WDS auf autonomen APs mit lokalem RADIUS-Server konfigurieren

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Wireless Domain Services (WDS) in einer Konfiguration eines autonomen Access Points (AP) mit einem lokalen RADIUS-Server konfiguriert werden. Das Dokument konzentriert sich auf Konfigurationen über die neue GUI, bietet aber auch CLI-Konfigurationen (Command Line Interface).

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse der grundlegenden GUI- und CLI-Konfiguration auf autonomen APs verfügen.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco Access Point der Serie 3602e auf der unabhängigen AP IOS® Software, Version 15.2(4)JA1; Dieses Gerät fungiert als WDS-AP und lokaler RADIUS-Server.
- Cisco Access Point der Serie 2602i auf der unabhängigen AP IOS-Software, Version 15.2(4)JA1; Dieses Gerät fungiert als WDS-Client-AP.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Konfigurieren

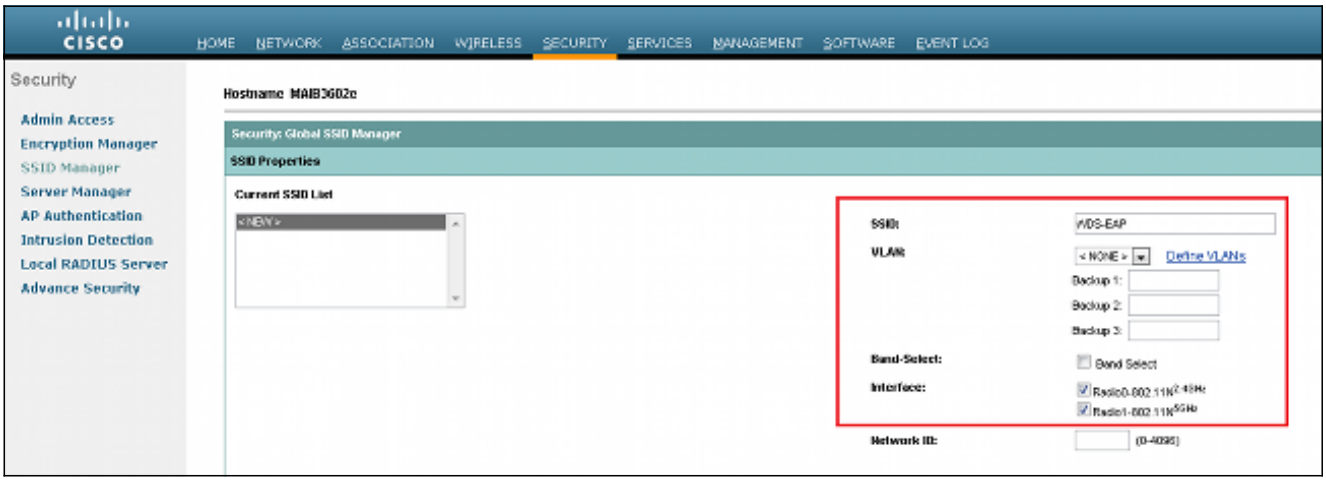
> **Anmerkung:** Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

GUI-Konfigurationen

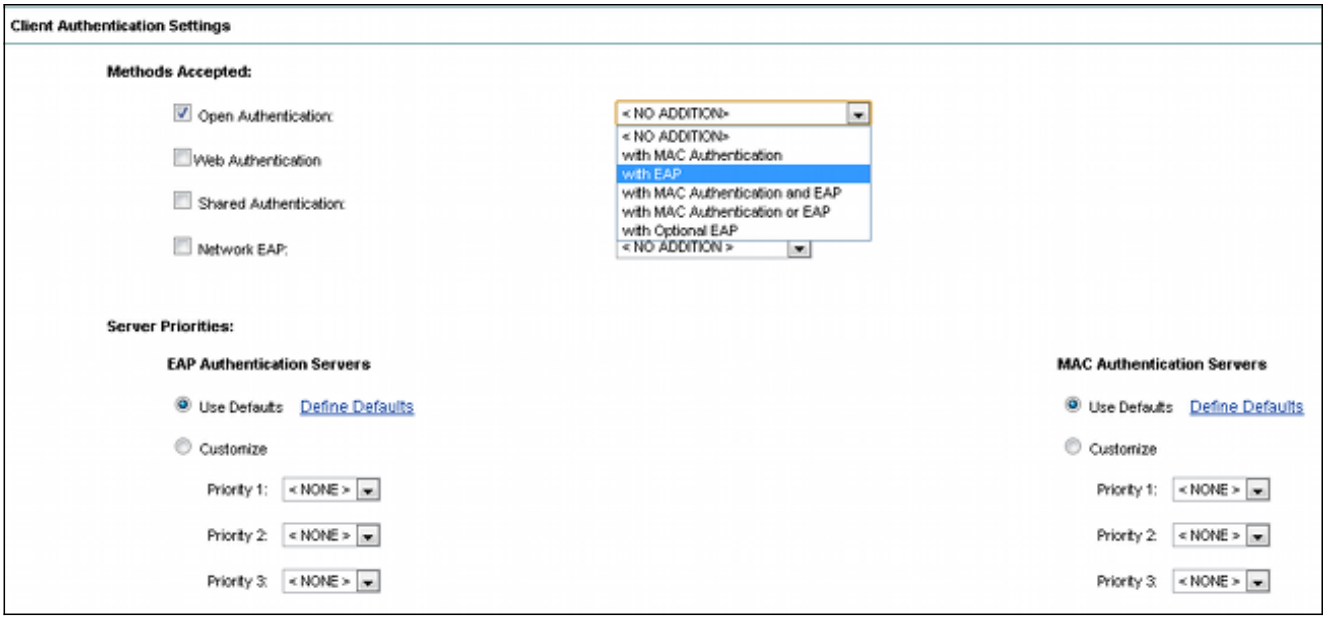
SSID erstellen

In diesem Verfahren wird beschrieben, wie Sie einen neuen Service Set Identifier (SSID) erstellen.

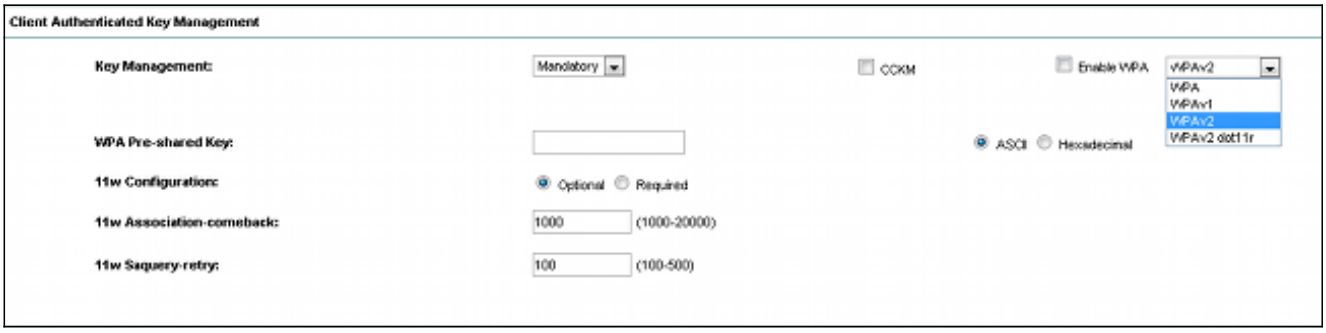
1. Navigieren Sie zu **Security > SSID Manager**, und klicken Sie auf **NEU**, um eine neue SSID zu erstellen.



2. Konfigurieren Sie die SSID für die EAP-Authentifizierung (Extensible Authentication Protocol).

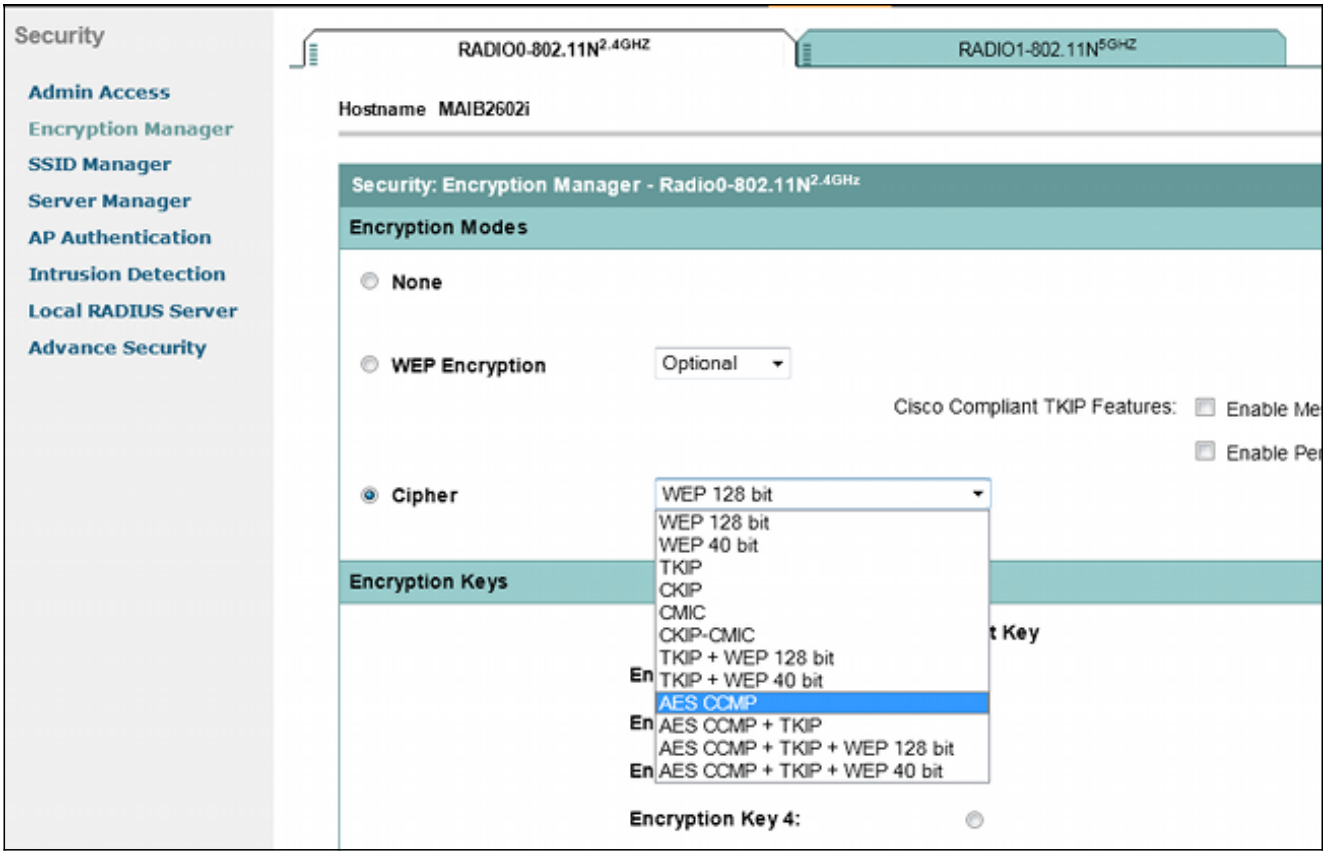


3. Legen Sie die gewünschte Verschlüsselungsstufe fest. Verwenden Sie in diesem Beispiel Wi-Fi Protected Access 2 (WPA2).



4. Klicken Sie auf **Übernehmen**, um die Einstellungen zu speichern.

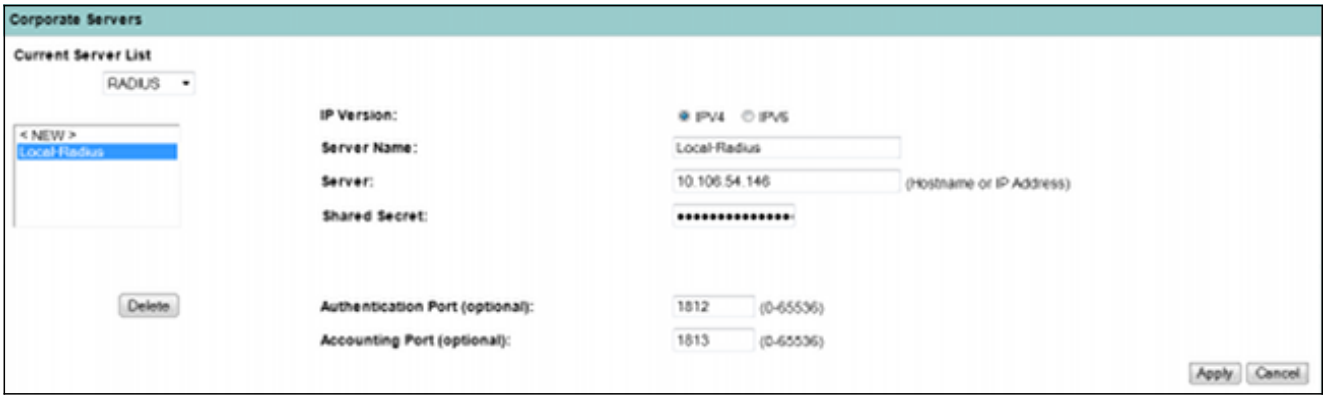
5. Navigieren Sie zu **Security > Encryption Manager**, und wählen Sie die erforderliche Verschlüsselungsmethode aus.



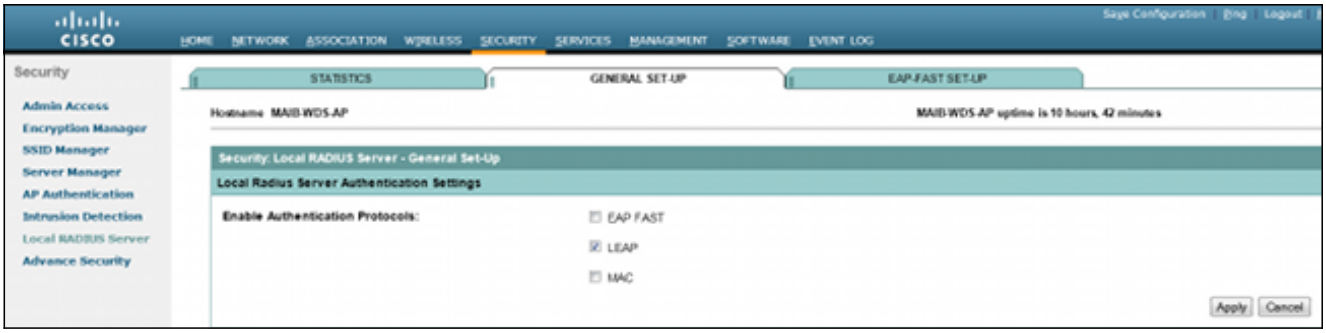
Lokale RADIUS-Serverkonfiguration für WDS AP

In diesem Verfahren wird beschrieben, wie der lokale RADIUS-Server auf dem WDS AP konfiguriert wird:

1. Navigieren Sie zu **Security > Server Manager**, fügen Sie die WDS AP Bridge Virtual Interface (BVI)-IP als lokalen RADIUS hinzu, und fügen Sie einen gemeinsamen geheimen Schlüssel hinzu.



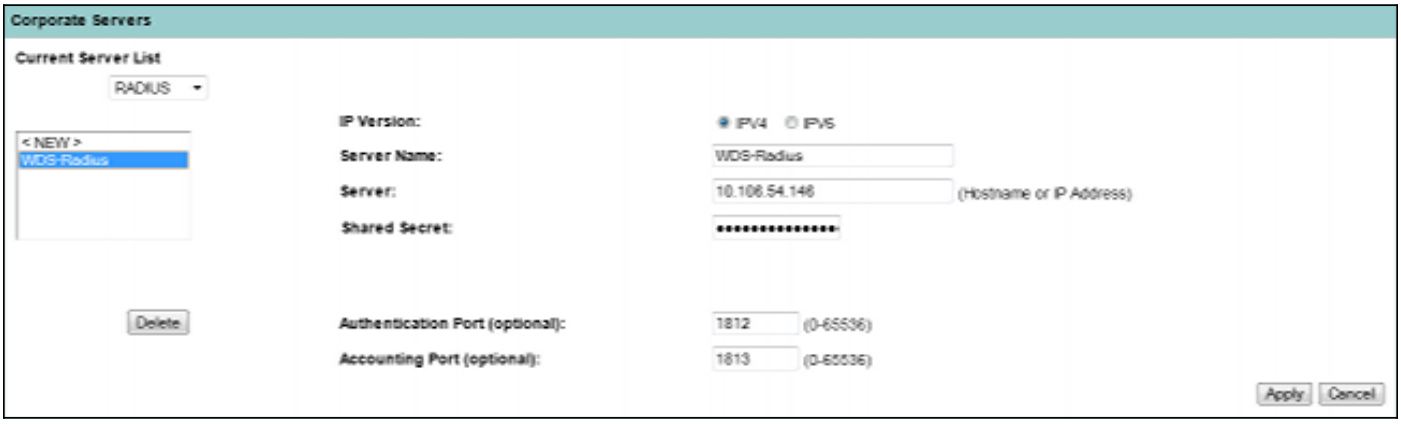
2. Navigieren Sie zu **Sicherheit > Lokaler Radius-Server > Registerkarte General Set-Up (Allgemeine Einrichtung)**. Definieren Sie die EAP-Protokolle, die Sie verwenden möchten. Aktivieren Sie in diesem Beispiel die LEAP-Authentifizierung (Light Extensible Authentication Protocol).



3. Sie können auf derselben Seite auch Network Access Server (NAS)-IPs und Anmeldeinformationen für den Client-Benutzernamen/Kennwort hinzufügen. Die Konfiguration eines lokalen RADIUS auf einem WDS AP ist abgeschlossen.

Lokale RADIUS-Serverkonfiguration auf dem WDS-Client-AP

In dieser Abbildung wird gezeigt, wie die IP-Adresse des WDS Access Points als RADIUS-Server konfiguriert wird:



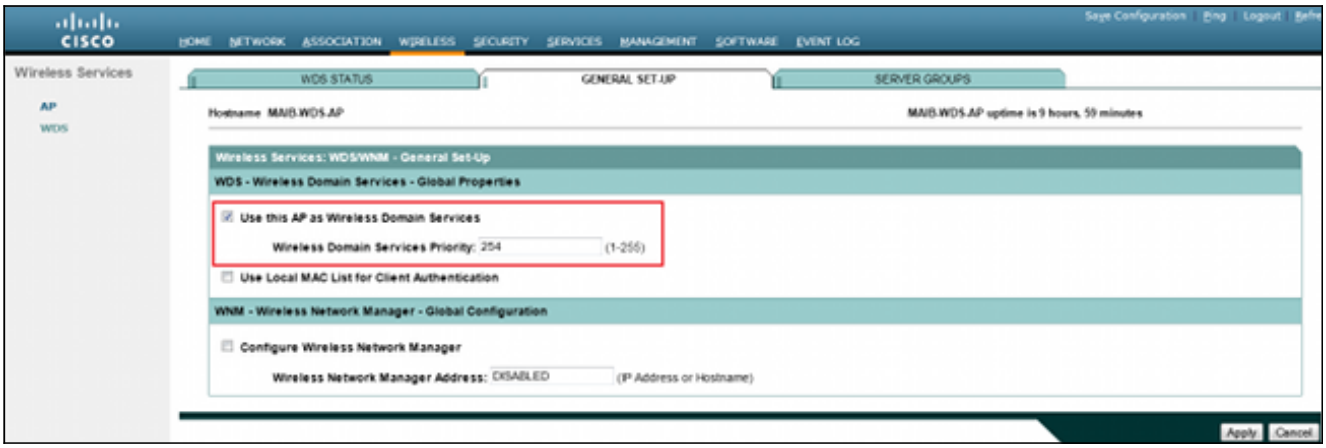
Beide APs sind jetzt mit SSIDs für die LEAP-Authentifizierung konfiguriert, und der WDS-Server fungiert als lokaler RADIUS. Verwenden Sie die gleichen Schritte für einen externen RADIUS. Nur die RADIUS-Server-IP wird geändert.

WDS für WDS AP aktivieren

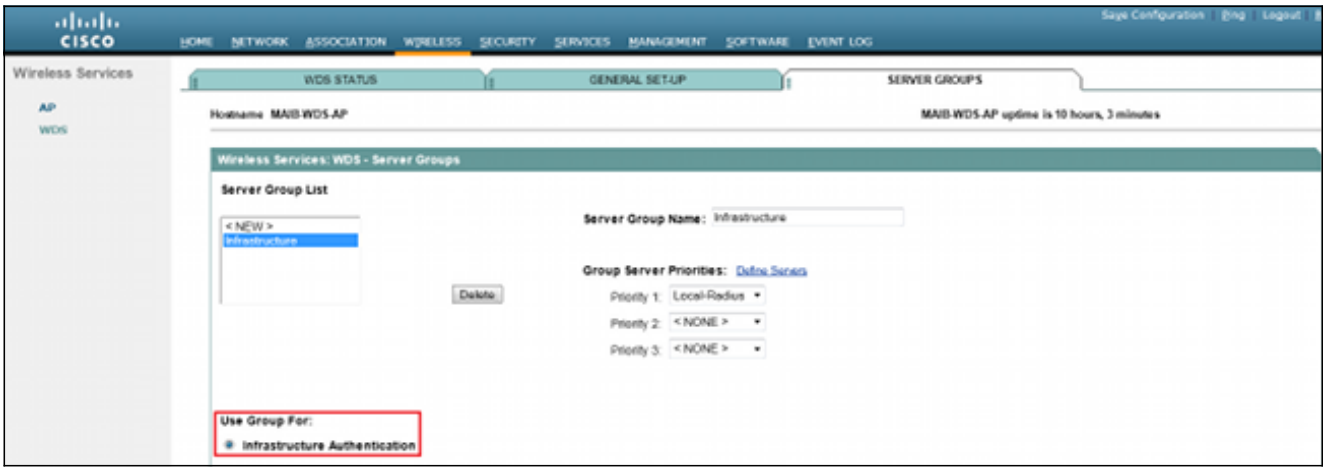
In diesem Verfahren wird beschrieben, wie WDS auf dem WDS AP aktiviert wird:

1. Navigieren Sie zur Registerkarte **Wireless > WDS > Allgemeine Einrichtung**, und aktivieren Sie das Kontrollkästchen **Diesen Access Point als Wireless-Domänendienste verwenden**. Dadurch wird der WDS-Dienst am Access Point aktiviert.

2. Verwenden Sie in einem Netzwerk mit mehreren WDS-APs die Wireless Domain Services Priority-Option, um das primäre WDS und das Backup-WDS zu definieren. Der Wert liegt zwischen 1 und 255, wobei 255 die höchste Priorität darstellt.



3. Navigieren Sie zur Registerkarte **Servergruppen** auf derselben Seite. Erstellen Sie eine Liste der Infrastrukturserver-Gruppen, für die alle WDS-Client-APs authentifiziert werden. Zu diesem Zweck können Sie den lokalen RADIUS-Server auf dem WDS AP verwenden. Da sie bereits hinzugefügt wurde, wird sie in der Dropdown-Liste angezeigt.



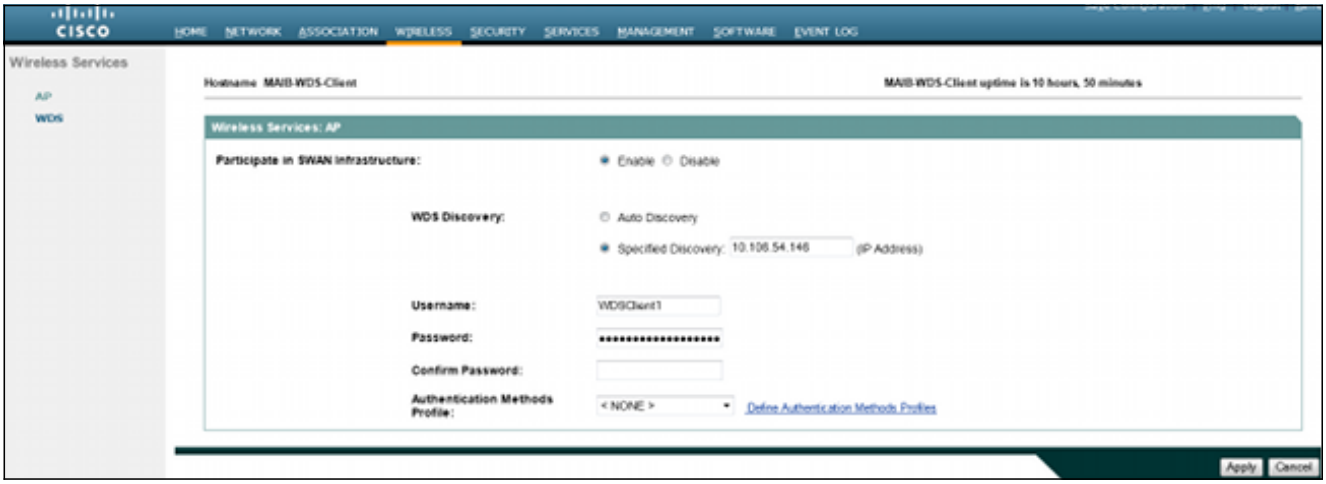
4. Aktivieren Sie das Optionsfeld **Gruppe verwenden für: Infrastrukturauthentifizierung**, und klicken Sie auf **Apply**, um die Einstellungen zu speichern.

5. Der WDS-AP-Benutzername und die Kennwörter können der lokalen RADIUS-Serverliste hinzugefügt werden.

WDS auf dem WDS-Client-AP aktivieren

In diesem Verfahren wird beschrieben, wie WDS auf dem WDS-Client-AP aktiviert wird:

1. Navigieren Sie zu **Wireless > AP**, und aktivieren Sie das Kontrollkästchen **An SWAN-Infrastruktur teilnehmen**. SWAN steht für Structured Wireless-Aware Network.



2. WDS-Client-APs können die WDS-APs automatisch erkennen. Alternativ können Sie im Textfeld **Specified Discovery** die IP-Adresse des WDS Access Points für die Client-Registrierung manuell eingeben.

   Sie können auch den WDS-Client-Benutzernamen und das Kennwort für die Authentifizierung mithilfe des auf dem WDS-AP konfigurierten lokalen RADIUS-Servers hinzufügen.

CLI-Konfigurationen

WDS-AP

Dies ist eine Beispielkonfiguration für den 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

Dies ist eine Beispielkonfiguration für den 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 $1$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
```

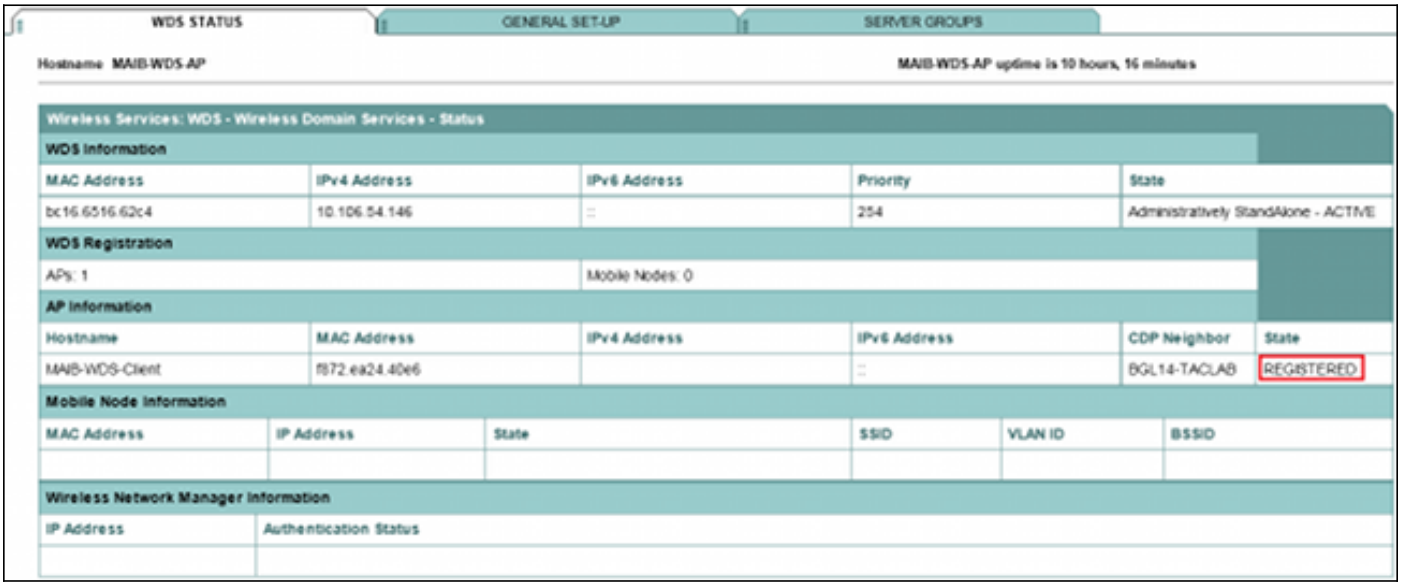
```
no ip address
no ip route-cache
!
encryption mode ciphers aes-ccm
!
ssid WDS-EAP
!
antenna gain 0
stbc
station-role root
bridge-group 1
bridge-group 1 subscriber-loop-control
bridge-group 1 spanning-disabled
bridge-group 1 block-unknown-source
no bridge-group 1 source-learning
no bridge-group 1 unicast-flooding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

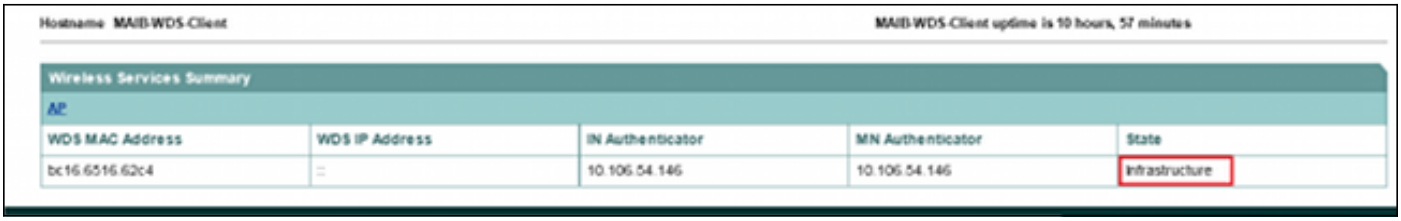
Überprüfung

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert. Nach Abschluss der Einrichtung sollte der WDS-Client-Access Point in der Lage sein, sich beim WDS-Access Point zu registrieren.

Auf dem WDS AP wird der WDS-Status als "Registriert" angezeigt.



Auf dem WDS-Client-AP lautet der WDS-Status Infrastruktur.



Anmerkung: Das Output Interpreter Tool (nur registrierte Kunden) unterstützt bestimmte **show**-Befehle. Verwenden Sie das Output Interpreter Tool, um eine Analyse der **Ausgabe des** Befehls **show** anzuzeigen.

CLI-Verifizierungs-Ausgabe auf WDS AP

Dieses Verfahren zeigt, wie Sie die WDS-AP-Konfiguration überprüfen:

```
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-Verifizierungs-Ausgabe auf WDS-Client-AP

Dieses Verfahren zeigt, wie die WDS-Client-AP-Konfiguration überprüft wird:

```
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::
```

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.