# Configurar WDS em APs autônomos com servidor RADIUS local

# Contents

Introduction **Prerequisites Requirements** Componentes Utilizados Configurar Configurações GUI Crie o SSID Configuração de servidor RADIUS local no AP WDS Configuração de servidor RADIUS local no AP cliente WDS Ativar WDS no WDS AP Ativar WDS no AP do cliente WDS Configurações de CLI **AP WDS** AP de cliente WDS Verificar Saída de verificação CLI no AP WDS Saída de verificação CLI no AP cliente WDS **Troubleshoot** 

# Introduction

Este documento descreve como configurar o Wireless Domain Services (WDS) em uma configuração de ponto de acesso autônomo (AP) com um servidor RADIUS local. O documento se concentra em configurações através da nova GUI, mas também fornece configurações de interface de linha de comando (CLI).

# Prerequisites

### Requirements

A Cisco recomenda que você tenha conhecimento da configuração básica de GUI e CLI em APs autônomos.

### **Componentes Utilizados**

As informações neste documento são baseadas nestas versões de software e hardware:

- Access Point Cisco 3602e Series em Software autônomo AP IOS<sup>®</sup>, versão 15.2(4)JA1; este dispositivo atuará como um AP WDS e servidor RADIUS local.
- Access Point Cisco 2602i Series em Software IOS AP autônomo, versão 15.2(4)JA1; este dispositivo atuará como um AP cliente WDS.

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.

# Configurar

Note: Use a <u>Command Lookup Tool (somente clientes registrados) para obter mais</u> informações sobre os comandos usados nesta seção.

### Configurações GUI

#### Crie o SSID

Este procedimento descreve como criar um novo SSID (Service Set Identifier).

1. Navegue até Security > SSID Manager e clique em NEW para criar um novo SSID.

uluili. cisco	Home Network Association Wireless Security Services Management	SOFTWARE EVENT LOG	
Security	Hostname MAIBJGD2e		
Encryption Manager SSID Manager	Security: Global SSD Manager SSD Properties		
Server Manager AP Authentication Intrusion Detection Local RADIUS Server	Corrent SHD Liet	SSID: VLAN:	WDS-EAP
Advance Security	×	Band-Select:	Backup 2:
		Interface:	Reside 602 11N <sup>2 48Hz</sup> Reside 1-602 11N <sup>25Hz</sup>
		Helwork ID:	(0-4036)

2. Configure o SSID para autenticação EAP (Extensible Authentication Protocol).

Client Authentication Settings		
Methods Accepted:		
Open Authentication:	< NO ADDITION>	
Web Authentication	with MAC Authentication	
Shared Authentication:	with MAC Authentication and EAP with MAC Authentication or EAP	
Network EAP:	<no addition=""></no>	
Server Priorities:		
EAP Authentication Servers		MAC Authentication Servers
Use Defaults <u>Define Defaults</u>		Use Defaults Define Defaults
Custonize		Customize
Priority 1: < NONE > .		Priority 1: < NONE >
Priority 2: < NONE > x		Priority 2: < NONE > 💌
Priority 3: < NONE > 💌		Priority 3. < NONE >

3. Defina o nível de criptografia desejado. Neste exemplo, use o WPA2 (Wi-Fi Protected Access 2).

Client Authenticated Key Management			
Key Management:	Mandatory 💌	ССКМ	Enable WPA V/Pav2  WPA WPAv1
WPA Pre-shared Key:			ASCI      Hexadecinal
11w Configuration:	Optional		
11w Association-comeback:	1000 (1000-20000)		
11w Saquery-retry:	100 (100-500)		

- 4. Clique em Aplicar para salvar as configurações.
- 5. Navegue até **Security > Encryption Manager** e escolha o método de criptografia necessário.

Security	RADIO0-802.11	N <sup>2.4GHZ</sup>	RADIO1-802.11N5GHZ	
Admin Access Encryption Manager	Hostname MAIB2602i			
SSID Manager Server Manager	Security: Encryption Mar	nager - Radio0-802.11N <sup>2.4GHz</sup>		
AP Authentication	Encryption Modes			
Intrusion Detection	None			
Local RADIUS Server Advance Security	© WEP Encryption	Optional -	isco Compliant TKIP Features:	Enable Me
				Enable Per
	Opher	WEP 128 bit	-	
		WEP 128 bit WEP 40 bit		
	Encryption Keys	TKIP		
		CMIC CKIP-CMIC TKIP + WEP 128 bit	t Key	
		AES COMP		
		En AES COMP + TKIP AES COMP + TKIP + WEP 1 En AES COMP + TKIP + WEP 4	28 bit 0 bit	
		Encryption Key 4:	0	

#### Configuração de servidor RADIUS local no AP WDS

Este procedimento descreve como configurar o servidor RADIUS local no AP WDS:

1. Navegue até **Security > Server Manager**, adicione o IP da WDS AP Bridge Virtual Interface (BVI) como o RADIUS local e adicione um segredo compartilhado.

Corporate Servers				
Current Server List RADUS				
	IP Version:	● IPV4 ○ IPV5		
< NEW > Local-Radius	Server Name:	Local-Radius		
	Server:	10.106.54.146	(Hostname or IP Address)	
	Shared Secret:			
Delete	Authentication Port (optional):	1812 (0.655%)		
(2000)	Accounting Boot (antionally	1012 (0 0000)		
	Accounting Port (optional).	1013 (0-60036)		
				Apply Cancel

2. Navegue até **Security > Local Radius Server > General Set-Up** tab. Defina os protocolos EAP que deseja usar. Neste exemplo, ative a autenticação LEAP (Light Extensible Authentication Protocol).

uluulu cisco	ROME	NETWORK	ASSOCIATION	WIRELESS	SECURITY	SERVICES	BANAGEMENT	SOFTWARE	EVENT LOG		Saya Configuration	E Pra I	Logout
Security	1		STATISTICS		1	GEN	IRAL SET-UP			EAP-FAST SET-UP			
Admin Access Encryption Manager	Host	name MAIB	WDS-AP							MAIB WDS AP uptime is 10 hos	urs, 42 minutes		
SSID Manager	54	curity: Loca	I RADIUS Server	- General S	n-Up								
Server Manager	Lo	cal Radius 1	Server Authentic	ation Setting	15								
Intrusion Detection	6	able Authe	ntication Protoc	ols:		0.0	AP FAST						
Local RADIUS Server						R L	LAP						
Advance security						🗉 M	AC						
												Αρρίγ	Cancel

 Você também pode adicionar IPs do Network Access Server (NAS) e credenciais de nome de usuário/senha do cliente na mesma página. A configuração de um RADIUS local em um AP WDS foi concluída.

Network Access Servers (AAA Clients)					
Current Network Access Servers	Network Acces	s Server:	10.106.54.146	(P Address)	
Delete	Shared Secret				
					Apply Cancel
Individual Users					
Current Users	Username: Password: Confirm Password:		● Text © NITHB	55	
Delete	Group Name:	< NONE > •	ation Only		Apply Concel

#### Configuração de servidor RADIUS local no AP cliente WDS

Esta figura mostra como configurar o endereço IP do AP WDS como o servidor RADIUS:

Corporate Servers				
Current Server List				
RADIUS -				
	IP Version:	PV4 0 PV5		
< NEW > WDS-Rodus	Server Name:	WDS-Radius		
	Server:	10.106.54.146	(Hostname or IP Address)	
	Shared Secret:	*******		
Delete	Authentication Port (optional):	1812 (0-65536)		
	Accounting Port (optional):	1813 (0-65536)		
				Apply Cancel

Ambos os APs agora estão configurados com SSIDs para autenticação LEAP, e o servidor WDS atua como o RADIUS local. Use as mesmas etapas para um RADIUS externo; somente o IP do servidor RADIUS será alterado.

#### Ativar WDS no WDS AP

Este procedimento descreve como ativar o WDS no AP WDS:

- 1. Navegue até a guia Wireless > WDS > General Set-Up e ative a caixa de seleção Use this AP as Wireless Domain Services. Isso ativa o serviço WDS no AP.
- 2. Em uma rede com vários APs WDS, use a opção Wireless Domain Services Priority para definir o WDS principal e o WDS de backup. O valor varia de 1 a 255, onde 255 é a prioridade mais alta.

uluilu cisco	Bone Betwook Resocration Werless Secrety Services Ranagement Software Event Log
Wireless Services	WOS STATUS
AP WDS	Hostname MAIB-WDS-AP MAIB-WDS-AP uptime is 9 hours, 59 minutes
	Wireless Services: WDS/WNM - 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; DBABLED (P Address or Hostname)
	Apply Quer

3. Navegue até a guia Server Groups na mesma página. Crie uma lista de grupos de servidores de infraestrutura, para a qual todos os APs de clientes WDS serão autenticados. Você pode usar o servidor RADIUS local no AP WDS para essa finalidade. Como já foi adicionado, ele aparece na lista suspensa.

uludu cisco	HOME NETWORK ASSOCIATION WIR	illiss sicurity survice	S MANAGEMENT SOFTWAR	EVENT LOG	Saye Configuration   Eng   Logout   B
Wireless Services	WDS STATUS	() CI	INERAL SET-UP	SERVER GROUPS	<u> </u>
AP WDS	Hostname MAIB WDS-AP			MAIB-WDS-AP uptime is 1	0 hours, 3 minutes
	Wireless Services: WDS - Server Gr	oups			
	Server Group List				
	< NEW > Intrastructure	Sec	ver Group Name: Infrastructure		
		Gri	oup Server Priorities: Dates Se	065	
		Delote	Priority 1: Local-Radius .		
			Priority 2: <none> +</none>		
			Priority 3: < NONE > +		
	Use Group For:				
	Infrastructure Authentication				

- 4. Ative o botão de opção Usar grupo para: Infrastructure Authentication e clique em Apply para salvar as configurações.
- 5. O nome de usuário e as senhas do AP WDS podem ser adicionados à lista de servidores RADIUS local.

#### Ativar WDS no AP do cliente WDS

Este procedimento descreve como ativar o WDS no AP do cliente WDS:

1. Navegue até **Wireless > AP** e marque a caixa de seleção para **Participar da Infraestrutura SWAN**. SWAN significa Structured Wireless-Aware Network.

cisco	Home Network Vispocration address Secretal Services Ranagement Solamate Salarices
Wireless Services	Hostname MAIB-WDS-Client uptime is 10 hours, 30 minutes
WDS	Wireless Services: AP
	Participate in SWAN intrastructure:
	WD\$ Discevery: © Auto Discovery Specified Discovery: 10.108.54.146 (IP Address)
	Username: WDSCIAnt1 Password:
	Confirm Password: Authentication Methods <a href="https://www.example.com/webods/Pusities/Profiles/">www.example.com/webods/Pusities/</a>
	Apply: Can

2. Os APs de cliente WDS podem descobrir automaticamente os APs WDS. Ou você pode inserir manualmente o endereço IP do AP WDS para registro do cliente na caixa de texto **Especificada de descoberta**.

Você também pode adicionar o nome de usuário e a senha do cliente WDS para autenticação no servidor RADIUS local configurado no AP WDS.

### Configurações de CLI

#### **AP WDS**

Esta é uma configuração de exemplo para o AP WDS:

```
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
1
hostname MAIB-WDS-AP
!
1
logging rate-limit console 9
enable secret 5 $1$EdDD$dG47yIKn86GCqmKjFf1Sy0
!
aaa new-model
1
1
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
!
1
1
1
1
aaa session-id common
no ip routing
no ip cef
1
1
!
1
dot11 syslog
1
dot11 ssid WDS-EAP
authentication open eap eap_methods
authentication network-eap eap_methods
authentication key-management wpa version 2
guest-mode
!
1
dot11 guest
!
1
!
username Cisco password 7 13261E010803
username My3602 privilege 15 password 7 10430810111F00025D56797F65
1
!
bridge irb
!
1
!
interface Dot11Radio0
no ip address
no ip route-cache
!
encryption mode ciphers aes-ccm
1
ssid WDS-EAP
1
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
1
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
1
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
1
interface BVI1
ip address 10.106.54.146 255.255.255.192
no ip route-cache
ipv6 address dhcp
ipv6 address autoconfig
ipv6 enable
1
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
!
1
radius-server local
no authentication eapfast
no authentication mac
nas 10.106.54.146 key 7 045802150C2E1D1C5A
user WDSClient1 nthash 7
072E776E682F4D5D35345B5A227E78050D6413004A57452024017B0803712B224A
1
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
1
1
wlccp authentication-server infrastructure method_Infrastructure
wlccp wds priority 254 interface BVI1
!
line con 0
line vty 0 4
transport input all
Т
end
```

AP de cliente WDS

#### Esta é uma configuração de exemplo para o AP cliente 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
1
1
logging rate-limit console 9
enable secret 5 $1$vx/M$qP6DY30TGiXmjvUDvKKjk/
1
aaa new-model
!
!
aaa group server radius rad_eap
server name WDS-Radius
1
aaa authentication login eap_methods group rad_eap
aaa authorization exec default local
1
1
1
1
1
aaa session-id common
no ip routing
no ip cef
!
1
1
1
dot11 syslog
1
dot11 ssid WDS-EAP
authentication open eap eap_methods
authentication network-eap eap_methods
authentication key-management wpa version 2
guest-mode
!
1
dot11 guest
!
eap profile WDS-AP
method leap
!
!
1
username Cisco password 7 062506324F41
username My2602 privilege 15 password 7 09414F000D0D051B5A5E577E6A
!
1
bridge irb
1
1
1
interface Dot11Radio0
```

```
no ip address
no ip route-cache
1
encryption mode ciphers aes-ccm
!
ssid WDS-EAP
1
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
1
interface Dot11Radio1
no ip address
no ip route-cache
!
encryption mode ciphers aes-ccm
!
ssid WDS-EAP
1
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
1
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
1
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
1
1
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
```

# Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente. Quando a configuração estiver concluída, o AP do cliente WDS deve ser capaz de se registrar no AP WDS.

No AP WDS, o status do WDS é mostrado como Registrado.

WDS STATUS	Ŭ.	GENERAL S	ETUP II	SERVER G	ROUPS			
Hostname MAIB-WDS-AP uptime is 10 hours, 16 minutes								
Wireless Services: WDS - Wireless Domain Services - Status								
WDS Information								
MAC Address	IPv4 Address		IPv6 Address	Priority		State		
bc16.6516.62c4	10.106.04.146		=	254		Administratively St	andAlone - ACTIVE	
WDS Registration								
APs: 1			Mobile Nodes: 0					
AP Information								
Hostname	MAC Address		IPv4 Address	IPv6 Addre	IPv6 Address		State	
MAIB-WDS-Client	1872.ea24.40e6			2	1		REGISTERED	
Mobile Node Information								
MAC Address	IP Address	State		SSID	VLAN ID	BSSID		
Wireless Network Manager Information								
IP Address	Authentication Status							

No AP do cliente WDS, o status do WDS é Infraestrutura.

fostname MAIB-WDS-Client			MAIB-WDS-Client uptime is 10 hours, 57 minutes	
Wireless Services Summary				
A2				
WDS MAC Address	WDS IP Address	IN Authenticator	MN Authenticator	State
bc16.6516.62c4	=	10.106.54.146	10.106.54.145	Infrastructure

**Note**: A <u>ferramenta Output Interpreter (exclusiva para clientes registrados) é compatível com</u> <u>alguns comandos de exibição.</u>. Use a ferramenta Output Interpreter para visualizar uma análise do resultado gerado pelo comando show..

### Saída de verificação CLI no AP WDS

Este procedimento mostra como verificar a configuração do AP WDS:

```
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
```

### Saída de verificação CLI no AP cliente WDS

Este procedimento mostra como verificar a configuração do AP do cliente 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::
```

## Troubleshoot

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.