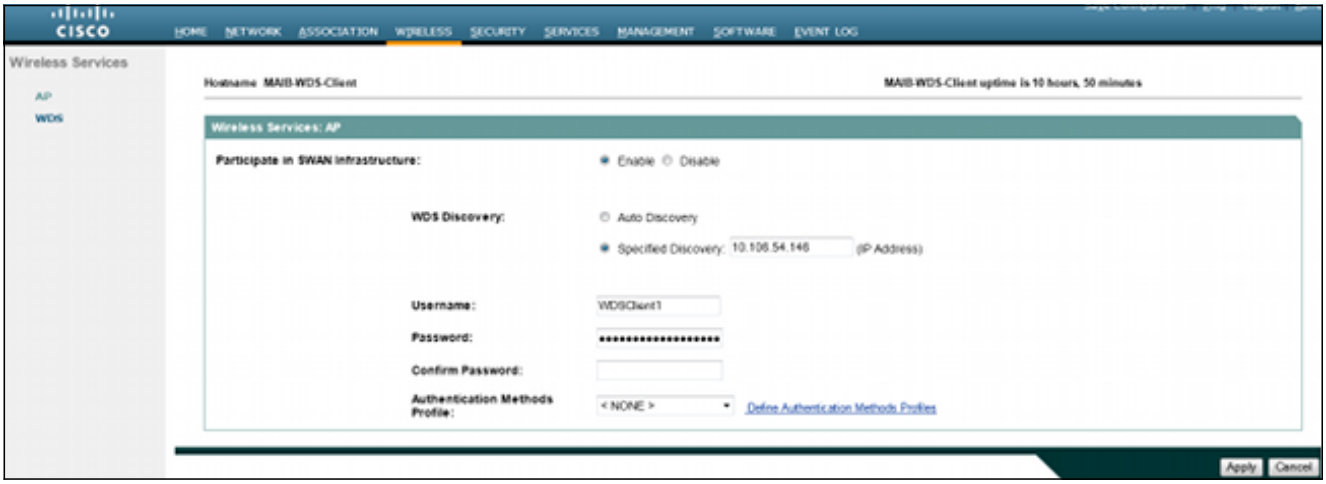
4. Activez le **groupe d'utilisation de** case d'option **pour : L'authentification d'infrastructure**, et cliquent sur Apply afin de sauvegarder les configurations.

5. Le nom d'utilisateur et mot de passe WDS AP peut être ajouté à la liste locale de serveur de RAYON.

Enable WDS sur le client AP WDS

Cette procédure décrit comment activer le WDS sur le client AP WDS :

1. Navigatge au **Wireless > AP**, et activent la case pour **Participate en infrastructure de CYGNE**. Le CYGNE signifie le réseau sans fil structuré.



2. Le client aps WDS mettent en boîte l'automatique découvrent le WDS aps. Ou, vous pouvez manuellement écrire l'adresse IP du WDS AP pour l'enregistrement de client dans la zone de texte **spécifiée de détection**.

   Vous pouvez également ajouter le nom d'utilisateur et mot de passe de client WDS pour l'authentification contre le serveur local de RAYON configuré sur le WDS AP.

Configurations CLI

WDS AP

C'est une configuration d'échantillon pour le WDS AP :

```
Current configuration : 2832 bytes
!
! Last configuration change at 05:54:08 UTC Fri Apr 26 2013
version 15.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname MAIB-WDS-AP
!
!
logging rate-limit console 9
enable secret 5 $1$EdDD$dG47yIKn86GCqmKjFf1Sy0
!
aaa new-model
!
!
aaa group server radius rad_eap
server name Local-Radius
!
aaa group server radius Infrastructure
server name Local-Radius
!
aaa authentication login eap_methods group rad_eap
```

```
aaa authentication login method_Infrastructure group Infrastructure
aaa authorization exec default local
!
!
!
!
!
aaa session-id common
no ip routing
no ip cef
!
!
!
!
dot11 syslog
!
dot11 ssid WDS-EAP
authentication open eap eap_methods
authentication network-eap eap_methods
authentication key-management wpa version 2
guest-mode
!
!
dot11 guest
!
!
!
username Cisco password 7 13261E010803
username My3602 privilege 15 password 7 10430810111F00025D56797F65
!
!
bridge irb
!
!
!
interface Dot11Radio0
no ip address
no ip route-cache
!
encryption mode ciphers aes-ccm
!
ssid WDS-EAP
!
antenna gain 0
stbc
station-role root
bridge-group 1
bridge-group 1 subscriber-loop-control
bridge-group 1 spanning-disabled
bridge-group 1 block-unknown-source
no bridge-group 1 source-learning
no bridge-group 1 unicast-flooding
!
interface Dot11Radio1
no ip address
no ip route-cache
!
encryption mode ciphers aes-ccm
!
ssid WDS-EAP
!
antenna gain 0
peakdetect
dfs band 3 block
```

```
stbc
channel dfs
station-role root
bridge-group 1
bridge-group 1 subscriber-loop-control
bridge-group 1 spanning-disabled
bridge-group 1 block-unknown-source
no bridge-group 1 source-learning
no bridge-group 1 unicast-flooding
!
interface GigabitEthernet0
no ip address
no ip route-cache
duplex auto
speed auto
bridge-group 1
bridge-group 1 spanning-disabled
no bridge-group 1 source-learning
!
interface BVI1
ip address 10.106.54.146 255.255.255.192
no ip route-cache
ipv6 address dhcp
ipv6 address autoconfig
ipv6 enable
!
ip forward-protocol nd
ip http server
no ip http secure-server
ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
ip radius source-interface BVI1
!
!
radius-server local
no authentication eapfast
no authentication mac
nas 10.106.54.146 key 7 045802150C2E1D1C5A
user WDSClient1 nthash 7
072E776E682F4D5D35345B5A227E78050D6413004A57452024017B0803712B224A
!
radius-server attribute 32 include-in-access-req format %h
radius-server vsa send accounting
!
radius server Local-Radius
address ipv4 10.106.54.146 auth-port 1812 acct-port 1813
key 7 060506324F41584B56
!
bridge 1 route ip
!
!
wlccp authentication-server infrastructure method_Infrastructure
wlccp wds priority 254 interface BVI1
!
line con 0
line vty 0 4
transport input all
!
end
```

Client AP WDS

C'est une configuration d'échantillon pour le client AP WDS :

```
Current configuration : 2512 bytes
!
! Last configuration change at 00:33:17 UTC Wed May 22 2013
version 15.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname MAIB-WDS-Client
!
!
logging rate-limit console 9
enable secret 5 $1$vx/M$qP6DY30TGiXmjvUDvKKjk/
!
aaa new-model
!
!
aaa group server radius rad_eap
server name WDS-Radius
!
aaa authentication login eap_methods group rad_eap
aaa authorization exec default local
!
!
!
!
!
aaa session-id common
no ip routing
no ip cef
!
!
!
!
dot11 syslog
!
dot11 ssid WDS-EAP
authentication open eap eap_methods
authentication network-eap eap_methods
authentication key-management wpa version 2
guest-mode
!
!
dot11 guest
!
eap profile WDS-AP
method leap
!
!
!
username Cisco password 7 062506324F41
username My2602 privilege 15 password 7 09414F000D0D051B5A5E577E6A
!
!
bridge irb
!
!
!
interface Dot11Radio0
no ip address
no ip route-cache
!
encryption mode ciphers aes-ccm
```

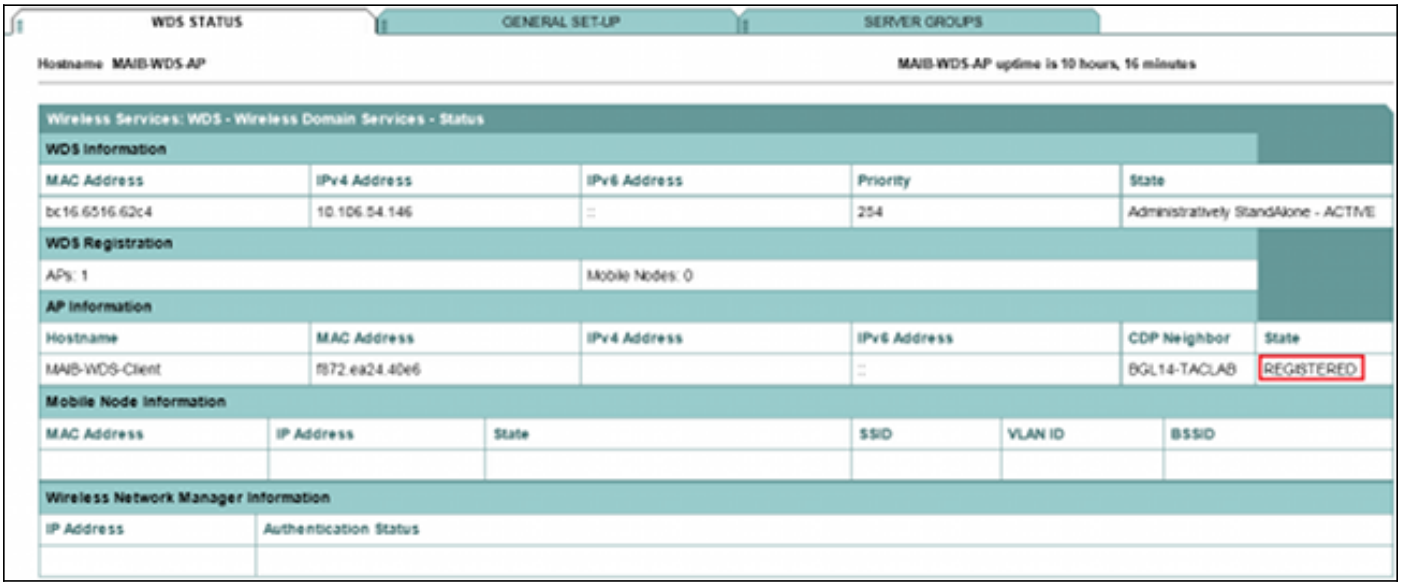
```
!
ssid WDS-EAP
!
antenna gain 0
stbc
station-role root
bridge-group 1
bridge-group 1 subscriber-loop-control
bridge-group 1 spanning-disabled
bridge-group 1 block-unknown-source
no bridge-group 1 source-learning
no bridge-group 1 unicast-flooding
!
interface Dot11Radio1
no ip address
no ip route-cache
!
encryption mode ciphers aes-ccm
!
ssid WDS-EAP
!
antenna gain 0
peakdetect
dfs band 3 block
stbc
channel dfs
station-role root
bridge-group 1
bridge-group 1 subscriber-loop-control
bridge-group 1 spanning-disabled
bridge-group 1 block-unknown-source
no bridge-group 1 source-learning
no bridge-group 1 unicast-flooding
!
interface GigabitEthernet0
no ip address
no ip route-cache
duplex auto
speed auto
bridge-group 1
bridge-group 1 spanning-disabled
no bridge-group 1 source-learning
!
interface BVI1
ip address 10.106.54.136 255.255.255.192
no ip route-cache
ipv6 address dhcp
ipv6 address autoconfig
ipv6 enable
!
ip forward-protocol nd
ip http server
no ip http secure-server
ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
ip radius source-interface BVI1
!
!
radius-server attribute 32 include-in-access-req format %h
radius-server vsa send accounting
!
radius server WDS-Radius
address ipv4 10.106.54.146 auth-port 1812 acct-port 1813
key 7 110A1016141D5A5E57
!
```

```
bridge 1 route ip
!
!
wlccp ap username WDSClient1 password 7 070C285F4D06485744
wlccp ap wds ip address 10.106.54.146
!
line con 0
line vty 0 4
transport input all
!
end
```

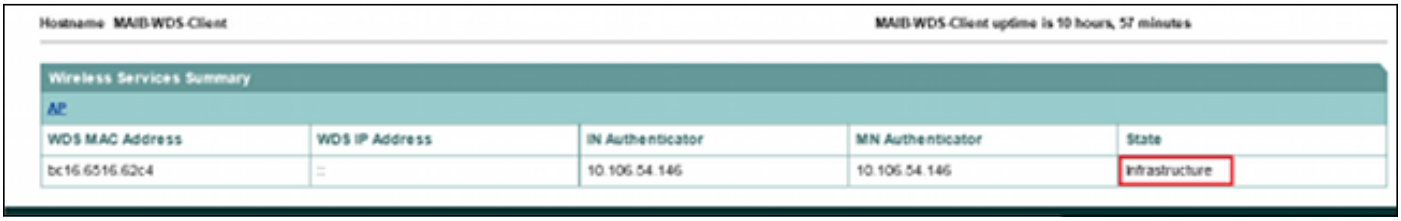
Vérifiez

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration. Une fois que l'installation est complète, le client AP WDS devrait pouvoir s'enregistrer au WDS AP.

Sur le WDS AP, l'état WDS est affiché comme enregistré.



Sur le client AP WDS, l'état WDS est infrastructure.



> Remarque: L'Output Interpreter Tool (clients enregistrés seulement) prend en charge certaines **commandes show**. Utilisez l'Output Interpreter Tool afin de visualiser une analyse de sortie de commande show.

Vérification CLI sortie sur WDS AP

Cette procédure affiche comment vérifier la configuration WDS AP :

```
MAIB-WDS-AP#sh wlccp wds ap

HOSTNAME MAC-ADDR IP-ADDR IPV6-ADDR STATE
MAIB-WDS-Client f872.ea24.40e6 10.106.54.136 :: REGISTERED

MAIB-WDS-AP#sh wlccp wds statistics

WDS Statistics for last 10:34:13:
Current AP count: 1
Current MN count: 0
AAA Auth Attempt count: 2
AAA Auth Success count: 2
AAA Auth Failure count: 0
MAC Spoofing Block count: 0
Roaming without AAA Auth count: 0
Roaming with full AAA Auth count:0
Fast Secured Roaming count: 0
MSC Failure count: 0
KSC Failure count: 0
MIC Failure count: 0
RN Mismatch count: 0
```

Vérification CLI sortie sur le client AP WDS

Cette procédure affiche comment vérifier la configuration du client AP WDS :

```
MAIB-WDS-Client#sh wlccp ap

WDS = bc16.6516.62c4, IP: 10.106.54.146 , IPV6: ::
state = wlccp_ap_st_registered
IN Authenticator = IP: 10.106.54.146 IPV6: ::
MN Authenticator = IP: 10.106.54.146 IPv6::
```

Dépannez

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