

# MSE - Guida alla distribuzione di una soluzione di mobilità sensibile al contesto

## Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Convenzioni](#)

[Premesse](#)

[Sezione 1: Panoramica della soluzione](#)

[Terminologia](#)

[Informazioni generali sulle tecnologie](#)

[RSSI \(Indicazione della forza del segnale ricevuto\)](#)

[TDOA \(Differenza tempo di arrivo\)](#)

[Tag RFID attivi](#)

[Sezione 2: Pianificazione e configurazione della rete sensibile al contesto](#)

[Posizionamento del punto di accesso](#)

[Modalità monitoraggio ottimizzato \(TOMM\)](#)

[Posizionamento del punto di accesso e dell'antenna](#)

[Attenuazione del segnale](#)

[Sorveglianza di edifici a più piani, ospedali e magazzini](#)

[Guide e aree geografiche](#)

[Creare una maschera in System Manager](#)

[Celle nel motore sensibile al contesto per i tag](#)

[Operazione iniziale per la configurazione delle celle](#)

[Taratura - Motore sensibile al contesto per client](#)

[Tecnologia Exciter \(Chokepoint Trigger\)](#)

[Considerazioni per la distribuzione con riconoscimento del contesto con i servizi voce e dati esistenti](#)

[Orientamenti generali - TDOA](#)

[Posizione cavi](#)

[Sezione 3: Convalida e miglioramento della rete sensibile al contesto](#)

[Strumento di precisione Sistema colori Windows](#)

[Strumento di preparazione alla posizione](#)

[Sensibile al contesto - Prestazioni del sistema](#)

[Tag RFID e configurazione/tuning WLC](#)

[Configurazione e tuning di WCS e MSE](#)

[Risoluzione dei problemi](#)

[Sezione 4: Elenco di controllo finale](#)

[Requisiti hardware](#)

[Sezione 5: Domande tecniche frequenti](#)

[Appendice A Installazione di MSE](#)

[Aggiungi MSE a Sistema colori Windows](#)

[Appendice B Comandi WLC e MSE](#)

[Appendice C: Aggiornamento di MSE dalla versione 5.X alla 6.0](#)

[Appendice D: Ripristino database MSE](#)

[Informazioni correlate](#)

## **Introduzione**

Lo scopo di questo documento è quello di fornire linee guida per la configurazione e l'installazione, nonché suggerimenti per la risoluzione dei problemi e risposte alle domande tecniche frequenti per coloro che aggiungono Cisco Mobility Services Engine (MSE) ed eseguono servizi compatibili con il contesto a una WLAN unificata Cisco. Il presente documento ha lo scopo di:

- Illustrare i vari elementi e la struttura della soluzione Cisco per la mobilità
- Fornire linee guida generali per l'installazione di Cisco Mobility Solution

Questo documento non fornisce i dettagli di configurazione per MSE e i componenti associati. Queste informazioni vengono fornite in altri documenti e vengono forniti i riferimenti. Fare riferimento alla sezione [Informazioni correlate](#) per un elenco di documenti sulla configurazione e la progettazione dei servizi di mobilità con riconoscimento del contesto. Nel presente documento, inoltre, non viene descritta la configurazione degli IPS adattivi.

## **Prerequisiti**

### **Requisiti**

Nessun requisito specifico previsto per questo documento.

### **Componenti usati**

Il documento può essere consultato per tutte le versioni software o hardware.

### **Convenzioni**

Per ulteriori informazioni sulle convenzioni usate, consultare il documento [Cisco sulle convenzioni nei suggerimenti tecnici](#).

## **Premesse**

Cisco MSE consente di tenere traccia della posizione fisica dei dispositivi di rete, sia cablati che wireless, tramite controller LAN wireless (WLC) e Cisco Aironet Lightweight Access Point (LAP). Questa soluzione consente al cliente di tenere traccia di qualsiasi dispositivo Wi-Fi, inclusi client, tag RFID attivi, client e punti di accesso (AP) non autorizzati. È stato progettato tenendo presenti i seguenti requisiti:

- **Gestibilità:** Cisco Wireless Control System (WCS) viene utilizzato per amministrare e monitorare MSE. Inoltre, MSE si integra direttamente nell'architettura LAN wireless, che fornisce una rete unificata da gestire anziché più reti wireless diverse.
- **Scalabilità:** la serie Cisco MSE può registrare simultaneamente fino a 18.000 elementi di rete. WCS può gestire più Mobility Services Engine per una maggiore scalabilità. Il controller, WCS e MSE vengono implementati tramite dispositivi separati per offrire maggiore scalabilità e prestazioni superiori.
- **Sicurezza:** MSE, WCS e controller LAN wireless forniscono interfacce sicure e protocolli sicuri per l'accesso ai dati. MSE registra informazioni cronologiche sulla posizione che possono essere utilizzate per gli audit trail e la conformità alle normative.
- **Aperto e basato su standard:** MSE dispone di un'API SOAP/XML a cui possono accedere sistemi e applicazioni esterni in grado di sfruttare le informazioni sulla posizione provenienti da MSE.
- **Facile distribuzione delle applicazioni aziendali:** il servizio MSE può essere integrato con le nuove applicazioni aziendali, quali il monitoraggio degli asset, la gestione dell'inventario, la sicurezza basata sulla posizione o la gestione automatizzata dei flussi di lavoro.

Il documento si divide in cinque sezioni:

1. [Panoramica della soluzione](#)
2. [Pianificazione e configurazione di una rete Wi-Fi compatibile con il contesto](#)
3. [Convalida e miglioramento della rete sensibile al contesto](#)
4. [Risoluzione dei problemi](#)
5. [Elementi assegni finali](#)

## Sezione 1: Panoramica della soluzione

Il servizio di riconoscimento del contesto (CAS, Context Aware Service) consente a una rete Wi-Fi 802.11a/b/g/n di determinare la posizione di una persona o di un oggetto con una periferica Wi-Fi attiva, ad esempio un client wireless o un tag RFID attivo e/o i dati associati che possono essere passati dal punto finale attraverso l'infrastruttura wireless a un client upstream. Quando un Cisco Mobility Service Engine (MSE) viene aggiunto a una rete wireless unificata (CUWN) Cisco con una versione di WCS con una licenza adeguata, si assume la responsabilità di diverse attività importanti:

- Esecuzione di algoritmi di posizionamento
- Manutenzione delle informazioni di taratura
- Attivazione e invio di notifiche di ubicazione
- Processo delle statistiche e ubicazione storica
- Depository per informazioni geografiche, mappe e tutti i dispositivi wireless

Sistema colori Windows è il sistema di gestione che si interfaccia con MSE e serve l'interfaccia utente per i servizi forniti da MSE. Sebbene sia possibile accedere al server MSE direttamente tramite SSH o una sessione console per scopi di manutenzione e diagnostica, tutte le interazioni tra l'operatore e l'utente e il server MSE vengono in genere eseguite tramite WCS (per la gestione) o un'applicazione client di localizzazione di terze parti.

## Terminologia

Grazie all'architettura WLAN centralizzata di Cisco e ai servizi di posizionamento contestuali, gli

amministratori possono determinare la posizione di qualsiasi dispositivo basato su 802.11, nonché il tipo specifico o lo stato di ogni dispositivo. Il sistema è in grado di identificare e individuare client (associati, in prova e così via), punti di accesso non autorizzati, client non autorizzati e tag attivi. Queste informazioni vengono rese disponibili tramite l'API entro pochi secondi da un evento e possono essere conservate dal database MSE per ricerche cronologiche o controlli di sicurezza.

**Mobility Services Engine (MSE):** MSE supporta una suite di programmi di servizi di mobilità. Progettato come piattaforma aperta, MSE supporta i servizi di mobilità software in modo modulare con varie opzioni di configurazione basate sulla topologia di rete e sui tipi di servizi richiesti. Il valore dell'MSE viene fornito attraverso le varie applicazioni dei servizi di mobilità. Cisco supporta software esistenti e futuri che includono:

- **Servizi sensibili al contesto:** Questi programmi acquisiscono e si integrano nei processi aziendali informazioni contestuali dettagliate su elementi quali posizione, temperatura, disponibilità e applicazioni utilizzate. Le applicazioni sensibili al contesto offrono un'ampia gamma di opzioni di posizione che includono la posizione in tempo reale, il rilevamento della presenza, la visibilità del punto di interruzione e la telemetria. Il supporto per la tecnologia avanzata RSSI (Received Signal Force Indication) e TDoA (Time Difference of Arrival) offre una maggiore accuratezza e prestazioni di scalabilità per un'ampia gamma di ambienti. Il software sensibile al contesto è costituito da due componenti principali:  
**Motore sensibile al contesto per i client:** Il Cisco Location Engine (RSSI) viene utilizzato per tenere traccia dei client Wi-Fi, dei client non autorizzati, dei punti di accesso non autorizzati e dei client cablati.  
**Motore sensibile al contesto per i tag:** Il motore di localizzazione partner (AeroScout) (sia RSSI che TDOA) viene utilizzato per tenere traccia del tag RFID attivo Wi-Fi. Le applicazioni di terze parti sono supportate tramite l'API MSE.
- **Adaptive Wireless Intrusion Prevention System (wIPS):** Il software wIPS fornisce visibilità e prevenzione completa delle minacce per la rete mobile tramite il monitoraggio, gli avvisi, la classificazione e la correzione delle vulnerabilità della rete wireless e cablata.

**Protocollo Network Mobility Services:** Protocollo definito da Cisco usato per garantire la comunicazione tra WLC e MSE.

**WCS (Wireless Control System):** Sistema di gestione di rete wireless sviluppato e supportato da Cisco Systems. Include le seguenti funzionalità:

- Configurazione della WLAN
- Monitoraggio delle prestazioni WLAN
- Creazione di report (in tempo reale e cronologico)
- Visualizzazione grafica della rete (controller LAN wireless, punti di accesso, client e tag)

**Controller LAN wireless (WLC):** L'architettura CUWN centralizza la configurazione e il controllo WLAN in un dispositivo chiamato controller WLAN (WLC). In questo modo l'intera WLAN può funzionare come una rete intelligente che utilizza il wireless come mezzo di accesso per supportare servizi avanzati, a differenza delle infrastrutture WLAN legacy 802.11 che sono costruite da punti di accesso autonomi e discreti. Il CUWN semplifica la gestione operativa attraverso la compressione di un gran numero di endpoint gestiti, ossia punti di accesso autonomi, in un unico sistema gestito costituito dai controller WLAN e dai corrispondenti punti di accesso uniti.

Nell'architettura CUWN, gli AP sono "lightweight", ossia non possono agire in modo indipendente dai WLC. I punti di accesso sono generalmente "zero-touch" implementati e non è richiesta alcuna configurazione individuale. Gli access point apprendono l'indirizzo IP di uno o più WLC tramite un

algoritmo di rilevamento dei controller e quindi stabiliscono una relazione di trust con un controller tramite un processo di "join". Una volta stabilita la relazione di trust, il WLC invia il firmware all'access point, se necessario, e una configurazione in fase di esecuzione. I punti di accesso non archiviano una configurazione localmente.

**Client:** Tutti i dispositivi associati a punti di accesso lightweight basati su controller in una rete wireless.

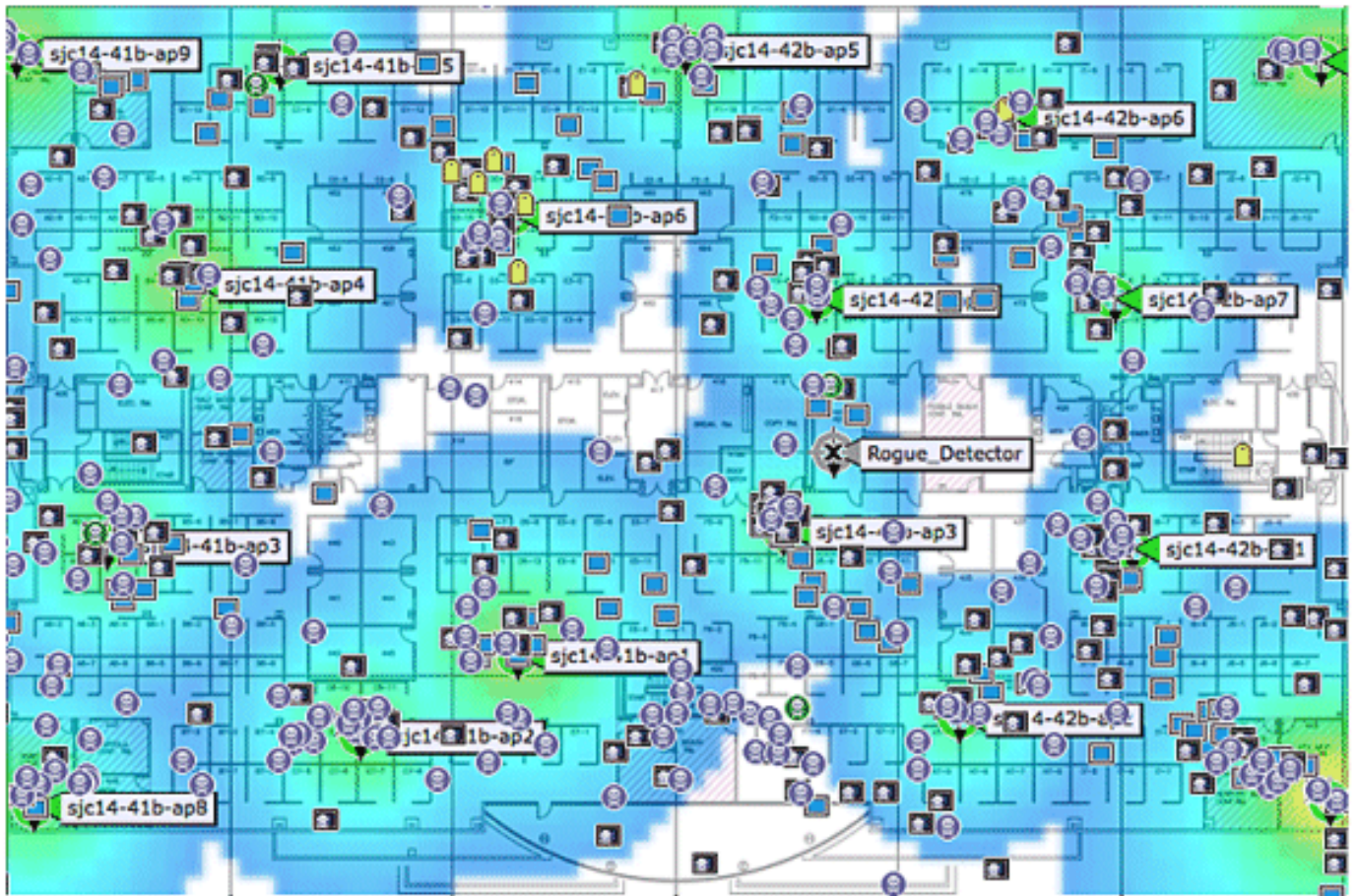
**Access point non autorizzato:** Qualsiasi punto di accesso che non fa parte del gruppo di mobilità LAN wireless che lo ha rilevato. Si tratta di tutti i punti di accesso non di sistema nell'intervallo RF di punti di accesso lightweight, inclusi quelli della rete cablata o quelli di un'altra rete cablata, ad esempio un punto di accesso di un router adiacente. Poiché tutti i punti di accesso lightweight utilizzano un hash come parte del frame del beacon con una chiave speciale, anche i punti di accesso dell'infrastruttura oggetto di spoofing vengono identificati come punti di accesso non autorizzati anziché essere erroneamente contrassegnati in WCS come punti di accesso di spoof.

**Client non autorizzati:** Tutti i dispositivi associati a punti di accesso non autorizzati.

**Tag RFID attivi:** Dispositivo Wi-Fi che può essere rilevato e situato su una rete Wi-Fi. Sul mercato è disponibile un'ampia varietà di etichette compatibili con Wi-Fi. I tag offrono una gamma di caratteristiche che includono la telemetria, come dati ambientali e di movimento, come temperatura e umidità, pulsanti di chiamata, funzionamento in interni ed esterni, versioni intrinsecamente sicure e opzioni di montaggio flessibili.

MSE consente di tenere traccia di fino a 18.000 dispositivi (tag, client e client/access point non autorizzati). **Nella Figura 1** è illustrato un esempio di mappa del pavimento, come mostrato nel WCS, in cui sono visualizzati tag, client, client non autorizzati e punti di accesso non autorizzati. La mappa del pavimento illustra la scala e la varietà di classi di dispositivi che possono essere tracciate da MSE. WCS consente di definire i parametri di ricerca da visualizzare solo in un sottoinsieme di dispositivi. Ad esempio, un utente biomedico può desiderare di vedere solo pompe per infusione e macchine ECG denominate con identificatori amichevoli piuttosto che dispositivi canaglia o dispositivi con indirizzi MAC o IP criptici.

**Figura 1: Mappa di base di Sistema colori Windows con dispositivi rilevati**



Cliente: 

Contrassegno: 

Punto di accesso non autorizzato (rosso=dannoso, verde=amichevole, grigio=non classificato)



Client non autorizzati:

## [Informazioni generali sulle tecnologie](#)

Per tenere traccia dei dispositivi Wi-Fi con Cisco Mobility Solution sono disponibili due tecnologie:

- RSSI (Indicazione della forza del segnale ricevuto)
- TDOA (Differenza tempo di arrivo)

I dettagli su queste tecnologie sono disponibili nella [Guida alla progettazione di Wi-Fi Location-Based Services 4.1](#).

## [RSSI \(Indicazione della forza del segnale ricevuto\)](#)

RSSI è la potenza misurata di un segnale radio ricevuto. I pacchetti trasmessi da qualsiasi dispositivo wireless vengono ricevuti da più punti di accesso (purché questi ultimi siano in ascolto sul canale su cui è stato trasmesso il frame). Gli access point inoltrano questi pacchetti al controller LAN wireless insieme alle informazioni RSSI corrispondenti misurate nell'access point. Il

controller LAN wireless aggrega queste informazioni per dispositivo da diversi punti di accesso. Questi dati vengono inoltrati al MSE tramite NMSP. I servizi sensibili al contesto che risiedono sul MSE utilizzano i dati RSSI ricevuti da uno o più WLC per determinare la posizione di un dispositivo wireless.

RSSI è generalmente preferibile per ambienti interni o a basso soffitto, che possono causare il riflesso dei segnali. A differenza di TDOA, RSSI non richiede la sincronizzazione esatta dell'ora tra i punti di accesso. Con i valori RSSI misurati da diversi punti di accesso, la probabilità della posizione di un dispositivo viene calcolata in punti diversi sul pavimento. In base a questa probabilità, l'ubicazione viene restituita come ubicazione stimata.

## [TDOA \(Differenza tempo di arrivo\)](#)

Quando si tiene traccia delle etichette in ambienti esterni ed interni, ad esempio in ambienti interni a soffitto elevato, il meccanismo TDOA (Time Difference On Arrival) è il metodo preferito per determinare la posizione del dispositivo. Con TDOA, la posizione di un dispositivo WLAN viene determinata in base alla differenza dell'ora di arrivo (TOA) del segnale che trasmette, come rilevato da tre o più ricevitori TDOA Wi-Fi sincronizzati all'ora. I dati sull'ora di arrivo vengono raccolti e segnalati al Context Aware Engine per i tag che risiedono sul MSE, che calcola le differenze di tempo di arrivo tra più coppie di ricevitori Wi-Fi TDOA. Il tempo richiesto per la ricezione di un determinato messaggio da parte di diversi ricevitori Wi-Fi TDOA è proporzionale alla lunghezza del percorso di trasmissione tra il dispositivo di trasmissione mobile e ciascun ricevitore TDOA. Questo meccanismo di calcolo della posizione del dispositivo richiede la sincronizzazione dell'ora tra i ricevitori Wi-Fi TDOA.

Per calcolare una posizione accuratamente, questo metodo richiede un set di almeno tre ricevitori Wi-Fi TDOA. La distanza tra i ricevitori Wi-Fi TDOA è relativamente maggiore della distanza tra i punti di accesso necessari per il posizionamento RSSI interno. Come per il posizionamento RSSI, questo metodo si basa sulla comunicazione unidirezionale (tag che trasmette il frame di notifica, nessuna associazione richiesta).

Fare riferimento alla [guida alla configurazione del software del servizio sensibile al contesto](#).

## [Tag RFID attivi](#)

I tag RFID attivi conformi a CCX vengono rilevati su una rete Wi-Fi in base ai frame di notifica dei tag inviati dal tag e ricevuti da un access point 802.11. La frequenza di fotogrammi delle notifiche dei tag può essere programmata in base allo scenario di utilizzo specifico. In genere, i tag sono configurati in modo da trasmettere frame di notifica dei tag ogni 3-5 minuti per ottimizzare gli aggiornamenti frequenti delle posizioni e la durata della batteria.

La funzione del pulsante di chiamata consente di attivare gli eventi in base al pulsante di comando del tag. In questo modo è possibile usufruire di funzionalità avanzate, ad esempio la creazione di rapporti di emergenza o il rifornimento dei componenti. Alcuni tag forniscono più di un pulsante di chiamata. Il pulsante per la seconda chiamata può essere programmato per ulteriori funzionalità.

I tag possono memorizzare messaggi pre-programmati che possono essere ricevuti dall'infrastruttura di rete wireless. La batteria viene utilizzata per alimentare le etichette attive, che forniscono fino a quattro anni di durata. La durata della batteria dipende da una serie di parametri di configurazione dei tag che includono la frequenza di trasmissione dei frame di notifica dei tag e la frequenza di ripetizione. I tag possono segnalare il livello di batteria e avvertire quando è basso. I tag possono anche avere un sensore di movimento integrato per trasmettere i frame di notifica

dei tag in caso di movimento. Ciò consente di conservare la durata della batteria quando l'etichetta è fissa; configurare le etichette in modo che trasmettano meno frequentemente quando non si spostano.

Esiste un'altra categoria di etichette che aggiungono tecnologie avanzate di sensori per monitorare accuratamente le condizioni di una risorsa, come la temperatura ambiente, oltre ad altre informazioni sulla posizione e lo stato. Queste etichette dei sensori utilizzano reti Wi-Fi standard per trasportare la posizione degli asset e i dati dei sensori e non richiedono reti di sensori dedicate o proprietarie.

Le etichette RFID Wi-Fi conformi alla specifica Cisco Compatible Extensions (CCX) for Wi-Fi Tags possono facoltativamente passare le informazioni di telemetria delle etichette al Cisco UWN che riconosce la posizione come parte del payload dei messaggi delle etichette. Le informazioni di telemetria vengono ricevute dai punti di accesso e raccolte dai WLC. All'avvio di MSE, MSE sottoscrive tutti i servizi a cui è interessato, ad esempio le misure per i tag. Il WLC continua a inviare le notifiche MSE al termine di ogni ciclo di aggregazione.

Le informazioni di telemetria vengono trasmesse da un tag compatibile CCX e vengono ricevute da uno o più access point e/o ricevitori di posizione, ovvero ricevitori TDOA Wi-Fi, che a loro volta passano le informazioni di telemetria ai rispettivi controller WLAN registrati. Se i tag sono configurati per inviare più copie di frame (o burst) per canale, il controller elimina qualsiasi telemetria di tag duplicata e passa i valori di telemetria distillata al MSE. Il database in MSE viene aggiornato con le nuove informazioni di telemetria e reso disponibile ai client di posizione tramite l'API SOAP/XML.

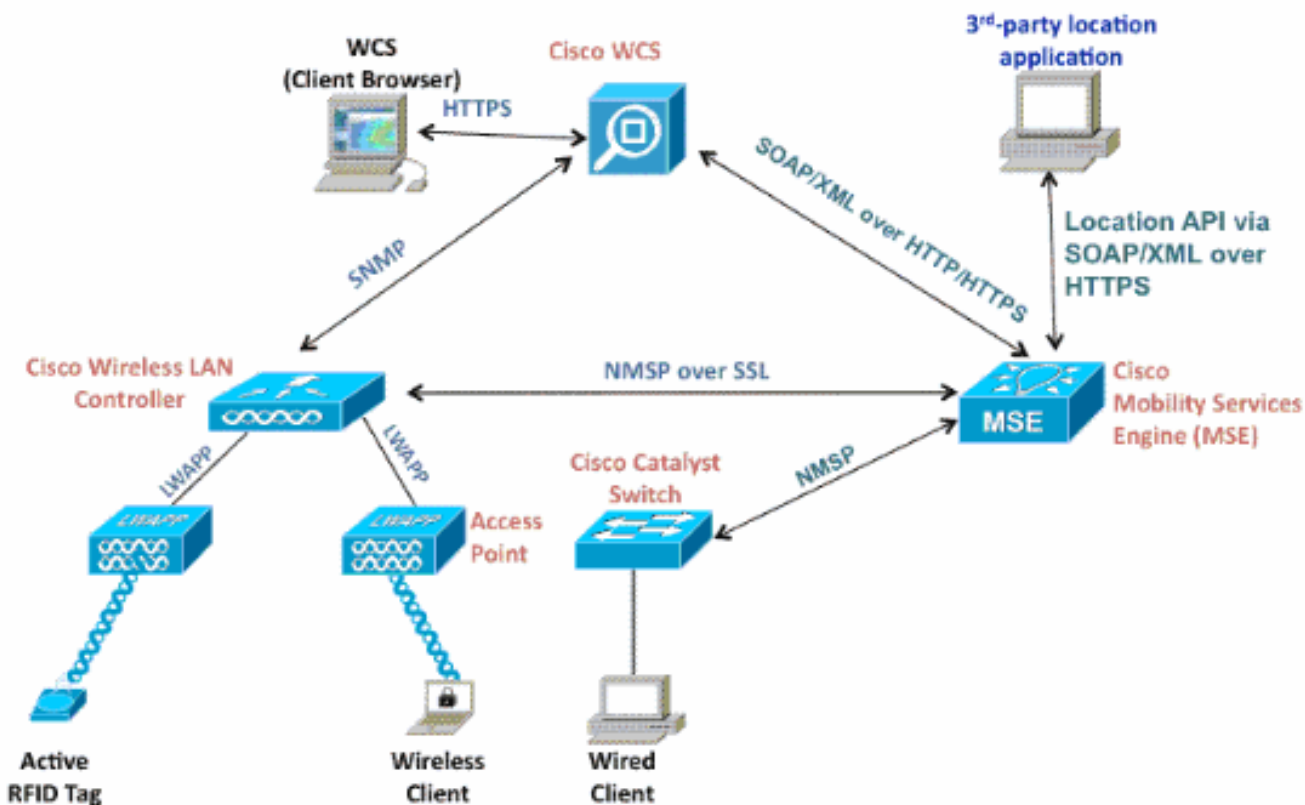
Nel caso di un tag che supera il valore di telemetria, NMSP è progettato per trasportare in modo efficiente i valori di telemetria da più tag in modo simile. Il traffico di telemetria da più tag viene aggregato dal WLC con ciascun endpoint NMSP in grado di eseguire la frammentazione del frame NMSP e, se necessario, di riassemblarlo. Tutti i dati dei tag possono essere inclusi nelle notifiche in direzione nord, che includono la telemetria, i pulsanti di chiamata, gli incontri con punti di interruzione, ecc.

## **Architettura di sistema**

Il MSE si integra con l'architettura WLAN centralizzata di Cisco, come mostrato nella **Figura 2**. Il MSE si trova al di fuori del percorso dati della LAN wireless (vedere il diagramma) e riceve i dati dal WLC tramite l'NMSP. Sistema colori Windows viene utilizzato per configurare MSE. Una volta configurato, MSE è autonomo.

## **Figura 2: Architettura di sistema**





Quando si distribuisce la soluzione sensibile al contesto, è necessario considerare il tipo di dispositivi rilevati e il numero massimo di dispositivi. È possibile tenere traccia di uno dei cinque tipi di dispositivi (client Wi-Fi, tag RFID attivi, client non autorizzati, access point non autorizzati o client cablati) da configurare singolarmente o per il rilevamento simultaneo.

Un MSE può essere gestito da un solo WCS, ovvero un singolo MSE non può essere gestito da più istanze WCS, ma un singolo WCS può gestire più MSE. Quando il numero di dispositivi da gestire supera la capacità di un singolo MSE, è necessario distribuire più MSE indipendenti. La possibilità di distribuire più MSE per la scalabilità si applica a tutti i servizi attualmente supportati da MSE. Un Cisco MSE 3350 può rilevare un massimo di 18.000 dispositivi (combinazione di client Wi-Fi, tag RFID attivi, client non autorizzati, access point non autorizzati e client cablati) come parte del servizio Context Aware. Cisco MSE 3310 può rilevare fino a 2.000 dispositivi. Quando il numero di dispositivi da gestire supera la capacità di un singolo dispositivo MSE, è necessario implementare più appliance MSE indipendenti. Ciò può richiedere MSE su controller specifici, soprattutto nei campus di grandi dimensioni dove il roaming di client o asset può attraversare edifici o domini fisici diversi. In questo caso, i controller possono comunicare con un massimo di 10 accessori MSE.

I Cisco LAP funzionano in una modalità doppia che consente di rilevare i dispositivi sia sui canali a cui servono i client sia su tutti gli altri canali, se eseguono periodicamente una scansione in background e forniscono comunque l'accesso ai dati ai client wireless. I dati grezzi raccolti sulla posizione vengono quindi inoltrati da ciascun punto di accesso al WLC associato tramite il protocollo LWAPP o il protocollo CAPWAP basato su standard. I dati vengono trasportati tra il controller LAN wireless e l'MSE attraverso una connessione NMSP protetta.

Cisco WCS viene utilizzato per gestire e configurare MSE e può anche diventare il front-end visivo di MSE per visualizzare i dispositivi Wi-Fi tracciati. È possibile accedere a tutti i dettagli relativi ai dispositivi (cablati e wireless) e a informazioni cronologiche specifiche sulla posizione con l'API MSE in direzione nord. WCS utilizza questa interfaccia per visualizzare le informazioni sulla posizione, nonché per visualizzare e configurare i parametri specifici del contesto.

Cisco Mobility Solution è costituita da due motori di posizione con un'unica interfaccia API (Application Programming Interface):

- Motore sensibile al contesto per i client (motore Cisco)
- Motore sensibile al contesto per tag (motore partner)

Context Aware Engine for Clients è una soluzione basata su RSSI ed è ideale per tenere traccia dei dispositivi client Wi-Fi in ambienti interni, ad esempio uffici, ospedali o altri ambienti a soffitto basso. Per impostazione predefinita, questo motore viene fornito su tutti i server Cisco MSE. Oltre al software Cisco MSE, i clienti devono acquistare due componenti aggiuntivi per il monitoraggio dei client:

- Licenza di monitoraggio client per MSE con numero di client appropriato
- Cisco WCS PLUS con ubicazione

Il Context Aware Engine for Tags ha la capacità di utilizzare sia un motore basato su RSSI che TDOA ed è progettato per essere utilizzato quando si tracciano dispositivi Wi-Fi in ambienti interni, a basso soffitto (RSSI), interni ad alto soffitto (TDOA) ed esterni (TDOA). Per impostazione predefinita, questo motore viene installato anche su tutte le piattaforme MSE ed è abilitato per le licenze. I clienti devono acquistare questi componenti aggiuntivi per il monitoraggio dei client:

- Licenza di tracking dei tag per MSE con il numero di tag appropriato (TDoA o RSSI)
- Ricevitori Wi-Fi TDoA (se e quando richiesto)
- Licenza LR per ciascun ricevitore Wi-Fi TDoA
- Cisco WCS PLUS con ubicazione

Quando si aggiunge un MSE Cisco a una rete wireless unificata, MSE si assume la responsabilità di diverse attività importanti:

- Esecuzione di algoritmi di posizionamento
- Manutenzione delle informazioni di taratura
- Attivazione e invio di notifiche di ubicazione
- Elaborazione delle statistiche e localizzazione storica

Sistema colori Windows è la piattaforma di gestione per i server MSE e l'interfaccia utente per i servizi forniti da MSE. L'accesso al server MSE avviene direttamente tramite SSH o una sessione console a scopo di manutenzione e diagnostica. Tutte le interazioni tra l'operatore e l'utente con MSE vengono in genere gestite tramite WCS.

L'integrazione di un Cisco MSE in un'architettura di rete wireless unificata di Cisco consente di migliorare immediatamente le funzionalità di base per la localizzazione. Sono inclusi i seguenti miglioramenti:

**Scalabilità:** se si aggiunge un Cisco MSE, la scalabilità del Cisco UWN aumenta dal rilevamento su richiesta di un singolo dispositivo alla volta a una capacità di tracciamento massima di 18.000 dispositivi simultanei (client WLAN, tag RFID, punti di accesso non autorizzati e client non autorizzati) per MSE. Per le installazioni che richiedono il supporto di un numero maggiore di dispositivi, è possibile installare e gestire ulteriori appliance MSE in uno o più server WCS.

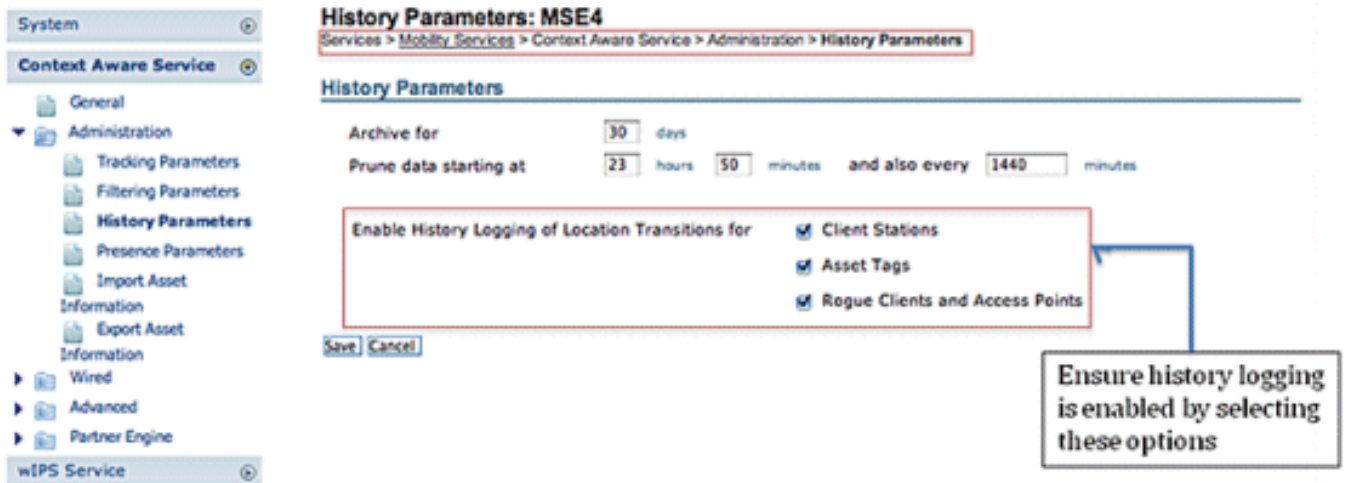
**Tendenze cronologiche e statistiche:** MSE registra e gestisce informazioni cronologiche su posizione e statistiche per client e tag. Queste informazioni sono disponibili per la visualizzazione tramite WCS o con client di posizione di terze parti. Queste informazioni cronologiche possono essere utilizzate per l'analisi dei trend di posizione, la ricerca sulla perdita di asset, la gestione della capacità RF e la risoluzione dei problemi di rete.

I parametri cronologici possono essere configurati in WCS come illustrato nella **Figura 3**.

Esistono diverse variabili che influiscono sulla quantità di dati cronologici che è possibile archiviare in MSE: numero medio di elementi che si spostano, distanza media percorsa ogni volta che si verifica un movimento, transizioni delle informazioni, informazioni di telemetria dai tag, ecc.

Per impostazione predefinita, 30 giorni di dati cronologici vengono archiviati in MSE.

**Figura 3: Configurazione dei parametri della cronologia**



Di seguito sono riportati alcuni punti importanti da tenere in considerazione per la cronologia delle posizioni:

1. Per recuperare informazioni cronologiche su un elemento, è necessario attivare la registrazione della cronologia, come illustrato nella figura.
2. Il numero di giorni precedenti e il tempo di potatura devono essere scelti correttamente (vedere la schermata).
3. Sebbene il numero di giorni per il salvataggio della cronologia non sia limitato nell'interfaccia utente, la cronologia archiviata nel server è limitata dallo spazio su disco e dall'impatto sulle prestazioni dell'intero sistema.
4. La cronologia di un elemento viene registrata solo se si verificano le seguenti condizioni: Si muove per più di 10 metri o 30 piedi. Se si preme il pulsante di emergenza o di panico sulle etichette. Se il tag passa di un eccitatore. Se il pavimento cambia, l'elemento si sposta tra i piani.
5. Un elemento viene dichiarato "inactive" se rimane inattivo per un'ora. Se rimane inattiva per 24 ore, viene rimossa dalla tabella di rilevamento. Una volta rimosso l'elemento dalla tabella di rilevamento, non è possibile visualizzare la posizione storica dell'elemento nella pagina di monitoraggio del Sistema colori Windows, sebbene la cronologia dell'elemento sia ancora presente nel MSE per 30 giorni. L'immissione Intervallo pulizia dati assente (vedere la Figura 4) consente di controllare la tabella di rilevamento. **Figura 4: Parametri posizione**

## Location Parameters: MSEWCS4

Services > Mobility Services > Context Aware Service > Advanced > Location Parameters

### Location Parameters

Enable calculation time ⓘ	<input type="checkbox"/> Enable
Enable OW Location ⓘ	<input type="checkbox"/> Enable
Relative discard RSSI time ⓘ	<input type="text" value="3"/> 1 - 99999 min
Absolute discard RSSI time ⓘ	<input type="text" value="60"/> 1 - 99999 min
RSSI Cutoff ⓘ	<input type="text" value="-75"/> -90 to -50 dBm
Enable Location Filtering ⓘ	<input checked="" type="checkbox"/> Enable
Chokepoint Usage ⓘ	<input checked="" type="checkbox"/> Enable
Use Chokepoints for Interfloor conflicts ⓘ	<input type="text" value="Never"/>
Chokepoint Out of Range Timeout ⓘ	<input type="text" value="60"/> 1-99999 secs
Absent Data cleanup interval ⓘ	<input type="text" value="1440"/> 1 - 99999 mins

Registrando ogni transizione come evento per l'archiviazione nel database cronologico e limitando la tabella Cronologia posizione a 10 milioni di righe per motivi di prestazioni, la **tabella 1** riepiloga il numero di giorni necessari per raggiungere tale limite. Maggiore è il numero di transizioni di elementi al minuto, maggiore è la quantità di spazio su disco utilizzata. Secondo la tabella, occorrono solo 7,14 giorni per raggiungere 10 milioni di righe con 1000 transizioni/minuto. Con l'impostazione predefinita di 30 giorni di dati cronologici, 1000 transizioni/minuto consumano una quantità eccessiva di spazio su disco poiché MSE non elimina i dati cronologici prima che sia stata raggiunta la finestra di 30 giorni.

Cisco consiglia di modificare il parametro history dei dispositivi che vengono spostati frequentemente a un valore inferiore a 30 giorni.

Tabella 1. Limite database cronologia percorso

Transizioni al minuto	Giorni per raggiungere 10 milioni di righe
100	69.44
200	34.72
300	23.15
400	17.36
500	13.89
600	11.57
700	9.92
800	8.68

900	7.75
1000	7.14

**Posizione punto di scelta:** il servizio MSE fornisce una localizzazione granulare e deterministica basata sul passaggio di una risorsa attraverso un'area fisica vincolata nota come punto di scelta. I trigger di Chokeypoint (detti anche "eccitatori") situati all'interno di queste aree e in prossimità di risorse contrassegnate stimolano i tag con segnalazione a bassa frequenza (125 kHz). I tag RFID trasmettono quindi l'identità del trigger del punto di interruzione all'infrastruttura Cisco WAN. Le informazioni di punto di interruzione contenute nel pacchetto di tag forniscono al MSE informazioni per ignorare le coordinate di posizione di impronta digitale RF e assumere la posizione di punto di interruzione per una determinata durata. La precisione della posizione di prossimità può variare da un raggio di meno di un piede a oltre venti piedi (da 25 a 650 cm), a seconda delle capacità del trigger di chokeypoint. Le applicazioni per l'ubicazione di chokeypoint variano da usi generici, come la prevenzione del furto di asset di alto valore, ad eventi di controllo dei processi specifici del settore, come quelli utilizzati negli impianti di produzione.

**Estensioni Cisco per Wi-Fi Tag: informazioni di telemetria e notifiche di emergenza** — Cisco ha stretto una partnership con diversi fornitori di tag degli asset per creare una specifica estensibile per i tag degli asset attivi basati su Wi-Fi 802.11. La specifica dei tag Wi-Fi di Cisco Compatible Extensions (CCX) definisce un formato di trasmissione comune che i fornitori di tag possono utilizzare per interagire con il nome utente Cisco sensibile al contesto. Questo include una serie di funzionalità di base che comprende telemetria, tagging, livello di potenza di trasmissione, informazioni sulla batteria e campi avanzati per gruppi di emergenza e punti di interruzione. L'aggiunta di un MSE consente ai clienti di trarre vantaggio da queste funzionalità e vantaggi offrendo la possibilità di combinare i codici di matricola conformi di diversi fornitori nella stessa rete. Attualmente, i fornitori di tag hanno implementato CCXv1. URL di riferimento tag: [http://www.cisco.com/web/partners/pr46/pr147/ccx\\_wifi\\_tags.html](http://www.cisco.com/web/partners/pr46/pr147/ccx_wifi_tags.html).

## [Sezione 2: Pianificazione e configurazione della rete sensibile al contesto](#)

Quando si installa una rete wireless che influisce direttamente sul livello di accuratezza della posizione, è necessario rispettare alcune linee guida.

### **Progettazione della LAN wireless per la posizione e la voce**

#### **Linee guida generali - RSSI**

Per determinare la posizione ottimale di tutti i dispositivi nelle aree di copertura della LAN wireless, prendere in considerazione la densità e il posizionamento dei punti di accesso.

#### [Posizionamento del punto di accesso](#)

La corretta collocazione dei punti di accesso, o meglio, la collocazione e il tipo di antenna sono alcune delle migliori pratiche che devono essere rispettate per poter sperimentare un livello ragionevole di accuratezza della posizione. In molte LAN wireless di ufficio i punti di accesso sono distribuiti principalmente negli spazi interni e forniscono servizi alle aree di lavoro circostanti. Questi punti di accesso sono stati tradizionalmente selezionati sulla base della copertura: Larghezza di banda WLAN, riutilizzo dei canali, sovrapposizione cella-cella, sicurezza, estetica e fattibilità di implementazione. In una progettazione WLAN con riconoscimento della posizione, i

requisiti delle applicazioni voce e dati sottostanti devono essere combinati con i requisiti per una buona fedeltà di posizione. A seconda del sito, i requisiti del Cisco UWN con riconoscimento della posizione sono sufficientemente flessibili da consentire, ad esempio, l'aggiunta di localizzazione della posizione a installazioni voce già progettate in conformità con le best practice di Cisco, potrebbe non richiedere una rielaborazione estesa. Al contrario, l'infrastruttura già installata in conformità con le best practice accettate in materia di voce può spesso essere potenziata in modo da soddisfare anche i requisiti delle best practice in materia di tracciamento della posizione (ad esempio il posizionamento dei punti di accesso perimetrali e angolari) a seconda delle caratteristiche delle aree interessate.

In un design adatto alla posizione, è importante garantire che i punti di accesso non siano raggruppati solo all'interno e verso il centro dei piani. I punti di accesso perimetrali sono invece complementari ai punti di accesso situati all'interno delle aree del pavimento. Inoltre, i punti di accesso devono essere posizionati in ciascuno dei quattro angoli del pavimento e in tutti gli altri angoli che si incontrano lungo il perimetro del pavimento. Questi punti di accesso perimetrali svolgono un ruolo fondamentale per garantire una buona fedeltà di posizionamento all'interno delle aree che circondano e, in alcuni casi, possono fornire anche una copertura generale di voce o dati.

Se si utilizza la posizione del punto di interruzione, verificare che tutte le aree pianificate per l'installazione del punto di interruzione siano chiaramente comprese nell'intervallo RF dei punti di accesso. A differenza degli scanner RFID passivi, il tag utilizza la WLAN per trasmettere i contenuti eccitanti all'infrastruttura. Oltre a garantire che i messaggi trasmessi dai codici di matricola situati all'interno delle aree di chokepoint vengano ricevuti correttamente dal sistema, una corretta pianificazione può contribuire a garantire che i codici di matricola possano essere tracciati con RF Fingerprinting quando si avvicinano e escono dai punti di chokepoint. La possibilità di tenere traccia dei codici di matricola con impronte digitali RF completa la capacità del sistema di individuare i codici di matricola all'interno delle aree di chokepoint con tecniche di localizzazione altamente granulare.

I punti di accesso che formano il perimetro e gli angoli del pavimento possono essere pensati come delineare lo scafo convesso o una serie di possibili posizioni di dispositivi dove esiste il miglior potenziale per l'alta precisione e precisione. Si può ritenere che l'area interna (all'interno dello scafo convesso) abbia un elevato potenziale per una buona accuratezza di posizionamento. Quando i dispositivi rintracciabili penetrano nell'area esterna allo scafo convesso, la precisione diminuisce.

Al fine di garantire una corretta sistemazione convessa dello scafo intorno alla serie di punti di dati di posizione che possiedono un elevato potenziale per una buona accuratezza, i punti di accesso devono essere posizionati in ogni angolo del pavimento, così come lungo il perimetro del pavimento tra gli angoli. La separazione tra i punti di accesso lungo il perimetro deve essere conforme alle linee guida generali per la separazione dei punti di accesso (descritte in una sezione successiva). Il progettista può ridurre questa spaziatura se necessario, in modo che questi punti di accesso forniscano servizi voce o dati al pavimento.

Accertarsi che non meno di tre punti di accesso coprano ogni area in cui è richiesta la posizione del dispositivo. La precisione ottimale richiede quattro o più punti di accesso. Ciò riduce anche il rischio che i punti di accesso non sempre contribuiscano alla localizzazione a causa di altre attività WLAN. In un normale ambiente di lavoro, i punti di accesso devono circondare la posizione di qualsiasi periferica Wi-Fi tracciata. Un punto di accesso deve essere posizionato ogni 40-70 piedi lineari (~12-20 metri). Ciò si traduce in un punto di accesso ogni 2.500-5.000 piedi quadrati (~230-450 metri quadrati). Ad esempio, in una struttura a 200.000 piedi quadrati, sono necessari 40 punti di accesso (200.000/5.000) per una corretta copertura Wi-Fi. Le antenne PA devono essere

posizionate a un'altezza minima di 10 piedi e a un'altezza massima di 20 piedi. Poiché tali linee guida dipendono in larga misura dalla costruzione dell'edificio e dai materiali utilizzati, è necessario prendere in considerazione altri fattori e raccomandazioni. Come regola generale -75dBm deve essere utilizzato come livello di segnale minimo per il rilevamento dei dispositivi da un minimo di tre punti di accesso sullo stesso piano.

Se si seguono queste linee guida, è più probabile che i punti di accesso rilevino correttamente i dispositivi rilevati.

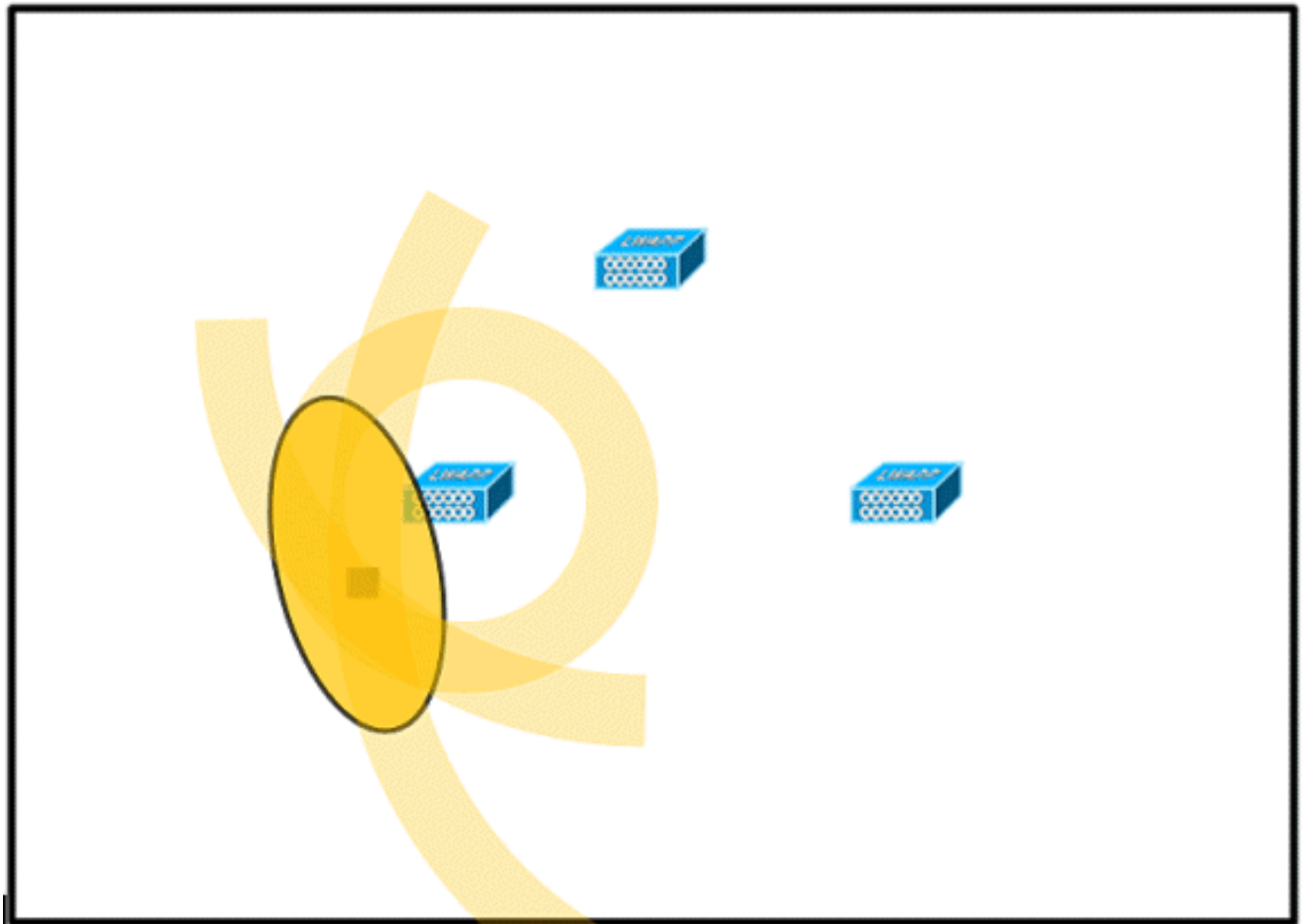
Raramente due ambienti fisici hanno le stesse caratteristiche RF. Gli utenti devono adeguare tali parametri in base all'ambiente e ai requisiti specifici.

Di seguito sono riportate le regole di base per il posizionamento dei punti di accesso che contribuiscono alla precisione della posizione.

1. Fornire copertura perimetrale AP.
2. Assicurare una densità AP sufficiente.
3. punti di accesso sfalsati, in particolare in aree di copertura lunghe e strette.
4. Progettare una rete wireless per tutte le applicazioni (dati, voce e posizione).
5. Verificare la distribuzione wireless con un sondaggio del sito.
6. In un edificio con pavimenti di forma simile, installare gli access point su ogni piano in un modello simile. Ciò migliora le prestazioni di separazione del pavimento del sistema.

Lo strumento di pianificazione di Sistema colori Windows può essere utilizzato per determinare/verificare il posizionamento e la densità corretti dei punti di accesso.

1. Posizionare i punti di accesso lungo la periferia e negli angoli delle aree di copertura per aiutare a individuare i dispositivi vicino all'esterno di stanze ed edifici. I punti di accesso situati al centro di queste aree di copertura forniscono buoni dati su dispositivi che altrimenti appaiono equidistanti da tutti gli altri punti di accesso (vedere le **figure da 5 a 8**). **Figura 5: I punti di accesso raggruppati insieme possono causare risultati insoddisfacenti**



Punto di accesso:



Dispositivo Wi-Fi:

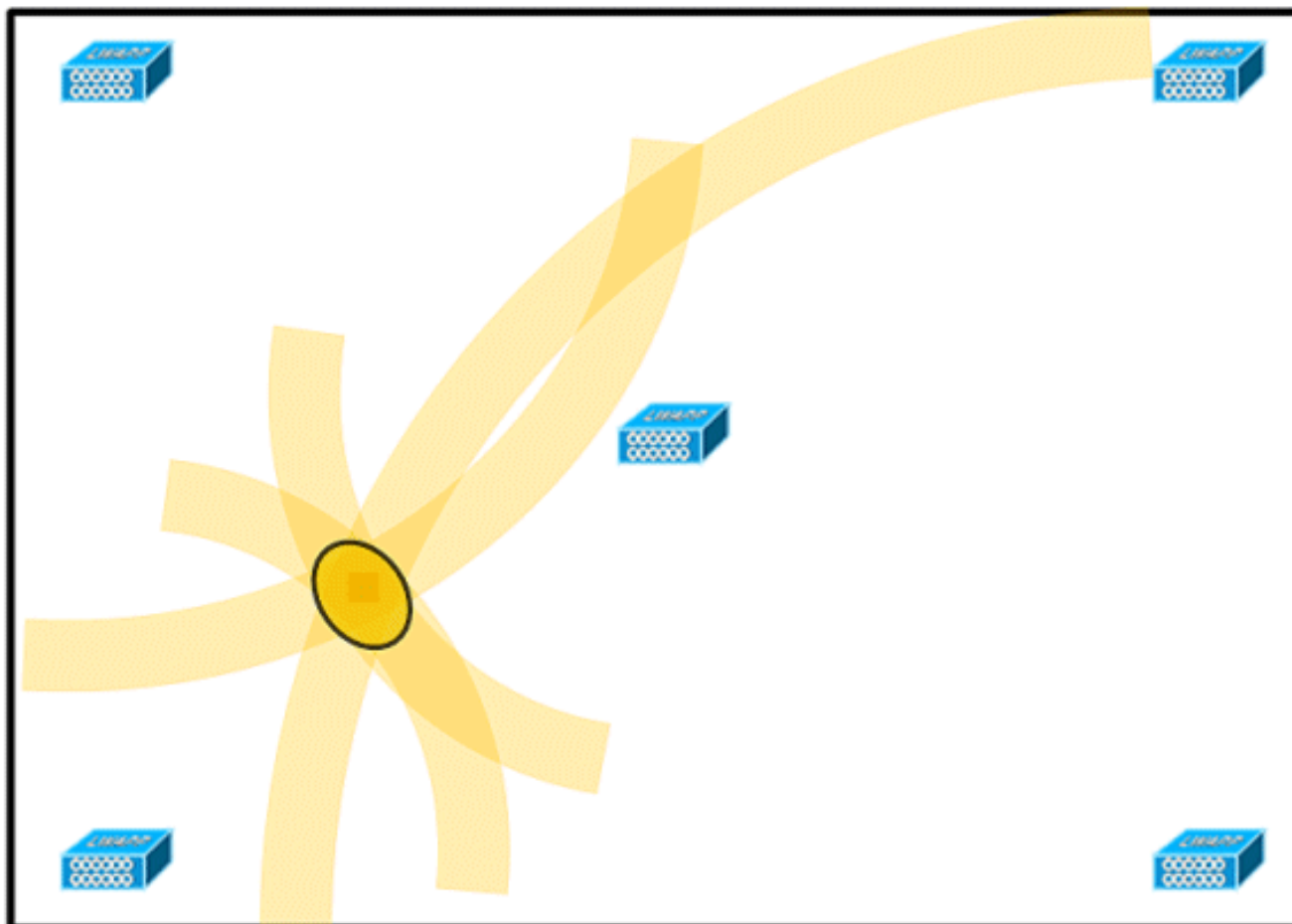


Jitter RF (posizione possibile):

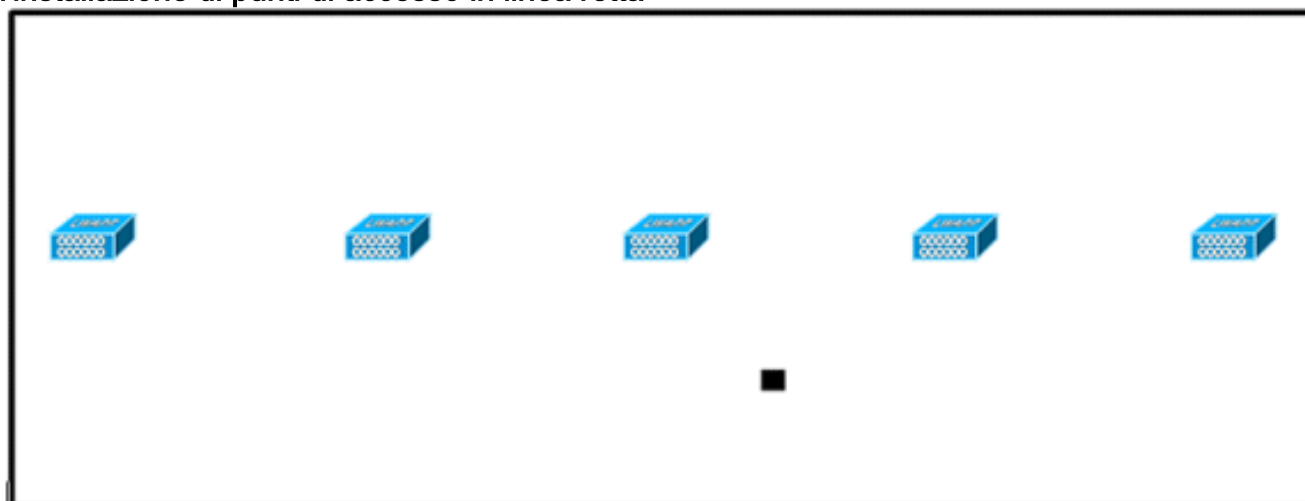


2. Aumentate la densità globale dei punti di accesso e spostateli verso il perimetro dell'area di copertura per migliorare notevolmente la precisione della posizione (vedere figura). **Figura 6: Miglioramento della precisione della posizione tramite il corretto posizionamento dei punti di accesso**



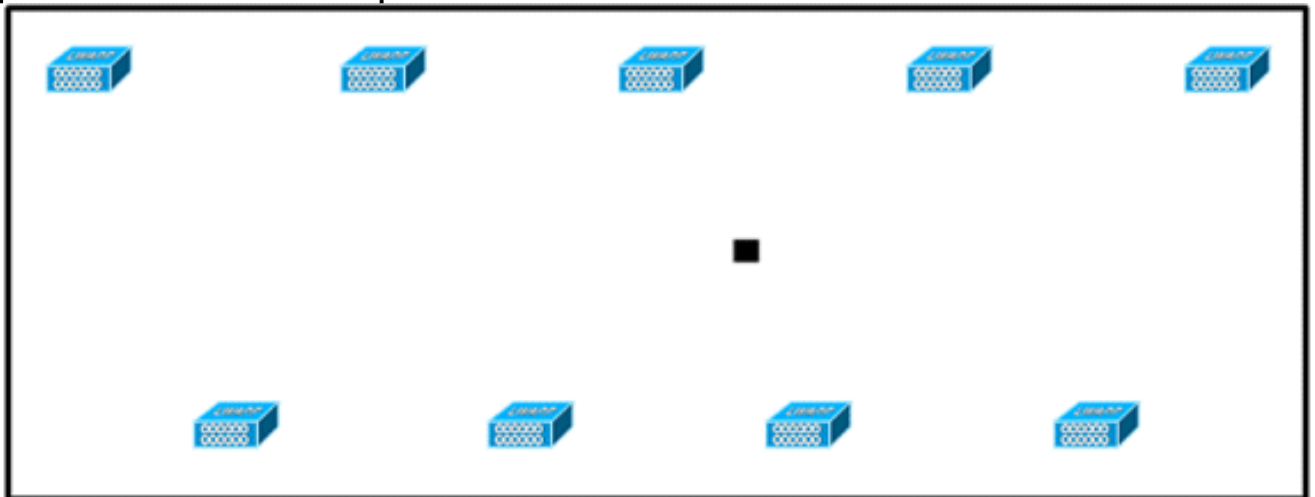


3. Nelle aree di copertura lunghe e strette, non posizionare i punti di accesso in linea retta (vedere le **figure 7 e 8**). Un'implementazione preferibile consiste nello sfalsare gli access point in quanto forniscono una firma RF univoca in qualsiasi punto della mappa di copertura Wi-Fi. Un'implementazione in linea retta fornisce una mappa RF simil-mirror. Con questo tipo di distribuzione, la firma RF di un punto nella parte superiore della mappa è molto simile alla firma RF nel punto di mirroring nella parte inferiore della mappa. **Figura 7: Evitare l'installazione di punti di accesso in linea retta**

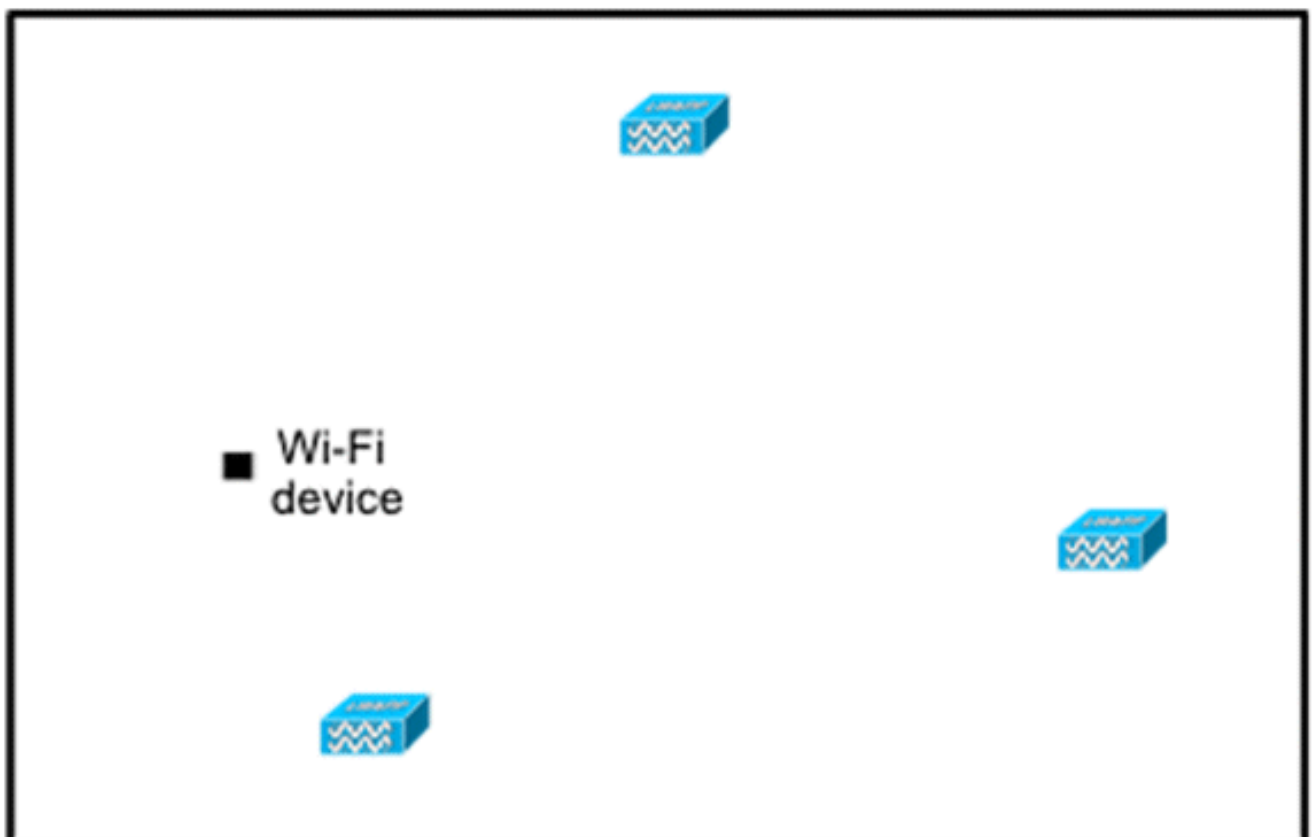


Sebbene il design della **Figura 7** possa fornire una densità di punti di accesso sufficiente per le applicazioni a elevata larghezza di banda, la posizione risente di un problema perché la vista di un singolo dispositivo di ciascun punto di accesso non varia abbastanza, quindi è difficile determinare la posizione del dispositivo. Spostare i punti di accesso al perimetro dell'area di copertura e sfalsarli. Ognuna di esse offre una visualizzazione nettamente diversa del dispositivo, il che determina una maggiore fedeltà di posizionamento (vedere la

Figura 8).Figura 8: Miglioramento della precisione della posizione grazie allo sfalsamento dei punti di accesso attorno al perimetro



4. Quando si progetta una LAN wireless per una soluzione di mobilità sensibile al contesto, mentre si pianifica anche la voce, è necessario tenere conto di una serie di fattori di progettazione. La maggior parte degli attuali telefoni wireless supportano solo 802.11b, che offre solo tre canali non sovrapposti, pertanto le LAN wireless progettate per la telefonia tendono ad essere meno dense di quelle previste per il trasporto di dati. Inoltre, quando il traffico è in coda nel bucket QoS Platinum (in genere riservato al traffico vocale e ad altro traffico sensibile alla latenza), i punti di accesso lightweight rimandano le funzioni di scansione che consentono loro di raggiungere il picco su altri canali e raccogliere, tra le altre cose, informazioni sulla posizione dei dispositivi. Pertanto, l'utente ha la possibilità di integrare l'installazione di LAN wireless con punti di accesso impostati sulla modalità di solo monitoraggio. I punti di accesso che si limitano al monitoraggio non forniscono servizi ai client e non creano interferenze. Si limitano a scansionare le onde radio per ottenere informazioni sui dispositivi (vedere le figure 9 e 10).**Figura 9: Installazioni LAN wireless meno dense**



Nelle installazioni LAN wireless meno dense, ad esempio quelle delle reti voce, la fedeltà della posizione risulta notevolmente migliorata dall'aggiunta e dalla corretta collocazione dei punti di accesso in modalità monitor ottimizzata per la posizione.

5. Eseguire una verifica della copertura con un laptop wireless, un palmare ed eventualmente un telefono per assicurarsi che il dispositivo rilevi almeno tre punti di accesso. Per verificare la posizione dei codici di matricola del client e dell'asset, verificare che i codici di matricola e i codici di matricola del client siano compresi nell'intervallo di precisione specificato (10m, 90%). Per raggiungere questo livello di precisione può essere necessaria una taratura.

### Modalità monitoraggio ottimizzato (TOMM)

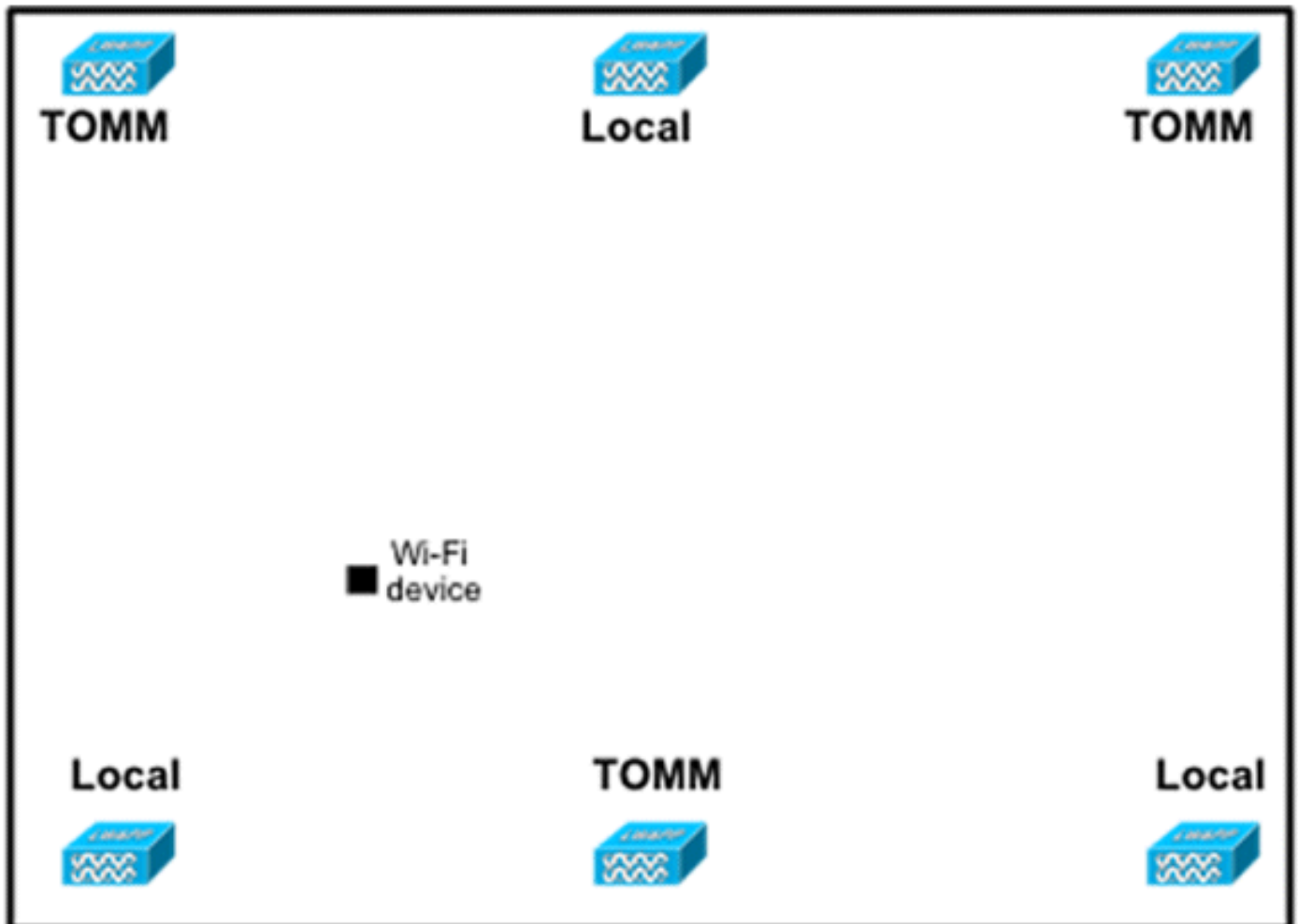
A partire dalla versione software 5.0, i Cisco Aironet 1100 e 1200 AP possono funzionare come punti di accesso in modalità monitoraggio ottimizzato. Questa funzione può essere utilizzata per i seguenti motivi:

- Coesistenza di voce e località: Con la modalità di monitoraggio AP in un'implementazione mista, non vi è alcun impatto negativo sulla voce poiché la posizione deve aumentare la densità AP.
- Il basso tocco non influisce sull'infrastruttura attuale.

La modalità Monitoraggio ottimizzato per la posizione può essere utilizzata quando si tiene traccia di client e/o tag.

Gli access point TOMM sono ideali per migliorare la copertura delle posizioni di rilevamento indipendentemente da dove esistono gap di copertura Wi-Fi, sia nel perimetro che all'interno dello scafo convesso. Gli access point TOMM non interferiscono con il funzionamento degli access point in modalità locale. Per ottimizzare il monitoraggio e il calcolo della posizione dei tag, TOMM può essere abilitato su un massimo di quattro canali nella banda a 2,4 GHz (radio 802.11b/g) di un access point. Ciò consente di mettere a fuoco le scansioni dei canali solo sui canali sui quali i tag sono solitamente programmati per funzionare (come i canali 1, 6 e 11).

**Figura 10: Distribuzione punto di accesso modalità monitoraggio ottimizzato**



## Posizionamento del punto di accesso e dell'antenna

Il posizionamento dei punti di accesso e delle antenne esterne può avere un impatto notevole sulle prestazioni delle reti wireless. Ciò è vero per la trasmissione di dati e voce, così come per la localizzazione. I punti di accesso e le antenne non devono essere collocati in una posizione (ad esempio in prossimità dei raggi I) che potrebbe distorcere i modelli di segnale. Un punto nullo RF viene creato dall'incrocio delle onde di segnale e la distorsione multipath viene creata quando i segnali RF vengono riflessi. Questo posizionamento comporta una copertura molto ridotta dietro l'access point e una qualità del segnale ridotta davanti all'access point. Il fascio I crea molti riflessi sia per i pacchetti ricevuti che per quelli trasmessi. I segnali riflessi determinano una scarsa qualità del segnale a causa dei punti nulli e dell'interferenza multipath, ma la forza del segnale può essere elevata perché le antenne AP sono così vicine al raggio I da poter amplificare il segnale. Al contrario, il punto di accesso e il posizionamento dell'antenna devono essere posizionati lontano dai raggi I in modo che vi siano meno segnali riflessi, meno punti nulli e meno interferenze a percorsi multipli. Il principio si applica anche quando si posizionano punti di accesso e antenne all'interno o vicino al soffitto in un ambiente aziendale standard. Se vi sono condotte d'aria metalliche, alberi di elevazione o altre barriere fisiche che possono causare riflessione del segnale o interferenze a percorsi multipli, Cisco consiglia di posizionare le antenne lontano da tali oggetti. Nel caso di oggetti metallici di grandi dimensioni, come ascensori e condotte d'aria, spostare l'antenna di qualche metro di distanza. Questo aiuta ad eliminare il riflesso e la distorsione del segnale. **Le figure da 11 a 13** illustrano un posizionamento non corretto dell'access point.

**Figura 11: Posizionamento inadeguato del punto di accesso: punto di accesso in prossimità di un'ostruzione fisica**



**Figura 12: Posizionamento inadeguato del punto di accesso: punto di accesso in prossimità di un'ostruzione fisica**



Figura 13: Posizionamento dei punti di accesso inadeguato - punti di accesso vicini



Quando si installano punti di accesso con antenne interne o esterne, sia la posizione del punto di accesso che l'orientamento scelto per le antenne del punto di accesso in WCS devono corrispondere alla posizione fisica effettiva del punto di accesso e all'orientamento dell'antenna. Ciò garantisce accuratezza e precisione sia nella localizzazione che nella visualizzazione di mappe di calore predittive. Il tipo di antenna, la posizione, l'orientamento e l'altezza dal pavimento sono fondamentali per garantire una buona accuratezza. Quando si inseriscono i punti di accesso in Servizi di gestione remota Windows, verificare che l'orientamento e il tipo dell'antenna corrispondano a quello distribuito.

**Nota:** quando si tiene traccia dei client wireless, solo le antenne Cisco sono ufficialmente supportate. Per le antenne non Cisco, le heatmap non vengono generate in WCS. Ciò significa anche che i valori RSSI ricevuti da queste antenne vengono ignorati nel calcolo dell'ubicazione. Per il tracking dei tag, si possono usare sia le antenne Cisco che quelle non Cisco.

Il tipico access point Cisco Aironet viene installato con diverse antenne. La diversità delle antenne assicura un range e un throughput ottimali in ambienti a percorsi multipli elevati. Si consiglia di abilitare sempre la diversità dell'antenna. Il nome utente Cisco sensibile al contesto è progettato per prendere in considerazione le informazioni RSSI di entrambe le antenne del punto di accesso quando si localizzano i dispositivi rilevati. Per una buona accuratezza, assicurarsi che le antenne siano fisicamente presenti su tutte le porte dell'antenna del punto di accesso abilitate. In caso contrario, è possibile che vengano segnalate letture RSSI irregolari sulle porte dell'antenna abilitate prive di antenna collegata. I valori RSSI anormalmente bassi delle porte dell'antenna senza antenne determinano una scarsa accuratezza della posizione.

La scelta dell'antenna da utilizzare con un punto di accesso è fondamentale per le caratteristiche

di qualsiasi installazione di rete wireless. Esistono essenzialmente due tipi di antenna: direzionale e omnidirezionale. Ogni tipo di antenna ha un uso specifico ed è più adatto per un tipo specifico di installazione. Poiché le antenne distribuiscono il segnale RF in ampie aree di copertura lobate determinate dal design dell'antenna, la copertura di successo dipende in gran parte dalla scelta dell'antenna.

Un'antenna ha tre proprietà fondamentali: guadagno, direttività e polarizzazione.

- **Guadagno:** Una misura dell'aumento di potere. Il guadagno è la quantità di energia che un'antenna aggiunge a un segnale RF. Tutte le antenne sono elementi passivi. L'energia non viene aggiunta da un'antenna ma ridistribuita per fornire più potenza irradiata in una data direzione di quella trasmessa da un'antenna omnidirezionale (isotropica). Se un'antenna ha un guadagno maggiore di 1 in una determinata direzione, deve avere un guadagno minore di 1 in altre direzioni, poiché l'energia è conservata dall'antenna.
- **Direttività:** Forma del motivo di trasmissione. Se il guadagno dell'antenna aumenta, l'area di copertura diminuisce. L'area di copertura o il modello di radiazione è misurato in gradi. Questi angoli sono misurati in gradi e sono chiamati larghezze di raggio.**Nota:** la larghezza del raggio è definita come una misura della capacità di un'antenna di focalizzare l'energia del segnale radio verso una particolare direzione nello spazio. L'ampiezza del fascio è generalmente espressa in gradi HB o in larghezza del fascio orizzontale, generalmente il più importante con VB come modello di radiazione dell'ampiezza del fascio verticale (su e giù). Quando si visualizza un plottaggio o un pattern dell'antenna, l'angolo viene in genere misurato in punti di mezza potenza (3 dB) del lobo principale quando si fa riferimento alla potenza irradiata effettiva del picco del lobo principale.
- **Polarizzazione:** L'orientamento del campo elettrico dell'onda elettromagnetica attraverso lo spazio. Le antenne possono essere polarizzate orizzontalmente o verticalmente, sebbene siano disponibili altri tipi di polarizzazione. Entrambe le antenne in un collegamento devono avere la stessa polarizzazione per evitare ulteriori perdite di segnale indesiderate. Al fine di migliorare le prestazioni, un'antenna può talvolta essere ruotata per alterare la polarizzazione e quindi ridurre l'interferenza. Una regola generale è che la polarizzazione verticale è preferibile per inviare onde RF su canyon di cemento, e la polarizzazione orizzontale è generalmente preferibile per la distribuzione ad ampio raggio. La polarizzazione può anche essere sfruttata per ottimizzare il bleed-over RF quando è importante ridurre l'energia RF alle strutture adiacenti. La maggior parte delle antenne omnidirezionali è dotata di polarizzazione verticale come impostazione predefinita. L'energia radio irradiata da un'antenna è chiamata EIRP (Effective Isotropic Radiated Power). Il valore EIRP è generalmente espresso in Watt o dBm. Al fine di consentire una condivisione equa ed equa della banda non autorizzata, i domini normativi impongono livelli massimi di EIRP. Poiché l'EIRP è una misura della potenza in uscita dell'antenna, l'EIRP deve includere il guadagno dell'antenna e la perdita del cavo insieme alla potenza in uscita del trasmettitore. I cavi dell'antenna possono causare perdite e quindi attenuare il segnale trasmesso. Più lungo è il cavo, maggiore è l'attenuazione e maggiore è la perdita di segnale nel cavo, che influisce sia sulla potenza di ricezione che su quella di trasmissione. L'attenuazione del cavo dipende dal tipo e dal produttore. Il cavo a bassa perdita è in genere di circa 6,7 dB per 30 m a 2,4 GHz.

## [Attenuazione del segnale](#)

L'attenuazione o la perdita del segnale si verificano quando un segnale RF passa attraverso un



supporto. L'attenuazione del segnale varia in base al tipo di materiale attraverso cui passa un segnale. **La tabella 2** fornisce i valori di perdita del segnale per vari oggetti.

**Tabella 2. Valori di attenuazione del segnale attraverso vari oggetti**

Oggetto nel percorso del segnale	Attenuazione del segnale attraverso l'oggetto
Parete in cartongesso	3 dB
Parete in vetro con struttura in metallo	6 dB
Muro a blocchi	4 dB
Finestra di Office	3 dB
Porta in metallo	6 dB
Porta in metallo nel muro di mattoni	12 dB
Corpo umano	3 dB

**Nota:** si tratta solo di una guida approssimativa; diversi paesi hanno diversi regolamenti edilizi. I diversi regolamenti si applicano al livello massimo di EIRP consentito, nonché ad altri parametri.

Una potenza di trasmissione di 20 mW equivale a 13 dBm. Se la potenza trasmessa al punto di ingresso di una parete di cartongesso è di 13 dBm, la forza del segnale è ridotta a 10 dBm quando esce da tale parete.

I sondaggi condotti in diversi tipi di strutture mostrano diversi livelli di distorsione multipath, perdita di segnale e rumore del segnale. Gli ospedali sono in genere gli ambienti più difficili da sorvegliare a causa dell'elevata distorsione multipath, delle perdite di segnale e del rumore del segnale. Gli ospedali generalmente impiegano più tempo per effettuare i controlli e probabilmente richiedono una popolazione più densa di punti di accesso. Produzione e officine sono anche ambienti difficili in cui condurre indagini in loco. Questi siti generalmente hanno un elevato contenuto di metallo nella loro struttura di edifici che produce segnali riflessi che ricreano la distorsione multipath. Gli edifici adibiti a uffici e le strutture ricettive generalmente hanno un'elevata attenuazione del segnale ma un minore grado di distorsione multipath. L'unico modo per determinare la distanza percorsa da un segnale RF in un determinato ambiente è condurre una corretta indagine del sito.

**Nota:** è importante prendere in considerazione il livello del segnale Rx sull'access point e i dispositivi tracciati e non tanto quello del client che raccoglie i dati del sondaggio del sito. Una buona regola pratica consiste nell'impostare i punti di accesso su un'alimentazione relativamente alta, ad esempio 50 mW, quando si esegue un'indagine in loco. Poiché la maggior parte delle antenne hanno caratteristiche Tx/Rx simmetriche, i modelli di copertura risultanti riflettono l'RSSI approssimativo degli access point

## [Sorveglianza di edifici a più piani, ospedali e magazzini](#)

Esistono numerosi fattori di cui è necessario tenere conto quando si esaminano gli edifici a più piani, gli ospedali e i magazzini.

È importante trovare il maggior numero possibile di dettagli relativi alla costruzione dell'edificio. Alcuni esempi di metodi e materiali di costruzione tipici che influenzano la gamma e l'area di copertura dei punti di accesso includono film metallici su vetri di finestre, vetro al piombo, pareti con chiodi di acciaio, pavimenti in cemento e pareti con rinforzo in acciaio, isolante a base di

lamine, pozzi per scale e alberi elevatori, tubi idraulici e attrezzature, e molti altri. Inoltre, diversi tipi e livelli di inventario possono influire sulla gamma RF, in particolare quelli con elevato contenuto di acciaio o acqua. Tra gli elementi da tenere in considerazione vi sono carta per la stampante, scatole di cartone, cibo per animali domestici, vernice, prodotti petroliferi, parti di motori e così via. Assicurarvi che l'indagine del sito venga eseguita ai massimi livelli di inventario o nei periodi di massima attività. Un magazzino con un livello di stoccaggio del 50% visualizza un ingombro RF molto diverso rispetto allo stesso impianto completamente occupato.

Analogamente, un'area ufficio non popolata ha un'impronta RF diversa rispetto alla stessa area quando è occupata. Anche se molte parti dell'indagine possono essere condotte senza una piena occupazione, è essenziale condurre la verifica del sito e regolare i valori chiave in un momento in cui le persone sono presenti e l'attività normale ha luogo.

Più elevati sono i requisiti di utilizzo e maggiore è la densità degli utenti, più importante è disporre di una soluzione Diversity ben progettata. Quando sono presenti più utenti, vengono ricevuti più segnali sul dispositivo di ogni utente. Segnali aggiuntivi causano più contesa, più punti nulli e più distorsione multipath. La diversità dell'antenna sul punto di accesso contribuisce a ridurre al minimo queste condizioni.

Quando si esegue un sondaggio in un sito per un tipico edificio con uffici a più piani, tenere presenti le seguenti linee guida:

- Gli alberi di ascensore bloccano e riflettono i segnali RF.
- Le sale di fornitura con l'inventario assorbono i segnali RF.
- Gli uffici interni con pareti impenetrabili assorbono i segnali RF.
- Le sale di pausa (cucine) possono produrre interferenze di 2,4 GHz causate dai forni a microonde.
- I laboratori di test possono produrre interferenze a 2,4 GHz o 5 GHz. Il problema dell'interferenza è che aumenta la soglia del rumore e diminuisce il rapporto SNR (segnale/rumore) del segnale ricevuto. Una soglia di rumore più elevata riduce l'intervallo effettivo degli access point.
- Le postazioni ufficio tendono ad assorbire e bloccare i segnali.
- Finestre di classe e partizioni riflettono e bloccano i segnali RF.
- Le piastrelle da bagno possono assorbire e bloccare i segnali RF.
- Le sale conferenze richiedono un'elevata copertura AP in quanto sono un'area di utilizzo Wi-Fi molto ampia.

Quando si esaminano le strutture a più piani, i punti di accesso su diversi piani possono interferire tra loro con la stessa facilità con cui si trovano sullo stesso piano. Questo può essere utile per le distribuzioni voce e/o dati, ma causa problemi quando si distribuisce Context Aware. La separazione del pavimento è fondamentale per il corretto funzionamento di questa soluzione. Negli edifici multi-tenant, ci possono essere problemi di sicurezza che richiedono l'uso di una minore potenza di trasmissione e antenne di guadagno inferiore per mantenere i segnali fuori dalle stanze o uffici vicini. Il processo di indagine di un ospedale è molto simile a quello di un'azienda, ma la struttura di una struttura ospedaliera tende a differire nei seguenti modi:

- Gli edifici ospedalieri hanno spesso progetti di ricostruzione e aggiunte ricorrenti. Ogni costruzione aggiuntiva può richiedere diversi materiali di costruzione con diversi livelli di attenuazione del segnale.
- La penetrazione del segnale attraverso pareti e pavimenti nelle aree dei pazienti è in genere minima, il che aiuta a creare micro-cellule. Di conseguenza, la densità dei punti di accesso deve essere molto più alta per garantire una sufficiente copertura RF.

- La necessità di larghezza di banda aumenta con l'aumento dell'uso di apparecchiature WLAN a ultrasuoni e di altre applicazioni di imaging portatili.
- A causa della necessità di una maggiore densità AP, la sovrapposizione delle celle può essere elevata, con conseguente riutilizzo del canale.
- Negli ospedali è possibile installare diversi tipi di reti wireless, incluse le apparecchiature da 2,4 GHz non 802.11. Questa apparecchiatura può causare il conflitto con altre reti a 2,4 GHz o 5 GHz.
- Le antenne patch di diversità montate a parete e le antenne omnidirezionali di diversità montate a soffitto sono popolari, ma tenete presente che la diversità è richiesta.

I magazzini dispongono di ampie aree aperte, che spesso contengono rack di storage elevati. Molte volte questi rack raggiungono quasi il soffitto, dove in genere vengono posizionati i punti di accesso. Tali rack di storage possono limitare l'area che il punto di accesso può coprire. In questi casi, è consigliabile posizionare gli access point in altri punti oltre al soffitto, ad esempio pareti laterali e pilastri di cemento. Quando si esamina un magazzino, tenere in considerazione anche i seguenti fattori:

- I livelli di magazzino influiscono sul numero di punti di accesso necessari. Copertura di prova con due o tre access point in posizioni stimate.
- Sovrapposizioni di celle impreviste sono probabilmente dovute a variazioni di copertura. La qualità del segnale varia più della forza del segnale. I client possono associarsi e operare meglio con i punti di accesso più lontani rispetto ai punti di accesso vicini.
- Durante un sondaggio, i punti di accesso e le antenne in genere non dispongono di un cavo antenna che li connetta, ma in un ambiente di produzione, il punto di accesso e l'antenna possono richiedere cavi antenna. Tutti i cavi dell'antenna hanno perdita di segnale. Il sondaggio più accurato include il tipo di antenna da installare e la lunghezza del cavo da installare. Un buon strumento da usare per simulare il cavo e la sua perdita è un attenuatore in un kit di indagine.

Quando si fa un'indagine su uno stabilimento di produzione, è simile alla sorveglianza di un magazzino. Una differenza chiave è che l'ambiente RF è molto più rumoroso in un impianto di produzione a causa di molte più fonti di interferenza RF. Inoltre, le applicazioni in una struttura di produzione richiedono in genere una larghezza di banda maggiore rispetto alle applicazioni utilizzate in un ambiente di magazzino. Queste applicazioni possono includere immagini video e voce wireless. La distorsione a percorsi multipli è probabilmente il problema di prestazioni più grave in un impianto di produzione.

È importante che l'indagine del sito non solo misuri i livelli del segnale, ma generi anche pacchetti e segnali gli errori dei pacchetti per caratterizzare correttamente l'ambiente RF.

Per le aree in cui il traffico degli utenti è elevato, come uffici, scuole, negozi e ospedali, Cisco consiglia di posizionare il punto di accesso fuori dalla vista e antenne discrete sotto il soffitto.

## [Guide e aree geografiche](#)

Le linee guida per l'installazione fornite offrono un buon livello di precisione: 10/90%, 5/50%. Il valore 10m/90% corrisponde a un raggio di 10m dalla posizione fisica effettiva di un dato dispositivo, quindi ci saranno casi in cui questi obiettivi di precisione vengono raggiunti, ma il dispositivo che viene tracciato può apparire in aree a livello di pavimento e/o di edificio dove i dispositivi non possono essere presenti.

La funzionalità Guide e aree offre agli amministratori di rete un meccanismo per definire aree di

inclusione/esclusione per i servizi di posizione. Questa funzionalità consente di definire aree specifiche di una mappa all'interno o all'esterno dell'ambito di un'area di posizione valida.

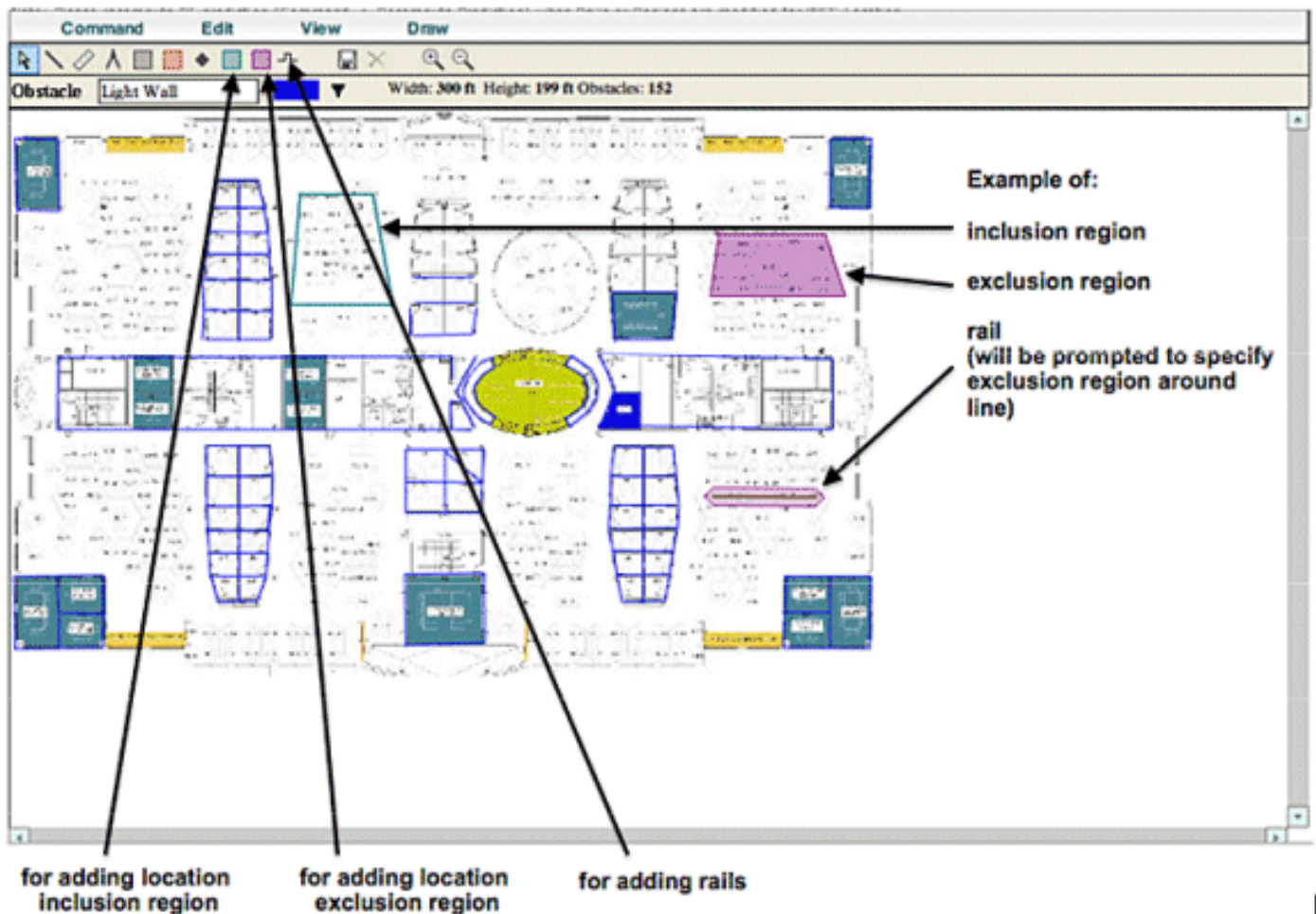
È possibile specificare tre tipi di regioni, come mostrato nella **Figura 14**:

- **Area inclusione ubicazione:** il dispositivo tracciato non può trovarsi all'esterno di questo poligono (esempio: all'esterno delle pareti esterne dell'edificio)
- **Area di esclusione ubicazione:** il dispositivo tracciato non può trovarsi all'interno di questo poligono (esempi: l'atrio aperto o gli ostacoli agli edifici). L'esclusione è privilegiata rispetto all'inclusione nel caso in cui vengano individuate regioni in conflitto.
- **Guide:** il dispositivo monitorato deve trovarsi all'interno di un'area definita con banda stretta, generalmente utilizzata all'interno dell'area di esclusione (ad esempio: nastro trasportatore).

Dopo aver definito le aree Rails e Region in WCS, è necessario eseguire il push dell'aggiornamento da WCS a MSE tramite il processo di sincronizzazione.

**Nota:** su MSE, Location Rails e Regions funzionano solo con Context Aware Engine per client. AeroScout ha implementato una funzionalità denominata Celle e maschere che fornisce funzionalità simili quando si tiene traccia dei tag. Per Cisco 2710 Location Appliance, la funzionalità Rails e Regions funziona sia con il client sia con il tag tracking.

**Figura 14: Guide e regioni**

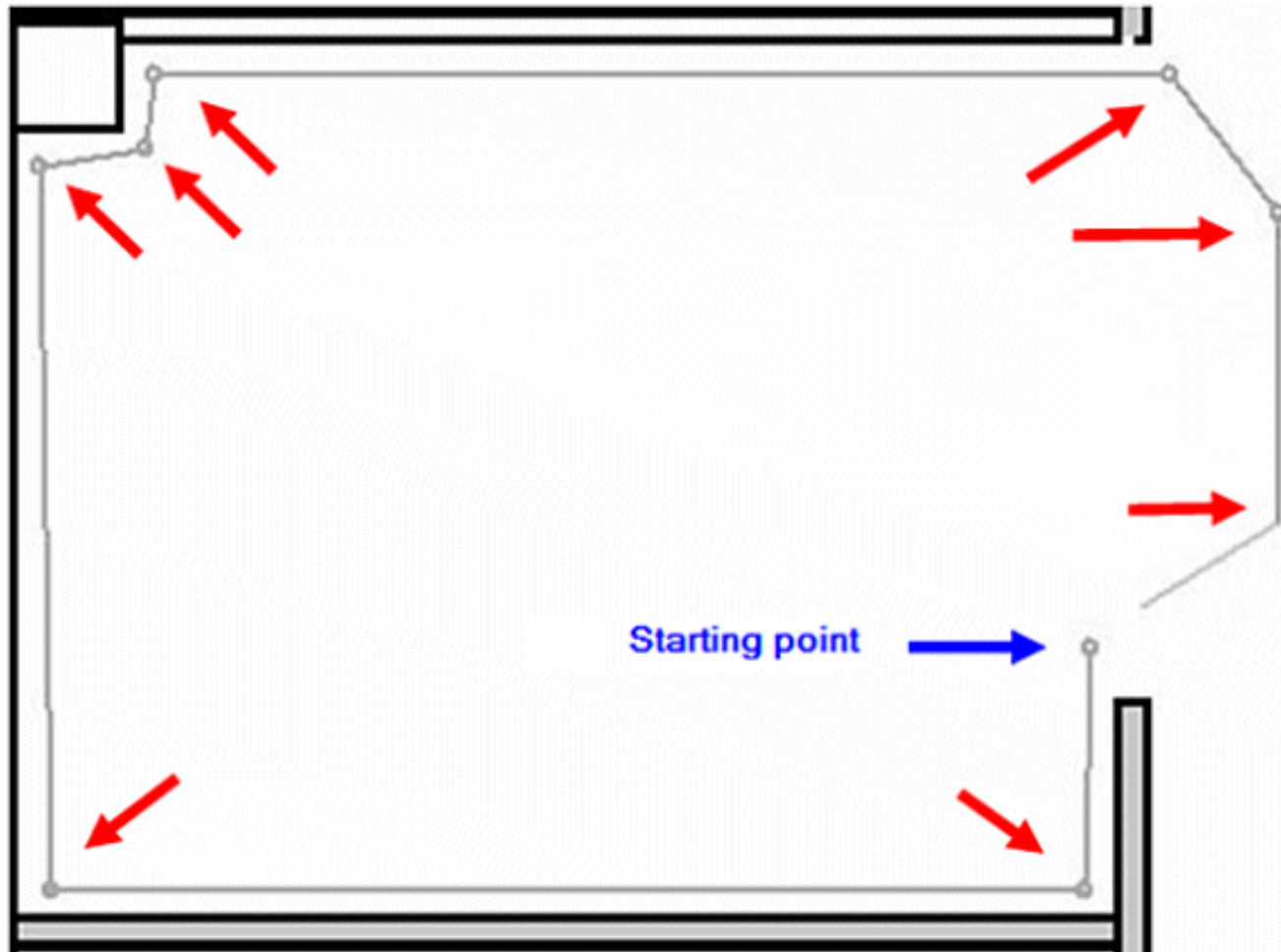


## [Creare una maschera in System Manager](#)

Una maschera viene definita disegnando un poligono su una mappa che delimita l'area da escludere.

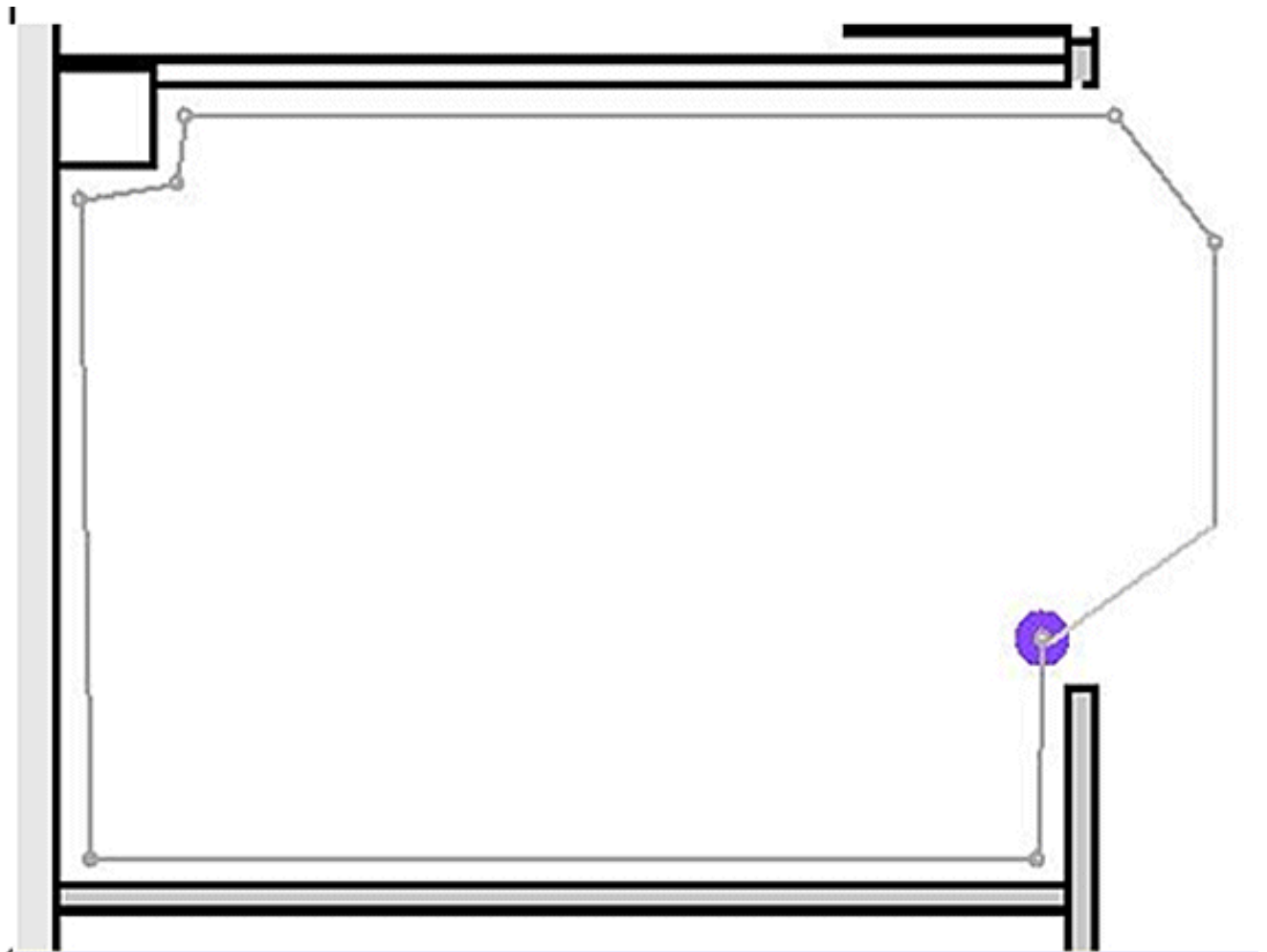
Per creare una maschera, effettuare le seguenti operazioni:

1. Selezionare **Configurazione, Mappe, Maschera e Modifica maschera**. Il sistema passa alla modalità di modifica maschera. Il puntatore del mouse si trasforma in una croce.
2. Fare clic su un punto della mappa. far scorrere il mouse fino al punto successivo, fare di nuovo clic e ripetere questa procedura per contrassegnare i vertici del poligono (vedere la Figura 15).

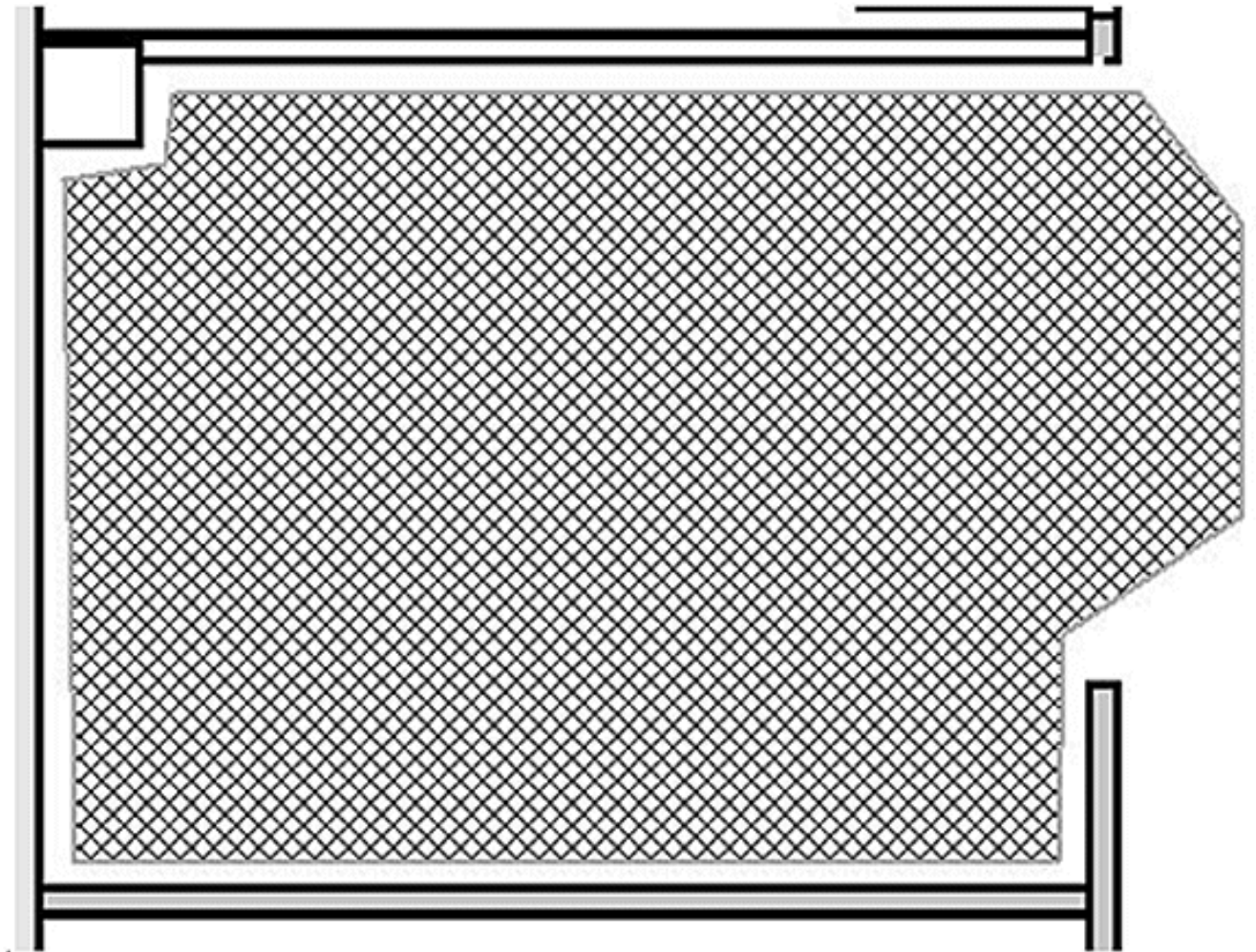


Quando si fa scorrere il mouse fino al punto iniziale, per chiudere il poligono viene visualizzato un cerchio viola che indica il punto di chiusura (vedere la Figura 16).

**Figura 16: Creazione di una maschera - Cerchio viola che indica il punto di chiusura**



Fate clic su [per completare la definizione della maschera](#). La maschera viene visualizzata sulla mappa (vedere la [Figura 17](#)).**Figura 17: Creazione di una maschera - La maschera viene visualizzata sulla mappa**



3. Fare clic con il pulsante destro del mouse in un punto qualsiasi della mappa e scegliere **Esci da modalità di disegno maschera** (o premere **ESC**) per uscire dalla modalità di modifica della maschera. Per impostazione predefinita, la maschera viene rimossa dalla visualizzazione dopo essere uscita dalla modalità di disegno della maschera. Inoltre, per abilitare / disabilitare o modificare le maschere, consultare la [documentazione di Aeroscout](#) per ulteriori informazioni.

### [Celle nel motore sensibile al contesto per i tag](#)

Le celle sono progettate per dividere una mappa in porzioni più piccole al fine di ottimizzare il processo di calcolo della posizione e migliorare la precisione del posizionamento. La cella definisce i limiti geografici per il posizionamento di un tag. Definisce inoltre quali dispositivi specifici (ricevitori e punti di accesso TDOA) partecipano al processo di calcolo della posizione entro tali limiti.

Il meccanismo di cella viene utilizzato per i calcoli di posizione RSSI e TDOA.

Il modulo di gestione elabora i dati di posizione in ingresso:

- Un report che indica la posizione di un tag può provenire da più punti di accesso o ricevitori TDOA Wi-Fi contemporaneamente. Gli algoritmi di differenziazione delle mappe del motore scelgono la mappa in cui è più probabile che si trovi il dispositivo e ignorano i report di posizione che puntano ad altre mappe.
- Una volta determinata la mappa, il motore cerca le celle. Se la mappa è suddivisa in celle, lo stesso meccanismo di ottimizzazione sceglie la cella dei ricevitori/punti di accesso TDOA di

quelli che probabilmente hanno fornito il report di posizione più accurato. La posizione del dispositivo viene quindi calcolata in base ai dati ricevuti dai ricevitori/punti di accesso TDOA associati a tale cella e all'interno dei limiti di tale cella.

I ricevitori/punti di accesso TDOA associati a una cella non devono necessariamente trovarsi all'interno dell'area delimitata dai limiti della cella.

## [Operazione iniziale per la configurazione delle celle](#)

Inizialmente, per ogni mappa viene creata automaticamente una cella predefinita che copre l'intera area della mappa. Per dividere la mappa in celle separate, eseguire le operazioni seguenti:

1. Modificate la cella di default in modo che copra solo un sottoinsieme dell'area mappa (consultate le istruzioni per modificare una cella).
2. Aggiungere altre celle alla mappa in base alle esigenze. Si noti che una cella non può essere inclusa completamente in un'altra cella.
3. Esaminare le proprietà di ciascun dispositivo di posizione (punti di accesso e ricevitori TDOA) e associare il dispositivo alle celle appropriate.
4. Le periferiche associate di una cella non possono essere un sottoinsieme delle periferiche associate di un'altra cella. Verificare che a ogni cella siano associate periferiche non associate ad altre celle.

## [Taratura - Motore sensibile al contesto per client](#)

La precisione della posizione dipende da due fattori principali:

- Posizione AP e numero di AP che contribuiscono alla posizione
- Corrette caratteristiche del segnale RF di un punto di accesso per un determinato ambiente (mappe di calore accurate del punto di accesso)

Durante la fase di calibrazione, i dati vengono raccolti sul server WCS quando viene eseguita una procedura di approssimazione dell'ambiente di destinazione con un dispositivo mobile che consente a più punti di accesso di campionare la potenza del segnale di questo dispositivo. Il metodo consigliato consiste nell'utilizzare uno o più notebook collegati al sistema WCS (massimo cinque dispositivi per banda radio) e scegliere una mappa dell'area da calibrare, che in genere viene sovrapposta a una serie di punti di griglia o notazioni per guidare l'operatore a determinare con precisione dove devono essere acquisiti i dati campione. In ciascun punto di esempio della mappa, il WLC inoltra al MSE l'insieme di valori RSSI associati al dispositivo di calibrazione. La dimensione di un dato set di dati si basa sul numero di punti di accesso riceventi che rilevano il dispositivo mobile. A causa della dissolvenza e di altre caratteristiche dell'ambiente RF, la potenza del segnale osservato di un dispositivo mobile in una particolare posizione è una variante di tempo, ovvero può cambiare nel tempo. Di conseguenza, molti campioni di dati vengono registrati per un dispositivo di calibrazione nell'ambito del processo di calibrazione.

Ogni ambiente è univoco e le caratteristiche del segnale di un punto di accesso in un determinato ambiente variano notevolmente. WCS fornisce un meccanismo che consente all'utente di calibrare le caratteristiche del segnale per il proprio ambiente. Il primo passo per ottimizzare l'accuratezza consiste nel garantire che l'installazione dell'access point sia conforme alle linee guida per l'installazione dei percorsi riepilogate. Un tentativo di migliorare la precisione della posizione con la calibrazione con una copertura e un posizionamento inadeguati dei punti di accesso potrebbe non fornire risultati adeguati e può persino essere dannoso per la precisione.



Con il sistema WCS vengono forniti tre modelli di calibrazione predefiniti:

- Cubi e uffici con pareti
- Solo ufficio
- Spazio aperto esterno

Ciascun modello è basato sui fattori più comuni di un ambiente tipico del cliente. Il primo di questi due modelli RF è utile nel normale ambiente di lavoro.

Se i modelli RF forniti non caratterizzano sufficientemente la disposizione del pavimento, è possibile creare modelli di calibrazione con WCS e applicarli al pavimento per rappresentare meglio le caratteristiche di attenuazione di un determinato ambiente. Negli ambienti in cui molti pavimenti condividono le stesse caratteristiche di attenuazione, è possibile creare un modello di calibrazione da applicare a tutti i pavimenti simili.

Alcuni ambienti interni possono avere un'attenuazione maggiore rispetto a quella che si trova in un tipico ambiente di ufficio. Nelle installazioni interne correttamente progettate, dove una maggiore attenuazione può contribuire a una precisione di posizionamento inferiore a quella ottimale, una calibrazione del sito può aiutare a ripristinare prestazioni non ottimali. Quando viene eseguita una calibrazione in loco, il sistema è autorizzato a campionare le perdite di percorso da punti noti in tutto l'ambiente, il che consente di formulare un modello di RF personalizzato che fornisce una migliore comprensione delle caratteristiche di propagazione specifiche di quell'ambiente.

In molti casi, l'utilizzo delle informazioni raccolte durante la calibrazione al posto di un modello predefinito può ridurre notevolmente l'errore rilevato tra la posizione del client calcolata e i dati empirici. In ambienti in cui molti pavimenti condividono caratteristiche di attenuazione quasi identiche, le forti somiglianze tra queste posizioni consentono di applicare il modello RF creato dalla calibrazione eseguita su una qualsiasi delle posizioni ad altre aree simili con buoni risultati.

Devono essere prese in considerazione anche le aree con attenuazione di radiofrequenza mista, ovvero i magazzini o i fabbricati in cui possono essere presenti merci impilate o ostruzioni ad alta densità in un'area dell'edificio e/o spazi aperti utilizzati per l'assemblaggio o la spedizione. Tali aree devono essere trattate come zone indipendenti che limitano la calibrazione alle aree in cui è richiesta la massima accuratezza. Se è richiesta la massima precisione per tutte queste zone in un'area mista, è consigliabile suddividere l'area del pavimento in singole celle o mappe e applicare modelli di RF separati.

**Nota:** le prestazioni di questo tipo di modellazione RF sono complesse e richiedono ulteriori considerazioni sulla distribuzione, che esulano dall'ambito di questo documento.

La calibrazione è in realtà un processo in più fasi che inizia con la definizione di un nuovo modello di calibrazione tramite **Monitor > Mappe > Modelli di calibrazione RF > Crea nuovo modello**. Per una descrizione dettagliata del processo di calibrazione, fare riferimento a *Creazione e applicazione di modelli di calibrazione* nella [Guida alla configurazione del software sensibile al contesto di Cisco](#).

Durante il processo di calibrazione, il client di calibrazione trasmette ripetutamente le richieste di sonda su tutti i canali. A seconda del client di calibrazione utilizzato, il client può essere attivato per trasmettere richieste di sonda su richiesta tramite una richiesta di rete. I client che non sono in grado di riconoscere queste richieste possono essere deautenticati e dissociati per fare in modo che inviino richieste di richiesta alla rete wireless e successivamente riassocino/riautenticano. I punti di accesso nelle vicinanze del client rilevano l'RSSI di queste richieste di sonda e passano queste informazioni ai loro controller registrati. I controller forniscono le informazioni RSSI rilevate

nel processo di calibrazione al sistema WCS per l'utilizzo nel calcolo delle perdite di percorso utilizzate per definire il nuovo modello di calibrazione.

Quando si crea un modello di calibrazione, il passaggio critico consiste nel raccogliere i punti dati. La fase di raccolta dei punti dati del processo di calibrazione nel sistema WCS può essere eseguita con uno dei due metodi. Può essere eseguito da un singolo dispositivo mobile abilitato per il Web associato alla WLAN, che controlla sia il probe della rete sia la raccolta dei dati effettivi. In alternativa, la fase di raccolta dei dati può essere eseguita da due dispositivi separati associati all'infrastruttura WLAN. In questo caso, l'interazione con l'interfaccia utente grafica di Sistema colori Windows viene controllata da un dispositivo primario dotato di funzionalità di tastiera e mouse, mentre la generazione effettiva di richieste di verifica si verifica su un secondo dispositivo associato quando si sceglie il relativo indirizzo MAC noto.

Si raccomanda di raccogliere i dati di taratura per ciascuna banda. Quando si utilizza un client dual band, utilizzare una delle alternative seguenti:

1. Eseguire la raccolta dei dati di calibrazione con un singolo notebook dotato di adattatore Cisco Aironet 802.11a/b/g Wireless CardBus (AIR-CB21AG) su ciascuna banda singolarmente. Quando si esegue un esercizio di calibrazione per la banda a 2,4 GHz, disattivare la banda a 5 GHz e completare la raccolta dei dati solo con la banda a 2,4 GHz. Al termine del processo di calibrazione, disabilitare la banda a 2,4 GHz, abilitare la banda a 5 GHz e ripetere il processo di raccolta dei dati di calibrazione con la banda a 5 GHz. **Nota:** in un ambiente di produzione in cui risulta difficile scegliere la banda radio del PC, è preferibile definire un SSID di calibrazione specifico con solo 11b/g o 11a attivi.
2. Eseguire la calibrazione con un massimo di cinque client per banda radio, ciascuno dotato di notebook. Ogni notebook deve disporre di un Cisco AIR-CB21AG ed essere associato all'infrastruttura con una banda dedicata. Ogni client di calibrazione può funzionare in modo indipendente.

Prima di eseguire una calibrazione, è necessario eseguire diverse operazioni preliminari alla configurazione:

1. In un ambiente di produzione, informare il personale o i lavoratori del processo. Ciò riduce le interruzioni e garantisce un maggiore livello di accuratezza. Ridurre il rischio di incidenti soprattutto negli impianti di produzione in cui sono in funzione carrelli elevatori a forca.
2. Disabilitare la modalità di alimentazione dinamica del punto di accesso RM sui controller o sui punti di accesso in cui si esegue la calibrazione.
3. Verificare che le mappe sul sistema WCS siano in scala e che i punti di accesso siano stati posizionati correttamente con l'orientamento e l'altezza corretti per il tipo di antenna.
4. Il PC o il dispositivo utilizzato per la taratura è associato a un punto di accesso situato sulla MAPPA in questione.
5. Il client wireless utilizzato per la calibrazione deve essere almeno CCXv2. Cisco consiglia CCXv4 per ottenere risultati ottimali. Le informazioni sulla versione CCX per i client possono essere visualizzate in WCS (vedere la **Figura 18**). **Figura 18: Verifica della versione CCX dei client**

## Client Details : Client 'Unknown' - Intel:73:22:e3

Monitor > [Clients](#) > Client Details

Properties			
Client User Name	<Unknown>	Controller	<a href="#">171.71.128.78</a>
Client IP Address	128.107.21.101	Port	2
Client MAC Address	00:1d:e0:73:22:e3	Protocol	<a href="#">802.11g</a>
Client Vendor	Intel	SSID	guestnet
CCX	V4	Profile Name	guestnet
Power Save	OFF	AP Name	<a href="#">sjc14-41b-ap4</a>
		AP IP Address	<a href="#">171.71.133.127</a>
		AP Type	Cisco AP
		AP Base Radio MAC	00:17:df:a8:59:40
		Interface	guest
		VLAN ID	240

6. Non utilizzare Cisco Secure Services Client (CSSC) per eseguire la calibrazione.
7. È necessario raccogliere almeno 50 punti di dati su una piantina.
8. Dopo aver creato il modello di calibrazione e aver applicato questo modello alle mappe di base, è necessario sincronizzare WCS con MSE.

Nel caso di edifici a più piani, la raccolta dei dati di taratura deve essere effettuata su un piano alla volta. Poiché esiste la possibilità che un client di calibrazione possa vedere ed essere visto dai punti di accesso su pavimenti adiacenti a causa di sanguinamento RF tra i pavimenti, la raccolta dei dati di calibrazione un piano alla volta riduce il rischio che il MSE mischi i dati di calibrazione tra i pavimenti.

Quando un client compatibile con CCXv2 o versione successiva viene associato all'infrastruttura WLAN e specificato come client di calibrazione in WCS, l'indirizzo MAC del client viene inserito nella tabella di calibrazione delle posizioni di tutti i controller che gestiscono i punti di accesso contenuti nel pavimento calibrato. Questo inserimento avviene inizialmente subito dopo che sono stati specificati l'indirizzo MAC del client di calibrazione, il campus di calibrazione, l'edificio e il piano. Dopo ogni salvataggio di un punto dati raccolto, l'indirizzo MAC del client viene rimosso dalla tabella di calibrazione della posizione del controller. L'indirizzo MAC del client viene quindi reinserito brevemente nelle tabelle di calibrazione della posizione del controller a ogni successivo salvataggio del datapoint e subito dopo rimosso. Questo processo viene ripetuto per ogni coordinata raccolta.

Quando gli indirizzi MAC dei client CCXv2 (o superiori) vengono visualizzati nella tabella di calibrazione della posizione di un WLC, le richieste di misurazione radio unicast vengono inviate a questi client. Allo stesso modo in cui le richieste di misurazione della radio broadcast aiutano a migliorare la precisione della posizione dei client compatibili all'interno del normale funzionamento, le richieste di misurazione della radio unicast inviate a brevi intervalli regolari (4 secondi) causano la trasmissione frequente di richieste di sonda da parte dei client di calibrazione compatibili. L'uso di CCX Radio Measurement Requests e di CCXv2 o di client superiori consente di ottenere questo risultato senza dover forzare il client a dissociarsi e riassociare continuamente. Ciò consente un'esecuzione più coerente e affidabile della sonda della rete e un funzionamento più fluido del client di calibrazione, soprattutto se utilizzato come workstation che interagisce con WCS tramite l'interfaccia grafica di raccolta dei dati di calibrazione.

Al pavimento viene applicato un modello di calibrazione che rappresenta meglio le caratteristiche

di attenuazione del pavimento. Negli ambienti in cui molti piani condividono le stesse caratteristiche di attenuazione, è possibile creare un modello di calibrazione da applicare ai piani con lo stesso layout fisico e la stessa distribuzione.

I dati di taratura possono essere raccolti con uno dei due metodi seguenti:

- **Raccolta in modalità punto** — Si scelgono i punti di taratura e si calcola la loro area di copertura, un punto alla volta (vedere le **figure 19 e 20**).
- **Raccolta in modalità lineare**: viene scelta una serie di percorsi lineari che vengono calcolati quando si attraversa il percorso. Questo approccio è in genere più rapido rispetto alla raccolta dei punti dati. È inoltre possibile utilizzare la raccolta dei punti dati per aumentare la raccolta dei dati per le posizioni mancanti dai percorsi lineari (vedere la **Figura 21**).

Sebbene entrambi i metodi siano ufficialmente supportati, Cisco consiglia di utilizzare la modalità punto per la calibrazione, in quanto consente di ottenere i risultati migliori.

Figura 19: Taratura - Modalità punto

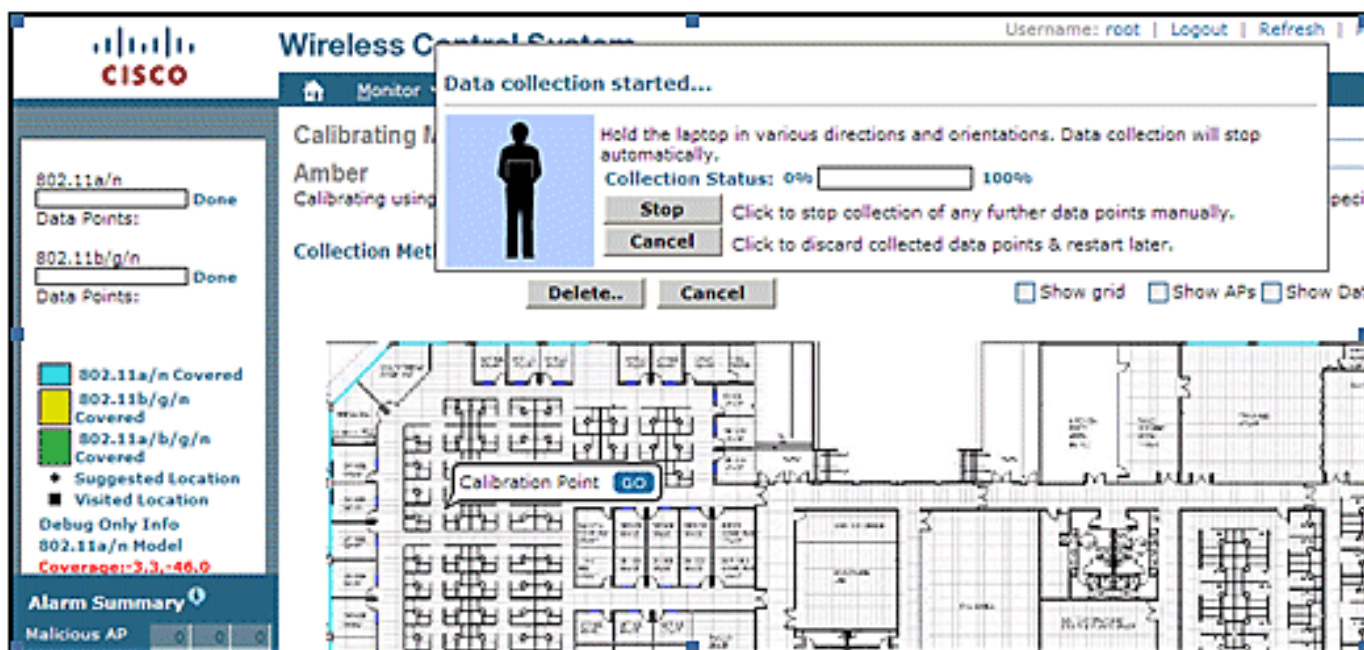


Figura 20: Modalità punto - Risultati calibrazione

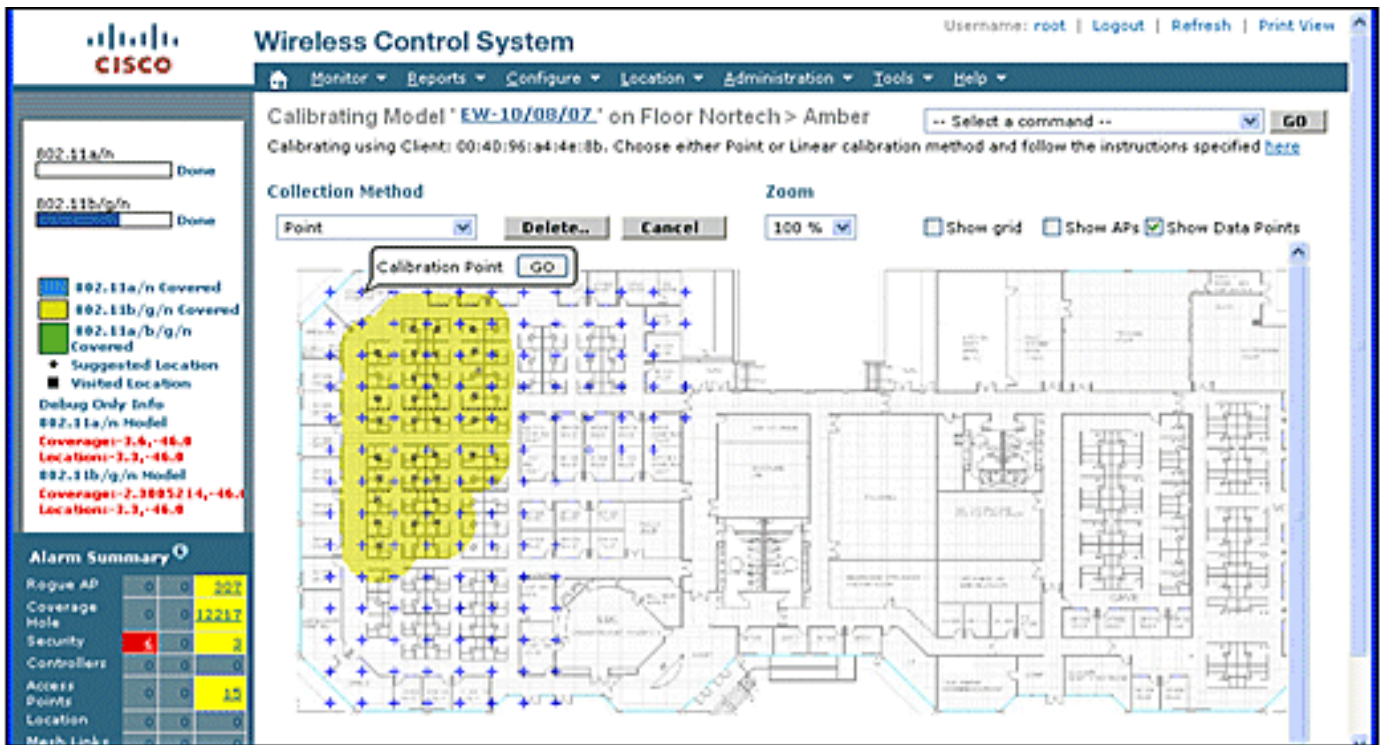
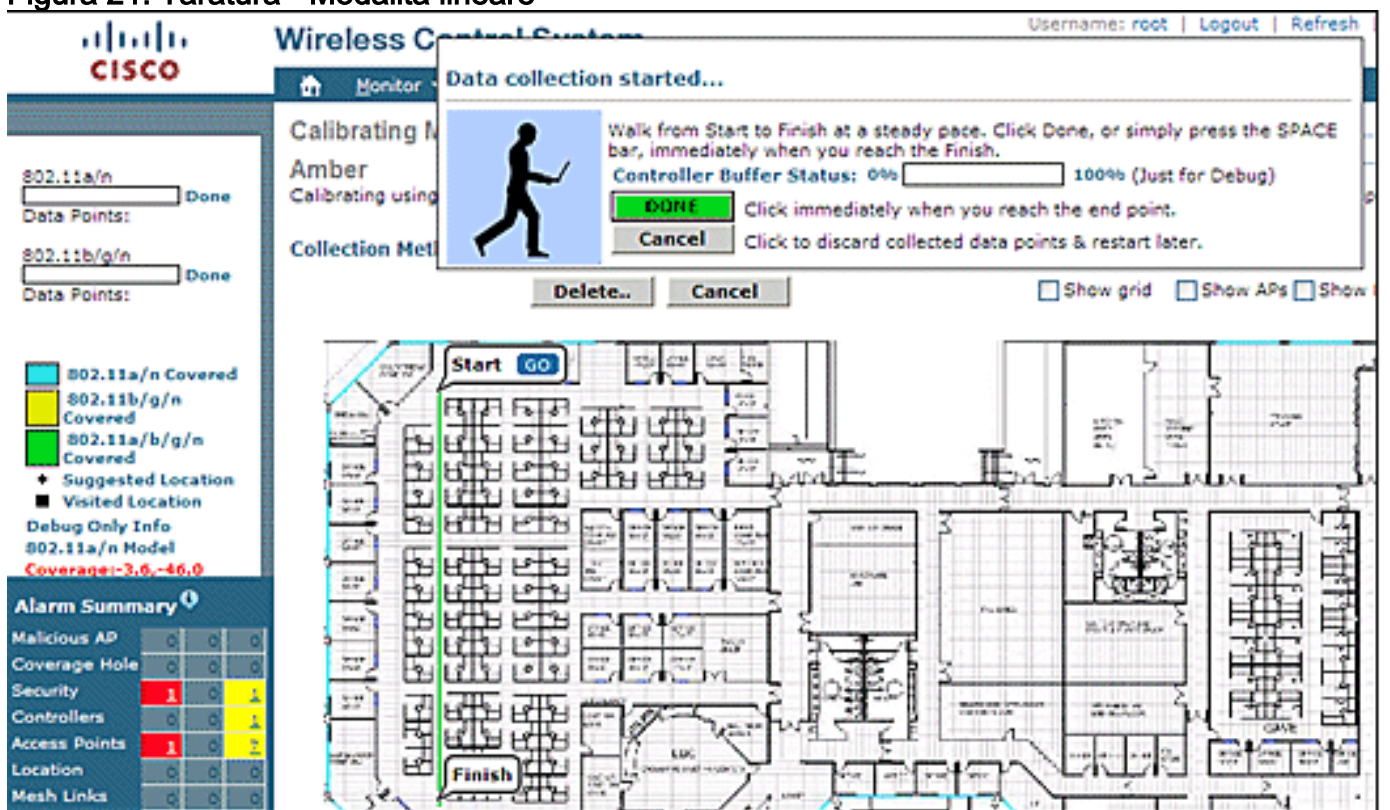


Figura 21: Taratura - Modalità lineare



I modelli di calibrazione possono essere applicati solo a client, client non autorizzati e punti di accesso non autorizzati. La taratura dei tag viene eseguita con AeroScout System Manager.

### Taratura - Motore sensibile al contesto per i tag

MSE dispone di due motori di posizione: uno per tenere traccia dei client (motore Cisco descritto nella sezione precedente) e uno per tenere traccia dei tag (AeroScout). Ogni motore ha un modello di calibrazione separato, quindi la calibrazione per i tag è un processo separato.

Il motore AeroScout utilizza il tipico modello di perdita di percorso RF predefinito di ufficio per tutte

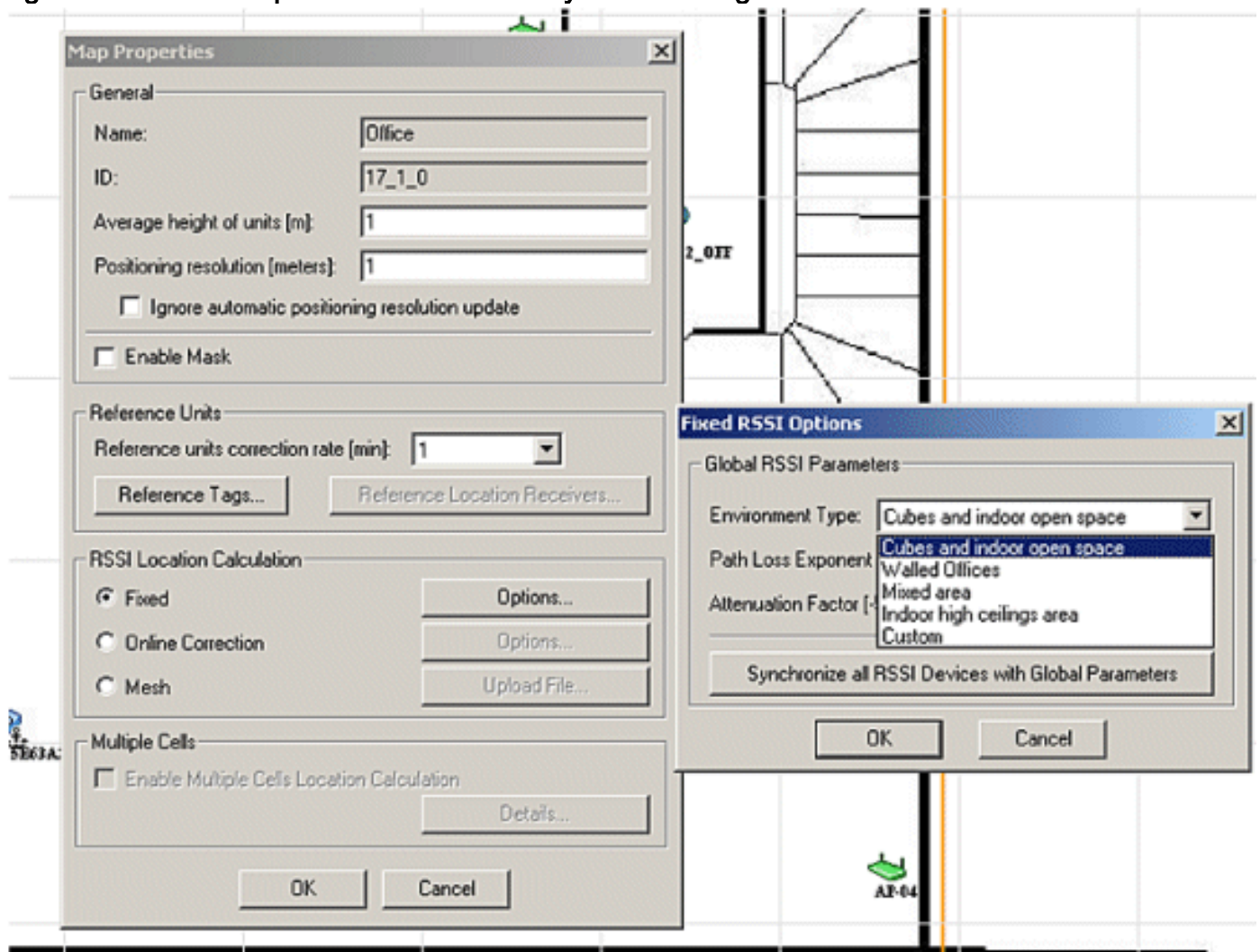
le mappe WCS importate. Se l'impostazione non rappresenta l'ambiente, è necessario apportare modifiche ai modelli di default per mappa e/o cella per migliorare la precisione della posizione.

**AeroScout System Manager:** per modificare le impostazioni predefinite di Path Loss Model (PLM), è necessario installare ed eseguire l'applicazione AeroScout System Manager. Per il download e l'installazione, consultare la [documentazione di AeroScout](#).

Dopo aver avviato l'applicazione, accedere al motore MSE e passare al piano delle mappe effettivo, che deve essere modificato. Utilizzare la scheda a discesa e selezionare **configurazione > Mappa > proprietà**. Le opzioni di calcolo della posizione RSSI possono essere utilizzate per scegliere il tipo di ambiente fisso appropriato alle specifiche fisiche rappresentate dai quattro modelli definiti mostrati nella **Figura 22**. Dopo aver scelto il modello, applicarlo al pavimento scelto. Utilizzare la scheda **OK** o l'opzione per **sincronizzare tutti i dispositivi RSSI con i parametri globali**, che consente di eseguire il push dello stesso modello a tutte le mappe esistenti come nuovo modello predefinito.

**Nota:** la quinta opzione, "Custom", deve essere utilizzata solo quando richiesto da AeroScout o dal supporto tecnico Cisco.

**Figura 22: Modelli disponibili in AeroScout Systems Manager**

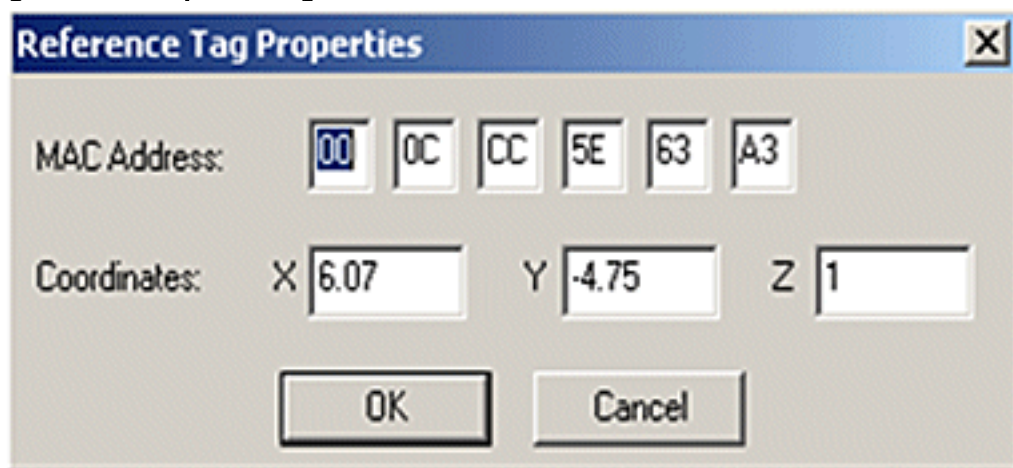


**Metodi di calibrazione** - Sono disponibili diverse opzioni con singoli tag come dispositivi di riferimento statici o se vengono eseguite registrazioni periodiche o una tantum, che possono essere utilizzate per analizzare e calcolare modelli precisi per mappa/cella.

**Etichette di riferimento:** sono etichette standard utilizzate per la registrazione delle risorse. L'unica differenza, se esistente, è la configurazione. Normalmente un tag di riferimento utilizza un periodo beacon più veloce per un intervallo di misurazione definito.

Le etichette di riferimento possono essere definite con l'indirizzo MAC, come mostrato nella **Figura 23**, e posizionate direttamente su una cella o mappa mostrata da un'etichetta ancorata blu. Le coordinate possono essere immesse manualmente facendo clic con il pulsante destro del mouse sulla mappa. Le etichette di riferimento utilizzate per l'adattamento dinamico della posizione devono essere attivate nella casella di selezione delle etichette di riferimento in **Proprietà mappa > Unità di riferimento** (vedere **Figura 22**). Questo metodo di calibrazione è descritto per la TDoA.

**Figura 23: Proprietà tag di riferimento**



Reference Tag Properties

MAC Address: 00 0C CC 5E 63 A3

Coordinates: X 6.07 Y -4.75 Z 1

OK Cancel



**Registrazione con un clic** - Un metodo di calibrazione più preferito è l'operazione di registrazione con un clic. Questo definisce uno o più gruppi di tag e li posiziona sulla mappa per un breve periodo di tempo preimpostato. Viene avviata una registrazione e i dati acquisiti vengono archiviati direttamente sul MSE in base all'indicatore orario e all'identificazione della mappa.

I migliori risultati si ottengono quando il gruppo di riferimento di etichette è disposto in ordine compatto montato su un piccolo cubo o un palo. È possibile riposizionare lo stesso gruppo e ripetere la procedura più volte sulla stessa mappa se si riposiziona il gruppo e si riavvia la registrazione con un clic del mouse. In alternativa, è possibile definire più gruppi sulla stessa mappa e registrarli in una sequenza.

**Figura 24: Strumenti AeroScout Systems Manager**

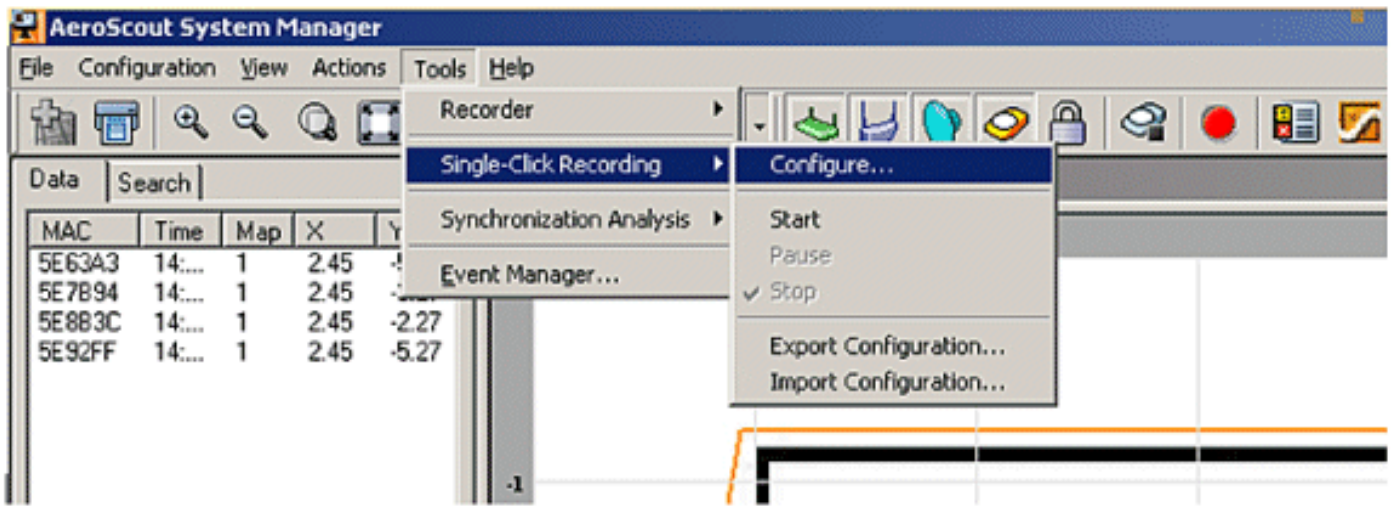
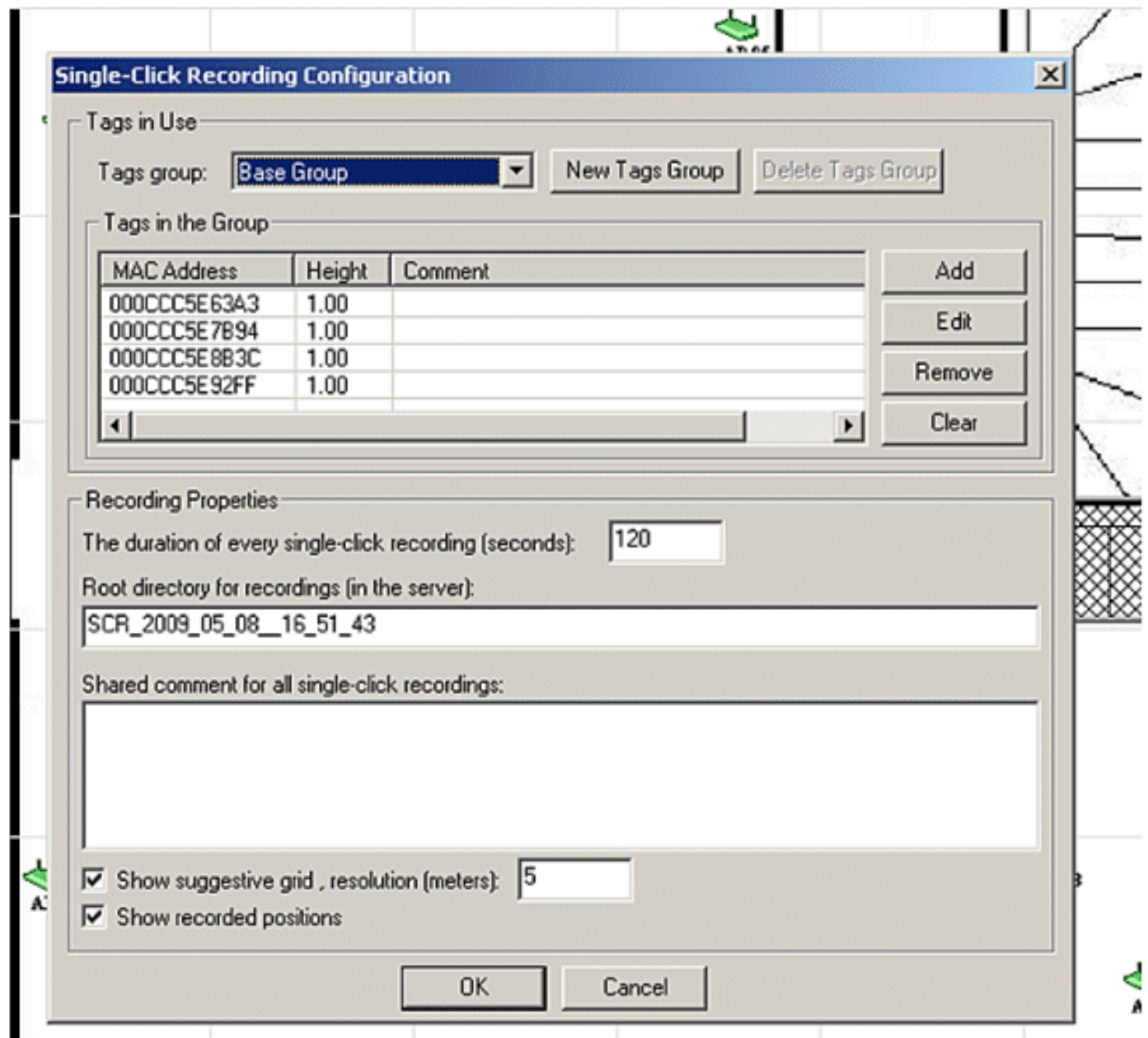


Figura 25: Configurazione registrazione con un clic



Per eseguire questo metodo, immettere le informazioni di configurazione in **Strumenti > Registrazione con un solo clic**, come mostrato nelle figure 24 e 25. Le proprietà di registrazione possono essere modificate se i valori predefiniti non sono appropriati. Le registrazioni vengono archiviate automaticamente in sottodirectory in base alla data e all'ora della registrazione.



**Analyzer Tool** - Prima di poter utilizzare i dati di registrazione con un clic per la calibrazione, è necessario visualizzarli e convertirli in un file Mesh. Con System Manager, i file di dati registrati memorizzati sul MSE devono essere esportati nel sistema in cui lo strumento Analyzer può essere utilizzato per visualizzare e modificare i dati registrati, se necessario, prima di creare un file Mesh. Il file Mesh risultante viene reimportato nel file MSE, dove può essere applicato alle proprietà della mappa se si sceglie Mesh calcolo posizione RSSI insieme alla scelta del file di caricamento.

Per ulteriori informazioni sulla configurazione e sul processo di calibrazione, consultare la [documentazione di AeroScout](#).

Fare riferimento alla sezione sulla generazione di file Mesh AeroScout nella [documentazione di AeroScout](#).

## **Tecnologia Exciter (Chokepoint Trigger)**

Gli eccitatori sono dispositivi di comunicazione di prossimità che attivano codici di matricola per alterare il loro comportamento quando un codice di matricola entra in prossimità di un eccitatore. Questa modifica può causare la trasmissione del tag RFID al suo identificatore univoco o la modifica della configurazione o dello stato interno del tag. Una delle funzioni principali di un trigger di chokepoint è quella di stimolare il tag asset in modo che fornisca indicazioni al MSE che il tag è entrato o uscito da una determinata area. I punti di scelta sono punti di entrata o di uscita che consentono il passaggio tra regioni collegate. I punti di interruzione più comuni sono le porte, i corridoi e le scale. I punti di interruzione interni includono le entrate o le uscite di connessione.

Poiché gli eccitatori non utilizzano la triangolazione, non è necessario che i segnali vengano rilevati da almeno tre punti di accesso.

Gli eccitatori possono avviare modifiche comportamentali nelle etichette che possono avvisare immediatamente il sistema di localizzazione che la risorsa con tag è entrata o uscita dall'area di punto di interruzione. I tag RFID trasmettono quindi l'identità del trigger del punto di interruzione all'infrastruttura Cisco WAN. Le informazioni di punto di interruzione contenute nel pacchetto di tag forniscono al MSE informazioni per ignorare le coordinate di posizione di impronta digitale RF e assumere la posizione di punto di interruzione per una determinata durata.

Le procedure ottimali per configurare e ottimizzare eccitatori e tag sono disponibili nella Guida alla configurazione di eccitatori e tag di [AeroScout Documentation](#).

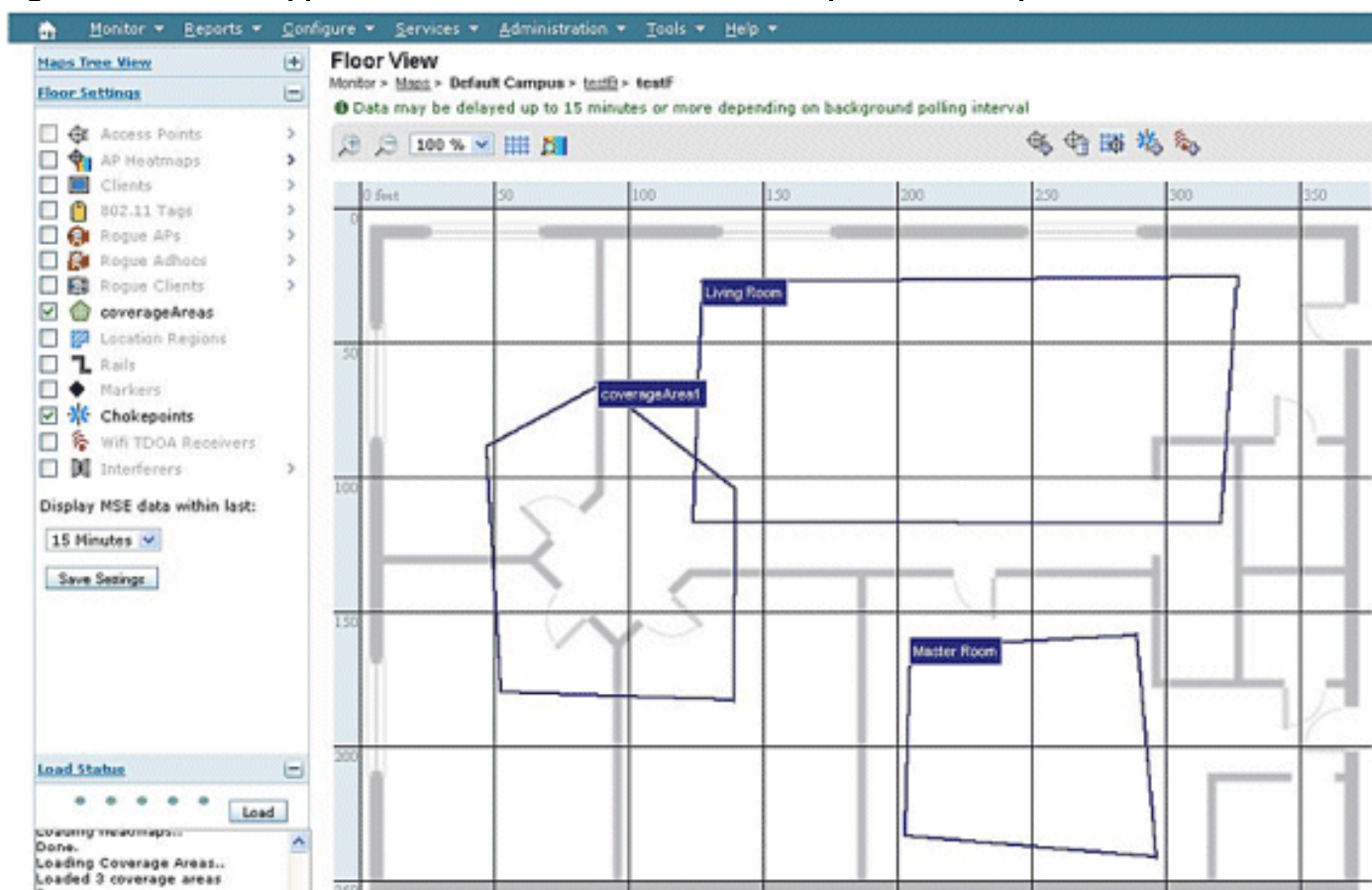
## **Considerazioni per la distribuzione con riconoscimento del contesto con i servizi voce e dati esistenti**

Negli ambienti delle sedi dei clienti in cui sono presenti reti wireless esistenti, sovrapposte a Context Aware Mobility Solution richiedono una nuova valutazione dell'installazione complessiva per garantire l'accuratezza e i potenziali problemi di copertura. Si tratta di orientamenti generali da seguire:

- Spaziatura ottimale tra i punti di accesso nella maggior parte degli ambienti di ufficio: 12-21 metri
- Almeno 3 punti di accesso nel range di trasmissione di ogni client (si consigliano 4 punti di accesso per la ridondanza)
- Posizionare i punti di accesso perimetrali per primi, poiché i punti di accesso devono circondare le aree desiderate di copertura della posizione

- Posizionare i punti di accesso interni per ridurre al minimo gli spazi di copertura per un minimo di -75 dBm
- Nell'area quadrilaterale, devono essere installati almeno 4 punti di accesso ai quattro angoli dell'area
- Fattori che influiscono sulla precisione: Posizionamento dei punti di accesso, materiali delle pareti, oggetti in movimento di grandi dimensioni e interferenze RF
- È possibile che sia necessario dividere lo spazio in sottoaree e progettare le sottoaree in modo indipendente, per tenere conto di grandi barriere che ostacolano i segnali RF (vedere la **Figura 26**). Sono supportate fino a 50 aree di copertura per il pavimento. Le dimensioni dell'area di copertura non possono essere inferiori all'intervallo di posizione tipico (~10 m)

**Figura 26: Editor mappe in Sistema colori Windows illustra più aree di copertura**



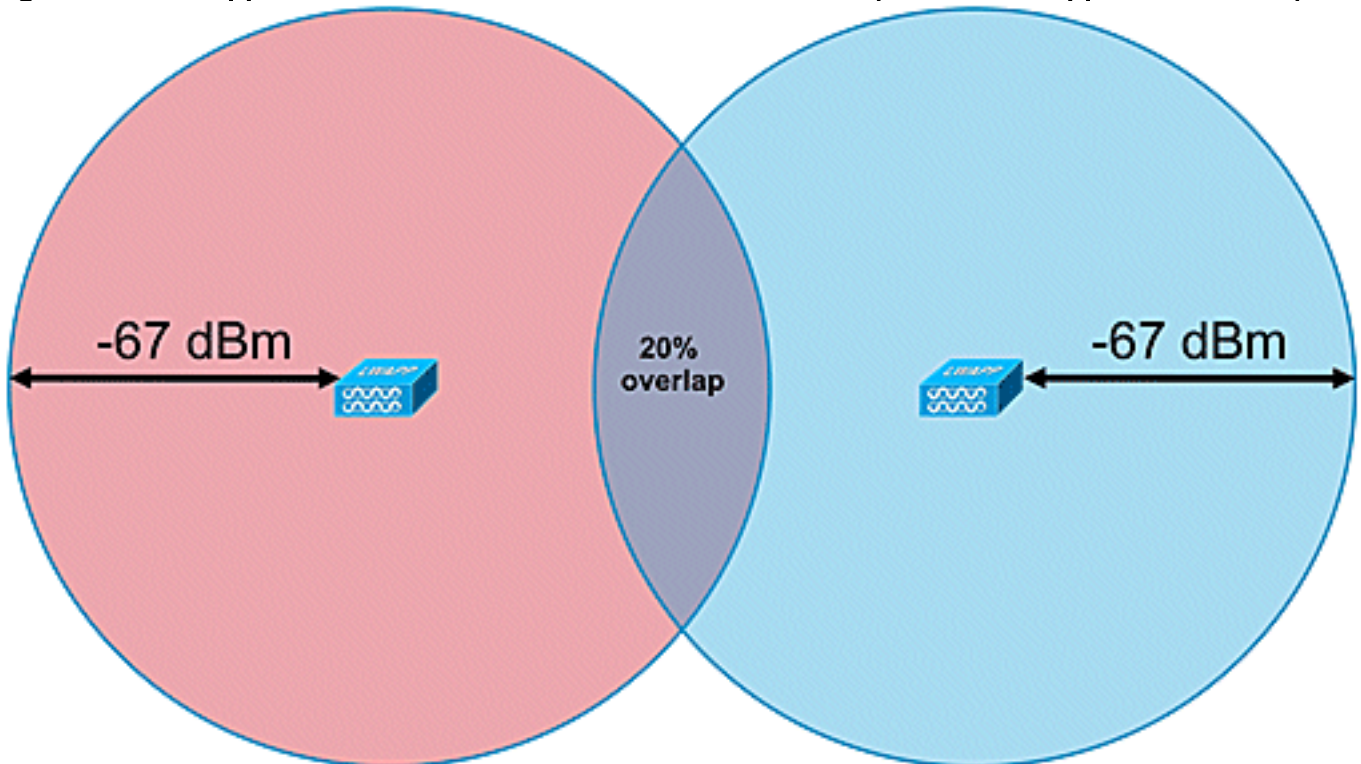
- I punti di accesso sono posizionati preferibilmente lungo e all'interno del perimetro di un'area chiusa.
- I punti di accesso devono essere distribuiti uniformemente, ovvero devono essere relativamente equidistanti l'uno dall'altro.
- Il posizionamento fisico dei punti di accesso deve essere non collineare, anche se posizionati a uguale distanza l'uno dall'altro.
- Utilizzare lo strumento di preparazione alla posizione in WCS per misurare l'efficacia della copertura totale del pavimento.
- Le forme geometriche formate dalla distribuzione dei punti di accesso influiscono sulla precisione: Il posizionamento del triangolo equilatero garantisce una maggiore precisione rispetto agli access point che formano un triangolo ottuso. Il posizionamento a quadrato produce risultati migliori rispetto ai punti di accesso che formano rettangoli.

La **Figura 27** illustra il concetto di sovrapposizione di celle per un ricevitore Cisco 7921G VoWLAN con 802.11bg. Per lo switch Cisco 7921G, le best practice consigliate nella guida alla

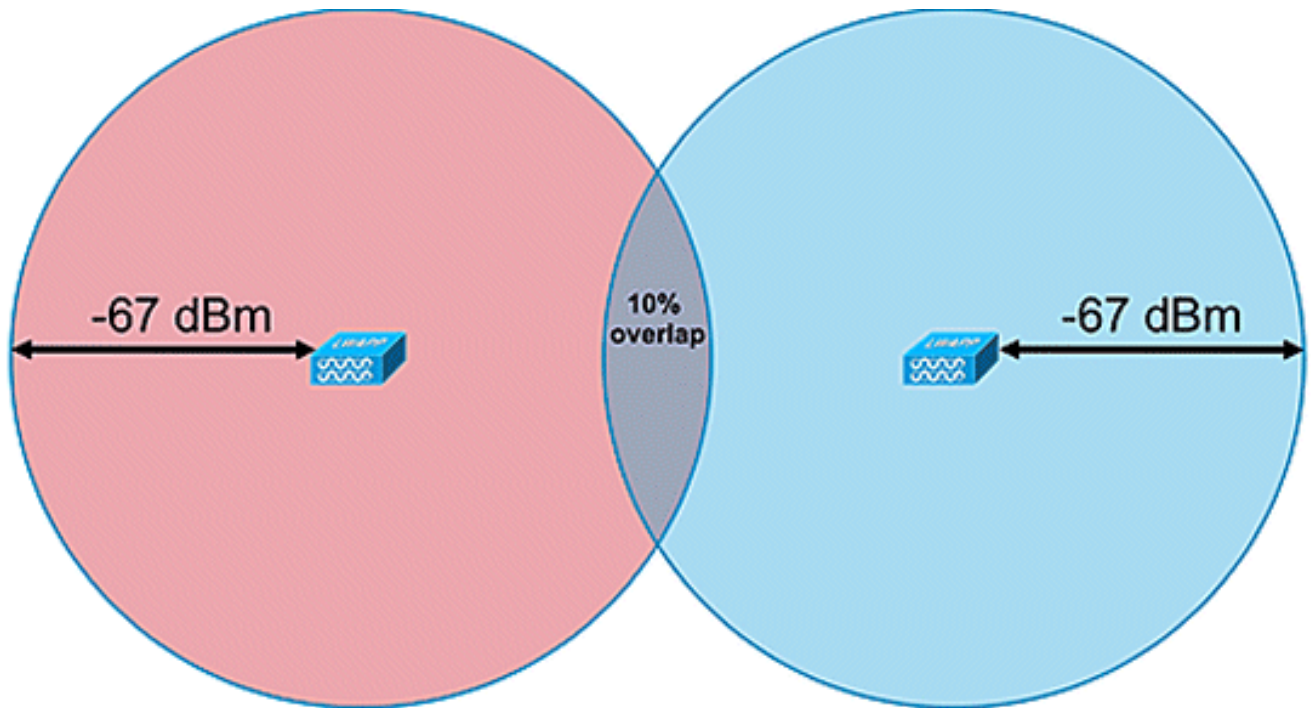
progettazione di LAN Voice Over Wireless consigliano una sovrapposizione cella-cella del 20% circa quando si utilizza 802.11bg e del 15% circa quando si utilizza 802.11a.

Le applicazioni dati non mostrano lo stesso livello di sensibilità alla perdita di pacchetti delle applicazioni voce. Di conseguenza, non richiedono lo stesso grado di sovrapposizione cella-cella delle implementazioni VoWLAN. Nella maggior parte dei casi, una sovrapposizione cella-cella pari almeno al 10% è sufficiente per un roaming affidabile con le applicazioni di dati, come mostrato nella **Figura 28**. Le applicazioni e le applicazioni di dati ad alta velocità che combinano funzionalità voce e dati in un unico dispositivo (ad esempio gli smartphone) potrebbero richiedere una sovrapposizione cella-cella che assomiglia molto più a una struttura VoWLAN che a una struttura di dati.

**Figura 27: Sovrapposizione tra celle: distribuzione voce e dati (20% di sovrapposizione cella)**



**Figura 28: Sovrapposizione tra celle: distribuzione dei dati (10% di sovrapposizione celle)**



## Orientamenti generali - TDOA

Con l'installazione basata su TDOA, sono richiesti almeno tre ricevitori, ma quattro di essi forniscono risultati più accurati. Di seguito sono riportate le regole generali relative alla densità dei ricevitori TDOA:

- All'aperto: la densità media è un ricevitore TDOA ogni 20.000 - 50.000 piedi quadrati. (1.900 - 4.700 mq).
- Grandi aree interne: la densità media è un ricevitore TDOA ogni 5.000 - 14.000 piedi quadrati. (450 - 1.300 mq).
- La distanza tra l'origine sincronizzata e i ricevitori TDOA è inferiore o uguale a 150 m per le installazioni all'aperto.
- La distanza tra la sorgente sincronizzata e i ricevitori TDOA è inferiore o uguale a 70m per installazioni in interni di grandi dimensioni.

Due importanti considerazioni per TDOA: la distribuzione della densità del ricevitore dipende dalla sincronizzazione del ricevitore e dalla sensibilità Rx della copertura RF dei dispositivi rilevati. La seconda considerazione importante è avere una copertura sufficiente dei ricevitori di posizione per garantire una densità ricettiva di almeno tre ricevitori di posizione in qualsiasi punto dell'area di posizione.

In alcuni scenari, può essere necessario suddividere le aree di grandi dimensioni in sottoaree. Se ad esempio un magazzino di grandi dimensioni è suddiviso in due sottoaree, è necessario che sia progettato come tale. I risultati migliori si verificano quando la linea di visuale viene mantenuta tra la fonte di sincronizzazione e i ricevitori Wi-Fi TDOA.

Ecco alcune linee guida aggiuntive per il posizionamento dei ricevitori Wi-Fi TDOA:

- I ricevitori Wi-Fi TDOA devono essere posizionati lungo il perimetro esterno e equidistanti.
- Ulteriori ricevitori Wi-Fi TDOA possono essere necessari entro i confini dei ricevitori perimetrali a seconda delle dimensioni dell'area.
- I ricevitori TDOA devono essere equidistanti e formare un triangolo equilatero (quando si usano tre ricevitori Wi-Fi TDOA) o un poligono (quattro o più ricevitori Wi-Fi TDOA).

Per quanto riguarda le antenne ricevitore Wi-Fi TDOA, utilizzare le antenne diversity per risolvere i problemi a percorsi multipli. I ricevitori Wi-Fi TDOA posizionati lungo il perimetro dell'area coperta devono includere antenne direzionali per concentrare la ricezione solo nell'area coperta. Nell'angolo di un perimetro, utilizzare un'antenna direzionale di 90 gradi e, lungo il perimetro, utilizzare antenne direzionali di 180 gradi. Le antenne omnidirezionali devono essere utilizzate con i ricevitori Wi-Fi TDOA situati all'interno del perimetro. Le antenne del ricevitore devono puntare sia all'origine della sincronizzazione (preferibilmente la linea di visuale) sia all'area in questione

Le antenne devono essere posizionate in aree in cui non sono ostruite da ostacoli, come pareti di cemento, grandi oggetti metallici o aree ad albero densamente coperte. Devono essere installati con una buona visuale (quanto più possibile) sulla zona coperta. L'altezza di montaggio preferita è di 10-16 piedi (da 3 a 5 metri) sopra la superficie degli asset tracciati. Quando ciò non è possibile a causa dell'ambiente, il modello di copertura, cioè il modello di elevazione - le antenne tipiche hanno un'elevazione di circa 35 gradi, devono essere regolati di conseguenza. Lungo il perimetro, le antenne in posizioni elevate devono essere inclinate verso l'area di copertura (fino a 30 gradi verso il basso per compensare l'elevazione).

Per ulteriori informazioni, consultare la *guida alla distribuzione di AeroScout TDOA*.

## Posizione cavi

Con la versione 6.0 del software, i dispositivi wireless e cablati (Ethernet) possono essere rintracciati con la soluzione Context Aware. Con la postazione cablata, MSE fornisce la funzionalità per raccogliere e gestire le informazioni sulla posizione CIVICA per switch e porte dello switch. È possibile identificare la posizione dei dispositivi cablati Ethernet connessi a uno dei seguenti switch Cisco: Switch Catalyst impilabili (switch 3750, 3750-E, 3560, 2960 e IE-3000) o blade switch (3110, 3120, 3130, 3040, 3030 e 3020) e Catalyst serie 4K (WS-C4948, WS-C4948-10GE, ME-44 924-10GE, WS-4928-10GE, WS-C4900M, WS-X4515, WS-X4516, WS-X4013+, WS-X4013+TS, WS-X4516-10GE, WS-X4013+10GE, WS-X45-SUP6-E e WS-X45-SUP6-LE). Per la postazione cablata, utilizzare le seguenti versioni di IOS relative al rispettivo modello di switch: IOS 12.2 (50)SE per gli switch Catalyst 3K e IOS 12.2(52)SG per gli switch Catalyst 4K. Le informazioni sulla posizione dei cavi vengono inviate da questi switch al MSE tramite NMSP.

Le informazioni sulla posizione vengono configurate sullo switch Cisco tramite la CLI di IOS. Gli switch cablati sono definiti in WCS e sincronizzati con MSE. I dettagli sui client cablati vengono inviati da uno switch abilitato per la posizione al server MSE tramite una connessione NMSP. È quindi possibile visualizzare switch e client cablati con Cisco WCS.

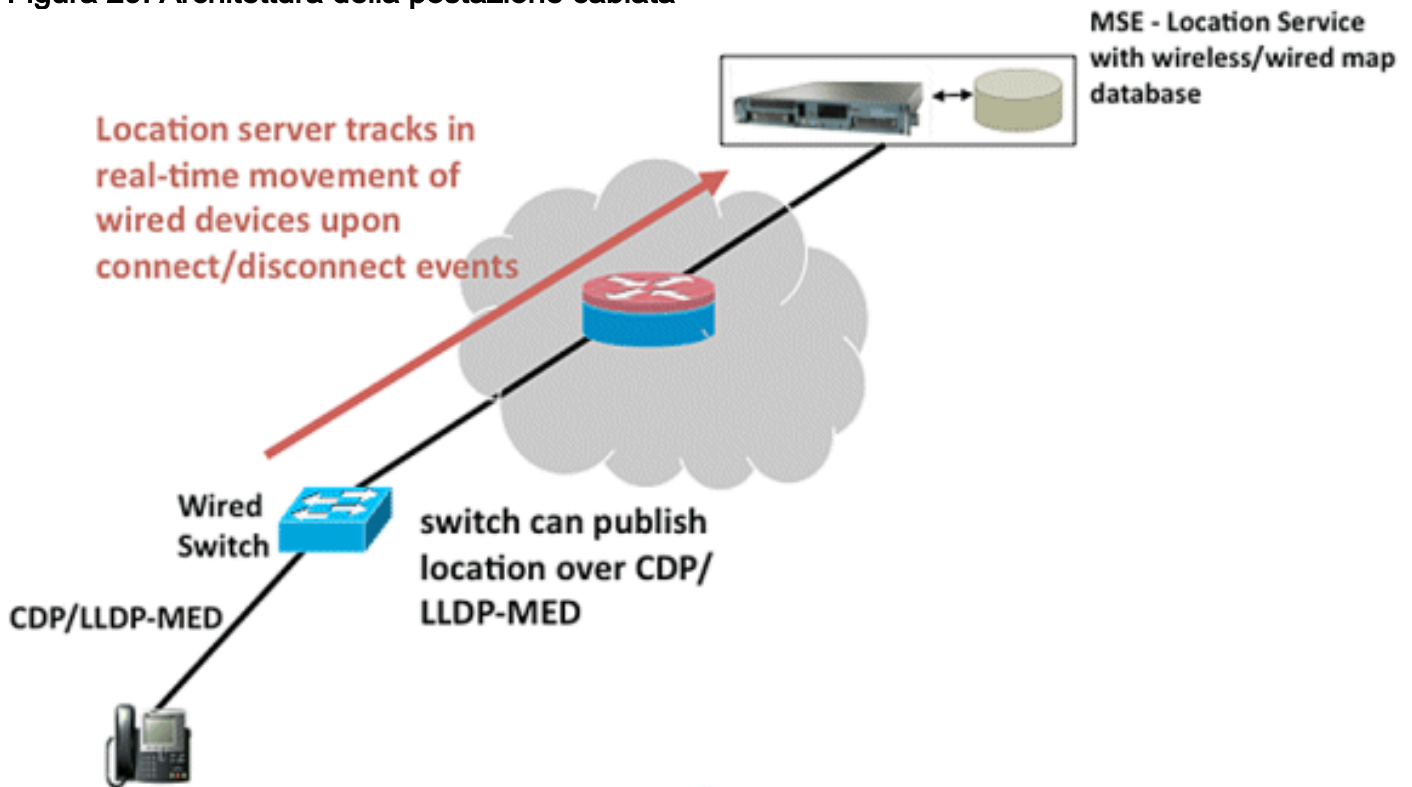
L'importazione e la visualizzazione di informazioni civiche e sulla posizione di emergenza (ELIN) sono conformi alle specifiche RFC4776 descritte all'indirizzo <http://tools.ietf.org/html/rfc4776#section-3.4>.

MSE non tiene traccia solo della cronologia delle posizioni dei client cablati, ma fornisce anche le API SOAP/XML ai sistemi esterni interessati alla posizione dello chassis o dei dispositivi endpoint oppure ricerca/traccia di un client tra categorie cablate e wireless. Fare riferimento alla **Figura 29**.

- Gli switch inviano un rapporto alla mappatura delle porte degli switch MSE dei dispositivi collegati che include la posizione e le informazioni UDI dello chassis, oltre alle schede di linea.
- MSE tiene traccia attivamente delle informazioni comunicate e della posizione di dispositivi e chassis.

**Nota:** la funzionalità di posizione cablata non consente attualmente di cercare o visualizzare visivamente i client cablati nelle mappe del pavimento.

Figura 29: Architettura della postazione cablata



Accertarsi di seguire la procedura per visualizzare la posizione del cavo.

Di seguito vengono riportati i passaggi della configurazione sul lato switch:

1. Comprendere la configurazione di slot/modulo/porta (1/0/20).
2. Utilizzare la versione IOS corretta relativa al rispettivo modello di switch: IOS 12.2 (50)SE per gli switch Catalyst 3K e IOS 12.2(52)SG per gli switch Catalyst 4K.
3. Abilitare l'NMSP.
4. Abilitare il rilevamento dei dispositivi IP.
5. Configurare la community SNMP con accesso in lettura/scrittura.
6. Configurare gli identificatori di posizione Civic/ELIN.
7. Assegnare gli identificatori alle interfacce dello switch.

Di seguito sono riportati i passaggi di configurazione del sistema di colori Windows:

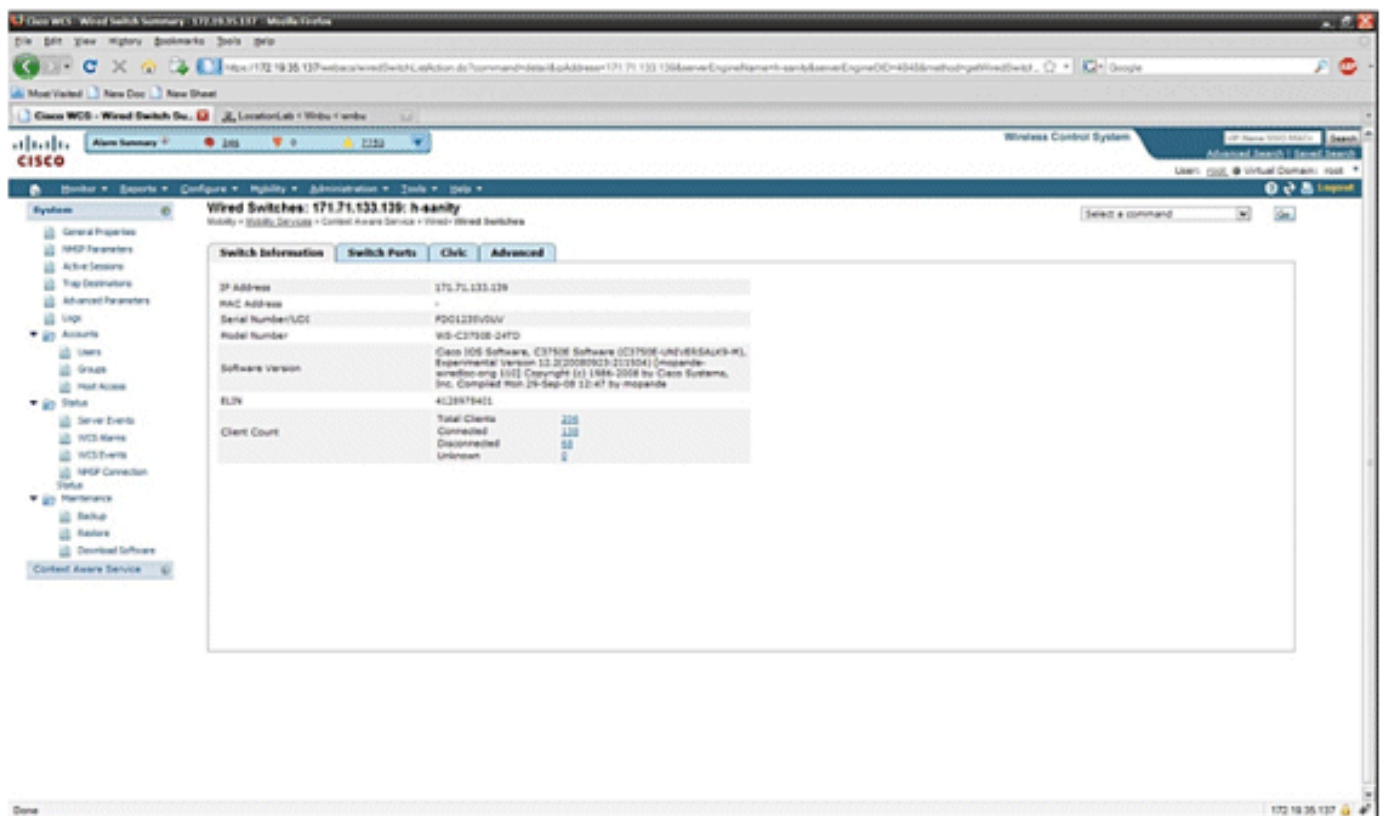
1. Selezionare **Configure > Ethernet Switches** (Configurazione > Switch Ethernet).
2. Aggiungere switch Ethernet. Aggiungere l'indirizzo IP. Abilita **funzionalità percorso**. Accedere alla community SNMP (lettura/scrittura). La stringa della community SNMP immessa deve corrispondere al valore assegnato allo switch Catalyst.
3. Selezionare **Servizi > Sincronizza servizi > Switch**. Fare clic su **Assegna** per assegnarlo al server MSE preferito. Scegliere lo switch e sincronizzarlo.
4. Selezionare **Servizi > Servizi di mobilità**, quindi fare clic su **MSE**. Selezionare **Sistema > Stato > Stato connessione NMSP**. Controllare lo stato NMSP attivo per ciascuno switch.

Dopo aver completato i passaggi sullo switch e sul WCS, è possibile visualizzare gli elementi cablati sul WCS:

- In Servizi compatibili con il contesto fare clic su **Switch cablati** in Cablati.
- Viene visualizzato un elenco degli switch.
- Fare clic su **Switch IP Address** per visualizzare i dettagli (vedere la **Figura 30**).

**Nota:** per aggiungere i WLC al WCS, è necessario l'accesso SNMP di lettura/scrittura. Il WLC non riceverà l'hash della chiave MSE con la modalità di accesso in sola lettura SNMP.

**Figura 30: Switch cablati - Informazioni switch**



- È inoltre possibile visualizzare le porte dello switch e le informazioni sullo switch (vedere la **Figura 31** alla **Figura 33**) o modificare l'ordine di visualizzazione (in ordine crescente o decrescente) degli indirizzi IP delle porte, dei numeri di slot, del numero di modulo e del numero di porta. È sufficiente fare clic sull'intestazione della colonna corrispondente.

**Figura 31: Switch cablati - Informazioni porte switch**

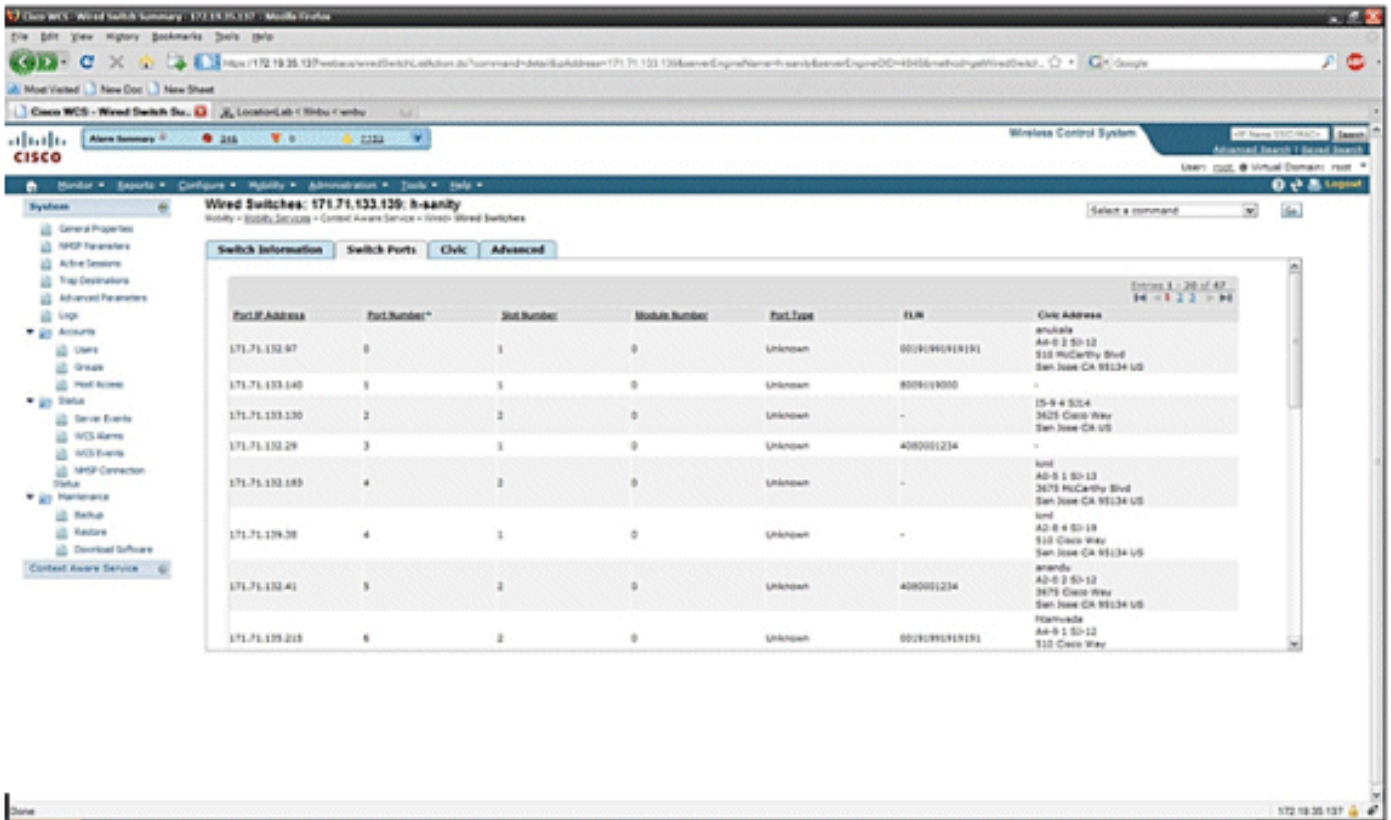
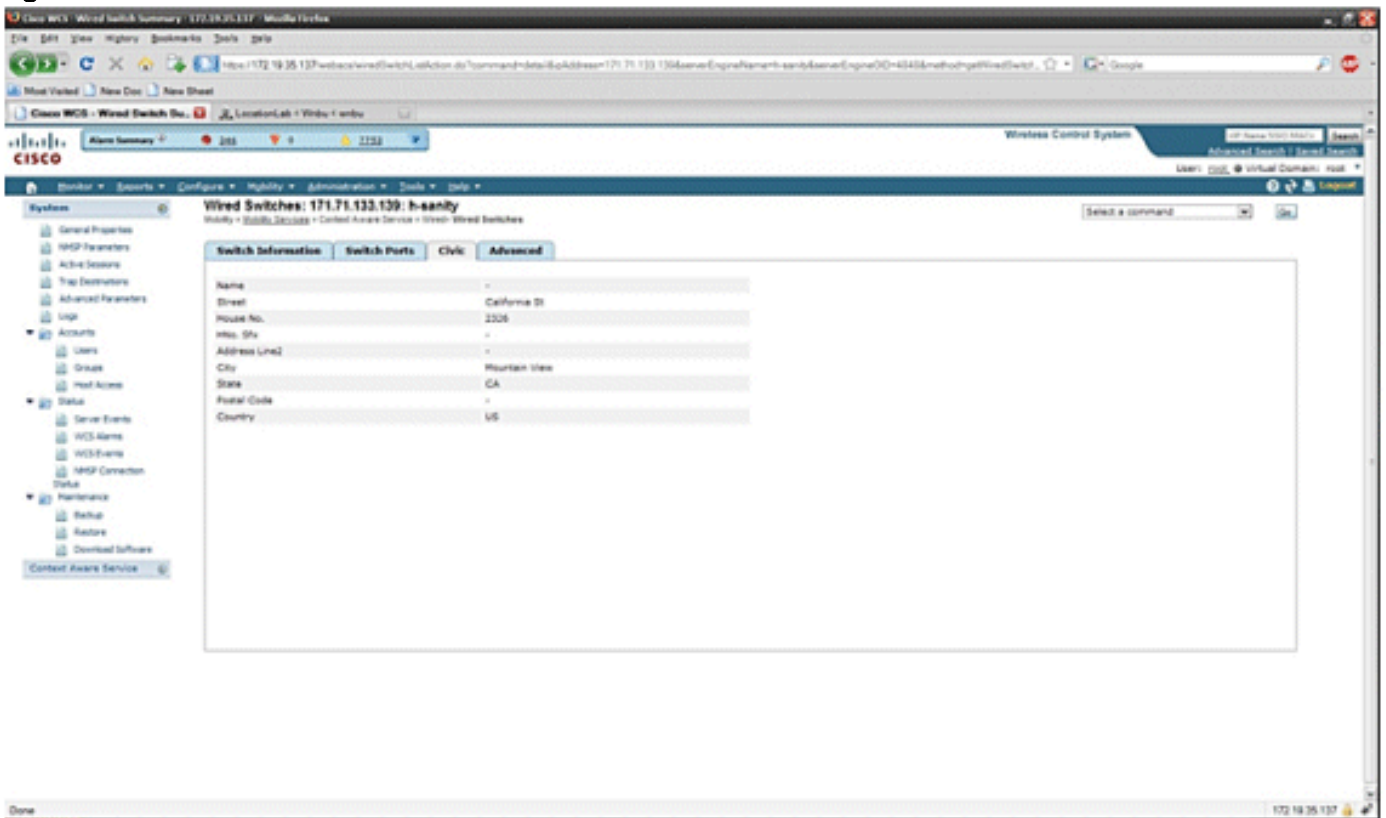


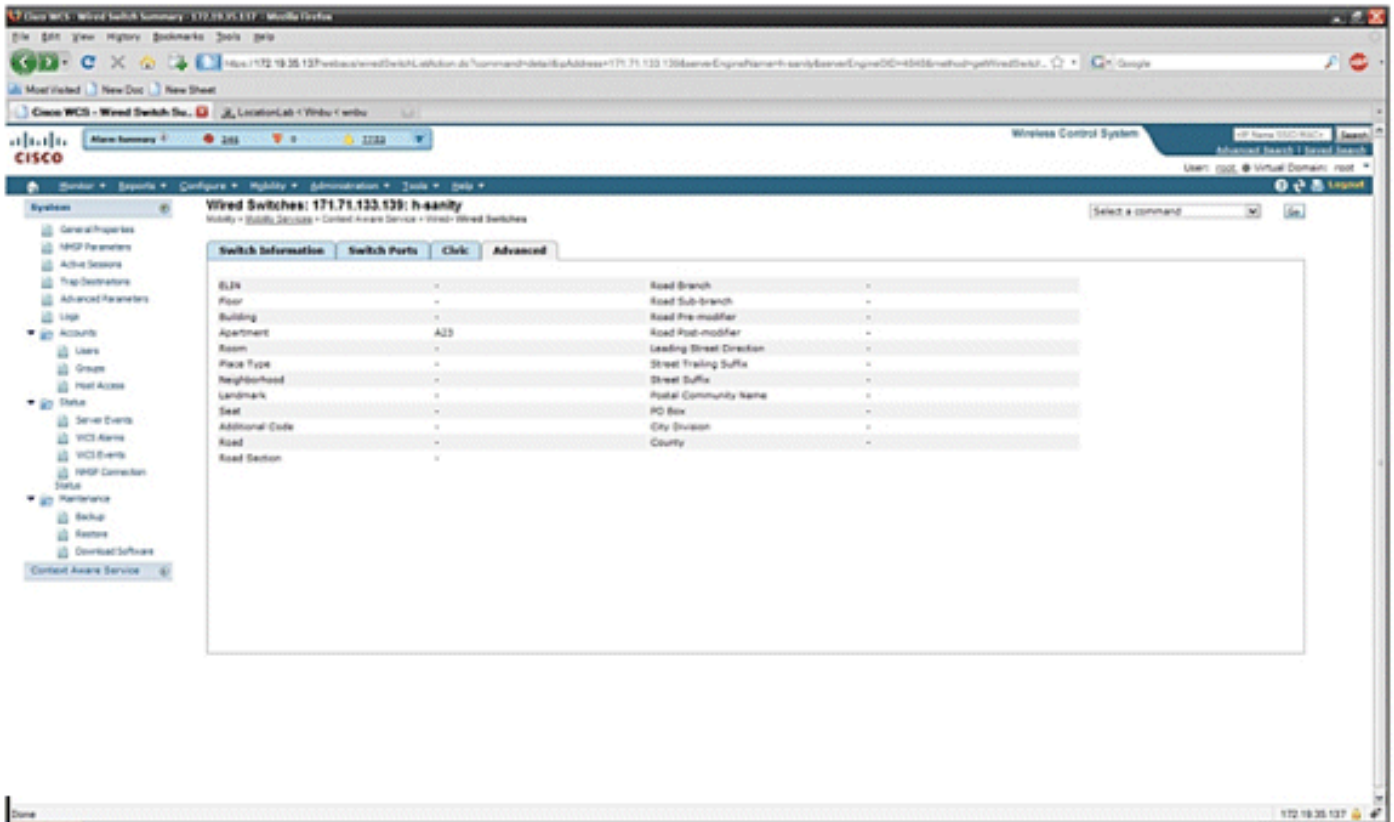
Figura 32: Switch cablati - Informazioni civiche



La scheda Avanzate fornisce ulteriori informazioni civiche:

Figura 33: Switch cablati - Informazioni avanzate

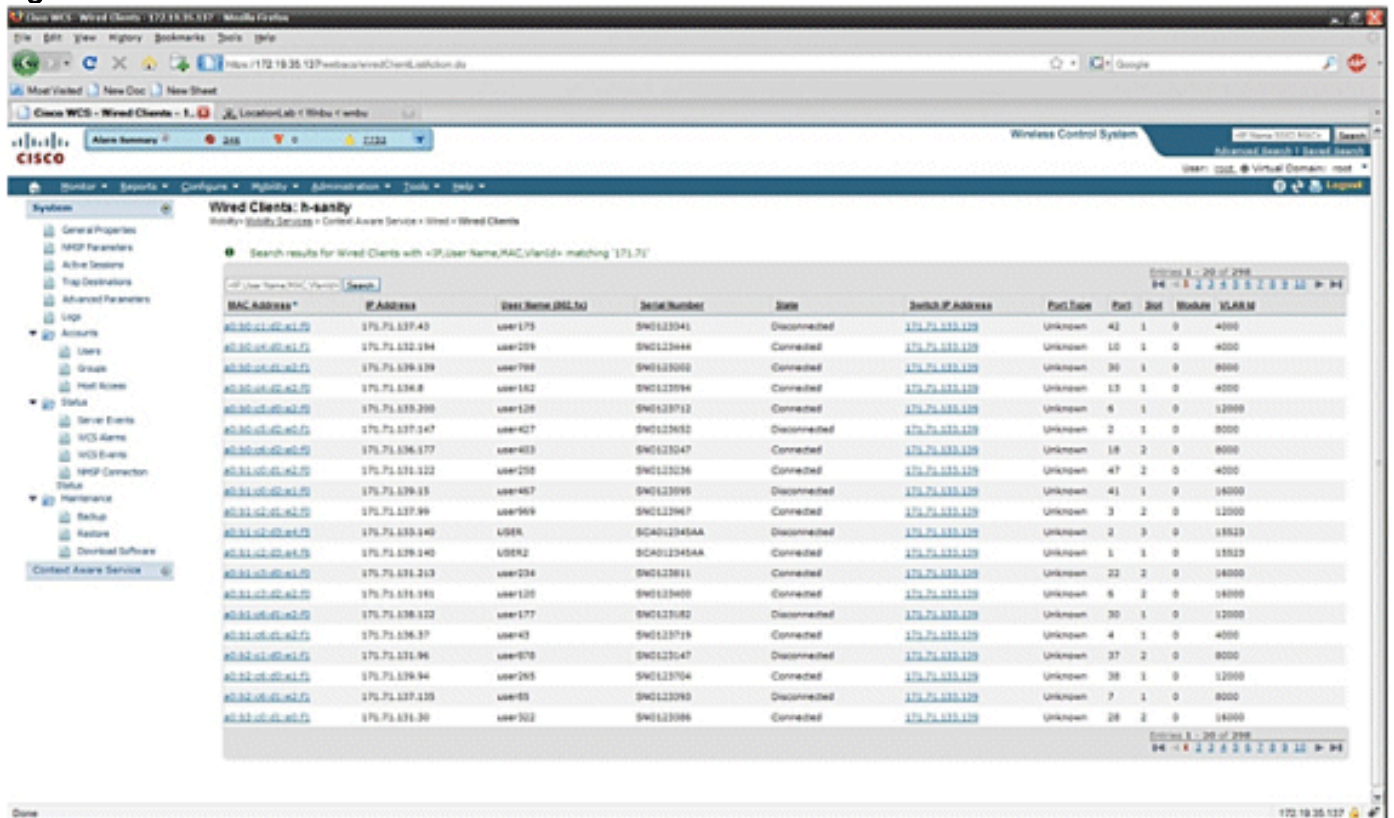




I client cablati rilevati da tutti gli switch possono essere visualizzati facendo clic su **Client cablati** in Servizio di riconoscimento del contesto cablato > Cablati > Client cablati.

I client cablati possono essere cercati per indirizzo IP/indirizzo IP parziale/indirizzo Mac/ indirizzo Mac parziale/nome utente 802.1x/ID VLAN, come mostrato nella **Figura 34**.

**Figura 34: Client cablati - Risultati della ricerca**



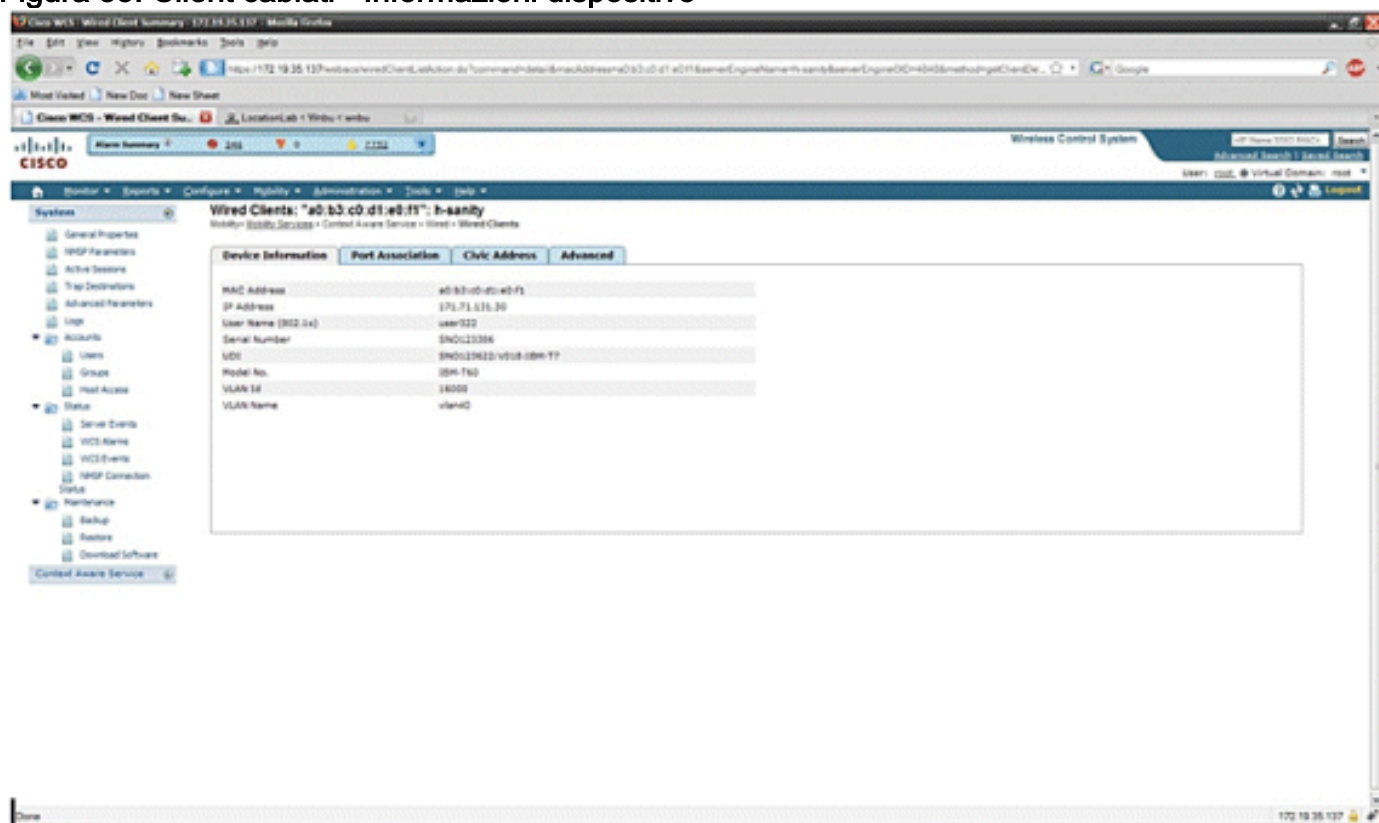
Uno switch ha un numero specificato di porte e client dello switch; gli host sono connessi a queste

porte. Quando si configura la posizione di una porta dello switch specifica, si presume che il client connesso a quella porta abbia la posizione della porta.

Se uno switch (switch2) è collegato a una porta (ad esempio porta1) su un altro switch (switch1), a tutti i client collegati allo switch2 viene assegnata la posizione configurata sulla porta1.

È inoltre possibile visualizzare i dettagli dei client cablati quando si fa clic sul rispettivo client per ottenere informazioni sui dispositivi, le associazioni delle porte, gli indirizzi civici, ecc. (vedere le figure da 35 a 38).

**Figura 35: Client cablati - Informazioni dispositivo**



Fare clic sulla scheda Associazione porta per visualizzare la posizione fisica della porta/slot/modulo dello switch su cui il client cablati termina, lo stato del client (connesso, disconnesso o sconosciuto) e l'indirizzo IP dello switch:

**Figura 36: Client cablati - Informazioni sull'associazione della porta**

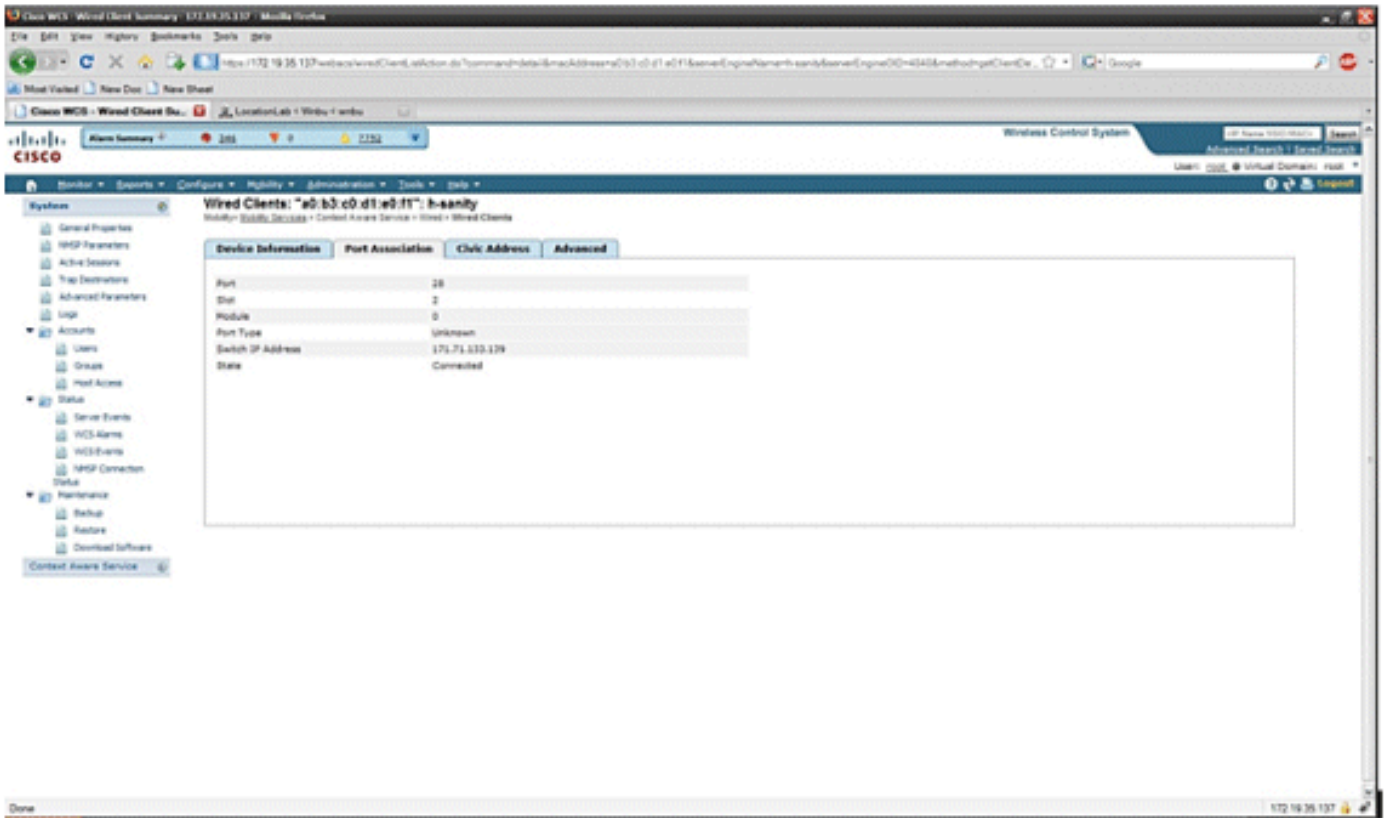


Figura 37: Client cablati - Informazioni indirizzo civico

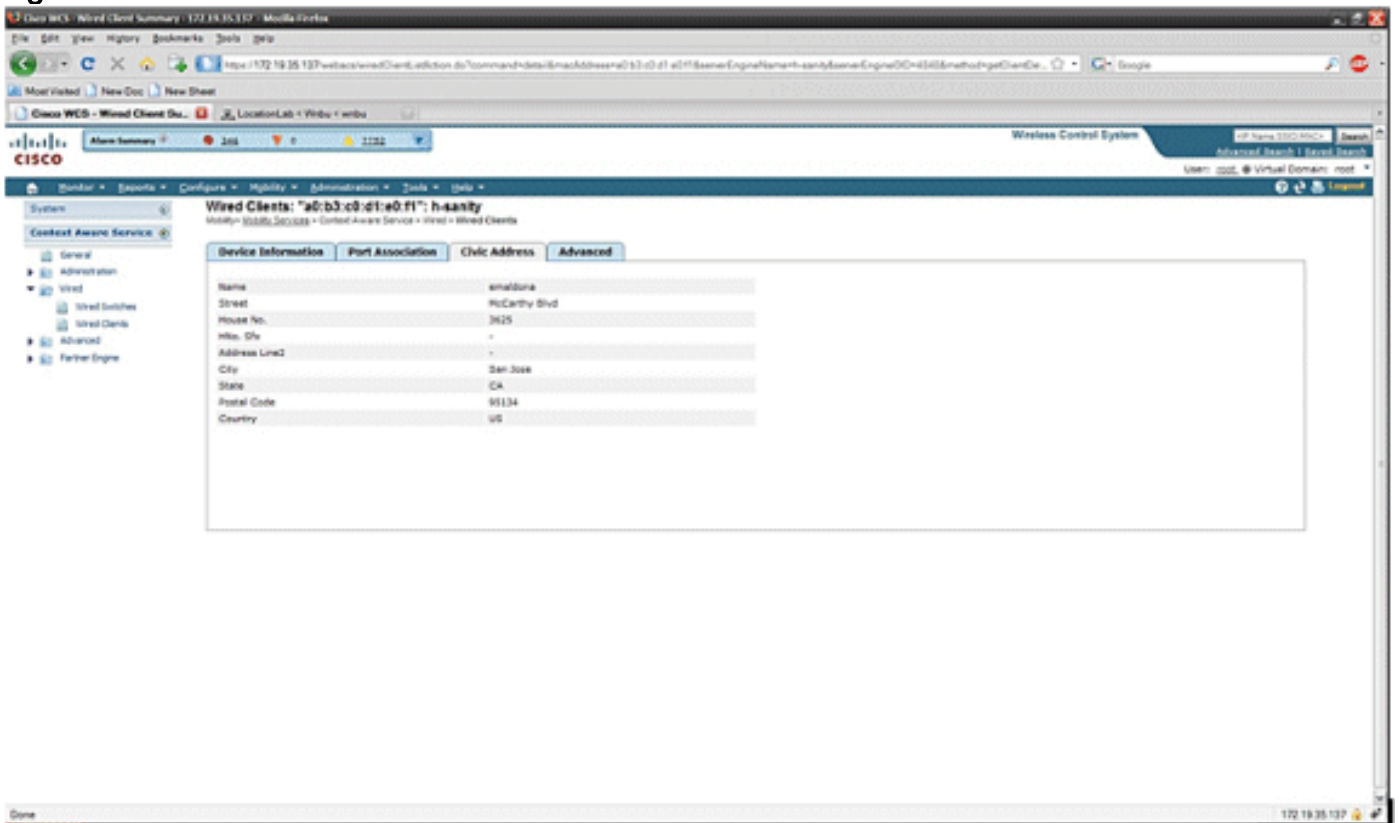
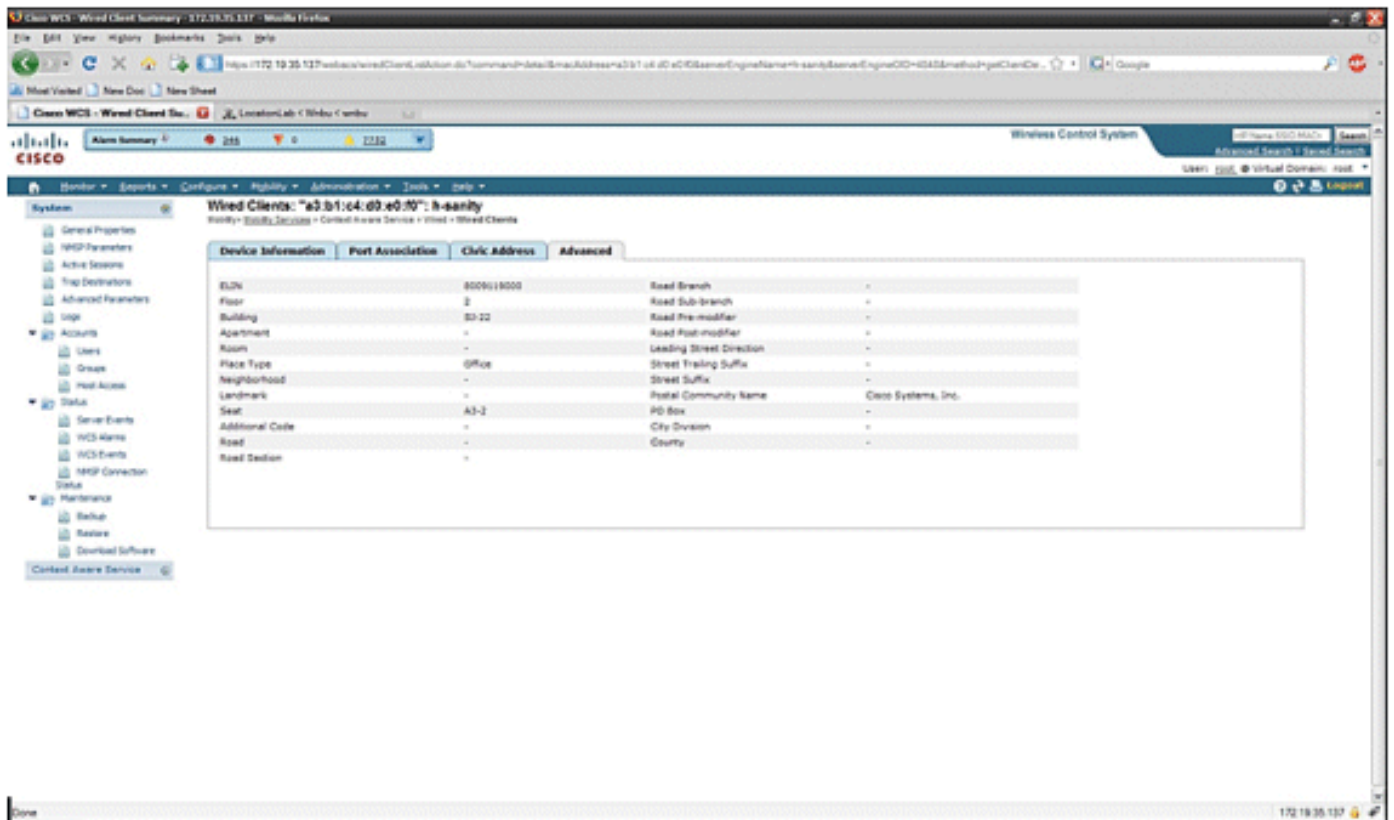


Figura 38: Client cablati - Informazioni avanzate



## Sezione 3: Convalida e miglioramento della rete sensibile al contesto

### Strumento di precisione Sistema colori Windows

Prima della release di WCS 5.0, gli utenti non potevano sapere con certezza quale precisione vedevano sulla rete wireless. Non esisteva un metodo standard per quantificare il livello di accuratezza con la distribuzione basata sul contesto. La release 5.0 di WCS ha introdotto uno strumento di precisione integrato. I client di tag e/o Wi-Fi sono posizionati in corrispondenza dei punti di riferimento sulla mappa del pavimento in WCS. Il sistema WCS genera un report dettagliato con diversi livelli di precisione e distribuzione degli errori nel tempo e nello spazio.

Esistono due tipi di test di accuratezza:

- Precisione programmata
- Precisione su richiesta

Gli utenti possono scegliere uno di questi metodi dopo aver scelto il piano in cui eseguire il test di accuratezza, come mostrato nella **Figura 39**. Questi test vengono eseguiti sullo stesso piano.

**Figura 39: Test di accuratezza su richiesta**

## Position Test Points for Test 'test'

Tools > Location Accuracy Tool > On Demand Accuracy Test > Position Test Points for Test 'test'



**Test di accuratezza programmato:** Questo test viene eseguito in un ambiente attivo (rete attiva). I client e/o i tag vengono preposizionati sul pavimento e il test viene pianificato tramite WCS. Questo test utilizza la posizione "effettiva" di un elemento rispetto alla posizione "misurata". L'utente può modificare il test:

- Aggiungere/eliminare gli elementi
- Modificare le posizioni
- Modificare le pianificazioni

Il test può essere eseguito come un'attività pianificata e generare allarmi se non rientra in un determinato intervallo di precisione. Questo tipo di test deve essere eseguito periodicamente poiché l'ambiente RF di una determinata distribuzione può cambiare, con un conseguente impatto sulla precisione della posizione.

Figura 40: Risultato test di accuratezza

## Accuracy Test Result (%)

98.14

Error Range (Meters)	% of Total
3.00 or less	49.31
3.01 to 5.00	25.86
5.01 to 7.00	17.53
7.01 to 10.00	5.11
10.01 or more	1.86

Nell'esempio della **Figura 40**, il 98,14% rappresenta il numero di dispositivi rilevati nel test entro 10 m, ovvero la somma di 49,31, 25,86, 17,53 e 5,11.

**Test di accuratezza su richiesta:** Questo test viene eseguito quando un utente non dispone di client e/o tag attivi distribuiti nella propria rete ed è interessato a misurare la precisione. Questo test può essere eseguito quando un reparto non dispone di tag/client preposizionati. Questa procedura è simile al test di accuratezza eseguito in WCS prima della release 5.0 con un singolo client. L'utente posiziona un client in una posizione particolare e indica tale posizione nella mappa del pavimento in WCS trascinando il test con "drag and drop". L'utente fa clic su **Start**, attende alcuni minuti il completamento del processo di raccolta RSSI e fa clic sul pulsante **Stop**. L'utente può quindi continuare il test e passare al punto successivo della mappa del pavimento. Una volta raccolti tutti i punti, l'utente può fare clic sul pulsante **Analizza risultati** per eseguire il test. In questo modo si ottiene il risultato della precisione in un formato di report.

Quando si esegue uno dei test di accuratezza, tenere presente quanto segue:

- Il client deve essere visualizzato da almeno tre punti di accesso
- La precisione dipende dalla triangolazione e dalle impronte digitali RF
- È necessario abilitare il **debug avanzato** su MSE
- In un determinato punto della mappa di pavimento, attendere circa un minuto con il client in posizione, ovvero fermo, prima di eseguire il test di accuratezza. In questo modo il client wireless ha tempo sufficiente per aggiornare MSE con la propria posizione. Eseguire il test per due minuti.

## Strumento di preparazione alla posizione

WCS fornisce uno strumento, la funzione di verifica della fattibilità dell'ubicazione, che consente a un progettista di rete di eseguire un rapido controllo predittivo delle prestazioni dell'ubicazione di un pavimento prima che il cavo venga tirato, che venga installata l'apparecchiatura o che vengano eseguite le calibrazioni.

Si tratta di uno strumento predittivo basato sulla distanza che presuppone un tipico edificio di tipo ufficio. Di conseguenza, si verifica un certo grado di varianza tra i risultati previsti e quelli effettivi. Cisco consiglia di utilizzare lo strumento di preparazione alla localizzazione insieme ad altre tecniche ottimali.

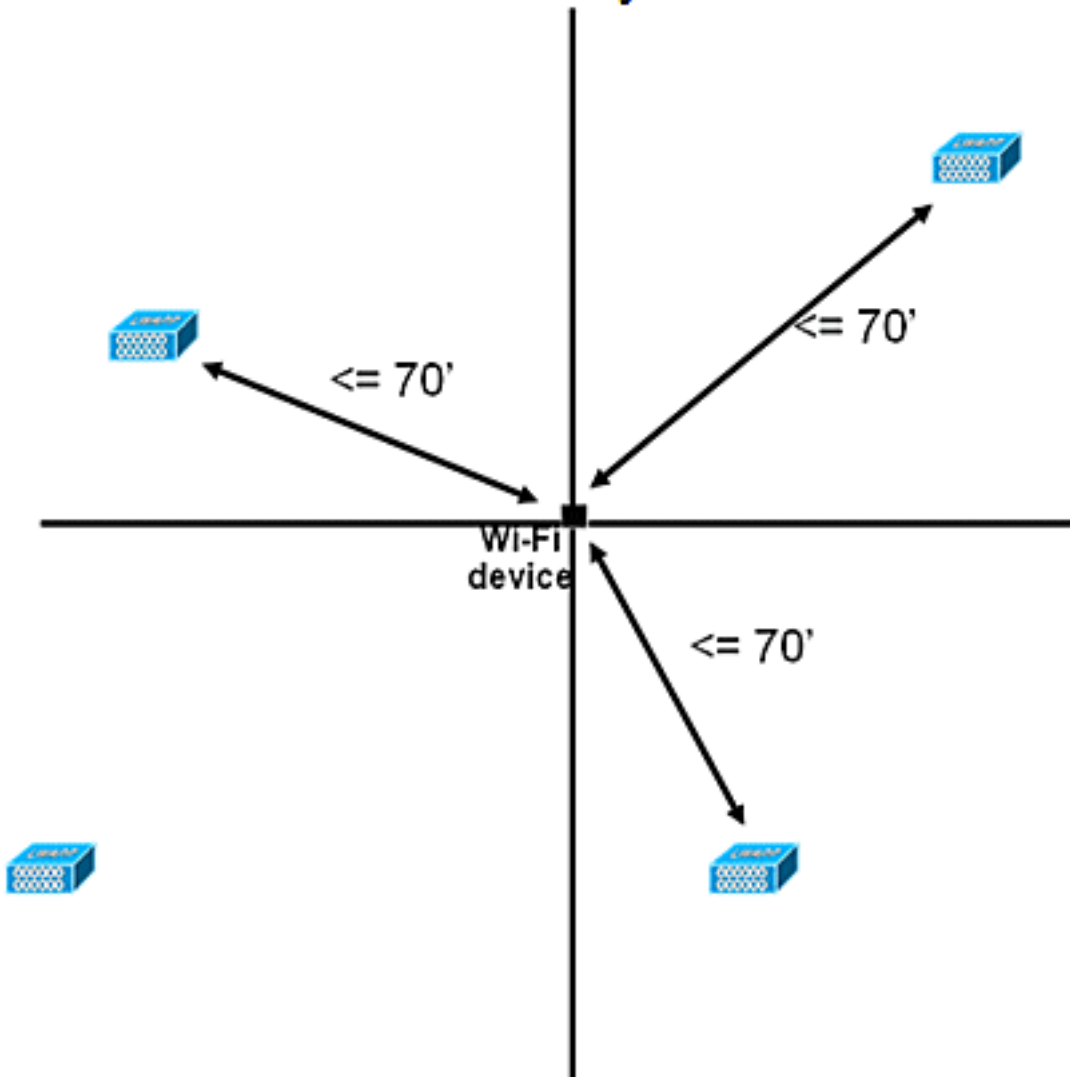
La fattibilità dell'ispezione prende in considerazione la posizione di ciascun punto di accesso insieme alla spaziatura tra i punti di accesso indicata sulle mappe del pavimento, per prevedere se la precisione stimata di tracciamento della posizione sarà entro 10 metri nel 90% di tutti i casi. L'output dell'ispezione di fattibilità ubicazione è rappresentato graficamente in verde e rosso delle aree che si prevede producano rispettivamente questo livello di accuratezza e aree problematiche.

Lo strumento Location Readiness Tool presuppone che i punti di accesso e i controller siano noti al sistema WCS e siano stati definiti nelle mappe di base del sistema. Anche se non è necessario installare effettivamente punti di accesso e antenne su pareti e soffitti per condurre una valutazione della fattibilità della posizione, tutti i controllori applicabili devono essere aggiunti al WCS insieme ai relativi punti di accesso registrati con le icone che rappresentano i punti di accesso posizionati sulle mappe del pavimento appropriate. Una volta che i punti di accesso da inserire nelle mappe di base sono stati aggiunti alla banca dati del Sistema di controllo della stabilità del sistema, le successive valutazioni della fattibilità della localizzazione possono essere effettuate con questi stessi punti di accesso, anche se non sono raggiungibili da tale sistema in quel momento. Poiché l'ispezione della fattibilità della posizione si basa sul posizionamento dei punti di accesso e sulle distanze tra i punti di accesso visualizzate sulle mappe del pavimento, quando si utilizza questo strumento è fondamentale che i punti di accesso siano posizionati correttamente. Lo strumento di preparazione alla localizzazione viene utilizzato solo per valutare la preparazione del progetto per eseguire il rilevamento della posizione basato su impronte digitali RF. Non convalida alcun aspetto del progetto per eseguire la posizione del punto di interruzione, in particolare per quanto riguarda la definizione o il posizionamento dei trigger del punto di interruzione. Dopo aver eseguito il posizionamento del punto di accesso, scegliere la mappa del pavimento di cui si desidera verificare la fattibilità della posizione, quindi scegliere **Ispezione fattibilità ubicazione** dal menu a discesa in alto a destra.

Un punto viene definito "pronto per la posizione" se tutti questi sono determinati come veri:

- Almeno quattro punti di accesso sono installati sul pavimento
  - È stato rilevato che almeno un punto di accesso risiede in ogni quadrante che circonda il punto in questione
  - Almeno un punto di accesso risiede in ciascuno di almeno tre quadranti circostanti situati entro 70 piedi dal punto in questione
- La Figura 41 illustra queste tre regole di idoneità alla posizione. **Figura 41: Punto Pronto Per La Posizione**

## Definition of a "Location-Ready" Point



L'acquisizione schermo del Sistema colori Windows mostra un esempio di installazione a pavimento in cui non tutte le aree hanno superato la valutazione della fattibilità in tre punti descritta in precedenza per una precisione del 10/90%. Anche se ci sono aree verdi verso il centro della figura, notare che le aree rosse abbondano mentre si va oltre i punti di accesso perimetrali che rappresentano lo scafo convesso. Grazie a una solida comprensione dei requisiti che definiscono la fattibilità della collocazione, le informazioni contenute in questa figura possono essere utilizzate per determinare il numero di access point da trasferire o aggiungere per migliorare le prestazioni. Ad esempio, se è richiesta una precisione di posizione di 10 m/90% o superiore all'interno delle aree rosse, è possibile introdurre punti di accesso aggiuntivi per stabilire un perimetro del pavimento più chiaramente delineato, che include la posizione dei punti di accesso negli angoli del pavimento e ricontrolla le distanze tra i punti di accesso. Quando si implementano questi tipi di modifiche, è probabile che la capacità del Cisco UWN di risolvere la posizione dei dispositivi tracciati in queste aree evidenziate venga notevolmente migliorata.

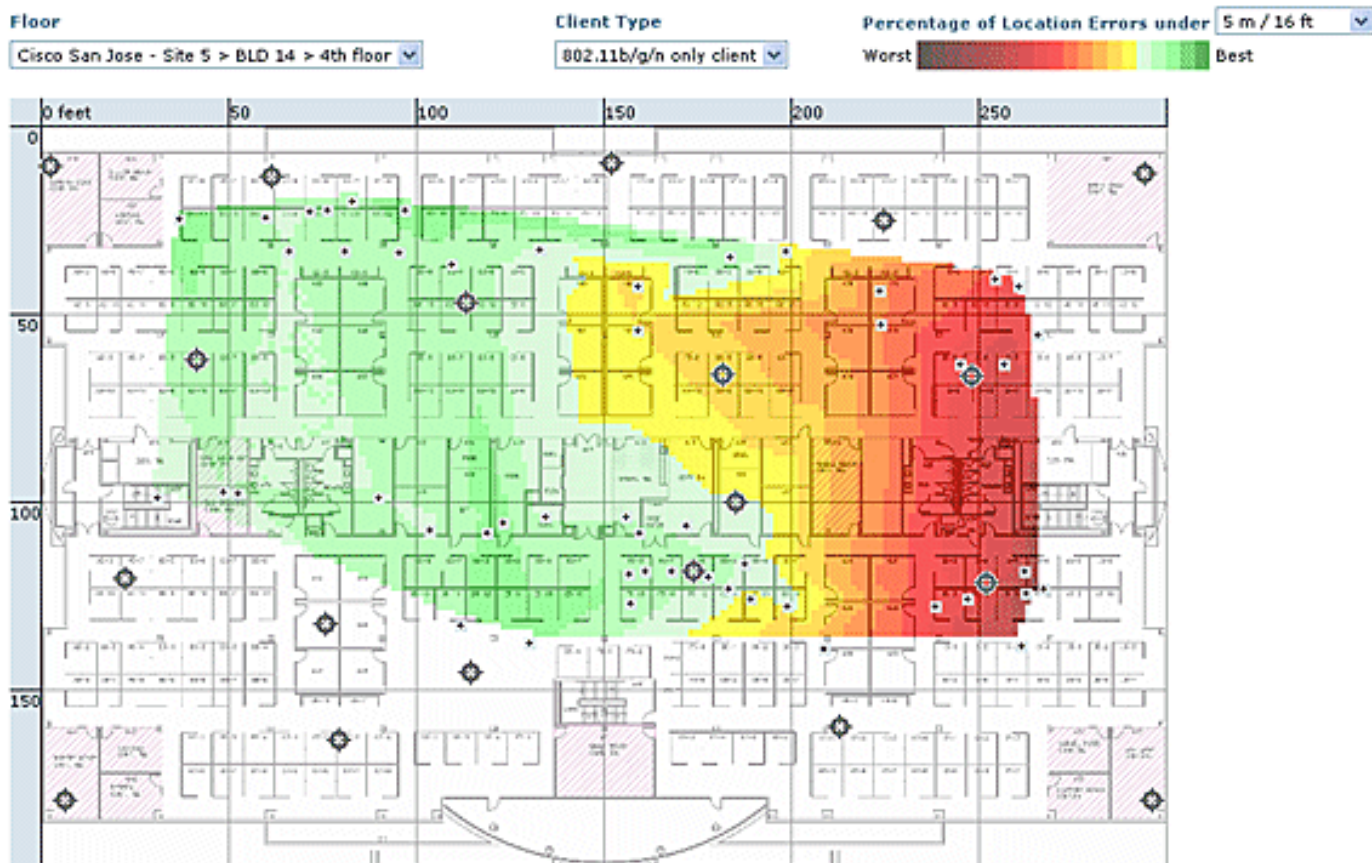
Figura 42: Esempio di utilizzo dello strumento Location Readiness





La qualità della posizione può essere verificata per un'installazione wireless in base alla capacità di soddisfare la specifica della posizione (10 m, 90%), in base ai punti dati raccolti durante un'ispezione fisica e una calibrazione, come mostrato nella **Figura 42**. Quando si utilizza lo strumento Location Readiness, viene visualizzata una mappa a colori che mostra le aree che soddisfano (verde=sì) e non soddisfano (rosso=no) la specifica della posizione del 90%, 10 metri.

**Figura 43: Strumento Ispeziona qualità ubicazione**



Dopo aver eseguito una calibrazione su un'area o una mappa specifica, è possibile rivedere questi dati per verificare i dati grezzi raccolti durante la calibrazione, come mostrato nella **Figura 43**. È importante verificare i dati grezzi in ciascun punto di raccolta dati rispetto alla misurazione fisica e al valore RSSI AP associato. Le anomalie nel posizionamento dei punti di accesso, nell'antenna o nei punti di riferimento delle misure possono essere facilmente identificate e corrette prima di essere applicate alle mappe. Ulteriori informazioni sul livello di accuratezza percepito e sui punti di accesso che contribuiscono possono aiutare a valutare la precisione complessiva della posizione.

### Sensibile al contesto - Prestazioni del sistema

In una soluzione distribuita basata sul contesto, è possibile spostare contemporaneamente più tag e/o client. Maggiore è il numero di dispositivi che si spostano, maggiore è il carico di elaborazione sul server MSE. Ciò, a sua volta, influisce sulla latenza complessiva della rete. La latenza in questo contesto si riferisce al ritardo tra il momento in cui l'MSE riceve informazioni RSSI su un dispositivo e il momento in cui la sua posizione viene calcolata dall'MSE. Si tratta del numero massimo di elementi che possono essere spostati in un dato momento:

- 100 elementi in movimento/secondo per MSE-3310
- 650 elementi in movimento/secondo per MSE-3350

Latenza completa del sistema:

- Client e tag: dieci secondi a pieno carico con 650 elementi in movimento/secondo (inizia con il software WLC versione 5.1)

La latenza è anche correlata alla finestra di aggregazione NMSP, che può essere ottimizzata. Vedere la sezione **Configurazione/tuning del tag RFID e del WLC** nella sottosezione intitolata "Quanto tempo tra le iterazioni?"

- Numero massimo di sessioni applicazione: 1024
  - Numero massimo di destinazioni dell'API northbound: 1024
  - Numero massimo di aree di copertura: 50/piano Le dimensioni dell'area di copertura non possono essere inferiori alla precisione di posizione tipica (10 m). La dimensione di copertura tipica è di almeno 50 piedi per 50 piedi (2.500 piedi quadrati).
- **Numero di punti di accesso per piano:**

MSE/2710 non presenta limitazioni. La restrizione principale è dovuta alla raccomandazione di avere meno di 100 punti di accesso secondo le raccomandazioni del Sistema colori Windows - altrimenti le mappe del Sistema colori Windows diventano ingestibili, forniscono una risoluzione scarsa e creano molto lentamente i dettagli delle mappe. Esiste inoltre un limite al numero di dispositivi rilevati che è possibile visualizzare in una mappa del Sistema colori Windows.

• **Numero di controller per MSE:**

Lo stesso controller può essere sincronizzato con più MSE con alcune eccezioni:

1. Se il controller è in codice 4.2 o 5.0, non sono supportate più connessioni NMSP, quindi non è necessario sincronizzarle con più di un MSE.
2. WLC con wIPS AP: impossibile stabilire una connessione NMSP con più di MSE. Ciò è dovuto al fatto che il punto di accesso wIPS può comunicare con un solo MSE che esegue servizi adattivi wIPS.

Un WLC può avere fino a 10 connessioni NMSP.

Un MSE supporta fino a 500 connessioni NMSP. Ma è importante comprendere questo aspetto dal punto di vista dell'implementazione CAS. Ogni WLC è in grado di tenere traccia di diversi client (5000 client per WLC4400). Quindi in implementazioni pragmatiche con pochissimi controller MSE CAS raggiunge il suo limite di tracciabilità fino a 18000 dispositivi. Ci sono due soffitti di vetro che si dovrebbe tenere a mente, uno è 5000 client per controller e l'altro è 18000 dispositivi per MSE 3350. Se raggiungiamo uno di questi limiti, massimizziamo la capacità del sistema.

C'è sempre un limite nell'eseguire test di scalabilità e abbiamo eseguito stress test con 100 controller per MSE che eseguono il traffico di posizione.

• **Numero di MSE per WCS:**

Sebbene MSE possa essere gestito da un singolo sistema WCS, quest'ultimo può gestire più sistemi MSE. Il sistema WCS è caratterizzato da limiti da diverse prospettive che possono determinare il numero di MSE che è in grado di gestire in base alla distribuzione di tali unità tra i sistemi MSE. Pertanto, entrano in gioco fattori quali il numero massimo di elementi supportati, il numero massimo di piani supportati o il numero massimo di punti di accesso supportati. Ufficialmente Dell supporta 5 MSE per sistema WCS.

• **Numero di progetti di rete:**

Non esistono limiti per i progetti di rete aggiunti a MSE. Tuttavia Aeroscout engine ha un limite a seconda del numero di piani, dimensioni e quantità di elementi per MSE. Il numero massimo di piani è limitato a 255. E supponendo che i dispositivi installati ogni 60m e la risoluzione griglia di 1m, installazione piccola può supportare 15 mappe e installazione grande (requisiti di memoria più elevati) può supportare 90 mappe.

## Notifiche Northbound

MSE può inoltrare tutti i dati dei tag noti a un listener SOAP in direzione nord. Se configurato, ogni volta che un frame di notifica dei tag viene segnalato al MSE o ogni volta che il MSE calcola la posizione di un tag, può inviare una notifica al listener. Ciò è utile se le applicazioni di terze parti desiderano ricevere aggiornamenti istantanei ogni volta che si sente un tag, anziché eseguire query periodiche. È possibile configurare questa opzione tramite l'interfaccia utente Parametri di notifica: **Servizi > Servizi di mobilità > Servizio sensibile al contesto > Avanzate > Parametri di notifica**.

Per supportare le notifiche Northbound, attenersi alle raccomandazioni seguenti:

- La distanza tra i normali beacon di tag non può essere inferiore a tre o cinque minuti.
- L'intervallo di frame di notifica dei tag per lo spostamento dei tag deve essere compreso tra uno e dieci secondi.
- Il limite della coda per i parametri di notifica deve essere impostato su un valore maggiore del numero di tag supportati.
- Assicurarsi che il listener SOAP non si arresti.
- Verificare che il listener SOAP restituisca una SOAP envelope vuota valida in risposta alla notifica.
- Verificare che il listener SOAP elabori rapidamente le notifiche in entrata.

Se queste condizioni non vengono soddisfatte, la coda di notifica di MSE può essere sottoposta a overflow. Questa condizione è visibile nella pagina Parametri di notifica come contatore "Notifiche eliminate" (vedere la **Figura 44**).

### Figura 44: Notifiche Northbound

- System
- Context Aware Service**
  - General
  - Administration
  - Wired
  - Advanced
    - Location Parameters
    - Notification Parameters**
  - Partner Engine
- wIPS Service

## Notification Parameters: MSE4

Services > Mobility Services > Context Aware Service > Advanced > Notification Parameters

### Northbound Notifications

Northbound Notifications  Enable

Tags

Chokepoints

Telemetry

Emergency

Battery Level

Vendor Data

Include tag location information in notification

	IP Address	Port	Transport
Destination1	<input type="text"/>	<input type="text"/>	SOAP
Destination2	<input type="text"/>	<input type="text"/>	SOAP
Destination3	<input type="text"/>	<input type="text"/>	SOAP

### Advanced

Rate Limit  0 - 9999999 msec

**Queue Limit  1 - 99999**

Retry Count  0-60

Refresh Time  0 - 99999 mins

Notifications Dropped

Questa intera sezione è valida solo se il listener in direzione nord non è in grado di gestire il traffico di notifiche in direzione nord e desidera eliminarle a meno che il tag non abbia qualcosa di importante (o di interessante) da segnalare:

Filtra le notifiche in direzione nord in base ai payload dei tag di interesse per rendere il sistema più scalabile. Ad esempio, se un tag segnala ogni pochi secondi, ma il payload del tag contiene solo informazioni sulla batteria o telemetria di movimento che non sono di interesse, la generazione di eventi in direzione nord alla ricezione di questi payload del tag può essere eliminata.

Il filtro eventi Northbound è controllato da sei nuovi parametri nel file aes-config.xml:

```
<entry key="send-event-on-location-calc">true</entry>
<entry key="send-event-on-every-beacon">true</entry>
<entry key="send-event-on-vendor">true</entry>
<entry key="send-event-on-emergency">true</entry>
<entry key="send-event-on-chokepoint">true</entry>
<entry key="send-event-on-telemetry">true</entry>
```

Per ricevere TUTTE le notifiche, attivare il calcolo send-event-on-location-calc e send-event-on-

each-beacon. Se ogni singolo payload tag non è importante, impostarlo in modo selettivo. Ad esempio, per fare in modo che MSE invii le notifiche solo per il calcolo della posizione, per fare in modo che prema un pulsante di chiamata o per attivare un'occorrenza di punto di interruzione. (Impostare su **"true"** nel file. NON ELIMINARE QUESTI VALORI!):

```
send-event-on-location-calc  
send-event-on-emergency  
send-event-on-chokepoint
```

Disattivare gli altri tre flag.

```
After install/upgrade, ssh into MSE and issue the following commands :  
rm /opt/mse/locserver/conf/aes-config.xml (won't exist for new install)  
/etc/init.d/msed start (creates the aes-config.xml)  
/etc/init.d/msed stop  
vi /opt/mse/locserver/conf/aes-config.xml
```

Modificare i filtri in base alle proprie esigenze. Salvate il file e uscite. Riavviare il processo indesiderato.

```
/etc/init.d/msed start
```

Per ulteriori dettagli sulla notifica, consultare il documento [API](#).

## [Tag RFID e configurazione/tuning WLC](#)

Un tag RFID è un dispositivo Wi-Fi dotato di un trasmettitore e un'antenna. Non è associato ai punti di accesso, quindi non si comporta come altri client wireless. Un tag RFID trasmette informazioni su base periodica, ovvero frame di notifica dei tag, ossia pacchetti multicast inviati a bassa velocità di trasmissione dati. Ogni x secondi, il tag RFID invia il frame di notifica del tag y sui canali configurati. Si consiglia di trasmettere i frame di notifica dei tag con un'intensità del segnale di 17 dBm. Quando completa un ciclo su tutti i canali configurati, il tag RFID rimane in standby e attende il periodo di trasmissione successivo per trasmettere i frame di notifica dei tag.

Quando si distribuisce la tecnologia RFID per il monitoraggio degli asset in Wi-Fi, è necessario configurare questa funzionalità:

### **1. Quanti frame di notifica tag per canale trasmetterà il tag RFID?**

Data la natura del traffico multicast sulle reti 802.11, è buona norma aumentare il numero di frame di notifica dei tag per canale.

In un ambiente RF pulito, i punti di accesso ricevono gli aggiornamenti dei tag e li segnalano al proprio WLC, anche se il tag è configurato per inviare un frame di notifica tag per canale. Nelle implementazioni reali, esiste un'alta probabilità che un aggiornamento dei tag non venga eseguito su un determinato punto di accesso a causa del rumore RF o di altre attività. La mancanza di un aggiornamento di tag in un punto di accesso vicino può causare calcoli di posizione non corretti. Ripetere il numero di frame di notifica dei tag per canale su due o tre, invece di quello predefinito, per ridurre la possibilità che l'aggiornamento dei tag non venga udito dagli access point vicini.

Anche la durata della batteria è un aspetto importante dell'accuratezza e dell'intervallo di

fotogramma per la notifica dei tag e spesso è necessario scendere a compromessi. Per tenere traccia degli oggetti in movimento, si consiglia di utilizzare i tag di rilevazione del movimento. Configurate un intervallo di fotogrammi di notifica tag, da 3 a 5 minuti quando stazionario, e aumentate l'intervallo di fotogrammi di 1 o 2 secondi quando in movimento per garantire una buona accuratezza e una lunga durata della batteria. La configurazione e le raccomandazioni per le best practice possono essere ottenute dalla produzione di etichette

Fare riferimento alla [documentazione di AeroScout](#).

Un altro modo per compensare la perdita di aggiornamento di un tag su un determinato Access Point è aumentare il valore di scadenza RFID RSSI sul WLC. Il valore consigliato deve essere tre volte il periodo di intervallo + 5 secondi. Con questo valore, l'ultimo RSSI sul WLC viene mantenuto se un access point non rileva l'ultima iterazione da un determinato tag. I nuovi aggiornamenti vengono inviati a MSE insieme ai dati conservati delle iterazioni precedenti.

Uno svantaggio di questo approccio è che può incidere sulla precisione. Se la trasmissione del movimento non è abilitata su un tag RFID e il tag si allontana rapidamente dall'ultima posizione in cui ha trasmesso un frame di notifica del tag, il calcolo della posizione si basa sui vecchi dati. Si consiglia di abilitare la funzione di Motion Probing per basare sempre il calcolo della posizione su nuovi dati AP e mantenere i timer WLC il più basso possibile per ridurre la latenza.

**Nota:** il codice WLC 5.x fornisce un nuovo comando che ha effetto anche sui dati conservati sul WLC. Questo timer di scadenza è configurabile singolarmente per tag RFID, client e router. L'impostazione di scadenza predefinita è di cinque secondi, che elimina i dati non aggiornati dal controller più vecchio di cinque secondi. L'impostazione di timeout RFID controlla il tempo totale in cui un tag RFID viene conservato sul controller dopo essere andato fuori intervallo o aver arrestato la trasmissione. La combinazione di questi timer con le impostazioni complementari sul MSE può fornire un'accuratezza ottimale con aggiornamenti NMSP minimi tra i controller e il MSE.

La scadenza RFID RSSI può essere configurata con la CLI WLC:

```
(Cisco Controller) >config location expiry tags ?
```

```
<seconds>      Time in seconds
```

Questo comando consente di verificare se un punto di accesso rileva un determinato tag RFID:

```
(Cisco Controller) >show location ap-detect rfid ?
```

```
<AP name>      Display information for AP name
```

## 2. Quali canali?

Nella distribuzione a 2,4 GHz, i canali 1, 6 e 11 sono i canali non sovrapposti nello spettro. I canali consigliati da configurare su un tag RFID sono 1, 6 e 11. Si noti che in alcuni scenari un punto di accesso è in grado di ascoltare gli aggiornamenti dei tag RFID su un canale diverso da quello su cui opera. Per impostazione predefinita, l'AP rifiuta questi aggiornamenti e non li inoltra al WLC.

## 3. Quanto tempo intercorre tra le iterazioni?

La configurazione dell'intervallo di frame di notifica dei tag svolge un ruolo importante per il rilevamento della posizione poiché definisce la separazione temporale tra i calcoli o gli aggiornamenti della posizione. Come accennato in precedenza, l'intervallo di fotogramma per la notifica dei tag deve essere configurato in modo da garantire una durata della batteria e una

precisione di posizionamento ottimali, ovvero 3-5 minuti per i tag fissi.

Tenete presente che quando un tag viene spostato, sono necessarie ulteriori informazioni in tempo reale per calcolare la posizione. Quando si tiene traccia delle etichette in movimento, la trasmissione del movimento deve essere attivata sul tag RFID con un intervallo di fotogrammi di notifica tag inferiore a 10 secondi.

#### **4. Quanto tempo attende un RFID tra due trasmissioni di frame?**

Quando trasmettono fotogrammi o segnali, un tag RFID Aeroscount attende un periodo di tempo preconfigurato tra le trasmissioni. Questo tempo di attesa può essere di 128, 256 o 512 millisecondi ed è noto come "Intervallo di ripetizione messaggio". Se sono stati configurati 512 msec e il tag sta inviando un beacon per canale, il tag RFID completa un'iterazione entro circa 1,5 secondi. Se vengono inviati due frame per canale con lo stesso "Intervallo di ripetizione messaggio", il tag completa un'iterazione entro 3 secondi.

Il tag RFID trasmette la quantità configurata di frame su un canale specifico e quindi si sposta sul canale successivo per eseguire la stessa routine. Il tempo che separa ogni trasmissione di frame è noto come "Intervallo di ripetizione del messaggio".

È fondamentale che il WLC riceva gli aggiornamenti dei tag da tutti gli access point che contribuiscono sui canali 1, 6 e 11 prima di inviare questi dati al MSE tramite l'NMSP. Il WLC attende un periodo di tempo configurabile, denominato finestra di aggregazione, prima di inviare l'elenco di access point vicino per un tag RFID al MSE.

A partire dal software WLC 5.1, la finestra di aggregazione NMSP è configurabile ed è impostata su due secondi per impostazione predefinita. Nelle versioni precedenti alla 5.1, la finestra di aggregazione sul WLC è di otto secondi e non è configurabile. Se un controller riceve lo stesso pacchetto da più access point nella stessa finestra di aggregazione, elimina i duplicati. Se riceve alcuni pacchetti in una finestra e il resto nel successivo, invia un pacchetto duplicato (il primo nella seconda finestra) ma scarta il resto dei duplicati.

È importante configurare le dimensioni corrette della finestra di aggregazione in modo da assicurarsi che il WLC abbia ricevuto aggiornamenti da tutti gli access point. Questa finestra deve essere maggiore del tempo impiegato da un tag RFID per completare un ciclo. La pratica comune è quella di aggiungere almeno un secondo in più per assicurarsi che il WLC attenda abbastanza. La configurazione di una finestra di aggregazione ridotta comporta un calcolo errato della posizione.

La funzione CCA (Clear Channel Assessment) consente di aumentare il tempo necessario per il completamento di tutti e tre gli aggiornamenti dei canali per un tag RFID. La maggior parte delle etichette RFID esegue il rilevamento portante prima della trasmissione. Se il supporto wireless è occupato, si ritorna indietro per un periodo di tempo aggiuntivo e si astiene dalla trasmissione. Trascorso un periodo di tempo predefinito, se il supporto non è impostato, trasmette e passa al canale successivo. Se il supporto è ancora occupato, il tag sospende la trasmissione per l'iterazione del canale e passa al canale successivo. Il tempo massimo per il backoff non è fisso e può variare da fornitore a fornitore.

**Nota:** quando si usano le versioni del software WLC 4.x o WLC 5.x insieme al MSE, la finestra di aggregazione NMSP sul MSE è impostata su 8 secondi.

## **[Configurazione e tuning di WCS e MSE](#)**



Esistono numerosi parametri di configurazione importanti che possono essere configurati in WCS e MSE che possono influire sulla localizzazione (vedere la **Figura 45**).











Figura 45: Parametri posizione

## Location Parameters: MSEWCS4

Services > Mobility Services > Context Aware Service > Advanced > Location Parameters

### Location Parameters

---

Enable calculation time 	<input type="checkbox"/> Enable
Enable OW Location 	<input type="checkbox"/> Enable
Relative discard RSSI time 	<input type="text" value="3"/> 1 - 99999 min
Absolute discard RSSI time 	<input type="text" value="60"/> 1 - 99999 min
RSSI Cutoff 	<input type="text" value="-75"/> -90 to -50 dBm
Enable Location Filtering 	<input checked="" type="checkbox"/> Enable
Chokepoint Usage 	<input checked="" type="checkbox"/> Enable
Use Chokepoints for Interfloor conflicts 	<input type="text" value="Never"/>
Chokepoint Out of Range Timeout 	<input type="text" value="60"/> 1-99999 secs
Absent Data cleanup interval 	<input type="text" value="1440"/> 1 - 99999 mins

Il limite RSSI è un campo importante che può essere regolato per un particolare ambiente. Questo campo specifica il valore RSSI minimo al di sotto del quale MSE ignora quando calcola la posizione per un determinato elemento. Questo valore è applicabile solo ai clienti di rilevamento, ovvero non si applica al rilevamento dei tag.

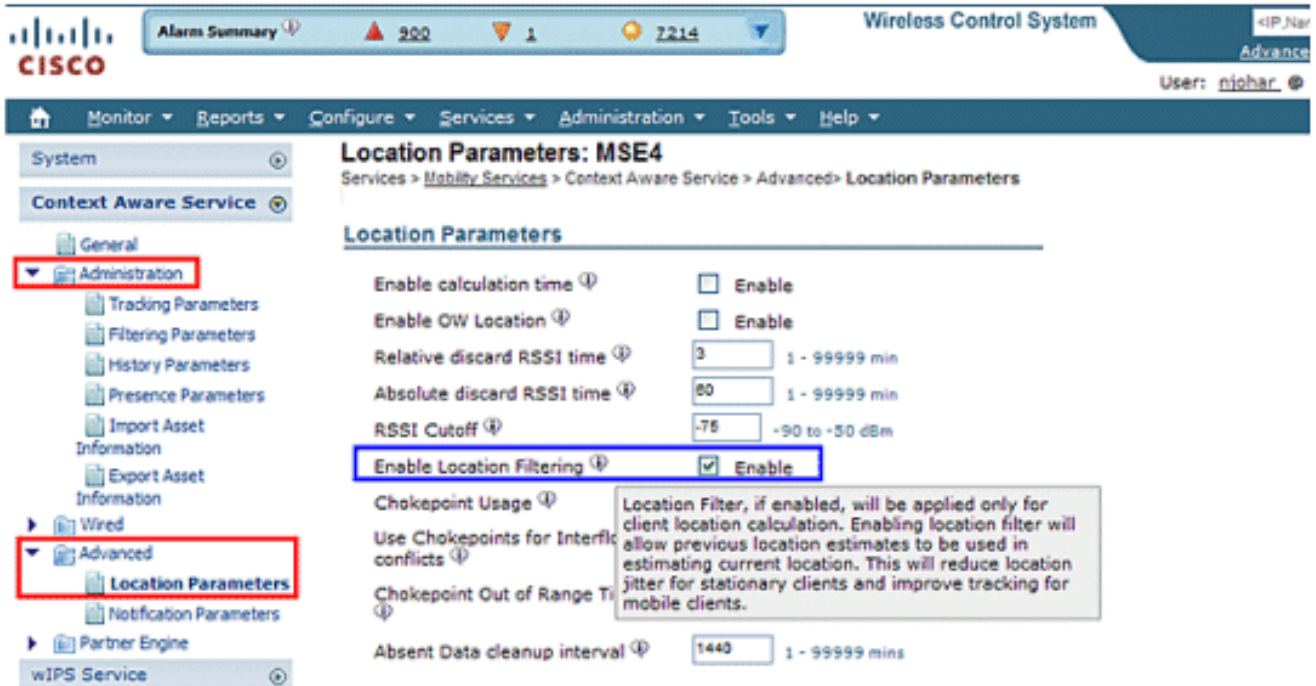
Se si specifica un limite RSSI molto alto, ad esempio -60 o -50 con densità AP bassa, il calcolo della posizione risulta errato in quanto il valore MSE esclude dal calcolo i valori RSSI degli access point di ascolto affidabili.

Se si utilizza un limite RSSI basso, ad esempio -85 di -90 e si opera in un'area di spazio aperto o con pareti basse, le aree di attenuazione tra i pavimenti determinano un calcolo di posizione inadeguato, in quanto il valore MSE include nel calcolo i valori RSSI degli access point esterni.

Sebbene il limite RSSI sia un valore fisso, l'algoritmo compensa i valori mancanti quando integra i valori RSSI inferiori dell'ultima iterazione o prende i valori dal relativo repository di eliminazione. Idealmente, il valore ottimale di limite RSSI consente di avere più di cinque punti di accesso con valori RSSI superiori a -75 dBm dallo stesso piano. Gli edifici che presentano una perdita di RF non caratteristica possono richiedere la regolazione di questo parametro, ma in genere rappresentano un'indicazione di un'installazione non ottimale.

**Variazione:** Prima della release 5.2, MSE utilizzava un meccanismo di localizzazione smussata per tenere traccia dei client. Per i clienti è stata calcolata la media mobile, ovvero è stata calcolata la media dei movimenti dei clienti. A partire dalla versione 5.2 del software, l'intero meccanismo è stato sostituito dai "filtri di posizione". Il filtro percorso viene applicato internamente per ogni client. MSE tiene traccia di quali client vengono spostati e quali rimangono fermi e applica i filtri di conseguenza. Ciò riduce lo jitter complessivo del sistema. Il filtro percorso è abilitato per impostazione predefinita. Vedere la **Figura 46**.

**Figura 46: Filtro percorso**



**Comunicazione WCS/MSE:** Si consiglia di configurare la comunicazione tra WCS e MSE:

- **MSE:** HTTPS è sempre abilitato (impostazione predefinita). HTTP è disabilitato per impostazione predefinita. L'abilitazione del protocollo HTTP richiede la configurazione manuale tramite l'accesso alla console (diretto o ssh) in MSE.
- **Sistema colori Windows:** Per impostazione predefinita, WCS utilizza HTTPS per comunicare con MSE. HTTP può essere abilitato tramite l'interfaccia utente di WCS.

In alcuni casi, WCS non è in grado di comunicare con MSE tramite HTTPS. In questo caso, l'aggiunta di MSE a WCS o la pagina Salva in MSE: Proprietà generali consente di continuare a segnalare l'errore "Connessione HTTPS al server non riuscita". MSE deve essere raggiungibile da WCS e il comando "getserverinfo" su MSE fornisce informazioni sullo stato. È consigliabile abilitare il protocollo HTTP su MSE e consentire a WCS di comunicare con MSE tramite il protocollo HTTP.

Su MSE, il supporto HTTP è disponibile nelle versioni 5.1, 5.2 e 6.0.

**Abilitare HTTP su MSE con software versione 6.0:** Accedere a MSE tramite ssh/console. Immettere questo comando

```
root@mse ~]# enablehttp
```

**Abilitare HTTP su MSE con software versione 5.x:** Accedere a MSE tramite ssh/console. Immettere questo comando

```
[root@mse ~]# getdatabaseparams
<DB PASSWORD>
```

Questo comando restituisce la password db. Utilizzare questa password in questo comando:

```
[root@mse ~]# /opt/mse/locserver/bin/tools/solid/solsql "tcp 2315" dba <DB PASSWORD>
Solid SQL Editor (teletype) v.06.00.1049
Copyright ©) Solid Information Technology Ltd 1993-2008
Connected to 'tcp 2315'.
Execute SQL statements terminated by a semicolon.
Exit by giving command: exit;
```

```
update AESSERVERINFO set USEHTTP=1;
Command completed successfully, 1 rows affected.
```

```
commit work;
Command completed successfully, 0 rows affected.
```

Premere Ctrl-C per uscire dalla shell del database. Eseguire il riavvio della piattaforma MSE con `/etc/init.d/mse stop; /etc/init.d/mse start`.

### Abilitare la comunicazione HTTP da WCS (versione software 6.x) a MSE:

- Verificare che HTTP sia abilitato su MSE con i passaggi precedenti.
- In Sistema colori Windows scegliere HTTP nella pagina Proprietà generali di MSE. In questo modo viene attivata la comunicazione HTTP tra WCS e MSE. Vedere la **Figura 47**.

WCS inizia ora a comunicare con MSE tramite HTTP.

**Nota:** per abilitare HTTP su WCS 5.2, fare riferimento alla [Guida alla configurazione di WCS 5.2](#).

**Figura 47: Abilitazione della comunicazione HTTP tra MSE e WCS**

The screenshot shows the 'General Properties: MSE4' configuration page. The left sidebar contains a tree view with 'System' expanded, showing 'General Properties' selected. The main content area has two tabs: 'General' and 'Performance'. The 'Performance' tab is active, displaying 'Server Details' with the following information:

Device Name	MSE4
Device Type	Cisco 3350 Mobility Services Engine
Device UDI	"AIR-MSE-3350-K9:V01:MXQ828A4L9"
Version	6.0.62.0
Start Time	5/6/09 5:43 PM
IP Address	172.20.224.30
Contact Name	Joe
Username	admin
Password	*****
HTTP	<input checked="" type="checkbox"/> Enable
Legacy Port	8001
Legacy HTTPS	<input type="checkbox"/> Enable

## Licenze MSE

Le licenze MSE sono necessarie per recuperare le informazioni contestuali su tag e client dai punti di accesso a partire dal codice 6.0. La licenza del client include il monitoraggio dei client wireless/cablati, dei client non autorizzati e dei punti di accesso non autorizzati. Le licenze per i codici di matricola e i client sono offerte in modo indipendente. Le licenze per etichette e clienti sono disponibili in diverse quantità, da 1.000, 3.000, 6.000 e 12.000 dispositivi. Cisco offre licenze per client e tag. La creazione effettiva di licenze e la gestione di informazioni relative allo SKU sono gestite dal sistema di licenze FlexLM sviluppato e gestito dal team SWIFT.

Sistema colori Windows è il sistema di gestione utilizzato per installare le licenze client e IPS su MSE. Le licenze per i tag devono essere attivate tramite AeroScout e installate su MSE con AeroScout Systems Manager.

Per informazioni dettagliate sulle licenze MSE, fare riferimento alla [Guida agli ordini e alle licenze di Cisco Mobility Services Engine 3300 Series](#).

## Nuovi acquisti

### Client

- Il cliente acquista la licenza software e riceve la chiave di autorizzazione del prodotto (PAK) per posta (documento di licenza).
- Il cliente registra la chiave PAK per i client sul sito <https://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet> (solo utenti [registrati](#)).
- Immettere le informazioni UDI MSE nel campo "ID host". Accettare il contratto e continuare. La licenza viene inviata al cliente tramite e-mail.
- È possibile ottenere MSE UDI nel Sistema colori Windows tramite le seguenti schede: **Servizi > Servizi di mobilità > MSE > Sistema > Proprietà generali**
- Senza una licenza, MSE fornisce la funzionalità "prova prima di acquistare" per 60 giorni (licenza di valutazione).
- La licenza di valutazione è basata sull'uso ed è valida per 60 giorni; può essere esteso una sola volta.
- Limiti licenza di valutazione: Client: 100Tag: 100AP wIPS: 20
- La licenza di valutazione viene sempre applicata, ma se il limite della piattaforma è stato raggiunto in base alle licenze installate, è comunque possibile utilizzare la licenza di valutazione di un servizio separato. Ad esempio, se un cliente ha un MSE-3350 e ha installato licenze per tenere traccia dei dispositivi a 18K (client e/o tag) e i dispositivi a 18K sono attivamente tracciati, può comunque usare una licenza di valutazione per wIPS, anche se viene superato il limite della piattaforma.
- Il timer della licenza di valutazione inizia dal giorno in cui viene generata, quindi l'estensione della licenza di valutazione deve essere installata immediatamente.
- Una volta installata, la licenza viene utilizzata in base al tipo di servizio abilitato/disabilitato.
- Se la licenza di valutazione scade e MSE non viene riavviato, i servizi MSE di base continuano a essere eseguiti e i servizi concessi in licenza, ad esempio Context Aware, continuano a essere eseguiti, ma non viene tenuta traccia dei dispositivi.
- Se la licenza di valutazione scade e MSE viene riavviato, i servizi concessi in licenza non vengono avviati. I dispositivi non vengono rilevati.

**Se la chiave PAK non è disponibile**

- Accedere allo strumento Stato ordine di vendita all'indirizzo <http://tools.cisco.com/qtc/status/tool/action/LoadOrderQueryScreen>.
- Dall'elenco a discesa Tipo di query scegliere **Ordine di vendita da**.
- Inserire il numero dell'ordine di vendita nel campo Valore.
- Visualizzare selezionando **Show Serial Number** (Mostra numero di serie), quindi fare clic su **Search** (Cerca).
- Viene visualizzata la finestra con le informazioni dettagliate sull'ordine MSE.
- Nella finestra Dettagli ordine della tabella fare clic su **Espandi riga 1.1**.
- Nella colonna Product (Prodotto), seconda riga, copiare il numero PAK (che inizia con 3201J) che si desidera registrare per ottenere la licenza.
- Per registrare la chiave PAK, visitare il sito <https://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet> (solo utenti [registrati](#)).
- Fare clic sul link di registrazione della licenza del prodotto da sinistra, immettere il numero PAK nel campo vuoto e inviare.
- Immettere le informazioni UDI MSE nel campo ID host. Accettare il contratto e continuare.
- Viene generata una licenza e viene inviata un'e-mail al tuo ID e-mail.

## Tag

1. Il cliente acquista la licenza software e riceve la chiave di autorizzazione del prodotto (PAK) per posta (documento di licenza).
2. Il cliente registra la chiave PAK per i tag all'indirizzo <http://support.AeroScout.com>.
3. Se non si dispone di un account, crearne uno nuovo con il collegamento "Crea nuovo account".
4. Una volta creato l'account, si riceve un messaggio di posta elettronica di notifica contenente il nome utente e la password.
5. Accedere al [portale di supporto AeroScout](#).
6. Nella scheda Home fare clic sul collegamento "Registra i prodotti acquistati da Cisco".
7. Registrare i prodotti e fornire i recapiti, PAK#, MSE ID (MSE S\N) e il tipo di installazione. Viene visualizzato un messaggio di posta elettronica che conferma la registrazione.
8. Il numero di serie SE può essere richiamato dalle schede WCS:**Servizi > Servizi di mobilità > MSE > Parametri avanzati**
9. AeroScout verifica il numero PAK entro due giorni lavorativi. Dopo la verifica, una notifica che contiene la chiave di licenza, istruzioni su come scaricare il software Context Aware Engine e le guide utente pertinenti vengono inviate al tuo indirizzo e-mail. Se il numero PAK non è valido, occorre registrare nuovamente un numero PAK valido.

## Aggiornamento - Licenza client

1. Il cliente acquista la nuova licenza e riceve la chiave PAK con la posta.
2. Il cliente riceve la chiave PAK e ottiene la chiave di licenza tramite e-mail.
3. Il cliente installa la chiave di licenza su MSE.
4. **Aggiunta del numero di licenze di valutazione (quando il numero di licenze client esistenti/installate è uguale a MSE max.):** WCS consente di aggiungere la licenza di valutazione anche se è stato raggiunto il numero massimo di dispositivi (client) MSE. Ad esempio, se il cliente ha installato MSE-3350, una licenza client 18K e desidera aggiungere la registrazione dei tag e/o i servizi WiFi, WCS può aggiungere una licenza di valutazione per uno o entrambi i servizi.

## Aggiornamento - Contrassegna licenza

- **Aggiunta del numero di licenze per i tag (quando il numero di licenze per i tag esistenti/installati è inferiore al numero massimo di MSE):** La licenza per i tag esistente viene sovrascritta da una nuova licenza. Ad esempio, se un cliente ha una licenza per tenere traccia dei tag 1K e desidera effettuare l'aggiornamento per tenere traccia dei tag 4K, acquista una licenza 3K da aggiungere alla licenza 1K esistente. AeroScout emette una licenza per i tag 4K che copre l'intero nuovo numero di tag.
- **Aggiunta del numero di licenze per i tag (se il numero di licenze per i tag esistenti/installati è uguale a MSE max.):** AeroScout System Manager restituisce un messaggio di errore. La licenza tag esistente rimane attiva. Ad esempio, un cliente ha installato MSE-3350 e una licenza per tag 18K su MSE. Se tentano di installare una licenza con tag 3K, AeroScout System Manager visualizza un messaggio di errore. È necessario eliminare manualmente la licenza tag da MSE poiché AeroScout System Manager non è in grado di eliminare le licenze tag. Per eliminare la nuova licenza per i tag, il cliente deve disinstallare l'immagine MSE, rimuovere l'opzione del database e reinstallare il software MSE.
- **Aggiunta del numero di licenze di valutazione (se il numero di licenze tag esistenti/installate è uguale al massimo a MSE):** WCS consente di aggiungere una licenza di valutazione anche se è stato raggiunto il numero massimo di dispositivi (tag) MSE. Ad esempio, se il cliente ha installato MSE-3350, una licenza con tag 18K e desidera aggiungere la registrazione dei client e/o i servizi WiFi, può aggiungere una licenza di valutazione per uno dei due servizi o per entrambi.

#### **Clienti esistenti (applicabile solo quando si esegue l'aggiornamento alla versione software 6.0)**

1. Visitare il sito <https://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet> (solo utenti [registrati](#)) per registrare la chiave PAK per i client e ottenere la chiave di licenza, come spiegato sopra nella sezione Nuovi acquisti. Se la chiave PAK è stata spostata, il cliente deve chiamare Cisco TAC/GLO.
2. Installare il file di licenza in MSE tramite WCS.
3. La licenza è legata all'UID MSE.
4. Composto da una piattaforma (MSE 3310 o 3350) e da un numero di serie univoco. UDI di esempio: AIR-MSE-3310-K9:V01:QCN1224001Y. Nell'esempio, il numero di serie è QCN1224001Y.
5. La licenza MSE è legata all'UDI (Unique Device Identifier). Se la stessa unità è fissabile, l'UDI è lo stesso e la stessa licenza può essere riallocata, ma se l'unità deve essere sostituita, l'UDI cambia, quindi deve essere generata una nuova licenza. MSE non accetta la licenza se l'UDI non corrisponde. I clienti possono chiamare Cisco TAC e fornire la vecchia e la nuova UDI. Cisco TAC disattiva la vecchia licenza e ne rilascia una nuova.
6. Il modello MSE-3350 è in grado di controllare fino a 18.000 dispositivi (con qualsiasi combinazione di client e tag) acquistando la licenza corretta. Gli aggiornamenti sulle posizioni degli elementi tracciati vengono forniti al modulo dei servizi di mobilità dal controller LAN wireless Cisco.
7. Nelle mappe, nelle query e nei report di Cisco WCS è possibile visualizzare solo gli elementi indicati per il rilevamento dal controller. Non vengono raccolti eventi o allarmi per gli elementi non tracciati e nessuno viene utilizzato per calcolare il limite di 18.000 elementi per client o tag.

Dopo aver installato correttamente la licenza, il tipo di licenza viene visualizzato come "Permanente", come mostrato nella **Figura 48**.

#### **Figura 48: Centro licenze**

## License Center

Administration > License Center > Summary > MSE Summary

Entries 1 - 3 of 3

MSE Name (UDI)	Type	Limit	Count	Unlicensed Count	% Used	License Type	Status
<b>(H) mse-3350 ( AIR-MSE-3350-K9:V01:MXQ821A31P)</b>							
	wIPS Monitor Mode APs	20	0	0	0%	Evaluation ( 60 days left)	Inactive
	Tag Elements	100	0	0	0%	Evaluation ( 60 days left)	Active
	Client Elements	100	0	0	0%	Evaluation ( 60 days left)	Active
<b>(H) heitz-3350 ( AIR-MSE-3350-K9:V01:USE810N5HR)</b>							
	wIPS Monitor Mode APs	20	0	0	0%	Evaluation ( 59 days left)	Active
	Tag Elements	100	5	0	5%	Evaluation ( 59 days left)	Active
	Client Elements	100	100	372	100%	Evaluation ( 59 days left)	Active
<b>(L) heitz-3310 ( AIR-MSE-3310-K9:V01:QSH78150059)</b>							
	wIPS Monitor Mode APs	20	0	0	0%	Evaluation ( Less than a day left )	Inactive
	Tag Elements	1000	4	0	0%	Permanent	Active
	Client Elements	1000	667	0	66%	Permanent	Active

**Nota:** quando un client o un tag rimane inattivo per 24 ore, non vengono più conteggiati rispetto al numero di licenze corrispondente.

Il file di licenza è memorizzato in "opt/mse/licensing" (scelta/modalità/licenza).

Quando si esegue l'aggiornamento da MSE 5.x a 6.x, verificare che i seguenti passaggi siano seguiti in sequenza:

1. Con WCS, eseguire un backup del database MSE di MSE 5.x, ovvero il sistema MSE attualmente in esecuzione.
2. Per eseguire il backup dei dati e della configurazione per i tag, consultare la [guida alla configurazione del software del servizio sensibile al contesto](#).
3. Aggiornare MSE al software 6.x. I messaggi di avviso vengono visualizzati durante il processo di aggiornamento su MSE in relazione alle licenze al momento dell'installazione.
4. Installare la licenza MSE tramite WCS. Viene visualizzato un messaggio di avviso se viene installata una licenza di capacità superiore a quella del sistema MSE e il processo di installazione della licenza viene bloccato. Ad esempio, se un cliente dispone di un MSE-3310 e tenta di installare una licenza client 6K, viene visualizzato un messaggio di avviso in quanto un MSE-3310 può rilevare un massimo di dispositivi 2K.
5. Ripristinare il database MSE con WCS.
6. Per ripristinare i dati e la configurazione del motore di tag, consultare la [documentazione di AeroScout](#).
7. Per i dettagli su questi passaggi, fare riferimento all'Appendice B di questo documento e alla [Guida alla configurazione sensibile al contesto per la release 6.x](#). **Nota:** con la versione software 6.0 per il controllo dei tag, le configurazioni del motore AeroScout e i dati delle licenze vengono conservati nei processi di backup e ripristino di WCS/MSE. Le configurazioni eseguite su MSE con versioni software precedenti alla 6.0 non vengono conservate automaticamente. Se si esegue l'aggiornamento dalla versione 6.0 alla 6.x, i dati di configurazione vengono conservati quando si utilizza la procedura di backup/ripristino MSE, come descritto nella documentazione di Cisco. Se un cliente esegue l'aggiornamento dalla versione 5.2 alla 6.0, deve seguire la procedura manuale descritta nella

[documentazione AeroScout](#) .**Attenzione:** quando si esegue l'aggiornamento alla release 6.x in assenza della licenza appropriata, il numero di client, tag e access point (wIPS) supportati viene reimpostato su 100 client, 100 tag e 20 AP. Tutti gli elementi tranne 100 sono contrassegnati come inattivi. I dati cronologici per tutti gli elementi rilevati rimangono nel database e possono essere recuperati nell'API della posizione su MSE. Tali limiti corrispondono alle licenze di valutazione della durata di 60 giorni fornite per impostazione predefinita su MSE non concesso in licenza.

Modificare questi parametri di tracciamento con Cisco WCS (vedere la **Figura 49**):

1. Abilitare e disabilitare le posizioni degli elementi (client cablati/wireless, codici di matricola attivi, client non autorizzati e punti di accesso) di cui si tiene traccia attivamente.
2. Impostare i limiti sul numero di elementi specifici di cui si desidera tenere traccia.
3. Ad esempio, con una licenza client di 12.000 dispositivi rintracciabili (cablati/wireless), è possibile impostare un limite per il rilevamento di solo 8.000 stazioni client (lasciando 4.000 dispositivi disponibili per il monitoraggio di client e punti di accesso non autorizzati). Una volta raggiunto il limite di tracciabilità per un determinato elemento, il numero di elementi non tracciati viene riepilogato nella pagina Parametri di tracciabilità.
4. Disabilitare la registrazione e la creazione di report per i client non autorizzati e i punti di accesso ad hoc.

**Figura 49: Parametri di rilevamento per i servizi sensibili al contesto**

The screenshot displays the 'Tracking Parameters: MSE4' configuration page. The left sidebar shows the navigation tree with 'Administration' > 'Tracking Parameters' selected. The main content area features two tables. The first table, 'Network Location Service Elements', has a 'Licensed Limit = 6000' and includes columns for 'Enable', 'Tracking Parameters', 'Enable Limiting', 'Limit Value', 'Active Value', and 'Not Tracked'. It lists 'Wireless Clients' (323 active), 'Wired Clients' (0 active), and 'Rogue Clients and AccessPoints' (1149 active). The second table, 'Asset Tracking Elements', has a 'Licensed Limit = 100' and lists 'Active RFID Tags' (20 active).

Network Location Service Elements: Licensed Limit = 6000					
Enable	Tracking Parameters	Enable Limiting	Limit Value	Active Value	Not Tracked
<input checked="" type="checkbox"/>	Wireless Clients	<input checked="" type="checkbox"/>	200	323	0
<input checked="" type="checkbox"/>	Wired Clients	<input type="checkbox"/>	0	0	0
<input checked="" type="checkbox"/>	Rogue Clients and AccessPoints	<input type="checkbox"/>	0	1149	0
<input type="checkbox"/> Exclude Adhoc Rogue APs					

Asset Tracking Elements: Licensed Limit = 100					
Enable	Tracking Parameters	Enable Limiting	Limit Value	Active Value	Not Tracked
<input checked="" type="checkbox"/>	Active RFID Tags	<input type="checkbox"/>	100	20	0

Il numero effettivo di client registrati è determinato dalla licenza acquistata.

**Valore attivo** (vedere **Figura 49**): Indica il numero di stazioni client attualmente rilevate.

**Non tracciato** (vedere **Figura 49**): Indica il numero di stazioni client oltre il limite.

Gli elementi in eccesso (tag/client/non autorizzati) non verranno tracciati come mostrato nella **Figura 50**.

**Figura 50: Utilizzo licenza**



MSE Name (UDI)	Type	Limit	Count	Unlicensed Count	% Used	License Type	Status
<b>(H) mse-3350 (AIR-MSE-3350-K9:V01:MXQ821A31P)</b>							
	wIPS Monitor Mode APs	20	0	0	0%	Evaluation ( 60 days left)	Inactive
	Tag Elements	100	0	0	0%	Evaluation ( 60 days left)	Active
	Client Elements	100	0	0	0%	Evaluation ( 60 days left)	Active
<b>(H) heitz-3350 (AIR-MSE-3350-K9:V01:USE810N5HR)</b>							
	wIPS Monitor Mode APs	20	0	0	0%	Evaluation ( 59 days left)	Active
	Tag Elements	100	5	0	5%	Evaluation ( 59 days left)	Active
	Client Elements	100	100	372	372%	Evaluation ( 59 days left)	Active

### Modalità di scalabilità di più servizi

MSE con la versione software 6.0 supporta il funzionamento simultaneo di Context-Aware e WIPS. Vengono imposti limiti di coesistenza delle funzionalità. Le combinazioni oltre il limite non saranno supportate da TAC e non sono possibili perché non è possibile aggiungere una licenza che causerà il superamento della capacità MSE.

Le combinazioni supportate sono mostrate nelle figure 51 e 52.

Figura 51: Capacità del sistema MSE-3350 : AP in modalità monitoraggio wIPS e dispositivi sensibili al contesto

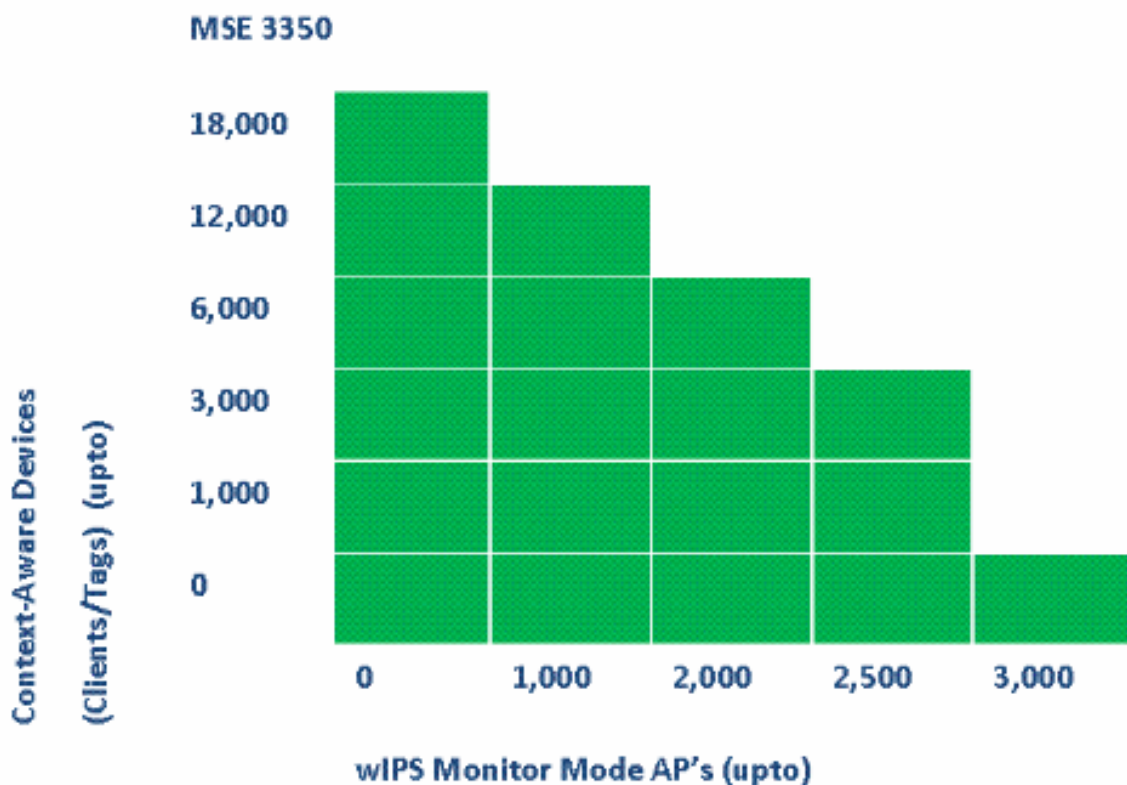
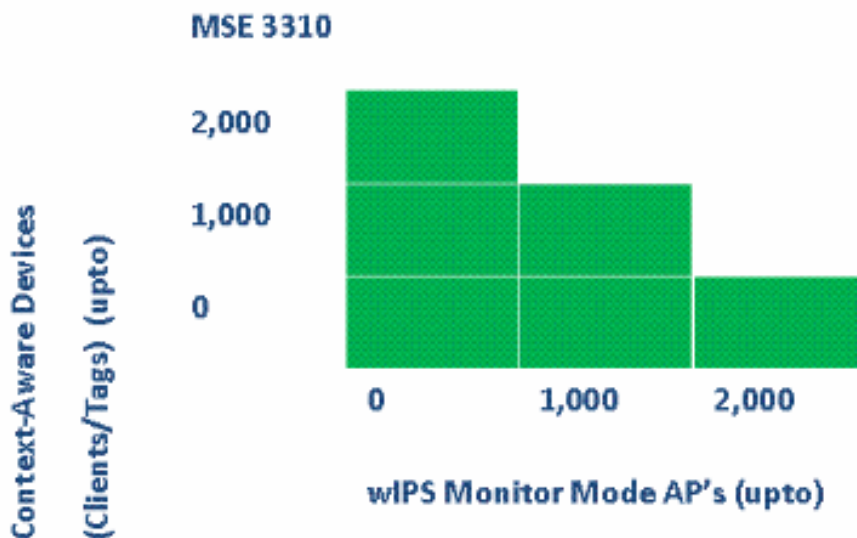


Figura 52: Capacità del sistema MSE-3310 : AP in modalità monitoraggio wIPS e dispositivi sensibili al contesto



Alcuni esempi:

- Il cliente è interessato a tenere traccia dei dispositivi 6K utilizzando il servizio sensibile al contesto, quindi ha la capacità di avere fino a 2.000 punti di accesso in modalità monitor wIPS su MSE 3350
- Il cliente è interessato a tenere traccia dei dispositivi 3K utilizzando il servizio Context-Aware, quindi ha la capacità di avere fino a 2.500 punti di accesso in modalità monitor wIPS su MSE 3350
- Il cliente è interessato a tenere traccia dei dispositivi 1K utilizzando il servizio sensibile al contesto, quindi ha la capacità di avere fino a 1.000 punti di accesso in modalità monitor wIPS su MSE 3310 e una capacità di avere 2.500 punti di accesso in modalità monitor wIPS su MSE 3350

## Risoluzione dei problemi

### MSE non è raggiungibile

Se MSE viene rilevato come non raggiungibile dal punto di vista di WCS, le possibili cause possono essere le seguenti:

- Le credenziali di accesso API in WCS non sono configurate correttamente. L'accessorio dispone di due gruppi di credenziali: uno per l'interfaccia shell dell'accessorio e l'altro per le credenziali API. WCS richiede le credenziali API quando aggiunge MSE. Fare riferimento all'Appendice A di questo documento.
- Le regole di connettività di route e firewall bloccano la connettività tra WCS e MSE. Fare riferimento alla sezione "Verifica della connettività di rete" in questo documento.
- L'attività in background relativa allo stato del servizio Mobility di Servizi Windows è stata disabilitata. Abilitarlo in WCS tramite **Amministrazione > Attività in background > Altre attività in background > Stato servizio Mobility** .
- Il riconoscimento del contesto del servizio MSE è abilitato e attivo dalla CLI di MSE.
- In rari casi, HTTPS può presentare problemi di connettività. È possibile attivare l'opzione

HTTP in Proprietà generali di MSE in WCS. Per ulteriori informazioni, consultare la sezione "Comunicazione WCS/MSE" di questo documento.

- MSE si è schiantato. Su MSE, CLI "getserverinfo" non può restituire un output. Raccogliere tutti i registri nella directory/opt/mse/logs e contattare Cisco TAC.

### **Nessun elemento individuato**

Se in MSE non sono presenti elementi, le possibili cause sono le seguenti:

- MSE non è raggiungibile.
- La licenza di valutazione è scaduta.
- MSE è raggiungibile e viene applicata una licenza, ma il servizio del modulo sensibile al contesto MSE non è abilitato.
- Il rilevamento per client e/o tag non è abilitato nella pagina Parametri di rilevamento MSE. Per ulteriori informazioni, consultare la sezione "Licenze MSE" di questo documento.
- I progetti di rete e/o i controller non sono stati sincronizzati con MSE.
- Punti di accesso non posizionati nelle mappe WCS.
- Non sono stabilite connessioni NMSP tra MSE e controller. Per ulteriori informazioni, vedere la sezione "Verifica della connessione NMSP tra WLC e MSE" di questo documento.
- I punti di accesso in WCS hanno antenne non Cisco (il tipo scelto è "Altro"). In questo caso, i punti di accesso in WCS devono essere impostati su un altro tipo di antenna supportato in modo simile e la progettazione di rete risincronizzata con MSE.
- Il controller WLC non rileva i client. Risoluzione dei problemi sul WLC con "show client summary" della CLI.
- Il controller WLC (Wireless LAN Controller) non rileva i tag RFID attivi. Risoluzione dei problemi sul WLC con "show rfid summary" della CLI.

### **Tag non individuati**

Quando i tag non vengono individuati (ma sono presenti altri client), è possibile che si sia verificato un problema all'interno di AeroScout Engine; le possibili cause sono:

- Il WLC non tiene traccia delle etichette RFID attive. Questo comando deve essere presente nella configurazione WLC: config rfid status enable.
- Il controller WLC (Wireless LAN Controller) non rileva i tag RFID attivi. Risoluzione dei problemi sul WLC con "show rfid summary" della CLI.
- I tag vengono visualizzati dal WLC ma non nel WCS. Verificare che le notifiche NMSP vengano inviate a MSE con questo comando: debug rfid nmsp enable.
- AeroScout Engine non installato in MSE. Nelle release 5.1 e 5.2 il motore deve essere installato separatamente. A partire dalla versione 6.0, il motore viene fornito con MSE.
- La licenza non è installata per AeroScout Engine.
- AeroScout Engine non viene registrato con MSE. Controllare la pagina Stato Partner Engine in WCS.
- MSE contiene troppe mappe o le mappe sono troppo grandi. Fare riferimento alle linee guida del motore AeroScout.
- Dopo un aggiornamento, può essere necessario ripristinare la configurazione nel motore AeroScout.
- La mappa del pavimento non contiene un'immagine (risolta nelle versioni recenti).
- MSE tiene traccia solo dei tag compatibili con CCX e la distribuzione include solo tag non CCX non supportati oppure questi tag non sono stati configurati per la trasmissione in formato

CCX.

### Alcuni elementi non sono individuati (client o tag)

Se MSE tiene traccia di alcuni elementi, ma altri non sono visibili, le possibili cause possono essere le seguenti:

- MSE viene eseguito su una licenza di valutazione, limitata a 100 elementi.
- MSE viene eseguito con una licenza valida, ma la capacità è stata superata, pertanto gli eventuali elementi aggiuntivi (client/tag/server non autorizzati) vengono eliminati.
- Alcuni controller non dispongono di connettività NMSP con MSE.
- L'elemento è scomparso dalla rete e non trasmette più. MSE memorizza l'elemento nel record della cronologia, ma scompare dalle schermate di WCS.
- Le opzioni di filtro sono state applicate nei livelli Mappe WCS impedendo la visualizzazione di alcuni elementi.
- Le opzioni di filtro MAC sono abilitate nei parametri di filtro MSE, eliminando alcuni elementi.
- MSE tiene traccia solo dei tag compatibili con CCX; l'implementazione prevede una combinazione di tag CCX e non CCX.
- Estensione per la risoluzione dei problemi di client/tag per il percorso: Verificare se WCS vede il client? Tramite SNMP, questa funzionalità esiste già per i client. (Risoluzione dei problemi del client). È necessario estendere questa funzionalità per i tag. Cercare il client nella posizione dei controller assegnati. Usare il comando WLC **show client summary**. Determinare quanto tempo fa il WLC ha visto il client usare il comando WLC **show client <indirizzo MAC>**. Determinare quando i punti di accesso hanno visto l'ultima volta il client con il comando WLC **show client <indirizzo MAC>**.

### WLC non connesso a MSE

Quando un controller non stabilisce la connettività con MSE, le possibili cause sono le seguenti:

- Il controller non è raggiungibile dal punto di vista di MSE o WCS.
- Problema temporaneo di connettività con il controller. Impossibile eseguire il push della chiave di sicurezza hash per la connessione SNMP. Verificare la connettività SNMP tra WCS e Controller.
- Il controller e MSE non hanno una configurazione NTP corretta o la differenza di tempo è significativa. Configurare correttamente gli orari.
- I controller precedenti alla versione 4.2 non supportano NMSP.
- I controller precedenti alla release 5.1 non supportano più connessioni MSE.
- Se un controller è assegnato a un MSE con wIPS abilitato, lo stesso controller non può essere assegnato contemporaneamente a un altro MSE.
- WCS non dispone di accesso in lettura/scrittura al WLC al termine della sincronizzazione. Il sistema WCS non è quindi in grado di eseguire il push dell'indirizzo MAC MSE e dell'hash della chiave nel WLC.

### Le notifiche non raggiungono le applicazioni di partner esterni

Nei casi in cui un'applicazione partner non riceve notifiche da MSE, i motivi possibili sono i seguenti:

- La connettività tra MSE e l'applicazione esterna non è stabilita. Verificare il traffico XML/API.
- L'applicazione listener esterna è inattiva.
- Il listener esterno è lento nell'analisi delle notifiche in arrivo. In questo caso, MSE attende

l'elaborazione del listener esterno, il che può causare congestione nelle code in uscita di MSE.

- MSE rifiuta le notifiche a causa delle dimensioni relativamente ridotte della coda in uscita rispetto alla quantità di frame di notifica dei tag previsti nella rete. Verificare che le etichette abbiano una configurazione ragionevole, in particolare per l'accelerazione/deaccelerazione del movimento. Aumentare le dimensioni della coda nei parametri di notifica di MSE. Fare riferimento alla sezione "Notifica Northbound" in questo documento.

### **La postazione cablata non funziona**

Se non viene tenuta traccia di alcun elemento quando si utilizza la posizione cablata, i possibili motivi sono i seguenti:

- Problema di connettività NMSP tra MSE e switch cablati.
- Lo switch cablato esegue una versione precedente che non supporta la posizione cablata.
- La versione dello switch cablato è corretta, ma NMSP non è abilitato. Abilitarlo con l'opzione CLI.
- Per avviare il rilevamento dei client connessi, è necessario che l'opzione di rilevamento IP sia abilitata sullo switch cablato.
- Switch cablato non aggiunto a WCS.
- Possibili problemi durante l'aggiunta di uno switch cablato in WCS:Stringhe della community SNMP errate.OID switch non supportato in WCS.
- Lo switch cablato è stato aggiunto a WCS ma non è sincronizzato con MSE.
- Lo switch cablato è disponibile per la sincronizzazione. Verificare che lo switch sia stato aggiunto con il flag "Location Capable" abilitato in WCS.
- Gli switch cablati supportano solo una connessione NMSP con MSE.
- Tracciamento reti cablate non abilitato nei parametri di tracciamento MSE.

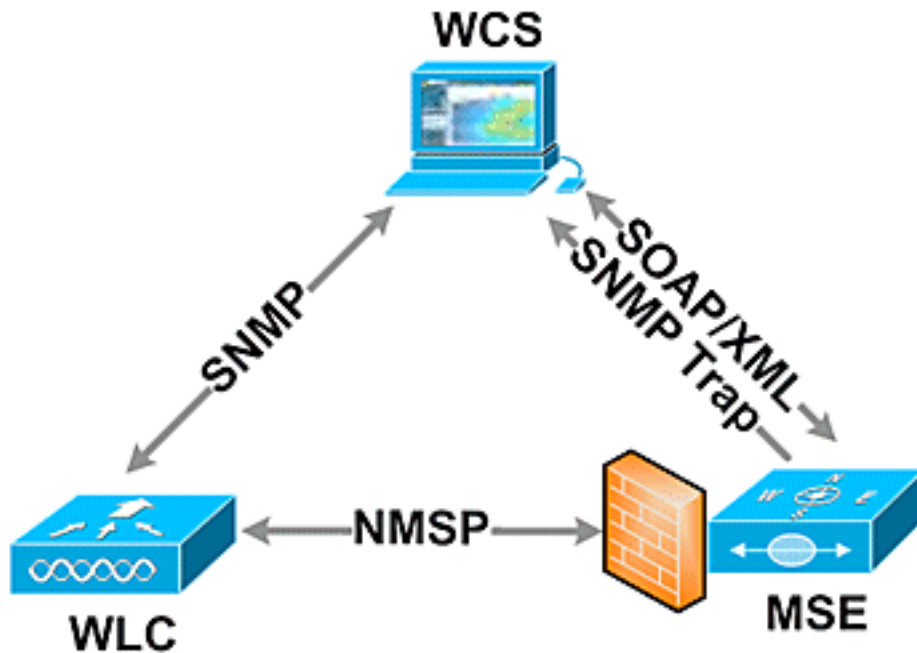
### **Licenze MSE**

- Messaggio di mancata corrispondenza UDI quando si installa la licenza - Le licenze MSE sono legate a MSE UDI, quindi accertarsi che la licenza installata sia stata creata per MSE corretto. Non è possibile scambiare licenze tra MSE diversi.
- L'installazione della licenza è bloccata a causa di un elemento che supera il limite consentito per tale MSE. Verificare la capacità della licenza per ogni servizio su piattaforme MSE diverse, come descritto nella sezione Prefazione.
- È possibile che venga visualizzato un errore se si tenta di installare o eliminare due licenze contemporaneamente. Il motivo è che ogni volta che vengono installate le licenze CAS, vengono riavviati tutti i servizi e ogni volta che viene installata la licenza wIPS, viene riavviato il servizio wIPS. Prima di procedere all'installazione immediata di un'altra licenza, verificare che tutti i servizi siano disponibili.
- Le licenze MSE vengono installate in /opt/mse/licenses.

### **Verifica della connettività di rete**

Verificare che nessun firewall blocchi la connettività tra MSE, WLC e WCS. Se è necessario creare un firewall per queste caselle, creare regole per i caratteri jolly in modo che questi computer possano comunicare tra loro in modo corretto (vedere la **Figura 53**).

### **Figura 53: Verifica della connettività di rete**



## Verifica della connessione NMSP tra WLC e MSE

```
(Cisco Controller) >show nmsp status
```

LocServer IP	TxEchoResp	RxEchoReq	TxData	RxData
172.20.224.17	18006	18006	163023	10

```
(Cisco Controller) >show auth-list
```

```
<snip>
```

Mac Addr	Cert Type	Key Hash
00:1e:0b:61:35:60	LBS-SSC	5384ed3cedc68eb9c05d36d98b62b06700c707d9

Se la connessione NMSP non viene stabilita dopo l'aggiunta di MSE a WCS, una possibile causa è la discrepanza di clock tra WLC e MSE. Si consiglia di utilizzare un server NTP per sincronizzare gli orologi. Se ciò non è possibile, gli orologi del WLC e del MSE possono essere configurati manualmente. Il problema principale degli orologi di sistema è assicurarsi che l'ora WLC non sia in ritardo rispetto a quella impostata sul MSE.

**Nota:** la sincronizzazione dell'ora tra i controller è essenziale in distribuzioni WLC multiple di grandi dimensioni.

Se non viene ancora stabilita una sessione NMSP, l'amministratore di rete può configurare manualmente la sessione NMSP immettendo l'hash della chiave MSE nel WLC.

```

MSE
root@mse ~]# cmdshell
cmd> show server-auth-info
invoke command: com.aes.server.cli.CmdGetServerAuthInfo
-----
Server Auth Info
-----
MAC Address: 00:1e:0b:61:35:60
Key Hash: 5384ed3cedc68eb9c05d36d98b62b06700c707d9
Certificate Type: SSC
  
```

WLC  
(Cisco controller) >config auth-list add lbs-ssc <MSE Ethernet MAC> <MSE key hash>  
**Verificare che MSE sia operativo e riceva le informazioni sui tag e sui client dal WLC**

Il comando **getserverinfo** sul server MSE restituisce questo output:

```
[root@MSEWCS4 ~]# getserverinfo
MSE Platform is up, getting the status

-----
Server Config
-----

Product name: Cisco Mobility Service Engine
Version: 6.0.49.0
Hw Version: V01
Hw Product Identifier: AIR-MSE-3350-K9
Hw Serial Number: MXQ828A4L9
Use HTTP: false
Legacy HTTPS: false
Legacy Port: 8001
Log Modules: 262143
Log Level: INFO
Days to keep events: 2
Session timeout in mins: 30
DB backup in days: 2

-----
Services
-----

Service Name: Context Aware Service
Service Version: 6.0.35.0
Admin Status: Enabled
Operation Status: Up

Service Name: Wireless Intrusion Protection Service
Service Version: 1.0.1096.0
Admin Status: Enabled
Operation Status: Up

-----
Server Monitor
-----

Mon Mar 16 14:43:52 PDT 2009
Server current time: Thu Apr 02 14:55:00 PDT 2009
Server timezone: America/Los_Angeles
Server timezone offset: -28800000
Restarts: 3
Used Memory (bytes): 166925392
Allocated Memory (bytes): 238354432
Max Memory (bytes): 1908932608
DB virtual memory (kbytes): 6694
DB virtual memory limit (bytes): 0
DB disk memory (bytes): 241696768
DB free size (kbytes): 6304

-----
Active Sessions
```

```
-----  
Session ID: 17155  
Session User ID: 1  
Session IP Address: 172.20.224.30  
Session start time: Tue Mar 17 16:50:48 PDT 2009  
Session last access time: Thu Apr 02 14:50:30 PDT 2009
```

```
-----  
Context Aware Service  
-----
```

```
Total Active Elements(Clients, Rogues, Interferers): 2263  
Active Clients: 591  
Active Tags: 24  
Active Rogues: 1648  
Active Interferers: 0  
Active Wired Clients: 0  
Active Elements(Clients, Rogues, Interferers) Limit: 6000  
Active Tag Limit: 100  
Active Wired Clients Limit: 0  
Active Sessions: 1  
Clients Not Tracked due to the limiting: 0  
Tags Not Tracked due to the limiting: 0  
Rogues Not Tracked due to the limiting: 0  
Interferers Not Tracked due to the limiting: 0  
Wired Clients Not Tracked due to the limiting: 0  
Total Elements(Clients, Rogues, Interferers)  
  Not Tracked due to the limiting: 0
```

```
-----  
Context Aware Sub Services  
-----
```

```
Sub Service Name: AeroScout  
Version: 3.2.0 - 4.0.14.9  
Description: AeroScout@ Location Engine  
  for RSSI and TDOA asset tracking  
Registered: true  
Active: true  
Watchdog Process ID: 8492  
Engine Process ID: 8665  
[root@MSEWCS4 ~]#
```

## **Verifica che il tag RFID sia visualizzato dal WLC**

I tag devono essere configurati per la trasmissione su 3 canali (1,6,11) e con 3 o più ripetizioni.

Esempio: 1,6,11, 1,6,11, 1,6,11

Controllare la configurazione RFID globale sul controller.

```
show rfid config
```

Se il rilevamento tag RFID non è abilitato, abilitarlo con questo comando:

```
config rfid status enable
```

Verificare/impostare i parametri di timeout.



```
config rfid timeout 1200
config rfid auto-timeout disable
```

Controllare il timeout di scadenza RSSI.

```
show location summary
```

Se il tag non viene ancora visualizzato dal WLC, utilizzare i seguenti comandi di debug:

```
debug mac addr <tag mac addr>
debug rfid receive enable
```

Verificare se il WLC vede il tag.

```
show rfid summary
show rfid detail <MAC address>
```

Se il tag viene visualizzato dal WLC ma non nel WCS, verificare se le notifiche NMSP vengono inviate a MSE.

```
debug rfid nmsp enable
```

Verificare che la notifica NMSP sia abilitata sul WLC

```
show nmsp subscription summary
Server IPServices
<MSE IP>RSSI, Info, Statistics, IDS
```

Verificare se il livello NMSP sul WLC invia una notifica.

```
debug nmsp message tx enable
```

Limite RSSI: MSE mantiene i quattro valori di intensità del segnale più alti e tutti i report di intensità del segnale che soddisfano o superano il valore limite RSSI. Predefinito = -75 dBm

comando **show rfid summary** (WLC)

Questo comando elenca tutte le etichette RFID segnalate dagli access point, incluse le seguenti informazioni:

- Indirizzo MAC RFID
- Punto di accesso più vicino
- Valore RSSI
- Tempo trascorso dall'ultima udienza del tag

```
(Cisco Controller) >show rfid summary
Total Number of RFID : 4
```

```
-----
RFID ID      VENDOR      Closest AP      RSSI  Time Since Last Heard
-----
00:04:f1:00:04:ea Wherenet  sjc14-42b-ap4   -69   52 seconds ago
00:04:f1:00:04:eb Wherenet  sjc14-42b-ap4   -75   27 seconds ago
00:0c:cc:5b:fc:54 Aerosct   sjc14-31b-ap9   -87   63 seconds ago
00:0c:cc:5b:fe:29 Aerosct   sjc14-31b-ap2   -92   22 seconds ago
```

## comando **show rfid detail**

Questo comando fornisce i dettagli dei parametri per un tag RFID quando specifica l'indirizzo MAC.

```
(Cisco Controller) >show rfid detail 00:0c:cc:5b:fe:29

RFID address..... 00:0c:cc:5b:fe:29
Vendor..... Aerosct
Last Heard..... 4 seconds ago
Packets Received..... 561211
Bytes Received..... 16836330
Detected Polling Interval..... 14 seconds
Bluesoft Type..... TYPE_NORMAL
Battery Status..... MEDIUM
Nearby AP Statistics:
    sjc14-41b-ap8(slot 0, chan 6) 3 seconds.... -88 dBm
```

```
(Cisco Controller) >
```

## **Verificare che il client Wi-Fi sia visto dal WLC**

Determinare gli access point a cui è associato il client e i valori RSSI rilevati dagli access point.

```
show client summary
show client detail <MAC address>
```

Verificare che i timeout RSSI per il client siano impostati sui valori predefiniti.

```
show location summary
```

Se i valori RSSI sono diversi dai valori predefiniti, impostarli come predefiniti con i seguenti comandi di configurazione:

```
config location expiry client <seconds>
config location rssi-half-life client <seconds>
```

Abilitare i debug di bilanciamento del carico; mostrare gli access point che hanno ascoltato il client e con quale RSSI.

```
debug mac addr <client mac>
debug dot11 load-balancing enable
```

Problemi correlati alle notifiche di debug con questi comandi:

```
debug mac addr <client mac>
debug dot11 locp enable
debug nmsp message tx enable
```

## comando "show client summary"

```
(Cisco Controller) >show client summary
```

```
Number of Clients..... 276
```

```
<snip>
```

```

MAC Address      AP Name      Status      WLAN/Guest-Lan Auth Protocol Port Wired
-----
00:02:8a:ea:55:15 sjc14-12b-ap5 Associated 7 Yes 802.11b 2 No

```

comando "show client detail"

Cisco Controller) >show client detail 00:02:8a:ea:55:15

<snip>

```

Nearby AP Statistics:
TxExcessiveRetries: 0
TxRetries: 0
RtsSuccessCnt: 0
RtsFailCnt: 0
TxFiltered: 0
TxRateProfile: [0,0,0,0,0,0,0,0,0,0,0,0]
sjc14-11b-ap2(slot 0) .....
antenna0: 308 seconds ago -86 dBm.....
antenna1: 308 seconds ago -80 dBm
sjc14-11b-ap1(slot 0) .....
antenna0: 307 seconds ago -82 dBm.....
antenna1: 307 seconds ago -91 dBm
sjc14-12b-ap6(slot 0) .....
antenna0: 307 seconds ago -66 dBm.....
antenna1: 307 seconds ago -66 dBm
sjc14-12b-ap3(slot 0) .....
antenna0: 307 seconds ago -76 dBm.....
antenna1: 307 seconds ago -64 dBm
sjc14-12b-ap5(slot 0) .....
antenna0: 7217 seconds ago -53 dBm.....
antenna1: 7217 seconds ago -48 dBm
sjc14-11b-ap5(slot 0) .....
antenna0: 7217 seconds ago -79 dBm.....
antenna1: 7217 seconds ago -75 dBm

```

## Sezione 4: Elenco di controllo finale

### Requisiti hardware

Tabella 3. Cisco MSE 3310 - Specifiche hardware

Articolo	Descrizione
Fattore di forma	Fattore di forma rack 1U Altezza 1,75" (4,45 cm), profondità 27,75" (70,5 cm)
Processore	Intel Core2 Duo (1,8 GHz)
Memoria	4 GB (PC2-5300)
Dischi rigidi	2 SATA da 250 GB
Capacità	Fino a 2.000 dispositivi (fino a 1.000 client e fino a 1.000 tag)

tracciabilità ubicazione	
Connettività	Rete: Due schede di rete Gigabit multifunzione integrate con TCP/IP Offload Engine
Alimentatori	Un alimentatore CA da 120/240 V
Gestione della rete	Cisco WCS Location versione 5.2 o successiva con Internet Explorer 6.0/Service Pack 1 o versione successiva
Dispositivi di rete supportati	Cisco serie 2100, 4400 Wireless LAN Controller; Cisco Catalyst serie 6500 Wireless Services Module, Cisco Catalyst 3750G Integrated Wireless LAN Controller, Cisco Wireless LAN Controller Module (WLCM e WLCM-E) per router di servizi integrati; Cisco Aironet Lightweight Access Point

**Tabella 4. Cisco MSE 3550 - Specifiche hardware**

<b>Articolo</b>	<b>Descrizione</b>
Fattore di forma	Fattore di forma rack 1U Altezza 1,75" (4,45 cm), profondità 27,75" (70,5 cm)
Processore	Due processori Intel Xeon quad-core (2,33 GHz)
Memoria	PC2-5300 da 8 GB (4 x 2 GB)
Dischi rigidi	Unità SAS (Serial Attached SCSI) hot-plug: 2 x 146 GB (10.000 rpm)
Capacità tracciabilità ubicazione	Fino a 18.000 dispositivi (qualsiasi combinazione di client e tag)
Connettività	Rete: Due schede di rete Gigabit multifunzione integrate con TCP/IP Offload Engine
Alimentatori	Due CA ridondanti da 120/240 V (sostituibili a caldo)
Gestione della rete	Cisco WCS Location versione 5.1 o successiva con Internet Explorer 6.0/Service Pack 1 o versione successiva

Dispositivi di rete supportati	Cisco serie 2100, 4400 Wireless LAN Controller; Cisco Catalyst serie 6500 Wireless Services Module, Cisco Catalyst 3750G Integrated Wireless LAN Controller, Cisco Wireless LAN Controller Module (WLCM e WLCM-E) per router di servizi integrati; Cisco Aironet Lightweight Access Point
--------------------------------	---

## Migrazione di Location Services da Cisco 2710 a Cisco MSE

Prima dell'introduzione della piattaforma MSE, Cisco offriva servizi basati sulla posizione con la soluzione basata su Cisco 2710. **La tabella 5** mette a confronto le due soluzioni e mostra i vantaggi della soluzione MSE.

**Tabella 5. Cisco 2710 rispetto a Cisco MSE**

Funzionalità	Cisco 2710	MSE
Ambienti dei clienti supportati	RSSI (Indoor Low-Ceiling)	Indoor low-ceiling (RSSI) Indoor high-ceiling (TDOA) Outdoor (TDOA)
Tecnologie di localizzazione supportate	Solo RSSI	RSSI TODOA
Motori di posizione supportati	Solo Cisco	Motore Cisco Partner
Max numero di dispositivi Wi-Fi rilevati	2,500	18,000
Numero di servizi supportati	Singolo (solo ubicazione)	Multipli (soluzione di mobilità sensibile al contesto, wIPS, servizi futuri)
Tag supportati	CCX o non CCX (solo polling)	CCX
Guide e regioni	Sì (client e tag)	Sì (solo client) Tag - funzionalità Celle e maschere AeroScout
Sensori di posizione	Non supportato	Non supportato

Per i clienti con installazioni di Cisco 2710 esistenti, è possibile migrare e mantenere la configurazione su un nuovo Cisco MSE.

### Requisiti software

I Cisco Aironet serie 1000 Access Point per software sensibile al contesto sono supportati solo nella versione 4.2.xxx (xxx>112).

**Nota:** i Cisco Aironet serie 1000 Access Point non sono più commercializzati. I Cisco Aironet serie 1000 Access Point per la soluzione sensibile al contesto di Cisco sono supportati solo nella versione 4.2.xxx (xxx>112). È supportata solo la soluzione sensibile al contesto di Cisco su Cisco serie 3300 Mobility Services Engine; Cisco serie 3300 Mobility Services Engine non supporta o non supporterà altri servizi. Le versioni 5.x.xxx e quelle future del software non supportano i Cisco Aironet serie 1000 Access Point. I clienti sono invitati a migrare ai Cisco Aironet serie 1130, 1140, 1240 o 1250 Access Point per sfruttare i vantaggi delle nuove funzionalità introdotte. Contattare Cisco per ulteriori informazioni relative ai prodotti sostitutivi.

**Nella tabella 6** sono elencate le versioni software da utilizzare su MSE, WLC e WCS. Ogni colonna verticale rappresenta versioni compatibili per MSE, WLC e WCS.

**Tabella 6. Matrice di compatibilità software**

Servizi o	Componente del sistema	Versione minima del software			
		Release	Release	Release	Release
CASA S e WIPS <sup>1</sup>	MSE	Release 5.1.30.0	Release 5.1.35.0	Release 5.2.91.0	Release 6.0.75.0
	Cisco Wireless LAN Controller (WLC)	Release 4.2: 4.2.130 (o superiore) Release 5.1: 5.1.151.0 (o superiore)	Release 4.2: 4.2.130 (o superiore) Release 5.1: 5.1.163.0 (o superiore)	Release 4.2: 4.2.130 (o superiore) Release 5.2: 5.2.157.0 (o superiore) Release 5.1: 5.1.151.0 (o superiore), o	Release 4.2: 4.2.130 (o superiore) Release 5.2: 5.2.157.0 (o superiore) Release 5.1: 5.1.151.0 (o superiore) Release 6.0: 6.0.182.0 o successiva <b>Nota:</b> La release 5.0.x non supporta MSE.
	Cisco WCS	Release 5.1: 5.1.64.0 (o superiore)	Release 5.1.65.4 (o superiore)	Release 5.2: 5.2.110.0 (o superiore)	Release 6.0: 6.0.132.0 o superiore
	Cisco WCS Navig	Release 1.3.64.	Release 1.3.65.	release 1.4.10.0 o successiva)	release 1.4.10.0 o successiva)

	ator	0 (o succes siva)	4 (o succes siva)		
--	------	-------------------------	-------------------------	--	--

**Nota:** <sup>1</sup> la release 5.2 è il requisito software minimo per il supporto di wIPS sul controller, WCS e MSE.

**Nota:** la versione del software WCS deve essere uguale alla versione del software MSE, ovvero, se si esegue MSE 6.0.x, anche WCS deve essere 6.0.x. Le licenze vengono applicate a partire dal software versione 6.0.

## Elenco di controllo per la distribuzione

### Pianificazione wireless

- Seguire le linee guida di posizionamento dell'access point appropriate (posizione e densità). Garantire una corretta copertura del perimetro AP. È possibile utilizzare Strumento di pianificazione Sistema colori Windows per determinare la densità e il posizionamento dei punti di accesso.
- Verificare la copertura Wi-Fi utilizzando lo strumento di indagine del sito e WCS (Location Readiness Tool).
- Verificare il posizionamento dell'access point per eliminare i fori di copertura. Utilizzare i punti di accesso in modalità di monitoraggio ottimizzato per la posizione per riempire i fori di copertura.
- Specificare quali controller devono comunicare con quale MSE utilizzando la pagina Sincronizzazione MSE di Sistema colori Windows.
- Verificare che i certificati siano scambiati correttamente.

### WLC

- Verificare che tutti i punti di accesso/radio siano attivi e che Radio Resource Manager (RRM) sia abilitato
  - Configurare il server NTP su entrambi i WLC e MSE o sincronizzare manualmente entrambi i dispositivi (e preferibilmente il WCS) con l'ora e il fuso orario corretti. **Nota:** il WLC utilizza l'ora GMT(UTC) con il fuso orario corretto per derivare l'ora locale, quindi è necessario immettere l'ora in UTC e specificare il fuso orario corretto.
  - Verificare che i client/tag siano rilevati dal WLC con questo comando `show [rfid] riepilogo [client]`
  - Verificare che NMSP sia stabilito tra MSE e il controller con questo comando su WLC `show nmsp status` o su WCS tramite **Servizi > Servizi di mobilità > "MSE" > Sistema > Sessioni attive**
  - Verificare se WLC è stato sottoscritto per i servizi appropriati con questo comando `show nmsp subscription summary`
  - Se si verifica l'accuratezza del client CCX, accertarsi che CCX sia abilitato. `config location plm client enable <interval>` Per verificare la configurazione, utilizzare questo comando `show location plm`
  - Il WLC deve avere i seguenti parametri nmsp predefiniti:
    - Algoritmo utilizzato: **Cliente**
    - Timeout scadenza RSSI: 5 sec
    - Mezza vita: 0 sec
    - Soglia di notifica: 0 db
    - Taratura client**
    - Timeout scadenza RSSI: 5 sec
    - Mezza vita: 0 sec
    - Rogue AP**
    - Timeout scadenza RSSI: 5 sec
    - Mezza vita: 0 sec
    - Soglia di notifica: 0 db
    - Tag RFID**
    - Timeout scadenza RSSI: 5 sec
    - Mezza vita: 0 sec
    - Soglia di notifica: 0 db
- Comando di configurazione **percorso di configurazione <cmd>** Per controllare

questi valori mostra riepilogo ubicazioni

## Sistema colori Windows/MSE

- Configurare il server NTP su MSE o sincronizzare manualmente entrambi i dispositivi (preferibilmente WCS) con l'ora e il fuso orario corretti.
- Verificare che i calcoli della posizione vengano eseguiti nella pagina di rilevamento o nella console MSE con il comando **getserverinfo**.
- Utilizzare la funzionalità di controllo in Sistema colori Windows per verificare che i valori di Sistema colori Windows corrispondano ai valori di Sistema colori Windows.
- Accertarsi che tutti gli access point siano assegnati alla mappa.
- MSE deve essere sincronizzato con la progettazione della rete, i WLC, gli switch cablati e gli eventi.
- Verificare che le mappe e le posizioni dei punti di accesso siano sincronizzate tra WCS e MSE.
- Il rilevamento di client/tag deve essere abilitato su MSE in **Servizi > Servizi di mobilità > <MSE> > Servizio sensibile al contesto > Amministrazione > Parametri di rilevamento**.
- Verificare che i client/tag siano visualizzati da Sistema colori Windows in **Monitor > Client/Tag**.
- Se i client e/o i tag non vengono visualizzati da WCS, verificare che le licenze client/tag siano installate in MSE. Verificare inoltre che sia installata la versione corretta di WCS che supporta la funzionalità di riconoscimento del contesto (WCS PLUS).
- Utilizzare lo strumento di calibrazione in Sistema colori Windows per calibrare le caratteristiche del segnale per l'ambiente specifico.
- Usare Location Rails e Regions (per la localizzazione dei client) e Cells and Mask (per la localizzazione dei tag) per includere/escludere aree specifiche della mappa del pavimento in cui i client Wi-Fi devono/devono non apparire.
- Verificate il livello di precisione della posizione con lo strumento di precisione in Sistema colori Windows.

### Per client

- Verificare che il rilevamento sia abilitato in MSE.
- Verificare che i client vengano rilevati dal WLC.

### Per i tag

- Verificare che il rilevamento sia abilitato in MSE.
- Verificare che i tag siano rilevati dal WLC.
- I canali 1,6,1 devono essere abilitati.
- La ripetizione per canale deve essere 3.
- Controllare lo stato della batteria.

## Sezione 5: Domande tecniche frequenti

D. Che cos'è l'impronta digitale RF? È la stessa cosa della triangolazione RF?

A. Le impronte digitali RF rappresentano un metodo di determinazione della posizione con due elementi attivi: per capire come si interfacciano le onde radio in un ambiente specifico della LAN wireless e per applicare queste caratteristiche di attenuazione alle informazioni sul segnale del dispositivo, in modo da poter determinare una posizione. La triangolazione non tiene conto delle variabili ambientali, ma si basa solo sulle letture della forza del segnale per approssimare la



posizione del dispositivo. Le impronte digitali RF prendono in considerazione le caratteristiche specifiche dell'edificio in quanto possono influire sulla propagazione dei segnali RF e sull'accuratezza della determinazione della posizione.

D. Che tipo di fedeltà di ubicazione posso aspettarmi?

A. L'ubicazione è di natura statistica. Cisco stima le specifiche della precisione della posizione in dieci metri il 90% del tempo e in cinque metri il 50% del tempo.

D. Le informazioni sono in tempo reale?

R. Il tempo di risposta delle informazioni sull'ubicazione, così come le informazioni sui clienti associate, è principalmente una funzione dell'elaborazione del sistema. I tempi di risposta variano in genere da pochi secondi a pochi minuti.

D. Qual è la scalabilità di MSE?

R. Cisco MSE 3350 può rilevare fino a 18.000 dispositivi. Per il supporto di più dispositivi, è possibile aggiungere altri MSE allo stesso sistema. Il limite superiore per i dispositivi simultanei si basa sulla capacità di elaborazione del MSE.

D. Per quanto tempo è possibile memorizzare la cronologia delle ubicazioni?

R. È possibile configurare la quantità di cronologia della posizione che MSE è in grado di memorizzare e riprodurre. Il valore predefinito è 30 giorni.

D. In che modo il traffico di posizione influisce sulla rete?

R. La quantità di traffico di posizione dipende dal numero di controller, access point e, in ultima analisi, dal numero di dispositivi di cui viene tenuta traccia in una determinata infrastruttura di rete. Con la crescita della rete, viene inoltrato più traffico dai punti di accesso ai controller wireless, che a loro volta vengono inoltrati al MSE. La quantità di traffico per una singola misurazione è molto ridotta, ma il numero di misurazioni dipende dal numero di dispositivi e dalla frequenza con cui vengono effettuate le misurazioni.

D. In che modo viene gestito MSE?

R. In caso di monitoraggio dei client con Context Aware Engine for Clients, tutte le operazioni di configurazione e gestione di MSE vengono eseguite tramite WCS, oltre l'installazione iniziale basata su comandi CLI. Quando si usa il Context Aware Engine for Tags (tag di tracciamento in ambienti interni ed esterni/esterni), sono necessarie soluzioni di gestione di rete Cisco (WCS) e AeroScout (System Manager).

D. Quali sono i requisiti dell'architettura LAN wireless per il supporto di MSE?

R. MSE funziona solo con l'architettura LAN wireless centralizzata Cisco, ad esempio un'infrastruttura abilitata per LWAPP. Il corretto posizionamento dell'access point è essenziale per la posizione. I punti di accesso devono essere posizionati vicino al perimetro delle aree di copertura e internamente come descritto nel presente documento. Vedere la sezione **Considerazioni sulla distribuzione con i servizi voce e dati esistenti**. È necessario disporre di una licenza per il motore sensibile al contesto.

D. Qual è la differenza tra l'ubicazione fornita nel sistema WCS e quella del sistema MSE?

A. La base del sistema di coordinate globali indica il punto di accesso in grado di rilevare un determinato dispositivo, nonché la potenza del segnale in corrispondenza della quale tale dispositivo viene rilevato. Sistema colori Windows con posizione utilizza impronte digitali RF avanzate e può individuare la posizione di un singolo dispositivo in modo on demand. MSE utilizza lo stesso metodo di rilevamento della posizione del sistema WCS, ma può rilevare fino a 18.000 dispositivi contemporaneamente quando utilizza Cisco MSE 3350. Questo consente alle applicazioni di terze parti di utilizzare la cronologia delle informazioni sui dispositivi per applicazioni quali il monitoraggio degli asset.

D. È necessario un software client per individuare i client?

R. Il software client non è necessario. Poiché la posizione è direttamente integrata nell'infrastruttura LAN wireless, i punti di accesso ascoltano i dispositivi Wi-Fi come di solito fanno per i dati, la voce e altre applicazioni. I client CCX vengono rilevati meglio rispetto ai client non CCX. Di conseguenza, Cisco consiglia di acquistare client compatibili con CCX (v4 o v5).

D. Per quanto tempo è possibile utilizzare i tag Wi-Fi prima di sostituire la batteria?

R. La durata della batteria dei tag è una funzione della durata della batteria di un dispositivo specifico, nonché della frequenza di beacon o blink. I tag possono durare da 100 giorni a un anno o anche più. Alcuni produttori pubblicizzano che possono durare 3-5 anni, ma dipende dal beacon rate.

D. Qual è il costo delle etichette Wi-Fi?

R. Contattare un produttore di etichette. Cisco non produce né rivende i tag. Inoltre, i prezzi delle etichette sono variabili e dipendono dal volume. Queste etichette hanno un prezzo più alto rispetto alle etichette RFID passive, in quanto forniscono una visibilità continua della posizione e etichette riutilizzabili alimentate a batteria. Essi inviano attivamente segnali, che in genere forniscono intervalli maggiori (diverse centinaia di piedi), e sono disponibili in una varietà di fattori di forma con più opzioni di montaggio. L'uso di RFID attiva è generalmente associato a una tracciabilità più continua di attività mobili di elevato valore o attività ad alta passività rispetto agli elementi che sono generalmente tracciati da RFID passiva.

## [Appendice A Installazione di MSE](#)

Attenersi alla seguente procedura:

1. **Accedi:** Accedere con queste credenziali: **root/password**.
2. **Avviare il processo di installazione:** Al primo avvio, MSE chiede all'amministratore di avviare lo script di installazione. Immettere **'yes'** per visualizzare questa richiesta. **Nota:** se il programma di installazione di MSE non viene richiesto, immettere questo comando:  
`/opt/mse/setup/setup.sh`
3. **Configurare il nome dell'host e il nome del dominio**  
**DNS:**

```

Current hostname=[mse]
Configure hostname? (Y)es/(S)kip/(U)se default [Skip]: y

The host name should be a unique name that can identify
the device on the network. The hostname should start with
a letter, end with a letter or number, and contain only
letters, numbers, and dashes.

Enter a host name [mse]: MSE-1

Current domain=[]
Configure domain name? (Y)es/(S)kip/(U)se default [Skip]: y

Enter a domain name for the network domain to which this device
belongs. The domain name should start with a letter, and it should
end with a valid domain name suffix such as ".com". It must contain
only letters, numbers, dashes, and dots.

Enter a domain name: cisco.com

```

#### 4. Configurare i parametri dell'interfaccia Ethernet:

```

Current IP address=[1.1.1.10]
Current eth0 netmask=[255.255.255.0]
Current gateway address=[1.1.1.1]
Configure eth0 interface parameters? (Y)es/(S)kip/(U)se default [Skip]: y

Enter an IP address for first ethernet interface of this machine.

Enter eth0 IP address [1.1.1.10]: 172.20.229.200

Enter the network mask for IP address 172.20.229.200.

Enter network mask [255.255.255.0]: 255.255.255.0

Enter an default gateway address for this machine.

Note that the default gateway must be reachable from
the first ethernet interface.

Enter default gateway address [1.1.1.1]: 172.20.229.1

```

Quando vengono richiesti i parametri dell'interfaccia 'eth1', immettere **Skip** per procedere alla fase successiva, poiché per il funzionamento non è necessaria una seconda scheda NIC. **Nota:** l'indirizzo configurato deve fornire connettività IP ai controller LAN wireless e al sistema di gestione WCS utilizzati con l'accessorio.

#### 5. Immettere le informazioni sui server DNS: Per la corretta risoluzione del dominio è necessario un solo server DNS. immettere i server di backup per la resilienza.

```

Domain Name Service (DNS) Setup
DNS is currently enabled.
No DNS servers currently defined
Configure DNS related parameters? (Y)es/(S)kip/(U)se default [Skip]: y

Enable DNS (yes/no) [yes]: y
Enter primary DNS server IP address: 172.20.229.10
Enter backup DNS server IP address (or none) [none]: 172.20.229.20
Enter another backup DNS server IP address (or none) [none]:

```

#### 6. Configura fuso orario: Se il fuso orario predefinito di New York non è applicabile al proprio ambiente, sfogliare i menu di posizione per impostarlo correttamente.

```
Current timezone=[America/New_York]
Configure timezone? (Y)es/(S)kip/(U)se default [Skip]: y

Enter the current date and time.

Please identify a location so that time zone rules can be set correctly.
Please select a continent or ocean.
 1) Africa
 2) Americas
 3) Antarctica
 4) Arctic Ocean
```

7. **Configurare l'ora NTP o di sistema:** L'NTP è opzionale, ma assicura che il sistema mantenga un'ora di sistema accurata. Se si sceglie "No", viene richiesto di impostare l'ora corrente del sistema.

```
Network Time Protocol (NTP) Setup.

If you choose to enable NTP, the system time will be
configured from NTP servers that you select. Otherwise,
you will be prompted to enter the current date and time.

NTP is currently disabled.
Configure NTP related parameters? (Y)es/(S)kip/(U)se default [Skip]: y

Enter whether or not you would like to set up the
Network Time Protocol (NTP) for this machine.

If you choose to enable NTP, the system time will be
configured from NTP servers that you select. Otherwise,
you will be prompted to enter the current date and time.

Enable NTP (yes/no) [no]: yes
Enter NTP server name or address: time.nist.gov
Enter another NTP server IP address (or none) [none]:
```

**Nota:** è essenziale impostare l'ora corretta su Mobility Services Engine, Wireless LAN Controller e WCS Management System. Per ottenere questo risultato, è necessario puntare tutti e tre i sistemi allo stesso server NTP e assicurarsi che abbiano i fusi orari configurati correttamente.

8. **Abilita login radice console locale:** Questo parametro viene utilizzato per abilitare/disabilitare l'accesso alla console locale al sistema. È necessario attivare questa opzione per consentire la risoluzione dei problemi a livello locale.

```
Remote root login is currently disabled.
Configure remote root access? (Y)es/(S)kip/(U)se default [Skip]: yes

Enter whether or not you would like to allow
remote root login via secure shell for this machine.

Enable remote root login (yes/no) [no]: yes
```

9. **Abilitare l'accesso alla radice SSH (Secure Shell): Facoltativo:** Questo parametro viene utilizzato per abilitare/disabilitare l'accesso della console remota al sistema. È necessario attivare questa opzione, in modo da poter eseguire la risoluzione remota dei problemi, ma i criteri di sicurezza aziendali possono rendere obbligatoria la disattivazione di questa opzione.

```
SSH root access is currently disabled.
Configure ssh access for root (Y)es/(S)kip/(U)se default [Skip]: yes

Enter whether or not you would like to enable ssh
root login. If you disable this option, only console
root login will be possible.

Enable ssh root access (yes/no): yes
```

10. **Configurare la modalità utente singolo e la lunghezza della password:** Questi parametri di configurazione non sono obbligatori e, per impostazione predefinita, vengono ignorati immettendo 's'.

```
Single user mode password check is currently disabled.
Configure single user mode password check (Y)es/(S)kip/(U)se default [Skip]: s

Login and password strength related parameter setup
Maximum number of days a password may be used : 99999
Minimum number of days allowed between password changes : 0
Minimum acceptable password length : 5
Login delay after failed login :
Checking for strong passwords is currently disabled.
Configure login/password related parameters? (Y)es/(S)kip/(U)se default [Skip]:
s
```

11. **Imposta banner di accesso:** Un banner di accesso viene utilizzato per informare gli utenti dell'uso del sistema e presentare un avviso per impedire agli utenti non autorizzati di accedere al sistema. Poiché il banner di accesso può essere un messaggio multiriga, un singolo punto (.) termina il messaggio e procede al passaggio successivo.

```
Current Login Banner = [Cisco Mobility Service Engine]
Configure login banner (Y)es/(S)kip/(U)se default [Skip]: yes

Enter text to be displayed as login banner. Enter a single period
on a line to terminate.

Login banner [Cisco Mobility Service Engine]:
MSE-1
Unauthorized Access is not allowed
.
```

12. **Modificare la password di root:** Questa fase è fondamentale per garantire la sicurezza del sistema; assicurarsi di scegliere una password complessa costituita da lettere e numeri senza parole del dizionario. La lunghezza minima della password è di 8 caratteri.

```
Configure root password? (Y)es/(S)kip/(U)se default [Skip]: y

Enter a password for the superuser.

Enter root password: [redacted]
Confirm root password: [redacted]
```

13. **Configurare una password di GRUB: Facoltativo:** Questo parametro di configurazione non è richiesto e per impostazione predefinita, il valore da ignorare è s.

```
GRUB password is not currently configured.
Configure GRUB password (Y)es/(D)isable/(S)kip/(U)se default [Skip]: s
```

14. **Configurare una password di comunicazione WCS.**

```

Configure WCS communication password? (Y)es/(S)kip/(U)se default [Skip]: yes
Enter a password for the admin user.
The admin user is used by the WCS and other northbound systems
to authenticate their SOAP/XML session with the server.
Once this password is updated, it must correspondingly be updated
on the WCS page for MSE General Parameters so that the WCS can
communicate with the MSE.
Enter WCS communication password: 
Confirm WCS communication password: 

```

15. **Salva le modifiche e riavvia:** Una volta completato lo script di installazione, salvare le modifiche quando richiesto. Dopo il salvataggio, seguire le istruzioni per riavviare MSE e verificare che tutte le impostazioni siano state applicate correttamente.
16. **Avviare il servizio MSE:** Accedere a MSE con il nome utente root e la password configurati in precedenza nel passaggio 12. Eseguire il comando **msed start** per avviare il servizio MSE.

```

login as: root
Cisco Mobility Service Engine

root@172.20.226.203's password: 
Last login: Wed Jul 23 10:11:58 2008 from dhcp-171-71-123-7.cisco.com
[root@MSE-1 ~]# service msed start
Starting MSE Platform
Cannot find UDI information. Exiting
null
Invalid Platform type. Now Exiting.
Starting MSE Platform, waiting to check the status.
Starting MSE Platform, waiting to check the status.
MSE Platform is up, getting the status

```

17. **Abilita l'avvio del servizio MSE all'avvio:** Eseguire il comando **chkconfig msed on**.

## [Aggiungi MSE a Sistema colori Windows](#)

Attenersi alla seguente procedura:

1. **Passare alla pagina Configurazione servizi di mobilità:** Accedere a WCS e fare clic su **Mobility Services** dal menu a discesa Mobility.



2. **Aggiungere Mobility Services Engine a WCS:** Dal menu a discesa sul lato destro, scegliere **Add Mobility Services Engine**, quindi fare clic su **Go**. Immettere un nome di dispositivo univoco per MSE, l'indirizzo IP precedentemente configurato nell'installazione di MSE, un nome di contatto per il supporto e la "Password di comunicazione WCS" configurata nell'installazione di MSE. Non modificare il nome utente predefinito di **admin**.

# Mobility Services Engine > General Properties > New

## General

Device Name	<input type="text" value="MSE Demo"/>
IP Address	<input type="text" value="172.20.226.199"/>
Contact Name	<input type="text" value="MSE Support Contact"/>
User Name	<input type="text" value="admin"/>
Password	<input type="password" value="•••••"/>

3. Scegliere il servizio sensibile al contesto da eseguire su MSE.

### Mobility Services

Admin Status	Name
<input checked="" type="checkbox"/>	Context Aware Service
<input type="checkbox"/>	Wireless Intrusion Protection Service

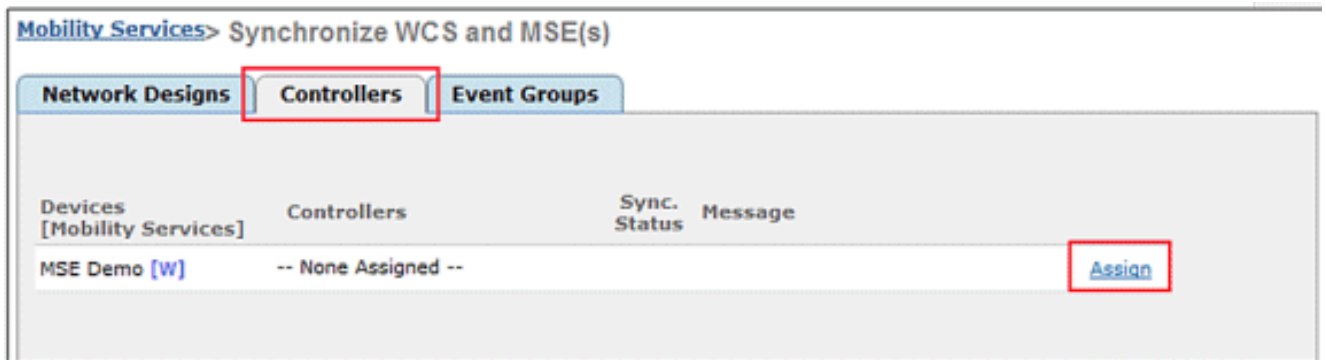
4. Sincronizza: Assicurarsi di sincronizzare i progetti di rete, i controller e i gruppi di eventi.

### Mobility Services Engine Added > 'MSE Demo'

WCS contains data, please go to the Synchronize page to push data to the Mobility Services Engine.

Please synchronize the following Controllers

WLC-1



5. **Controller da sincronizzare:** Viene visualizzato un popup con un elenco di controller con cui sincronizzare MSE. Scegliere i controller desiderati per la sincronizzazione e fare clic su OK.



	Controller Name	Controller IP Address	Version	Supported Services	Currently Assigned To
<input checked="" type="checkbox"/>	WLC-1	172.20.226.197	5.2.72.0	[C, W, M]	

Una volta chiusa la finestra popup, fare clic su **Sincronizza** in fondo alla finestra di dialogo "Sincronizza WCS e MSE". **Nota:** il servizio Context Aware Cisco dipende molto da un orologio sincronizzato tra il controller LAN wireless, WCS e MSE. Se tutti e tre questi sistemi non sono indirizzati allo stesso server NTP e configurati con le stesse impostazioni di fuso orario, l'applicazione Context Aware non funziona correttamente. Prima di tentare di risolvere il problema, verificare che l'orologio di sistema sia lo stesso su tutti i componenti del sistema sensibile al contesto.

## Appendice B Comandi WLC e MSE

### Comandi WLC

#### **config location expiry ?**

```
client          Timeout for clients
calibrating-client Timeout for calibrating clients
tags           Timeout for RFID tags
rogue-aps      Timeout for Rogue APs
```

#### **show location ap-detect ?**

```
all            Display all (client/rfid/rogue-ap/rogue-client) information
client        Display client information
rfid          Display rfid information
rogue-ap      Display rogue-ap information
rogue-client  Display rogue-client information
(Cisco Controller) >show location ap-detect client
```

#### **show client summary**

```
Number of Clients..... 7
MAC Address      AP Name      Status      WLAN/Guest-Lan Auth Protocol Port Wired
-----
00:0e:9b:a4:7b:7d AP6          Probing     N/A         No 802.11b 1 No
```



00:40:96:ad:51:0c AP6 Probing N/A No 802.11b 1 No

(Cisco Controller) >show location summary

Location Summary

Algorithm used: Average  
Client

RSSI expiry timeout: 5 sec  
Half life: 0 sec  
Notify Threshold: 0 db

Calibrating Client

RSSI expiry timeout: 5 sec  
Half life: 0 sec

Rogue AP

RSSI expiry timeout: 5 sec  
Half life: 0 sec  
Notify Threshold: 0 db

RFID Tag

RSSI expiry timeout: 5 sec  
Half life: 0 sec  
Notify Threshold: 0 db

### show rfid config

RFID Tag data Collection..... Enabled  
RFID timeout..... 1200 seconds  
RFID mobility..... Oui:00:14:7e : Vendor:pango State:Disabled

(Cisco Controller) >config location ?

plm Configure Path Loss Measurement (CCX S60) messages  
algorithm Configures the algorithm used to average RSSI and SNR values  
notify-threshold Configure the LOCP notification threshold for RSSI measurements  
rssi-half-life Configures half life when averaging two RSSI readings  
expiry Configure the timeout for RSSI values

### config location expiry client ?

<seconds> A value between 5 and 3600 seconds

### config location rssi-half-life client ?

<seconds> Time in seconds (0,1,2,5,10,20,30,60,90,120,180,300 sec)

### show nmsp subscription summary

Mobility Services Subscribed:

Server IP	Services
-----	-----
172.19.32.122	RSSI, Info, Statistics, IDS

## Comandi MSE

to determine status of MSE services

```
[root@MSE ~]# getserverinfo
```

to start Context Aware engine for client tracking

```
[root@MSE ~]# /etc/init.d/msed start
```

to determine status of Context Aware engine for client tracking

```
[root@MSE ~]# /etc/init.d/msed status
```

to stop Context Aware engine for client tracking

```
[root@MSE ~]# /etc/init.d/msed stop
```

diagnostics command

```
[root@MSE ~]# rundiag
```

**Nota:** il comando **rundiag** può essere utilizzato anche per visualizzare le informazioni UDI MSE

necessarie per ottenere il file di licenza per il motore sensibile al contesto per i client.

## [Appendice C: Aggiornamento di MSE dalla versione 5.X alla 6.0](#)

Attenersi alla seguente procedura:

1. Eseguire il backup del database MSE delle immagini precedenti alla 6.x da WCS; passare a questo collegamento: **Servizio >Servizi di mobilità >selezionare MSE >Manutenzione >Backup.**
2. Per eseguire il backup dei dati e della configurazione per i tag, consultare la [documentazione di AeroScout](#) .
3. Scaricare l'immagine 6.x su MSE da WCS; passare a questo collegamento: **Services >Mobility Service >** scegli MSE quindi dal riquadro di sinistra, vai a **Manutenzione >Download Software**, sfoglia per scegliere l'immagine MSE dal PC e fai clic su **Scarica**. Una volta scaricata, l'immagine MSE viene automaticamente decompressa e inserita nella cartella /opt/installers di MSE. È necessario installare manualmente l'immagine dalla CLI di MSE.

### Transfer Software Image

Select from uploaded images to transfer into the Server

AIR-LOC2700-L-K9-3-1-38-0.bin.gz

Browse a new software image to transfer into the Server

Browse...

Timeout 180 1 - 999999 secs

Download Cancel

4. Utilizzare questo comando per arrestare il framework MSE: **/etc/init.d/msed stop**.
5. Dalla console MSE, usare il comando **cd /opt/installers**. In questa directory è visualizzato il file scaricato nel passaggio 3. La directory ha il seguente aspetto:

```
[root@heitz-3350 installers]# cd /opt/installers
[root@heitz-3350 installers]# ls
CISCO-MSE-L-K9-6-0-73-0-64bit.bin  diagnostics.log
CISCO-MSE-L-K9-6-0-75-0-64bit.bin  MSE_6_0_70_0.bin
[root@heitz-3350 installers]#
```

6. Per installare l'immagine MSE, eseguire il file e seguire le istruzioni:

```
[root@heitz-3350 installers]# ./CISCO-MSE-L-K9-6-0-73-0-64bit.bin
```

**Nota:** il messaggio di avviso relativo ai requisiti di licenza su MSE per tenere traccia degli elementi viene visualizzato in primo piano con la versione 6.0 MR1 in poi. Questo messaggio di avviso viene visualizzato anche alla fine al termine dell'installazione. Nella release 6.0 questo messaggio viene visualizzato solo alla fine dell'installazione. È stato aggiunto un avviso con 6.0 MR1 per dare all'utente un ulteriore avviso sull'applicazione della licenza. Il messaggio è simile al seguente: "Con questa versione del software verranno applicate le

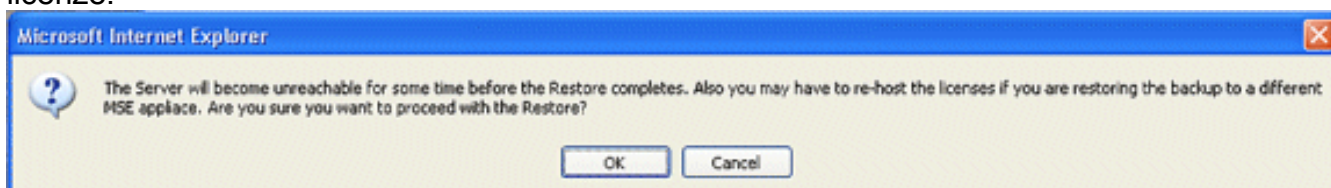
licenze di Mobility Services Engine. Per abilitare la licenza sul sistema, verificare di avere a disposizione la chiave di autorizzazione del prodotto (PAK) e consultare le istruzioni indicate nel certificato PAK cartaceo e la Guida dell'utente di MSE."Durante l'esecuzione del file, l'utente può scegliere se mantenere o rimuovere il database.

7. Una volta installata l'immagine, eseguire questo comando per avviare il framework MSE:  
**/etc/init.d/mseed start.**
8. MSE inizia a utilizzare le licenze di valutazione incluse nella versione 6.0 del software.
9. Aggiungere la licenza permanente ricevuta registrando un numero PAK da WCS; passare a questo collegamento: **Amministrazione > Centro licenze > File > File MSE > Aggiungi** . Scegliere MSE dal menu a discesa, cercare il file di licenza sul PC e caricarlo.
10. I servizi MSE vengono riavviati dopo il caricamento della licenza in MSE, quindi attendere alcuni minuti prima di eseguire altre operazioni. Ottenere lo stato MSE usando il comando **/etc/init.d/mseed status**.
11. Durante l'installazione dell'immagine MSE, se si sceglie di mantenere l'opzione del database come nel passaggio 6, non è necessario ripristinare il database di cui è stato eseguito il backup in precedenza (per client e tag); in caso contrario, è necessario ripristinare il database MSE. Selezionare **Servizio > Servizi di mobilità**, scegliere **MSE** dal pannello sinistro Manutenzione e fare clic su **Ripristina**. **Nota:** per ripristinare le informazioni sui tag, consultare la [documentazione di AeroScout](#) .

## Appendice D: Ripristino database MSE

È possibile ripristinare MSE DB in tre modi diversi:

- **Opzione 1:** Durante l'aggiornamento dell'immagine MSE alla versione 6.0, scegliere di continuare quando il programma di installazione rileva che MSE è già in esecuzione. Il messaggio mostra quanto segue: "Nel sistema è già installato un Cisco Mobility Services Engine. Se si sceglie **Continua**, tutti i componenti attualmente installati verranno rimossi in modo permanente (verranno mantenuti solo i file di database e di licenza)."
- **Opzione 2:** Durante la disinstallazione dell'immagine MSE sono disponibili due opzioni. La prima opzione prevede la conservazione del database, mentre la seconda consiste nella rimozione del database. Se il database viene mantenuto, non è necessario alcun ripristino manuale. Se il database viene rimosso, seguire la terza opzione.
- **Opzione 3:** Eseguire una nuova installazione, ossia prendere una nuova casella MSE con un'immagine precedente alla 6.0 o una casella MSE con il database rimosso. È necessario ripristinare il database di cui è stato eseguito il backup (vedere l'opzione 1 in MSE versione 6.0). Se l'immagine MSE di backup è stata ripristinata su un altro MSE, è necessario riallocare la licenza in modo che possa essere utilizzata sul MSE corrente. Le licenze MSE sono legate all'UDI MSE. All'interno del ripristino, l'utente riceve un messaggio in WCS: "Se si ripristina il backup su un altro dispositivo MSE, potrebbe essere necessario riospitare le licenze."



## Informazioni correlate

- [Guida introduttiva ai servizi di mobilità Cisco 3350](#)
- [Cisco 3310 Mobility Services Engine - Guida introduttiva](#)
- [Cisco Mobility Services Engine - Guida all'installazione della soluzione di mobilità sensibile al contesto](#)
- [Domande frequenti sui gruppi di mobilità](#)
- [Guida alla progettazione di Wi-Fi Location-Based Services 4.1](#)
- [Guida alla configurazione di Cisco Context-Aware Service, versione 6.0](#)
- [Cisco serie 3300 Mobility Services Engine - Guida agli ordini e alle licenze](#)
- [Guida alla configurazione di Cisco Wireless LAN Controller](#)
- [Etichette RFID, una visione più ravvicinata a loro e alla loro configurazione](#)
- [Guida di riferimento per antenne e accessori Cisco Aironet](#)
- [Supporto AeroScout](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)