

# WDS on Cisco Autonomous Access Points Version 15.2(4)JA with Local RADIUS Server Configuration Example



Document ID: 116597

Contributed by Maithri B and Surendra BG, Cisco TAC Engineers.

Oct 18, 2013

## Contents

### Introduction

### Prerequisites

- Requirements

- Components Used

### Configure

- GUI Configurations

  - Create the SSID

  - Local RADIUS Server Configuration on WDS AP

  - Local RADIUS Server Configuration on WDS Client AP

  - Enable WDS on WDS AP

  - Enable WDS on WDS Client AP

- CLI Configurations

  - WDS AP

  - WDS Client AP

### Verify

- CLI Verification Output on WDS AP

- CLI Verification Output on WDS Client AP

### Troubleshoot

## Introduction

This document describes how to configure Wireless Domain Services (WDS) on an autonomous access point (AP) setup with a local RADIUS server. The document focuses on configurations through the new GUI, but also provides command-line interface (CLI) configurations.

## Prerequisites

### Requirements

Cisco recommends that you have knowledge of basic GUI and CLI configuration on autonomous APs.

### Components Used

The information in this document is based on these software and hardware versions:

- Cisco 3602e Series Access Point on Autonomous AP IOS® Software, Release 15.2(4)JA1; this device will act as a WDS AP and local RADIUS server.

- Cisco 2602i Series Access Point on Autonomous AP IOS Software, Release 15.2(4)JA1; this device will act as a WDS client AP.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

## Configure

**Note:** Use the Command Lookup Tool (registered customers only) in order to obtain more information on the commands used in this section.

## GUI Configurations

### Create the SSID

This procedure describes how to create a new Service Set Identifier (SSID).

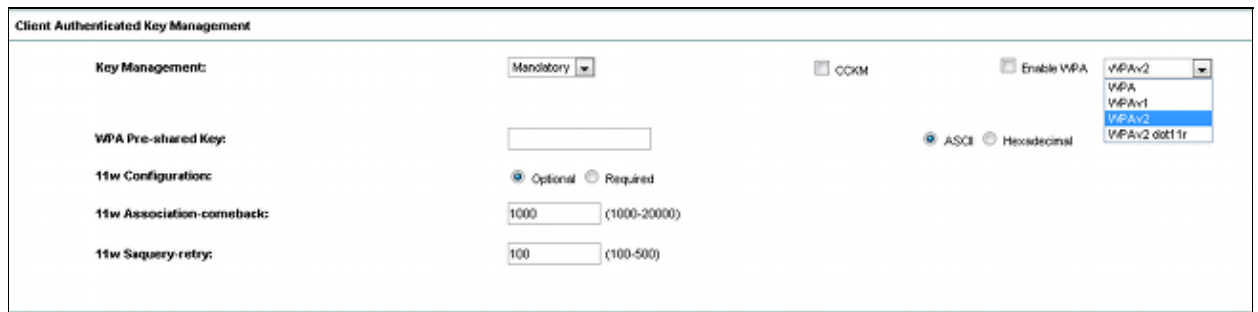
1. Navigate to **Security > SSID Manager**, and click **NEW** in order to create a new SSID.

The screenshot shows the Cisco SSID Manager configuration page. The left sidebar contains navigation links: Admin Access, Encryption Manager, SSID Manager, Server Manager, AP Authentication, Intrusion Detection, Local RADIUS Server, and Advance Security. The main content area is titled "Security Global SSID Manager" and "SSID Properties". It includes a "Current SSID List" with a dropdown menu showing "<NEW>". A red box highlights the configuration fields on the right: SSID (WDS-EAP), VLAN (None), Backup 1, Backup 2, Backup 3, Band Select (Band Select), Interface (Radio0-002.11b/g/43H), and Network ID (0-4095).

2. Configure the SSID for Extensible Authentication Protocol (EAP) authentication.

The screenshot shows the "Client Authentication Settings" page. It includes sections for "Methods Accepted" and "Server Priorities". Under "Methods Accepted", there are checkboxes for Open Authentication, Web Authentication, Shared Authentication, and Network EAP. A dropdown menu is open, showing options: "< NO ADDITION >", "< NO ADDITION > with MAC Authentication", "with EAP" (highlighted), "with MAC Authentication and EAP", "with MAC Authentication or EAP", "with Optional EAP", and "< NO ADDITION >". Under "Server Priorities", there are two sections: "EAP Authentication Servers" and "MAC Authentication Servers". Each section has radio buttons for "Use Defaults" and "Customize", and three priority dropdown menus (Priority 1, Priority 2, Priority 3) all set to "< NONE >".

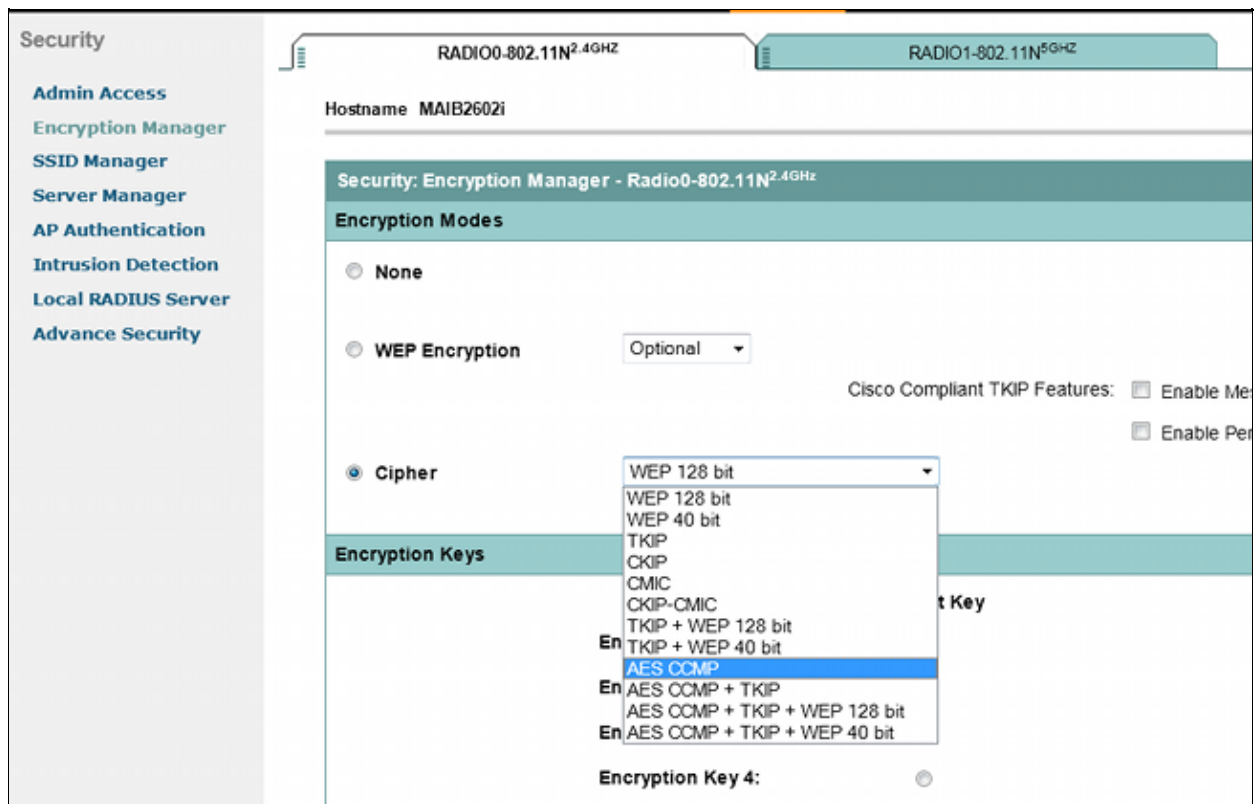
3. Set the desired encryption level. In this example, use Wi-Fi Protected Access 2 (WPA2).



The screenshot shows the 'Client Authenticated Key Management' configuration window. It includes fields for 'Key Management' (set to 'Mandatory'), 'WPA Pre-shared Key', '11w Configurations' (set to 'Optional'), '11w Association-comeback' (set to '1000'), and '11w Saquery-retry' (set to '100'). There are also checkboxes for 'COCKM', 'Enable WPA', and 'Enable WPA2'. A dropdown menu for 'WPA2' is open, showing options: 'WPA2', 'WPA2-PSK', 'WPA2-PSK (AES)', 'WPA2-PSK (TKIP)', 'WPA2-PSK (TKIP+AES)', 'WPA2-PSK (TKIP+AES+CCMP)', and 'WPA2-PSK (TKIP+AES+CCMP+SHA-256)'.

4. Click **Apply** in order to save the settings.

5. Navigate to **Security > Encryption Manager**, and choose the required encryption cipher method.



The screenshot shows the 'Security: Encryption Manager - Radio0-802.11N2.4GHz' configuration window. The left sidebar contains a 'Security' menu with options: 'Admin Access', 'Encryption Manager', 'SSID Manager', 'Server Manager', 'AP Authentication', 'Intrusion Detection', 'Local RADIUS Server', and 'Advance Security'. The main area shows 'Encryption Modes' with radio buttons for 'None', 'WEP Encryption', and 'Cipher'. The 'Cipher' option is selected, and a dropdown menu is open showing options: 'WEP 128 bit', 'WEP 40 bit', 'TKIP', 'CKIP', 'CMIC', 'CKIP-CMIC', 'TKIP + WEP 128 bit', 'TKIP + WEP 40 bit', 'AES CCMP', 'AES CCMP + TKIP', 'AES CCMP + TKIP + WEP 128 bit', and 'AES CCMP + TKIP + WEP 40 bit'. The 'Encryption Keys' section is also visible.

## Local RADIUS Server Configuration on WDS AP

This procedure describes how to configure the local RADIUS server on the WDS AP:

1. Navigate to **Security > Server Manager**, add the WDS AP Bridge Virtual Interface (BVI) IP as the local RADIUS, and add a shared secret.

**Corporate Servers**

Current Server List

RADIUS

< NEW >  
Local-Radius

IP Version: ☒ IPv4 ☐ IPv6

Server Name: Local-Radius

Server: 10.106.54.146 (Hostname or IP Address)

Shared Secret: [redacted]

Authentication Port (optional): 1812 (0-65536)

Accounting Port (optional): 1813 (0-65536)

Delete Apply Cancel

2. Navigate to **Security > Local Radius Server > General Set-Up** tab. Define the EAP protocols you wish to use. In this example, enable Light Extensible Authentication Protocol (LEAP) authentication.

**CISCO** HOME NETWORK ASSOCIATION WIRELESS SECURITY SERVICES MANAGEMENT SOFTWARE EVENT LOG

Security

Admin Access  
Encryption Manager  
SSID Manager  
Server Manager  
AP Authentication  
Intrusion Detection  
Local RADIUS Server  
Advance Security

STATISTICS GENERAL SET-UP EAP-FAST SET-UP

Hostname: MAIB-WDS-AP MAIB-WDS-AP uptime is 10 hours, 42 minutes

Security: Local RADIUS Server - General Set-Up

Local Radius Server Authentication Settings

Enable Authentication Protocols:

☐ EAP-FAST

☒ LEAP

☐ MAC

Apply Cancel

3. You can also add Network Access Server (NAS) IPs and client username/password credentials on the same page. The configuration of a local RADIUS on a WDS AP is complete.

**Network Access Servers (AAA Clients)**

Current Network Access Servers

< NEW >  
10.106.54.146

Network Access Server: 10.106.54.146 (IP Address)

Shared Secret: [redacted]

Delete Apply Cancel

**Individual Users**

Current Users

< NEW >  
WDSClient1

Username: [redacted]

Password: [redacted] ☒ Text ☐ NT Hash

Confirm Password: [redacted]

Group Name: < NONE >

☐ MAC Authentication Only

Delete Apply Cancel

## Local RADIUS Server Configuration on WDS Client AP

This figure shows how to configure the IP address of the WDS AP as the RADIUS server:

**Corporate Servers**

Current Server List

RADIUS

Server Name	Server	Shared Secret	Authentication Port (optional)	Accounting Port (optional)
WDS-Radius	10.106.54.146	*****	1812	1813

IP Version: ☒ IPv4 ☐ IPv6

Server Name: WDS-Radius

Server: 10.106.54.146 (Hostname or IP Address)

Shared Secret: \*\*\*\*\*

Authentication Port (optional): 1812 (0-65536)

Accounting Port (optional): 1813 (0-65536)

Buttons: Delete, Apply, Cancel

Both APs are now configured with SSIDs for LEAP authentication, and the WDS server acts as the local RADIUS. Use the same steps for an external RADIUS; only the RADIUS server IP will change.

## Enable WDS on WDS AP

This procedure describes how to enable WDS on the WDS AP:

1. Navigate to **Wireless > WDS > General Set-Up** tab, and enable the check box **Use this AP as Wireless Domain Services**. This enables the WDS service on the AP.
2. In a network with multiple WDS APs, use the Wireless Domain Services Priority option in order to define the primary WDS and the backup WDS. The value ranges from 1–255, where 255 is the highest priority.

**CISCO**

HOME NETWORK ASSOCIATION **WIRELESS** SECURITY SERVICES MANAGEMENT SOFTWARE EVENT LOG

Wireless Services

AP

WDS

WDS STATUS GENERAL SET-UP SERVER GROUPS

Hostname: MAIB.WDS.AP

MAIB.WDS.AP uptime is 9 hours, 59 minutes

Wireless Services: WDS/WHM - General Set-Up

WDS - Wireless Domain Services - Global Properties

☒ Use this AP as Wireless Domain Services

Wireless Domain Services Priority: 254 (1-255)

☐ Use Local MAC List for Client Authentication

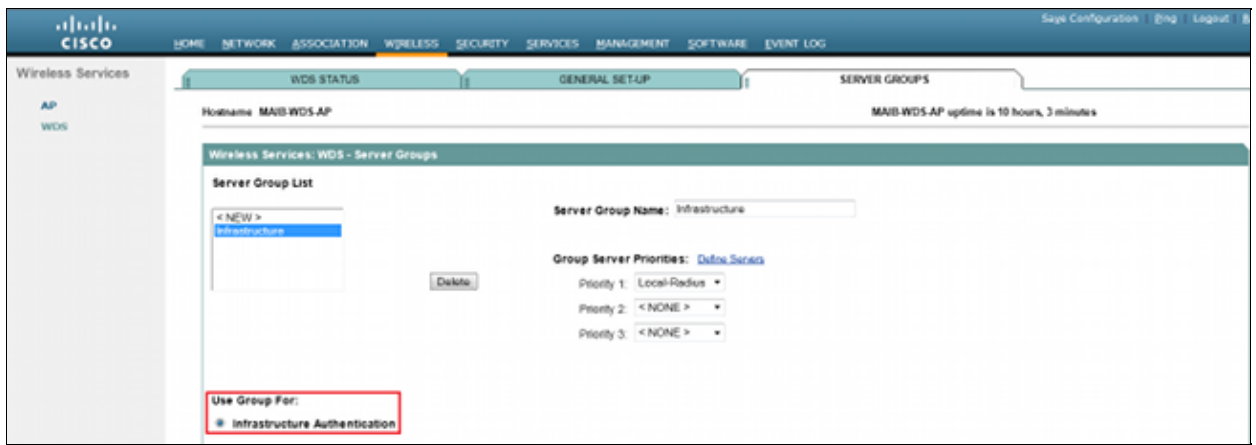
WNM - Wireless Network Manager - Global Configuration

☐ Configure Wireless Network Manager

Wireless Network Manager Address: DISABLED (IP Address or Hostname)

Buttons: Apply, Cancel

3. Navigate to the **Server Groups** tab on the same page. Create an infrastructure server group list, to which all the WDS client APs will authenticate. You can use the local RADIUS server on the WDS AP for this purpose. Since it has already been added, it appears in the drop-down list.

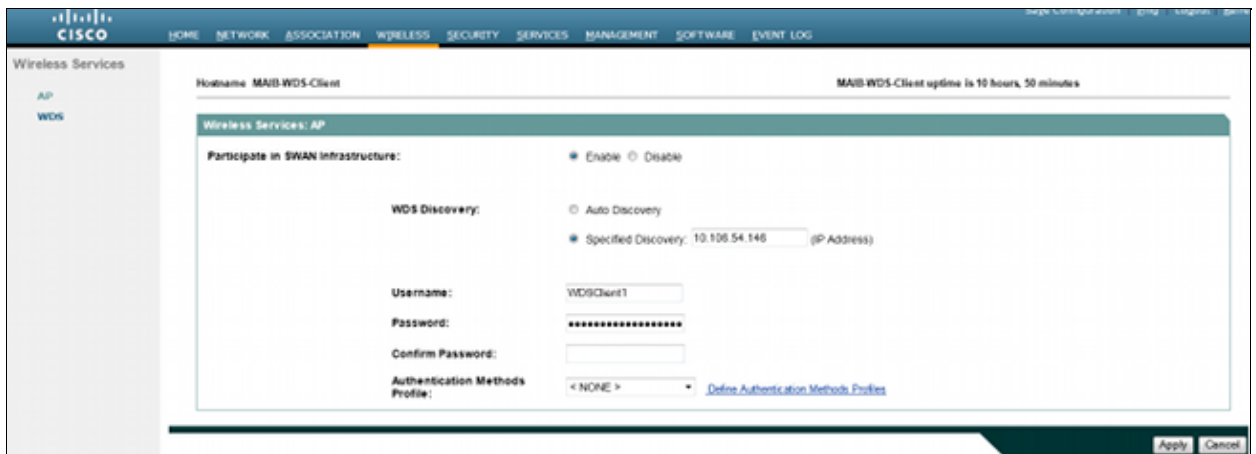


4. Enable the radio button *Use Group For: Infrastructure Authentication*, and click *Apply* in order to save the settings.
5. The WDS AP username and passwords can be added to the local RADIUS server list.

## Enable WDS on WDS Client AP

This procedure describes how to enable WDS on the WDS client AP:

1. Navigatge to *Wireless > AP*, and enable the check box for *Participate in SWAN Infrastructure*. SWAN stands for Structured Wireless–Aware Network.



2. WDS client APs can auto discover the WDS APs. Or, you can manually enter the IP address of the WDS AP for client registration in the *Specified Discovery* text box.

You can also add the WDS client username and password for authentication against the local RADIUS server configured on the WDS AP.

## CLI Configurations

### WDS AP

This is a sample configuration for the 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

```

## WDS Client AP

This is a sample configuration for the WDS client AP:

```

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 $l$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  
!
```



**Note:** The Output Interpreter Tool (registered customers only) supports certain *show* commands. Use the Output Interpreter Tool in order to view an analysis of *show* command output.

## CLI Verification Output on WDS AP

This procedure shows how to verify the WDS AP configuration:

```
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
```

## CLI Verification Output on WDS Client AP

This procedure shows how to verify the WDS client AP configuration:

```
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::
```

## Troubleshoot

There is currently no specific troubleshooting information available for this configuration.