# Vertrauenswürdige AP-Richtlinien auf einem Wireless LAN-Controller

# Inhalt

Einführung Voraussetzungen Anforderungen Konventionen Vertrauenswürdige AP-Richtlinien Was ist ein vertrauenswürdiger Access Point? Wie wird ein Access Point über die WLC-GUI als vertrauenswürdiger Access Point konfiguriert? Einstellungen für vertrauenswürdige AP-Richtlinien Konfigurieren vertrauenswürdiger AP-Richtlinien auf dem WLC Warnmeldung für vertrauenswürdige AP-Policy-Verletzung Zugehörige Informationen

# **Einführung**

In diesem Dokument werden die Richtlinien zum *vertrauenswürdigen WAP*-WLAN-Schutz auf einem WLAN-Controller (WLC) beschrieben, vertrauenswürdige AP-Richtlinien definiert und alle vertrauenswürdigen AP-Richtlinien kurz beschrieben.

# Voraussetzungen

## Anforderungen

Vergewissern Sie sich, dass Sie über grundlegende Kenntnisse der Wireless LAN-Sicherheitsparameter verfügen (z. B. SSID, Verschlüsselung, Authentifizierung usw.).

## **Konventionen**

Weitere Informationen zu Dokumentkonventionen finden Sie unter <u>Cisco Technical Tips</u> Conventions (Technische Tipps von Cisco zu Konventionen).

# Vertrauenswürdige AP-Richtlinien

Vertrauenswürdige AP-Richtlinien sind eine Sicherheitsfunktion im Controller, die für die Verwendung in Szenarien entwickelt wurde, in denen Kunden ein paralleles autonomes AP-Netzwerk mit dem Controller haben. In diesem Szenario kann der autonome Access Point als vertrauenswürdiger Access Point auf dem Controller markiert werden, und der Benutzer kann Richtlinien für diese vertrauenswürdigen Access Points definieren (die nur WEP oder WPA, unsere eigene SSID, kurze Präambel usw. verwenden sollten). Wenn einer dieser Access Points diese Richtlinien nicht erfüllt, löst der Controller einen Alarm für das Netzwerkmanagementgerät (Wireless Control System) aus, das angibt, dass ein vertrauenswürdiger Access Point gegen eine konfigurierte Richtlinie verstößt.

### Was ist ein vertrauenswürdiger Access Point?

Vertrauenswürdige APs sind APs, die nicht Teil eines Unternehmens sind. Sie stellen jedoch keine Sicherheitsbedrohung für das Netzwerk dar. Diese APs werden auch als freundliche APs bezeichnet. Es gibt mehrere Szenarien, in denen Sie einen Access Point als vertrauenswürdigen Access Point konfigurieren möchten.

Sie können beispielsweise verschiedene Kategorien von Access Points in Ihrem Netzwerk einrichten, z. B.:

- APs, die Sie besitzen und LWAPP nicht ausführen (möglicherweise führen sie IOS oder VxWorks aus)
- LWAPP APs, die Mitarbeiter mitbringen (mit Wissen des Administrators)
- LWAPP APs zum Testen des vorhandenen Netzwerks
- LWAPP APs, die Nachbarn besitzen

Vertrauenswürdige APs sind normalerweise APs, die in **Kategorie 1** fallen, d. h. APs, die Sie besitzen und die LWAPP nicht ausführen. Es kann sich um alte APs handeln, die VxWorks oder IOS ausführen. Um sicherzustellen, dass diese APs das Netzwerk nicht beschädigen, können bestimmte Funktionen wie richtige SSIDs und Authentifizierungstypen erzwungen werden. Konfigurieren Sie die vertrauenswürdigen AP-Richtlinien auf dem WLC, und stellen Sie sicher, dass die vertrauenswürdigen APs diese Richtlinien erfüllen. Andernfalls können Sie den Controller so konfigurieren, dass er mehrere Aktionen ausführt, z. B. einen Alarm für das Netzwerkmanagementgerät (WCS).

Bekannte APs, die zu den Nachbarn gehören, können als vertrauenswürdige APs konfiguriert werden.

Normalerweise sollte MFP (Management Frame Protection, Management Frame Protection) APs, die keine legitimen LWAPP-APs sind, daran hindern, dem WLC beizutreten. Wenn NIC-Karten MFP unterstützen, dürfen sie keine Authentifizierungen von anderen Geräten als den echten APs akzeptieren. Weitere Informationen zum MFP finden Sie unter <u>Infrastructure Management Frame</u> Protection (MFP) mit WLC und LAP Configuration Example.

Wenn Sie APs haben, die VxWorks oder IOS ausführen (wie in Kategorie 1), werden diese nie der LWAPP-Gruppe beitreten oder MFP ausführen. Sie können jedoch die auf dieser Seite aufgeführten Richtlinien durchsetzen. In solchen Fällen müssen vertrauenswürdige AP-Richtlinien auf dem Controller konfiguriert werden, um die APs zu ermitteln, die von Interesse sind.

Wenn Sie einen nicht autorisierten Access Point kennen und feststellen, dass er keine Bedrohung für Ihr Netzwerk darstellt, können Sie diesen Access Point im Allgemeinen als einen bekannten vertrauenswürdigen Access Point identifizieren.

Wie wird ein Access Point über die WLC-GUI als vertrauenswürdiger Access Point konfiguriert?

Gehen Sie wie folgt vor, um einen Access Point als vertrauenswürdigen Access Point zu konfigurieren:

- 1. Melden Sie sich über HTTP- oder HTTPS-Anmeldung bei der GUI des WLC an.
- 2. Klicken Sie im Hauptmenü des Controllers auf Wireless.
- 3. Klicken Sie im Menü links auf der Seite Wireless auf Nicht autorisierte

Cisco - Microsoft Internet Ex Ele Edt Yew Fgvorkes	plorer provided by Cisco System Tools Help	ns, Inc.	85 (A.A.A.A.A.A.A.A.A.A.A.A.A.A.A.A.A.A.A.	U S			_ 0
na Sentar	MONITOR WLANS CO		S SECURITY MA	NAGEMENT COM	Sava Configurati IMANDS HELP	on   Ping	Logout   Refre
Wireless Access Points All APs 802.11a Radios	All APs Search by Ethernet NAC		Search				
802.11b/g Radios Third Party APs	AP Name	AP ID	Ethernet MAC	Admin Status	Operational Status	Port	
aridging	ap:5b:fb:d0	34	00:0b:85:5b:fb:d0	Enable	REG	2	Detail
Rogue APs Rogue APs Rogue Clients	ap:51:5a:e0	35	00:0b:85:51:5a:e0	Enable	REG	2	Detail
Adhoc Rogues							
Iobal RF 802.11a Network 802.11b/g Network							
ountry							
imers							
Disputies # 101 (2+ 00)	Desen Island	at multile as been dree as	144 1047				
vecusions - D C U		ox avalable on http://10.77.	en evy				

Auf der Seite für nicht autorisierte APs werden alle APs aufgelistet, die im Netzwerk als nicht autorisierte APs erkannt werden.

- 4. Suchen Sie in dieser Liste von nicht autorisierten Access Points den Access Point, den Sie als vertrauenswürdigen Access Point konfigurieren möchten, der unter Kategorie 1 fällt (wie im vorherigen Abschnitt erläutert). Sie können die APs mit den MAC-Adressen finden, die auf der Seite zu nicht autorisierten Access Points aufgeführt sind. Wenn der gewünschte Access Point nicht auf dieser Seite angezeigt wird, klicken Sie auf Weiter, um den Access Point von der nächsten Seite zu identifizieren.
- 5. Wenn sich der gewünschte Access Point aus der Liste der nicht autorisierten Access Points befindet, klicken Sie auf die Schaltfläche **Bearbeiten**, die dem Access Point entspricht. Diese führt Sie zur Detailseite des Access Points.

Next

MAC Address	SSID	# Detecting Radios	Number of Clients	Status	
00:02:8a:0e:33:f5	Unknown	1	0	Pending	Edit
00:07:50:d5:cf:b9	Unknown	1	0	Pending	Edit
00.01.05.51.5	Heles and	â	0	Containment Des die e	10.00

	00:07:50:d5:cf:b9	Unknown	1	0	Pending	Edit
	00:0b:85:51:5a:ee	Unknown	0	0	Containment Pending	Edit
	00:0c:85:eb:de:62	Unknown	1	0	Alert	Edit
	00:0d:ed:be:f6:70	Unknown	2	0	Alert	Edit
$\leq$	00:12:01:a1:f5:10	auto-2	1	0	Pending	Edit

Auf der Seite mit Details zu nicht autorisierten Access Points finden Sie detaillierte Informationen zu diesem Access Point (z. B. ob dieser Access Point mit einem kabelgebundenen Netzwerk verbunden ist, sowie den aktuellen Status des Access Points usw.).

6. Um diesen Access Point als vertrauenswürdigen Access Point zu konfigurieren, wählen Sie in der Dropdown-Liste Update Status (Aktualisierungsstatus) die Option Known Internal (Bekannte Interne Verbindung) aus, und klicken Sie auf Apply (Übernehmen). Wenn Sie den AP-Status auf "Bekannte interne Verbindungen" aktualisieren, wird dieser AP als vertrauenswürdiger AP dieses Netzwerks

Ele Edit Yew Favorite	s Iools Help						Ju	nks 🏁					
					Save Config	puration   P	ing Logou	t   Refres					
A., A.	MONITOR WLANS CONTROLLE	R WIRELESS SEC	URITY MANAGEME	NT COMP	IANDS H	IEUP							
Wireless	Rogue AP Detail					< Back	As	ply					
Access Points All APs 802.11a Radios	MAC Address	00:12	:01:a1:f5:10										
002.11b/g Radios Third Party APs	Туре	AP											
ridging	Is Rogue On Wired Network?	No											
Rogues Rogue APs Known Rogue APs	First Time Reported On	Wed 0	ec 12 12:27:28 2007										
Rogue Clients Adhoc Rogues	Last Time Reported On	Wed 0	ec 12 13:13:09 2007										
lients	Current Status	Know											
802.11a Network 802.11b/g Network	Update Status		Choose New Status	<u> </u>									
ountry		Conti	hoose New Status in Rogue										
imers		Know	Unknown n Internal										
	APs that detected this Rogue	ACKIN	wiedge External										
	Base Radio MAC AP Name	SSID	Channel	Radio Type	WEP	WPA	Pre- Amble	RSSI					
	00:0b:85:51:5a:e0 ap:51:5a:	e0 auto-2	1	802.119	Enabled	Enabled	Short	-71					
	Clients associated to this Roge	Clients associated to this Roque AP											
	MAC Address L	ast Time Heard											

7. Wiederholen Sie diese Schritte für alle APs, die Sie als vertrauenswürdige APs konfigurieren möchten.

Überprüfen der Konfiguration des vertrauenswürdigen Access Points

Gehen Sie wie folgt vor, um zu überprüfen, ob der Access Point über die Controller-GUI korrekt als vertrauenswürdiger Access Point konfiguriert ist:

- 1. Klicken Sie auf Wireless.
- 2. Klicken Sie im Menü links auf der Seite Wireless auf Known Rogue

e Ber Terr (Brauns	Toos Geb						
	MONITOR WLANS CONTROLL		S SECURITY MAN	AGEMENT COM	Save Configurati IMANDS HELP	on Ping Lo	gout Refre
ireless	All APs						
<b>cess Points</b> MI APs 802.11a Radios	Search by Ethernet MAC		Search				
802.11b/g Radios Third Party APs	AP Name	AP ID	Ethernet MAC	Admin Status	Operational Status	Port	
dging	ap:5b:fb:d0	34	00:0b:85:5b:fb:d0	Enable	REG	2	Detail
nown Rogue APs	ap:51:5a:e0	35	00:0b:85:51:5a:e0	Enable	REG	2	Detail
dhoc Rogues							
bal RF 02.11a Network 02.11b/g Network 02.11b							
untry							
ners							

Der gewünschte Access Point sollte auf der Seite "Bekannte Access Points" (Zugangspunkte für nicht autorisierte APs) angezeigt werden, deren Status als *bekannt* aufgeführt ist.

Eisco - Microsoft Internet E	oplorer provided by Cisco	Systems, Inc.	19		8		_@×
Ele Edit Yew Fgvorites	Tools Rielp						<b>1</b>
Cases Systems						ve Configuration	Ping   Logout   Refresh
A. A.	MONITOR WLANS	CONTROLLER	WIRELESS	SECURITY MAN	AGEMENT COMMA	NDS HELP	
Wireless	Known Rogue AP	s			Items 1	to 4 of 4	New
Access Points All APs	MAC Address	SSID		# Detecting Radios	Number of Clients	Status	
802.11a Radios 802.11b/g Radios	00:02:8a:0e:33:f5	Unknown		2	0	Known	Edit Remove
Third Party APs	00:07:85:92:4d:c9	Unknown		2	0	Known	Edit Remove
Bridging	00:0b:fc:fc:15:00	Unknown		1	0	Known	Edit Remove
Rogues	00:12:01:a1:f5:10	auto-2		2	0	Known	Edit Remove
Roque Clients Adhoc Roques Clients Global RF 802.11a Network 802.11b/g Network 802.11h Country Timers							
X Superstant PLO	- The start of the line of the second			-			
* Discussions * 🞲 💮 🙂	99918100	ussions not available on	http://10.77.244	.204/			9
Done							Internet

## Einstellungen für vertrauenswürdige AP-Richtlinien

Der WLC verfügt über folgende vertrauenswürdige AP-Richtlinien:

- Durchgesetzte Verschlüsselungsrichtlinie
- Durchgesetzte Präambelrichtlinie
- Durchgesetzte Funktyp-Richtlinie
- <u>SSID validieren</u>
- Warnung bei fehlendem vertrauenswürdigen Access Point
- <u>Ablaufzeit für vertrauenswürdige AP-Einträge (Sekunden)</u>

#### Durchgesetzte Verschlüsselungsrichtlinie

Diese Richtlinie wird verwendet, um den Verschlüsselungstyp zu definieren, den der vertrauenswürdige Access Point verwenden soll. Sie können einen dieser Verschlüsselungstypen unter Durchgesetzte Verschlüsselungsrichtlinie konfigurieren:

- Keine
- Öffnen
- WEP
- WPA/802.11i

Der WLC überprüft, ob der auf dem vertrauenswürdigen Access Point konfigurierte Verschlüsselungstyp mit dem Verschlüsselungstyp übereinstimmt, der auf der Einstellung "Enforced Encryption Policy" (Durchgesetzte Verschlüsselungsrichtlinie) konfiguriert wurde. Wenn der vertrauenswürdige Access Point den angegebenen Verschlüsselungstyp nicht verwendet, löst der WLC einen Alarm für das Managementsystem aus, um geeignete Maßnahmen zu ergreifen.

#### Durchgesetzte Präambelrichtlinie

Die Funkpräambel (manchmal auch als Header bezeichnet) ist ein Datenabschnitt am Kopf eines Pakets, der Informationen enthält, die Wireless-Geräte benötigen, wenn sie Pakete senden und empfangen. **Kurze** Präambel verbessern die Durchsatzleistung, sodass sie standardmäßig aktiviert sind. Einige Wireless-Geräte, wie beispielsweise SpectraLink NetLink-Telefone, erfordern jedoch **lange** Präambel. Sie können eine der folgenden Präambeloptionen unter Durchgesetzte Präambelrichtlinie konfigurieren:

- Keine
- Kurz
- lang

Der WLC überprüft, ob der auf dem vertrauenswürdigen Access Point konfigurierte Preamble-Typ mit dem Präambeltyp übereinstimmt, der auf der Einstellung "**Enforced Preamble policy**" konfiguriert wurde. Wenn der vertrauenswürdige Access Point den angegebenen Präambeltyp nicht verwendet, löst der WLC einen Alarm für das Managementsystem aus, um geeignete Maßnahmen zu ergreifen.

#### Durchgesetzte Funktyp-Richtlinie

Diese Richtlinie wird verwendet, um den Funktyp zu definieren, den der vertrauenswürdige Access Point verwenden soll. Sie können einen der folgenden Funktypen unter Enforced Radio Type Policy (Richtlinie für durchgesetzten Funktyp) konfigurieren:

- Keine
- Nur 802.11b
- Nur 802.11a
- Nur 802.11b/g

Der WLC überprüft, ob der auf dem vertrauenswürdigen Access Point konfigurierte Funktyp mit dem Funktyp übereinstimmt, der auf der Einstellung **"Enforced Radio Type Policy**" konfiguriert wurde. Wenn der vertrauenswürdige AP die angegebenen Funkmodule nicht verwendet, löst der WLC einen Alarm für das Managementsystem aus, um geeignete Maßnahmen zu ergreifen.

#### **SSID validieren**

Sie können den Controller so konfigurieren, dass eine SSID der vertrauenswürdigen Access Points anhand der auf dem Controller konfigurierten SSIDs validiert wird. Wenn die SSID der vertrauenswürdigen APs mit einer der SSIDs des Controllers übereinstimmt, löst der Controller einen Alarm aus.

#### Warnung, wenn Trusted AP fehlt

Wenn diese Richtlinie aktiviert ist, benachrichtigt der WLC das Managementsystem, wenn der vertrauenswürdige Access Point in der Liste der bekannten nicht autorisierten Access Points fehlt.

Dieser Timeout-Wert gibt die Anzahl der Sekunden an, bevor der vertrauenswürdige Access Point als abgelaufen gilt und vom WLC-Eintrag geleert wird. Sie können diesen Timeout-Wert in Sekunden (120-3600 Sekunden) angeben.

## Konfigurieren vertrauenswürdiger AP-Richtlinien auf dem WLC

Gehen Sie wie folgt vor, um vertrauenswürdige AP-Richtlinien auf dem WLC über die GUI zu konfigurieren:

Hinweis: Alle vertrauenswürdigen AP-Richtlinien befinden sich auf derselben WLC-Seite.

- 1. Klicken Sie im Hauptmenü der WLC-GUI auf Sicherheit.
- 2. Klicken Sie im Menü links auf der Seite Sicherheit auf Vertrauenswürdige AP-Richtlinien unter der Überschrift Wireless Protection Policies (Wireless-



 Wählen Sie auf der Seite Trusted AP Policies (Vertrauenswürdige AP-Richtlinien) den gewünschten Verschlüsselungstyp (Keine, Offen, WEP, WPA/802.11i) aus der Dropdown-Liste Enforced Encryption Policy (Durchgesetzte Verschlüsselungsrichtlinie) aus.



 Wählen Sie den gewünschten Präambeltyp (None, Short, Long) aus der Dropdown-Liste Enforced Preamble Type policy (Richtlinie für durchgesetzten Präambeltyp) aus.



 Wählen Sie in der Dropdown-Liste "Enforced radio type policy" (Richtlinie durchgesetzt) den gewünschten Funktyp aus (nur Keine, nur 802.11b/g, nur 802.11a, nur 802.11b/g).

Cisco - Microsoft Internet Ex	glorer provided by Cisco Systems, Inc.			in the		<u>9122</u>	_ @ ×
Ele Edit View Favorites	Took Rep						- 18
Cases Searcas					Save Co	nfiguration   Ping	Logout Refresh
A. A.	MONITOR WLANS CONTROLLE	R WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	
Security	Trusted AP Policies					< Back	Apply
AAA General RADIUS Authentication RADIUS Accounting Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies Access Control Lists IPSec Certificates CA Certificate ID Certificate Web Auth Certificate Wireless Protection Policies Standard Signatures Custom Signatures Client Exclusion Policies AP Authentication	Enforced encryption policy Enforced preamble policy Enforced radio type policy Validate SSID Alert if Trusted AP is missing Expiration Timeout for Trusted	AP Entries (s	econds)	rEP   hort  one  rEP  rep  to ne  rep  rep  rep  rep  rep  rep  rep  r			
× Discussions • 况 🕃 🕄	의 행 행 🔄 🖉 Discussions not available	on http://10.77.244	4.204/				ø
<ul> <li>Image: A set of the set of the</li></ul>						i in	ternet

- 6. Aktivieren oder deaktivieren Sie das Kontrollkästchen **SSID aktiviert validieren**, um die Einstellung SSID validieren zu aktivieren oder zu deaktivieren.
- 7. Aktivieren oder deaktivieren Sie das Kontrollkästchen Alert if Trusted AP is missing Enabled (Vertrauenswürdiger Access Point fehlt), um die Warnung zu aktivieren oder zu deaktivieren, wenn die Einstellung für den vertrauenswürdigen Access Point fehlt.
- 8. Geben Sie einen Wert (in Sekunden) für die Option Ablaufzeitüberschreitung bei vertrauenswürdigen AP-Einträgen ein.



9. Klicken Sie auf Übernehmen.

**Hinweis:** Um diese Einstellungen über die WLC-CLI zu konfigurieren, können Sie den Befehl **config wps trust-ap** mit der entsprechenden Richtlinienoption verwenden.

Cisco Controller) >config wps trusted-ap ? encryption Configures the trusted AP encryption policy to be enforced. missing-ap Configures alert of missing trusted AP. preamble Configures the trusted AP preamble policy to be enforced. radio Configures the trusted AP radio policy to be enforced. timeout Configures the expiration time for trusted APs, in seconds.

#### Warnmeldung für vertrauenswürdige AP-Policy-Verletzung

Im Folgenden sehen Sie ein Beispiel für eine Warnung, dass der Controller eine vertrauenswürdige AP-Richtlinie verletzt.

Thu Nov 16 12:39:12 2006 [WARNING] apf\_rogue.c 1905: Possible AP impersonation of xx:xx:xx:xx:xx:xx, using source address of 00:16:35:9e:6f:3a, detected by 00:17:df:7d:e1:70 on slot 0 Thu Nov 16 12:39:12 2006 [SECURITY] apf\_rogue.c 1490: **Trusted AP Policy failed for AP xx:xx:xx:xx:xx:xx - invalid SSID 'SSID1'** Thu Nov 16 12:39:12 2006 [SECURITY] apf\_rogue.c 1457: **Trusted AP Policy failed for AP xx:xx:xx:xx:xx:xx - invalid encryption type** Thu Nov 16 12:39:12 2006 Previous message occurred 6 times **Beachten Sie die hervorgehobenen Fehlermeldungen hier.** Diese Fehlermeldungen weisen darauf hin dass die SSID und der auf dem vertrauenswürdigen Access Deint kenfigurierte.

hin, dass die SSID und der auf dem vertrauenswürdigen Access Point konfigurierte Verschlüsselungstyp nicht mit der Richtlinieneinstellung für vertrauenswürdige Access Points

#### übereinstimmen.

Die gleiche Warnmeldung wird auch in der WLC-GUI angezeigt. Um diese Meldung anzuzeigen, gehen Sie zum Hauptmenü der WLC-GUI, und klicken Sie auf **Monitor**. Klicken Sie im Abschnitt Zuletzt verwendete Traps auf der Seite Monitor (Überwachung) auf **View All (Alle anzeigen)**, um alle letzten Warnungen auf dem WLC anzuzeigen.

CO STOTEME							Save Config	ration Ping	Logout R	
15 A.	(MONITOR WLAN	s CONTR	ROLLER	WIREU	ESS	SECURITY	MANAGEMENT COMMANDS HI	ELP		
lonitor ummary	Canadarman Andre -	-				i es q	100 Access Points Supporter Cisce 4400 Series Weekes LAN Costruler			
Controller Ports	Controller Summ	hary					Rogue Summary			
Wireless	Management IP Add	Address 10.77.244.204					Active Rogue APs	25	Detail	
Known Rogue APs	Service Port IP Add	ress	0.0.0.0				Active Rogue Clients	0	Detail	
Rogue Clients Adhoc Rogues 802.11a Radios 802.11b/g Radios Clients RADIUS Servers	Software Version		3.2.150.10				Adhoc Rogues	0	Detail	
	System Name		WLC-4	400-TS1	WEB		Rogues on Wired Network	0		
	Up Time		16 day	s, 8 hou	ırs, 42	minutes				
	System Time		Wed Dec 12 12:40:03 2007				Top WI AND			
	Internal Temperatu	re	+38 C				TOP WEARS			
	802.11a Network St	tate	Enabled				WLAN	# of (	lients	
	802.11b/g Network	State	Enabled				wcs	by ss	1D Detail	
							WCS123	0	Detail	
	Access Point Sur	mmary								
		Total	Up		Down		Most Recent Traps			
	802.11a Radios	2	• 2	٠	0	Deteil				
	802.11b/g Radios	2	• 2	٠	0	Detail	Rogue AP : 00:13:19:49:08:	70 detected on	Base Radio	
	All APs	2	• 2	٠	0	Detail	Rogue AP : 00:13:19:49:08:	70 detected or	Base Radio	
							Rogue AP : 00:11:21:b4:ff:0	0 detected on	Base Radio I	
	Client Summary						Trusted AP 00:07:85:92:4d:c	9 has invalid r	adio policy. I	
	,	cheft summary					Trusted AP 00:07:85:92:4d:c9 has invalid encryption			
	Current Clients		6			Detail			View All	
	Excluded Clients		0			Detail				
	mi 11 1 mi		0			Detail	This page refreshes every 30 st	econds.		

Auf der Seite Zuletzt verwendete Traps (Aktuelle Traps) können Sie den Controller identifizieren, der die Warnmeldung für vertrauenswürdige AP-Richtlinienverstöße generiert, wie in diesem Bild gezeigt:

Cisco - Microsoft Internet Ex	plorer provided by Cisco Sys	tems, Inc.	<u>iiiinee</u>					_@×	
Ele Edit Yew Favorites	Tools Fleib							- <b>1</b>	
Cases Systems						Save Co	nfiguration Ping	Logout Refresh	
A.A.	MONITOR WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP		
Monitor	Trap Logs							Clear Log	
Summary	Number of Traps sinc	e last reset	12516						
Statistics Controller	Number of Traps sinc	e log last view	ed 3						
Ports	Log System Time	Trap							
Rogue APs	0 Wed Dec 12 12:40:32 2007	Rogue : 00:0 Interface no	f:f8:58:a8:5c :1(802.11b/	removed fro	om Base Radio M	IAC : 00:0b:85:	5b:fb:d0		
Known Rogue APs Rogue Clients	1 Wed Dec 12 12:40:32 2007	Rogue : 00:1 Interface no	3:19:ab:99:00 :1(802.11b/	) removed fr	rom Base Radio	MAC: 00:0b:85	:5b:fb:d0		
Adhoc Rogues 802.11a Radios	2 Wed Dec 12 12:40:32 2007	Rogue : 00:1 Interface no	3:19:ab:99:00 :1(802.11b/	0 removed fr	rom Base Radio	MAC : 00:0b:85	:51:5a:e0		
802.11b/g Radios Clients	3 Wed Dec 12 12:39:31 2007	Rogue AP : 0 Interface no	0:13:19:49:0 :1(802.11b/	8:70 detecte ) with RSSI:	d on Base Radio -47 and SNR: 48	MAC:00:0b:8	5:51:5a:e0		
RADIUS Servers	4 Wed Dec 12 12:39:31 2007	Rogue AP : 0 Interface no	0:13:19:49:0 :1(802.11b/	8:70 detecte ) with RSSI:	d on Base Radio -55 and SNR: 4-	MAC:00:0b:8	5:5b:fb:d0		
	5 Wed Dec 12 12:39:31 2007	Rogue AP : 0 Interface no	0:11:21:b4:ff	:00 detected	on Base Radio	MAC : 00:0b:85	:Sb:fb:d0		
	6 Wed Dec 12 12:39:29 2007	Trusted AP 0 802.11b/g	0:07:85:92:4	d:c9 has inv	alid radio policy	. It's using 802	2.11a instead of		
	7 Wed Dec 12 12:39:29 2007	Trusted AP 0	0:07:85:92:4 EP	d:c9 has inv	alid encryption	configuration.	It's using Open		
	8 Wed Dec 12 12:39:29 2007	Dec 12 Trusted AP 00:02:8a:0e:33:f5 has invalid radio policy. It's using 802.11a instead of 802.11b/a							
	9 Wed Dec 12 12:39:29 2007	Trusted AP 0	0:02:8a:0e:3	3:fS has inv	alid encryption (	configuration.	It's using Open		
	10 Wed Dec 12 12:39:29 2007	Trusted AP 0	00:12:01:a1:f5:10 is advertising an invalid SSID.						
	11 Wed Dec 12	Regue : 00:1	1-5c:93:d3:bi	removed fr	om Base Radio	HAC: 00:06:85	:51:5a:e0		
	12:30:12 2007	Rogue : 00:14:f1:ae:9d:70 removed from Base Radio MAC : 00:0b:85:51:5a:e0							
	12:38:10 2007	Interface no	:1(802.11b/	)	en Baca Badia I	war - no-ob-er-	FI-F		
	13 Wed Dec 12 12:38:10 2007	Interface no	1(802.11b/	removed fr j)	om base kadio r	HAC : 00:00:05:	51:54:60		
	14 Wed Dec 12 Rogue : 00:19:a9:41:12:b4 removed from Base Radio MAC : 00:0b:85:51:5a:e0 12:38:10 2007 Interface no:1(802.11b/g)						:51:5a:e0		
	15 Wed Dec 12 12:37:32 2007	Rogue : 00:1 Interface no	4:1b:b6:23:60 :1(802.11b/c	) removed fr	rom Base Radio	MAC : 00:0b:85	:5b:fb:d0		
	16 Wed Dec 12 12:37:18 2007	Rogue AP : 0 Interface no	0:12:d9:e2:b :0(802.11a)	9:20 detecte with RSSI: -8	d on Base Radio 3 and SNR: 8	MAC : 00:0b:8	5:51:5a:e0		
× Discussions • 🎲 🕑 🕄	0 10 10 🖭 🖉 Discussion	ns not available on h	etp://10.77.244.	204/				9	
Done								Internet	

# Zugehörige Informationen

- <u>Cisco Wireless LAN Controller Configuration Guide, Release 5.2 Aktivieren der Erkennung</u> von Rouge Access Points in RF-Gruppen
- <u>Konfigurationsleitfaden für Cisco Wireless LAN Controller, Version 4.0 Konfigurieren von</u> <u>Sicherheitslösungen</u>
- Erkennung nicht autorisierter APs unter Unified Wireless Networks
- Design- und Implementierungsleitfaden für SpectraLink-Telefone
- Konfigurationsbeispiel für eine grundlegende WLAN-Verbindung
- Fehlerbehebung bei Verbindungen in einem Wireless-LAN-Netzwerk
- Konfigurationsbeispiele für die Authentifizierung auf Wireless LAN-Controllern
- Technischer Support und Dokumentation Cisco Systems