

Konfigurieren des Aironet OfficeExtend Access Point der Serie 600

Inhalt

- [Einleitung](#)
- [Voraussetzungen](#)
- [Anforderungen](#)
- [Verwendete Komponenten](#)
- [Konventionen](#)
- [Hintergrundinformationen](#)
- [Setup-Richtlinien](#)
- [Office Extend-Lösung - Übersicht](#)
- [Firewall-Konfigurationsrichtlinien](#)
- [Office Extend AP-600 - Konfigurationsschritte](#)
- [WLAN- und Remote-LAN-Konfigurationseinstellungen](#)
- [WLAN-Sicherheitseinstellungen](#)
- [MAC-Filterung](#)
- [Anzahl unterstützter Benutzer](#)
- [Channel-Management und -Einstellungen](#)
- [Zusätzliche Hinweise](#)
- [Konfiguration des OEAP-600-Access Points](#)
- [OEAP-600 Access Point - Hardwareinstallation](#)
- [Fehlerbehebung beim OEAP-600](#)
- [Debuggen von Clientzuordnungsproblemen](#)
- [Interpretieren des Ereignisprotokolls](#)
- [Wenn die Internetverbindung unzuverlässig erscheint](#)
- [Zusätzliche Debug-Befehle](#)
- [Bekannt Probleme/Problem](#)
- [Zugehörige Informationen](#)

Einleitung

Dieses Dokument enthält Informationen zu den Voraussetzungen für die Konfiguration eines Cisco Wireless LAN (WLAN) Controllers für die Verwendung mit dem Cisco Aironet® OfficeExtend Access Point (OEAP) der Serie 600^a. Der OEAP der Cisco Aironet Serie 600 unterstützt den Split-Mode-Betrieb und verfügt über Einrichtungen, die eine Konfiguration über den WLAN-Controller erfordern, sowie über Funktionen, die vom Endbenutzer lokal konfiguriert werden können. Dieses Dokument enthält außerdem Informationen zu den Konfigurationen, die für eine ordnungsgemäße Verbindung erforderlich sind, sowie zu den unterstützten Feature-Sets.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf der Cisco Aironet Serie 600 OfficeExtend Access Point (OEAP).

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.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter [Cisco Technical Tips Conventions \(Technische Tipps von Cisco zu Konventionen\)](#).

Hintergrundinformationen

Setup-Richtlinien

- Cisco Aironet 600 Series OEAP wird von den folgenden Controllern unterstützt: Cisco 5508, WiSM-2 und Cisco 2504.
- Die erste Controller-Version, die OEAP für die Cisco Aironet Serie 600 unterstützt, ist 7.0.116.0.
- Die Verwaltungsschnittstellen des Controllers müssen sich in einem routbaren IP-Netzwerk befinden.
- Die Firewall-Konfiguration des Unternehmens muss geändert werden, um Datenverkehr mit den UDP-Portnummern **5246** und **5247** zuzulassen.

Office Extend-Lösung - Übersicht

- Einem Benutzer wird ein Access Point (AP) mit der IP-Adresse des Unternehmens-Controllers zugewiesen, oder der Benutzer kann die IP-Adresse des Controllers über den Konfigurationsbildschirm eingeben (HTML-Seiten für die Einrichtung).
- Der Benutzer schließt den AP an seinen Router zu Hause an.
- Der Access Point erhält vom Router zu Hause eine IP-Adresse, schließt sich dem primären Controller an und erstellt einen geschützten Tunnel.
- Anschließend informiert Cisco Aironet OEAP der Serie 600 über die unternehmenseigene SSID, die dieselben Sicherheitsmethoden und -services über das WAN auf das Zuhause des Benutzers erweitert.
- Wenn das Remote-LAN konfiguriert ist, wird ein kabelgebundener Port des Access Points zum Controller zurückgetunnelt.
- Der Benutzer kann dann zusätzlich eine lokale SSID für den persönlichen Gebrauch aktivieren.

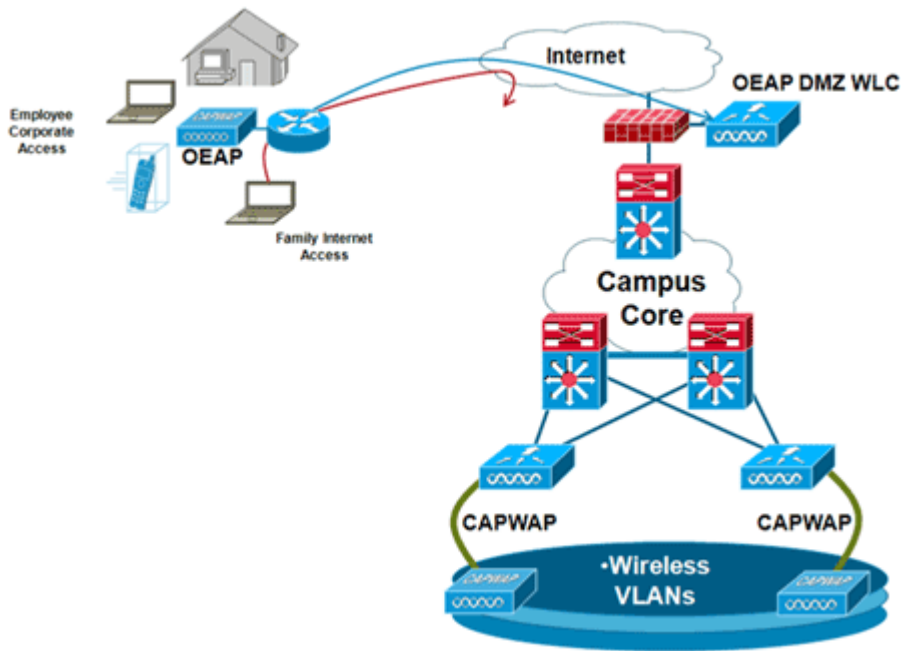
Firewall-Konfigurationsrichtlinien

Die allgemeine Konfiguration der Firewall sieht vor, dass die CAPWAP-Steuerung und die CAPWAP-Management-Portnummern über die Firewall zugelassen werden. Der Cisco Aironet OEAP-Controller der Serie 600 kann in der DMZ-Zone platziert werden.

Hinweis: Die Ports UDP **5246** und **5247** müssen auf der Firewall zwischen dem WLAN-Controller und dem

OEAP der Cisco Aironet Serie 600 geöffnet werden.

Dieses Diagramm zeigt einen Cisco Aironet OEAP-Controller der Serie 600 in der DMZ:



Nachfolgend finden Sie ein Beispiel für eine Firewall-Konfiguration:

```
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address X.X.X.X 255.255.255.224

!--- X.X.X.X represents a public IP address

!
interface Ethernet0/2
 nameif dmz
 security-level 50
 ip address 172.16.1.2 255.255.255.0
!
access-list Outside extended permit udp any host X.X.X.Y eq 5246

!--- Public reachable IP of corporate controller

access-list Outside extended permit udp any host X.X.X.Y eq 5247

!--- Public reachable IP of corporate controller

access-list Outside extended permit icmp any any
!
global (outside) 1 interface
nat (dmz) 1 172.16.1.0 255.255.255.0
static (dmz,outside) X.X.X.Y 172.16.1.25 netmask 255.255.255.255
access-group Outside in interface outside
```

Um die interne IP-Adresse des AP-Managers als Teil des CAPWAPP Discovery Response-Pakets an den

OfficeExtend-Access-Point zu übertragen, muss der Controller-Administrator sicherstellen, dass NAT in der AP-Manager-Schnittstelle aktiviert ist und die richtige IP-Adresse des NAT an den Access-Point gesendet wird.

Hinweis: Standardmäßig antwortet der WLC während der AP-Erkennung nur mit der NAT-IP-Adresse, wenn NAT aktiviert ist. Wenn sich innerhalb und außerhalb des NAT-Gateways APs befinden, führen Sie diesen Befehl aus, damit der WLC sowohl mit der NAT-IP-Adresse als auch mit der Nicht-NAT-Management-IP-Adresse antworten kann:

```
<#root>
```

```
config network ap-discovery nat-ip-only disable
```

Hinweis: Dies ist nur erforderlich, wenn der WLC über eine NAT-IP-Adresse verfügt.

Das Diagramm zeigt, dass NAT aktiviert ist, vorausgesetzt, der WLC verfügt über eine NAT-IP-Adresse:

The screenshot shows the Cisco WLC configuration interface for the 'management' interface. The 'NAT Address' section is highlighted with a red circle, indicating that NAT is enabled. The configuration details are as follows:

Section	Field	Value
General Information	Interface Name	management
	MAC Address	00:24:97:69:52:8f
Configuration	Quarantine	<input type="checkbox"/>
	Quarantine Vlan Id	0
NAT Address	Enable NAT Address	<input checked="" type="checkbox"/>
	NAT IP Address	X.X.X.Y
Interface Address	VLAN Identifier	0
	IP Address	172.16.1.25
	Netmask	255.255.255.0
	Gateway	172.16.1.2
Physical Information	The interface is attached to a LAG	
	Enable Dynamic AP Management	<input checked="" type="checkbox"/>
DHCP Information	Primary DHCP Server	172.20.225.153
	Secondary DHCP Server	0.0.0.0

Hinweis: Diese Konfiguration ist im Controller nicht erforderlich, vorausgesetzt, sie ist mit einer über das Internet routbaren IP-Adresse konfiguriert und befindet sich nicht hinter einer Firewall.

Office Extend AP-600 - Konfigurationsschritte

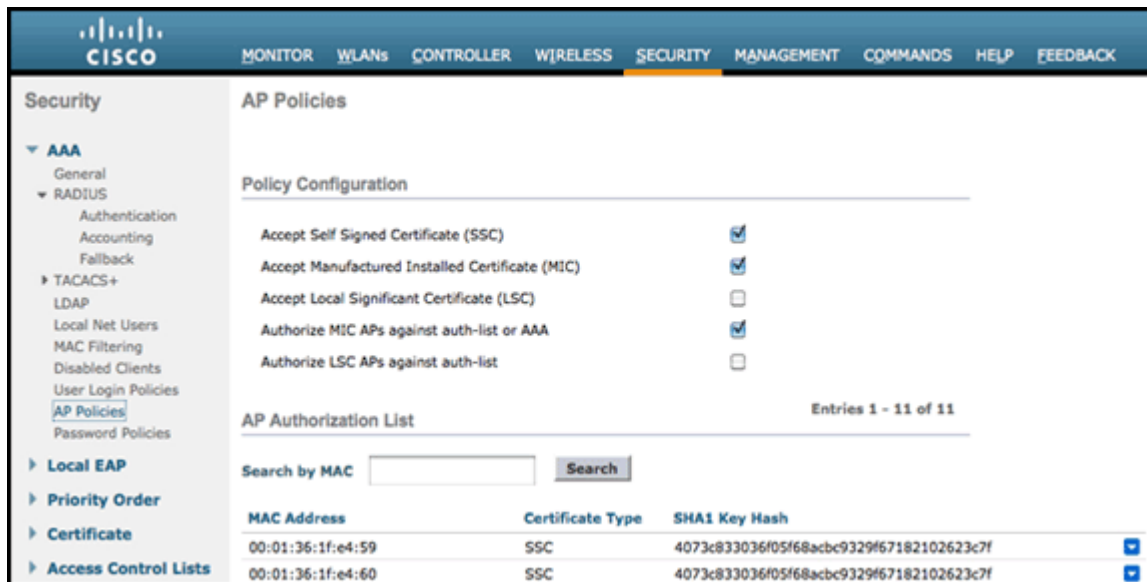
Der Cisco Aironet OEAP der Serie 600 wird als Local Mode Access Point mit dem WLC verbunden.

Hinweis: Die Modi Monitor, H-REAP, Sniffer, Rogue Detection, Bridge und SE-Connect werden von der

Serie 600 nicht unterstützt und können nicht konfiguriert werden.

Hinweis: Die OEAP-Funktion der Cisco Aironet Serie 600 in den Access Points der Serien 1040, 1130, 1140 und 3502i erfordert die Konfiguration der APs für Hybrid REAP (H-REAP) und die Einstellung des Submodus für den AP für OEAP der Cisco Aironet Serie 600. Dies geschieht nicht mit der Serie 600, da sie den lokalen Modus verwendet und nicht geändert werden kann.

MAC-Filterung kann bei der AP-Authentifizierung während des Join-Vorgangs verwendet werden, um zu verhindern, dass nicht autorisierte Cisco Aironet OEAP-Einheiten der Serie 600 dem Controller beitreten. Dieses Bild zeigt, wo Sie die MAC-Filterung aktivieren und die AP-Sicherheitsrichtlinien konfigurieren:



Hier wird die Ethernet-MAC-Adresse (nicht die Radio-MAC-Adresse) eingegeben. Wenn Sie die MAC-Adresse in einen Radius-Server eingeben, müssen Sie Kleinbuchstaben verwenden. Im AP-Ereignisprotokoll finden Sie Informationen zur Erkennung der Ethernet-MAC-Adresse (weitere Informationen hierzu später).

WLAN- und Remote-LAN-Konfigurationseinstellungen

Die Cisco Aironet OEAP der Serie 600 verfügt über einen physischen Remote-LAN-Port (gelber Port #4). Die Konfiguration ähnelt der eines WLAN. Da es sich jedoch nicht um einen Wireless-LAN-Port und einen kabelgebundenen LAN-Port auf der Rückseite des Access Points handelt, wird dieser als Remote-LAN-Port bezeichnet und verwaltet.

Das Gerät verfügt zwar nur über einen physischen Port, bei Verwendung eines Hub oder Switches können jedoch bis zu vier kabelgebundene Clients angeschlossen werden.

Hinweis: Das Limit für den Remote-LAN-Client unterstützt die Verbindung eines Switches oder Hubs mit dem Remote-LAN-Port für mehrere Geräte oder die direkte Verbindung mit einem Cisco IP-Telefon, das an diesen Port angeschlossen ist.

Hinweis: Nur die ersten vier Geräte können eine Verbindung herstellen, bis eines der Geräte länger als eine Minute inaktiv ist. Bei Verwendung der 802.1x-Authentifizierung kann es Probleme beim Versuch geben, mehr als einen Client auf dem kabelgebundenen Port zu verwenden.

Hinweis: Diese Zahl wirkt sich nicht auf die Fünfzehn aus, die für die Controller-WLANs festgelegt wurden.

Ein Remote-LAN wird ähnlich konfiguriert wie ein WLAN und ein Gast-LAN, die auf dem Controller

konfiguriert sind.

WLANs sind Wireless-Sicherheitsprofile. Dies sind die Profile, die von Ihrem Unternehmensnetzwerk verwendet werden. Der Cisco Aironet OEAP der Serie 600 unterstützt maximal zwei WLANs und ein Remote-LAN.

Ein Remote-LAN ähnelt einem WLAN, ist jedoch dem kabelgebundenen Port auf der Rückseite des Access Points (Port #4 in Gelb) zugeordnet, wie in diesem Bild gezeigt:

WLANs > New

Type: WLAN

Profile Name: Guest LAN, WLAN, Remote LAN

SSID:

ID: 4

Hinweis: Wenn Sie über mehr als zwei WLANs oder mehr als ein Remote-LAN verfügen, müssen alle in einer AP-Gruppe zusammengefasst werden.

Die Abbildung zeigt, wo WLANs und das Remote-LAN konfiguriert sind:

WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
1	WLAN	EvoraData	EvoraData	Enabled	[WPA2][Auth(802.1X)]
2	WLAN	EvoraVoice	Evora_Voice	Enabled	[WPA2][Auth(802.1X)]
3	Remote LAN	EthernetTunnel	---	Enabled	None

Dieses Bild zeigt einen Beispiel-OEAP-Gruppennamen:

AP Group Name	AP Group Description
EvoraOEAP	Group for EvoraOEAPs
default-group	

Dieses Bild zeigt eine WLAN-SSID- und RLAN-Konfiguration:

WLANs Ap Groups > Edit 'EvoraOEAP'

General WLANs APs

WLAN ID	WLAN SSID	Interface/Interface Group(G)	SNMP NAC State
1	EvoraData	management	Disabled
2	Evora_Voice	management	Disabled
3	EthernetTunnel	management	Disabled

Wenn der Cisco Aironet OEAP der Serie 600 in eine AP-Gruppe aufgenommen wird, gelten für die Konfiguration der AP-Gruppe die gleichen Einschränkungen wie für zwei WLANs und ein Remote-LAN. Wenn sich der Cisco Aironet OEAP der Serie 600 in der Standardgruppe befindet, d. h. wenn er nicht zu einer definierten AP-Gruppe gehört, müssen die WLAN-/Remote-LAN-IDs auf weniger als ID 8 festgelegt werden, da dieses Produkt die höheren ID-Sätze nicht unterstützt.

Bewahren Sie ID-Sätze auf weniger als 8 auf, wie in diesem Bild gezeigt:

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT

WLANs > New

Type: WLAN

Profile Name: New Evora WLAN

SSID: EvoraWLAN

ID: 4

4 5 6 7 8 9 10 11 12 13

Hinweis: Wenn zusätzliche WLANs oder Remote-LANs mit der Absicht erstellt werden, die WLANs oder das Remote-LAN zu ändern, die vom Cisco Aironet OEAP der Serie 600 verwendet werden, deaktivieren Sie die aktuellen WLANs oder das Remote-LAN, die Sie entfernen, bevor Sie die neuen WLANs oder das Remote-LAN auf der Serie 600 aktivieren. Wenn für eine Access Point-Gruppe mehr als ein Remote-LAN aktiviert ist, deaktivieren Sie alle Remote-LANs, und aktivieren Sie dann nur eines.

Wenn für eine AP-Gruppe mehr als zwei WLANs aktiviert sind, deaktivieren Sie alle WLANs, und aktivieren Sie dann nur zwei.

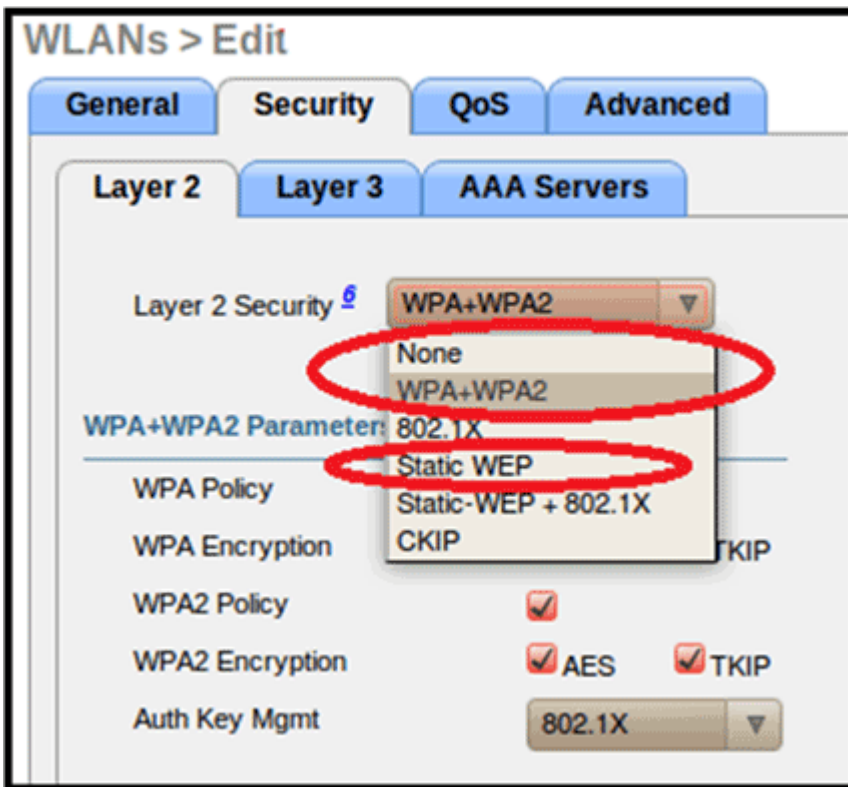
WLAN-Sicherheitseinstellungen

Beim Festlegen der Sicherheitseinstellungen im WLAN gibt es bestimmte Elemente, die von der Serie 600 nicht unterstützt werden.

Für Layer-2-Sicherheit werden für Cisco Aironet OEAP der Serie 600 nur folgende Optionen unterstützt:

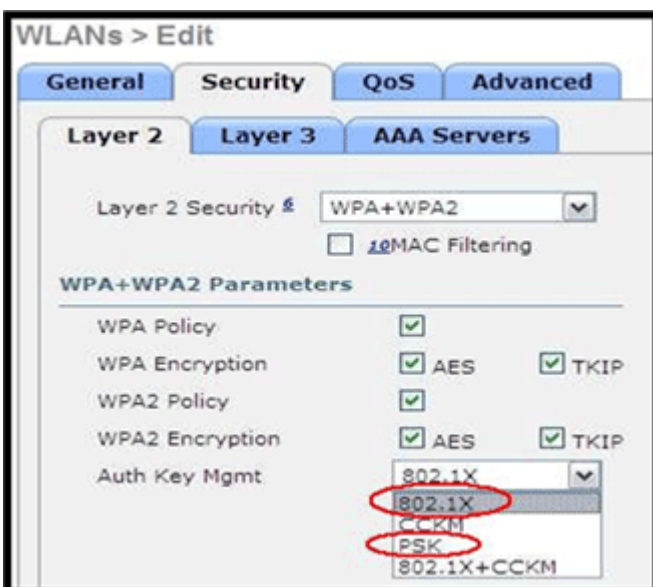
- None

- WPA+WPA2
- Statische WEPs können ebenfalls verwendet werden, jedoch nicht für .11n-Datenraten.

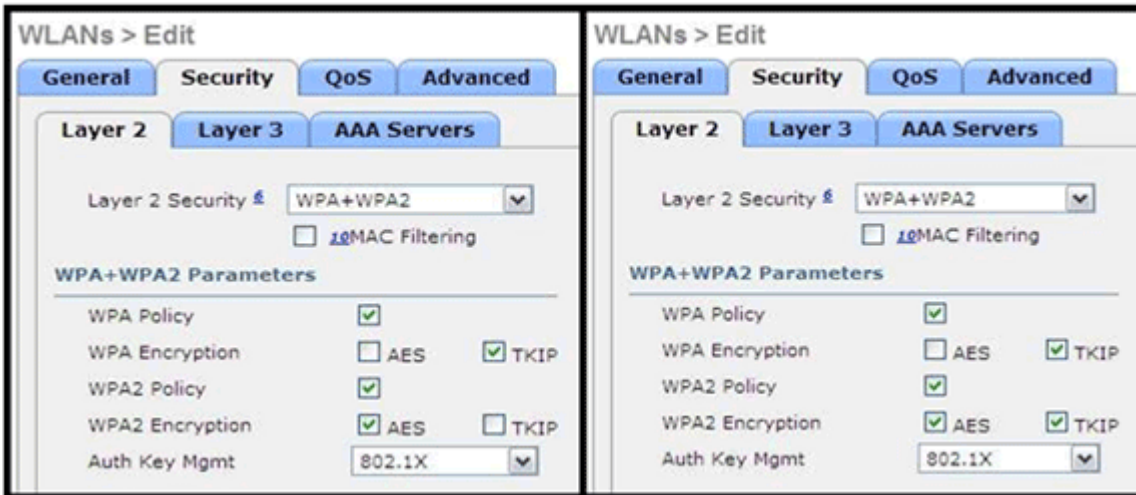


Hinweis: Nur 802.1x oder PSK sollte ausgewählt werden.

Die Einstellungen für die Sicherheitsverschlüsselung müssen für WPA und WPA2 für TKIP und AES identisch sein, wie in diesem Bild gezeigt:

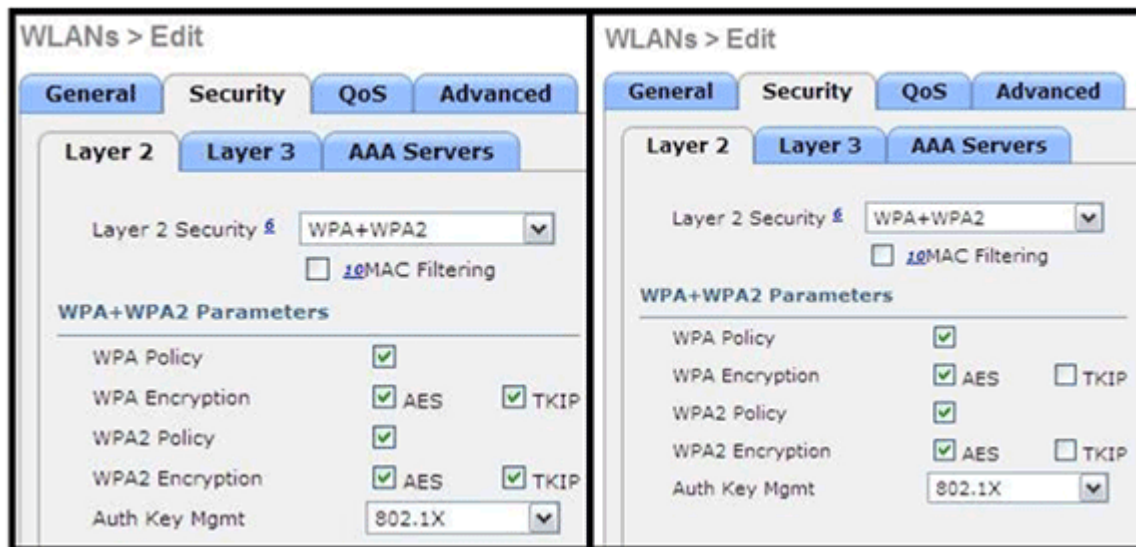


Diese Images enthalten Beispiele für inkompatible Einstellungen für TKIP und AES:



Hinweis: Beachten Sie, dass Sicherheitseinstellungen nicht unterstützte Funktionen zulassen.

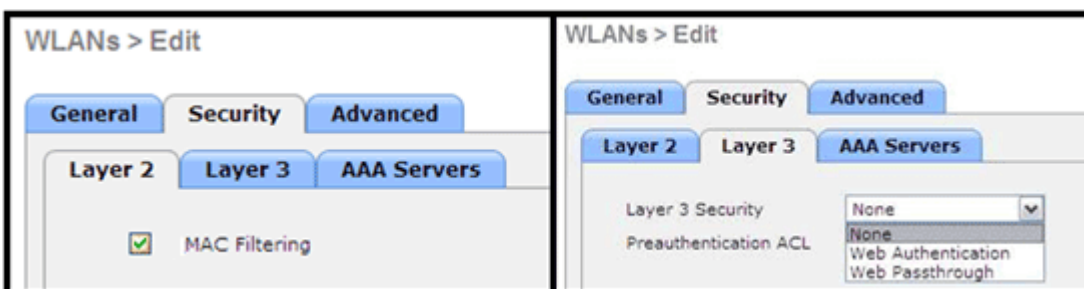
Diese Images bieten Beispiele für kompatible Einstellungen:



MAC-Filterung

Die Sicherheitseinstellungen können offen gelassen, für die MAC-Filterung oder für die Webauthentifizierung festgelegt werden. Standardmäßig wird die MAC-Filterung verwendet.

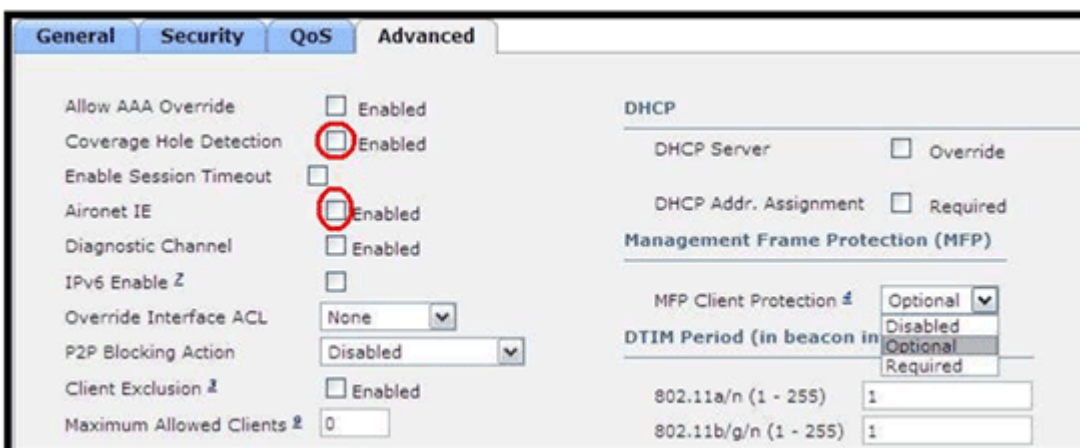
Dieses Bild zeigt die MAC-Filterung für Layer 2 und Layer 3:



QoS-Einstellungen werden verwaltet:

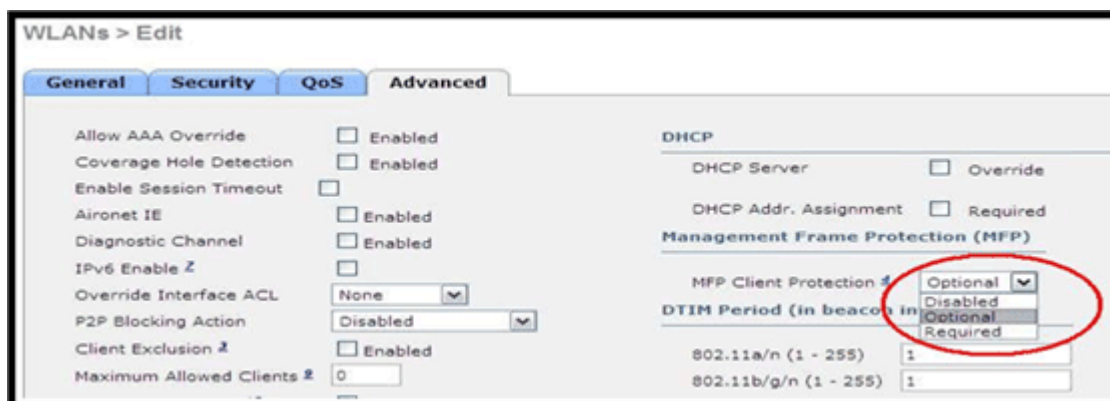


Erweiterte Einstellungen sollten ebenfalls verwaltet werden:



Hinweise:

- Coverage-Bohrungserkennung sollte nicht aktiviert werden.
- Aironet IE (Informationselemente) sollte nicht aktiviert werden, da sie nicht verwendet werden.
- Management Frame Protection (MFP) wird ebenfalls nicht unterstützt und sollte deaktiviert oder als optional konfiguriert werden, wie in diesem Bild gezeigt:



- Client-Lastenausgleich und Client-Band-Auswahl werden nicht unterstützt und sollten nicht aktiviert werden:



Anzahl unterstützter Benutzer

Auf den WLAN-Controller-WLANs der Serie 600 können jeweils nur fünfzehn Benutzer eine Verbindung herstellen. Ein sechzehnter Benutzer kann sich erst authentifizieren, wenn einer der ersten Clients die Authentifizierung aufhebt oder auf dem Controller ein Timeout aufgetreten ist.

Hinweis: Diese Zahl ist in den Controller-WLANs der Serie 600 kumuliert.

Wenn beispielsweise zwei Controller-WLANs konfiguriert sind und sich in einem der WLANs fünfzehn Benutzer befinden, können zu diesem Zeitpunkt keine Benutzer dem anderen WLAN der Serie 600 beitreten. Diese Beschränkung gilt nicht für lokale private WLANs, die der Endbenutzer auf den für den persönlichen Gebrauch konzipierten Geräten der Serie 600 konfiguriert, und die mit diesen privaten WLANs oder den kabelgebundenen Ports verbundenen Clients wirken sich nicht auf diese Beschränkungen aus.

Channel-Management und -Einstellungen

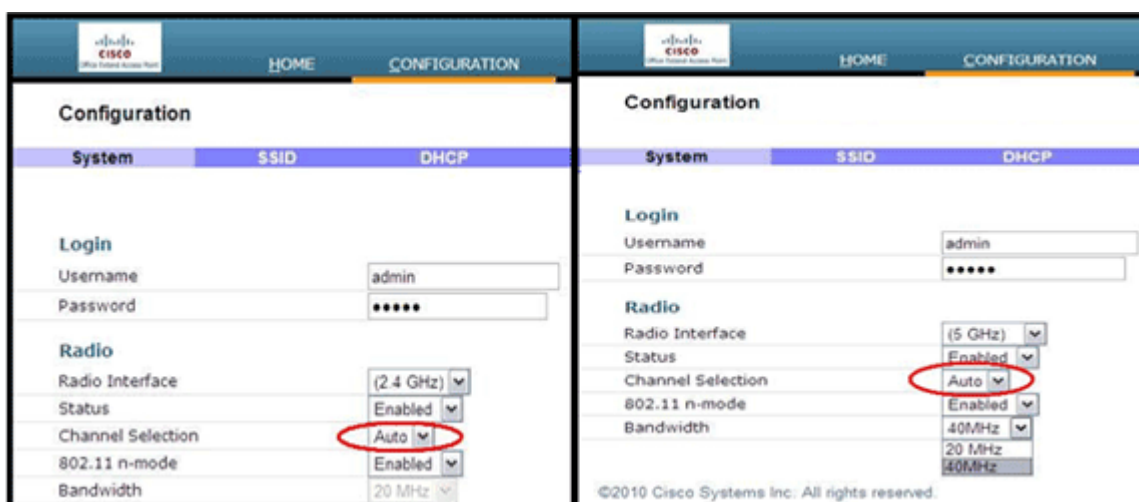
Die Steuerung der Funkmodule für die Serie 600 erfolgt über die lokale Benutzeroberfläche der Serie 600 und nicht über den Wireless LAN Controller.

Wenn Sie versuchen, den Spektrumskanal zu steuern, die Stromversorgung zu aktivieren oder die Funkverbindung über den Controller zu deaktivieren, hat dies keine Auswirkungen auf die Serie 600.

Die 600-Serie scannt und wählt beim Start Kanäle für 2,4 GHz und 5,0 GHz aus, solange die Standardeinstellungen auf der lokalen Benutzeroberfläche in beiden Spektren als Standard beibehalten werden.

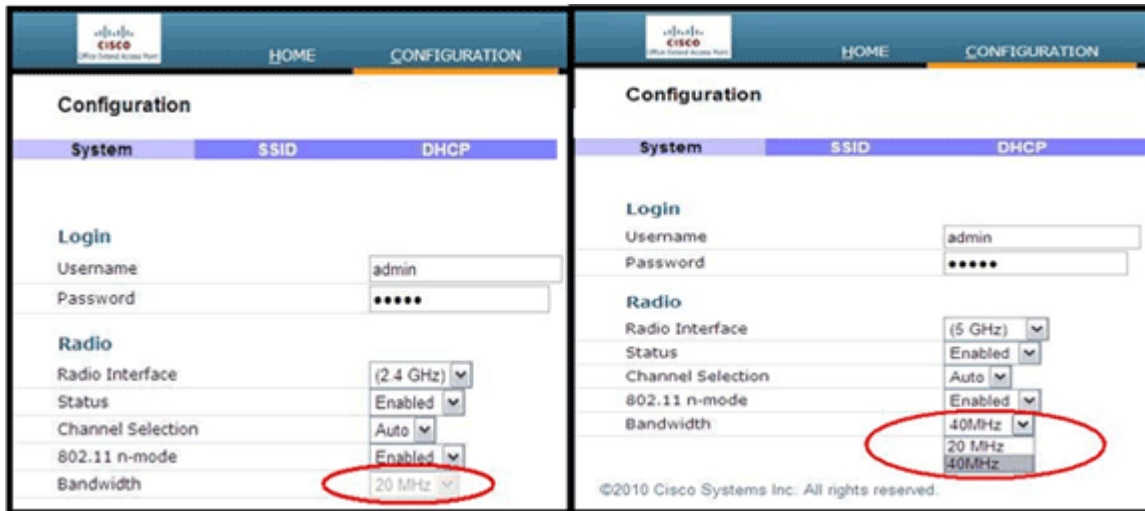
Hinweis: Wenn der Benutzer, wie bereits erwähnt, ein oder beide Funkmodule lokal deaktiviert (dieses Funkmodul ist auch für den Zugriff durch das Unternehmen deaktiviert), übersteigen RRM und erweiterte Funktionen wie Monitor, H-REAP, Sniffer die Funktionen des Cisco Aironet OEAP der Serie 600, das für den Einsatz zu Hause und für Telearbeiter positioniert ist.

Die Kanalauswahl und die Bandbreite für 5,0 GHz werden hier auf der lokalen Benutzeroberfläche des Cisco Aironet OEAP der Serie 600 konfiguriert.



Hinweise:

- Die 20- und 40-MHz-Einstellungen für 5 GHz sind verfügbar.
- Die 2,4-GHz-Frequenz von 40 MHz wird nicht unterstützt und ist auf 20 MHz festgelegt.
- Eine Bandbreite von 40 MHz (Channel Bonding) wird bei 2,4 GHz nicht unterstützt.

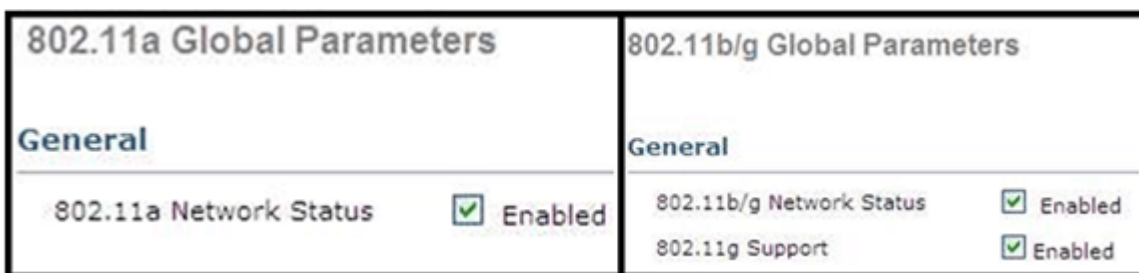


Zusätzliche Hinweise

Die Cisco Aironet Serie 600 OEAP wurde für Einzelzugriffs-Bereitstellungen entwickelt. Daher wird Client-Roaming zwischen den 600-Serien nicht unterstützt.

Hinweis: Durch Deaktivieren von 802.11a/n oder 802.11b/g/n auf dem Controller werden diese Spektren auf dem OEAP der Cisco Aironet Serie 600 möglicherweise nicht deaktiviert, da die lokale SSID möglicherweise weiterhin funktioniert.

Der Endbenutzer hat die Kontrolle über die Funkmodule innerhalb des OEAP der Cisco Aironet Serie 600 aktiviert/deaktiviert.



802.1x-Unterstützung für kabelgebundenen Port

In dieser ersten Version wird 802.1x nur von der Befehlszeilenschnittstelle (CLI) unterstützt.

Hinweis: Die GUI-Unterstützung wurde noch nicht hinzugefügt.

Dies ist der kabelgebundene Port (Port #4 in gelb) auf der Rückseite des Cisco Aironet OEAP der Serie 600 und ist mit dem Remote-LAN verbunden (siehe vorheriger Abschnitt zur Konfiguration des Remote-LAN).

Sie können jederzeit den Befehl **show** verwenden, um die aktuelle LAN-Fernkonfiguration anzuzeigen:

```
<#root>
```

```
show remote-lan <remote-lan-id>
```

Um die Remote-LAN-Konfiguration zu ändern, müssen Sie sie zunächst deaktivieren:

```
<#root>
```

```
remote-lan disable <remote-lan-id>
```

802.1X-Authentifizierung für das Remote-LAN aktivieren:

```
<#root>
```

```
config remote-lan security 802.1X enable <remote-lan-id>
```

Sie können sie mit dem folgenden Befehl rückgängig machen:

```
<#root>
```

```
config remote-lan security 802.1X disable <remote-lan-id>
```

Für das Remote-LAN ist "Encryption" immer "None" (Keine) (wie in **show remote-lan** angezeigt) und kann nicht konfiguriert werden.

Wenn Sie einen lokalen EAP (im Controller) als Authentifizierungsserver verwenden möchten:

```
<#root>
```

```
config remote-lan local-auth enable <profile-name> <remote-lan-id>
```

Dabei wird das Profil entweder über die Controller-GUI (Sicherheit > Lokales EAP) oder über die CLI (**config local-auth**) definiert. Weitere Informationen zu diesem Befehl finden Sie im Controller-Handbuch.

Sie können es mit folgendem Befehl rückgängig machen:

```
<#root>
```

```
config remote-lan local-auth disable <remote-lan-id>
```

Wenn Sie einen externen AAA-Authentifizierungsserver verwenden:

- **config remote-lan radius_server auth add/delete <remote-lan-id> <server-id>**

- **config remote-lan radius_server auth enable/disable** <remote-lan-id>

Hierbei wird der Server über die grafische Benutzeroberfläche des Controllers (Sicherheit > RADIUS > Authentifizierung) oder die CLI (**Konfigurationsradius-Authentifizierung**) konfiguriert. Weitere Informationen zu diesem Befehl finden Sie im Controller-Handbuch.

Aktivieren Sie nach Abschluss der Konfiguration das Remote-LAN:

```
<#root>
```

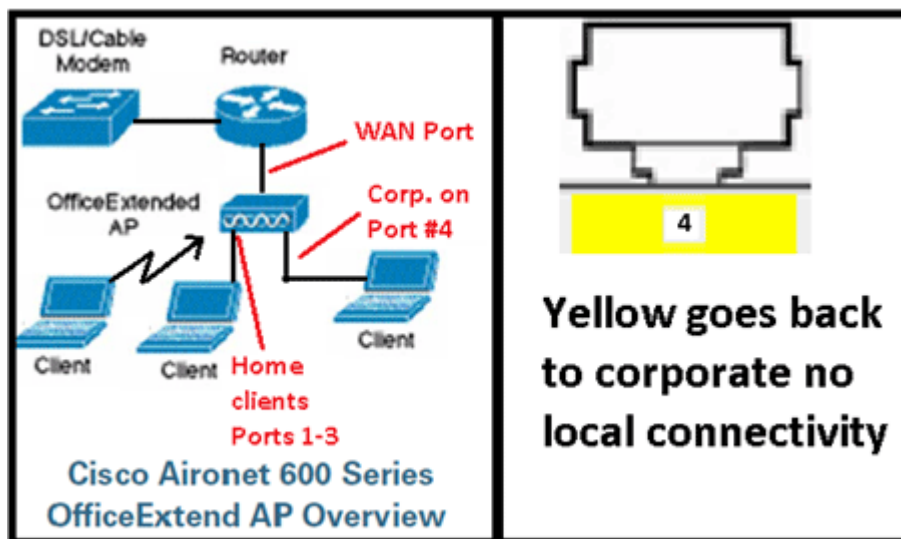
```
config remote-lan enable <remote-lan-id>
```

Verwenden Sie den Befehl **show remote-lan** <remote-lan-id>, um Ihre Einstellung zu überprüfen.

Für den Remote-LAN-Client muss die 802.1X-Authentifizierung aktiviert und entsprechend konfiguriert werden. Weitere Informationen finden Sie im Benutzerhandbuch Ihres Geräts.

Konfiguration des OEAP-600-Access Points

Dieses Bild zeigt das Verdrahtungsdiagramm für das OEAP der Cisco Aironet Serie 600:

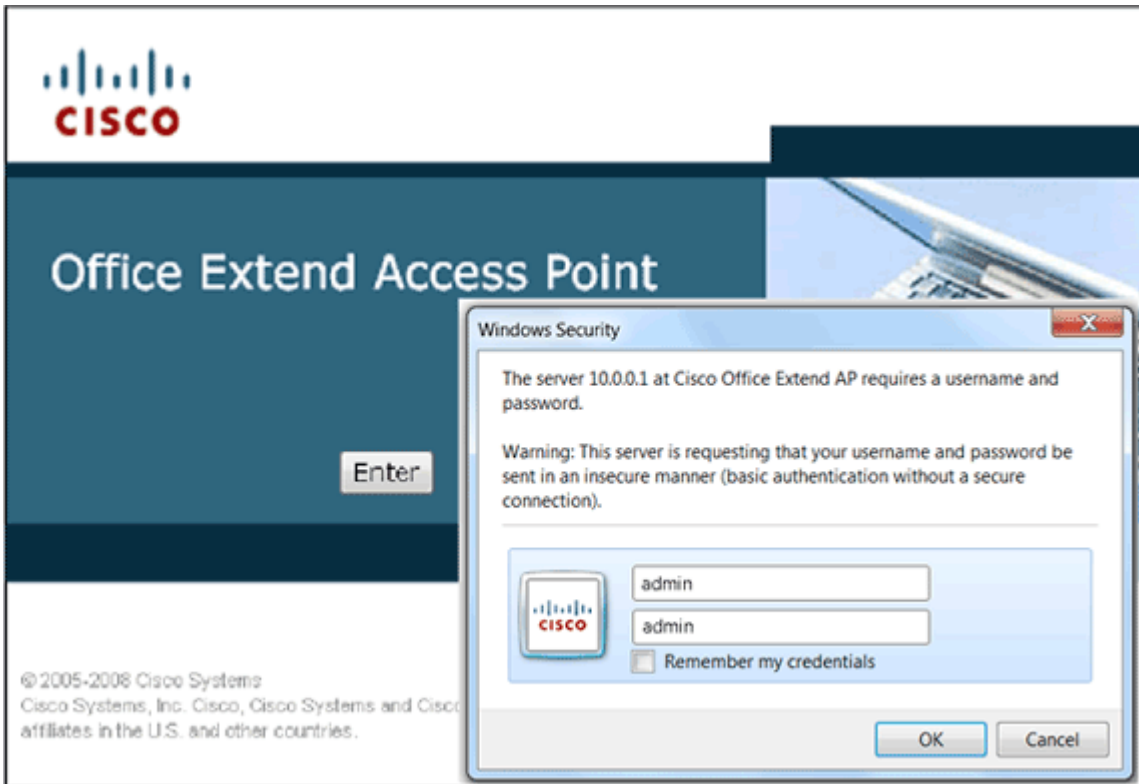


Der standardmäßige DHCP-Bereich des OEAP der Cisco Aironet Serie 600 ist 10.0.0.x, sodass Sie mit der Adresse 10.0.0.1 zum Access Point an den Ports 1-3 wechseln können. Standardmäßig lauten Benutzername und Kennwort admin.

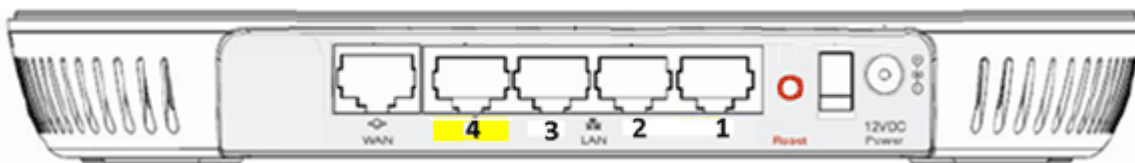
Hinweis: Dies unterscheidet sich vom AP1040, 1130, 1140 und 3502i, bei denen Cisco als Benutzername und Kennwort verwendet wurde.

Wenn die Funkmodule hochgefahren sind und bereits eine persönliche SSID konfiguriert wurde, können Sie drahtlos auf den Konfigurationsbildschirm zugreifen. Andernfalls müssen Sie die lokalen Ethernet-Ports 1-3 verwenden.

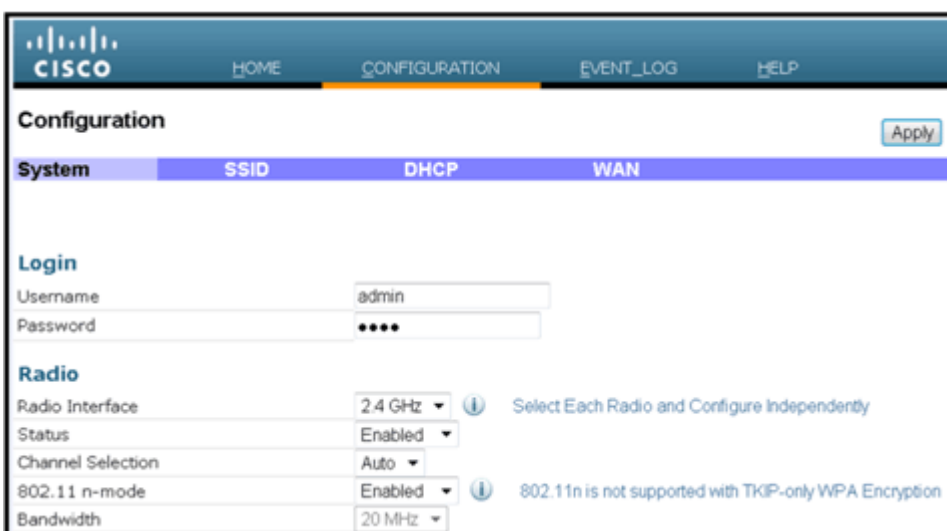
Für die Anmeldung sind der Standardbenutzername und das Standardkennwort admin.



Hinweis: Der gelbe Port #4 ist nicht für die lokale Verwendung aktiv. Wenn auf dem Controller ein Remote-LAN konfiguriert ist, wird dieser Port nach erfolgreicher Verbindung des Access Points mit dem Controller zurücktunnelt. Verwenden Sie zum Navigieren zum Gerät lokal die Ports 1-3:



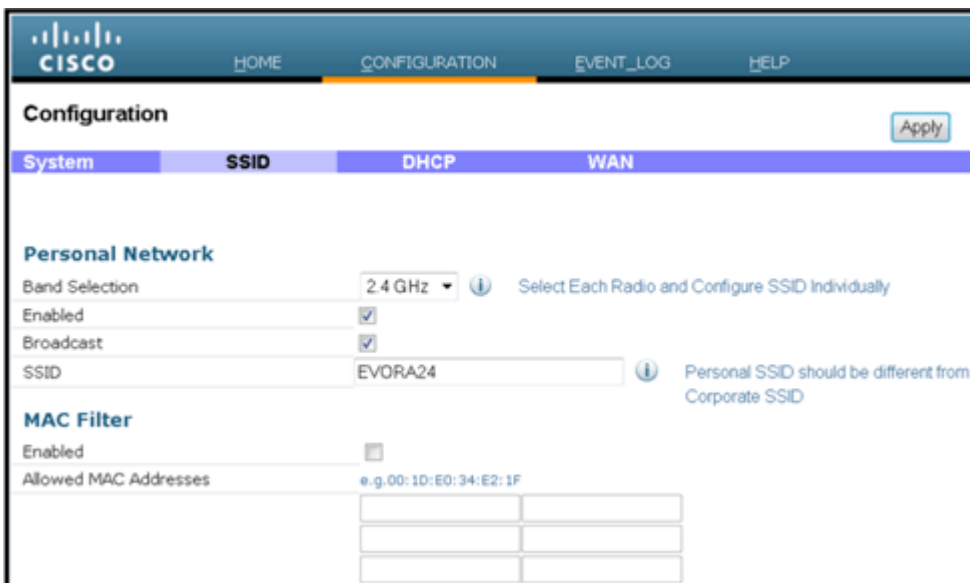
Sobald Sie erfolgreich zum Gerät navigieren, wird der Hauptstatusbildschirm angezeigt. Dieser Bildschirm enthält Funk- und MAC-Statistiken. Wenn keine Funkmodule konfiguriert wurden, kann der Benutzer auf dem Konfigurationsbildschirm die Funkmodule aktivieren, Kanäle und Modi festlegen, lokale SSIDs konfigurieren und die WLAN-Einstellungen aktivieren.



Auf dem SSID-Bildschirm kann der Benutzer das persönliche WLAN-Netzwerk konfigurieren. Die SSID

und die Sicherheitsparameter für die Funkverbindung des Unternehmens werden eingerichtet und vom Controller nach unten verschoben (nachdem Sie das WAN mit der IP des Controllers konfiguriert haben), und die Verbindung wurde erfolgreich hergestellt.

Dieses Bild zeigt eine lokale SSID-MAC-Filterkonfiguration:



Nachdem der Benutzer die persönliche SSID konfiguriert hat, kann der Benutzer auf dem folgenden Bildschirm die Sicherheit für die private SSID zu Hause einrichten, Funkmodule aktivieren und bei Bedarf die MAC-Filterung konfigurieren. Wenn das persönliche Netzwerk 802.11n-Raten verwendet, wird empfohlen, dass der Benutzer einen Authentifizierungstyp, einen Verschlüsselungstyp und eine Passphrase auswählt, die WPA2-PSK und AES aktivieren.

Hinweis: Diese SSID-Einstellungen unterscheiden sich von den Unternehmenseinstellungen, wenn der Benutzer eines oder beide Funkmodule deaktiviert (beide sind auch für den geschäftlichen Gebrauch deaktiviert).

Benutzer, die lokal auf die Einstellungen der Admin-Steuerung zugreifen können, haben die Kontrolle über Kernfunktionen wie Aktivieren/Deaktivieren von Funkmodulen, es sei denn, das Gerät ist durch den Administrator kennwortgeschützt und konfiguriert. Daher muss darauf geachtet werden, dass nicht beide Funkmodule deaktiviert werden, da dies zu einem Verbindungsverlust führen kann, selbst wenn das Gerät erfolgreich in den Controller integriert wird.

Dieses Bild zeigt die Systemsicherheitseinstellungen:



Es wird davon ausgegangen, dass der Telearbeiter zu Hause den Cisco Aironet OEAP der Serie 600 hinter einem Heimrouter installiert, da dieses Produkt nicht als Ersatz für die Funktionalität eines Heimrouters

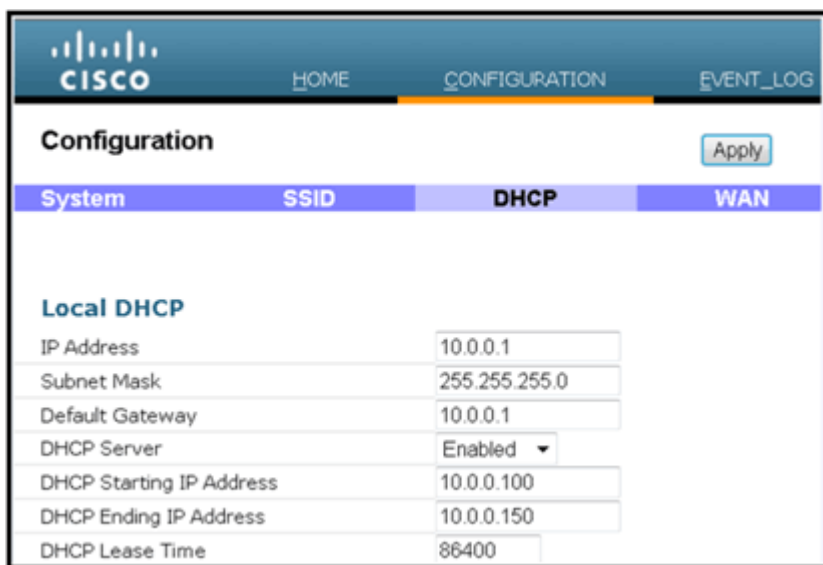
konzipiert ist. Dies liegt daran, dass die aktuelle Version dieses Produkts keine Firewall-, PPPoE- oder Port Forwarding-Unterstützung bietet. Dies sind Funktionen, die Kunden von einem Heimrouter erwarten.

Dieses Produkt kann zwar ohne Heimrouter eingesetzt werden, es wird jedoch aus den genannten Gründen empfohlen, diesen Router nicht entsprechend zu positionieren. Außerdem können Kompatibilitätsprobleme auftreten, wenn eine direkte Verbindung zu einigen Modems hergestellt wird.

Da die meisten Heim-Router einen DHCP-Bereich im Bereich 192.168.x.x haben, verfügt dieses Gerät über den Standard-DHCP-Bereich 10.0.0.x und ist konfigurierbar.

Wenn der Heimrouter zufällig 10.0.0.x verwendet, müssen Sie den OEAP der Cisco Aironet Serie 600 so konfigurieren, dass er eine 192.168.1.x- oder kompatible IP-Adresse verwendet, um Netzwerkkonflikte zu vermeiden.

Dieses Bild zeigt eine DHCP-Bereichskonfiguration:



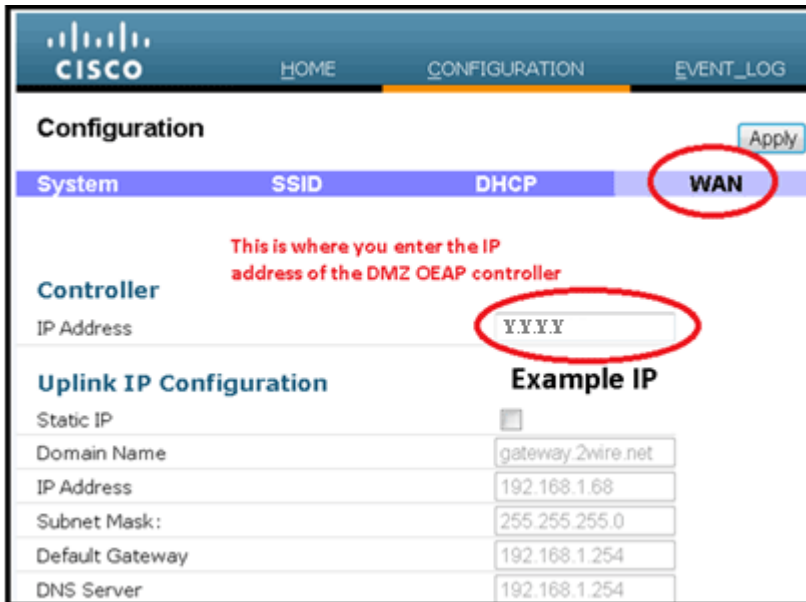
The screenshot shows the Cisco configuration interface for a device. The top navigation bar includes 'HOME', 'CONFIGURATION', and 'EVENT_LOG'. The main section is titled 'Configuration' and contains an 'Apply' button. Below this is a table with columns for 'System', 'SSID', 'DHCP', and 'WAN'. The 'Local DHCP' section is expanded, showing the following settings:

System	SSID	DHCP	WAN
Local DHCP			
IP Address		10.0.0.1	
Subnet Mask		255.255.255.0	
Default Gateway		10.0.0.1	
DHCP Server		Enabled	
DHCP Starting IP Address		10.0.0.100	
DHCP Ending IP Address		10.0.0.150	
DHCP Lease Time		86400	

Achtung: Wenn das OEAP der Cisco Aironet Serie 600 nicht vom IT-Administrator bereitgestellt oder konfiguriert wird, muss der Benutzer die IP-Adresse des Unternehmens-Controllers eingeben (siehe unten), damit der Access Point dem Controller erfolgreich beitreten kann. Nach dem erfolgreichen Beitritt sollte der WAP das neueste Image vom Controller und die Konfigurationsparameter wie die WLAN-Einstellungen des Unternehmens herunterladen. Bei entsprechender Konfiguration wurde für die Remote-LAN-Einstellungen der Port #4 auf der Rückseite des Cisco Aironet OEAP der Serie 600 verwendet.

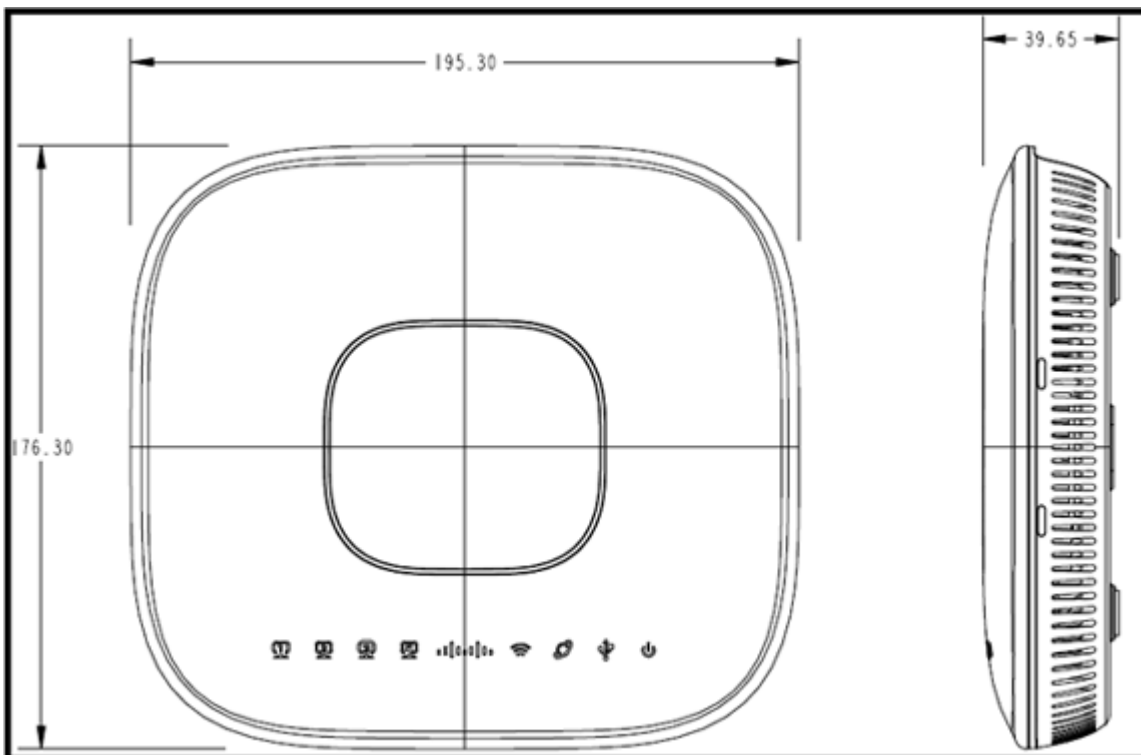
Wenn der Controller nicht hinzugefügt wird, stellen Sie sicher, dass die IP-Adresse des Controllers über das Internet erreichbar ist. Wenn die MAC-Filterung aktiviert ist, stellen Sie sicher, dass die MAC-Adresse erfolgreich in den Controller eingegeben wurde.

Dieses Bild zeigt die IP-Adresse des Cisco Aironet OEAP-Controllers der Serie 600:



OEAP-600 Access Point - Hardwareinstallation

Dieses Bild zeigt die physischen Aspekte des OEAP der Cisco Aironet Serie 600:

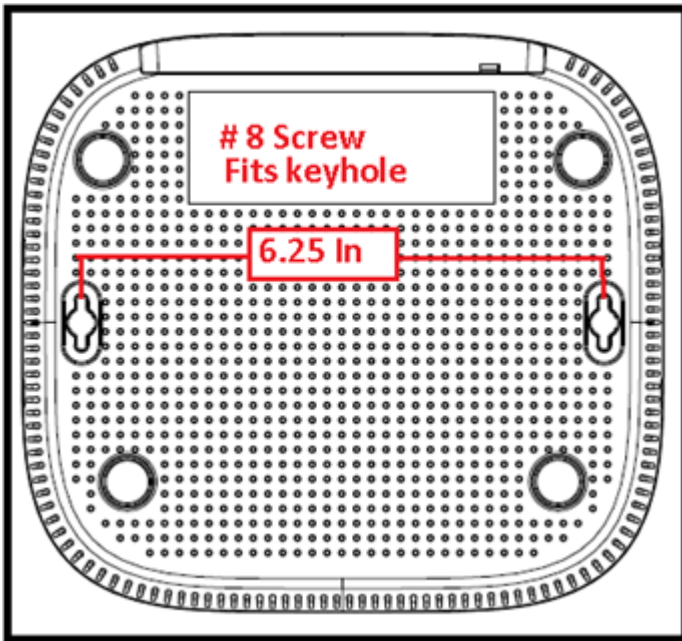


Dieser Access Point ist für die Montage auf einem Tisch ausgelegt und verfügt über GummifüÙe. Es kann auch an der Wand montiert werden, oder aufrecht sitzen mit der mitgelieferten Wiege. Versuchen Sie, den Access Point so nahe wie möglich an den vorgesehenen Benutzern zu platzieren. Vermeiden Sie Bereiche mit großen Metalloberflächen, wie z. B. das Aufstellen des Geräts auf einem Metallschreibtisch oder in der Nähe eines großen Spiegels. Je mehr Wände und Objekte sich zwischen dem Access Point und dem Benutzer befinden, desto geringer ist die Signalstärke und desto geringer ist die Leistung.

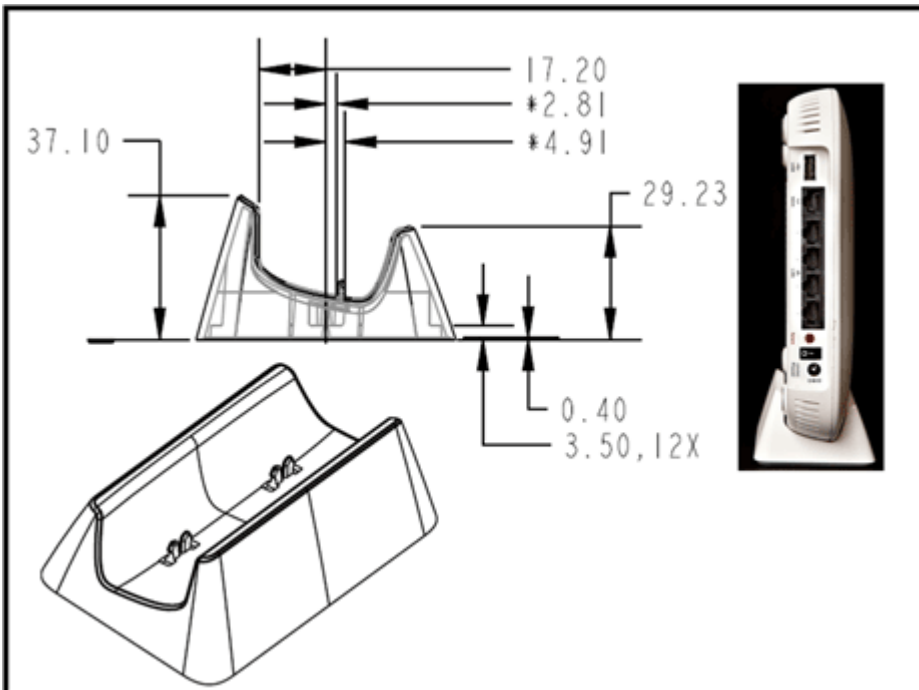
Hinweis: Dieser Access Point verwendet ein +12-Volt-Netzteil und verwendet kein Power over Ethernet (PoE). Außerdem liefert das Gerät kein PoE. Stellen Sie sicher, dass der richtige Netzadapter mit dem Access Point verwendet wird. Stellen Sie außerdem sicher, dass Sie keine anderen Adapter von anderen

Geräten wie Laptops und IP-Telefone verwenden, da diese den Access Point beschädigen können.

Das Gerät kann mit Kunststoffdübeln oder Holzschrauben an der Wand befestigt werden.



Die Einheit kann mit der mitgelieferten Halterung aufrecht montiert werden.



Die Cisco Aironet Serie 600 OEAP verfügt über Antennen, die sich an den Rändern des AP befinden. Der Benutzer sollte darauf achten, den Access Point nicht in Bereiche in der Nähe von Metallgegenständen oder Hindernissen zu platzieren, die eine Richtungsänderung oder Abnahme des Signals verursachen können. Die Antennenverstärkung beträgt in beiden Bändern ca. 2 dBi und ist für eine Abstrahlung in einem 360-Grad-Muster ausgelegt. Ähnlich wie bei einer Glühbirne (ohne Lampenschirm), ist das Ziel, in alle Richtungen zu strahlen. Stellen Sie sich den Access Point wie eine Lampe vor, und versuchen Sie, ihn in unmittelbarer Nähe der Benutzer anzuordnen.

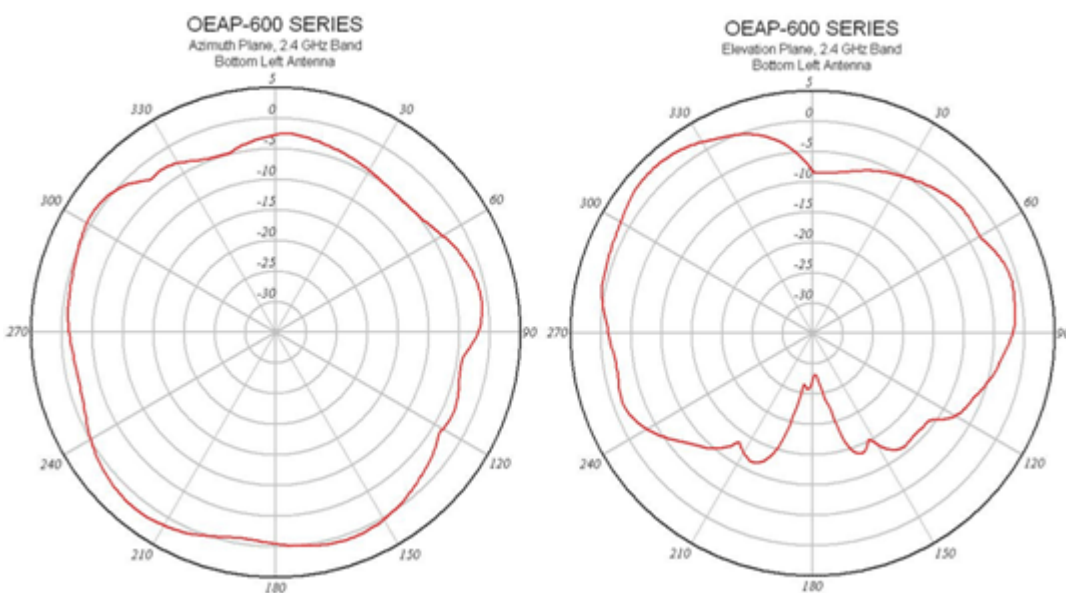
Metallobjekte wie Spiegel behindern das Signal ähnlich wie die Lampenschirm-Analogie. Der Durchsatz oder die Reichweite kann beeinträchtigt werden, wenn das Signal in feste Objekte eindringen oder diese

durchdringen muss. Wenn Sie eine Konnektivität erwarten, z. B. in einem dreistöckigen Zuhause, vermeiden Sie es, den AP im Untergeschoss zu platzieren, und versuchen Sie, den AP an einer zentralen Stelle im Zuhause zu montieren.

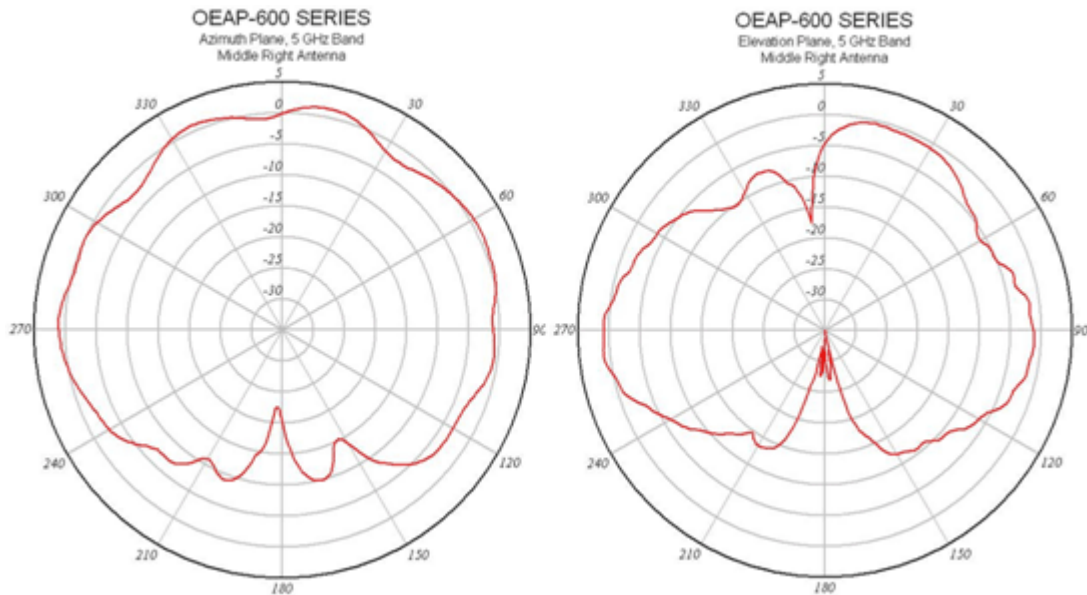
Der Access Point verfügt über sechs Antennen (drei pro Band).



Dieses Bild zeigt ein 2,4-GHz-Antennenstrahlungsmuster (aufgenommen von der Antenne unten links).



Dieses Bild zeigt ein 5-GHz-Antennenstrahlungsmuster (von der Mitte-Rechts-Antenne):



Fehlerbehebung beim OEAP-600

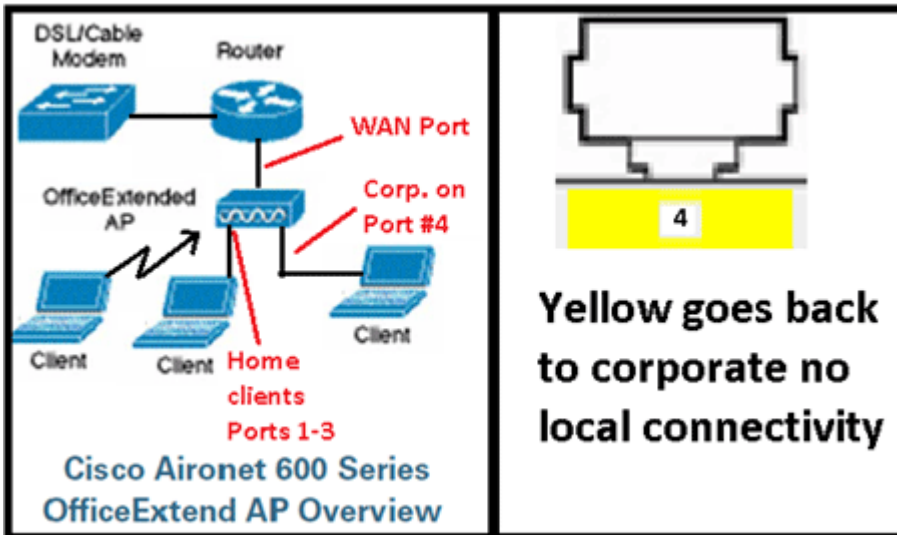
Überprüfen Sie, ob die erste Verkabelung richtig ist. Dies bestätigt, dass der WAN-Port am Cisco Aironet OEAP der Serie 600 mit dem Router verbunden ist und erfolgreich eine IP-Adresse erhalten kann. Wenn der Access Point nicht mit dem Controller verbunden zu sein scheint, schließen Sie einen PC an Port 1-3 (private Client-Ports) an, und prüfen Sie, ob Sie mit der Standard-IP-Adresse 10.0.0.1 zum Access Point wechseln können. Standardmäßig lautet Benutzername und Kennwort admin.

Überprüfen Sie, ob die IP-Adresse für den Unternehmens-Controller eingestellt ist. Wenn nicht, geben Sie die IP-Adresse ein, und starten Sie das OEAP der Cisco Aironet Serie 600 neu, damit eine Verbindung zum Controller hergestellt werden kann.

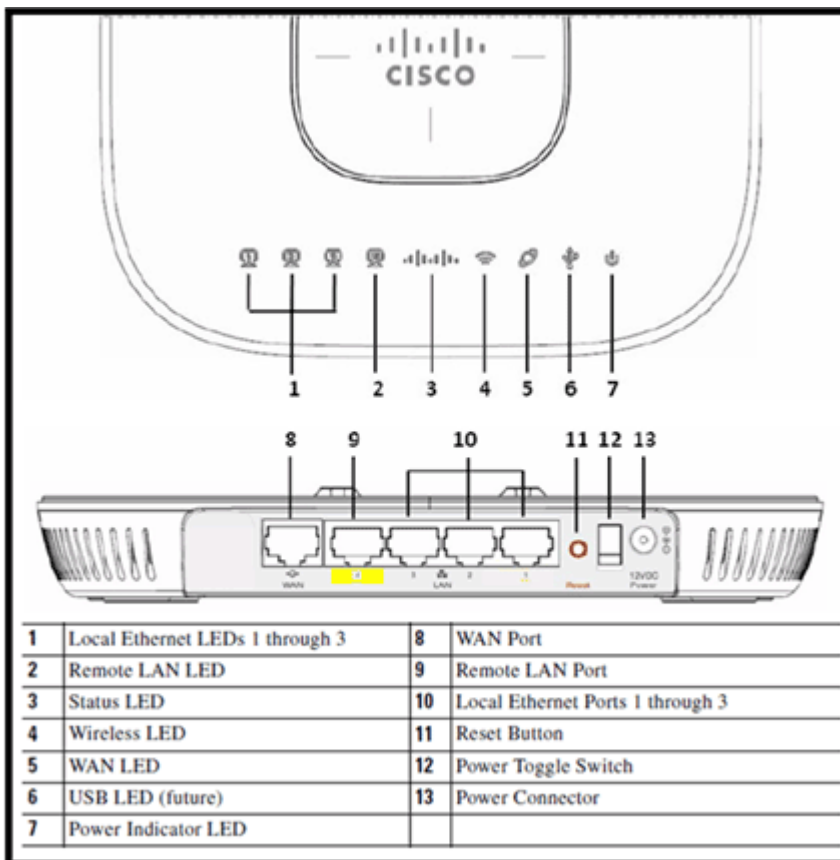
Hinweis: Der Unternehmensport #4 (gelb) kann nicht verwendet werden, um das Gerät zu Konfigurationszwecken zu öffnen. Dies ist im Wesentlichen ein "toter Port", es sei denn, ein Remote-LAN wird konfiguriert. Anschließend erfolgt die Tunnelverbindung zurück zum Unternehmen (für kabelgebundene Enterprise-Verbindungen verwendet).

Überprüfen Sie das Ereignisprotokoll, um zu sehen, wie die Zuordnung fortgeschritten ist (mehr dazu später).

Dieses Bild zeigt das OEAP-Verdrahtungsdiagramm für die Cisco Aironet Serie 600:



Dieses Bild zeigt die OEAP-Konnektivitätsports der Cisco Aironet Serie 600:

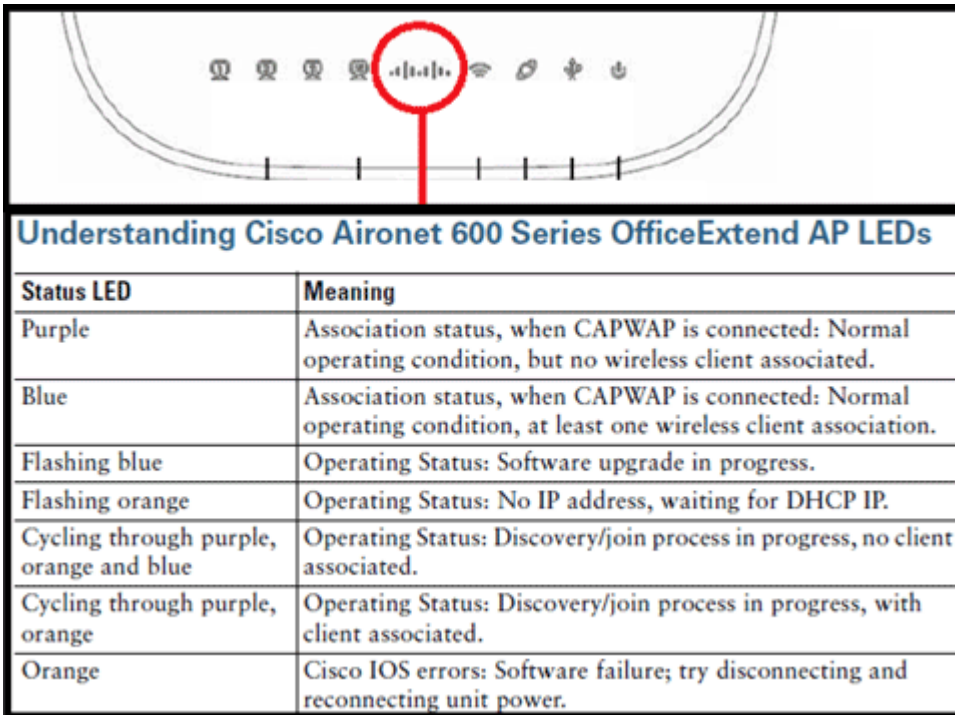


Wenn die Cisco Aironet OEAP-Module der Serie 600 nicht mit dem Controller verbunden werden können, sollten Sie die folgenden Elemente aktivieren:

1. Überprüfen Sie, ob der Router funktioniert und mit dem WAN-Port des OEAP der Cisco Aironet Serie 600 verbunden ist.
2. Schließen Sie einen PC an einen der Ports 1-3 des OEAP der Cisco Aironet Serie 600 an. Es sollte das Internet sehen.
3. Überprüfen Sie, ob sich die IP-Adresse des Unternehmens-Controllers im Access Point befindet.
4. Stellen Sie sicher, dass sich der Controller in der DMZ befindet und über das Internet erreichbar ist.

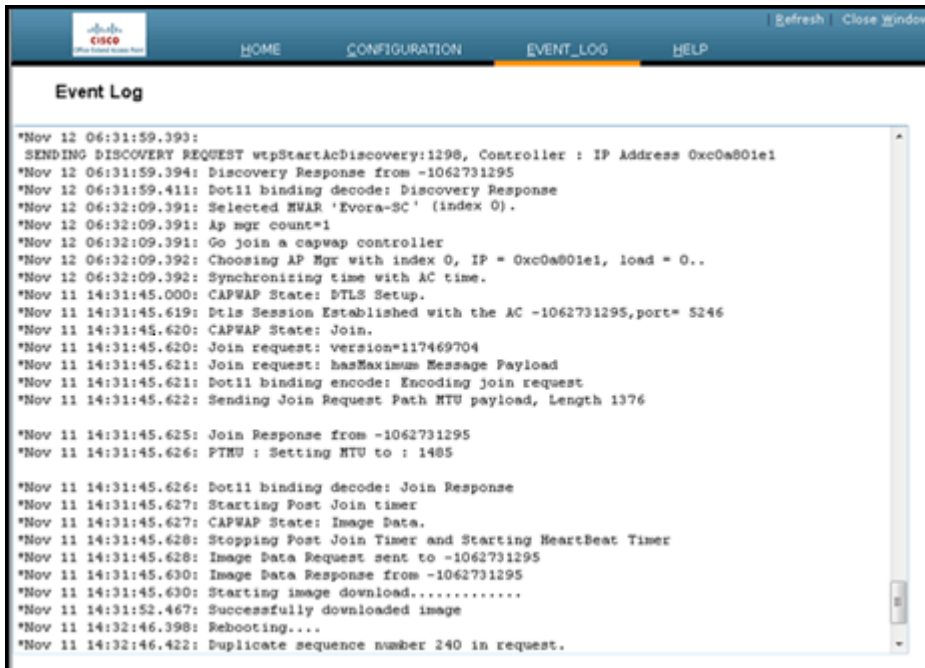
5. Überprüfen Sie die Verbindung, und vergewissern Sie sich, dass die Cisco Logo-LED blau oder lila leuchtet.
6. Lassen Sie genügend Zeit für den Fall, dass der Access Point ein neues Image laden und neu starten muss.
7. Wenn eine Firewall verwendet wird, stellen Sie sicher, dass die UDP 5246- und 5247-Ports nicht blockiert sind.

Dieses Bild zeigt die OEAP-Logo-LED der Cisco Aironet Serie 600:

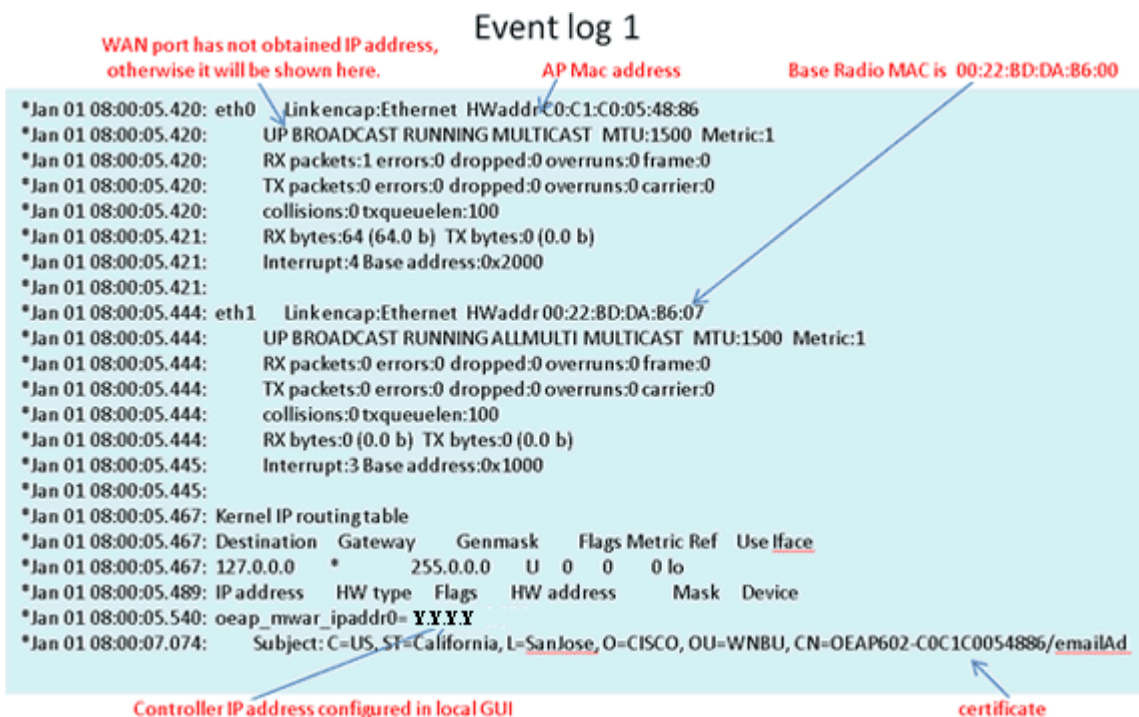


Wenn der Join-Vorgang fehlschlägt, wechselt die LED durch die Farben oder blinkt möglicherweise orange. Wenn dies der Fall ist, überprüfen Sie das Ereignisprotokoll auf weitere Details. Um zum Ereignisprotokoll zu gelangen, rufen Sie den Access Point auf (mit persönlicher SSID oder kabelgebundenen Ports 1-3), und erfassen Sie diese Daten für den IT-Administrator.

Dieses Bild zeigt das OEAP-Ereignisprotokoll der Cisco Aironet Serie 600:



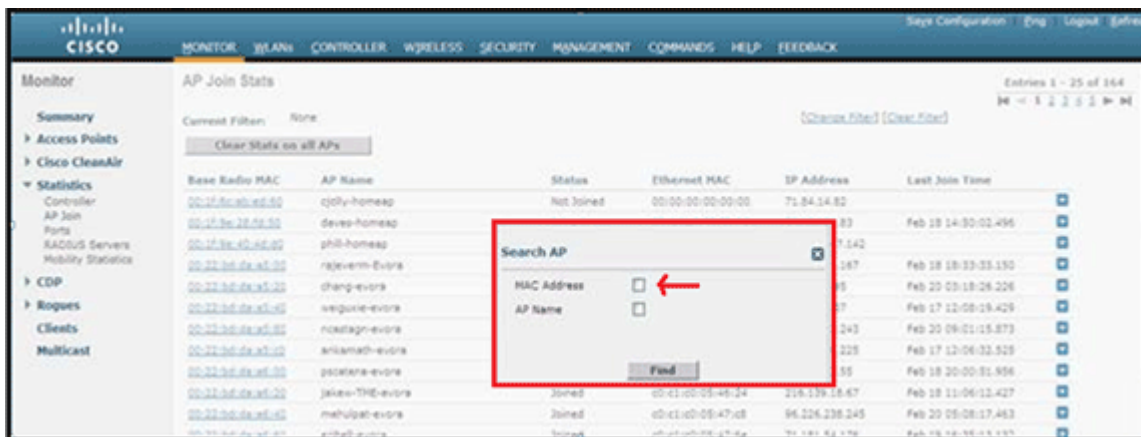
Wenn der Join-Prozess fehlschlägt und dies das erste Mal ist, dass OEAP der Cisco Aironet Serie 600 versucht, eine Verbindung zum Controller herzustellen, überprüfen Sie die AP-Join-Statistiken für OEAP der Cisco Aironet Serie 600. Dazu benötigen Sie die Basisfunk-MAC des AP. Diese finden Sie im Ereignisprotokoll. Hier ist ein Beispiel eines Ereignisprotokolls mit Kommentaren, die Sie bei der Interpretation unterstützen:



Sobald dies bekannt ist, können Sie in den Controller-Monitor-Statistiken feststellen, ob die Cisco Aironet OEAP der Serie 600 mit dem Controller verbunden ist oder noch nie mit dem Controller verbunden wurde. Außerdem sollte dies Aufschluss darüber geben, warum oder ob ein Fehler aufgetreten ist.

Wenn eine AP-Authentifizierung erforderlich ist, überprüfen Sie, ob die OEAP-Ethernet-MAC-Adresse (nicht die Funk-MAC-Adresse) der Cisco Aironet Serie 600 in Kleinbuchstaben in den Radius-Server eingegeben wurde. Sie können die Ethernet-MAC-Adresse auch aus dem Ereignisprotokoll ermitteln.

Suchen auf dem Controller nach OEAP der Cisco Aironet Serie 600



Wenn Sie festgestellt haben, dass der Zugriff auf das Internet von einem PC aus möglich ist, der mit dem lokalen Ethernet-Port verbunden ist, der Access Point jedoch weiterhin nicht dem Controller beitreten kann, und Sie bestätigt haben, dass die IP-Adresse des Controllers in der lokalen AP-GUI konfiguriert ist und erreichbar ist, stellen Sie sicher, dass der Access Point jemals erfolgreich beigetreten ist. Möglicherweise befindet sich der AP nicht im AAA-Server. Wenn das DTLS-Handshaking fehlschlägt, weist der Access Point möglicherweise ein fehlerhaftes Zertifikat oder einen Datums-/Uhrzeitfehler auf dem Controller auf.

Wenn keine Cisco Aironet OEAP-Einheiten der Serie 600 mit dem Controller verbunden werden können, stellen Sie sicher, dass der Controller in der DMZ erreichbar ist und die UDP-Ports 5246 und 5247 offen sind.

Debuggen von Clientzuordnungsproblemen

Der WAP verbindet den Controller ordnungsgemäß, aber der WLAN-Client kann keine Verbindung zum Unternehmens-SSID herstellen. Überprüfen Sie das Ereignisprotokoll, um festzustellen, ob eine Zuordnungsmeldung beim Access Point eingeht.

Die nächste Abbildung zeigt die normalen Ereignisse für die Client-Zuordnung mit der Unternehmens-SSID mit WPA oder WPA2. Für SSID mit offener Authentifizierung oder statischem WEP gibt es nur ein ADD MOBILE-Ereignis.

Ereignisprotokoll - Client-Zuordnung

```
*Feb 19 20:26:58.876: (Re)Assoc-Req from 00:24:d7:2a:72:c0 forwarded to WLC, wired: no
*Feb 19 20:26:58.941: received assoc-rsp for wireless client, status=0000
*Feb 19 20:26:58.942:
ADD_MOBILE from WLC,wmeEnabled=1,encrptPolicy=1
*Feb 19 20:26:58.942: ADD_MOBILE: client 00:24:d7:2a:72:c0, slot=0,vapid=1
*Feb 19 20:27:00.648:
ADD_MOBILE from WLC,wmeEnabled=1,encrptPolicy=4
*Feb 19 20:27:00.649: ADD_MOBILE: client 00:24:d7:2a:72:c0, slot=0,vapid=1
```

Wenn sich das (Re)Assoc-Req-Ereignis nicht im Protokoll befindet, stellen Sie sicher, dass der Client über die richtigen Sicherheitseinstellungen verfügt.

Wenn ein (Re)Assoc-Req-Ereignis im Protokoll angezeigt wird, der Client jedoch keine ordnungsgemäße

Zuordnung herstellen kann, aktivieren Sie den Befehl **debug client <MAC address>** auf dem Controller für den Client, und untersuchen Sie das Problem auf die gleiche Weise wie ein Client, der mit anderen Access Points von Cisco arbeitet, die nicht OEAP sind.

Interpretieren des Ereignisprotokolls

Die folgenden Ereignisprotokolle mit Kommentaren können Ihnen bei der Fehlerbehebung für andere OEAP-Verbindungsprobleme mit der Cisco Aironet Serie 600 helfen.

Nachfolgend finden Sie einige Beispiele aus den OEAP-Ereignisprotokolldateien der Cisco Aironet Serie 600 mit Kommentaren zur besseren Interpretation des Ereignisprotokolls:

Event log 2

```

*Jan 01 08:00:07.093: Build version 7.0.112.66 (compiled Feb 19 2011 at 16:29:58).
*Jan 01 08:00:08.975: CAPWAPState: Init.
*Jan 01 08:00:09.009: CAPWAPState: Discovery.
*Jan 01 08:00:09.042: Starting Discovery.
*Jan 01 08:00:09.044: CAPWAPState: Discovery.
*Jan 01 08:00:09.193: Discovery Request sent to Y.Y.Y.Y with discovery type set to 1
*Jan 01 08:00:09.194: Discovery Request sent to Y.Y.Y.Y with discovery type set to 1
*Jan 01 08:00:09.194:
SENDING DISCOVERY REQUEST wtpStartAcDiscovery:1338, Controller Cisco_7d:88:00: IP Address
*Jan 01 08:00:09.195: Discovery Request sent to Y.Y.Y.Y with discovery type set to 0
*Jan 01 08:00:09.256: Discovery Response from Y.Y.Y.Y
*Jan 01 08:00:09.272: Dot11 binding decode: Discovery Response
*Jan 01 08:00:09.272: wtpDecodeDiscoveryResponse Discovery Latency: 0, WLC: IP= Y.Y.Y.Y , name=Cisco_7d:88:00, index
*Jan 01 08:00:09.272: Discovery Response from Y.Y.Y.Y
*Jan 01 08:00:09.273: Dot11 binding decode: Discovery Response
*Jan 01 08:00:09.273: wtpDecodeDiscoveryResponse Discovery Latency: 0, WLC: IP= Y.Y.Y.Y , name=Cisco_7d:88:00, index
*Jan 01 08:00:09.273: Discovery Response from Y.Y.Y.Y
*Jan 01 08:00:09.274: Dot11 binding decode: Discovery Response
*Jan 01 08:00:09.274: wtpDecodeDiscoveryResponse Discovery Latency: 0, WLC: IP= Y.Y.Y.Y , name=Cisco_7d:88:00, index
*Jan 01 08:00:12.133: Dropping dtls packet since session is not established. ab462383, 147e, c0a80121, 147e, 0
*Jan 01 08:00:19.182: Selected MWAR 'Cisco_7d:88:00'(index 0).
*Jan 01 08:00:19.183: Selected MWAR 'Cisco_7d:88:00' (index 0).
*Jan 01 08:00:19.183: Ap mgr count=1
*Jan 01 08:00:19.183: Go join a capwap controller
*Jan 01 08:00:19.183: Choosing AP Mgr with index 0, IP = Y.Y.Y.Y ,load=151.
*Jan 01 08:00:19.183: Synchronizing time with AC time.
*Feb 19 23:33:56.000: CAPWAPState: DTLS Setup.
*Feb 19 23:34:16.813: Dtls Session Established with the AC Y.Y.Y.Y , port= 5246

```

**Discovery Request sent
If AP can not get IP address,
then Discovery Req. will not be sent**

**Discovery resp. received from
controller. If no response from
controller, then need to check
whether controller
is accessible**

Selected controller to join, timestamp synced to the controller

**DTLS handshaking with the controller
completed. If certificate has problem, then
the failure will happen here**

Event log 3

```

*Feb 19 23:34:16.813: CAPWAPState: Join.
*Feb 19 23:34:16.814: Join request: version=7.0.114.76

*Feb 19 23:34:16.815: Join request: hasMaximum Message Payload
*Feb 19 23:34:16.815: Dot11 binding encode: Encoding join request
*Feb 19 23:34:16.815: Sending Join Request Path MTU payload, Length 1376

*Feb 19 23:34:16.887: Join Response from Y.Y.Y.Y
*Feb 19 23:34:16.888: PTMU: Setting MTU to: 1485

*Feb 19 23:34:16.888: Dot11 binding decode: Join Response
*Feb 19 23:34:16.889: Starting Post Join timer
*Feb 19 23:34:16.890: CAPWAPState: Image Data.
*Feb 19 23:34:16.890: Controller Version: 7.0.114.76
*Feb 19 23:34:16.890: AP Version: 7.0.114.76
*Feb 19 23:34:16.891: CAPWAPState: Configure.
*Feb 19 23:34:16.891: Dot11 binding encode: Encoding configuration status request.
*Feb 19 23:34:16.893: lwapp_encode_ap_reset_button_payload: reset button state off
*Feb 19 23:34:16.895: Configuration Status sent to Y.Y.Y.Y
*Feb 19 23:34:17.019: Configuration Status Response from Y.Y.Y.Y
*Feb 19 23:34:17.022: CAPWAPState: Run.
*Feb 19 23:34:17.022: Dot11 binding encode: Encoding change state event request.
*Feb 19 23:34:17.023: CAPWAPState: Run.

```

**Join Resp. from controller
If AP is not added to AAA server,
this step will fail.**

**Controller and AP have same version
SW, no image download is need. When
controller is upgraded to new version
SW, image download will happen.**

Capwap configuration completes

Event log 4

```
*Feb 19 23:34:17.023: CAPWAP moved to RUN state stopping post join timer
*Feb 19 23:34:17.399: capwapWtpDlForwarding() returned 1

*Feb 19 23:34:17.602: capwapWtpDlForwarding() returned 1

*Feb 19 23:34:17.762: Change State Event Response from -1421466749
*Feb 19 23:34:17.853: SSID alpha,WLAN ID 1, added to the slot[0], enabled
*Feb 19 23:34:18.045: SSID alpha_phone,WLAN ID 2, added to the slot[0], enabled
*Feb 19 23:34:18.118: Ethernet Backhaul WLAN ID = 3,qos=0

*Feb 19 23:34:18.281: SSID alpha,WLAN ID 1, added to the slot[1], enabled
*Feb 19 23:34:18.522: SSID alpha_phone,WLAN ID 2, added to the slot[1], enabled
```

WLANs are configured for 2.4 GHz Radio

Remote-lan is configured

WLANs are configured for 5 GHz Radio

Wenn die Internetverbindung unzuverlässig erscheint

Das Beispiel für ein Ereignisprotokoll in diesem Abschnitt kann auftreten, wenn die Internetverbindung ausfällt, sehr langsam ist oder unterbrochen wird. Dies kann durch Ihr ISP-Netzwerk, das ISP-Modem oder Ihren Router zu Hause verursacht werden. Manchmal wird die Verbindung vom ISP unterbrochen oder unterbrochen. In diesem Fall kann die CAPWAP-Verbindung (zurück zum Unternehmen) fehlschlagen oder Probleme haben.

Im Folgenden finden Sie ein Beispiel für einen solchen Fehler im Ereignisprotokoll:

```
*Feb 16 07:13:24.918: Re-Tx Count= 0, Max Re-Tx Value=5, NumofPendingMsgs=1
*Feb 16 07:13:36.919: Re-Tx Count= 4, Max Re-Tx Value=5, NumofPendingMsgs=2
*Feb 16 07:13:39.919: Max retransmission count exceeded going back to DISCOVER mode.
*Feb 16 07:13:39.919: Retransmission count for packet exceeded max{UNKNOWN_MESSAGE_TYPE (218103808), 2}
*Feb 16 07:13:39.919: Retransmission count exceeded max, ignoring as the ethernet is overloaded
*Feb 16 07:13:42.918: Re-Tx Count= 6, Max Re-Tx Value=5, NumofPendingMsgs=2
Comment : This Retransmission continues on..... Multiple times..
*Feb 16 07:13:42.919: Max retransmission count exceeded going back to DISCOVER mode.
*Feb 16 07:13:42.919: Retransmission count for packet exceeded max{UNKNOWN_MESSAGE_TYPE (218103808)
*Feb 16 07:14:09.919: GOING BACK TO DISCOVER MODE
*Feb 16 07:14:09.920: CAPWAP State: DTLS Teardown.
*Feb 16 07:14:14.918: DTLS session cleanup completed. Restarting capwap state machine.
*Feb 16 07:14:14.919:
Lost connection to the controller, going to re-start evora...
```

Zusätzliche Debug-Befehle

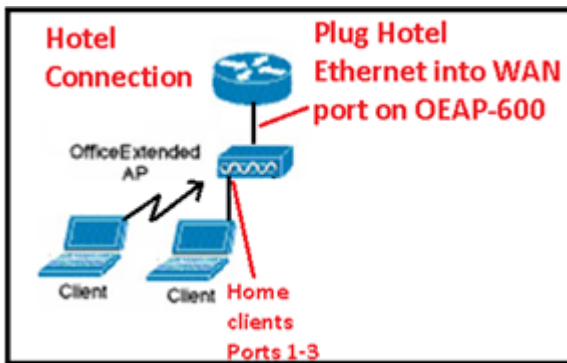
Wenn Sie das Cisco Aironet OEAP der Serie 600 in einem Hotel oder einem anderen Pay-for-Use-Bereich nutzen, bevor das Cisco Aironet OEAP der Serie 600 zurück zum Controller tunneln kann, müssen Sie durch den Walled Garden gelangen. Schließen Sie dazu einen Laptop an einen der verdrahteten lokalen Ports (Port 1-3) an, oder verwenden Sie einen persönlichen SSID, um sich beim Hotel anzumelden und den Splash-Screen zu befriedigen.

Sobald Sie vom Zuhause des Access Points aus über eine Internetverbindung verfügen, richtet die Einheit einen DTLS-Tunnel und die SSIDs Ihres Unternehmens ein. Anschließend wird der kabelgebundene Port #4 (vorausgesetzt, ein Remote-LAN ist konfiguriert) aktiviert.

Hinweis: Dieser Vorgang kann einige Minuten in Anspruch nehmen. Achten Sie darauf, wie die Cisco Logo-LED stetig blau oder lila leuchtet, um den erfolgreichen Beitritt anzuzeigen. An diesem Punkt sind sowohl die persönliche als auch die geschäftliche Anbindung aktiv.

Hinweis: Der Tunnel bricht, wenn das Hotel oder ein anderer ISP die Verbindung trennt (in der Regel 24 Stunden). Dann müssen Sie den gleichen Prozess neu starten. Dies ist von der Konstruktion her normal.

Dieses Bild zeigt Office Extend in der Pay-for-Use-Konfiguration:



In diesem Bild werden zusätzliche Debug-Befehle (Informationen zur Funkschnittstelle) angezeigt:

```
Below are the new diagnostics commands for the OEAP 600
The WLC CLI of "show tech" is:
debug ap enable <apname>
then:
debug ap command "evoraTechSupport" <apname> → the information about system and radio slot 0/1
debug ap command "evoraTechSupport 2" <apname> → more info about radio slot 0 (2.4G)
debug ap command "evoraTechSupport 3" <apname> → more info about radio slot 1 (5G)

The "show eventlog" is the same as other APs:
show ap eventlog <apname>
```

Bekanntes Problem/Problem

Wenn Sie die Konfigurationsdatei von einem Controller auf einen TFTP-/FTP-Server hochladen, werden Remote-LAN-Konfigurationen als WLAN-Konfigurationen hochgeladen. Weitere Informationen finden Sie in den [Versionshinweisen für Cisco Wireless LAN-Controller und Lightweight Access Points für Version 7.0.116.0](#).

Wenn beim OEAP-600 die CAPWAP-Verbindung aufgrund eines Authentifizierungsfehlers am Controller fehlschlägt, kann die Cisco Logo-LED am OEAP-600 für einige Zeit ausgeschaltet werden, bevor der OEAP-600 versucht, den CAPWAP-Versuch neu zu starten. Dies ist normal, Sie sollten sich also bewusst sein, dass der Access Point nicht abstürzt, wenn die Logo-LED vorübergehend ausgeschaltet wird.

Dieses OEAP-600-Produkt hat einen anderen Anmeldenamen als frühere OEAP Access Points, um mit Heimprodukten wie Linksys konsistent zu sein. Der Standardbenutzername lautet *admin* mit einem Kennwort *admin*. Die anderen Cisco OEAP Access Points wie AP-1130 und AP-1140 haben einen Standardbenutzernamen *Cisco* mit einem Passwort von *Cisco*.

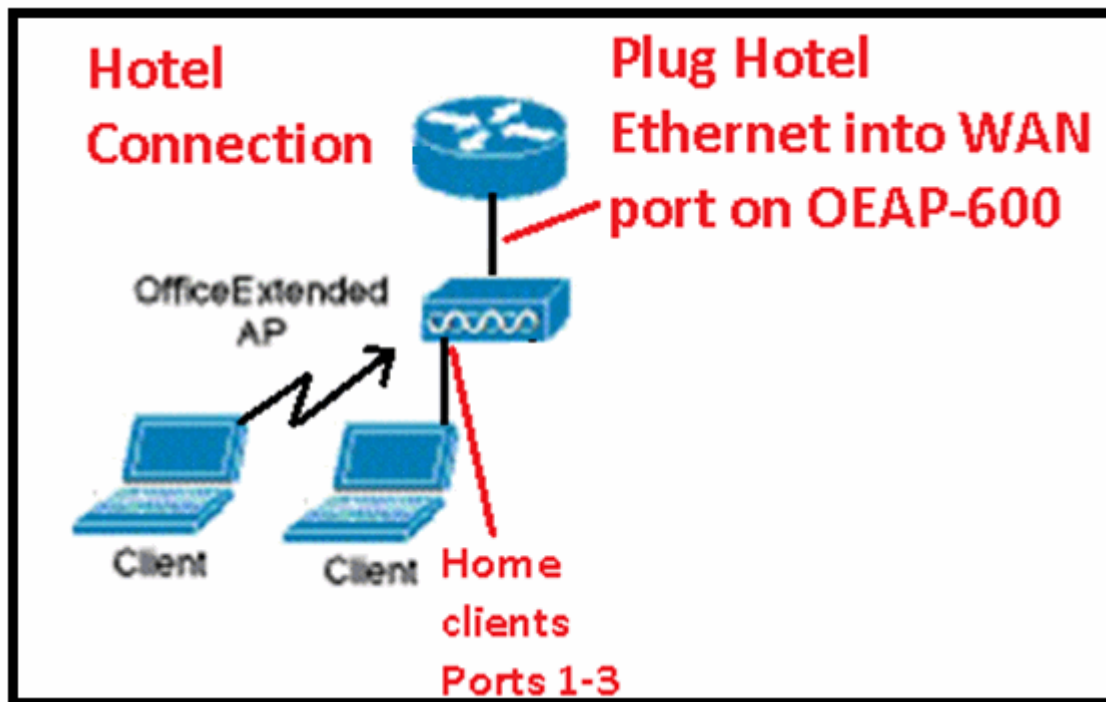
Diese erste Version von OEAP-600 unterstützt 802.1x, wird jedoch nur von der CLI unterstützt. Benutzer, die versuchen, Änderungen an der GUI vorzunehmen, können ihre Konfigurationen verlieren.

Wenn Sie den OEAP-600 in einem Hotel oder einem anderen Pay-for-Use-Bereich nutzen, bevor der OEAP-600 zum Controller zurücktunneln kann, müssen Sie durch den ummauerten Garten gelangen. Schließen Sie einfach einen Laptop an einen der verdrahteten lokalen Ports (Port 1-3) an, oder verwenden Sie einen persönlichen SSID-Login in das Hotel, um den Splash-Screen zu befriedigen. Sobald Sie über eine Internetverbindung von der Startseite des Access Points verfügen, richtet das Gerät einen DTLS-Tunnel ein, und die SSIDs Ihres Unternehmens sowie der kabelgebundene Port #4 werden aktiviert. Dies wird vorausgesetzt, dass Remote-LAN konfiguriert ist. Beachten Sie, dass dieser Vorgang einige Minuten dauern kann. Achten Sie auf die LED für das Cisco Logo, die stetig blau oder lila leuchtet, um den erfolgreichen

Beitritt anzuzeigen. An diesem Punkt sind sowohl die persönliche als auch die geschäftliche Anbindung aktiv.

Hinweis: Der Tunnel kann unterbrochen werden, wenn das Hotel oder ein anderer ISP die Verbindung trennt (in der Regel 24 Stunden), und Sie müssen den gleichen Prozess neu starten. Dies ist von der Konstruktion her normal.

Büro Erweiterung des Pay-for-Use-Standorts

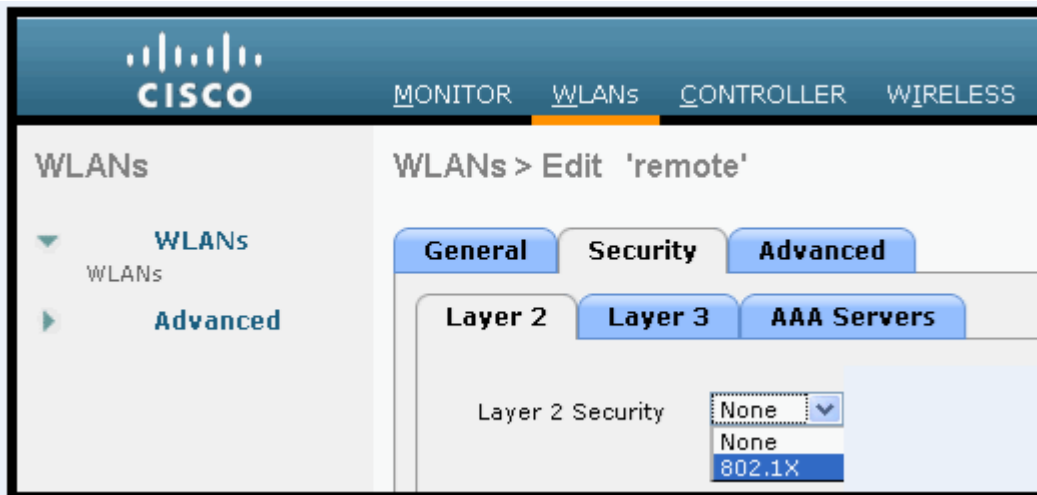


In Version 7.2 von Cisco wurden folgende Verbesserungen eingeführt:

- Hinzufügen von 802.1x-Sicherheit in der GUI
- Deaktivierung des lokalen WLAN-Zugriffs auf dem Access Point über den Controller - Deaktivierung der persönlichen SSID, sodass nur die Unternehmenskonfiguration möglich ist
- Auswahl der Kanalzuweisung
- Unterstützung von 2 Unternehmens-SSID auf 3 SSIDs geändert
- Unterstützung für Dual-RLAN-Port-Funktion

Hinzufügen von 802.1x-Sicherheit in der GUI

802.1x jetzt zur GUI hinzugefügt



Hinweise zur Authentifizierung für Remote-LAN-Ports.

802.1x authentication for remote-LAN port

WCS shall be provided to enable 802.1x Layer 2 Security and configure AAA server for remote-LAN. WEP encryption shall be always disabled.

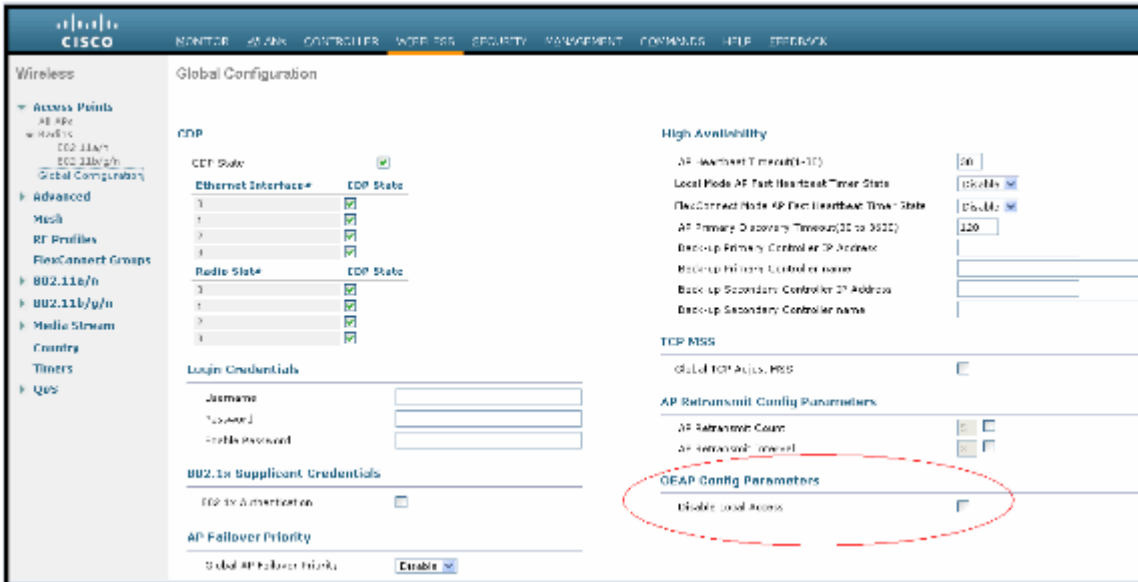
Same as 802.1x authentication for wireless clients, in 802.1x authentication for remote-LAN client, WLC acts as authenticator. Evora AP just forwards the EAPOL packets. AP converts EAPOL Ethernet packet to 802.11 data frame before sending it to WLC. The destination address in the 802.11 data frame shall be set to BSSID for remote-LAN. There is no data encryption for the Ethernet packets transferred on remote-LAN port. So there is no key exchange on EAPOL. The data security is provided by DTLS on CAPWAP data channel.

Following EAP methods are supported:

- EAP-TLS
- PEAP
- EAP-TTLS.

Deaktivierung des lokalen WLAN-Zugriffs auf dem Access Point über den Controller - Deaktivierung der persönlichen SSID, sodass nur die Unternehmenskonfiguration möglich ist

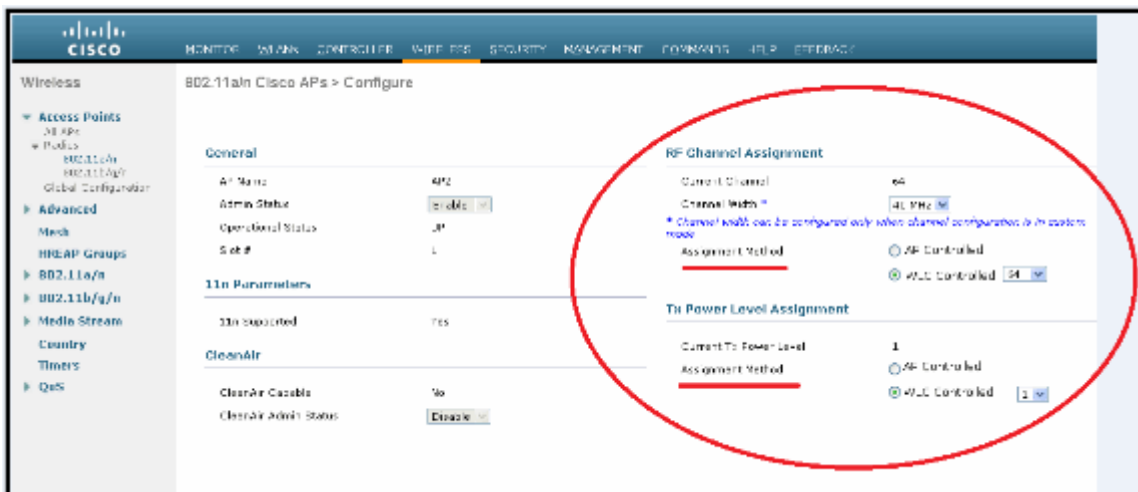
Lokalen WLAN-Zugriff deaktivieren



Folgende Optionen können für die Kanalzuweisung ausgewählt werden:

- AP lokal gesteuert
- WLC-gesteuert

RF-Kanal und Leistungszuweisungen jetzt lokal oder WLC-gesteuert



Manually configure channel and power level

In JMR1 release, there is no configuration option for 802.11a/n and 802.11b/g/n radios for the OEAP-600 AP. In 7.2 release, the configuration window is added back with only "General", "RF Channel Assignment" and "Tx Power Level Assignment" portions. The "Admin Status" in "General" shall be display only. The options for "Assign Method" are changed to "Custom Configured" and "AP Controlled". By default "AP Controlled" is selected. Channel and Tx power level can be configured only when they are in "Custom Configured" mode.

OEAP-600 does not support DFS channels so that WLC shall not allow these channels to be configured. This new assignment method is passed to AP with CAPWAP payload.

In AP, when the channel is "AP Controlled", then the channel is controlled by the setting from local AP GUI. Otherwise the channel set by WCS is used.

The channel assign method and the assigned channel are saved in NVRAM and displayed in local GUI.

In AP, when the power is "AP controlled", then the maximum power level is always used. Otherwise the power level set by WCS is used.

The assign method for TX power level and assigned TX power level shall be saved in flash so that they can take effect after AP reboots.

When "Reset to Default" operation is performed, the assign method is set to "AP controlled".

Unterstützung für duale RLAN-Port-Funktion (nur CLI)

Dieser Hinweis gilt für APs der Serie OEAP-600 unter Verwendung der Funktion für duale RLAN-Ports, die den Betrieb des OEAP-600-Ethernet-Ports 3 als Remote-LAN ermöglicht. Die Konfiguration ist nur über die CLI zulässig. Hier ein Beispiel:

```
Config network oep-600 dual-rlan-ports enable|disable
```

Falls diese Funktion nicht konfiguriert ist, funktioniert der Remote-LAN mit einem Port 4 weiterhin. Jeder Port verwendet für jeden Port ein eindeutiges Remote-LAN. Die Remote-LAN-Zuordnung ist unterschiedlich, je nachdem, ob die Standardgruppe oder die AP-Gruppen verwendet werden.

Standardgruppe

Wenn die Standardgruppe verwendet wird, wird Port 4 ein einzelnes Remote-LAN mit einer geraden Remote-LAN-ID zugeordnet. Der Remote-LAN mit der Remote-LAN-ID 2 ist beispielsweise Port 4 (am OEAP-600) zugeordnet. Der Remote-LAN mit einer ungeraden Nummer für den Remote-LAN-ID wird Port 3 (am OEAP-600) zugeordnet.

Nehmen wir als Beispiel die beiden folgenden Remote-Pläne:

(Cisco Controller) >show remote-lan summary

Number of Remote LANS..... 2

RLAN ID	RLAN Profile Name	Status	Interface Name
2	rlan2	Enabled	management
3	rlan3	Enabled	management

rlan2 hat eine gerade nummerierte Remote-LAN-ID, 2, und als solche Karten an Port 4. rlan3 hat eine ungerade Remote-LAN-ID 3, und so Karten an Port 3.

AP-Gruppen

Wenn Sie eine AP-Gruppe verwenden, wird die Zuordnung zu den OEAP-600-Ports durch die Reihenfolge der AP-Gruppen bestimmt. Um eine AP-Gruppe zu verwenden, müssen Sie zunächst alle Remote-LANs und WLANs aus der AP-Gruppe löschen und leer lassen. Fügen Sie dann die beiden Remote-LANs zur AP-Gruppe hinzu. Fügen Sie zunächst das Remote-LAN mit Port 3 AP hinzu, fügen Sie dann die Remote-Gruppe mit Port 4 hinzu, und fügen Sie schließlich alle WLANs hinzu.

Ein Remote-LAN an der ersten Position in der Liste ist Port 3 zugeordnet, und ein Remote-LAN an der zweiten Position in der Liste ist Port 4 zugeordnet, wie in diesem Beispiel:

RLAN ID	RLAN Profile Name	Status	Interface Name
2	rlan2	Enabled	management
3	rlan3	Enabled	management

Zugehörige Informationen

- [Cisco Wireless LAN Controller Configuration Guide, Release 7.0](#)
- [Technischer Support und Dokumentation für Cisco Systeme](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.