Criteri access point attendibili su un controller LAN wireless

Sommario

Introduzione

Questo documento descrive i criteri di protezione wireless *Trusted AP* su un controller WLC (Wireless LAN Controller), definisce i criteri Trusted AP e fornisce una breve descrizione di tutti i criteri Trusted AP.

Prerequisiti

Requisiti

Verificare di avere una conoscenza di base dei parametri di sicurezza della LAN wireless (ad esempio SSID, crittografia, autenticazione e così via).

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Criteri Trusted AP

I criteri Trusted AP (Trusted AP Policies) sono una funzione di sicurezza del controller progettata per essere utilizzata in scenari in cui i clienti hanno una rete parallela autonoma AP insieme al controller. In questo scenario, l'access point autonomo può essere contrassegnato come l'access

point attendibile sul controller e l'utente può definire criteri per questi access point attendibili (che dovrebbero utilizzare solo WEP o WPA, il proprio SSID, un breve preambolo e così via). Se uno di questi punti di accesso non rispetta questi criteri, il controller invia un allarme al dispositivo di gestione della rete (Wireless Control System) che indica che un punto di accesso attendibile ha violato un criterio configurato.

Che cos'è un Trusted AP?

I punti di accesso attendibili sono punti di accesso che non fanno parte di un'organizzazione. Tuttavia, non rappresentano una minaccia per la sicurezza della rete. Questi punti di accesso sono anche chiamati punti di accesso amichevoli. Esistono diversi scenari in cui è possibile configurare un punto di accesso come attendibile.

Ad esempio, nella rete potrebbero essere presenti diverse categorie di access point, quali:

- **Punti di accesso che non eseguono LWAPP (probabilmente eseguono IOS o VxWorks)**
- Punti di accesso LWAPP introdotti dai dipendenti (con l'autorizzazione dell'amministratore)
- AP LWAPP utilizzati per verificare la rete esistente
- Access point LWAPP di proprietà dei vicini

In genere, i punti di accesso attendibili sono punti di accesso che rientrano nella **categoria 1**, ovvero punti di accesso di proprietà dell'utente che non eseguono LWAPP. Potrebbe trattarsi di vecchi access point con VxWorks o IOS. Per garantire che questi access point non danneggino la rete, è possibile applicare alcune funzionalità, ad esempio gli SSID corretti e i tipi di autenticazione. Configurare i criteri degli access point attendibili sul WLC e verificare che gli access point attendibili soddisfino tali criteri. In caso contrario, è possibile configurare il controller in modo che esegua diverse azioni, ad esempio l'invio di un avviso al dispositivo di gestione della rete (WCS).

I punti di accesso noti appartenenti ai punti di accesso adiacenti possono essere configurati come punti di accesso attendibili.

In genere, la funzionalità MFP (Management Frame Protection) deve impedire agli access point non legittimi di unirsi al WLC. Se le schede NIC supportano i dispositivi multifunzione, non è consentito accettare disautenticazioni da dispositivi diversi dai veri access point. Per ulteriori informazioni sull'opzione MFP, fare riferimento agli esempi di configurazione di Infrastructure Management Frame Protection (MFP) con WLC e LAP.

Se sono presenti access point che eseguono VxWorks o IOS (come nella categoria 1), non verranno mai aggiunti al gruppo LWAPP o eseguiranno la funzionalità MFP, ma è possibile che si desideri applicare i criteri elencati in tale pagina. In questi casi, è necessario configurare sul controller i criteri dei punti di accesso attendibili per i punti di accesso desiderati.

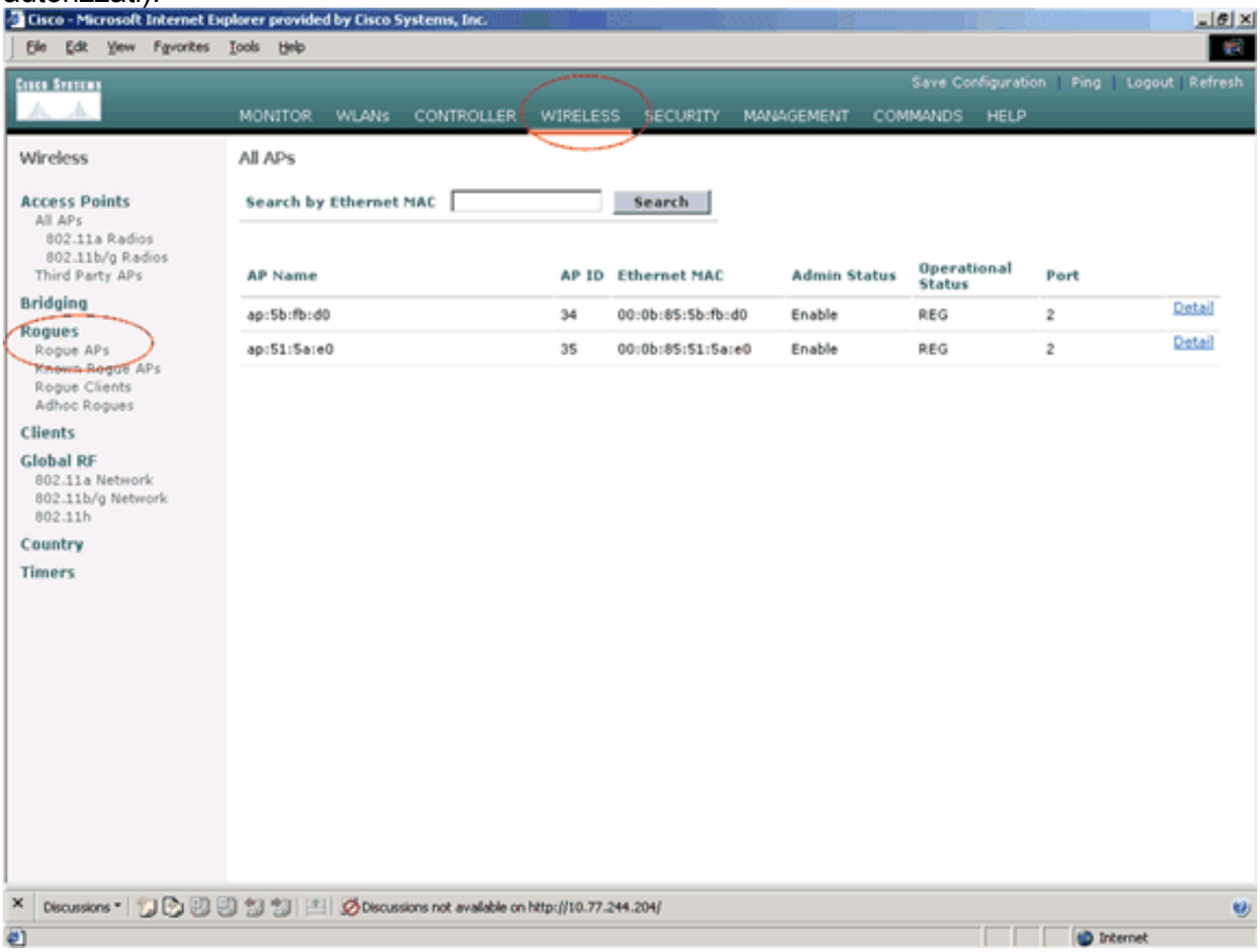
In generale, se si è a conoscenza di un punto di accesso non autorizzato e si è certi che non rappresenti una minaccia per la rete, è possibile identificarlo come punto di accesso attendibile.

Come configurare un access point come access point attendibile dall'interfaccia utente grafica del WLC?

Per configurare un access point come access point attendibile, completare la procedura seguente:

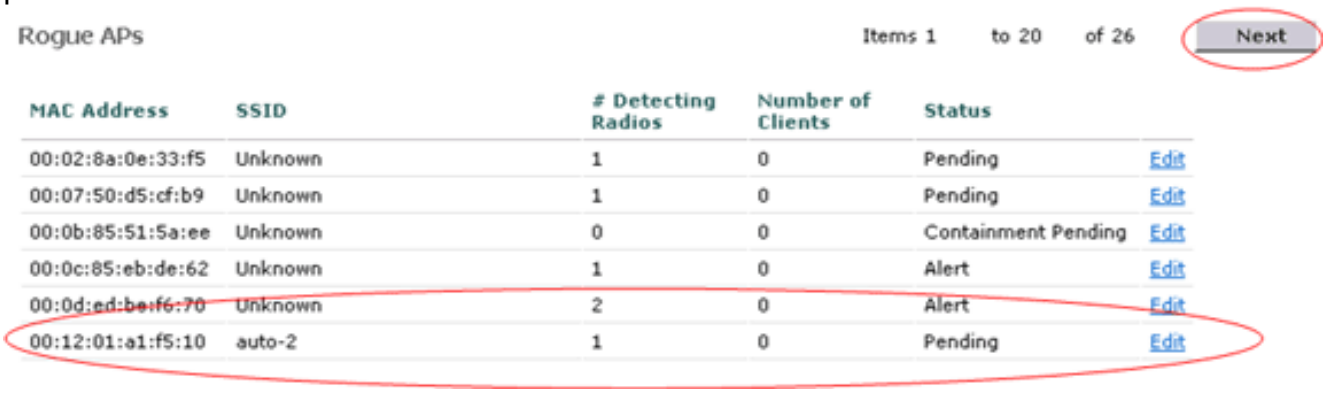
1. Accedere alla GUI del WLC tramite HTTP o https.

2. Dal menu principale del controller, fare clic su **Wireless**.
3. Nel menu sul lato sinistro della pagina Wireless, fare clic su **Rogue AP** (Punti di accesso non autorizzati).



Nella pagina Access point non autorizzati vengono elencati tutti gli access point rilevati come access point non autorizzati nella rete.

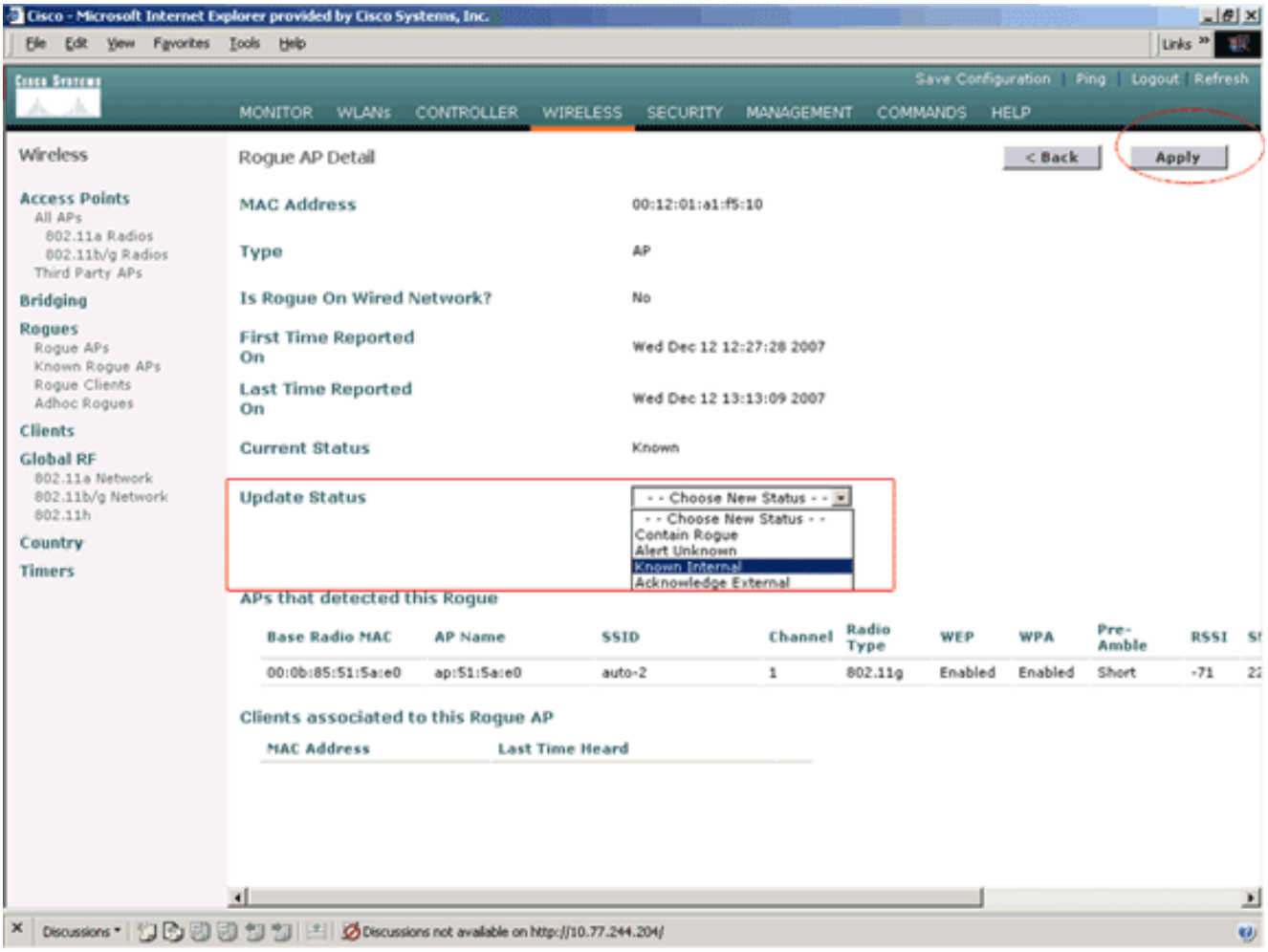
4. Da questo elenco di access point anomali, individuare l'access point che si desidera configurare come trusted che rientra nella categoria 1 (come spiegato nella sezione precedente).Èpossibile individuare gli access point con gli indirizzi MAC elencati nella pagina degli access point non autorizzati. Se l'access point desiderato non si trova in questa pagina, fare clic su **Avanti** per identificarlo nella pagina successiva.
5. Una volta individuato l'access point desiderato dall'elenco degli access point non autorizzati, fare clic sul pulsante **Modifica** corrispondente all'access point per visualizzare la pagina dei dettagli dell'access
point.



Nella pagina dei dettagli dell'access point non autorizzato sono disponibili informazioni

dettagliate sull'access point, ad esempio se è connesso alla rete cablata, lo stato corrente dell'access point e così via.

6. Per configurare questo access point come attendibile, selezionare **Interno noto** dall'elenco a discesa Aggiorna stato e fare clic su **Applica**.Quando lo stato dell'access point viene aggiornato su *Interno noto*, l'access point viene configurato come attendibile nella rete.

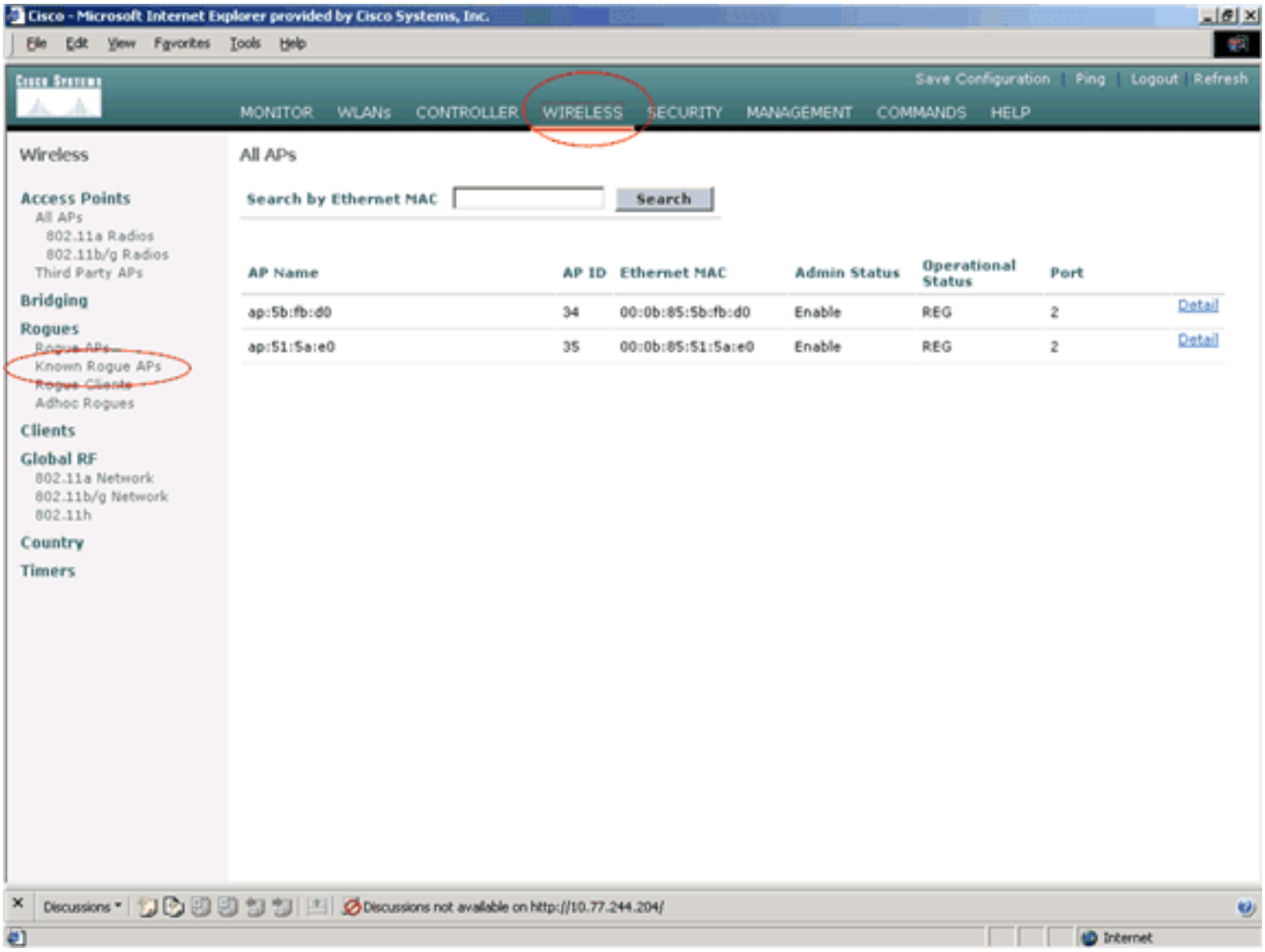


7. Ripetere questa procedura per tutti gli access point che si desidera configurare come trusted.

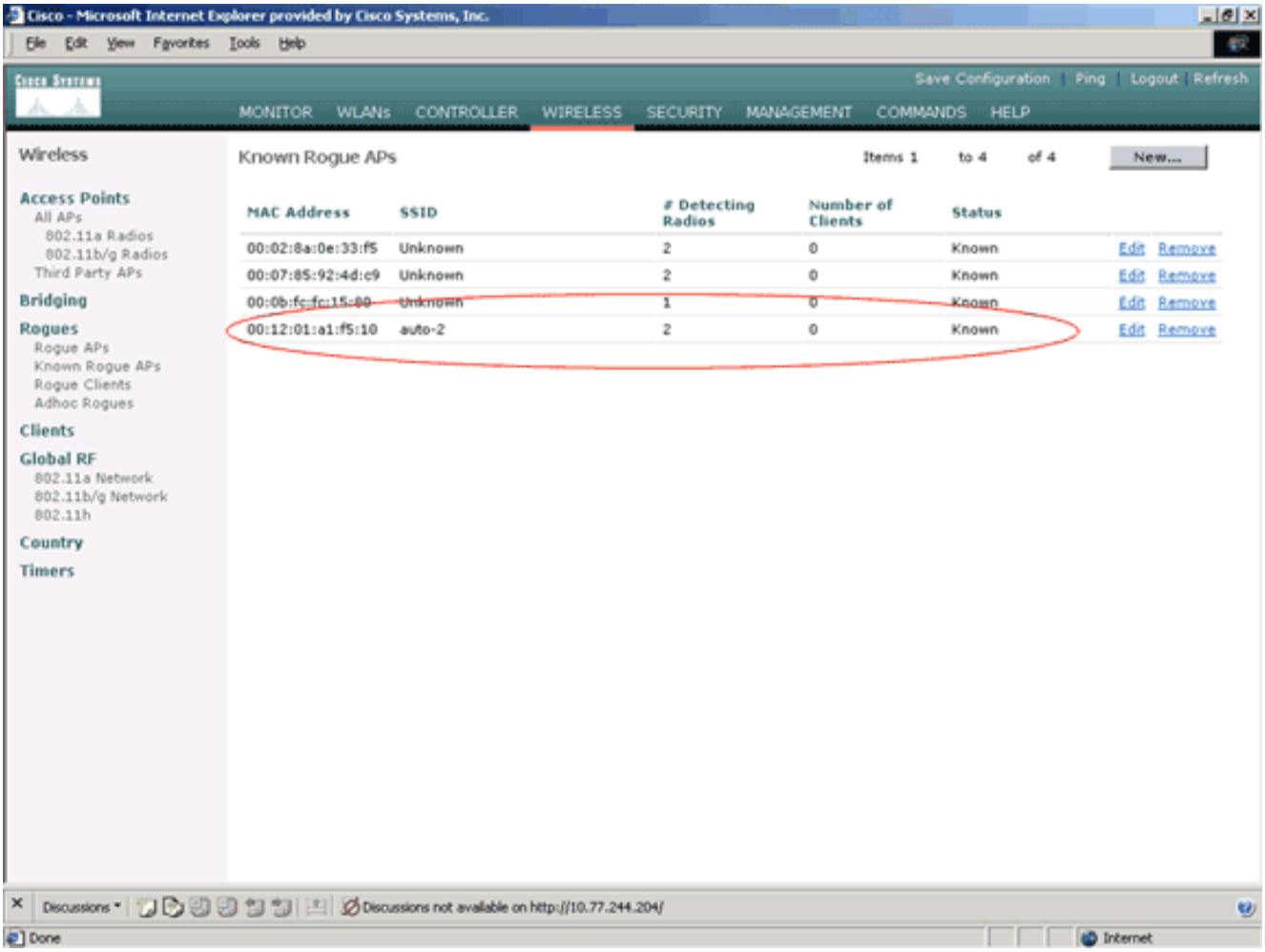
Verifica la configurazione Trusted AP

Completare questa procedura per verificare che l'access point sia configurato correttamente come attendibile dall'interfaccia utente del controller:

1. Fare clic su **Wireless**.
2. Nel menu sul lato sinistro della pagina Wireless, fare clic su **Punti di accesso non autorizzati noti**.



L'access point desiderato dovrebbe essere visualizzato nella pagina Access point non autorizzati con lo stato
Known.



Informazioni sulle impostazioni dei criteri Trusted AP

Il WLC ha questi criteri dell'access point attendibile:

- Criterio di crittografia imposto
- Criterio preambolo imposto
- Criterio tipo di radio imposto
- Convalida SSID
- Avvisa se il punto di accesso attendibile è mancante
- Timeout scadenza per voci di access point attendibili (secondi)

Criterio di crittografia imposto

Questo criterio viene utilizzato per definire il tipo di crittografia che l'access point attendibile deve utilizzare. In Criterio di crittografia imposto è possibile configurare uno qualsiasi di questi tipi di crittografia:

- Nessuna
- Open (Aperto)
- WEP
- WPA/802.11i

Il WLC verifica se il tipo di crittografia configurato nell'access point attendibile corrisponde al tipo di crittografia configurato nell'impostazione "**Criteri di crittografia imposti**". Se l'access point attendibile non usa il tipo di crittografia designato, il WLC invia un allarme al sistema di gestione

per prendere le misure appropriate.

Criterio preambolo imposto

Il preambolo radio (talvolta chiamato intestazione) è una sezione di dati alla base di un pacchetto che contiene le informazioni di cui i dispositivi wireless hanno bisogno quando inviano e ricevono i pacchetti. I preamboli **brevi** migliorano le prestazioni di throughput, pertanto sono abilitati per impostazione predefinita. Tuttavia, alcuni dispositivi wireless, ad esempio i telefoni SpectraLink NetLink, richiedono preamboli **lunghi**. In Criterio di preambolo imposto è possibile configurare una delle opzioni seguenti:

- Nessuna
- Breve
- Lunga

Il WLC verifica se il tipo di preambolo configurato nell'access point attendibile corrisponde al tipo di preambolo configurato nell'impostazione "**Criterio di preambolo imposto**". Se l'access point attendibile non utilizza il tipo di preambolo specificato, il WLC invia un allarme al sistema di gestione per prendere le misure appropriate.

Criterio tipo di radio imposto

Questo criterio viene utilizzato per definire il tipo di radio che l'access point attendibile deve utilizzare. In Criterio tipo radio imposto è possibile configurare uno qualsiasi di questi tipi di radio:

- Nessuna
- Solo 802.11b
- Solo 802.11a
- Solo 802.11b/g

Il WLC verifica se il tipo di radio configurato nell'access point attendibile corrisponde al tipo di radio configurato nell'impostazione "**Criterio del tipo di radio imposto**". Se l'access point attendibile non utilizza le radio specificate, il WLC invia un allarme al sistema di gestione per prendere le misure appropriate.

Convalida SSID

Èpossibile configurare il controller per convalidare un SSID di punti di accesso trusted rispetto agli SSID configurati nel controller. Se l'SSID degli access point attendibili corrisponde a uno degli SSID dei controller, il controller genera un allarme.

Avvisa se l'access point attendibile è mancante

Se questo criterio è abilitato, il WLC avvisa il sistema di gestione se l'access point attendibile non è presente nell'elenco degli access point non autorizzati noti.

Timeout scadenza voci di access point attendibili (secondi)

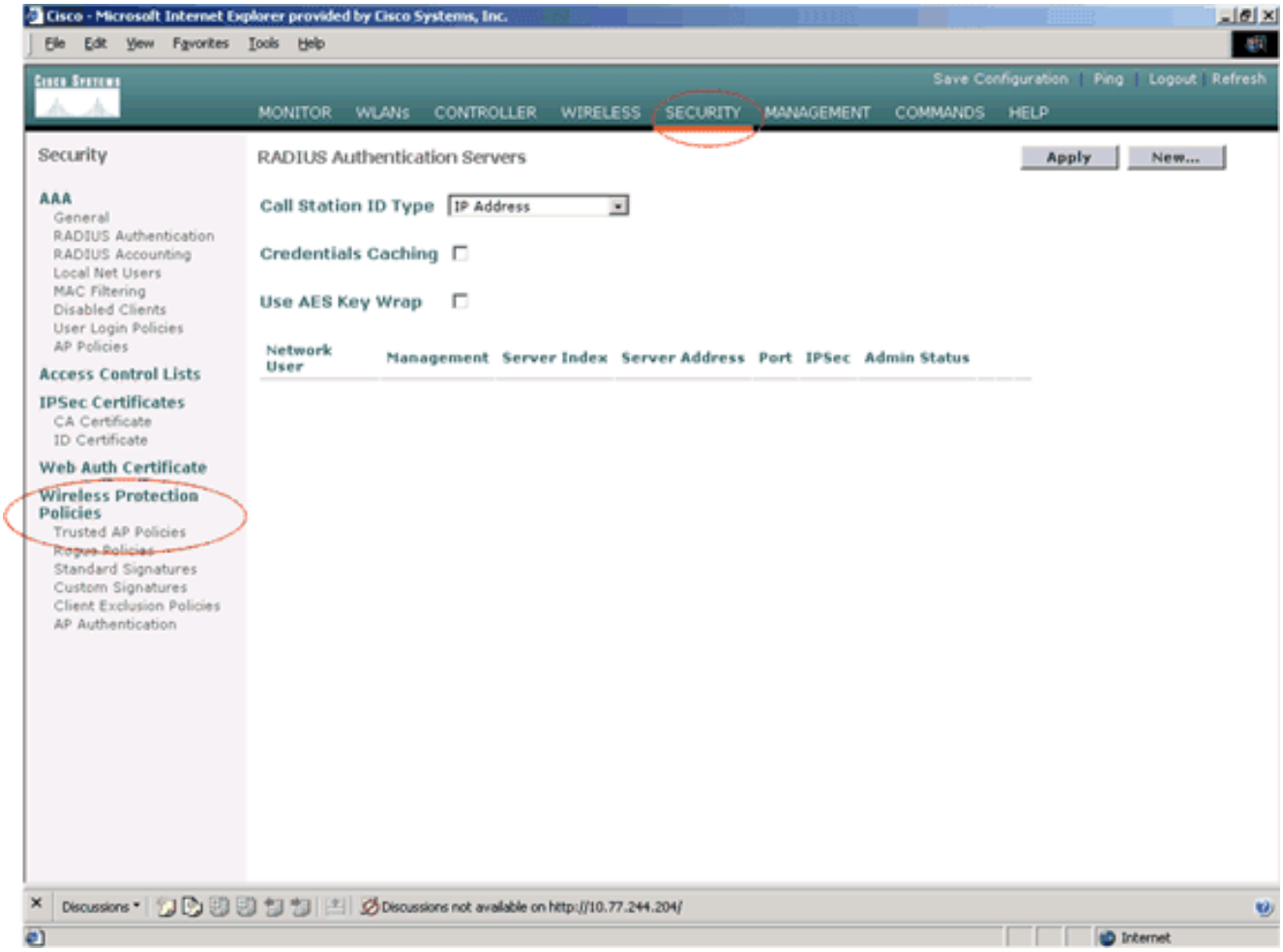
Questo valore di timeout di scadenza specifica il numero di secondi prima che l'access point attendibile venga considerato scaduto e scaricato dalla voce WLC. È possibile specificare questo valore di timeout in secondi (120 - 3600 secondi).

Come configurare i criteri Trusted AP sul WLC?

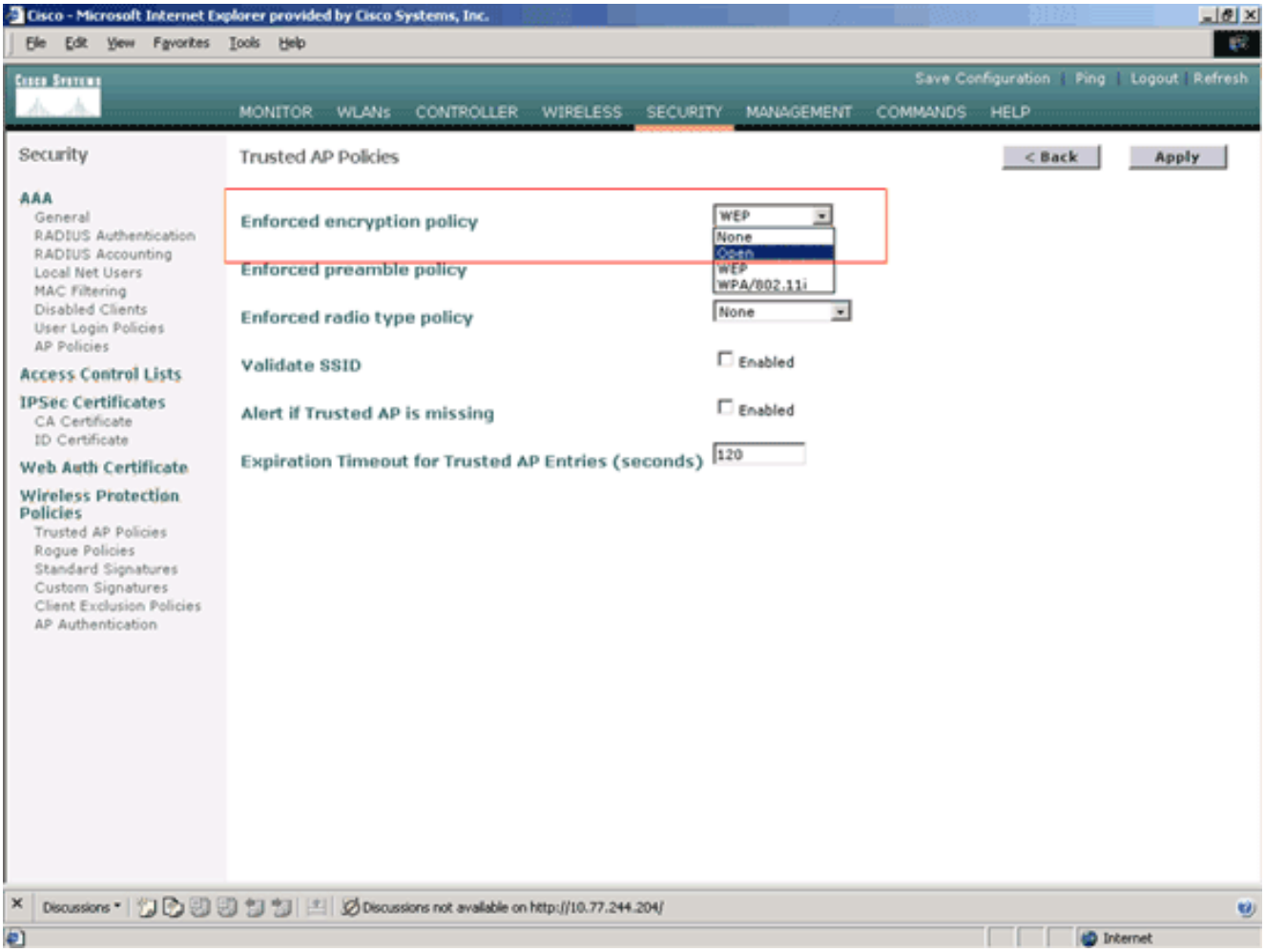
Completare questi passaggi per configurare i criteri Trusted AP sul WLC tramite la GUI:

Nota: tutti i criteri PA trusted si trovano sulla stessa pagina WLC.

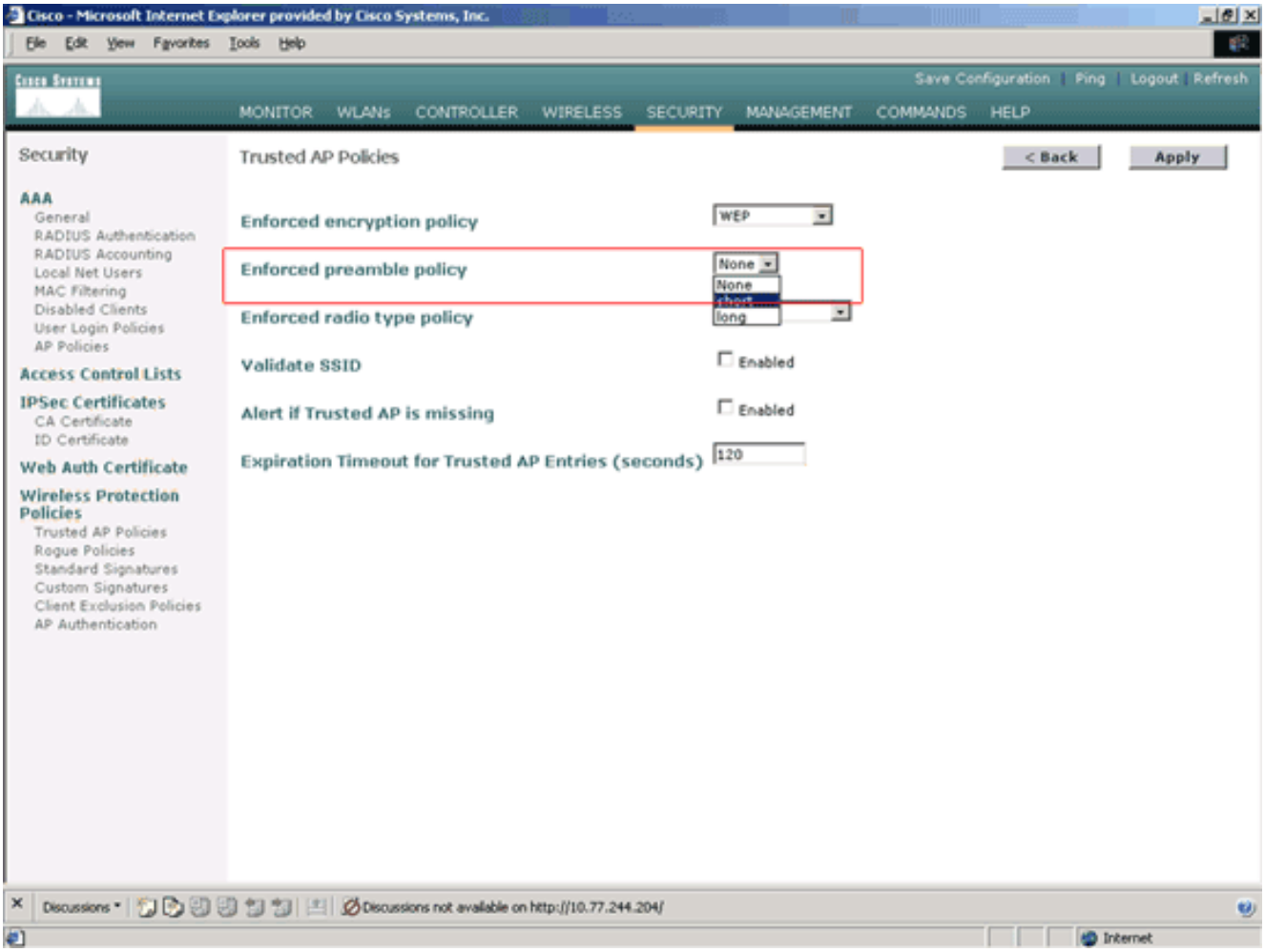
1. Dal menu principale della GUI del WLC, fare clic su **Security** (Sicurezza).
2. Dal menu visualizzato sul lato sinistro della pagina Sicurezza, fare clic su **Trusted AP policies** (Criteri access point attendibili) elencato sotto l'intestazione Criteri di protezione wireless.



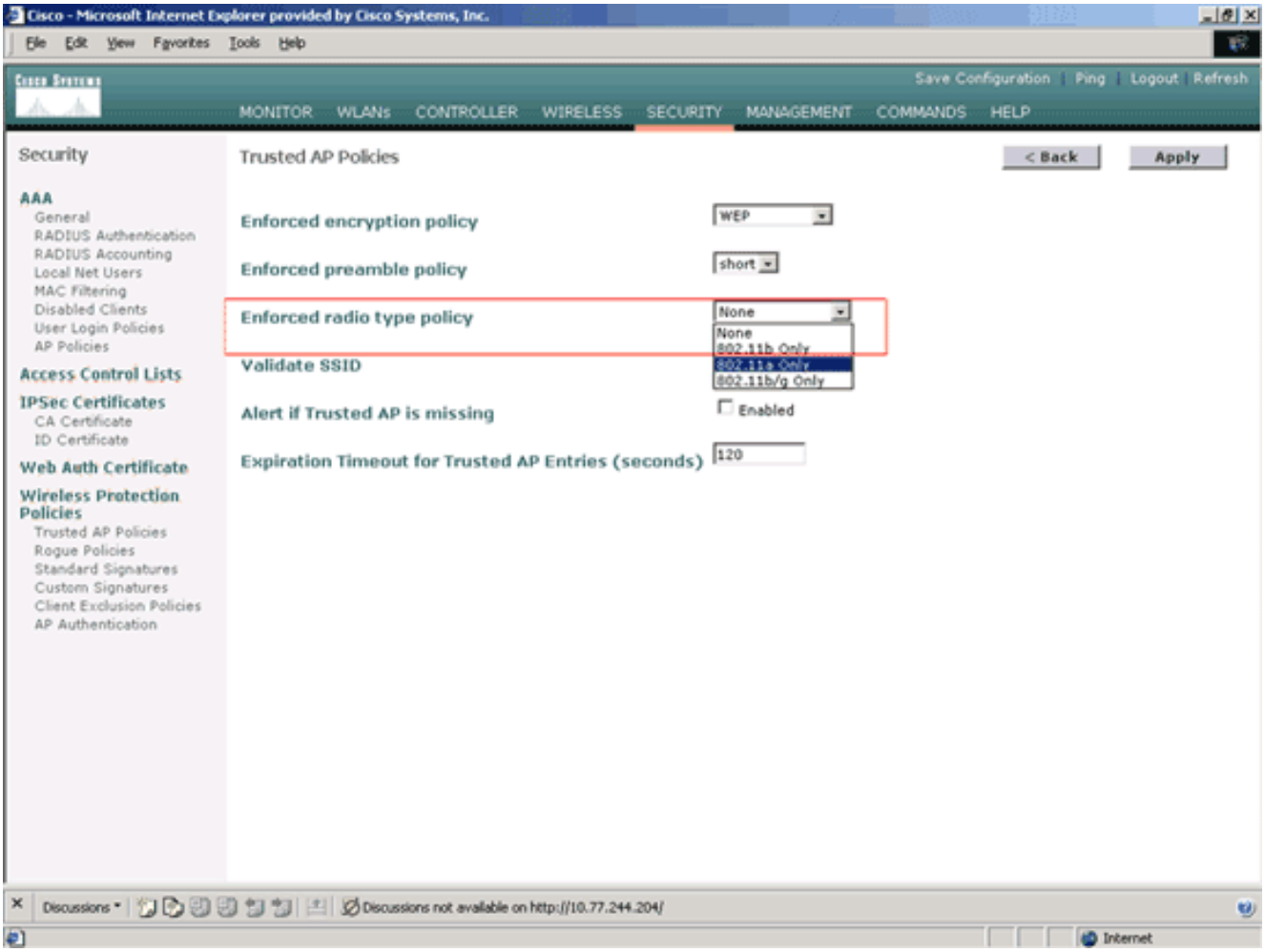
3. Nella pagina Criteri Trusted AP, selezionare il tipo di crittografia desiderato (Nessuno, Aperto, WEP, WPA/802.11i) dall'elenco a discesa Criterio di crittografia applicato.



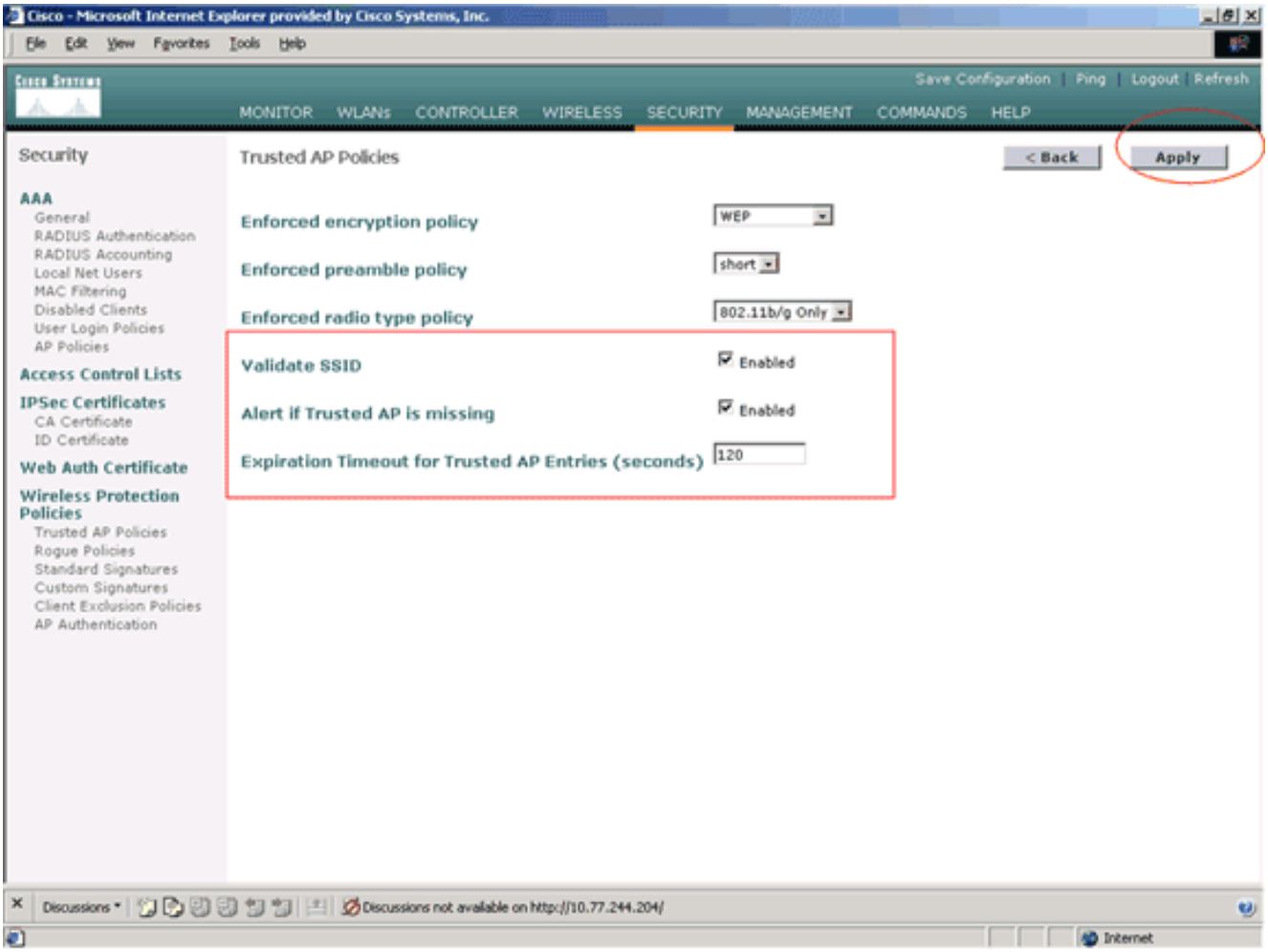
4. Selezionare il tipo di preambolo desiderato (None, Short, Long) dall'elenco a discesa Criterio tipo di preambolo
imposto.



5. Selezionare il tipo di radio desiderato (Nessuno, solo 802.11b, solo 802.11a, solo 802.11b/g) dall'elenco a discesa Criterio tipo radio
imposto.



6. Per abilitare o disabilitare l'impostazione Convalida SSID, selezionare o deselezionare la casella di controllo **Convalida SSID abilitato**.
7. Per abilitare o disabilitare l'impostazione **Avvisa se** il punto di accesso attendibile è mancante, selezionare o deselezionare la casella di controllo Avvisa se il punto di accesso attendibile è mancante.
8. Immettere un valore (in secondi) per l'opzione **Timeout scadenza per voci PA attendibili**.



9. Fare clic su **Apply** (Applica).

Nota: per configurare queste impostazioni dalla CLI del WLC, è possibile usare il comando **config wps trusted-ap** con l'opzione di criterio appropriata.

```
Cisco Controller) >config wps trusted-ap ?

encryption      Configures the trusted AP encryption policy to be enforced.
missing-ap      Configures alert of missing trusted AP.
preamble        Configures the trusted AP preamble policy to be enforced.
radio           Configures the trusted AP radio policy to be enforced.
timeout         Configures the expiration time for trusted APs, in seconds.
```

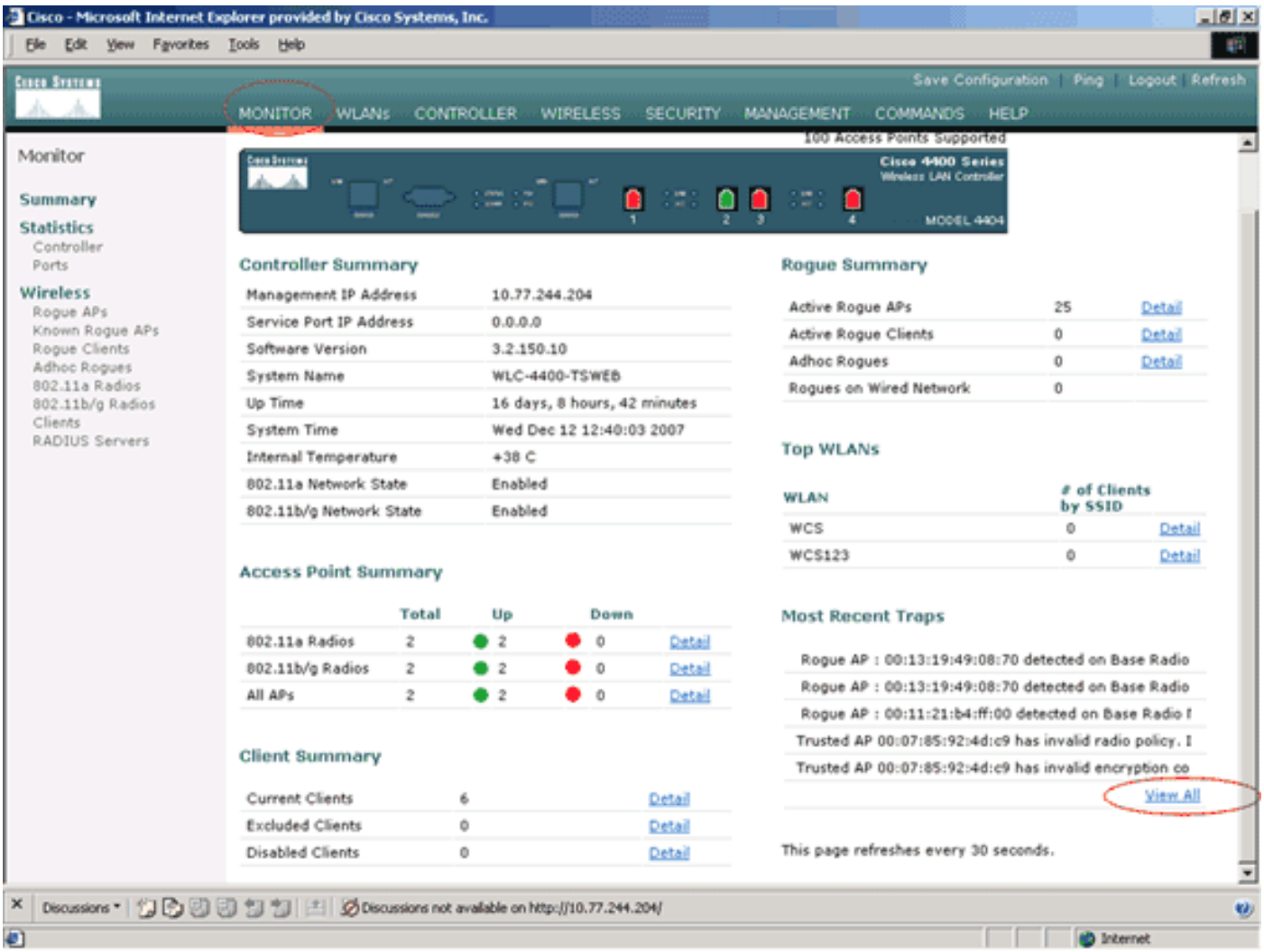
Messaggio di avviso di violazione dei criteri PA trusted

Di seguito è riportato un esempio di messaggio di avviso di violazione dei criteri del punto di accesso attendibile visualizzato dal controller.

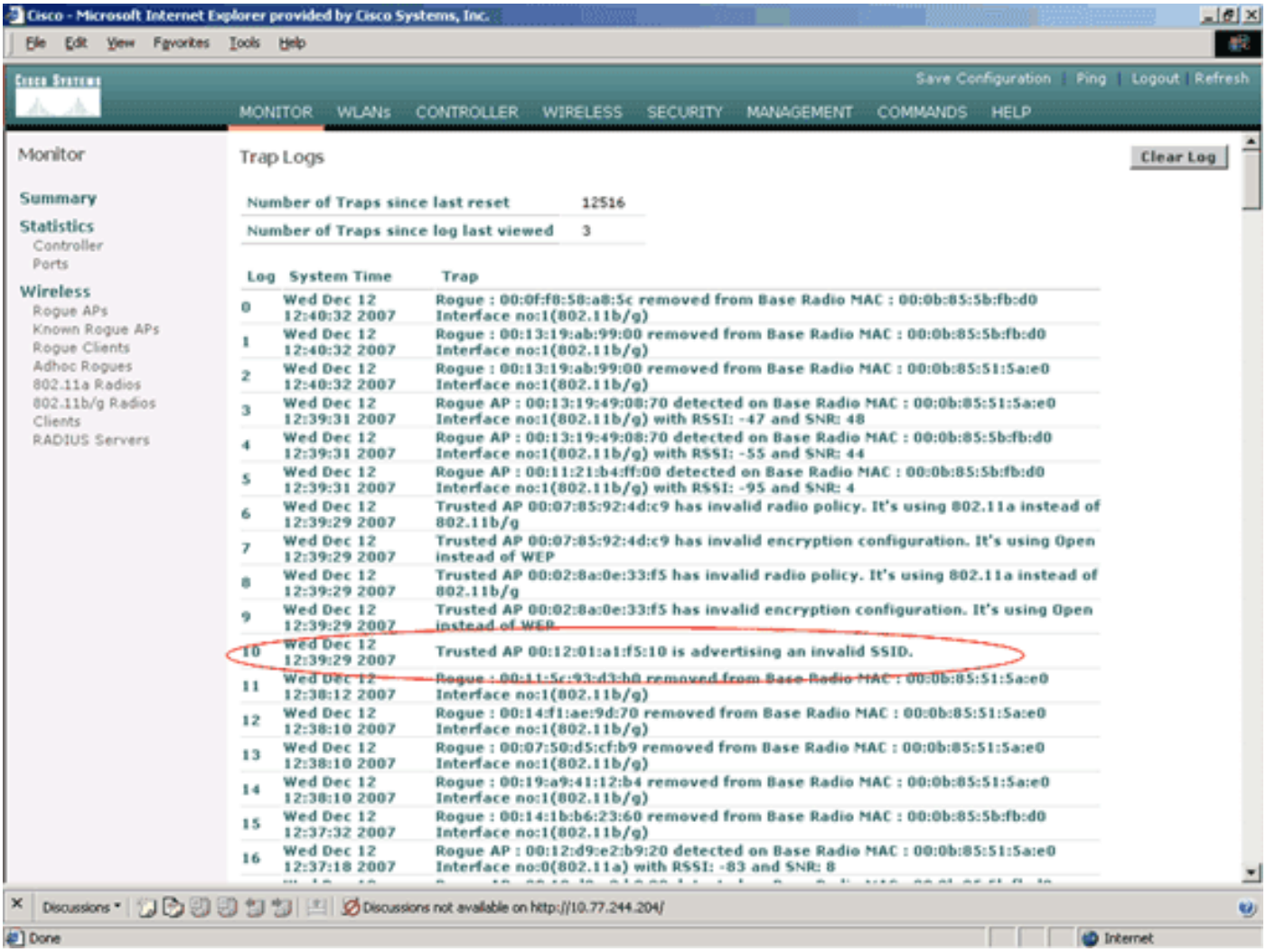
```
Thu Nov 16 12:39:12 2006  [WARNING] apf_rogue.c 1905: Possible AP
impersonation of xx:xx:xx:xx:xx:xx, using source address of
00:16:35:9e:6f:3a, detected by 00:17:df:7d:e1:70 on slot 0
 Thu Nov 16 12:39:12 2006  [SECURITY] apf_rogue.c 1490: Trusted AP Policy
failed for AP xx:xx:xx:xx:xx:xx - invalid SSID 'SSID1'
Thu Nov 16 12:39:12 2006  [SECURITY] apf_rogue.c 1457: Trusted AP Policy
failed for AP xx:xx:xx:xx:xx:xx - invalid encryption type
Thu Nov 16 12:39:12 2006  Previous message occurred 6 times
```

Si notino qui i messaggi di errore evidenziati. Questi messaggi di errore indicano che il SSID e il tipo di crittografia configurato nell'access point attendibile non corrispondono all'impostazione dei criteri dell'access point attendibile.

Lo stesso messaggio di avviso può essere visualizzato dalla GUI del WLC. Per visualizzare questo messaggio, andare al menu principale dell'interfaccia utente del WLC e fare clic su **Monitor**. Nella sezione Trap più recenti della pagina Monitor, fare clic su **View All** per visualizzare tutti gli alert recenti sul WLC.



Nella pagina Trap più recenti è possibile identificare il controller che ha generato il messaggio di avviso di violazione dei criteri del punto di accesso attendibile, come mostrato nell'immagine seguente:



Informazioni correlate

- Guida alla configurazione di Cisco Wireless LAN Controller, versione 5.2 - Abilitazione del rilevamento dei punti di accesso di routing nei gruppi RF
- Guida alla configurazione di Cisco Wireless LAN Controller, versione 4.0 - Configurazione delle soluzioni di sicurezza
- Rilevamento di anomalie nelle reti wireless unificate
- Guida alla progettazione e all'installazione dei telefoni SpectraLink
- Esempio di configurazione della connessione base della LAN wireless
- Risoluzione dei problemi di connettività in una rete LAN wireless
- Esempi di configurazione dell'autenticazione sui controller LAN wireless
- Documentazione e supporto tecnico – Cisco Systems