# WDS en la versión 15.2(4)JA autónoma de los Puntos de acceso de Cisco con el ejemplo local de la configuración de servidor de RADIUS

## Contenido



## Introducción

Este documento describe cómo configurar el Wireless Domain Services (WDS) en un punto de acceso autónomo puesto con un servidor de RADIUS local. El documento se centra en las configuraciones con el nuevo GUI, pero también proporciona las configuraciones del comando line interface(cli).

## Prerequisites

### Requisitos

Cisco recomienda que usted tiene el conocimietno básico GUI y configuración CLI en los AP autónomos.

### Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Punto de acceso de las Cisco 3602e Series en el software autónomo AP IOS®, versión 15.2(4)JA1; este dispositivo actuará como WDS AP y servidor de RADIUS local.
- Punto de acceso de las Cisco 2602i Series en el software IOS autónomo AP, versión 15.2(4)JA1; este dispositivo actuará como cliente AP WDS.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

## Configurar

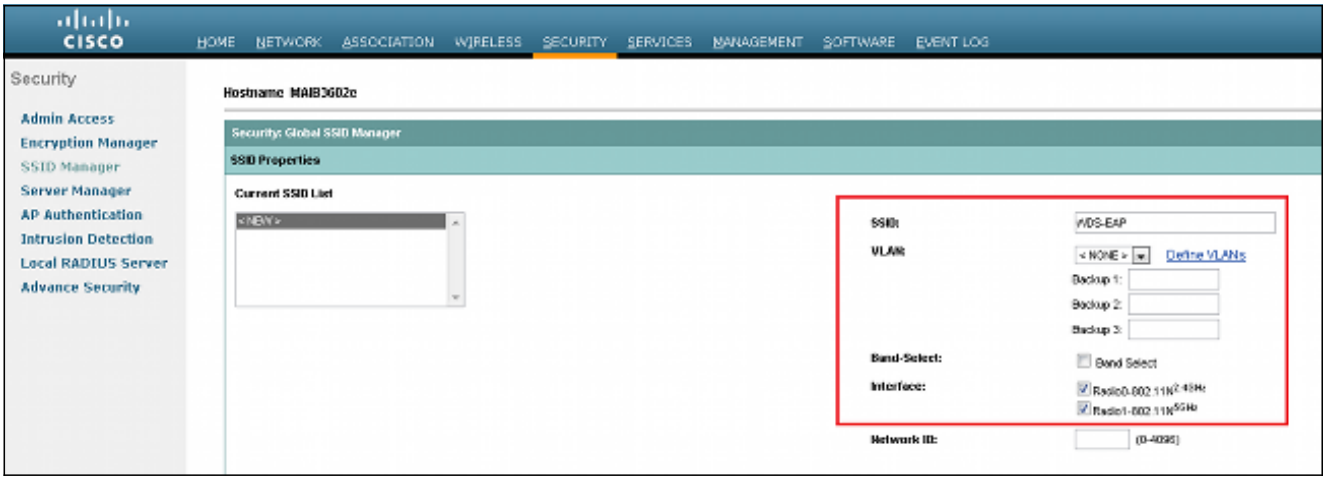
> **Note**: Use la Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos usados en esta sección.

### Configuraciones del GUI

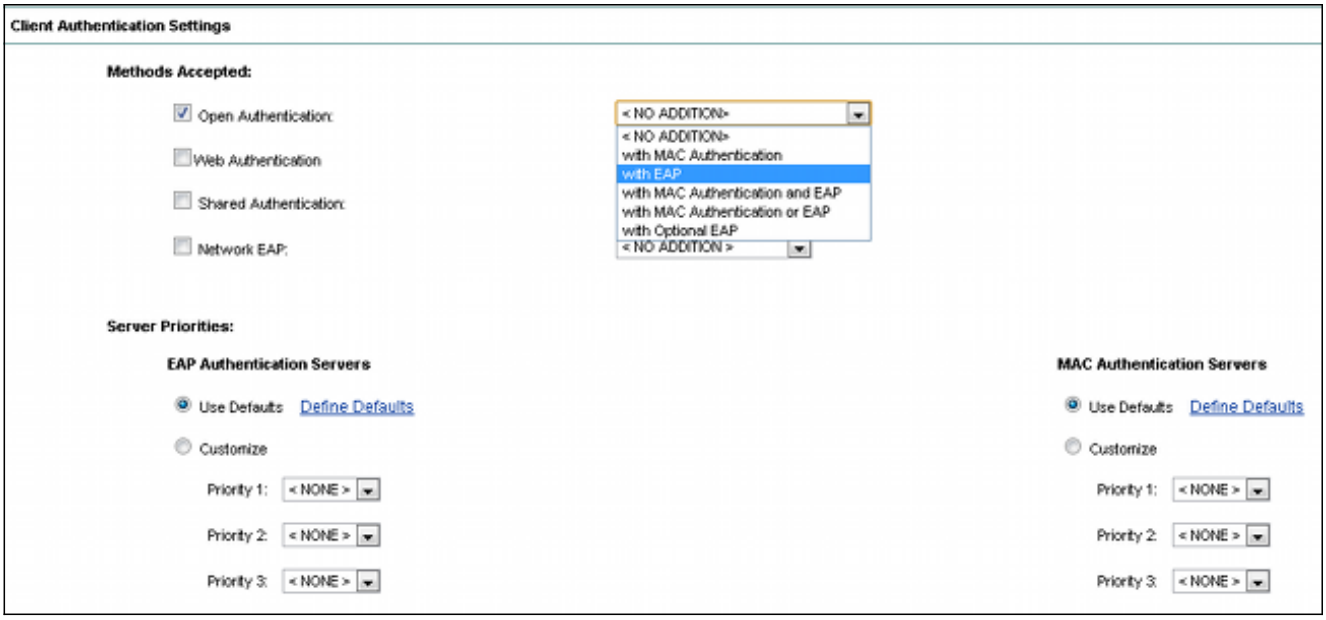
#### Cree el SSID

Este procedimiento describe cómo crear un nuevo Service Set Identifier (SSID).

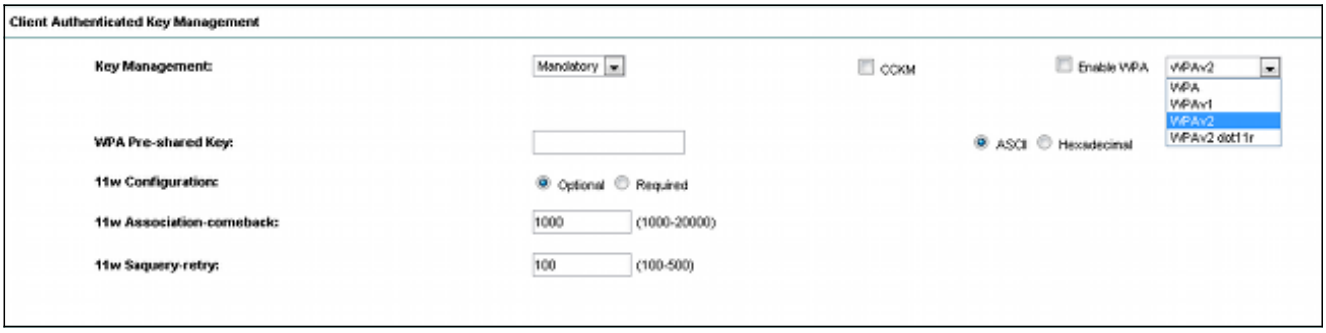
1. Navegue a la **Seguridad** > al **administrador SSID**, y haga clic **NUEVO** para crear un nuevo SSID.




2. Configure el SSID para la autenticación del Protocolo de Autenticación Extensible (EAP).

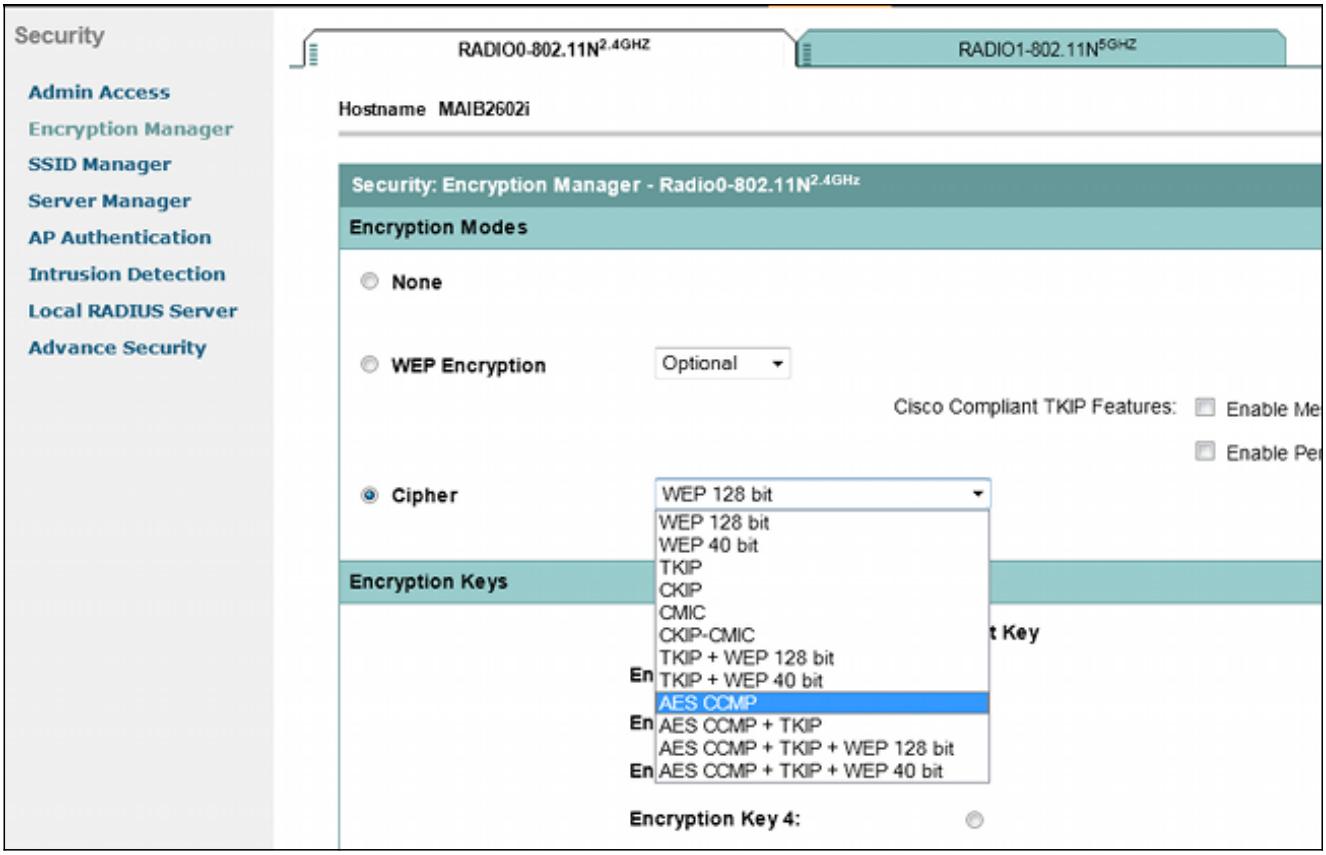



3. Fije el nivel deseado del cifrado. En este ejemplo, utilice el Wi-Fi el acceso protegido 2 (WPA2).




4. Haga clic en **Aplicar** para guardar las configuraciones.

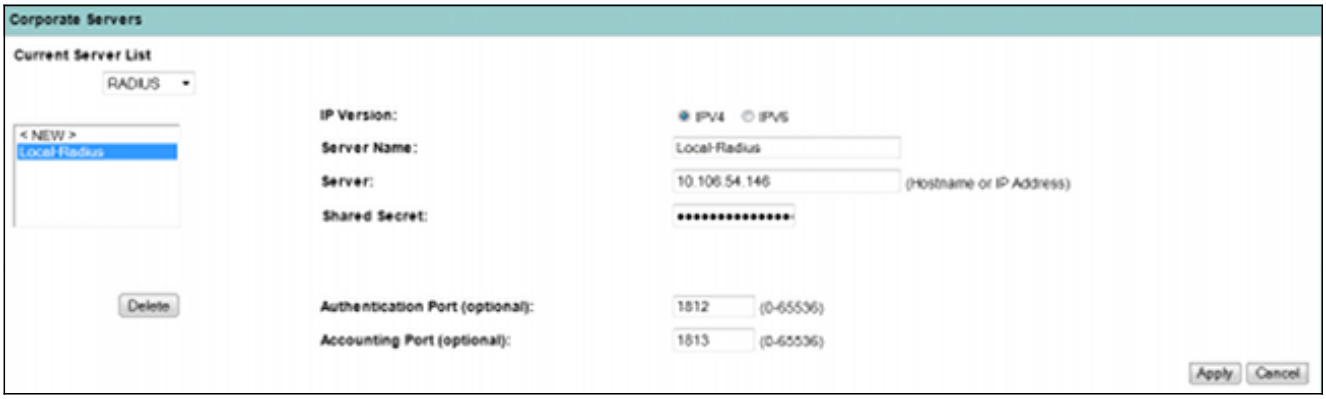
5. Navegue al **administrador de la Seguridad** > del **cifrado**, y elija el método requerido de la cifra del cifrado.



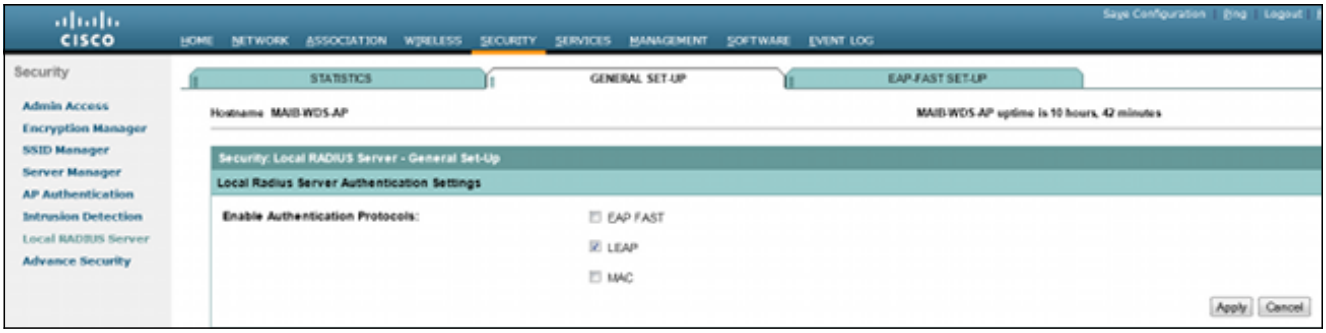

## Configuración de servidor de RADIUS local en WDS AP

Este procedimiento describe cómo configurar al servidor de RADIUS local en el WDS AP:

1. Navegue a la **Seguridad** > al **administrador de servidor**, agregue el IP del (BVI) del Interfaz Virtual de Bridge WDS AP como el RADIUS local, y agregue un secreto compartido.



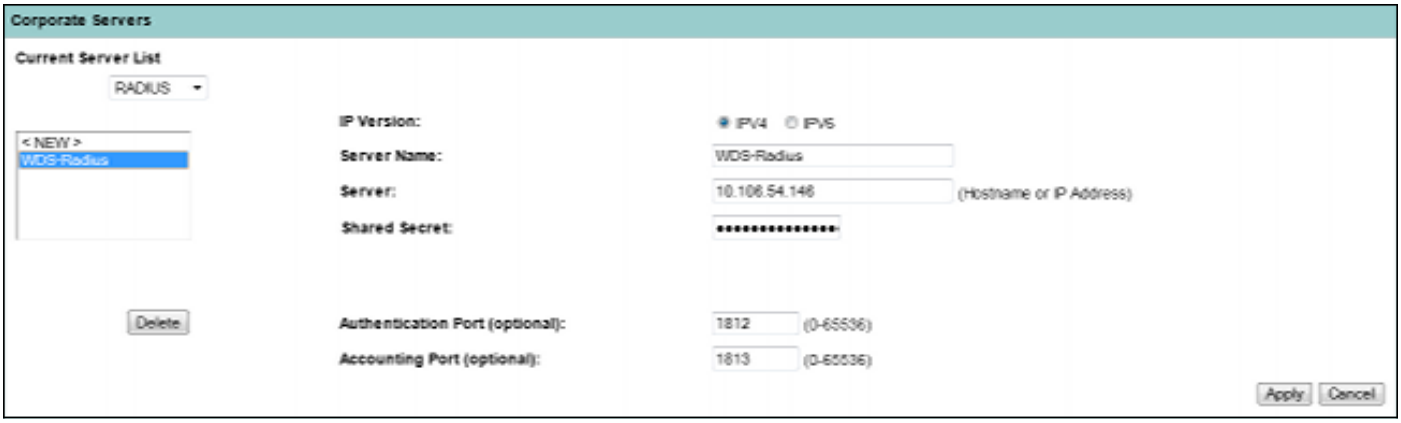

2. Navegue a la **Seguridad > servidor de RADIUS local > configuración general** cuadro definen los protocolos EAP que usted desea utilizar. En este ejemplo, habilite la autenticación del protocolo light extensible authentication (SALTO).




3. Usted puede también agregar el servidor de acceso a la red (NAS) IP y el nombre de usuario del cliente/los credenciales de contraseña en lo mismo página. La configuración de un RADIUS local en un WDS AP es completa.


## Configuración de servidor de RADIUS local en el cliente AP WDS

Esta figura muestra cómo configurar la dirección IP del WDS AP como el servidor de RADIUS:



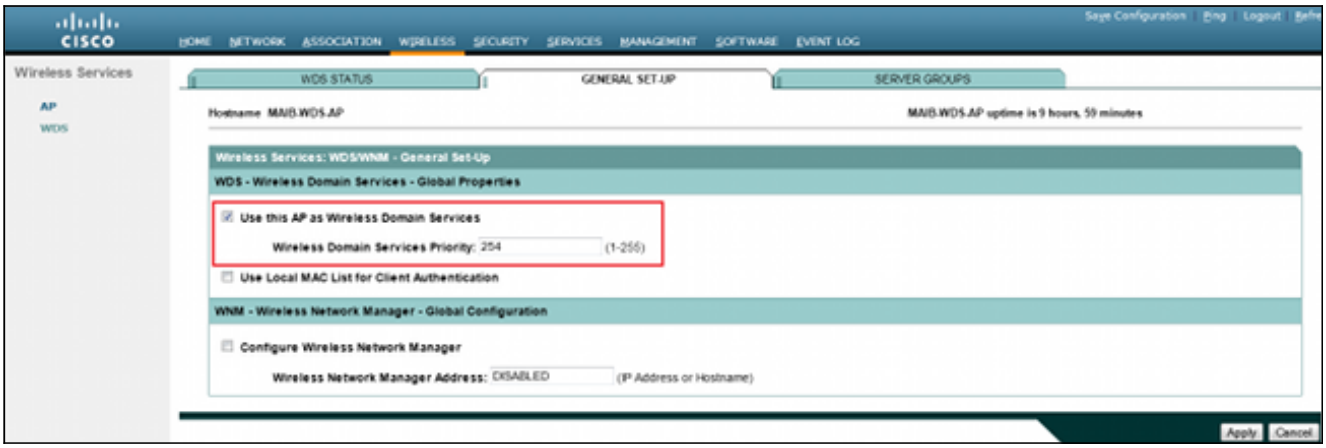

Ambos AP ahora se configuran con los SSID para la autenticación LEAP, y el servidor WDS actúa como el RADIUS local. Utilice los mismos pasos para un externo RADIUS; solamente el IP del servidor de RADIUS cambiará.

## Permiso WDS en WDS AP

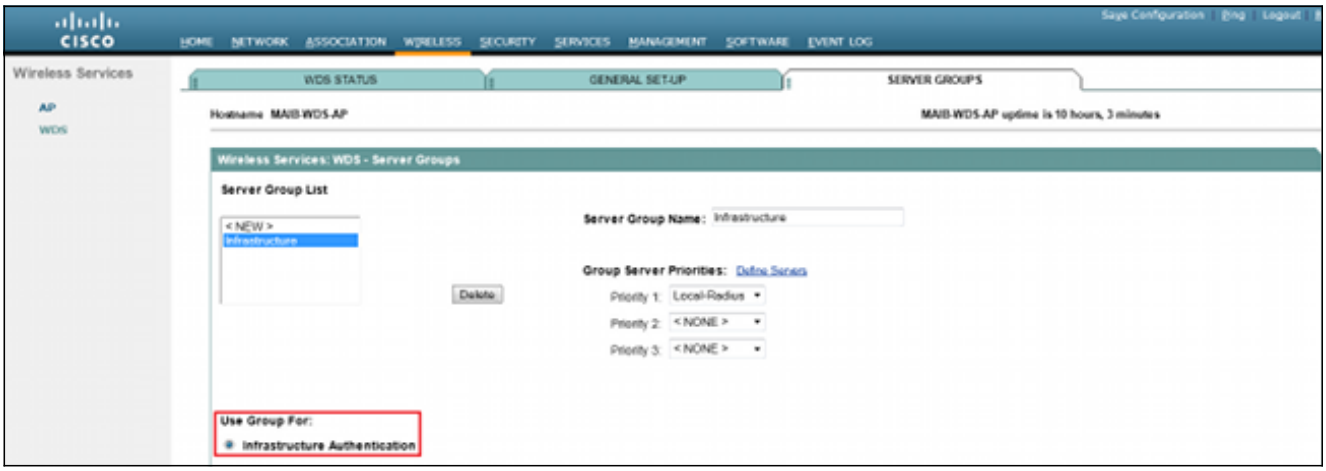
Este procedimiento describe cómo habilitar el WDS en el WDS AP:

1. Navegue a la **Tecnología inalámbrica** > al **WDS** > lengueta **general de la configuración**, y habilite el **uso de la** casilla de verificación **este AP como servicios del dominio de red inalámbrica**. Esto habilita el servicio WDS en el AP.

2. En una red con WDS múltiple AP, utilice la opción de prioridad de los servicios del dominio de red inalámbrica para definir el WDS primario y el respaldo WDS. El valor se extiende a partir de la 1-255, donde está la prioridad más alta 255.




3. Navegue a la lengueta de los **grupos de servidores** en la misma página. Cree una lista del grupo de servidores de la infraestructura, a la cual todo el cliente WDS los AP autenticará. Usted puede utilizar al servidor de RADIUS local en el para este propósito WDS AP. Puesto que se ha agregado ya, aparece en la lista desplegable.



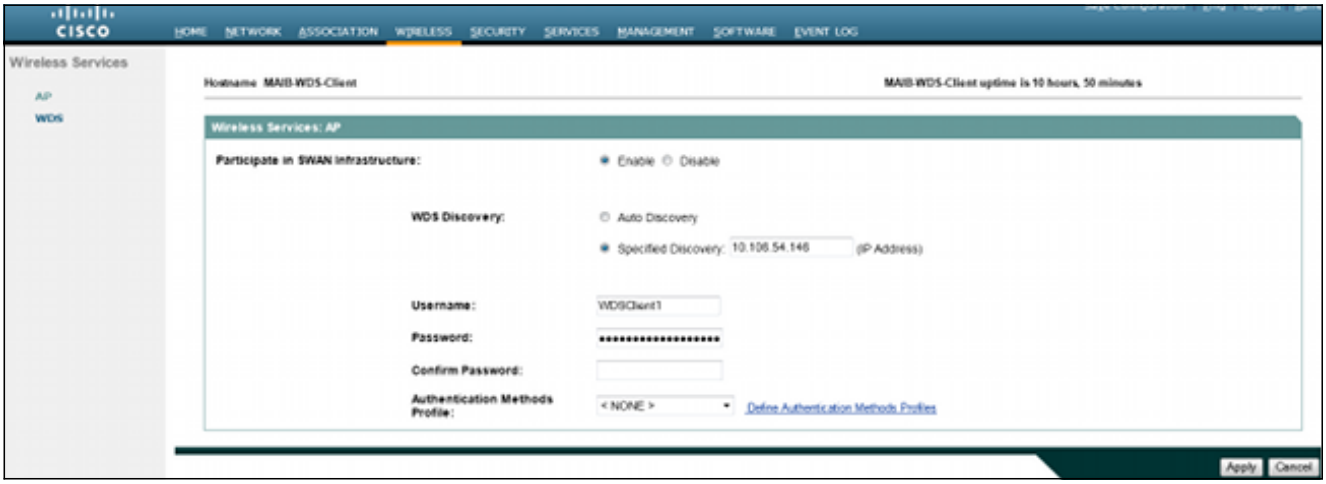

4. Habilite al **grupo del uso del** botón de radio **para: La autenticación de infraestructura**, y el tecleo **se aplican** para salvar las configuraciones.

5. El nombre de usuario y contraseña WDS AP se puede agregar a la lista local del servidor de RADIUS.

### Permiso WDS en el cliente AP WDS

Este procedimiento describe cómo habilitar el WDS en el cliente AP WDS:

1. Navigatge a la **Tecnología inalámbrica >** al **AP**, y habilita la casilla de verificación para **Participate en la infraestructura swan**. La significa del CISNE estructuró la red Tecnología inalámbrica-enterada.




2. El cliente AP WDS puede el auto descubre el WDS AP. O, usted puede ingresar manualmente el IP Address del WDS AP para el registro del cliente en el cuadro de texto **especificado de la detección**.

   Usted puede también agregar el nombre de usuario del cliente y la contraseña para autenticación WDS contra el servidor de RADIUS local configurado en el WDS AP.

## Configuraciones CLI

### WDS AP

Esto es una configuración de muestra para el 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
```

## Cliente AP WDS

Esto es una configuración de muestra para el cliente 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
```

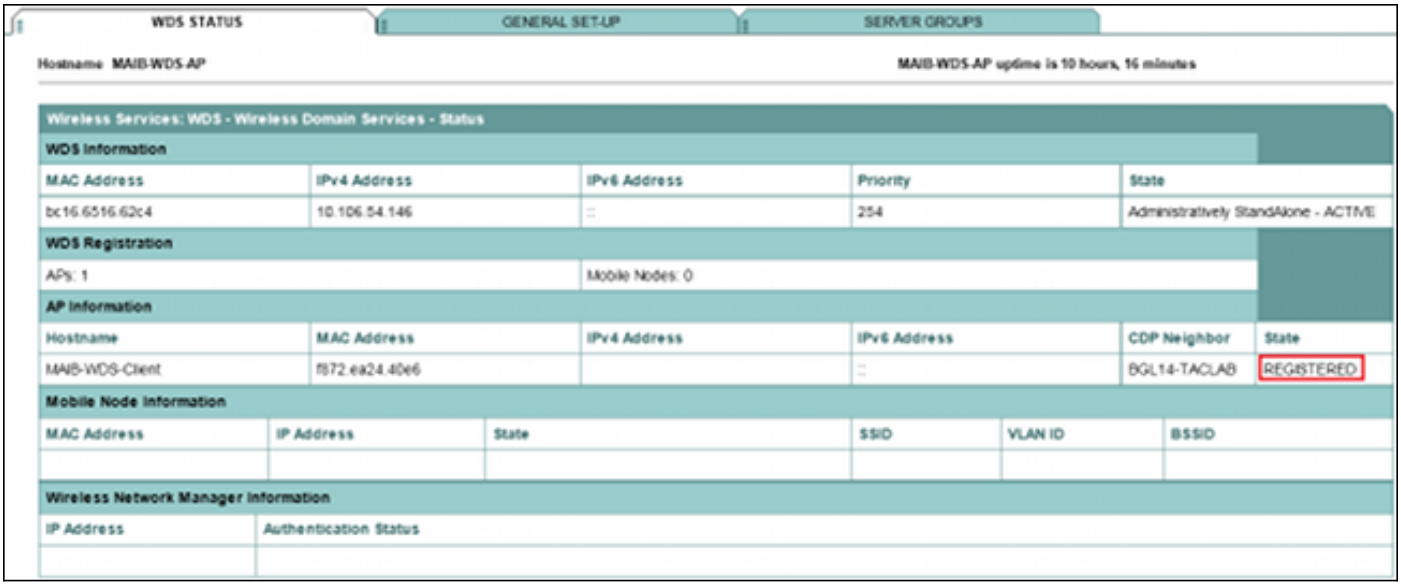
```
no ip address
no ip route-cache
!
encryption mode ciphers aes-ccm
!
ssid WDS-EAP
!
antenna gain 0
stbc
station-role root
bridge-group 1
bridge-group 1 subscriber-loop-control
bridge-group 1 spanning-disabled
bridge-group 1 block-unknown-source
no bridge-group 1 source-learning
no bridge-group 1 unicast-flooding
!
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
```

# Verificación

Use esta sección para confirmar que su configuración funciona correctamente. Una vez que la configuración es completa, el cliente AP WDS debe poder registrarse al WDS AP.

En el WDS AP, muestran el estado WDS según lo registrado.




En el cliente AP WDS, el estado WDS es infraestructura.


> **Note**: La herramienta del Output Interpreter (clientes registrados solamente) apoya los ciertos comandos show. Utilice la herramienta del Output Interpreter para ver una análisis de la salida del comando show.

## Verificación CLI hecha salir en WDS AP

Este procedimiento muestra cómo verificar la configuración 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
```

### Verificación CLI hecha salir en el cliente AP WDS

Este procedimiento muestra cómo verificar la configuración del cliente 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::
```

## Troubleshooting

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.