

Risoluzione dei problemi di rilevamento e mitigazione in una rete wireless unificata

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Panoramica sul server non autorizzato](#)

[Rilevamento server non autorizzati](#)

[Scansione off-channel](#)

[Modalità di scansione](#)

[Modalità locale e confronto tra le modalità monitor](#)

[Identificazione non autorizzata](#)

[Rogue Records](#)

[Dettagli sul server non autorizzato](#)

[Per esportare gli eventi indesiderati](#)

[Timeout record non autorizzato](#)

[Punto di accesso rilevamento server non autorizzati](#)

[Considerazioni sulla scalabilità](#)

[RLDP](#)

[Avvertenze di RLDP](#)

[Tracce porte switch](#)

[Classificazione non autorizzati](#)

[Regole di classificazione non valide](#)

[Fatti HA](#)

[Fatti su Flex-Connect](#)

[Mitigazione dei server non autorizzati](#)

[Controllo di elementi non autorizzati](#)

[Dettagli contenimento Rogue](#)

[Contenimento automatico](#)

[Avvertenze di contenimento Rogue](#)

[Chiusura porta switch](#)

[Configurazione](#)

[Configura rilevamento server non autorizzati](#)

[Configura rilevamento canali non autorizzati](#)

[Configura classificazione non autorizzati](#)

[Configurazione della mitigazione dei problemi non gravi](#)

[Configura contenimento manuale](#)

[Contenimento automatico](#)

[Con Prime Infrastructure](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Se Il Rogue Non Viene Rilevato](#)

[Debug utili](#)

[Registri Trap Previsti](#)

[Consigli](#)

[Se il server non autorizzato non è classificato](#)

[Debug utili](#)

[Consigli](#)

[RLDP non individua i server non autorizzati](#)

[Debug utili](#)

[Consigli](#)

[Punto di accesso rilevamento server non autorizzati](#)

[Comandi di debug utili in una console AP](#)

[Controllo di elementi non autorizzati](#)

[Debug previsti](#)

[Consigli](#)

[Conclusioni](#)

[Informazioni correlate](#)

Introduzione

Questo documento descrive il rilevamento e la mitigazione dei problemi sulle reti wireless Cisco.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Wireless Lan Controller.
- Cisco Prime Infrastructure.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco Unified Wireless Lan Controller (serie 5520, 8540 e 3504) con versione 8.8.120.0.
- Wave 2 AP serie 1832, 1852, 2802 e 3802.
- Serie Wave 1 AP 3700, 2700 e 1700.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Panoramica sul server non autorizzato

Le reti wireless estendono le reti cablate e aumentano la produttività dei dipendenti e l'accesso alle informazioni. Tuttavia, una rete wireless non autorizzata presenta un livello aggiuntivo di problemi di sicurezza. La sicurezza delle porte nelle reti cablate è meno studiata e le reti wireless rappresentano una facile estensione delle reti cablate. Pertanto, un dipendente che inserisce il proprio punto di accesso (Cisco o Non Cisco) in un'infrastruttura wireless o cablata ben protetta e consente a utenti non autorizzati di accedere a questa rete altrimenti protetta, può facilmente compromettere una rete protetta.

Il rilevamento dei server non autorizzati consente all'amministratore di rete di monitorare ed eliminare questo problema di sicurezza. L'architettura di rete unificata Cisco fornisce metodi per il rilevamento rogue che consentono di identificare i rogue e creare soluzioni di contenimento complete senza dover realizzare reti e strumenti di sovrapposizione costosi e difficili da giustificare.

Qualunque dispositivo che condivida il tuo spettro e non sia gestito da te può essere considerato un ladro. Una canaglia diventa pericolosa in questi scenari:

- Quando è impostato l'utilizzo dello stesso SSID (Service Set Identifier) della rete (honeypot)
- Quando viene rilevato sulla rete cablata
- Rughe ad-hoc
- Quando è impostato da un estraneo, la maggior parte delle volte, con intento dannoso

La procedura ottimale consiste nell'utilizzare il rilevamento rogue per ridurre al minimo i rischi di sicurezza, ad esempio in un ambiente aziendale.

Tuttavia, in alcuni scenari non è necessario il rilevamento di server non autorizzati, ad esempio nell'implementazione di Office Extend Access Point (OEAP), in tutta la città e all'esterno.

L'uso di punti di accesso mesh esterni per il rilevamento di manomissioni non avrebbe alcun valore, mentre l'uso di risorse per l'analisi.

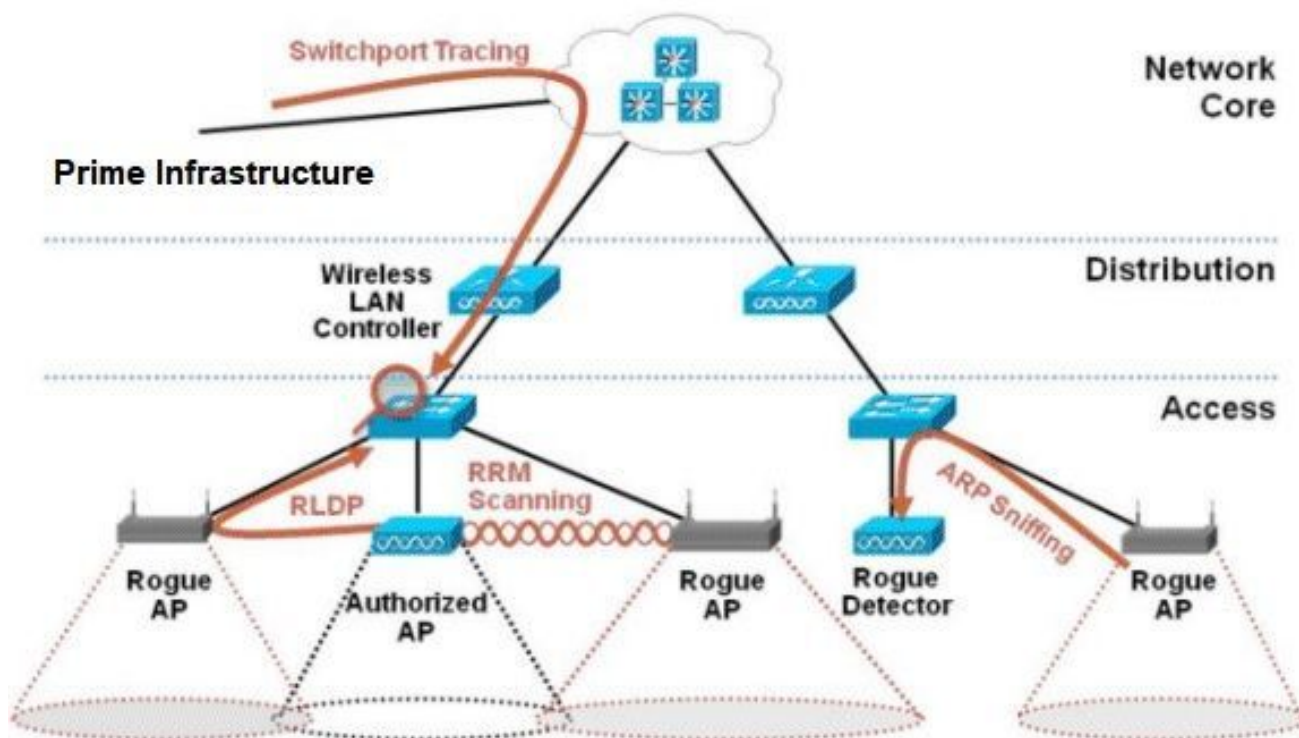
Infine, è fondamentale valutare (o evitare del tutto) il contenimento automatico disonesto, in quanto vi sono potenziali problemi legali e responsabilità se lasciato operare automaticamente.

La soluzione Cisco Unified Wireless Network (UWN) prevede tre fasi principali di gestione di dispositivi non autorizzati:

- Rilevamento: per rilevare la presenza di dispositivi non autorizzati viene utilizzata una scansione RRM (Radio Resource Management).
- Classificazione: il protocollo RLDP (Rogue Location Discovery Protocol), i rilevatori di anomalie (solo punti di accesso Wave 1) e le tracce delle porte dello switch vengono utilizzati per identificare se il dispositivo non autorizzato è connesso alla rete cablata. Le regole di classificazione non autorizzate aiutano anche a filtrare i non autorizzati in categorie specifiche in base alle loro caratteristiche.

- Attenuazione - La chiusura delle porte degli switch, la localizzazione dei dispositivi non autorizzati e il contenimento dei dispositivi non autorizzati vengono utilizzati per rintracciarne la posizione fisica e per annullare la minaccia del dispositivo non autorizzato.

Cisco Rogue Management Diagram Multiple Methods



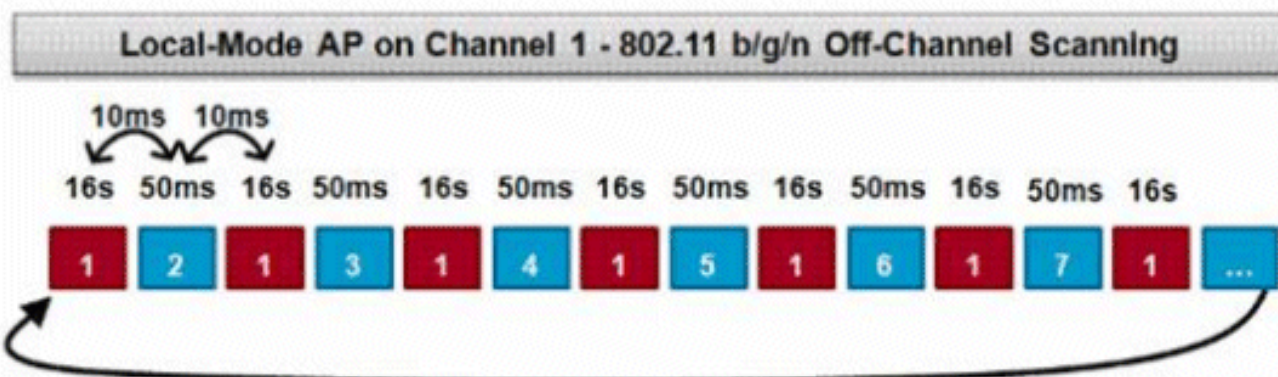
Rilevamento server non autorizzati

Un canaglia è essenzialmente qualsiasi dispositivo che condivide il vostro spettro, ma non è sotto il vostro controllo. Tra questi vi sono i punti di accesso non autorizzati, i router wireless, i client non autorizzati e le reti ad-hoc non autorizzate. Cisco UWN utilizza una serie di metodi per rilevare i dispositivi anomali basati su Wi-Fi, ad esempio una scansione off-channel e funzionalità di modalità monitor dedicata. Cisco Spectrum Expert può essere utilizzato anche per identificare dispositivi non basati sul protocollo 802.11, ad esempio bridge Bluetooth.

Scansione off-channel

Questa operazione viene eseguita dai punti di accesso in modalità locale e Flex-Connect (in modalità connessa) e utilizza una tecnica di suddivisione del tempo che consente il servizio client e la scansione dei canali con l'uso della stessa radio. Con il passaggio all'off-channel per un periodo di 50 ms ogni 16 secondi, per impostazione predefinita l'access point impiega solo una piccola percentuale del suo tempo per non servire i client. Si noti inoltre che si verifica un intervallo di modifica del canale di 10 ms. Nell'intervallo di scansione predefinito di 180 secondi, ciascun canale FCC da 2,4 Ghz (1-11) viene analizzato almeno una volta. Per altri settori normativi, come l'ETSI, il punto di accesso è fuori canale per una percentuale di tempo leggermente superiore. Sia

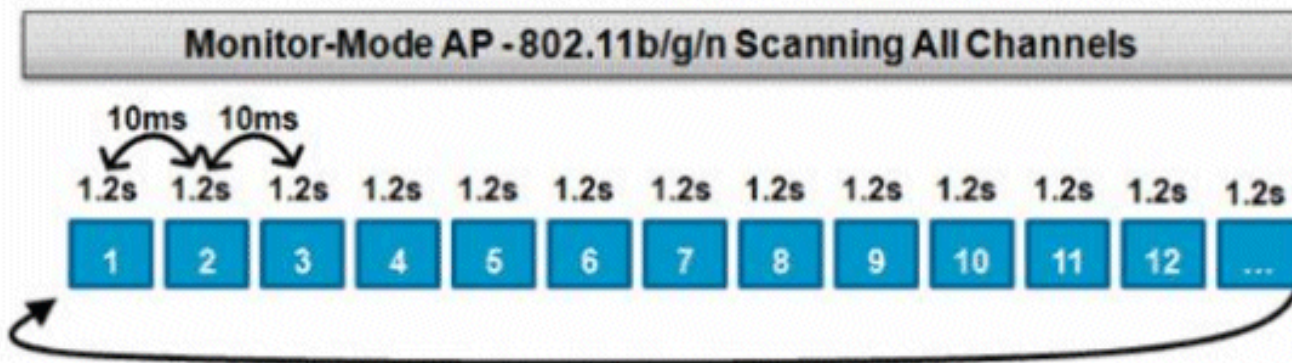
l'elenco dei canali che l'intervallo di scansione possono essere regolati nella configurazione RRM. Questo limita l'impatto sulle prestazioni a un massimo dell'1,5% e l'intelligenza è integrata nell'algoritmo per sospendere la scansione quando è necessario distribuire frame QoS ad alta priorità, come la voce.



L'immagine mostra l'algoritmo di scansione off-channel per un punto di accesso in modalità locale nella banda di frequenza di 2,4 GHz. Un'operazione simile viene eseguita in parallelo sulla radio da 5 GHz se l'access point ne possiede una. Ogni quadratino rosso rappresenta il tempo trascorso sul canale principale degli access point, mentre ogni quadratino blu rappresenta il tempo trascorso sui canali adiacenti a scopo di scansione.

Modalità di scansione

Questa operazione viene eseguita dai punti di accesso in modalità monitor e in modalità monitor IPS adattivo, che utilizzano il 100% del tempo radio per scansionare tutti i canali in ciascuna rispettiva banda di frequenza. Questo velocizza il rilevamento e permette di dedicare più tempo ai singoli canali. I punti di accesso in modalità di monitoraggio sono anche superiori nel rilevamento di client non autorizzati in quanto hanno una visione più completa dell'attività che si verifica in ogni canale.



L'immagine mostra l'algoritmo di scansione off-channel per un punto di accesso in modalità monitor nella banda di frequenza di 2,4 GHz. Un'operazione simile viene eseguita in parallelo sulla radio da 5 GHz se l'access point ne possiede una.

Modalità locale e confronto tra le modalità monitor

Un access point in modalità locale suddivide i cicli tra il servizio dei client WLAN e la ricerca di minacce nei canali. Di conseguenza, un access point in modalità locale impiega più tempo per passare in rassegna tutti i canali e impiega meno tempo nella raccolta dei dati su un particolare canale in modo che le operazioni del client non vengano interrotte. Di conseguenza, i tempi di rilevamento di attacchi anomali e di attacchi sono più lunghi (da 3 a 60 minuti) ed è possibile rilevare una gamma inferiore di attacchi over-the-air rispetto a un punto di accesso in modalità monitor.

Inoltre, il rilevamento di traffico bursty, come ad esempio i client non autorizzati, è molto meno deterministico in quanto il punto di accesso deve trovarsi sul canale del traffico nello stesso momento in cui il traffico viene trasmesso o ricevuto. Questo diventa un esercizio di probabilità. Un access point in modalità monitor passa tutti i suoi cicli nella scansione dei canali per cercare guai e attacchi over-the-air. Un punto di accesso in modalità monitor può essere utilizzato contemporaneamente per IPS adattivi, servizi di posizione (sensibili al contesto) e altri servizi in modalità monitor.

L'implementazione di punti di accesso in modalità monitor comporta una riduzione del tempo di rilevamento. Quando i punti di accesso in modalità monitor sono configurati con i punti di accesso wireless adattivi, è possibile rilevare una gamma più ampia di minacce e attacchi over-the-air.

AP in modalità locale	Modalità di monitoraggio AP
Offre ai client la possibilità di suddividere i tempi di scansione su più canali	Scansione dedicata
Ascolta per 50 ms su ogni canale	Ascolta 1.2s su ciascun canale
Configurabile per la scansione: <ul style="list-style-type: none"> • Tutti i canali • Canali del paese (predefinito) • canali DCA 	Analizza tutti i canali

Identificazione non autorizzata

Se la risposta della sonda o i beacon di un dispositivo non autorizzato vengono sentiti da punti di accesso in modalità locale, flex-connect o monitor, queste informazioni vengono comunicate tramite CAPWAP al controller WLC (Wireless LAN Controller) per il processo. Per evitare falsi positivi, vengono utilizzati diversi metodi per garantire che altri access point Cisco gestiti non vengano identificati come dispositivi anomali. Questi metodi includono aggiornamenti dei gruppi di mobilità, pacchetti di RF adiacenti e punti di accesso descrittivi consentiti tramite Prime Infrastructure (PI).

Rogue Records

Mentre il database dei dispositivi non autorizzati del controller contiene solo l'insieme corrente dei problemi rilevati, la PI include anche una cronologia degli eventi e registra i problemi non più visibili.

Dettagli sul server non autorizzato

Un CAPWAP esce dal canale per 50 ms per ascoltare i client non autorizzati, monitorare i disturbi e le interferenze dei canali. Tutti i client o gli access point non autorizzati rilevati vengono inviati al controller che raccoglie le seguenti informazioni:

- Indirizzo MAC punto di accesso non autorizzato
- Nome dell'access point rilevato come non autorizzato
- Indirizzo MAC del client o dei client connessi non autorizzati
- Criteri di sicurezza
- Il preambolo
- Il rapporto segnale/rumore (SNR)
- L'indicatore di potenza del segnale del ricevitore (RSSI)
- Rilevamento canale non autorizzato
- Radio in cui viene rilevato il server non autorizzato
- SSID non autorizzato (se il SSID non autorizzato è trasmesso)
- Indirizzo IP non autorizzato
- Prima e ultima volta in cui viene segnalato il caso anomalo
- Larghezza canale

Per esportare gli eventi indesiderati

Per esportare gli eventi anomali in un Network Management System (NMS) di terze parti per l'archiviazione, il WLC consente di aggiungere ulteriori ricevitori trap SNMP. Quando un router non autorizzato viene rilevato o cancellato dal controller, una trap che contiene queste informazioni viene comunicata a tutti i ricevitori di trap SNMP. Un avvertimento dell'esportazione di eventi tramite SNMP è che se più controller rilevano lo stesso rogue, gli eventi duplicati vengono visti dal NMS, in quanto la correlazione viene effettuata solo a PI.

Timeout record non autorizzato

Una volta aggiunto ai record del WLC, un rogue AP rimane lì fino a quando non viene più visto. Dopo un timeout configurabile dall'utente (1200 secondi per impostazione predefinita), un router non autorizzato nella categoria_unclassified_viene escluso.

I "Rogues" in altri stati, ad esempio_Contains_and_Friendly_ persistono in modo che ad essi venga applicata la classificazione appropriata se ricompaiono.

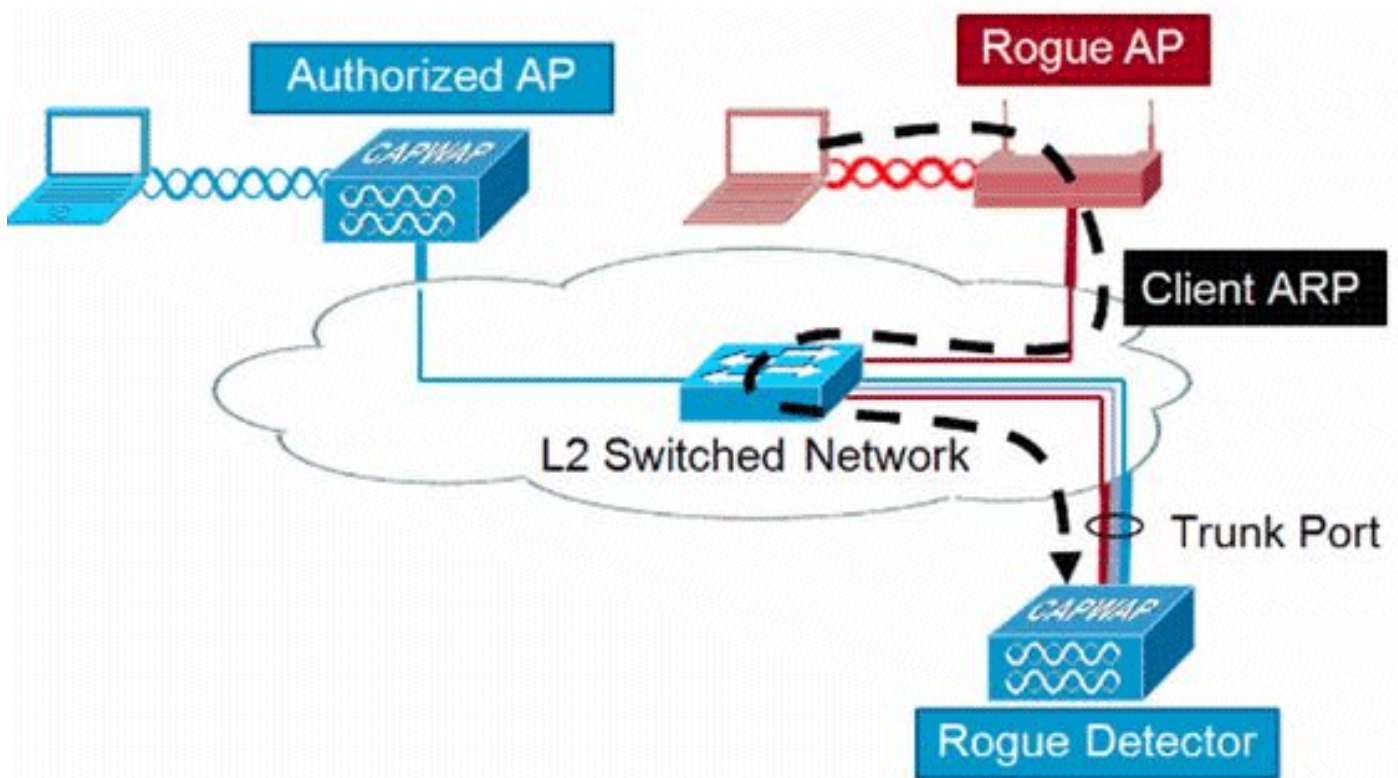
Esiste una dimensione massima del database per i record non autorizzati che è variabile tra le piattaforme di controller:


- 3504 - Rilevamento e contenimento di un massimo di 600 punti di accesso non autorizzati e 1.500 client non autorizzati
- 5520 - Rilevamento e contenimento di un massimo di 24.000 punti di accesso non autorizzati e 3.200 client non autorizzati
- 8540 - Rilevamento e contenimento di un massimo di 24.000 punti di accesso non autorizzati e 3.200 client non autorizzati

Punto di accesso rilevamento server non autorizzati

Un punto di accesso per il rilevamento rogue ha lo scopo di correlare le informazioni rogue udite via etere con le informazioni ARP ottenute dalla rete cablata. Se un indirizzo MAC viene ascoltato via etere come un access point o un client non autorizzato e viene anche ascoltato sulla rete cablata, il server non autorizzato viene determinato come appartenente alla rete cablata. Se viene rilevato che il server non autorizzato si trova sulla rete cablata, la gravità dell'allarme per il punto di accesso non autorizzato viene impostata su_critical_. Un punto di accesso del rilevatore di anomalie non riesce a identificare i client non autorizzati dietro un dispositivo che utilizza il protocollo NAT.

Questo approccio viene utilizzato quando un access point non autorizzato dispone di una forma di autenticazione, WEP o WPA. Quando una forma di autenticazione è configurata in un access point non autorizzato, il Lightweight Access Point non può associarsi perché non conosce il metodo di autenticazione e le credenziali configurate nel server non autorizzato.



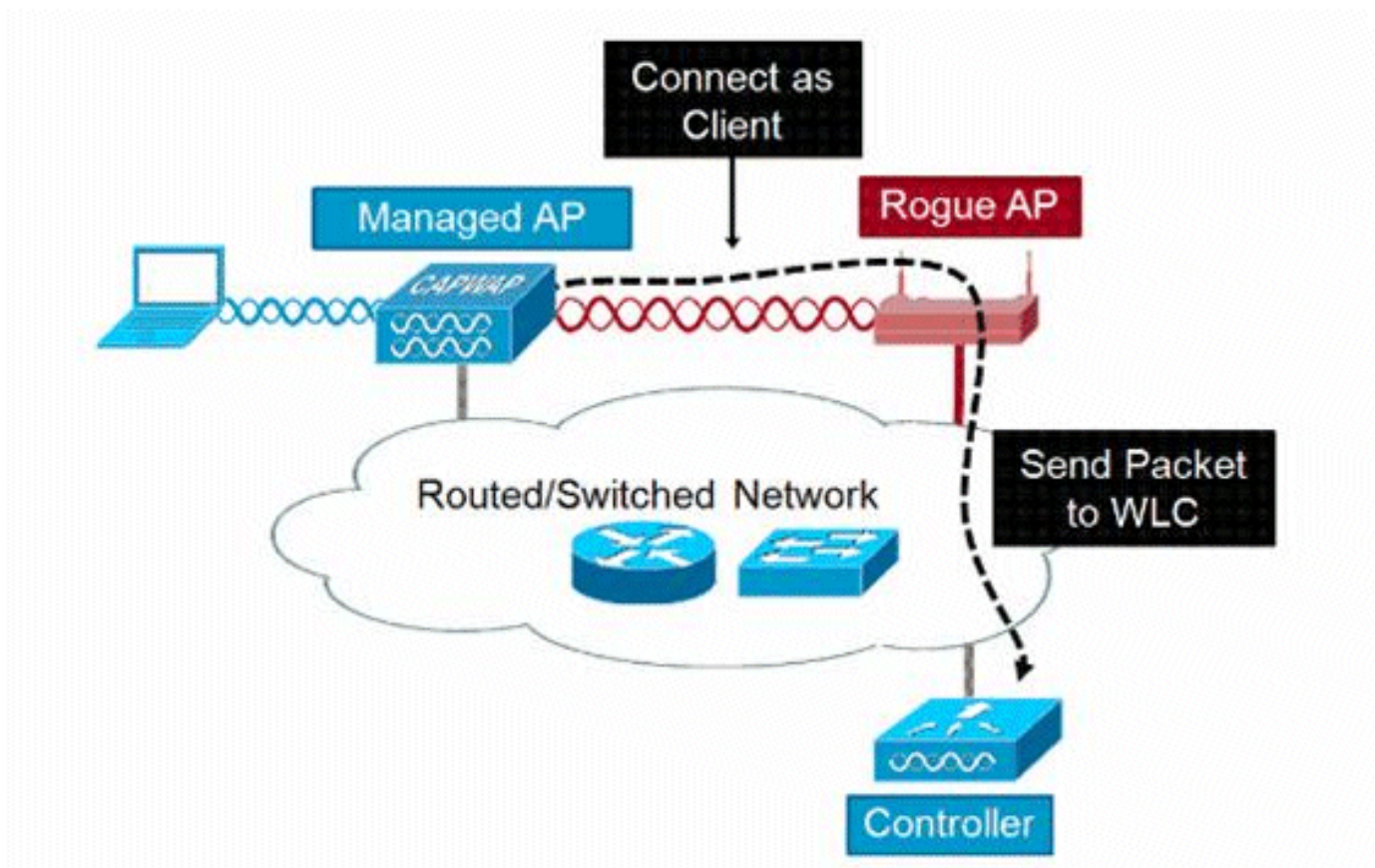
 Nota: solo i punti di accesso Wave 1 possono essere configurati come rilevatori di server non autorizzati.

Considerazioni sulla scalabilità

Un punto di accesso per il rilevamento di anomalie può rilevare fino a 500 anomalie e 500 client non autorizzati. Se il rilevatore di anomalie è posizionato su un trunk con troppi dispositivi anomali, questi limiti vengono superati, causando problemi. Per evitare che ciò si verifichi, mantenere i punti di accesso per il rilevamento di anomalie a livello di distribuzione o di accesso alla rete.


RLDP

Lo scopo del protocollo RLDP è quello di identificare se un access point anomalo specifico è collegato all'infrastruttura cablata. Questa funzionalità utilizza essenzialmente l'access point più vicino per connettersi al dispositivo non autorizzato come client wireless. Dopo la connessione come client, viene inviato un pacchetto con l'indirizzo di destinazione del WLC per valutare se l'AP è connesso alla rete cablata. Se il server non autorizzato viene rilevato sulla rete cablata, la gravità dell'allarme per il punto di accesso non autorizzato viene elevata a critico.



L'algoritmo di RLDP è elencato di seguito:

1. Identificare l'access point unificato più vicino al server non autorizzato utilizzando i valori di intensità del segnale.
2. L'access point si connette quindi al server non autorizzato come client WLAN e tenta tre associazioni prima del timeout.
3. Se l'associazione ha esito positivo, l'access point utilizza quindi DHCP per ottenere un indirizzo IP.
4. Se è stato ottenuto un indirizzo IP, l'access point (che funziona come client WLAN) invia un pacchetto UDP a ciascuno degli indirizzi IP dei controller.
5. Se il controller riceve anche uno dei pacchetti RLDP dal client, il server non autorizzato viene contrassegnato come in transito con un livello di gravità critico.

 Nota: i pacchetti RLDP non sono in grado di raggiungere il controller se sono state applicate le regole di filtro tra la rete del controller e la rete in cui si trova il dispositivo non autorizzato.

Avvertenze di RLDP

- Il protocollo RLDP funziona solo con access point non autorizzati aperti che trasmettono il proprio SSID con l'autenticazione e la crittografia disabilitate.

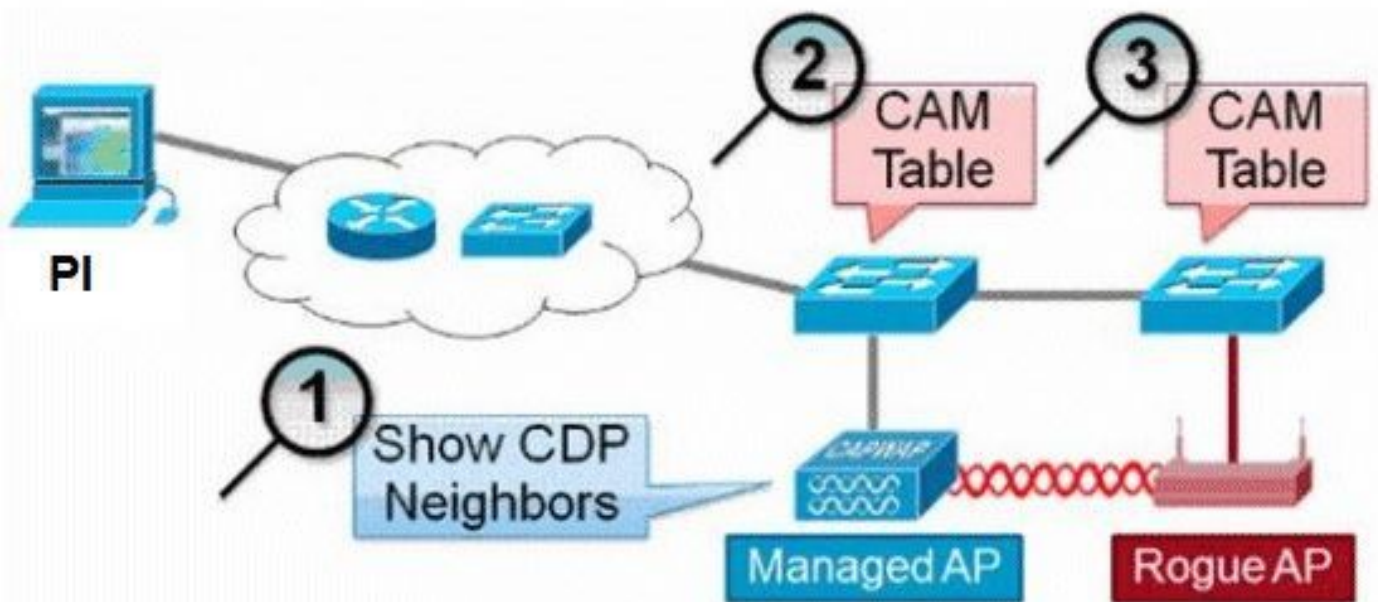
- Per il protocollo RLDP, l'access point gestito che opera come client deve essere in grado di ottenere un indirizzo IP tramite DHCP nella rete non autorizzata
- È possibile utilizzare RLDP manuale per tentare più volte di eseguire il trace RLDP su un router non autorizzato.
- Sul processo RLDP, l'access point non è in grado di servire i client. Questo influisce negativamente sulle prestazioni e sulla connettività dei punti di accesso in modalità locale.
- RLDP non tenta di connettersi a un access point non autorizzato che funziona in un canale DFS a 5 GHz.

Tracce porte switch

La traccia della porta dello switch è una tecnica di mitigazione dei punti di accesso non autorizzati. Anche se la traccia della porta dello switch viene avviata dalla porta IP, utilizza le informazioni CDP e SNMP per tracciare un router verso il basso fino a una porta specifica della rete.

Per eseguire la traccia della porta dello switch, tutti gli switch della rete devono essere aggiunti alla PI con credenziali SNMP. Sebbene le credenziali di sola lettura servano a identificare la porta su cui si trova il router non autorizzato, le credenziali di lettura/scrittura consentono anche alla porta di chiudere la porta, in modo che contenga la minaccia.

Al momento, questa funzione funziona solo sugli switch Cisco con Cisco IOS® e CDP abilitato, e CDP deve essere abilitato anche sugli access point gestiti.



L'algoritmo per la traccia della porta dello switch è elencato di seguito:

1. L'API trova l'access point più vicino, che rileva l'access point anomalo via etere e recupera i relativi vicini CDP.

2. La PI utilizza quindi il protocollo SNMP per esaminare la tabella CAM all'interno dello switch adiacente e cerca una corrispondenza positiva per identificare la posizione dei router non autorizzati.
3. Una corrispondenza positiva si basa sull'indirizzo MAC non autorizzato esatto, +1/-1 sull'indirizzo MAC non autorizzato, su qualsiasi indirizzo MAC di client non autorizzati o su una corrispondenza OUI basata sulle informazioni del fornitore relative a un indirizzo MAC.
4. Se non viene trovata una corrispondenza positiva sullo switch più vicino, la PI continua la ricerca negli switch adiacenti fino a due hop di distanza (impostazione predefinita).

Wired-Side Tracing Techniques Comparison

	How it Works	What It Detects	Accuracy
Switchport Tracing	<ol style="list-style-type: none"> 1. AP hears rogue over air 2. Detecting AP advises of nearby switches 3. Trace starts on nearby switches 4. Results reported in order of probability 5. Administrator may disable port 	<ul style="list-style-type: none"> • Open APs • Secured APs • NAT APs 	<ul style="list-style-type: none"> • Moderate
RLDP	<ol style="list-style-type: none"> 1. AP hears rogue over air 2. Detecting AP connects as client to rogue AP 3. Detecting AP sends RLDP packet 4. If RLDP packet seen at WLC, then on wire 	<ul style="list-style-type: none"> • Open APs • NAT APs 	<ul style="list-style-type: none"> • 100%
Rogue Detector	<ol style="list-style-type: none"> 1. Place detector AP on trunk 2. Detector receives all rogue MACs from WLC 3. Detector AP matches rogue MACs from wired-side ARPs 	<ul style="list-style-type: none"> • Open APs • Secured APs • NAT APs 	<ul style="list-style-type: none"> • High

Classificazione non autorizzati

Per impostazione predefinita, tutti i router rilevati dal Cisco UWN sono considerati non classificati. Come illustrato nell'immagine, i router possono essere classificati in base a diversi criteri, tra cui RSSI, SSID, tipo di protezione, rete di attivazione/disattivazione e numero di client:

Lower Severity

Higher Severity

Off-Network
Secured
Foreign SSID
Weak RSSI
No clients

On-Network
Open
Our SSID
Strong RSSI
Attracts clients

Regole di classificazione non valide

Regole di classificazione non autorizzate, consentono di definire un insieme di condizioni che contrassegnano un non autorizzato come dannoso o amichevole. Queste regole vengono configurate sulla PI o sul WLC, ma vengono sempre eseguite sul controller quando vengono rilevati nuovi router.

Per ulteriori informazioni sulle regole non [autorizzate](#) nei WLC, consultare il [documento Rule Based Rogue Classification in Wireless LAN Controller \(WLC\) e Prime Infrastructure \(PI\)](#).

Fatti HA

Se si sposta manualmente un dispositivo anomalo in uno stato confinato (qualsiasi classe) o in uno stato descrittivo, queste informazioni vengono memorizzate nella memoria flash Cisco WLC in standby; tuttavia, il database non viene aggiornato. Quando si verifica lo switchover HA, viene caricato l'elenco dei dispositivi non autorizzati dalla memoria flash Cisco WLC in standby precedente.

In uno scenario ad alta disponibilità, se il livello di sicurezza del rilevamento rogue è impostato su Alta o Critica, il timer rogue sul controller di standby inizia solo dopo il tempo di stabilizzazione del rilevamento rogue, che è di 300 secondi. Pertanto, le configurazioni attive sul controller di standby vengono riflesse solo dopo 300 secondi.

Fatti su Flex-Connect

Un punto di accesso FlexConnect (con rilevamento rogue abilitato) in modalità connessa preleva l'elenco di contenimento dal controller. Se nel controller sono impostati i parametri auto-contains SSID e auto-contains ad hoc, queste configurazioni vengono impostate su tutti gli access point FlexConnect in modalità connessa e l'access point lo memorizza.

Quando l'access point FlexConnect passa alla modalità standalone, vengono eseguite le attività successive:

- Il contenimento impostato dal controller continua.

- Se il punto di accesso FlexConnect rileva un punto di accesso non autorizzato con lo stesso SSID di quello dell'SSID infra (SSID configurato nel controller a cui è connesso il punto di accesso FlexConnect), il contenimento viene avviato se l'opzione Contenuto automatico SSID è stata abilitata dal controller prima del passaggio alla modalità standalone.
- Se l'access point FlexConnect rileva un router ad hoc, il contenimento viene avviato se l'opzione di contenimento automatico ad hoc è stata abilitata dal controller in modalità connessa.

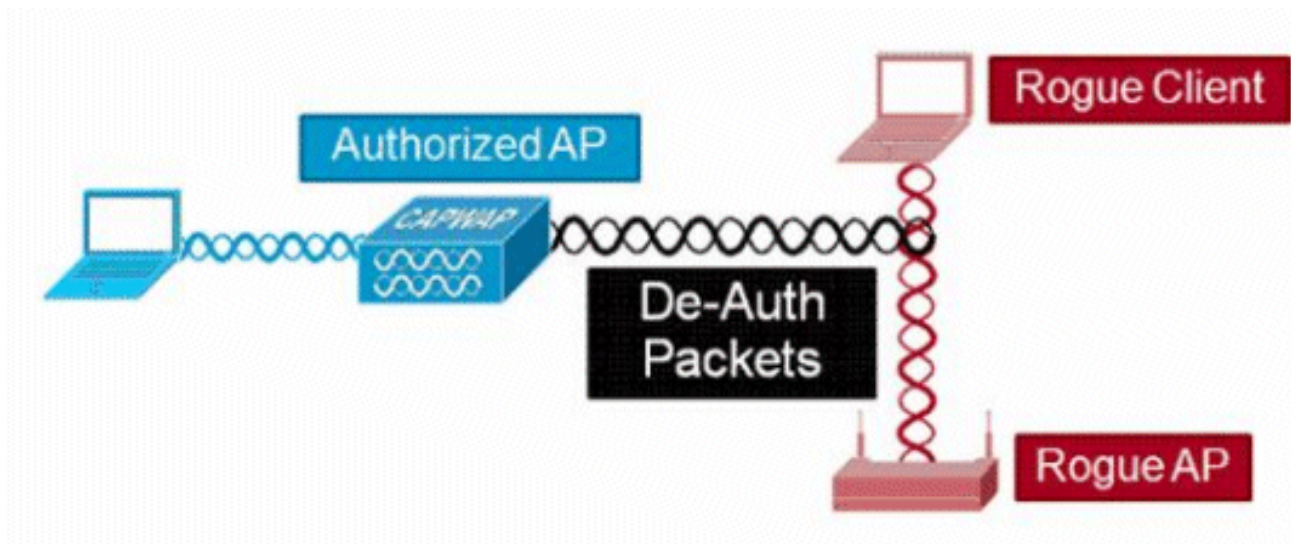
Quando l'access point FlexConnect standalone torna alla modalità di connessione, vengono eseguite le seguenti attività:

- Tutto il contenimento viene cancellato.
- Il contenimento avviato dal controller subentra.

Mitigazione dei server non autorizzati

Controllo di elementi non autorizzati

Il contenimento è un metodo che utilizza pacchetti via etere per interrompere temporaneamente il servizio su un dispositivo non autorizzato fino a quando non può essere rimosso fisicamente. Il contenimento funziona con lo spoof dei pacchetti di deautenticazione con l'indirizzo di origine falsificato del rogue AP, in modo che tutti i client associati vengano espulsi.



Dettagli contenimento Rogue

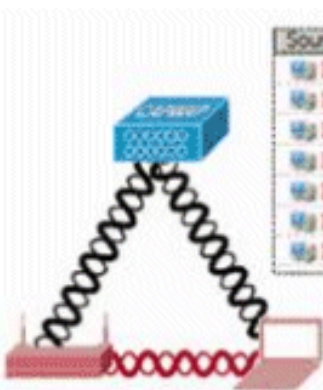
Un contenimento avviato su un access point non autorizzato senza client utilizza solo frame di deautenticazione inviati all'indirizzo di broadcast:



Source	Destination	Data Rate	Size	Protocol
Rogue AP	Ethernet Broadcast	6.0	144	802.11 Beacon
Rogue AP	Ethernet Broadcast	6.0	56	802.11 Deauth
Rogue AP	Ethernet Broadcast	6.0	30	802.11 Deauth

Broadcast Deauth frames only

Un contenimento avviato su un access point non autorizzato con i client utilizza i frame di deautenticazione inviati all'indirizzo di broadcast e all'indirizzo del client:



Source	Destination	Data Rate	Size	Protocol
Rogue AP	Ethernet Broadcast	6.0	144	802.11 Beacon
Rogue AP	Ethernet Broadcast	6.0	56	802.11 Deauth
Rogue AP	Ethernet Broadcast	6.0	30	802.11 Deauth
Rogue AP	Rogue Client	6.0	30	802.11 Deauth
Rogue AP	Rogue Client	6.0	30	802.11 Deauth
Rogue AP	Rogue Client	6.0	30	802.11 Deauth
Rogue AP	Rogue Client	6.0	30	802.11 Deauth

Broadcast and Unicast Deauth frames

I pacchetti di contenimento vengono inviati al livello di alimentazione dell'access point gestito e alla velocità dati abilitata più bassa.

Container invia un minimo di 2 pacchetti ogni 100 ms:

Source	Destination	Data Rate	Size	Relative Time	Protocol
Rogue AP	Ethernet Broadcast	6.0	56	0.000000	802.11 Deauth
Rogue AP	Ethernet Broadcast	6.0	30	0.000004	802.11 Deauth
Rogue AP	Ethernet Broadcast	6.0	144	0.000007	802.11 Beacon
Rogue AP	Ethernet Broadcast	6.0	56	0.102414	802.11 Deauth
Rogue AP	Ethernet Broadcast	6.0	30	0.102419	802.11 Deauth

~100ms

Nota: i punti di accesso in modalità non monitor inviano un contenimento a un intervallo di 500 ms anziché di 100 ms usato dai punti di accesso in modalità monitor.

- Un singolo dispositivo non autorizzato può essere contenuto da 1 a 4 punti di accesso gestiti che operano congiuntamente per ridurre temporaneamente la minaccia.
- Il contenimento può essere ottenuto usando la modalità locale, la modalità monitor e la modalità flex-connect (Connesso) dei punti di accesso. Per la modalità locale dei punti di accesso flex-connect, è possibile contenere un massimo di tre dispositivi non autorizzati per radio. Per i punti di accesso in modalità monitor, è possibile contenere un massimo di sei dispositivi non autorizzati per radio.

Contenimento automatico

Oltre all'avvio manuale di un sistema sigillato su un dispositivo malintenzionato tramite PI o l'interfaccia utente grafica del WLC, è possibile avviare automaticamente il sistema sigillato in determinati scenari. Questa configurazione si trova in General in sezione Rogue Policies della PI o dell'interfaccia del controller. Ognuna di queste funzionalità è disabilitata per impostazione predefinita e deve essere abilitata solo per annullare le minacce che causano il maggior numero di danni.

- Rogue on Wire - Se un dispositivo non autorizzato viene identificato per essere collegato alla rete cablata, viene automaticamente inserito in un contenitore.
- Uso del nostro SSID - Se un dispositivo malintenzionato utilizza un SSID uguale a quello configurato sul controller, questo è automaticamente contenuto. Questa funzione ha lo scopo di affrontare un attacco di erba di miele prima che causi danni.
- Client valido su punto di accesso non autorizzato: se un client elencato in un server Radius/AAA risulta associato a un dispositivo non autorizzato, il contenimento viene avviato solo per tale client e impedisce l'associazione a qualsiasi punto di accesso non gestito.
- Ad hoc Rogue AP: se viene individuata una rete ad hoc, questa viene automaticamente contenuta.

Avvertenze di contenimento Rogue

- Poiché il contenimento utilizza una parte del tempo radio del punto di accesso gestito per inviare i frame di deautenticazione, le prestazioni dei client voce e dati subiscono un impatto negativo fino al 20%. Per i client di dati, l'impatto è una riduzione della velocità effettiva. Per i client voce, il contenimento può causare interruzioni nelle conversazioni e ridurre la qualità della voce.
- Il contenimento può avere implicazioni legali quando viene avviato contro le reti adiacenti. Verificare che il dispositivo non autorizzato si trovi all'interno della rete e che presenti un rischio per la sicurezza prima di avviare il contenimento.

Chiusura porta switch

Una volta che una porta dello switch viene tracciata dall'uso di SPT, è possibile disabilitare tale porta in PI.GRECO. L'amministratore deve eseguire questo esercizio manualmente. È disponibile un'opzione per abilitare la porta dello switch tramite IP se il router non autorizzato viene rimosso fisicamente dalla rete.

Configurazione

Configura rilevamento server non autorizzati

Il rilevamento dei server non autorizzati è abilitato nel controller per impostazione predefinita.

Per configurare diverse opzioni, selezionare Security > Wireless Protection Policies > Rogue Policies > General (Sicurezza > Criteri di protezione wireless > Criteri non autorizzati > Generale). Esempio:

Passaggio 1. Modificare il timeout per i punti di accesso non autorizzati.

Passaggio 2. Abilitare il rilevamento di reti anomale ad hoc.

The screenshot displays the Cisco WLC configuration page for 'Rogue Policies'. The left sidebar shows the navigation tree under 'Security' > 'Wireless Protection Policies' > 'Rogue Policies' > 'General'. The main content area is titled 'Rogue Policies' and includes an 'Apply' button. The 'Rogue Detection Security Level' is set to 'Custom'. Below this, various detection and reporting options are configured, including 'Rogue Location Discovery Protocol' (All Aps), 'Expiration Timeout for Rogue AP and Rogue Client entries' (3600 Seconds), and 'Detect and report Ad-Hoc Networks' (checked and enabled). The 'Auto Contain' section is also visible, with 'Auto Containment Level' set to 'Auto' and several other options enabled.

Dalla CLI:

```
<#root>
```

```
(Cisco Controller) >
```

```
config rogue ap timeout ?
```

```
<seconds> The number of seconds<240 - 3600> before rogue entries are flushed
```

```
(Cisco Controller) >
```

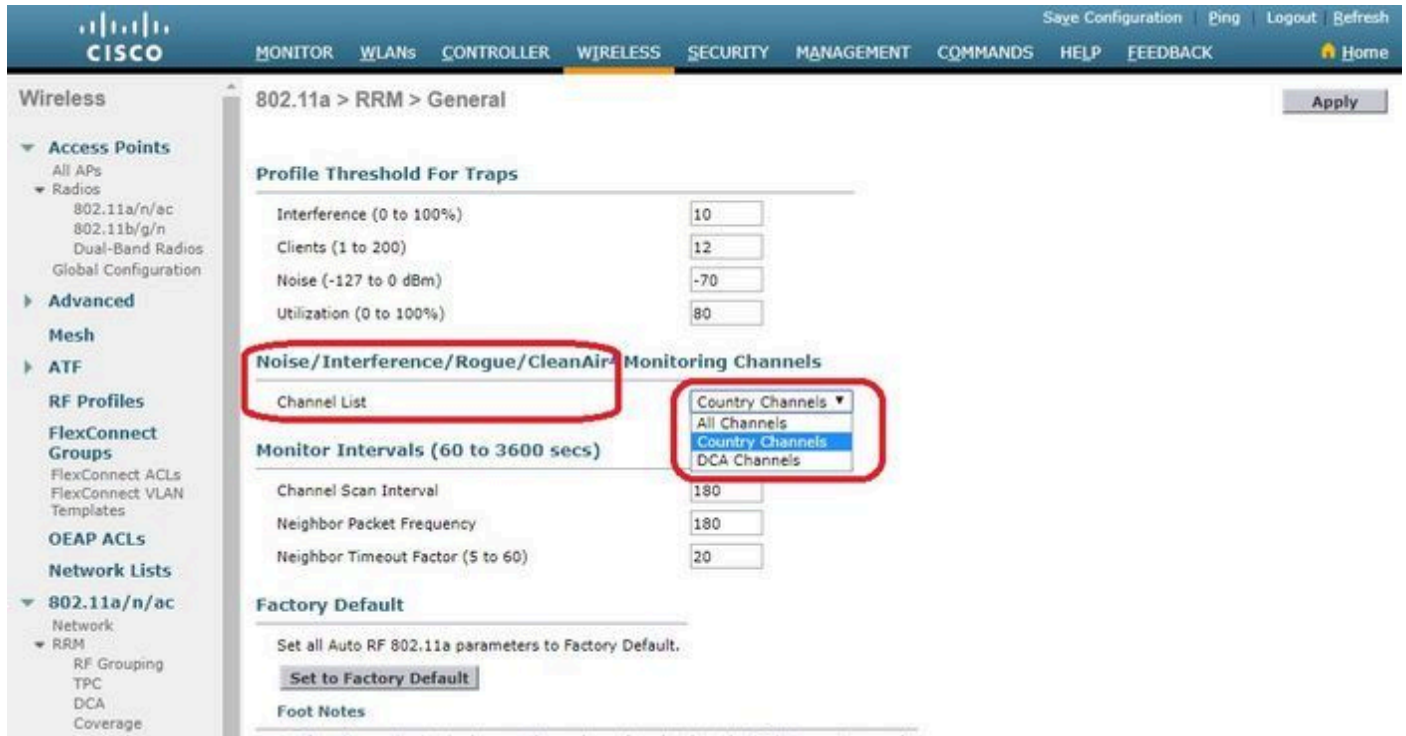
```
config rogue adhoc enable/disable
```

Configura analisi canale per rilevamento server non autorizzati

Per un punto di accesso in modalità locale/Flex-Connect/Monitor, è disponibile un'opzione in

configurazione RRM che consente all'utente di scegliere i canali da analizzare per individuare i router. A seconda della configurazione, l'access point analizza tutti i canali/canali di paese/canali DCA per rilevare i router non autorizzati.

Per configurarlo dalla GUI, selezionare Wireless > 802.11a/802.11b > RRM > Generale, come mostrato nell'immagine.



Dalla CLI:

```
<#root>
```

```
(Cisco Controller) >
```

```
config advanced 802.11a monitor channel-list ?
```

```
all           Monitor all channels
country       Monitor channels used in configured country code
dca           Monitor channels used by automatic channel assignment
```

Configura classificazione non autorizzati

Classificazione manuale di un punto di accesso non autorizzato

Per classificare un access point non autorizzato come descrittivo, dannoso o non classificato, selezionare Monitoraggio > Non autorizzato > Access point non classificati e fare clic sul nome dell'access point non autorizzato. Scegliere l'opzione dall'elenco a discesa, come mostrato nell'immagine.

The screenshot shows the Cisco Meraki Monitor interface. The top navigation bar includes links for Save Configuration, Ping, Logout, Refresh, and Home. The main menu on the left lists various monitoring categories like Access Points, Cisco CleanAir, Statistics, CDP, Rogues, Clients, and Applications. The 'Rogues' section is expanded, showing a tree view of rogue types such as Friendly APs, Malicious APs, Custom APs, Unclassified APs, Rogue Clients, and Adhoc Rogues. The 'Rogue AP Detail' page for a specific rogue AP shows the following information:

- MAC Address:** 00:06:91:43:6d:e2
- Type:** AP
- Is Rogue On Wired Network?:** No
- First Time Reported On:** Thu May 30 16:21:30 2019
- Last Time Reported On:** Fri May 31 13:07:11 2019
- Class Type:** A dropdown menu is open, showing options: Unclassified, Friendly, Malicious (selected), Unclassified, and Custom.
- State:** No
- Manually Contained:** No
- Update Status:** A dropdown menu showing "-- Choose New Status --".

Below the details, there is a section titled "APs that detected this Rogue" with a table:

Base Radio MAC	AP Name	SSID	Channel	Channel Width (Mhz)	Radio Type	Security Policy	Pre-A
b4:de:31:c6:30:c0	AP2800-1	Cisco-17D90F4C	6	20	802.11n2.4G	Open	Long

There is also a link for "Clients associated to this Rogue AP".

Dalla CLI:

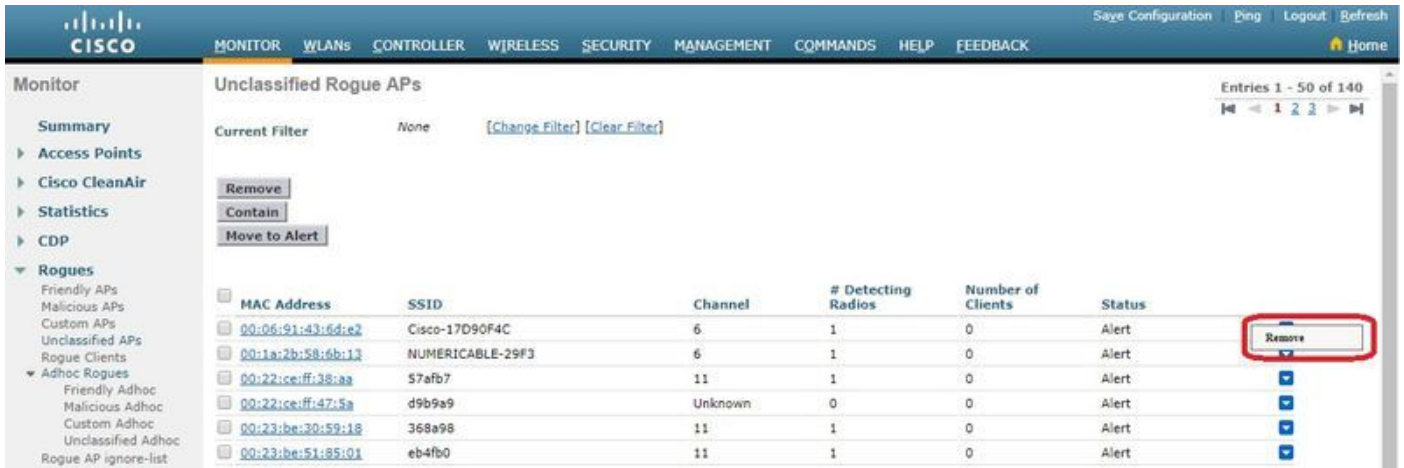
```
<#root>
```

```
(Cisco Controller) >
```

```
config rogue ap ?
```

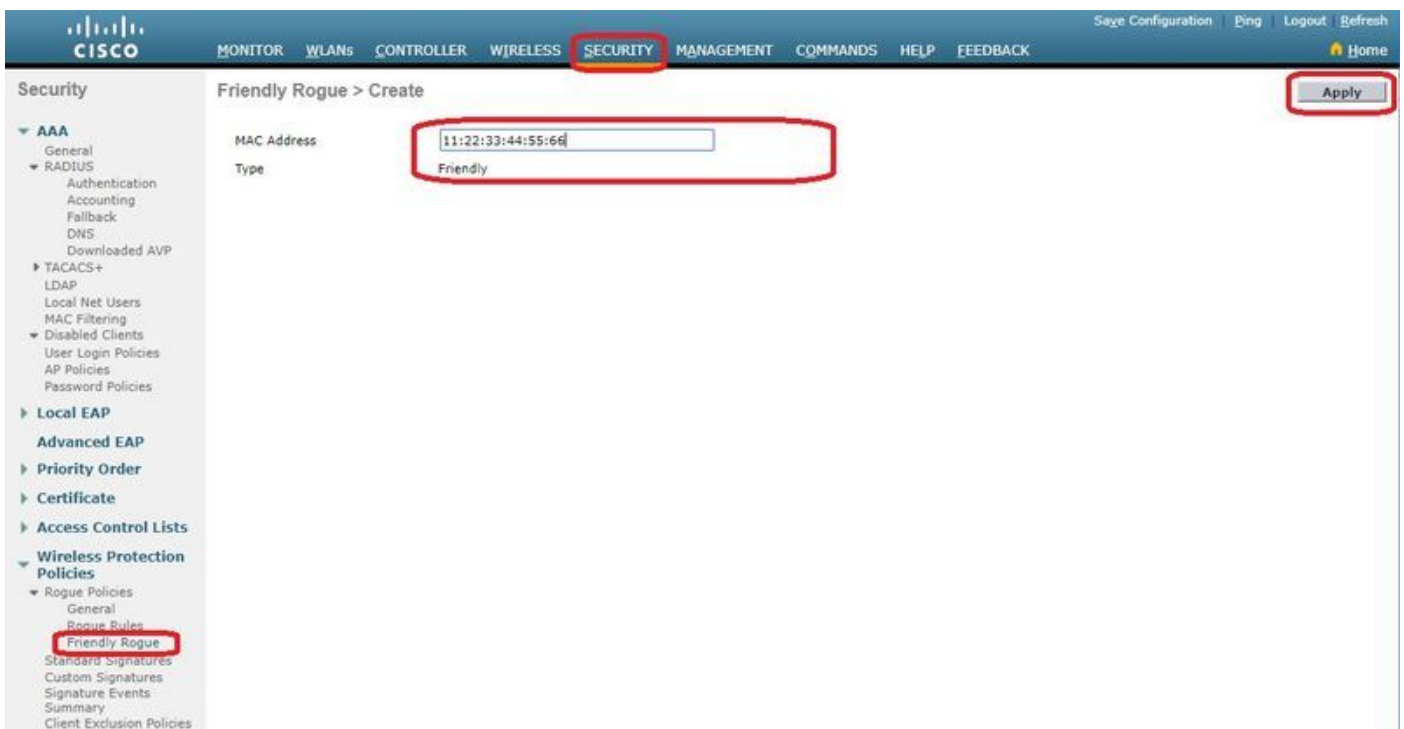
- classify Configures rogue access points classification.
- friendly Configures friendly AP devices.
- rldp Configures Rogue Location Discovery Protocol.
- ssid Configures policy for rogue APs advertsing our SSID.
- timeout Configures the expiration time for rogue entries, in seconds.
- valid-client Configures policy for valid clients which use rogue APs.

Per rimuovere manualmente una voce non autorizzata dall'elenco, selezionare Monitor > Non autorizzato > Punti di accesso non classificati e fare clic su Rimuovi, come mostrato nell'immagine.



Per configurare un punto di accesso non autorizzato come punto di accesso non autorizzato, selezionare Sicurezza > Criteri di protezione wireless > Criteri non autorizzati > Indirizzi non autorizzati e aggiungere l'indirizzo MAC non autorizzato.

Le voci rogue aggiunte possono essere verificate da Monitor > Rogues > Friendly Roguepage, come mostrato nell'immagine.



Configurare un punto di accesso per il rilevamento dei server non autorizzati

Per configurare l'access point come rilevatore di errori dalla GUI, selezionare Wireless > Tutti gli access point. Scegliere il nome del punto di accesso e modificare la modalità come mostrato nell'immagine.

Dalla CLI:

```
<#root>
```

```
(Cisco Controller) >
```

```
config ap mode rogue AP_Managed
```

Changing the AP's mode cause the AP to reboot.
Are you sure you want to continue? (y/n) y

Configurare Switchport per un punto di accesso rilevamento server non autorizzati

```
interface GigabitEthernet1/0/5
description Rogue Detector
switchport trunk native vlan 100
switchport mode trunk
```



Nota: la VLAN nativa in questa configurazione è una VLAN con connettività IP al WLC.

Configurare RLDP


Per configurare il protocollo RLDP nella GUI del controller, selezionare Security > Wireless Protection Policies > Rogue Policies > General (Sicurezza > Criteri di protezione wireless > Criteri non autorizzati > Generale).

The screenshot shows the Cisco Security configuration interface. The 'Rogue Policies' section is active, and the 'Rogue Location Discovery Protocol' is highlighted. The 'MonitorModeAps' option is selected in the dropdown menu. The 'Auto Contain' section shows various options with checkboxes for enabling or disabling them.

AP in modalità monitor: consentono solo ai punti di accesso in modalità monitor di partecipare al programma RLDP.

Tutti i punti di accesso - in modalità locale/Flex-Connect/Monitor partecipano al processo RLDP.

Disabilitato: RLDP non viene attivato automaticamente. Tuttavia, l'utente può attivare manualmente il protocollo RLDP per un particolare indirizzo MAC dalla CLI.

 Nota: la modalità di monitoraggio AP ha la preferenza sull'access point locale/Flex-Connect per eseguire il protocollo RLDP se entrambi rilevano un particolare router in eccesso rispetto a -85 dbm RSSI.

Dalla CLI:

```
<#root>
```

```
(Cisco Controller) >
```

```
config rogue ap rldp enable
```

```
?
```

```
alarm-only      Enables RLDP and alarm if rogue is detected
```

```
auto-contain    Enables RLDP, alarm and auto-contain if rogue is detected.
```

```
(Cisco Controller) >config rogue ap rldp enable alarm-only ?
```

```
monitor-ap-only Perform RLDP only on monitor AP
```

La pianificazione RLDP e l'attivazione manuale sono configurabili solo al prompt dei comandi. Per avviare manualmente RLDP:

```
<#root>
```

```
(Cisco Controller) >
```

```
config rogue ap rldp initiate
```

```
?
```

```
<MAC addr> Enter the MAC address of the rogue AP (e.g. 01:01:01:01:01:01).
```

Per la pianificazione di RLDP:

```
<#root>
```

```
(Cisco Controller) >
```

```
config rogue ap rldp schedule ?
```

```
add          Enter the days when RLDP scheduling to be done.
delete       Enter the days when RLDP scheduling needs to be deleted.
enable       Configure to enable RLDP scheduling.
disable      Configure to disable RLDP scheduling.
```

```
(Cisco Controller) >
```

```
config rogue ap rldp schedule add ?
```

```
fri          Configure Friday for RLDP scheduling.
sat          Configure Saturday for RLDP scheduling.
sun          Configure Sunday for RLDP scheduling.
mon          Configure Monday for RLDP scheduling.
tue          Configure Tuesday for RLDP scheduling.
wed          Configure Wednesday for RLDP scheduling.
thu          Configure Thursday for RLDP scheduling.
```

I tentativi RLDP possono essere configurati con il comando:

```
<#root>
```

```
(Cisco Controller) >
```

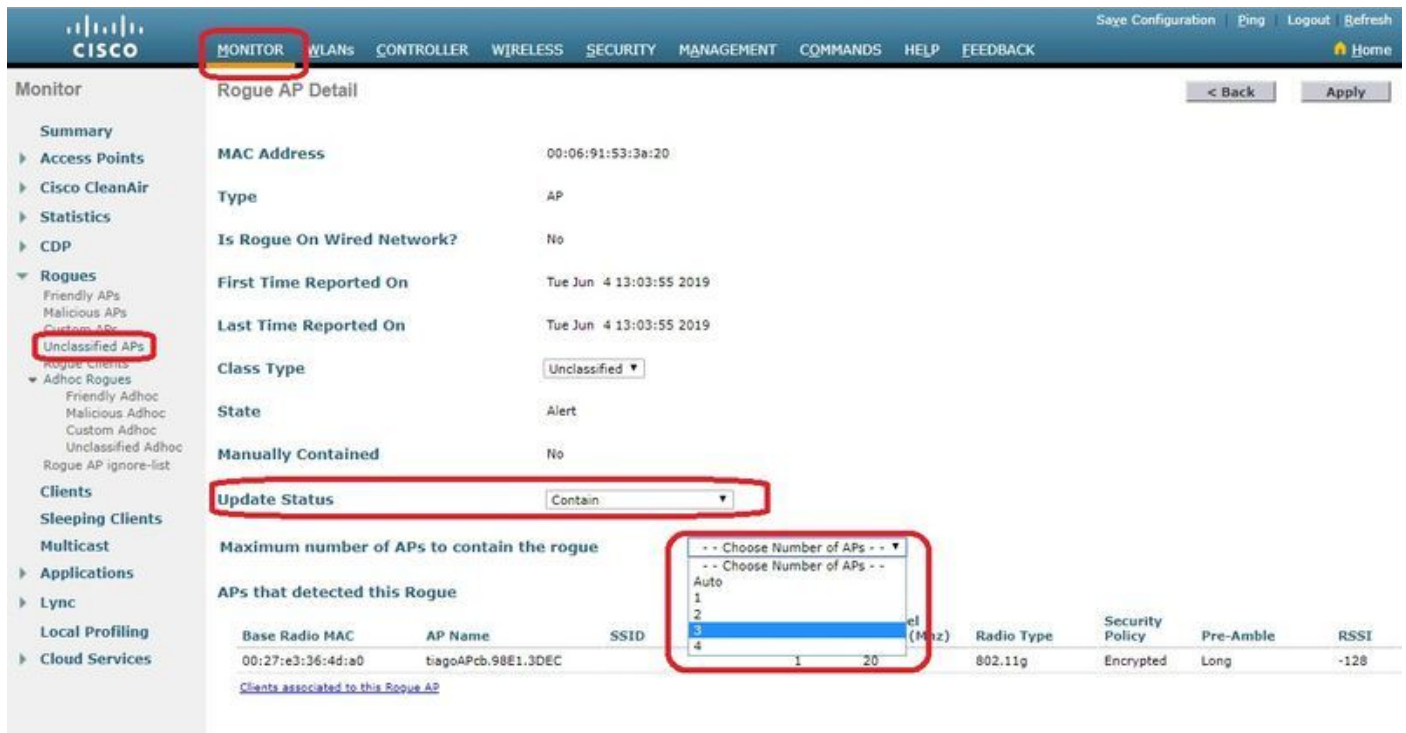
```
config rogue ap rldp retries ?
```

```
<count>     Enter the no.of times(1 - 5) RLDP to be tried per Rogue AP.
```

Configurazione della mitigazione dei problemi non gravi

Configura contenimento manuale

Per contenere manualmente un punto di accesso non autorizzato, selezionare Monitor > Rogues > Unclassified, come mostrato nell'immagine.



Dalla CLI:

```
<#root>
```

```
(Cisco Controller) >
```

```
config rogue client
```

```
?
```

```
aaa
```

Configures to validate if a rogue client is a valid client which uses AAA/local databases

```
alert
```

Configure the rogue client to the alarm state.

```
contain
```

Start to contain a rogue client.

```
delete
```

Delete rogue Client

```
mse
```

Configures to validate if a rogue client is a valid client which uses MSE.


```
(Cisco Controller) >
```

```
config rogue client contain 11:22:33:44:55:66
```

```
?
```

```
<num of APs>
```


Enter the maximum number of Cisco APs to actively contain the rogue client [1-4].

 Nota: un particolare server non autorizzato può essere contenuto con 1-4 punti di accesso. Per impostazione predefinita, il controller utilizza un punto di accesso per contenere un client. Se due access point sono in grado di rilevare un determinato server non autorizzato, l'access point con l'RSSI più alto contiene il client indipendentemente dalla modalità dell'access point.

Contenimento automatico

Per configurare il contenimento automatico, passare a **Sicurezza > Criteri di protezione wireless > Criteri non autorizzati > Generale** e abilitare tutte le opzioni applicabili per la rete.

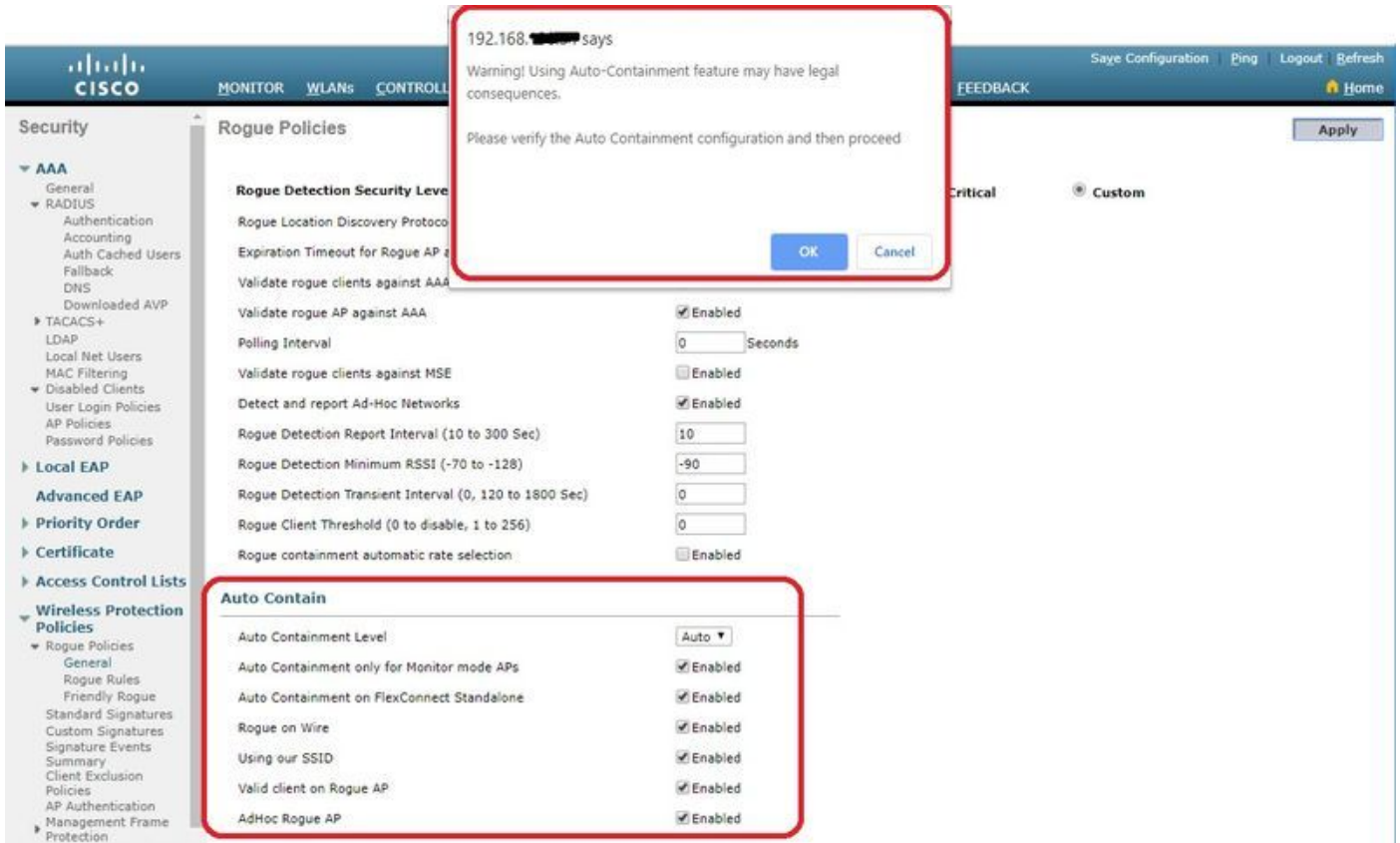
Se si desidera che il WLC Cisco contenga automaticamente alcuni dispositivi non autorizzati, selezionare queste caselle. In caso contrario, lasciare deselezionate le caselle di controllo, che rappresenta il valore predefinito.

 **Avvertenza:** quando si abilita uno di questi parametri, viene visualizzato il messaggio: "L'uso di questa funzione ha conseguenze legali. Vuoi continuare?" Le frequenze a 2,4 e 5 GHz nella banda Industrial, Scientific, and Medical (ISM) sono aperte al pubblico e possono essere utilizzate senza licenza. In quanto tale, il contenimento dei dispositivi sulla rete di un'altra parte potrebbe avere conseguenze giuridiche.

Di seguito sono riportati i parametri di contenimento automatico.

Parametro	Descrizione
Livello di contenimento automatico	<p>Elenco a discesa da cui è possibile scegliere il livello di contenimento automatico da 1 a 4.</p> <p>È possibile scegliere fino a quattro punti di accesso per il contenimento automatico quando un utente non autorizzato viene spostato in uno stato contenuto tramite uno qualsiasi dei criteri di contenimento automatico.</p> <p>È inoltre possibile scegliere Automatico per la selezione automatica del numero di punti di accesso utilizzati per il contenimento automatico. Per un contenimento efficace, il Cisco WLC sceglie il numero di access point richiesto in base all'RSSI.</p> <p>Il valore RSSI associato a ciascun livello di contenimento è il seguente:</p> <ul style="list-style-type: none">• 1 — da 0 a -55 dBm• 2 — da -75 a -55 dBm• 3 — da -85 a -75 dBm

Parametro	Descrizione
	<ul style="list-style-type: none"> • 4 — Inferiore a -85 dBm
Contenimento automatico solo per i punti di accesso in modalità Monitor	Casella di controllo che è possibile selezionare per abilitare i punti di accesso in modalità di monitoraggio per il contenimento automatico. Lo stato predefinito è disabled.
Contenimento automatico su FlexConnect standalone	Casella di controllo che è possibile selezionare per abilitare il contenimento automatico sui punti di accesso FlexConnect in modalità standalone. Lo stato predefinito è disabled. Quando gli access point FlexConnect sono in modalità standalone, è possibile abilitare solo i criteri di contenimento automatico Use our SSID o AdHoc Rogue AP. Il contenimento si arresta dopo che l'access point standalone si riconnette al WLC Cisco.
Rogue on Wire	Casella di controllo che consente di includere automaticamente i router rilevati nella rete cablata. Lo stato predefinito è disabled.
Usa il nostro SSID	Casella di controllo che consente di includere automaticamente i router che annunciano l'SSID della rete. Se si lascia questo parametro non selezionato, il WLC di Cisco genera un allarme solo quando viene rilevato un tale anomalo. Lo stato predefinito è disabled.
Client valido su punto di accesso non autorizzato	Casella di controllo che consente di contenere automaticamente un punto di accesso non autorizzato a cui sono associati client attendibili. Se si lascia questo parametro non selezionato, il WLC di Cisco genera un allarme solo quando viene rilevato un tale anomalo. Lo stato predefinito è disabled.
Ad hoc Rogue AP	Selezionare la casella di controllo che consente di contenere automaticamente le reti ad hoc rilevate dal WLC Cisco. Se si lascia questo parametro non selezionato, il WLC Cisco genera un allarme solo quando viene rilevata una rete di questo tipo. Lo stato predefinito è disabled.



Fare clic su Apply (Applica) per inviare i dati al WLC Cisco, ma i dati non vengono conservati durante un ciclo di alimentazione. Questi parametri vengono memorizzati temporaneamente nella RAM volatile.

Dalla CLI:

```
<#root>
```

```
(Cisco Controller) >
```

```
config rogue adhoc ?
```

```
alert          Stop Auto-Containment, generate a trap upon detection of the
                adhoc rogue.
```

```
auto-contain   Automatically contain adhoc rogue.
```

```
contain        Start to contain adhoc rogue.
```

```
disable        Disable detection and reporting of Ad-Hoc rogues.
```

```
enable         Enable detection and reporting of Ad-Hoc rogues.
```

```
external       Acknowledge presence of a adhoc rogue.
```

```
(Cisco Controller) >
```

```
config rogue adhoc auto-contain ?
```

```
(Cisco Controller) >
```

```
config rogue adhoc auto-contain
```

```
Warning! Use of this feature has legal consequences
Do you want to continue(y/n) :y
```

Con Prime Infrastructure

Cisco Prime Infrastructure può essere utilizzato per configurare e monitorare uno o più controller e i relativi access point. Cisco IP dispone di strumenti per facilitare il monitoraggio e il controllo di sistemi di grandi dimensioni. Quando si utilizza Cisco IP in una soluzione wireless Cisco, i controller determinano periodicamente il client, il punto di accesso non autorizzato, il client del punto di accesso non autorizzato, la posizione dei tag RFID (Radio Frequency ID) e memorizzano i percorsi nel database Cisco IP.

Cisco Prime Infrastructure supporta la classificazione basata su regole e utilizza le regole di classificazione configurate sul controller. Il controller invia trap a Cisco Prime Infrastructure dopo i seguenti eventi:

- Se un punto di accesso sconosciuto passa allo stato Amichevole per la prima volta, il controller invia una trap a Cisco Prime Infrastructure solo se lo stato non autorizzato è Alert. Non invia trap se theroguestate è Interno o Esterno.
- Se una voce di accesso viene rimossa dopo la scadenza del timeout, il controller invia una trap a Cisco Prime Infrastructure per i punti di accesso non autorizzati classificati come Dannosi (Alert, Threat) o Non classificati (Alert). Il controller non rimuove le voci con questi domoestati: Contenuto, Contenuto in sospeso, Interno ed Esterno.

Verifica

Per individuare i dettagli anomali in un controller nell'interfaccia grafica, selezionare Monitor > Rogues, come mostrato nell'immagine.

The screenshot shows the Cisco Prime Infrastructure web interface. The top navigation bar includes 'MONITOR' (highlighted with a red box), 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', 'HELP', and 'FEEDBACK'. The left sidebar shows a navigation menu with 'Rogues' selected and highlighted with a red box. The main content area is titled 'Unclassified Rogue APs' and shows a table of detected rogue access points.


MAC Address	SSID	Channel	# Detecting Radios	Number of Clients	Status
00:a3:8e:db:01:a0	blizzard	13	1	0	Alert
00:a3:8e:db:01:a1	Unknown	13	1	0	Alert
00:a3:8e:db:01:a2	Unknown	13	1	0	Alert
00:a3:8e:db:01:b1	Unknown	40	2	0	Alert
00:a3:8e:db:01:b2	Unknown	40	2	0	Alert
50:2f:a8:a2:0d:40	buterfly	11	1	0	Alert
2c:97:26:61:d2:79	MEO-61D279	Unknown	0	0	Alert
9e:97:26:61:d2:7a	MEO-WiFi	6	1	0	Alert
ac:22:05:ea:21:26	NOWO-A2121	1	1	0	Alert
c4:e9:84:c1:c8:90	MEO-50E3EC	6	1	0	Alert

In questa pagina sono disponibili diverse classificazioni per i tizi:

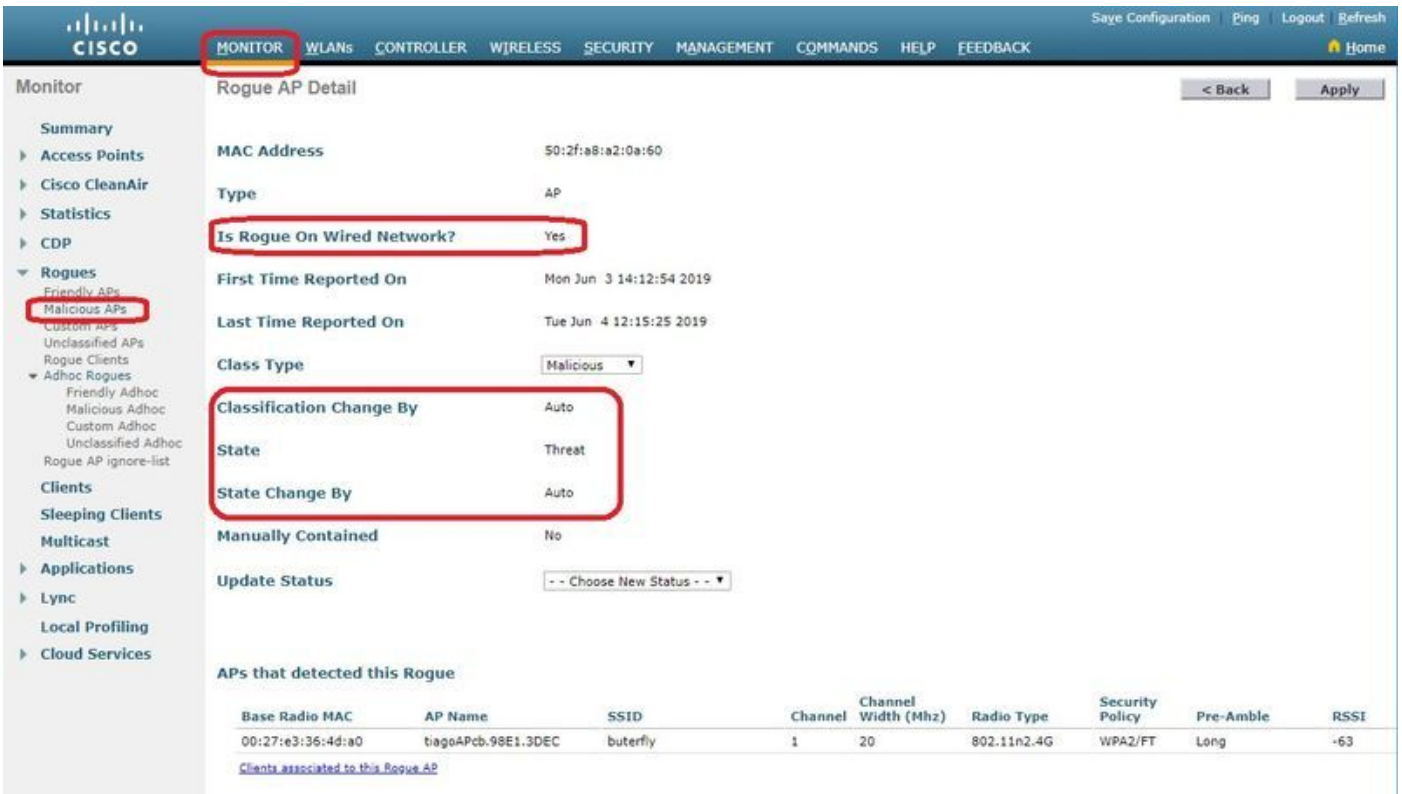
- Punti di accesso descrittivi: punti di accesso contrassegnati come descrittivi dall'amministratore.
- Punti di accesso dannosi - Punti di accesso identificati come dannosi tramite RLDP o Rogue

Detector AP.

- Punti di accesso personalizzati: punti di accesso classificati come personalizzati da regole non valide.
- Access point non classificati: per impostazione predefinita, i access point non autorizzati vengono visualizzati come elenco non classificati nel controller.
- Rogue Client - Client connessi a punti di accesso non autorizzati.
- Rogues ad hoc - Client anomali ad hoc.
- Elenco punti di accesso non autorizzati - Come elencato tramite PI.

 Nota: se il WLC e l'access point autonomo sono gestiti dalla stessa PI, il WLC lo elenca automaticamente nell'elenco dei punti di accesso non autorizzati ignorati. Per abilitare questa funzione, non è necessaria alcuna configurazione aggiuntiva in WLC.

Fare clic su una voce specifica per ottenere i dettagli relativi a tale persona. Di seguito è riportato un esempio di server non autorizzati rilevato in una rete cablata:



The screenshot shows the Cisco WLC Monitor interface. The 'MONITOR' tab is selected. The left sidebar shows the navigation menu with 'Rogues' expanded and 'Malicious APs' selected. The main content area displays 'Rogue AP Detail' for a specific AP. Key fields are highlighted with red boxes: 'Is Rogue On Wired Network?' (Yes), 'Classification Change By' (Auto), and 'State' (Threat). Below the details is a table of APs that detected this Rogue.

Base Radio MAC	AP Name	SSID	Channel	Channel Width (Mhz)	Radio Type	Security Policy	Pre-Ambble	RSSI
00:27:e3:36:4d:a0	tiagoAPcb.98E1.3DEC	butterfly	1	20	802.11n2-4G	WPA2/FT	Long	-63

Dalla CLI:

```
<#root>
```

```
(Cisco Controller) >
```

```
show rogue ap summary
```

```

Rogue Detection Security Level..... custom
Rogue Pending Time..... 180 secs
Rogue on wire Auto-Contain..... Disabled
Rogue uses our SSID Auto-Contain..... Disabled
Valid client on rogue AP Auto-Contain..... Disabled
Rogue AP timeout..... 1200
Rogue Detection Report Interval..... 10
Rogue Detection Min Rssi..... -90
Rogue Detection Transient Interval..... 0
Rogue Detection Client Num Threshold..... 0
Validate rogue AP against AAA..... Enabled
Rogue AP AAA validation interval..... 0 secs
Total Rogues(AP+Ad-hoc) supported..... 600
Total Rogues classified..... 12

```

MAC Address	Class	State	#Det Aps	#Rogue Clients	#Highest RSSI det-Ap	#RSSI	#Channel
00:a3:8e:db:01:a0	Unclassified	Alert	1	0	00:27:e3:36:4d:a0	-16	13
00:a3:8e:db:01:a1	Unclassified	Alert	1	0	00:27:e3:36:4d:a0	-16	13
00:a3:8e:db:01:a2	Unclassified	Alert	1	0	00:27:e3:36:4d:a0	-16	13
00:a3:8e:db:01:b0	Malicious	Threat	2	1	00:27:e3:36:4d:a0	-27	40
00:a3:8e:db:01:b1	Unclassified	Alert	2	0	00:27:e3:36:4d:a0	-28	40
00:a3:8e:db:01:b2	Unclassified	Alert	2	0	00:27:e3:36:4d:a0	-28	40
50:2f:a8:a2:0a:60	Malicious	Threat	1	2	00:27:e3:36:4d:a0	-66	1
50:2f:a8:a2:0d:40	Unclassified	Alert	1	0	00:27:e3:36:4d:a0	-65	11
9c:97:26:61:d2:79	Unclassified	Alert	1	0	00:27:e3:36:4d:a0	-89	6
ac:22:05:ea:21:26	Unclassified	Alert	1	0	00:27:e3:36:4d:a0	-89	(1,5)
c4:e9:84:c1:c8:90	Unclassified	Alert	1	0	00:27:e3:36:4d:a0	-89	(6,2)
d4:28:d5:da:e0:d4	Unclassified	Alert	1	0	00:27:e3:36:4d:a0	-85	13

(Cisco Controller) >

```
show rogue ap detailed 50:2f:a8:a2:0a:60
```

```

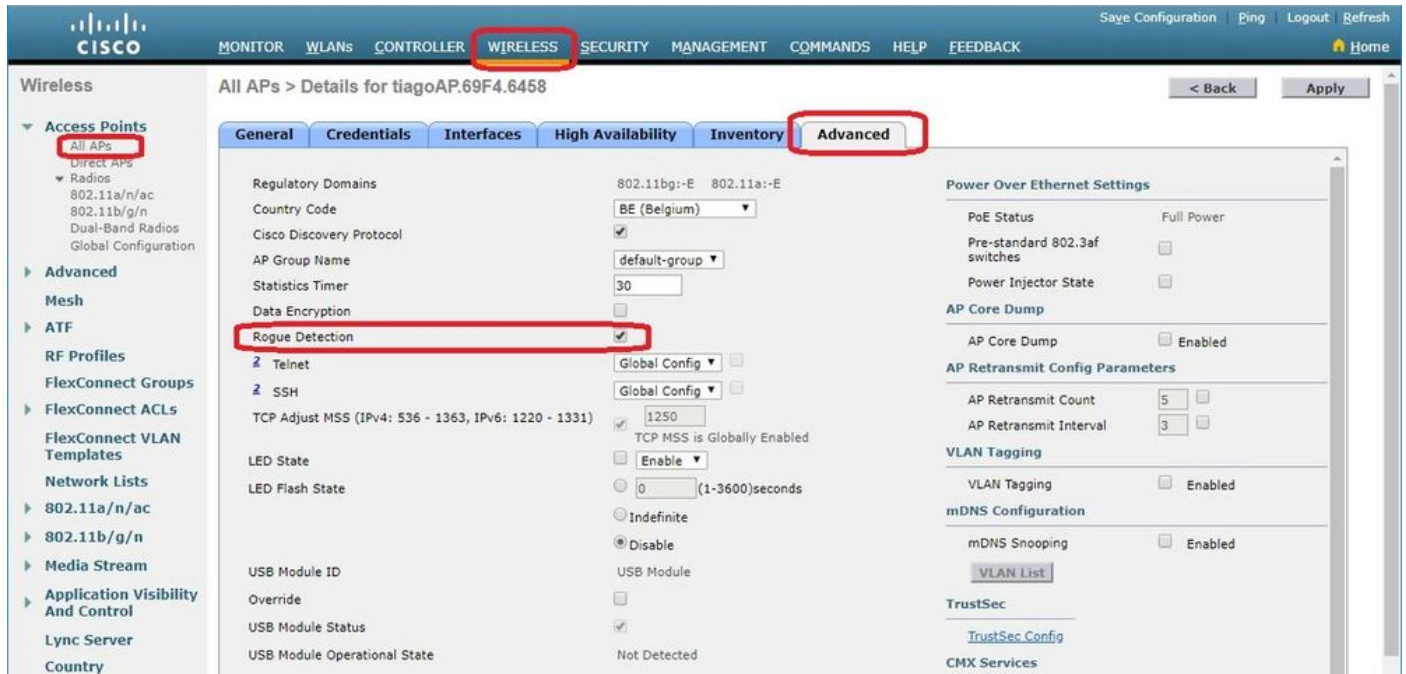
Rogue BSSID..... 50:2f:a8:a2:0a:60
Is Rogue on Wired Network..... Yes
Classification..... Malicious
Classification change by..... Auto
Manual Contained..... No
State..... Threat
State change by..... Auto
First Time Rogue was Reported..... Tue Jun 4 13:06:55 2019
Last Time Rogue was Reported..... Wed Jun 5 08:25:57 2019
Reported By
  AP 1
    MAC Address..... 00:27:e3:36:4d:a0
    Name..... tiagoAPcb.98E1.3DEC
    Radio Type..... 802.11n2.4G
    SSID..... buterfly
    Channel..... 1
    RSSI..... -64 dBm
    SNR..... 29 dB
    Security Policy..... WPA2/FT
    ShortPreamble..... Disabled
    Last reported by this AP..... Wed Jun 5 08:25:57 2019

```

Risoluzione dei problemi

Se Il Rogue Non Viene Rilevato

Verificare che il rilevamento rogue sia abilitato nell'access point. Dalla GUI:



Nella CLI:

```
<#root>
```

```
(Cisco Controller) >show ap config general tiagoAPcb.98E1.3DEC
```

```
Cisco AP Identifier..... 13
Cisco AP Name..... tiagoAPcb.98E1.3DEC
[...]
Administrative State ..... ADMIN_ENABLED
Operation State ..... REGISTERED
Mirroring Mode ..... Disabled
AP Mode ..... Local
Public Safety ..... Disabled
AP SubMode ..... Not Configured

Rogue Detection ..... Enabled

Remote AP Debug ..... Disabled
Logging trap severity level ..... informational
KPI not configured .....
Logging syslog facility ..... kern
S/W Version ..... 8.8.120.0
Boot Version ..... 1.1.2.4
[...]
Power Type/Mode..... PoE/Full Power
Number Of Slots..... 3
AP Model..... AIR-AP3802I-I-K9
AP Image..... AP3G3-K9W8-M
Cisco IOS Version..... 8.8.120.0
```

```
Reset Button..... Enabled
AP Serial Number..... FGL2114A4SU
[...]
```

È possibile abilitare il rilevamento dei server non autorizzati in un access point con questo comando:

```
<#root>
```

```
(Cisco Controller) >
```

```
config rogue detection enable ?
```

```
all          Applies the configuration to all connected APs.
```

```
<Cisco AP>  Enter the name of the Cisco AP.
```

Un access point in modalità locale esegue la scansione solo dei canali nazionali/DCA e dipende dalla configurazione. Se il dispositivo non autorizzato si trova su un altro canale, il controller non sarà in grado di identificare il dispositivo se sulla rete non sono presenti access point in modalità monitor. Utilizzare questo comando per verificare:

```
<#root>
```

```
(Cisco Controller) >
```

```
show advanced 802.11a monitor
```

```
Default 802.11a AP monitoring
```

```
802.11a Monitor Mode..... enable
```

```
802.11a Monitor Mode for Mesh AP Backhaul..... disable
```

```
802.11a Monitor Channels..... Country channels
```

```
802.11a RRM Neighbor Discover Type..... Transparent
```

```
802.11a RRM Neighbor RSSI Normalization..... Enabled
```

```
802.11a AP Coverage Interval..... 90 seconds
```

```
802.11a AP Load Interval..... 60 seconds
```

```
802.11a AP Monitor Measurement Interval..... 180 seconds
```

```
802.11a AP Neighbor Timeout Factor..... 20
```

```
802.11a AP Report Measurement Interval..... 180 seconds
```

- L'access point non autorizzato non trasmette l'SSID.
- Verificare che l'indirizzo MAC del punto di accesso non autorizzato non sia stato aggiunto all'elenco di indirizzi non autorizzati o sia stato consentito elencato tramite IP.
- I beacon provenienti dal punto di accesso non autorizzato non sono raggiungibili dal punto di accesso che ha rilevato i non autorizzati. È possibile verificare questa condizione

acquisendo i pacchetti con uno sniffer vicino al dispositivo di rilevamento dell'access point.

- Un access point in modalità locale può impiegare fino a 9 minuti per rilevare un server non autorizzato (3 cicli 180x3).
- I Cisco AP non sono in grado di rilevare i router danneggiati sulle frequenze, come il canale di sicurezza pubblica (4,9 Ghz).
- Gli access point Cisco non sono in grado di rilevare i router che funzionano su FHSS (Frequency Hopping Spread Spectrum).

Debug utili

```
<#root>
```

```
(Cisco Controller) >
```

```
debug client
```

```
(If rogue mac is known)
```

```
(Cisco Controller) >
```

```
debug client 50:2f:a8:a2:0a:60
```

```
(Cisco Controller) >*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 Found Rogue AP: 50:2f:a8:a2:0a:60
```

```
*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 New RSSI report from AP 00:27:e3:36:4d:a0 rssi -55
```

```
*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 Rogue SSID timestmap set to 1559724417. Detected by AP: 00:27:e3:36:4d:a0
```

```
*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 SYNC for Channel (new/old : 1/0) or channel width changed
```

```
*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 rg changed rssi prev -64, new -55
```

```
*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 Updated AP report 00:27:e3:36:4d:a0 rssi -55, channel 1
```

```
*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 Rogue detected by AP: 00:27:e3:36:4d:a0
```

```
*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 RadioType: 3 1radInfo->containSlotId = 2 Received from AP: 00:27:e3:36:4d:a0
```

```
*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 Rogue before Rule Classification : Class malicious
```

```
*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 Rogue doesnt qualify for rule classification : Class malicious
```

```
*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 Manual Contained Flag = 0, trustlevel = 7
```

```
*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 ssidLen = 8 min = 8 50:2f:a8:a2:0a:60
```

```
*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 This rogue does not use my ssid. Rogue ssid=buterfly
```

```
*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 Rogue AP: 50:2f:a8:a2:0a:60 autocontain = 2 Monitored
```

```
*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 Checking Impersonation source 50:2f:a8:a2:0a:60
```

```
*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 Known AP 0 mfp global 0 AP Auth Global 0 mfp Impersonation
```

```
*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 Rogue Client ssid: buterfly
```

```
*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 Rogue Client ssid: buterfly
```

<#root>

(Cisco Controller) >

debug dot11 rogue enable

(Cisco Controller) >*emWeb: Jun 05 08:39:46.828:

Debugging session started on Jun 05 08:39:46.828 for WLC AIR-CT3504-K9 Version :8.8.120.0 SN :FCW22

*iappSocketTask: Jun 05 08:39:57.104: 00:27:e3:36:4d:a0 Posting Rogue AP Iapp Report from AP for proces

*apfRogueTask_2: Jun 05 08:39:57.104: 00:27:e3:36:4d:a0 fakeAp check: slot=0, entryIndex=0, (Radio_upTi

*apfRogueTask_2: Jun 05 08:39:57.105: 00:27:e3:36:4d:a0 entries 5 slotId 0 bssid b0:72:bf:93:e0:d7 src

*apfRogueTask_2: Jun 05 08:39:57.105: 00:27:e3:36:4d:a0 entries 5 slotId 0 bssid 50:2f:a8:a2:0a:60 src

*apfRogueTask_2: Jun 05 08:39:57.105: 00:27:e3:36:4d:a0 entries 5 slotId 0 bssid 00:a3:8e:db:01:a1 src

*apfRogueTask_2: Jun 05 08:39:57.105: 00:27:e3:36:4d:a0 entries 5 slotId 0 bssid 00:a3:8e:db:01:b0 src

*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 New RSSI report from AP 00:27:e3:36:4d:a0 rssi

*apfRogueTask_2: Jun 05 08:39:57.105: 00:27:e3:36:4d:a0 entries 5 slotId 0 bssid 00:a3:8e:db:01:b2 src

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 Found Rogue AP: 00:a3:8e:db:01:a1 on slot 0

*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 Rogue SSID timestmap expired. last update at 0

*apfRogueTask_2: Jun 05 08:39:57.105: 00:27:e3:36:4d:a0 fakeAp check: knownApCount=0, totalNumOfRogueE

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 New RSSI report from AP 00:27:e3:36:4d:a0 rssi

*apfRogueTask_2: Jun 05 08:39:57.105: 00:27:e3:36:4d:a0 fakeAp check: avgNumOfRogues[0]/10=4, rogueAla

*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 SYNC for Channel (new/old : 40/0) or channel w

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 Rogue SSID timestmap expired. last update at 0

*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 rg changed rssi prev -28, new -28

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 SYNC for Channel (new/old : 13/0) or channel w

*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 Updated AP report 00:27:e3:36:4d:a0 rssi -28,

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 Updated AP report 00:27:e3:36:4d:a0 rssi -16,

*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 RadioType: 3 lradInfo->containSlotId = 1 Receiv

*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 Rogue before Rule Classification : Class unclas

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Created rogue client table for Rogue AP at 0xff

*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 Rogue is Rule candidate for : Class Change by

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Added Rogue AP: b0:72:bf:93:e0:d7

*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 Applying Rogue rule to this MAC

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Looking for Rogue b0:72:bf:93:e0:d7 in known AP

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Rogue AP b0:72:bf:93:e0:d7 is not found either

*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 Rogue After Rule Classification : Class unclass

*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 Manual Contained Flag = 0, trustlevel = 2

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Scheduled pending Time 184 and expiry time 1200

*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 ssidLen = 0 min = 0 00:a3:8e:db:01:b2

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Change state from 0 to 1 for rogue AP b0:72:bf:

*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 This rogue does not use my ssid. Rogue ssid=

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 rg change state Rogue AP: b0:72:bf:93:e0:d7

*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 Rogue AP: 00:a3:8e:db:01:b2 autocontain = 2 Mo

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 Rogue detected by AP: 00:27:e3:36:4d:a0

*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 Checking Impersonation source 00:a3:8e:db:01:b2

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 RadioType: 3 lradInfo->containSlotId = 2 Receiv

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 New RSSI report from AP 00:27:e3:36:4d:a0 rssi

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 Rogue is Rule candidate for : Class Change by

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Send Rogue Info Notificaiton for AP report 00:

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 Applying Rogue rule to this MAC

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Rogue SSID timestmap set to 1559723997. Detecti

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 rg send new rssi -59

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 Rogue After Rule Classification : Class unclass

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Updated AP report 00:27:e3:36:4d:a0 rssi -59,

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 Manual Contained Flag = 0, trustlevel = 2

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Rogue detected by AP: 00:27:e3:36:4d:a0

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 ssidLen = 0 min = 0 00:a3:8e:db:01:a1

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 RadioType: 3 lradInfo->containSlotId = 2 Receiv

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 This rogue does not use my ssid. Rogue ssid=

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Rogue before Rule Classification : Class unconf

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 Rogue AP: 00:a3:8e:db:01:a1 autocontain = 2 Mo

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Rogue state is pending or lrad, cannot apply ro

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Rogue doesnt qualify for rule classification :

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 Checking Impersonation source 00:a3:8e:db:01:a1

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Manual Contained Flag = 0, trustlevel = 1

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 Known AP 0 mfp global 0 AP Auth Global 0 mfp Im

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Checking Impersonation source b0:72:bf:93:e0:d7

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Known AP 0 mfp global 0 AP Auth Global 0 mfp Im

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0 Found Rogue AP: 00:a3:8e:db:01:b0 on slot 0

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 rg new Rogue AP: b0:72:bf:93:e0:d7

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0 New RSSI report from AP 00:27:e3:36:4d:a0 rssi

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0 Rogue SSID timestmap set to 1559723997. Detecti

*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 New RSSI report from AP 00:27:e3:36:4d:a0 rssi

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0 SYNC for Channel (new/old : 40/0) or channel w

*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 Rogue SSID timestmap set to 1559723997. Detecti

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0 rg changed rssi prev -28, new -26

*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 SYNC for Channel (new/old : 1/0) or channel wi

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0 Updated AP report 00:27:e3:36:4d:a0 rssi -26,

*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 rg changed rssi prev -65, new -63

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0 Rogue detected by AP: 00:27:e3:36:4d:a0

*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 Updated AP report 00:27:e3:36:4d:a0 rssi -63,

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0 RadioType: 3 lradInfo->containSlotId = 1 Receiv

*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 Rogue detected by AP:00:27:e3:36:4d:a0

*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 RadioType: 3 lradInfo->containSlotId = 2 Receiv

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0 Manual Contained Flag = 0, trustlevel = 7

*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 Rogue before Rule Classification : Class malicious

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0 ssidLen = 8 min = 8 00:a3:8e:db:01:b0

*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 Manual Contained Flag = 0, trustlevel = 7

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0 This rogue does not use my ssid. Rogue ssid=blizzard

*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 ssidLen = 8 min = 8 50:2f:a8:a2:0a:60

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0 Rogue AP: 00:a3:8e:db:01:b0 autocontain = 2 Months

*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 This rogue does not use my ssid. Rogue ssid=butterfly

*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 Rogue AP: 50:2f:a8:a2:0a:60 autocontain = 2 Months

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0 Known AP 0 mfp global 0 AP Auth Global 0 mfp Impersonation 0

*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 Checking Impersonation source 50:2f:a8:a2:0a:60

*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 Known AP 0 mfp global 0 AP Auth Global 0 mfp Impersonation 0

*apfRogueTask_3: Jun 05 08:39:57.105: a4:c3:f0:cf:db:18 APF processing Rogue Client: on slot 0

*apfRogueTask_3: Jun 05 08:39:57.105: a4:c3:f0:cf:db:18 Rogue Client IPv6 addr: Not known

*apfRogueTask_2: Jun 05 08:39:57.105: b4:82:fe:54:b3:14 APF processing Rogue Client: on slot 0

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0 Rogue Client ssid: blizzard

*apfRogueTask_2: Jun 05 08:39:57.105: b4:82:fe:54:b3:14 Rogue Client IPv6 addr: Not known

*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 Rogue Client ssid: butterfly

*apfRogueTask_3: Jun 05 08:39:57.105: a4:c3:f0:cf:db:18 New AP report 00:27:e3:36:4d:a0 rssi -37, snr -37

*apfRogueTask_3: Jun 05 08:39:57.105: a4:c3:f0:cf:db:18 rgc change from -38 RSSI -37

*apfRogueTask_2: Jun 05 08:39:57.105: b4:82:fe:54:b3:14 rgc change from -39 RSSI -39

*apfRogueTask_3: Jun 05 08:39:57.105: a4:c3:f0:cf:db:18 Updated AP report 00:27:e3:36:4d:a0 rssi -37, snr -37

*apfRogueTask_2: Jun 05 08:39:57.105: b4:82:fe:54:b3:14 Updated AP report 00:27:e3:36:4d:a0 rssi -39, snr -39

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 APF processing Rogue Client: on slot 0

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Rogue Client IPv6 addr: Not known

*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 Rogue Client ssid: butterfly

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 New AP report 00:27:e3:36:4d:a0 rssi -62, snr -62

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 rgc change from -61 RSSI -62

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Updated AP report 00:27:e3:36:4d:a0 rssi -62, snr -62

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Looking for Rogue b0:72:bf:93:e0:d7 in known AP table

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Rogue AP b0:72:bf:93:e0:d7 is not found either in known AP table

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Change state from 1 to 2 for rogue AP b0:72:bf:93:e0:d7

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 rg change state Rogue AP: b0:72:bf:93:e0:d7

*apfRogueTask_2: Jun 05 08:39:57.106: b0:72:bf:93:e0:d7 rg change state Rogue AP: b0:72:bf:93:e0:d7

*apfRogueTask_2: Jun 05 08:39:57.106: b0:72:bf:93:e0:d7 Deleting Rogue AP: b0:72:bf:93:e0:d7

*apfRogueTask_2: Jun 05 08:39:57.106: b0:72:bf:93:e0:d7 Freed rogue client table for Rogue AP at 0xffff0000

*apfRogueTask_2: Jun 05 08:39:57.106: b0:72:bf:93:e0:d7 rg delete for Rogue AP: b0:72:bf:93:e0:d7

Registri Trap Previsti

Una volta che un rogue è stato rilevato/rimosso dall'elenco:

0	Mer Giu 5 09:01:57 2019	Rogue client: b4:c0:f5:2b:4f:90 è rilevato da 1 punto di accesso Rogue Client Bssid: a6:b1:e9:f0:e8:41, Stato: Alert, Ultimo rilevamento punto di accesso: 00:27:e3:36:4d:a0 Rogue Client gateway mac 00:00:00:02:02:02.
1	Mer Giu 5 09:00:39 2019	Rogue AP : 9c:97:26:61:d2:79 rimosso da Base Radio MAC : 00:27:e3:36:4d:a0 Interfaccia no:0(802.11n(2,4 GHz))
2	Mer Giu 5 08:53:39 2019	Rogue AP : 7c:b7:33:c0:51:14 rimosso da MAC radio base : 00:27:e3:36:4d:a0 Interfaccia no:0(802.11n(2,4 GHz))
3	Mer Giu 5 08:52:27 2019	Rogue client: fc:3f:7c:5f:b1:1b è rilevato da 1 punto di accesso Rogue Client Bssid: 50:2f:a8:a2:0a:60, Stato: Alert, Ultimo rilevamento punto di accesso: 00:27:e3:36:4d:a0 Rogue Client gateway mac 00:26:44:73:c5:1d.
4	Mer Giu 5 08:52:17 2019	Rogue AP : d4:28:d5:da:e0:d4 rimosso da MAC radio base : 00:27:e3:36:4d:a0 Interfaccia no:0(802.11n(2,4 GHz))

Consigli

1. Configurare la scansione dei canali su tutti i canali se si sospetta la presenza di potenziali anomalie nella rete.
2. Il numero e la posizione dei punti di accesso per il rilevamento di anomalie possono variare da uno a piano a uno per edificio e dipendono dalla configurazione della rete cablata. È consigliabile disporre di almeno un access point anomalo in ogni piano di un edificio. Poiché un access point con rilevamento anomalo richiede un trunk per tutti i domini di trasmissione di rete di livello 2 che devono essere monitorati, il posizionamento dipende dal layout logico della rete.

Se il server non autorizzato non è classificato

Verificare che le regole non valide siano configurate correttamente.

Debug utili

```
<#root>
```

```
(Cisco Controller) >
```

```
debug dot11 rogue rule enable
```

```
(Cisco Controller) >*emWeb: Jun 05 09:12:27.095:
```

```
Debugging session started on Jun 05 09:12:27.095 for WLC AIR-CT3504-K9 Version :8.8.120.0 SN :FCW2245M0
```

(Cisco Controller) >

```
*apfRogueTask_1: Jun 05 09:12:57.135: 00:a3:8e:db:01:a0 Rogue Rule Classify Params: rssi=-16, maxRssiLr
*apfRogueTask_3: Jun 05 09:12:57.135: 00:a3:8e:db:01:a1 Rogue Rule Classify Params: rssi=-15, maxRssiLr

*apfRogueTask_1: Jun 05 09:12:57.135: ac:22:05:ea:21:26 Rogue Rule Classify Params: rssi=-89, maxRssiLr

*apfRogueTask_1: Jun 05 09:13:27.135: ac:22:05:ea:21:26 Rogue Rule Classify Params: rssi=-89, maxRssiLr
*apfRogueTask_3: Jun 05 09:13:27.135: 50:2f:a8:a2:0d:40 Rogue Rule Classify Params: rssi=-62, maxRssiLr
*apfRogueTask_3: Jun 05 09:13:27.135: 50:2f:a8:a2:0d:40
```

Rogue Classification:malicious, RuleName:TestRule, Rogue State:Containment Pending

```
*apfRogueTask_3: Jun 05 09:13:27.136: 00:a3:8e:db:01:a1 Rogue Rule Classify Params: rssi=-15, maxRssiLr

*apfRogueTask_1: Jun 05 09:13:57.136: 00:a3:8e:db:01:a0 Rogue Rule Classify Params: rssi=-16, maxRssiLr
*apfRogueTask_3: Jun 05 09:13:57.136: 50:2f:a8:a2:0d:40 Rogue Classification:malicious, RuleName:TestRu

*apfRogueTask_3: Jun 05 09:13:57.136: 00:a3:8e:db:01:a1 Rogue Rule Classify Params: rssi=-15, maxRssiLr
```

Consigli

Se si conoscono voci non autorizzate, aggiungerle all'elenco descrittivo o abilitare la convalida con AAA e assicurarsi che le voci client conosciute siano presenti nel database di autenticazione, autorizzazione e accounting (AAA).

RLDP non individua i server non autorizzati

- Se il server non autorizzato si trova nel canale DFS, RLDP non funzionerà.
- Il protocollo RLDP funziona solo se la WLAN non autorizzata è aperta e se il protocollo DHCP è disponibile.
- Se il punto di accesso in modalità locale serve il client nel canale DFS, non partecipa al processo RLDP.
- Il protocollo RLDP non è supportato sui punti di accesso serie 1800i, 1810 OEAP, 1810W, 1815, 1830, 1850, 2800 e 3800.

Debug utili

<#root>

(Cisco Controller) >

```
debug dot11 rldp enable
```

!--- RLDP not available when AP used to contain only has invalid channel for the AP country code

```
*apfRLDP: Jun 05 12:24:41.291: 50:2f:a8:a2:0a:61 Received request to detect Rogue
*apfRLDP: Jun 05 12:24:41.291: 50:2f:a8:a2:0a:61 Entering apfFindClosestLrad
*apfRLDP: Jun 05 12:24:41.292: Rogue detected slot :0 Rogue contains SlotId :2
*apfRLDP: Jun 05 12:24:41.292: 50:2f:a8:a2:0a:61
```

Invalid channel 1 for the country IL for AP 00:27:e3:36:4d:a0

*apfRLDP: Jun 05 12:24:41.292: 50:2f:a8:a2:0a:61 Cannot find any AP to perform RLDP operation
*apfRLDP: Jun 05 12:24:41.292: 50:2f:a8:a2:0a:61 Exiting apfFindClosestLrad
*apfRLDP: Jun 05 12:24:41.292: Waiting for ARLDP request

!--- ROGUE detected on DFS channel

*apfRLDP: Jun 05 12:43:16.659: 50:2f:a8:a2:0d:4e Received request to detect Rogue
*apfRLDP: Jun 05 12:43:16.659: 50:2f:a8:a2:0d:4e Entering apfFindClosestLrad
*apfRLDP: Jun 05 12:43:16.660: Rogue detected slot :1 Rogue contains SlotId :1
*apfRLDP: Jun 05 12:43:16.660: 50:2f:a8:a2:0d:4e

Our AP 00:27:e3:36:4d:a0 detected this rogue on a DFS Channel 100

*apfRLDP: Jun 05 12:43:16.660: 50:2f:a8:a2:0d:4e Cannot find any AP to perform RLDP operation
*apfRLDP: Jun 05 12:43:16.660: 50:2f:a8:a2:0d:4e Exiting apfFindClosestLrad
*apfRLDP: Jun 05 12:43:16.660: Waiting for ARLDP request

!--- RLDP is not supported on AP model 1800i, 1810 OEAP, 1810W, 1815, 1830, 1850, 2800, and 3800 Series

*apfRLDP: Jun 05 12:52:41.980: 9e:97:26:a2:a1:1a Received request to detect Rogue
*apfRLDP: Jun 05 12:52:41.980: 9e:97:26:a2:a1:1a Entering apfFindClosestLrad
*apfRLDP: Jun 05 12:52:41.980: 9e:97:26:a2:a1:1a

Skipping RLDP on AP 94:d4:69:f5:f7:e0 AP Model: AIR-AP1852I-E-K9

*apfRLDP: Jun 05 12:52:41.980: 9e:97:26:a2:a1:1a Cannot find any AP to perform RLDP operation
*apfRLDP: Jun 05 12:52:41.980: 9e:97:26:a2:a1:1a Exiting apfFindClosestLrad
*apfRLDP: Jun 05 12:52:41.980: Waiting for ARLDP request

!--- Association TO ROGUE AP

*apfRLDP: Jun 05 15:02:49.602: 50:2f:a8:a2:0a:61 Received request to detect Rogue
*apfRLDP: Jun 05 15:02:49.602: 50:2f:a8:a2:0a:61 Entering apfFindClosestLrad
*apfRLDP: Jun 05 15:02:49.602: 50:2f:a8:a2:0a:61 Skipping RLDP on AP 94:d4:69:f5:f7:e0 AP Model: AIR-AP
*apfRLDP: Jun 05 15:02:49.602: Rogue detected slot :0 Rogue contains SlotId :0
*apfRLDP: Jun 05 15:02:49.602: 50:2f:a8:a2:0a:61

Monitor Mode AP found b4:de:31:a4:e0:30 with RSSI -61

*apfRLDP: Jun 05 15:02:49.602: 50:2f:a8:a2:0a:61 found closest monitor AP b4:de:31:a4:e0:30 slot = 0, c
*apfRLDP: Jun 05 15:02:49.602: 50:2f:a8:a2:0a:61 Exiting apfFindClosestLrad
*apfRLDP: Jun 05 15:02:49.602: 50:2f:a8:a2:0a:61 Found RAD: 0xffd682b5b8, slotId = 0, Type=1
*apfRLDP: Jun 05 15:02:50.102: 50:2f:a8:a2:0a:61 AP b4:de:31:a4:e0:30 Client b4:de:31:a4:e0:31 Slot = 0
*apfRLDP: Jun 05 15:02:50.102: 50:2f:a8:a2:0a:61 WARNING!!!! mscb already exists!
*apfRLDP: Jun 05 15:02:50.102: b4:de:31:a4:e0:31 In rldpSendAddMobile:724 setting Central switched to T
*apfRLDP: Jun 05 15:02:50.302: 50:2f:a8:a2:0a:61

rldp started association, attempt 1

*apfRLDP: Jun 05 15:02:55.346: 50:2f:a8:a2:0a:61 RLDP could not finish the association in time. RLDP St
*apfRLDP: Jun 05 15:02:55.346: 50:2f:a8:a2:0a:61 rldp started association, attempt 2
*apfRLDP: Jun 05 15:03:00.390: 50:2f:a8:a2:0a:61 RLDP could not finish the association in time. RLDP St
*apfRLDP: Jun 05 15:03:00.390: 50:2f:a8:a2:0a:61 rldp started association, attempt 3
*apfOpenDtSocket: Jun 05 15:03:00.608: apfRoguePreamble = 0 mobile b4:de:31:a4:e0:31.
*apfOpenDtSocket: Jun 05 15:03:00.808:

50:2f:a8:a2:0a:61 RLDLP state RLDLP_ASSOC_DONE

(3).

*apfRLDP: Jun 05 15:03:00.870: 50:2f:a8:a2:0a:61

Successfully associated with rogue: 50:2F:A8:A2:0A:61

!--- Attempt to get ip from ROGUE

*apfRLDP: Jun 05 15:03:00.870: 50:2f:a8:a2:0a:61

Starting dhcp

*apfRLDP: Jun 05 15:03:00.870: 50:2f:a8:a2:0a:61

Initializing RLDLP DHCP for rogue 50:2f:a8:a2:0a:61

*apfRLDP: Jun 05 15:03:00.870: 50:2f:a8:a2:0a:61 RLDLP DHCPSTATE_INIT for rogue 50:2f:a8:a2:0a:61

*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31 BOOTP[rldp] op: REQUEST

*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31 htype: Ethernet

*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31 hlen: 6

*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31 hops: 1

*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31 xid: 0x3da1f13

*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31 secs: 0

*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31 flags: 0x0

*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31 hw_addr: B4:DE:31:A4:E0:31

*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31 client IP: 0.0.0.0

*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31 my IP: 0.0.0.0

*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31 server IP: 0.0.0.0

*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31 gateway IP: 0.0.0.0

*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31 options:

*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31 DHCP message: 1 DISCOVER

*apfRLDP: Jun 05 15:03:00.870: DHCP option: 39/57.2: (2)

*apfRLDP: Jun 05 15:03:00.870: [0000] 02 40

*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31 host name: RLDLP

*apfRLDP: Jun 05 15:03:00.870: 50:2f:a8:a2:0a:61 Sending DHCP packet through rogue AP 50:2f:a8:a2:0a:61

*apfRLDP: Jun 05 15:03:00.870: 50:2f:a8:a2:0a:61 RLDLP DHCP SELECTING for rogue 50:2f:a8:a2:0a:61

*apfRLDP: Jun 05 15:03:10.877: 50:2f:a8:a2:0a:61 Initializing RLDLP DHCP for rogue 50:2f:a8:a2:0a:61

*apfRLDP: Jun 05 15:03:10.877: 50:2f:a8:a2:0a:61 RLDLP DHCPSTATE_INIT for rogue 50:2f:a8:a2:0a:61

*apfRLDP: Jun 05 15:03:10.877: b4:de:31:a4:e0:31 BOOTP[rldp] op: REQUEST

*apfRLDP: Jun 05 15:03:10.877: b4:de:31:a4:e0:31 htype: Ethernet

*apfRLDP: Jun 05 15:03:10.877: b4:de:31:a4:e0:31 hlen: 6


```
*apfRLDP: Jun 05 15:03:10.877: b4:de:31:a4:e0:31      hops: 1
*apfRLDP: Jun 05 15:03:10.877: b4:de:31:a4:e0:31      xid: 0x3da1f13
*apfRLDP: Jun 05 15:03:10.877: b4:de:31:a4:e0:31      secs: 0
*apfRLDP: Jun 05 15:03:10.877: b4:de:31:a4:e0:31      flags: 0x0
*apfRLDP: Jun 05 15:03:10.877: b4:de:31:a4:e0:31      hw_addr: B4:DE:31:A4:E0:31
*apfRLDP: Jun 05 15:03:10.877: b4:de:31:a4:e0:31      client IP: 0.0.0.0
*apfRLDP: Jun 05 15:03:10.877: b4:de:31:a4:e0:31      my IP: 0.0.0.0
*apfRLDP: Jun 05 15:03:10.878: b4:de:31:a4:e0:31      server IP: 0.0.0.0
*apfRLDP: Jun 05 15:03:10.878: b4:de:31:a4:e0:31      gateway IP: 0.0.0.0
*apfRLDP: Jun 05 15:03:10.878: b4:de:31:a4:e0:31      options:
*apfRLDP: Jun 05 15:03:10.878: b4:de:31:a4:e0:31      DHCP message: 1 DISCOVER
*apfRLDP: Jun 05 15:03:10.878: DHCP option: 39/57.2: (2)
*apfRLDP: Jun 05 15:03:10.878:      [0000] 02 40
*apfRLDP: Jun 05 15:03:10.878: b4:de:31:a4:e0:31      host name: RLDP
*apfRLDP: Jun 05 15:03:10.878: 50:2f:a8:a2:0a:61 Sending DHCP packet through rogue AP 50:2f:a8:a2:0a:61
*apfRLDP: Jun 05 15:03:10.878: 50:2f:a8:a2:0a:61 RLDP DHCP SELECTING for rogue 50:2f:a8:a2:0a:61
*apfRLDP: Jun 05 15:03:20.885: 50:2f:a8:a2:0a:61 Initializing RLDP DHCP for rogue 50:2f:a8:a2:0a:61
*apfRLDP: Jun 05 15:03:20.885: 50:2f:a8:a2:0a:61 RLDP DHCPSTATE_INIT for rogue 50:2f:a8:a2:0a:61
*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31 BOOTP[rldp] op: REQUEST
*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31      htype: Ethernet
*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31      hlen: 6
*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31      hops: 1
*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31      xid: 0x3da1f13
*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31      secs: 0
*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31      flags: 0x0
*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31      hw_addr: B4:DE:31:A4:E0:31
*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31      client IP: 0.0.0.0
*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31      my IP: 0.0.0.0
*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31      server IP: 0.0.0.0
*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31      gateway IP: 0.0.0.0
*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31      options:
*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31      DHCP message: 1 DISCOVER
*apfRLDP: Jun 05 15:03:20.885: DHCP option: 39/57.2: (2)
```

```
*apfRLDP: Jun 05 15:03:20.885: [0000] 02 40
*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31 host name: RLDP
*apfRLDP: Jun 05 15:03:20.885: 50:2f:a8:a2:0a:61 Sending DHCP packet through rogue AP 50:2f:a8:a2:0a:61
!--- RLDP DHCP fails as there is no DHCP server providing IP address
*apfRLDP: Jun 05 15:03:20.885: 50:2f:a8:a2:0a:61 RLDP DHCP FAILED state for rogue 50:2f:a8:a2:0a:61
*apfRLDP: Jun 05 15:03:20.885: 50:2f:a8:a2:0a:61 DHCP failed
*apfRLDP: Jun 05 15:03:20.885: Waiting for ARLDP request
```

Consigli

1. Avviare manualmente RLDP in caso di voci potenzialmente anomale.
2. Pianificare periodicamente RLDP.
3. I punti di accesso RLDP possono essere distribuiti sui punti di accesso in modalità locale o monitor. Per le implementazioni più scalabili ed eliminare l'impatto sul servizio client, il protocollo RLDP deve essere implementato sui punti di accesso in modalità di monitoraggio, quando possibile. Tuttavia, questa raccomandazione richiede la distribuzione di un access point in modalità monitor con un rapporto tipico di 1 access point in modalità monitor ogni 5 access point in modalità locale. Per questa attività è possibile utilizzare anche i punti di accesso in modalità di monitoraggio WIPS adattivo.

Punto di accesso rilevamento server non autorizzati

Le voci non autorizzate in un rilevatore di anomalie possono essere visualizzate con questo comando nella console AP. Per le reti cablate, l'indicatore passa allo stato impostato.

```
<#root>
```

```
tiagoAP.6d09.eff0#
```

```
show capwap rm rogue detecto
```

```
r
```

```
LWAPP Rogue Detector Mode
```

```
Current Rogue Table:
```

```
Rogue hindex = 0: MAC 502f.a8a2.0a61,
```

```
flag = 0
```

```
, unusedCount = 1
```

```
Rogue hindex = 0: MAC 502f.a8a2.0a60,
```

```
flag = 0
```

```
, unusedCount = 1
```

```
Rogue hindex = 7: MAC 502f.a8a2.0d41,
```

```
flag = 0
```

```
, unusedCount = 1
  Rogue hindex = 7: MAC 502f.a8a2.0d40,
```

```
flag = 0
```

```
, unusedCount = 1
```

```
!--- once rogue is detected on wire, the flag is set to 1
```

Comandi di debug utili in una console AP

```
<#root>
```

```
Rogue_Detector#
```

```
debug capwap rm rogue detector
```

```
*Jun 05 08:37:59.747: ROGUE_DET: Received a rogue table update of length 170
*Jun 05 08:37:59.747: ROGUE_DET: Got wired mac 0023.ebdc.1ac4
*Jun 05 08:37:59.747: ROGUE_DET: Got wired mac 0023.ebdc.1ac5
*Jun 05 08:37:59.747: ROGUE_DET: Got wired mac 0023.ebdc.1aca
*Jun 05 08:37:59.747: ROGUE_DET: Got wired mac 0023.ebdc.1acb
*Jun 05 08:37:59.747: ROGUE_DET: Got wired mac 0023.ebdc.1acc
*Jun 05 08:37:59.747: ROGUE_DET: Got wired mac 0023.ebdc.1acd
*Jun 05 08:37:59.747: ROGUE_DET: Got wired mac 0023.ebdc.1acf
*Jun 05 08:37:59.747: ROGUE_DET: Got wired mac 0024.1431.e9ef
*Jun 05 08:37:59.747: ROGUE_DET: Got wired mac 0024.148a.ca2b
*Jun 05 08:37:59.748: ROGUE_DET: Got wired mac 0024.148a.ca2d
*Jun 05 08:37:59.748: ROGUE_DET: Got wired mac 0024.148a.ca2f
*Jun 05 08:37:59.748: ROGUE_DET: Got wired mac 0024.14e8.3570
*Jun 05 08:37:59.748: ROGUE_DET: Got wired mac 0024.14e8.3574
*Jun 05 08:37:59.748: ROGUE_DET: Got wired mac 0024.14e8.357b
*Jun 05 08:37:59.748: ROGUE_DET: Got wired mac 0024.14e8.357c
*Jun 05 08:37:59.749: ROGUE_DET: Got wired mac 0024.14e8.357d
*Jun 05 08:37:59.749: ROGUE_DET: Got wired mac 0024.14e8.357f
*Jun 05 08:37:59.749: ROGUE_DET: Got wired mac 0024.14e8.3dcd
*Jun 05 08:37:59.749: ROGUE_DET: Got wired mac 0024.14e8.3ff0
*Jun 05 08:37:59.749: ROGUE_DET: Got wired mac 0024.14e8.3ff2
*Jun 05 08:37:59.774: ROGUE_DET: Got wired mac 0040.96b9.4aec
*Jun 05 08:37:59.774: ROGUE_DET: Got wired mac 0040.96b9.4b77
*Jun 05 08:37:59.774: ROGUE_DET: Flushing rogue entry 0040.96b9.4794
*Jun 05 08:37:59.774: ROGUE_DET: Flushing rogue entry 0022.0c97.af80
*Jun 05 08:37:59.775: ROGUE_DET: Flushing rogue entry 0024.9789.5710
*Jun 05 08:38:19.325: ROGUE_DET: Got ARP src 001d.a1cc.0e9e
*Jun 05 08:38:19.325: ROGUE_DET: Got wired mac 001d.a1cc.0e9e
*Jun 05 08:39:19.323: ROGUE_DET: Got ARP src 001d.a1cc.0e9e
*Jun 05 08:39:19.324: ROGUE_DET: Got wired mac 001d.a1cc.0e9e
```

Controllo di elementi non autorizzati

Debug previsti

<#root>

```
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Updated AP report b4:de:31:a4:e0:30 rssi -33, s
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Looking for Rogue 00:a3:8e:db:01:b0 in known AP
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Rogue AP 00:a3:8e:db:01:b0 is not found either
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Rogue in same state as before : 6 ContainmentLev

*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Rogue detected by AP: b4:de:31:a4:e0:30
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 RadioType: 2 lradInfo->containSlotId = 1 Receiv

*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Rogue before Rule Classification :

Class malicious, Change by Auto State Contained Change by Auto

*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Rogue doesnt qualify for rule classification :
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Manual Contained Flag = 0, trustlevel = 6
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0

Rogue AP: 00:a3:8e:db:01:b0 autocontain = 1 Mode = 6

*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 apfRogueMode : 6 apfRogueContainmentLevel : 4 1

*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Trying Containment on 1 band for rogue
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Skipping xor radio for 1 band and cont slotid 1
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Found 0 channels to try containment for rogue
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Trying Containment on 2 band for rogue
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Rogue detected on detected slot 0 contains slot
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Found 1 channels to try containment for rogue
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 RSSI SORTED AP MAC 00:27:e3:36:4d:a0 RSSI = -28
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 RSSI SORTED AP MAC 00:27:e3:36:4d:a0 RSSI = -31
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 RSSI SORTED AP MAC b4:de:31:a4:e0:30 RSSI = -33
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Detecting AP MAC 00:27:e3:36:4d:a0 RSSI = -28 t
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Detecting AP MAC 00:27:e3:36:4d:a0 RSSI = -31 t
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Detecting AP MAC b4:de:31:a4:e0:30 RSSI = -33 t
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Rogue already contained by AP 00:27:e3:36:4d:a0
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Rogue already contained by AP 00:27:e3:36:4d:a0
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Rogue already contained by AP b4:de:31:a4:e0:30
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0

Contains rogue with 3 container AP(s).Requested containment level : 4

*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Checking Impersonation source 00:a3:8e:db:01:b0
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Known AP 0 mfp global 0 AP Auth Global 0 mfp Im
```

Consigli

1. L'access point in modalità locale/Flex-Connect può contenere 3 dispositivi alla volta per radio e l'access point in modalità monitor può contenere 6 dispositivi per radio. Di conseguenza, accertarsi che l'access point non contenga già il numero massimo di dispositivi consentiti. In questo scenario, il client si trova in uno stato di contenimento in sospeso.
2. Verificare le regole di contenimento automatico.

Conclusioni

Il rilevamento e il contenimento dei problemi all'interno della soluzione di controller centralizzato Cisco è il metodo più efficace e meno intrusivo del settore. La flessibilità fornita all'amministratore di rete consente di adattare il sistema a qualsiasi esigenza di rete.

Informazioni correlate

- [Guida alla configurazione di Cisco Wireless Controller, release 8.8 - Rogue Management](#)
- [Best practice per la configurazione di Cisco Wireless LAN Controller \(WLC\)](#)
- [Guida alla distribuzione di WLC 3504 release 8.5](#)
- [Guida all'installazione di Cisco 5520 Wireless LAN Controller](#)
- [Note sulla versione di Cisco Wireless Controller e Lightweight Access Point, Cisco Wireless release 8.8.120.0](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).