Vertrauenswürdige AP-Richtlinien auf einem Wireless LAN-Controller

Inhalt

Einführung

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

Voraussetzungen

Anforderungen

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

Konventionen

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

Vertrauenswürdige AP-Richtlinien

Vertrauenswürdige AP-Richtlinien sind eine Sicherheitsfunktion im Controller, die für die Verwendung in Szenarien entwickelt wurde, in denen Kunden ein paralleles autonomes AP-Netzwerk mit dem Controller haben. In diesem Szenario kann der autonome Access Point als vertrauenswürdiger Access Point auf dem Controller markiert werden, und der Benutzer kann

Richtlinien für diese vertrauenswürdigen Access Points definieren (die nur WEP oder WPA, unsere eigene SSID, kurze Präambel usw. verwenden sollten). Wenn einer dieser Access Points diese Richtlinien nicht erfüllt, löst der Controller einen Alarm für das Netzwerkmanagementgerät (Wireless Control System) aus, das angibt, dass ein vertrauenswürdiger Access Point gegen eine konfigurierte Richtlinie verstößt.

Was ist ein vertrauenswürdiger Access Point?

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

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

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

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

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

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

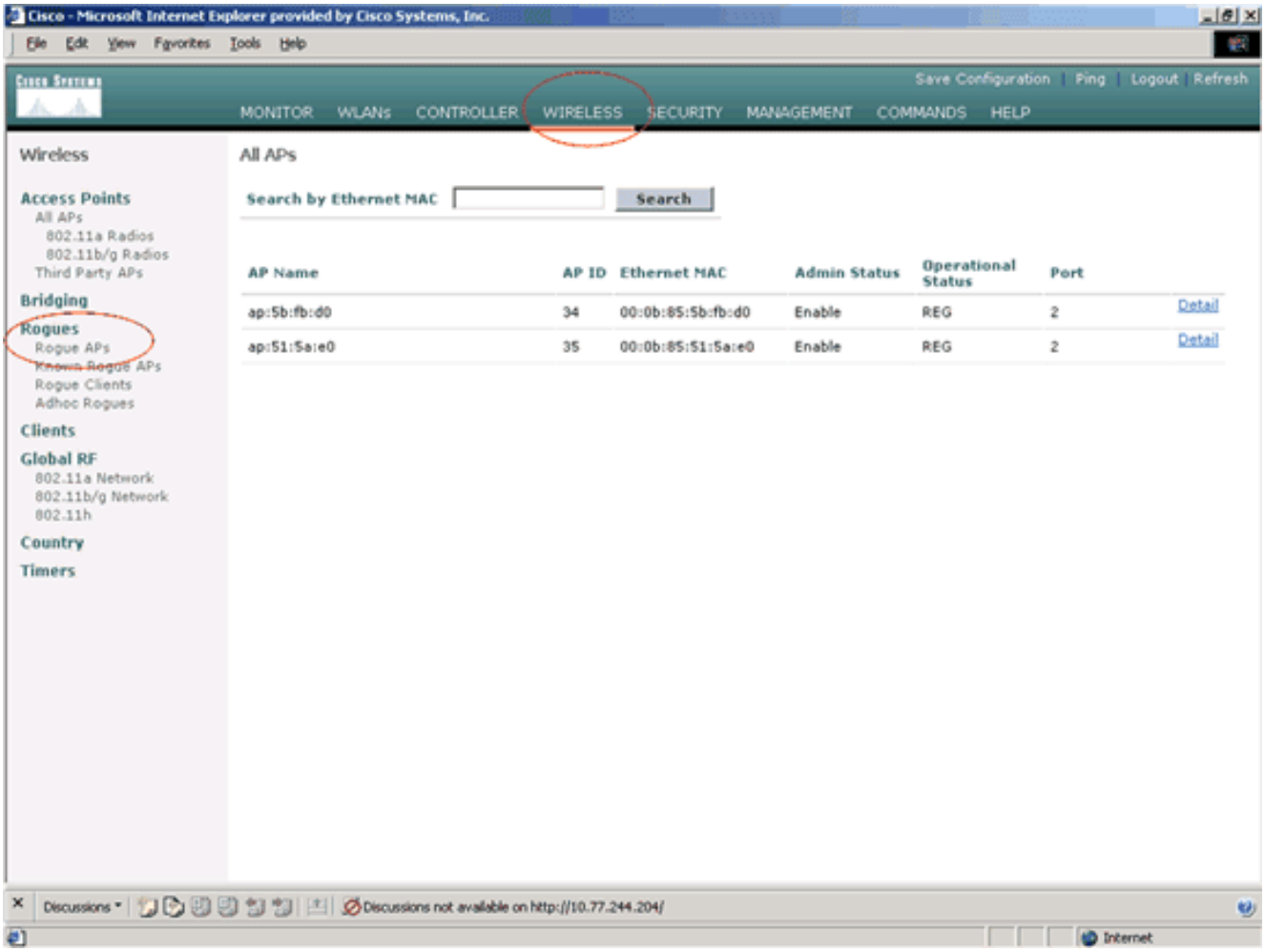
Wenn Sie APs haben, die VxWorks oder IOS ausführen (wie in Kategorie 1), werden diese nie der LWAPP-Gruppe beitreten oder MFP ausführen. Sie können jedoch die auf dieser Seite aufgeführten Richtlinien durchsetzen. In solchen Fällen müssen vertrauenswürdige AP-Richtlinien auf dem Controller konfiguriert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

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

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

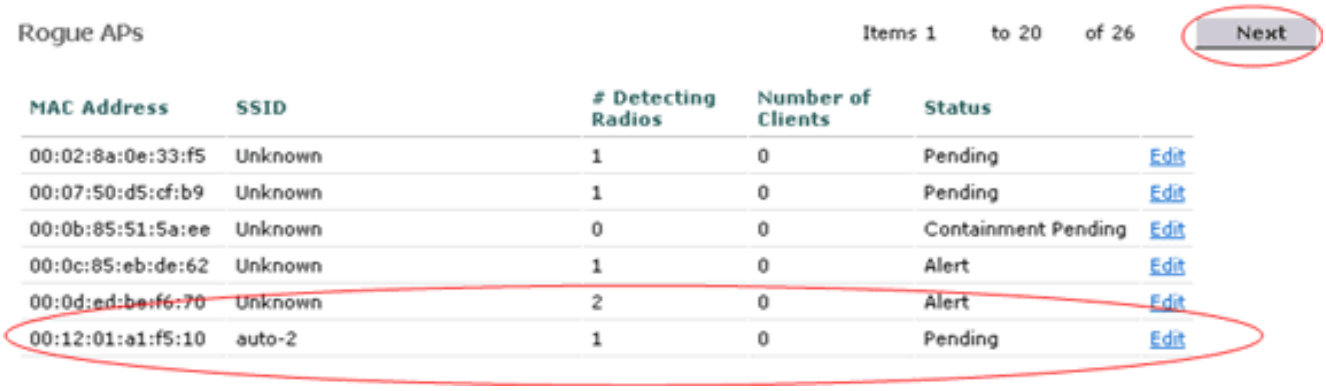
Gehen Sie wie folgt vor, um einen Access Point als vertrauenswürdigen Access Point zu konfigurieren:

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



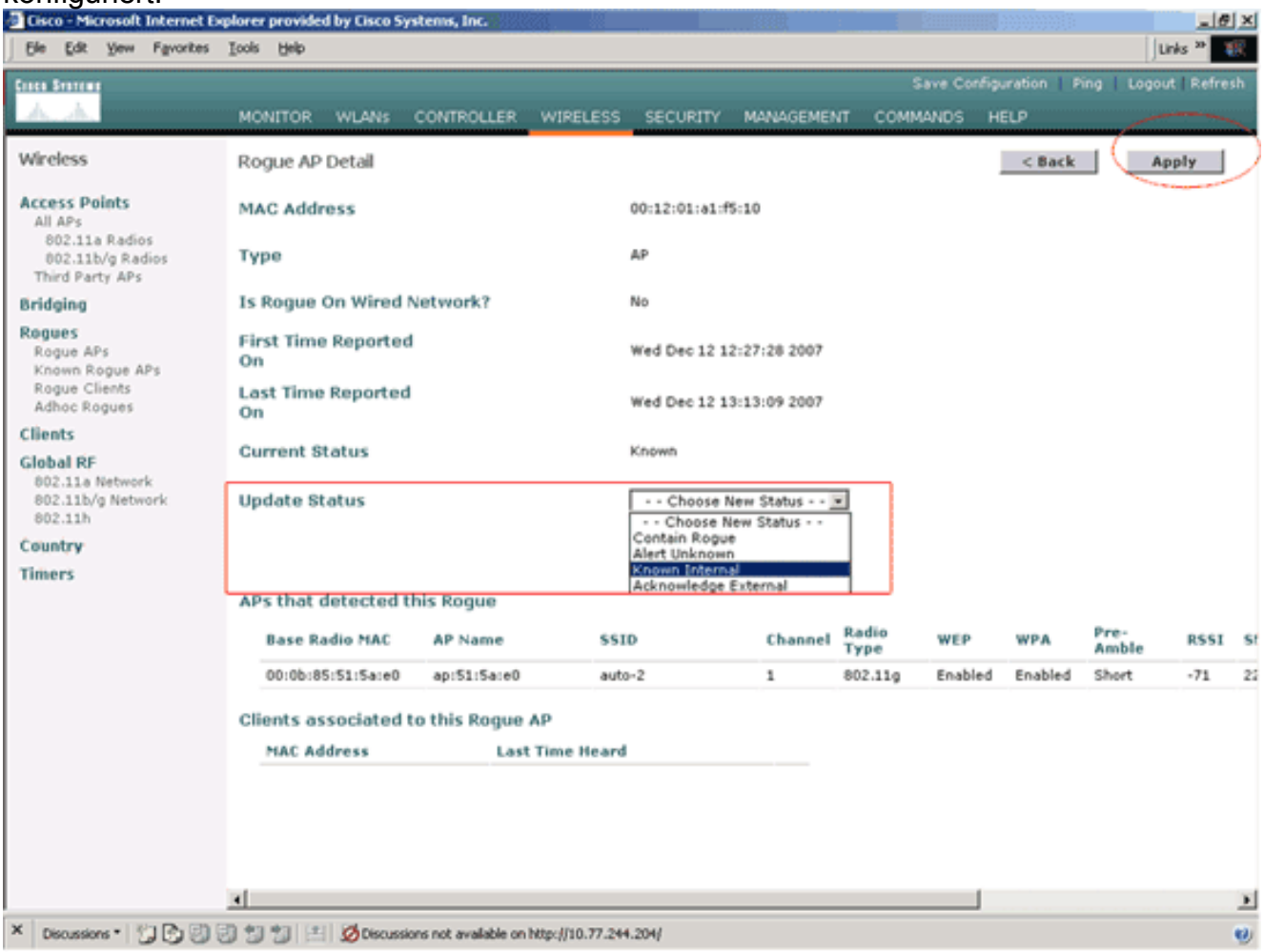
Auf der Seite für nicht autorisierte APs werden alle APs aufgelistet, die im Netzwerk als nicht autorisierte APs erkannt werden.

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



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

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

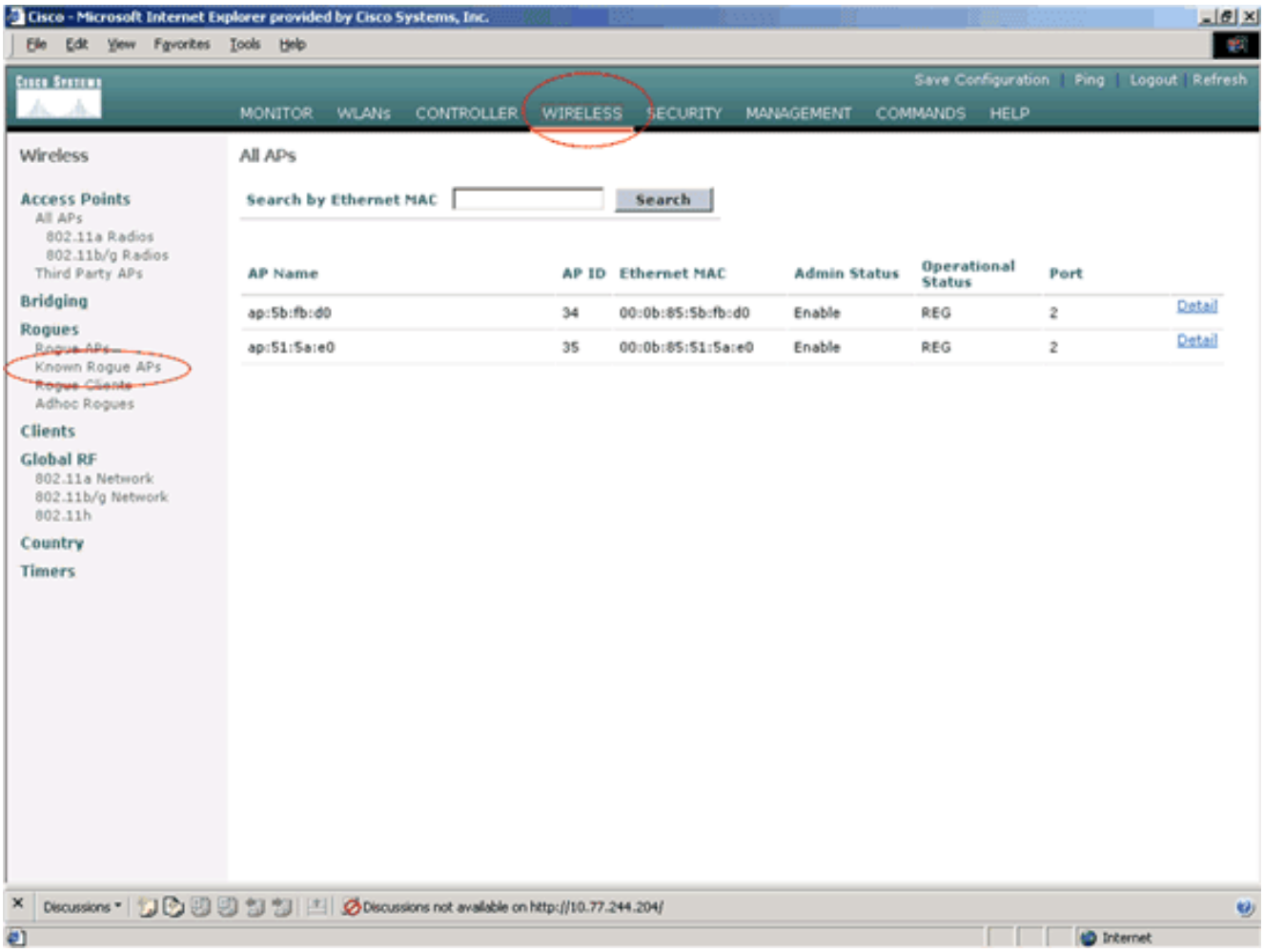


7. Wiederholen Sie diese Schritte für alle APs, die Sie als vertrauenswürdige APs konfigurieren möchten.

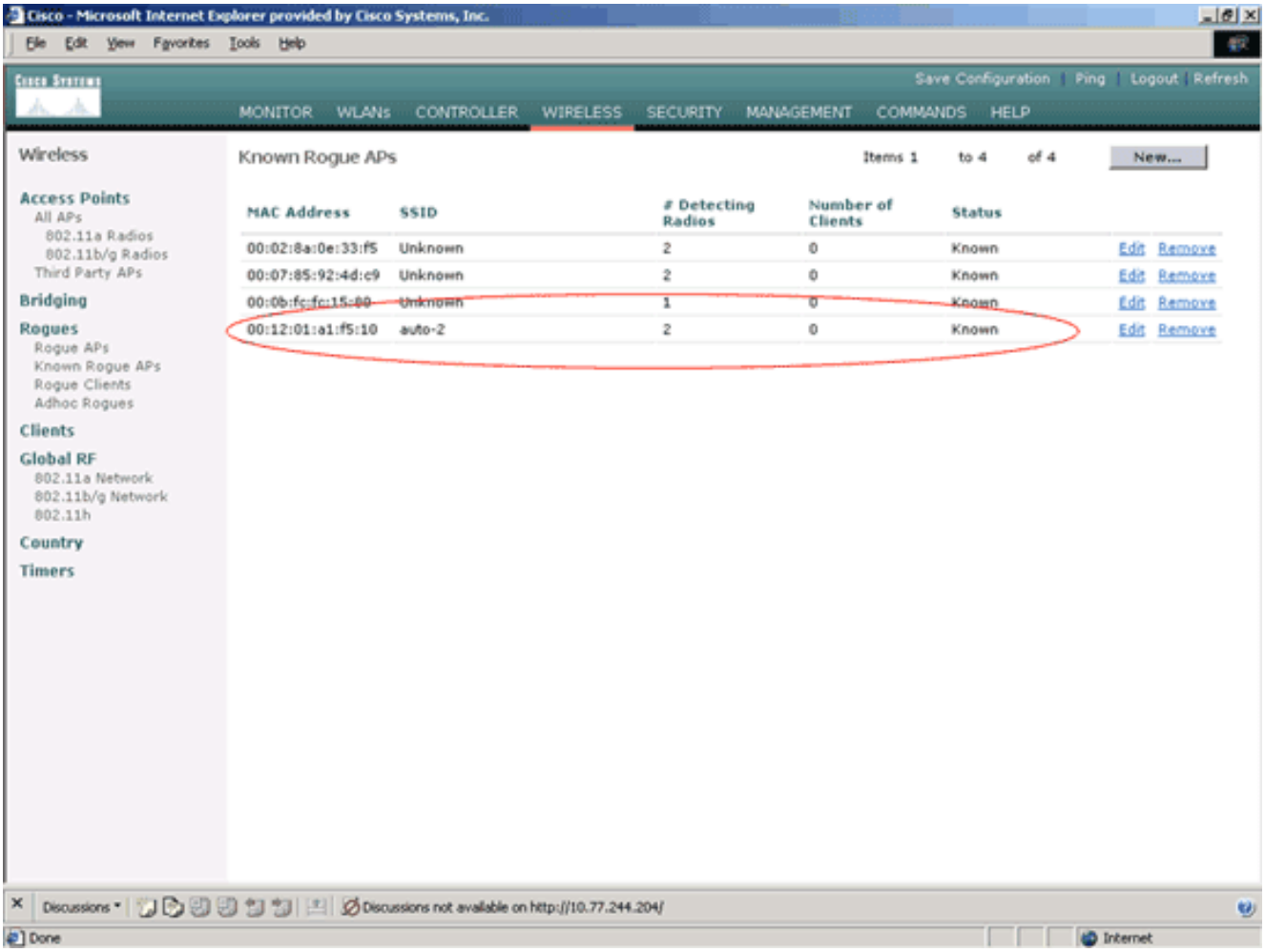
Überprüfen der Konfiguration des vertrauenswürdigen Access Points

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

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



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



Einstellungen für vertrauenswürdige AP-Richtlinien

Der WLC verfügt über folgende vertrauenswürdige AP-Richtlinien:

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

Durchgesetzte Verschlüsselungsrichtlinie

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

- Keine
- Öffnen
- WEP
- WPA/802.11i

Der WLC überprüft, ob der auf dem vertrauenswürdigen Access Point konfigurierte Verschlüsselungstyp mit dem Verschlüsselungstyp übereinstimmt, der auf der Einstellung "**Enforced Encryption Policy**" (**Durchgesetzte Verschlüsselungsrichtlinie**) konfiguriert wurde. Wenn

der vertrauenswürdige Access Point den angegebenen Verschlüsselungstyp nicht verwendet, löst der WLC einen Alarm für das Managementsystem aus, um geeignete Maßnahmen zu ergreifen.

Durchgesetzte Präambelrichtlinie

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

- Keine
- Kurz
- lang

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

Durchgesetzte Funktyp-Richtlinie

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

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

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

SSID validieren

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

Warnung, wenn Trusted AP fehlt

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

Ablaufzeitüberschreitung für vertrauenswürdige AP-Einträge (Sekunden)

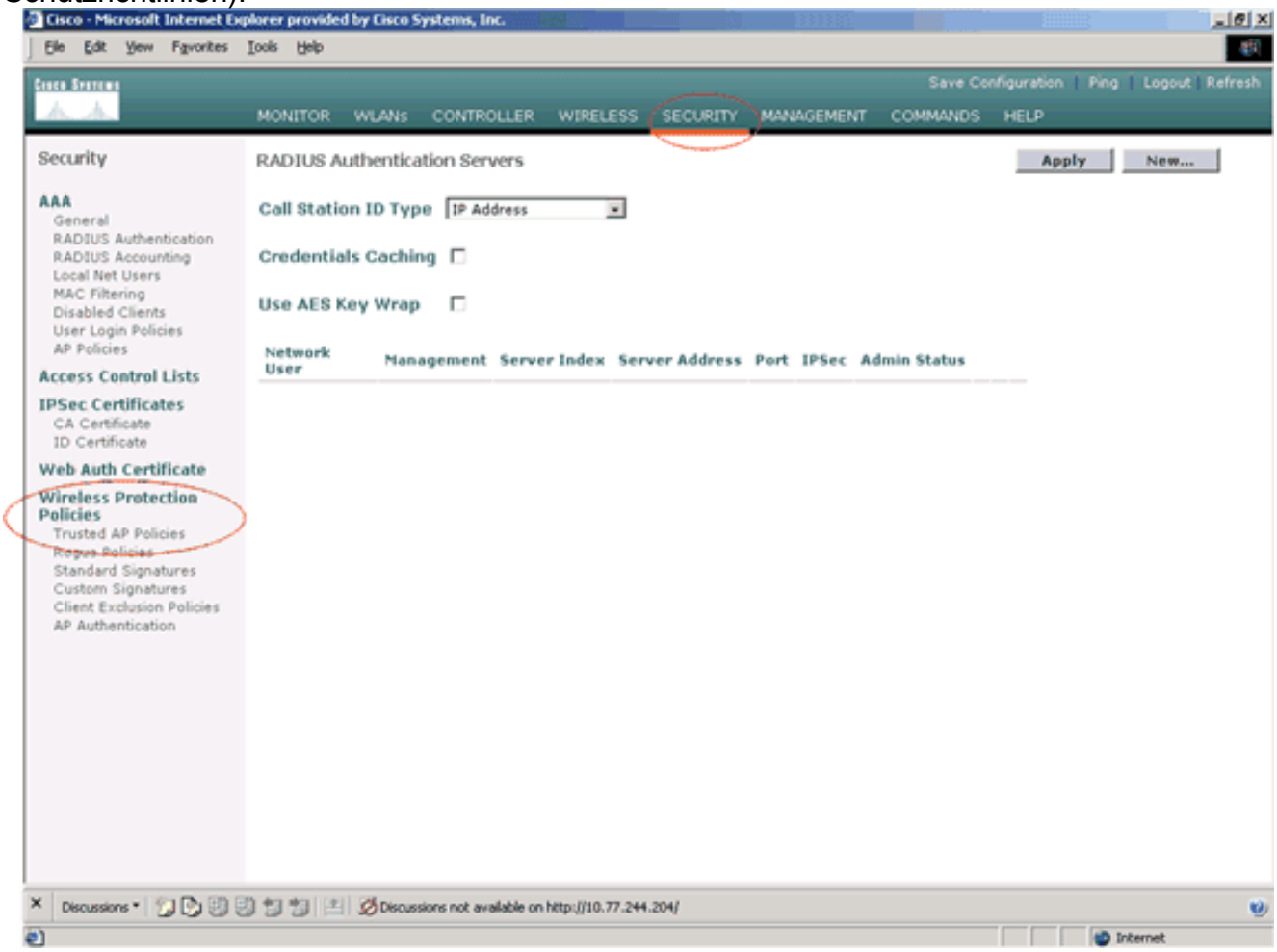
Dieser Timeout-Wert gibt die Anzahl der Sekunden an, bevor der vertrauenswürdige Access Point als abgelaufen gilt und vom WLC-Eintrag geleert wird. Sie können diesen Timeout-Wert in Sekunden (120-3600 Sekunden) angeben.

Konfigurieren vertrauenswürdiger AP-Richtlinien auf dem WLC

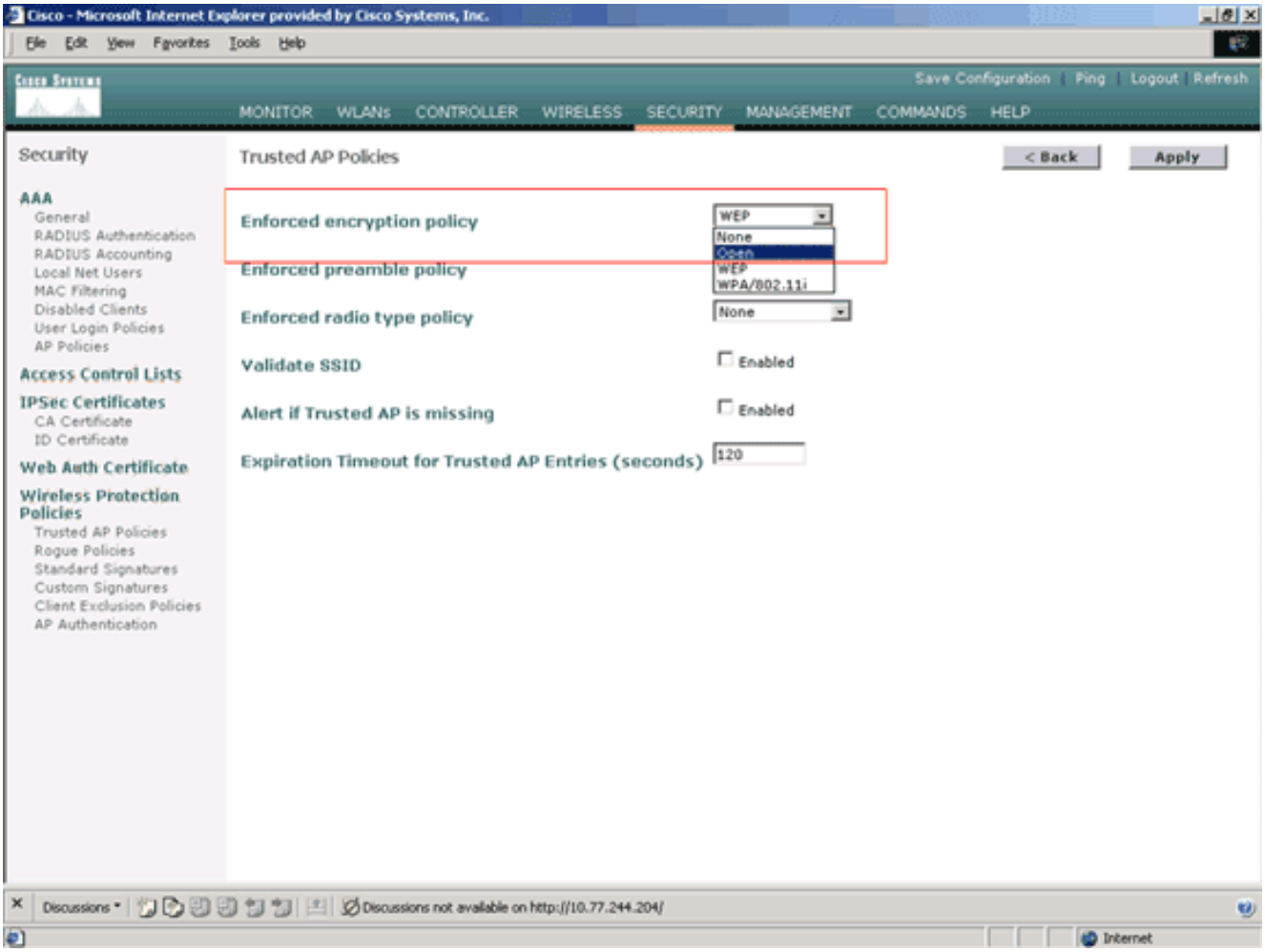
Gehen Sie wie folgt vor, um vertrauenswürdige AP-Richtlinien auf dem WLC über die GUI zu konfigurieren:

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

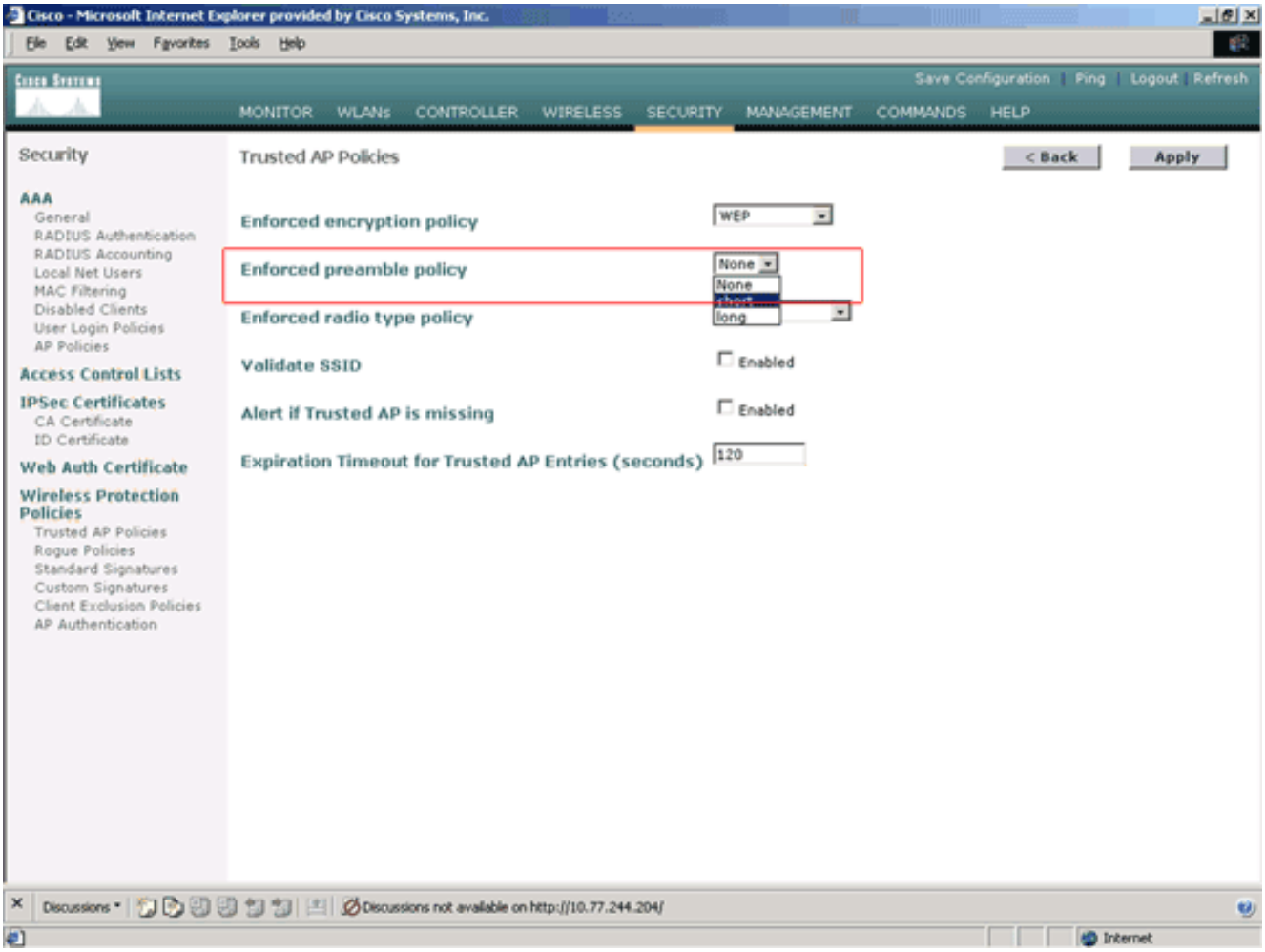
1. Klicken Sie im Hauptmenü der WLC-GUI auf **Sicherheit**.
2. Klicken Sie im Menü links auf der Seite Sicherheit auf **Vertrauenswürdige AP-Richtlinien** unter der Überschrift Wireless Protection Policies (Wireless-Schutzrichtlinien).



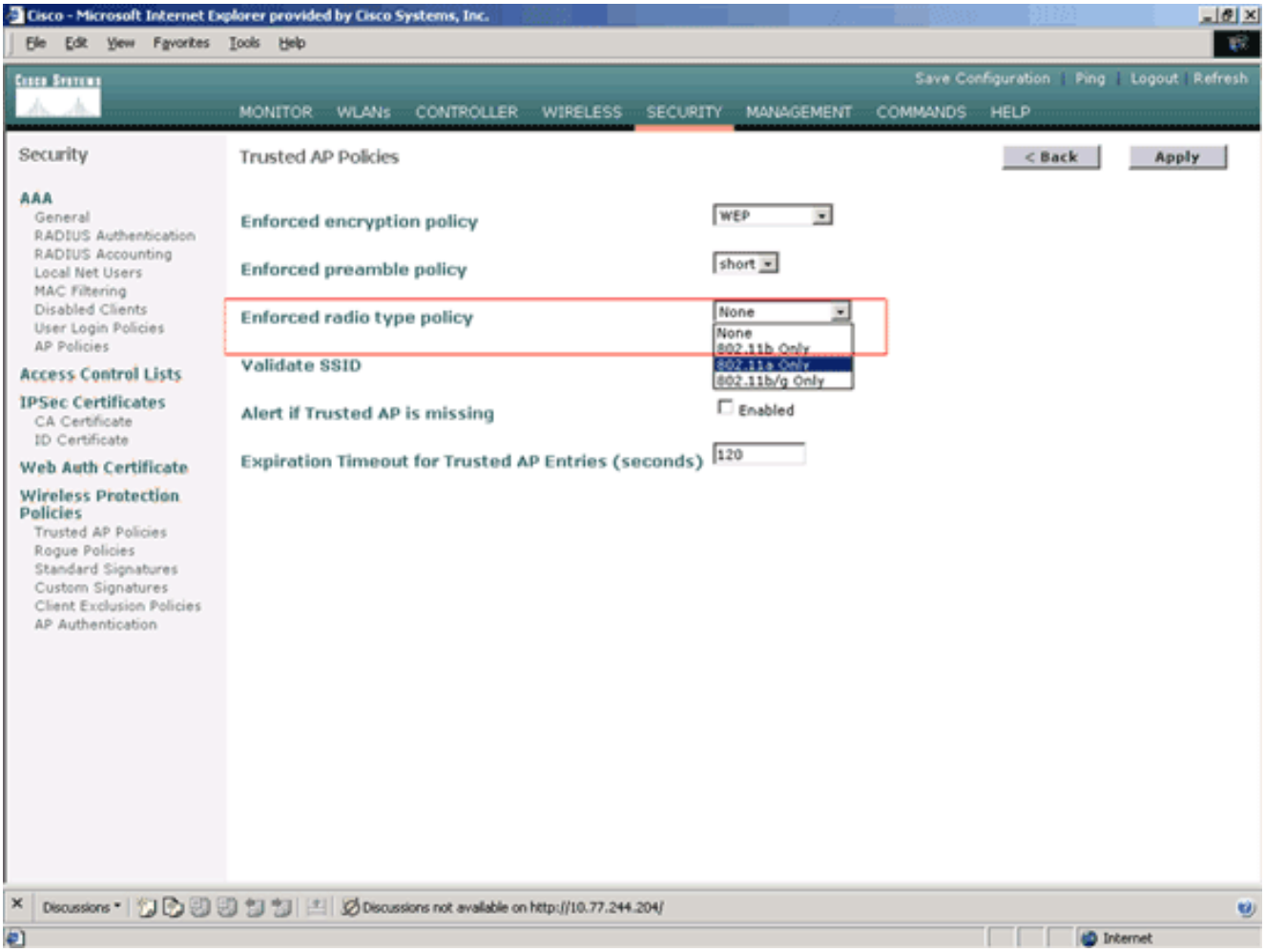
3. Wählen Sie auf der Seite Trusted AP Policies (Vertrauenswürdige AP-Richtlinien) den gewünschten Verschlüsselungstyp (Keine, Offen, WEP, WPA/802.11i) aus der Dropdown-Liste Enforced Encryption Policy (Durchgesetzte Verschlüsselungsrichtlinie) aus.



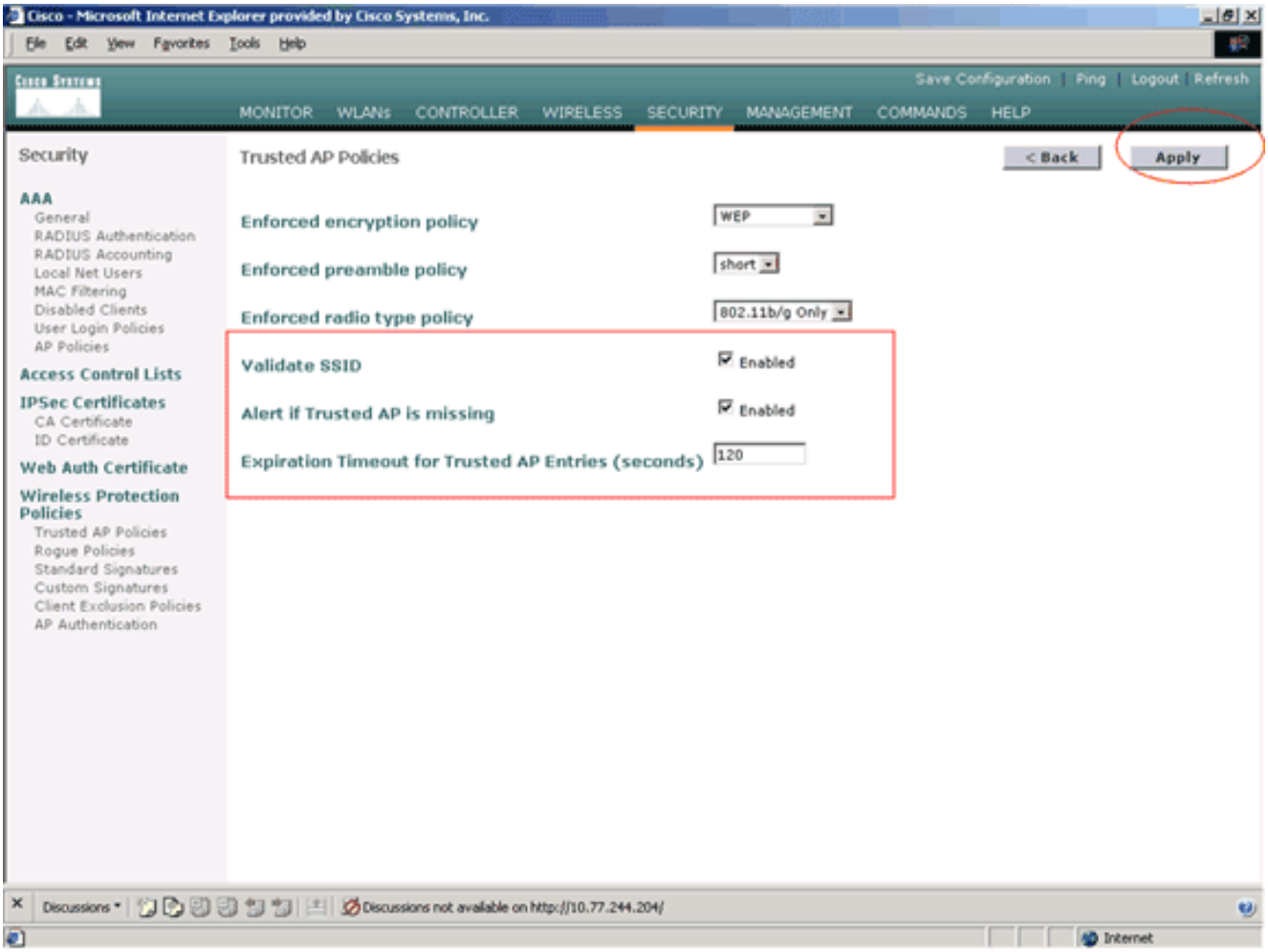
4. Wählen Sie den gewünschten Präambeltyp (None, Short, Long) aus der Dropdown-Liste Enforced Preamble Type policy (Richtlinie für durchgesetzten Präambeltyp) aus.



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



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



9. Klicken Sie auf **Übernehmen**.

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

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

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

Warnmeldung für vertrauenswürdige AP-Policy-Verletzung

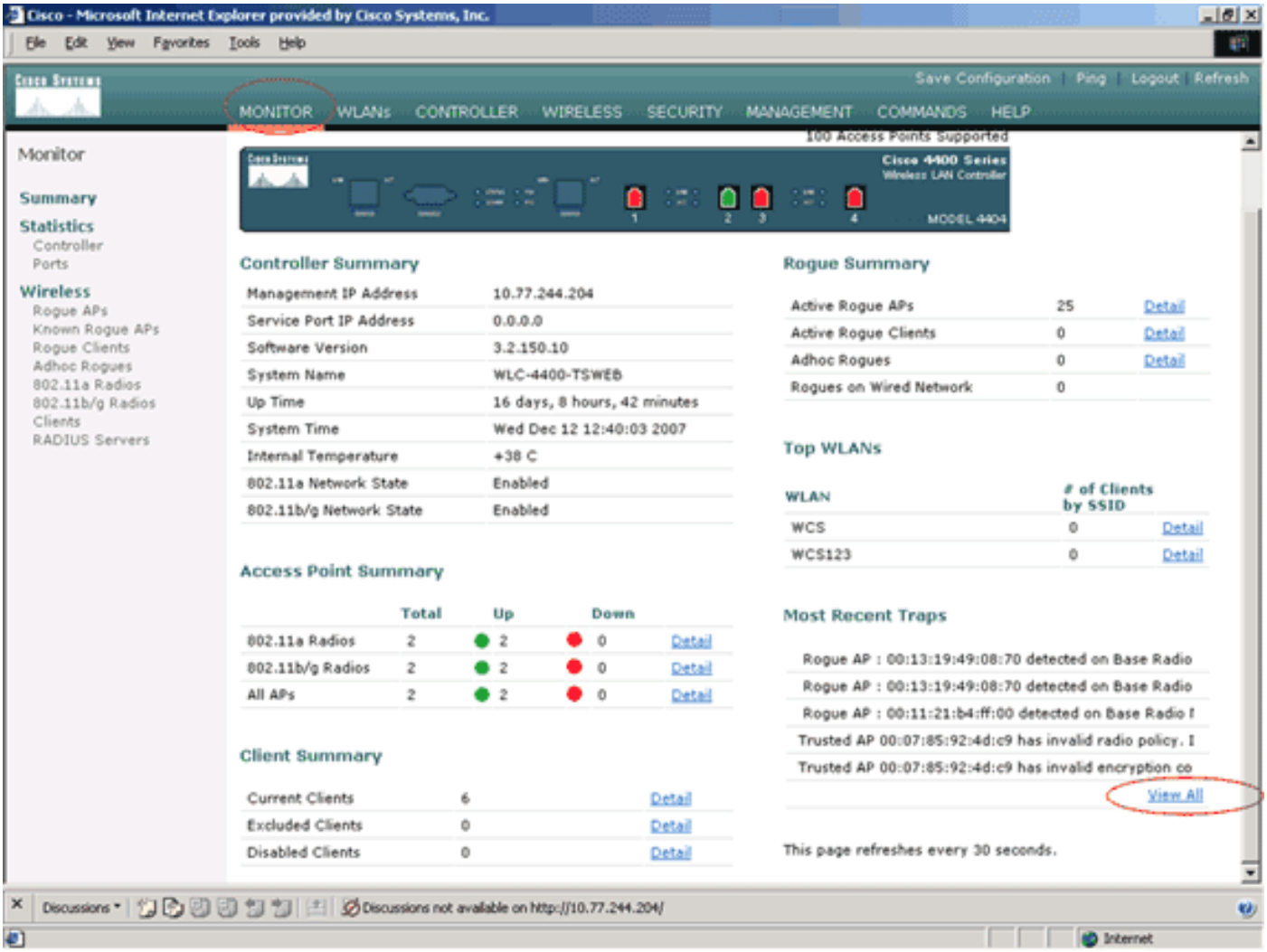
Im Folgenden sehen Sie ein Beispiel für eine Warnung, dass der Controller eine vertrauenswürdige AP-Richtlinie verletzt.

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

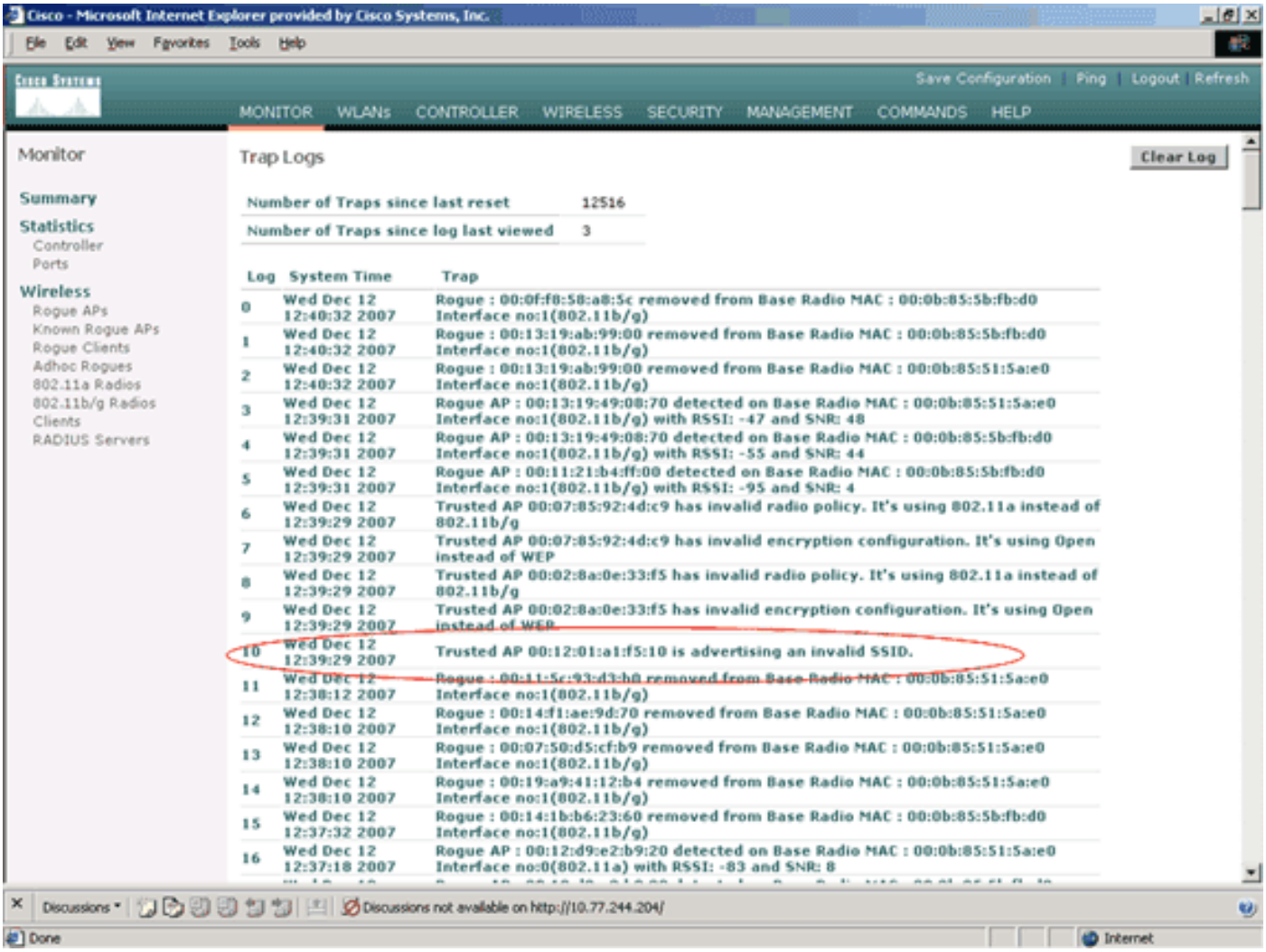
Beachten Sie die hervorgehobenen Fehlermeldungen hier. Diese Fehlermeldungen weisen darauf hin, dass die SSID und der auf dem vertrauenswürdigen Access Point konfigurierte Verschlüsselungstyp nicht mit der Richtlinieneinstellung für vertrauenswürdige Access Points

übereinstimmen.

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



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



Zugehörige Informationen

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