Políticas AP de confianza en un controlador LAN inalámbrico

Contenido

Introducción

Este documento describe las políticas de protección inalámbrica *AP* de confianza en un controlador de LAN inalámbrica (WLC), define las políticas AP de confianza y proporciona una breve descripción de todas las políticas AP de confianza.

Prerequisites

Requirements

Asegúrese de tener una comprensión básica de los parámetros de seguridad de LAN inalámbrica (como SSID, cifrado, autenticación, etc.).

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Políticas de AP de confianza

Las políticas AP de confianza es una función de seguridad en el controlador que está diseñada para ser utilizada en escenarios donde los clientes tienen una red AP autónoma paralela junto con el controlador. En ese escenario, el AP autónomo se puede marcar como el AP confiable en el controlador, y el usuario puede definir políticas para estos AP de confianza (que deberían utilizar

solamente WEP o WPA, nuestro propio SSID, breve preámbulo, etc.). Si alguno de estos AP no cumple con estas políticas, el controlador emite una alarma al dispositivo de administración de red (Wireless Control System) que indica que un AP de confianza violó una política configurada.

¿Qué es un AP de confianza?

Los AP de confianza son AP que no forman parte de una organización. Sin embargo, no suponen una amenaza para la seguridad de la red. Estos AP también se llaman AP amistosos. Existen varios escenarios donde puede que desee configurar un AP como un AP de confianza.

Por ejemplo, puede tener diferentes categorías de AP en su red como:

- **AP que posee que no ejecutan LWAPP (tal vez ejecuten IOS o VxWorks)**
- AP LWAPP que los empleados aportan (con el conocimiento del administrador)
- AP LWAPP utilizados para probar la red existente
- AP LWAPP que poseen los vecinos

Normalmente, los APs confiables son APs que caen en la **categoría 1**, que son APs que posee que no ejecutan LWAPP. Pueden ser AP antiguos que ejecutan VxWorks o IOS. Para asegurarse de que estos AP no dañen la red, se pueden aplicar ciertas características, como SSID correctos y tipos de autenticación. Configure las políticas AP confiables en el WLC, y asegúrese de que los AP confiables cumplan estas políticas. Si no es así, puede configurar el controlador para realizar varias acciones, como alarmar al dispositivo de administración de red (WCS).

Los AP conocidos que pertenecen a los vecinos se pueden configurar como AP de confianza.

Normalmente, la MFP (protección de tramas de administración) debería evitar que los AP que no son AP LWAPP legítimos se unan al WLC. Si las tarjetas NIC soportan MFP, no se les permite aceptar desautenticaciones de dispositivos que no sean los AP reales. Consulte Ejemplo de Configuración de Protección de Tramas de Administración de Infraestructura (MFP) con WLC y LAP para obtener más información sobre MFP.

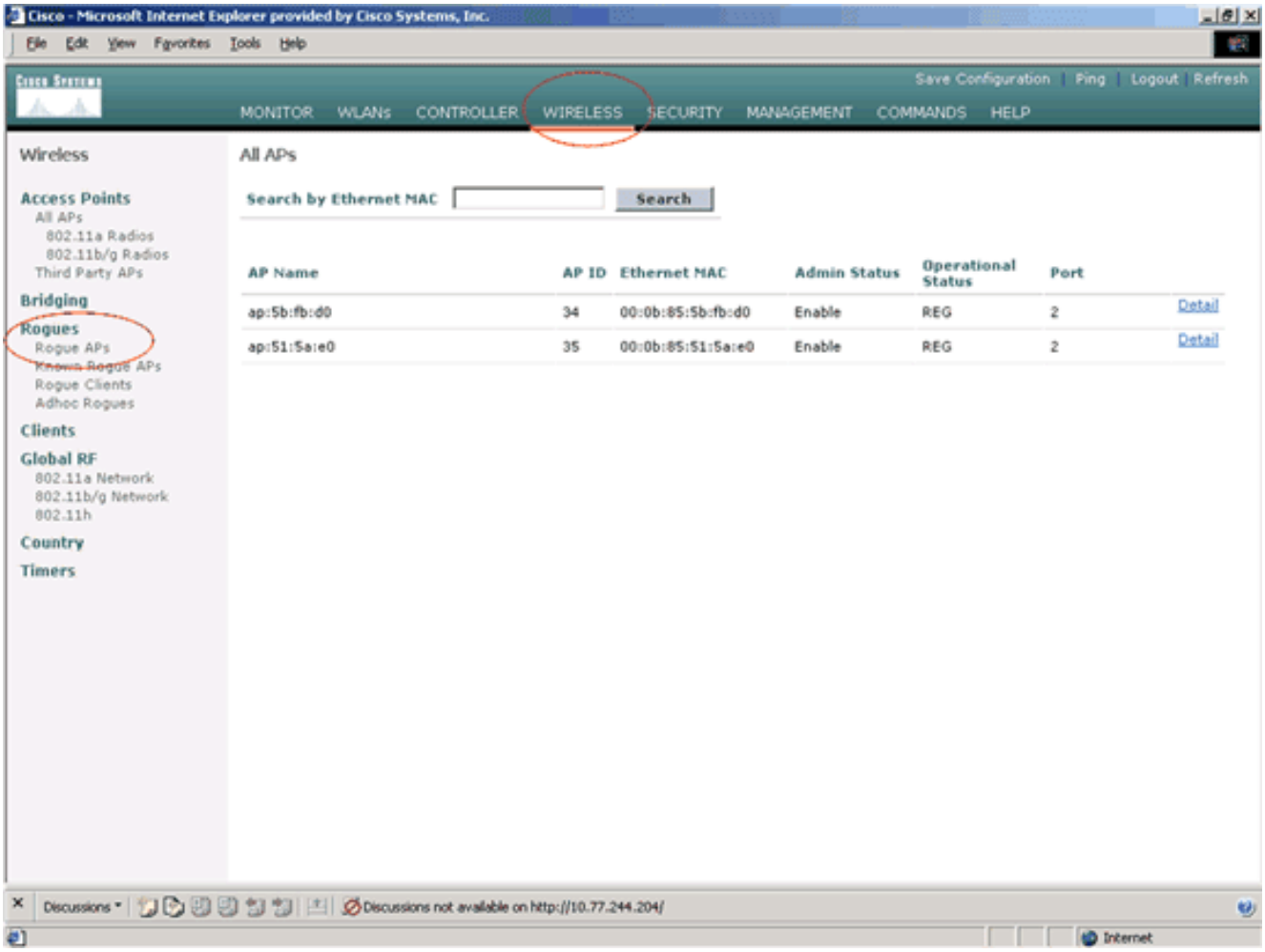
Si tiene AP que ejecutan VxWorks o IOS (como en la categoría 1), nunca se unirán al grupo LWAPP ni realizarán MFP, pero es posible que desee aplicar las políticas enumeradas en esa página. En tales casos, las políticas AP confiables deben configurarse en el controlador para los AP de interés.

En general, si conoce un AP no autorizado e identifica que no es una amenaza para su red, puede identificar ese AP como un AP confiable conocido.

¿Cómo Configurar un AP como AP de Confianza desde la GUI del WLC?

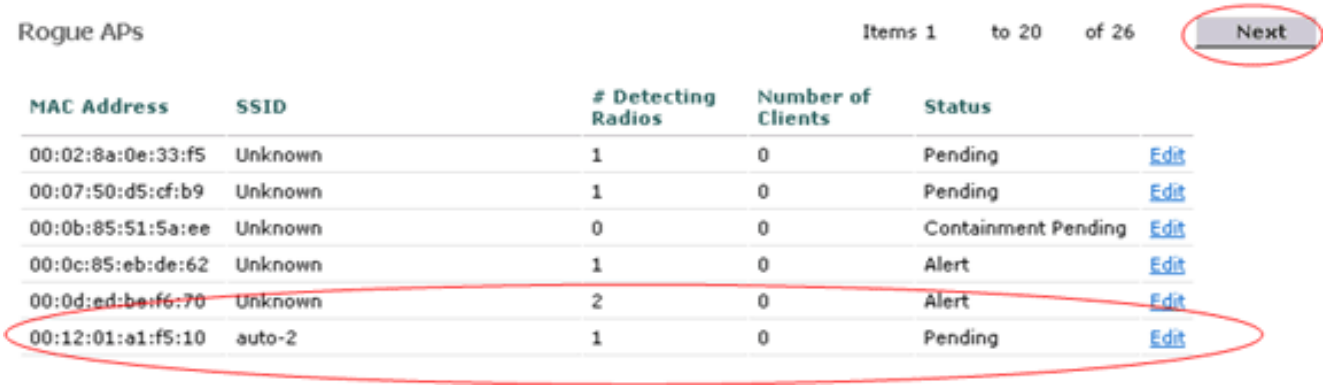
Complete estos pasos para configurar un AP como AP confiable:

1. Inicie sesión en la GUI del WLC a través del login HTTP o https.
2. En el menú principal del controlador, haga clic en **Wireless**.
3. En el menú ubicado en el lado izquierdo de la página Inalámbrica, haga clic en **AP rogue**.



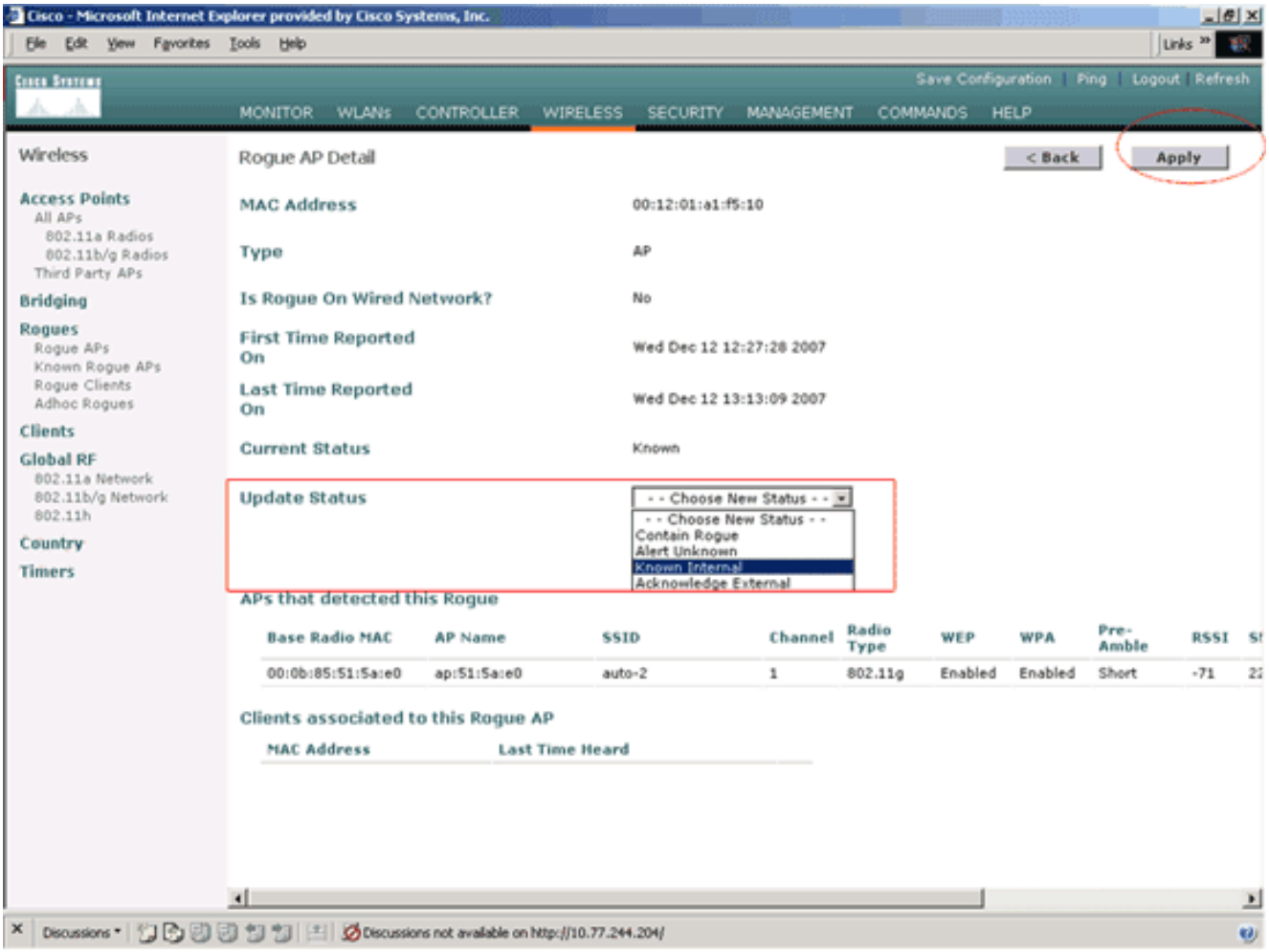
La página de AP rogue enumera todos los AP que se detectan como AP rogue en la red.

4. De esta lista de AP rogue, localice el AP que desea configurar como AP confiable que cae en la categoría 1 (como se explicó en la sección anterior).Puede localizar los AP con las direcciones MAC enumeradas en la página de AP rogue. Si el AP deseado no está en esta página, haga clic en **Next** para identificar el AP de la siguiente página.
5. Una vez que el AP deseado se encuentra desde la lista de AP rogue, haga clic en el botón **Edit** que corresponde al AP, que lo lleva a la página de detalles del AP.



En la página de detalles de AP rogue, puede encontrar información detallada acerca de este AP (como si ese AP se conectó a la red por cable, así como el estado actual del AP y así sucesivamente).

6. Para configurar este AP como un AP confiable, seleccione **Interno Conocido** en la lista desplegable Update Status y haga clic en **Apply**.Cuando usted actualiza el estado de AP a *Interno Conocido*, este AP se configura como el AP confiable de esta red.

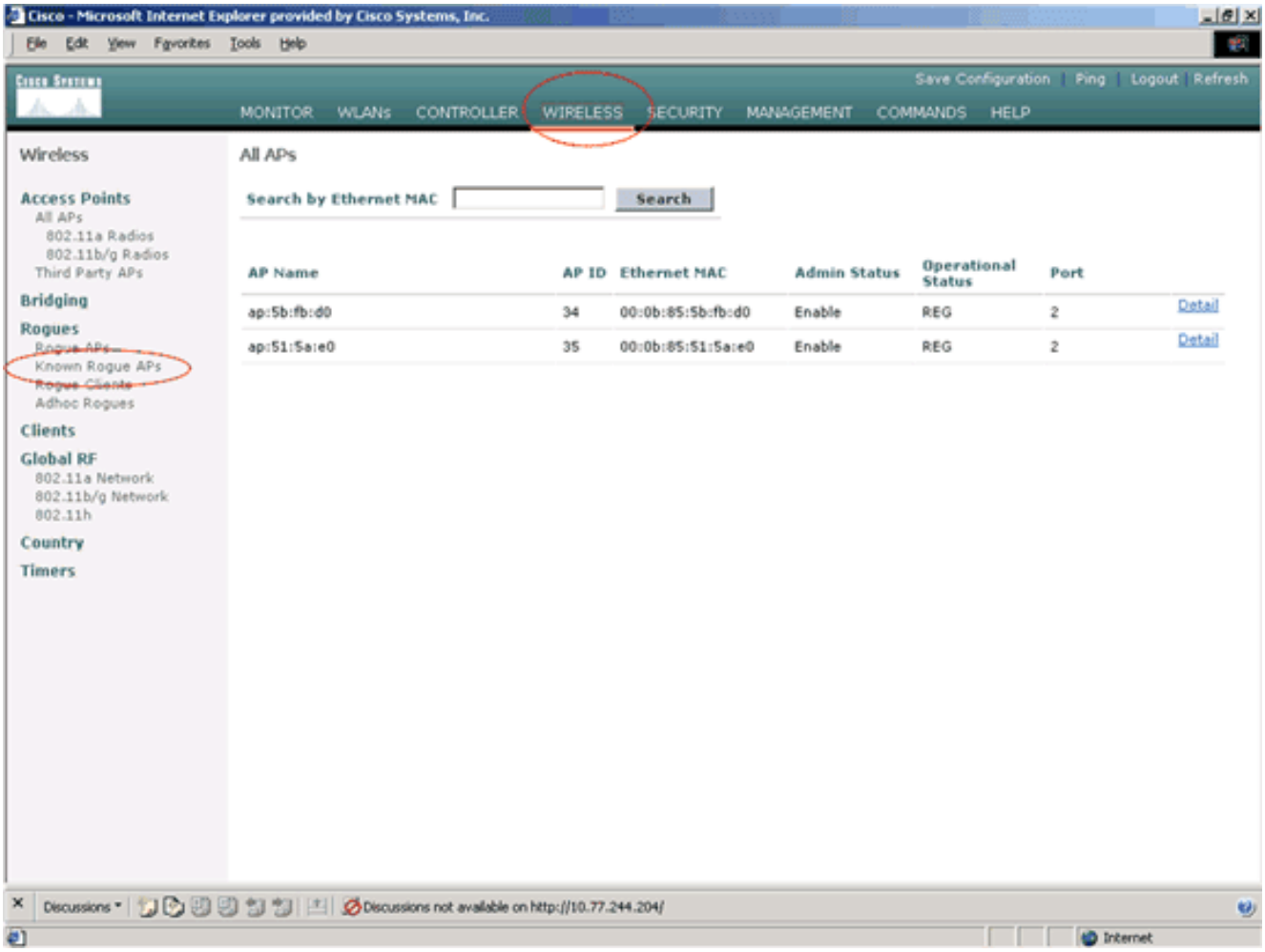


7. Repita estos pasos para todos los AP que desee configurar como AP de confianza.

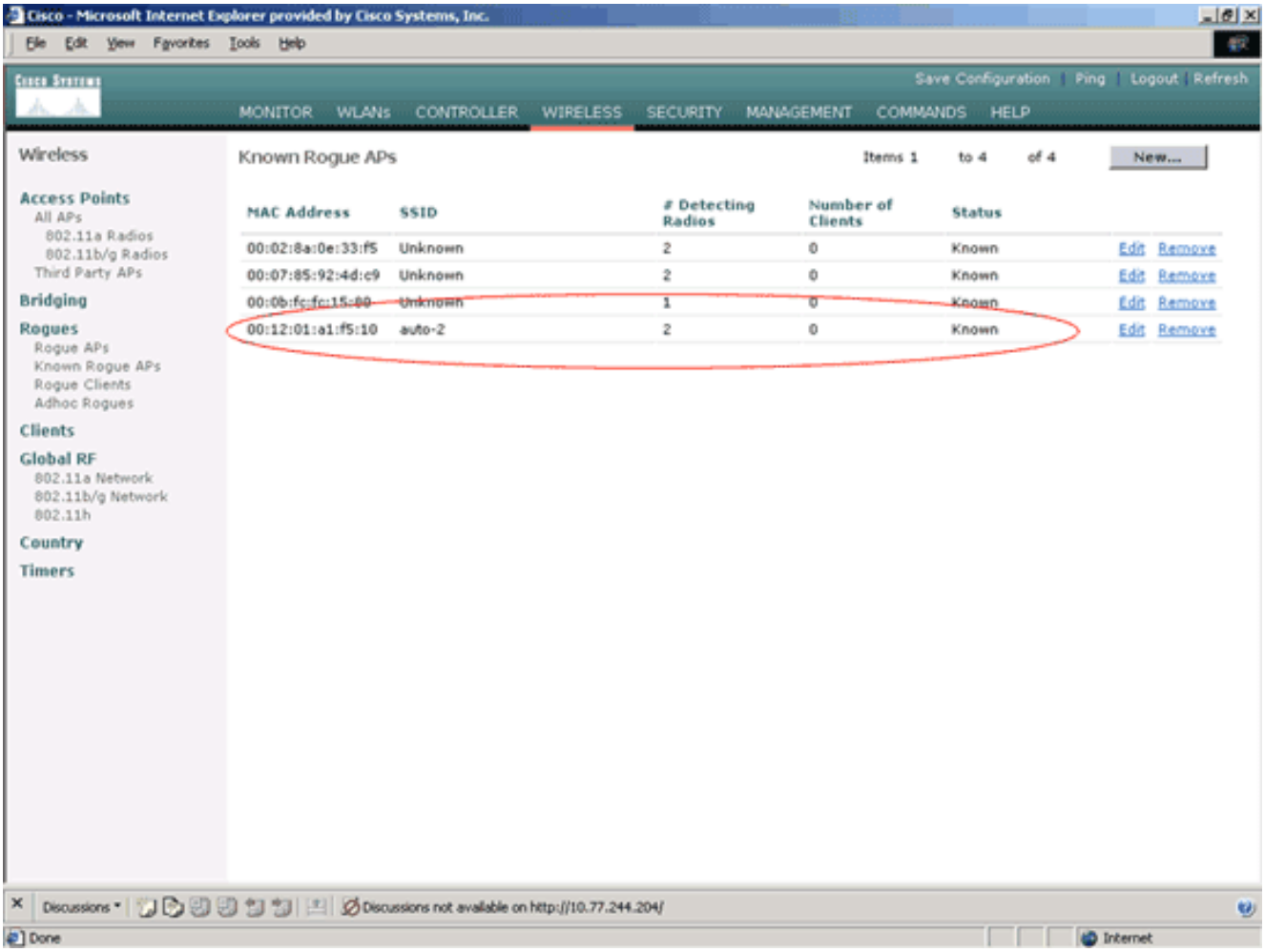
Verificar la configuración de AP de confianza

Complete estos pasos para verificar que el AP esté configurado correctamente como AP confiable desde la GUI del controlador:

1. Haga clic en **Wireless**.
2. En el menú ubicado en el lado izquierdo de la página Inalámbrico, haga clic en **AP rogue conocidos**.



El AP deseado debe aparecer en la página AP rogue conocidos con el estado enumerado como
Conocido.



Introducción a la configuración de la política AP de confianza

El WLC tiene estas políticas AP confiables:

- Política de cifrado aplicada
- Política de Preámbulo aplicada
- Política de tipos de radio aplicada
- Validar SSID
- Alerta si falta el AP confiable
- Tiempo de espera de vencimiento para las entradas AP de confianza (segundos)

Política de cifrado aplicada

Esta política se utiliza para definir el tipo de encriptación que el AP confiable debe utilizar. Puede configurar cualquiera de estos tipos de cifrado en Política de cifrado aplicada:

- Ninguno
- Abierto
- WEP
- WPA/802.11i

El WLC verifica si el tipo de encripción configurado en el AP confiable coincide con el tipo de encripción configurado en la configuración de "**Política de encripción forzada**". Si el AP confiable no utiliza el tipo de encripción designado, el WLC genera una alarma al sistema de administración para tomar las acciones apropiadas.

Política de Preámbulo aplicada

El preámbulo de radio (a veces llamado encabezado) es una sección de datos en la cabeza de un paquete que contiene información que los dispositivos inalámbricos necesitan cuando envían y reciben paquetes. **Los** preámbulos **cortos** mejoran el rendimiento, por lo que están habilitados de forma predeterminada. Sin embargo, algunos dispositivos inalámbricos, como los teléfonos SpectraLink NetLink, requieren preámbulos **largos**. Puede configurar cualquiera de estas opciones de preámbulo en la política de preámbulo implementada:

- Ninguno
- Breve
- Largo

El WLC verifica si el tipo Preamble configurado en el AP confiable coincide con el tipo de preámbulo configurado en la configuración de "**Política de preámbulo forzada**". Si el AP confiable no utiliza el tipo de preámbulo especificado, el WLC genera una alarma al sistema de administración para tomar las acciones apropiadas.

Política de tipos de radio aplicada

Esta política se utiliza para definir el tipo de radio que debe utilizar el AP de confianza. Puede configurar cualquiera de estos tipos de radio en Política de tipo de radio aplicada:

- Ninguno
- Solo 802.11b
- Solo 802.11a
- Solo 802.11b/g

El WLC verifica si el tipo de radio configurado en el AP confiable coincide con el tipo de radio configurado en la configuración "**Política de tipo de radio aplicada**". Si el AP de confianza no utiliza las radios especificadas, el WLC emite una alarma al sistema de administración para tomar las acciones apropiadas.

Validar SSID

Puede configurar el controlador para validar un SSID de APs de confianza contra los SSID configurados en el controlador. Si el SSID de APs confiable coincide con uno de los SSID del controlador, el controlador genera una alarma.

Alerta si falta el AP de confianza

Si se habilita esta política, el WLC alerta al sistema de administración si el AP confiable falta de la lista de AP rogue conocidos.

Tiempo de espera de vencimiento para las entradas AP de confianza (segundos)

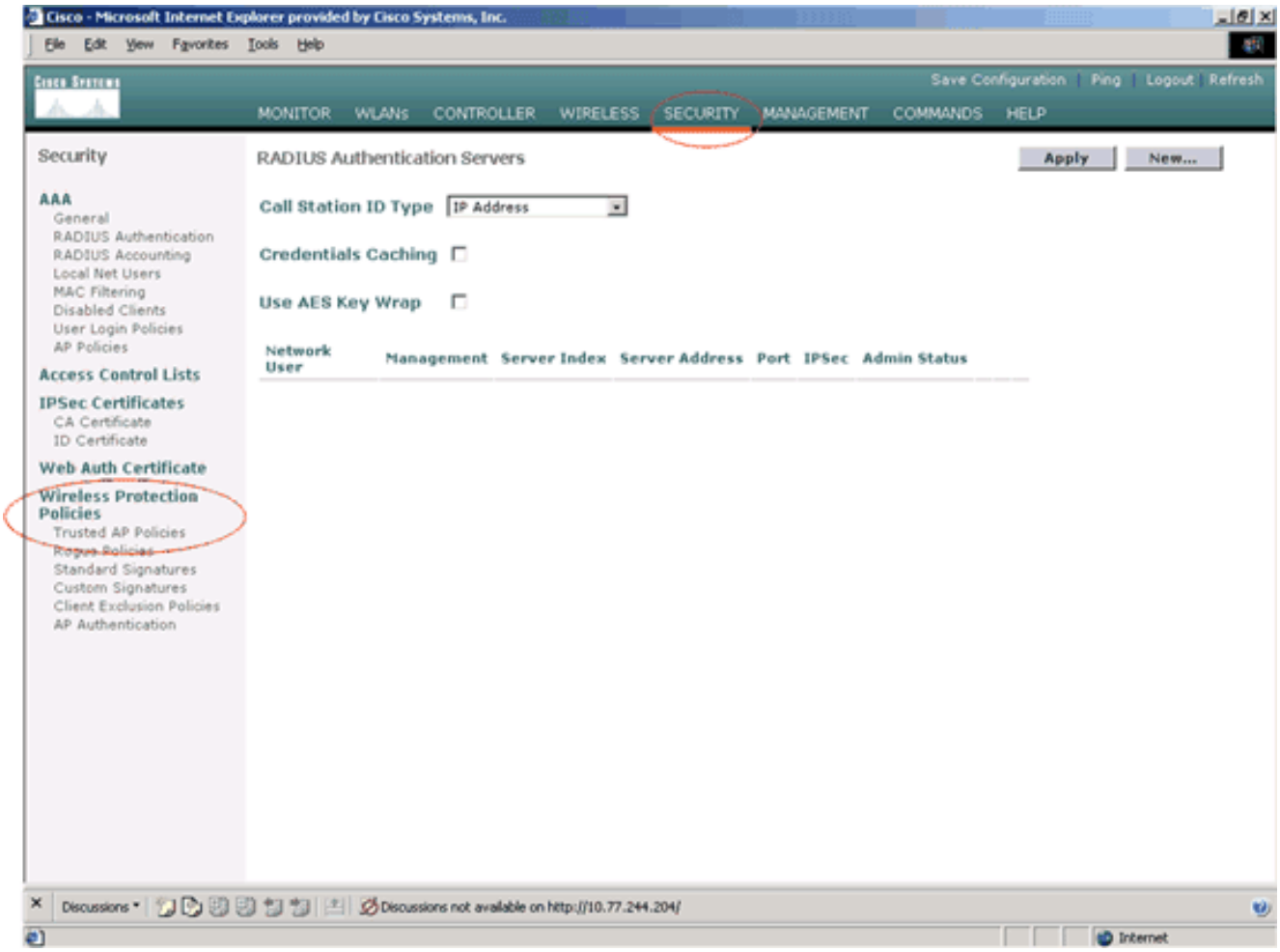
Este valor de tiempo de espera de vencimiento especifica el número de segundos antes de que el AP confiable se considere expirado y vaciado de la entrada del WLC. Puede especificar este valor de tiempo de espera en segundos (120 - 3600 segundos).

¿Cómo Configurar las Políticas AP de Confianza en el WLC?

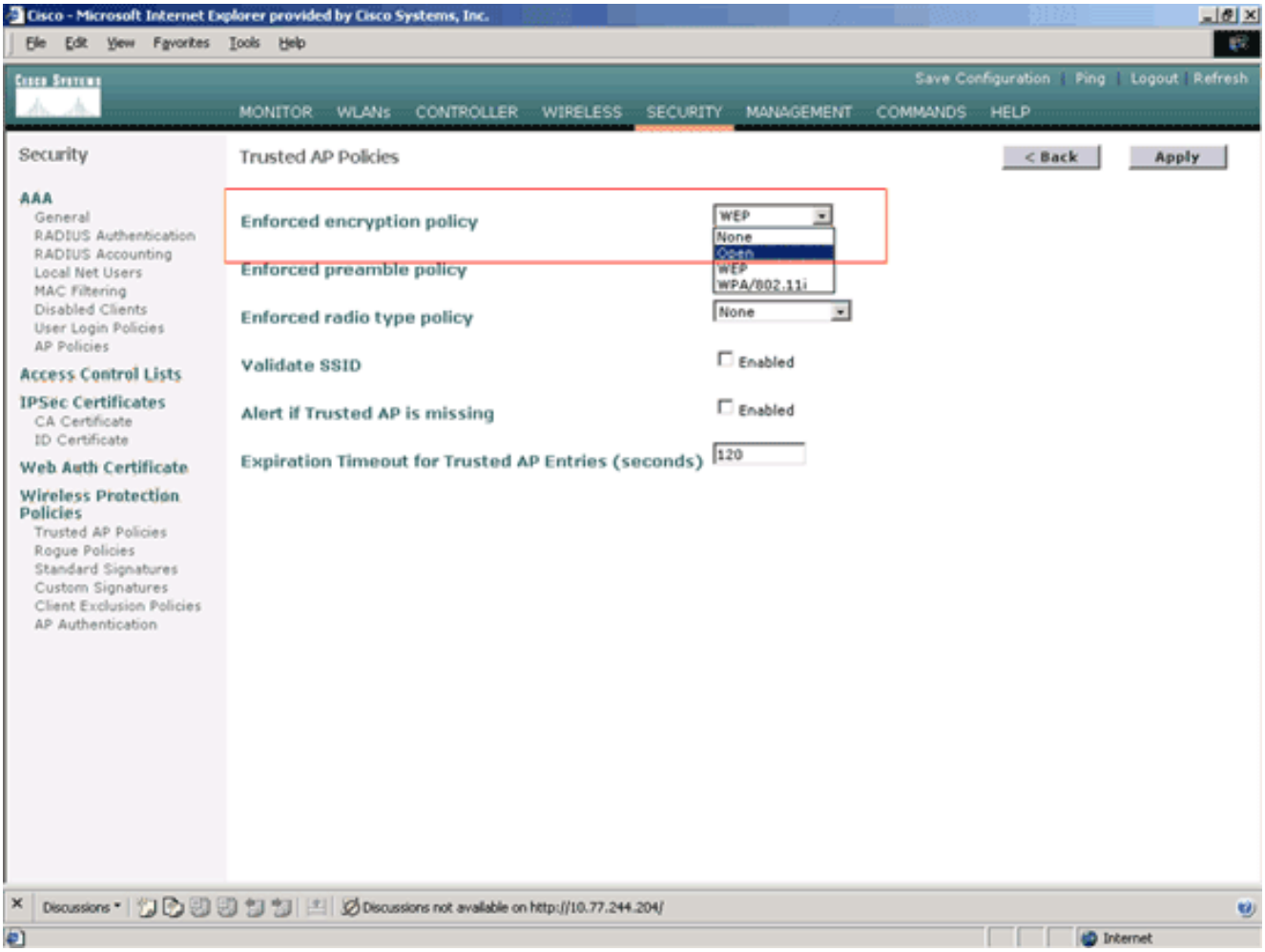
Complete estos pasos para configurar las políticas AP confiables en el WLC a través de la GUI:

Nota: Todas las políticas AP confiables residen en la misma página WLC.

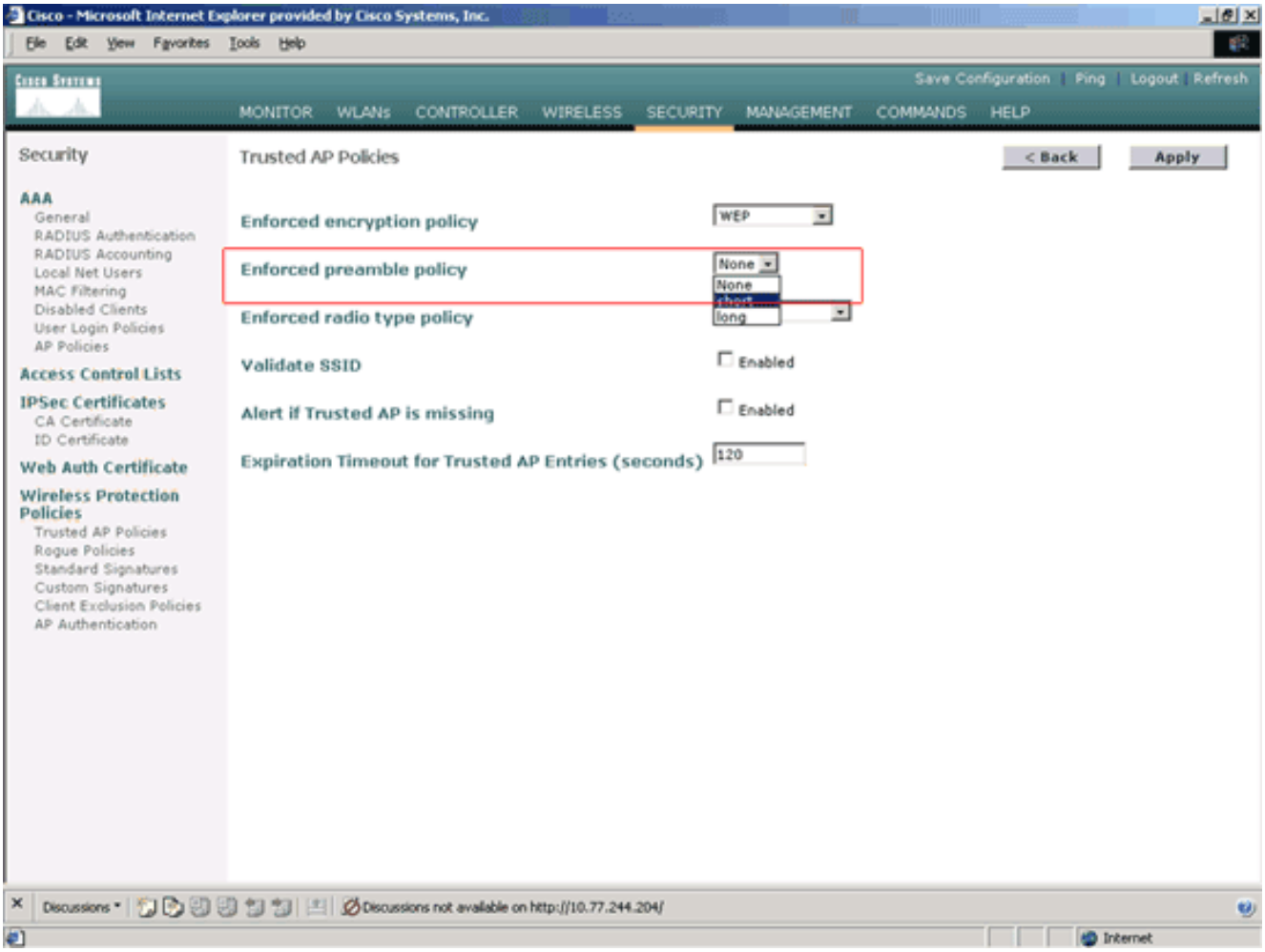
1. Desde el menú principal de la GUI del WLC, haga clic en **Seguridad**.
2. En el menú ubicado en el lado izquierdo de la página Seguridad, haga clic en **Trusted AP policies** enumeradas en el encabezado Wireless Protection Policies
   .



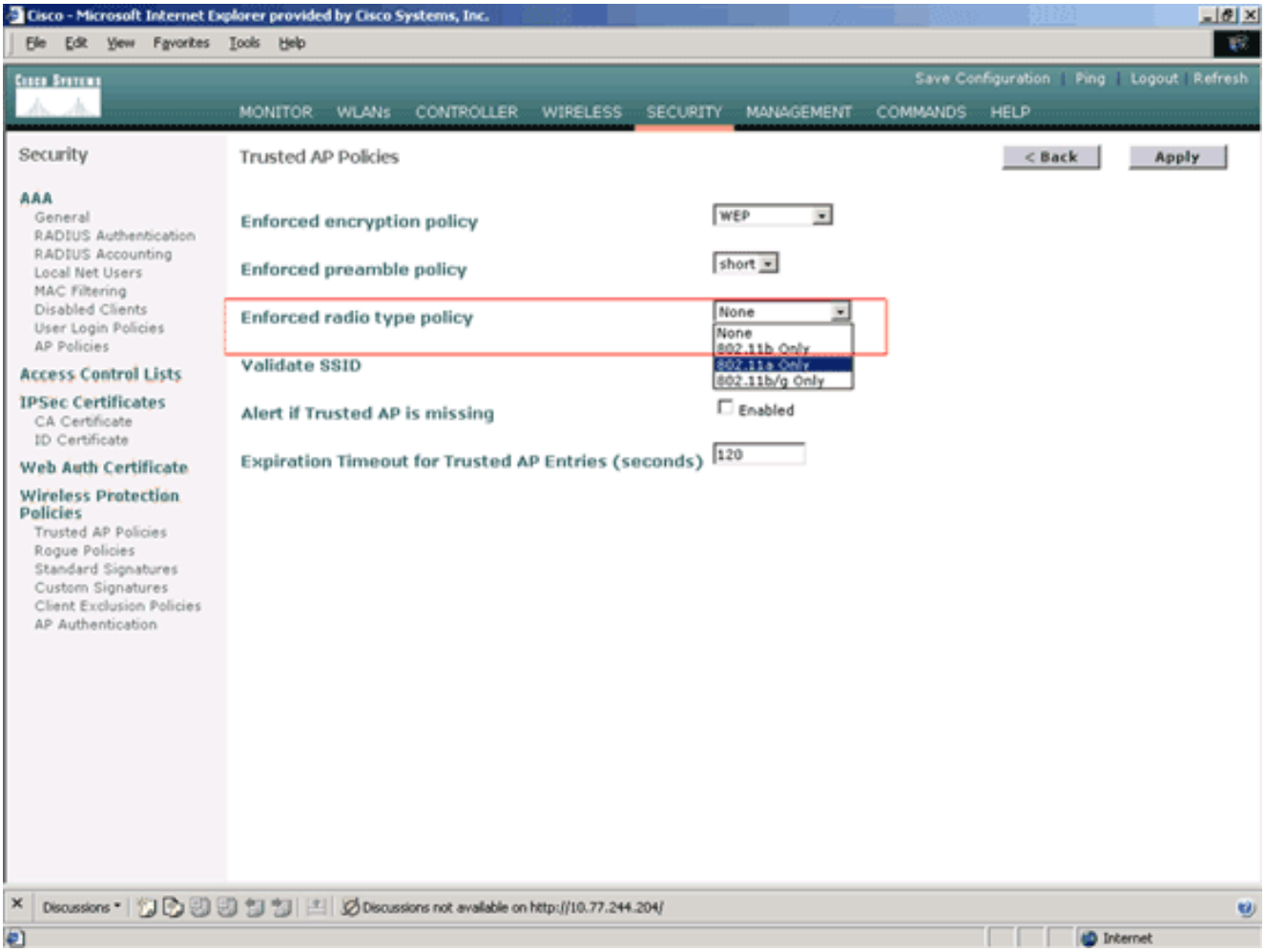
3. En la página Trusted AP policies (Políticas de punto de acceso de confianza), seleccione el tipo de encriptación deseado (Ninguno, Abrir, WEP, WPA/802.11i) en la lista desplegable Enforce Encryption Policy (Política de cifrado
   aplicada).



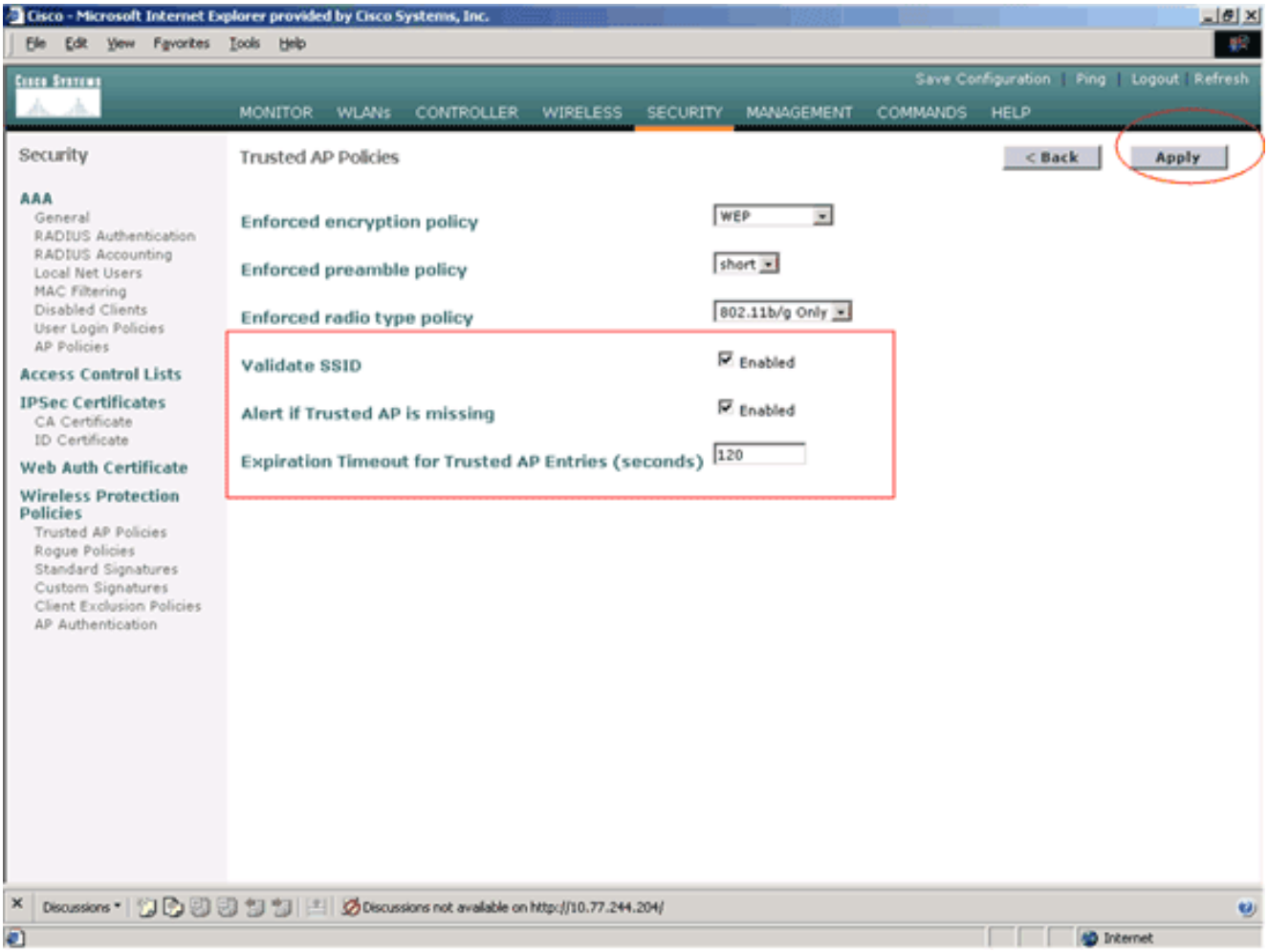
4. Seleccione el tipo de preámbulo deseado (Ninguno, Corto, Largo) en la lista desplegable Política de tipos de preámbulo
aplicada.



5. Seleccione el tipo de radio deseado (Ninguno, sólo 802.11b, sólo 802.11a, sólo 802.11b/g) en la lista desplegable Política de tipo de radio aplicada.



6. Marque o desmarque la casilla de verificación **Validar SSID habilitado** para habilitar o inhabilitar la configuración Validar SSID.
7. Marque o desmarque la casilla de verificación **Alerta si falta el AP confiable habilitado** para habilitar o inhabilitar la Alerta si falta el AP confiable.
8. Introduzca un valor (en segundos) para la opción **Expiration Timeout for Trusted AP entries**.



9. Haga clic en Apply (Aplicar).

Nota: Para configurar estos parámetros desde la CLI del WLC, puede utilizar el **comando config wps trust-ap** con la opción de política apropiada.

```
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.
```

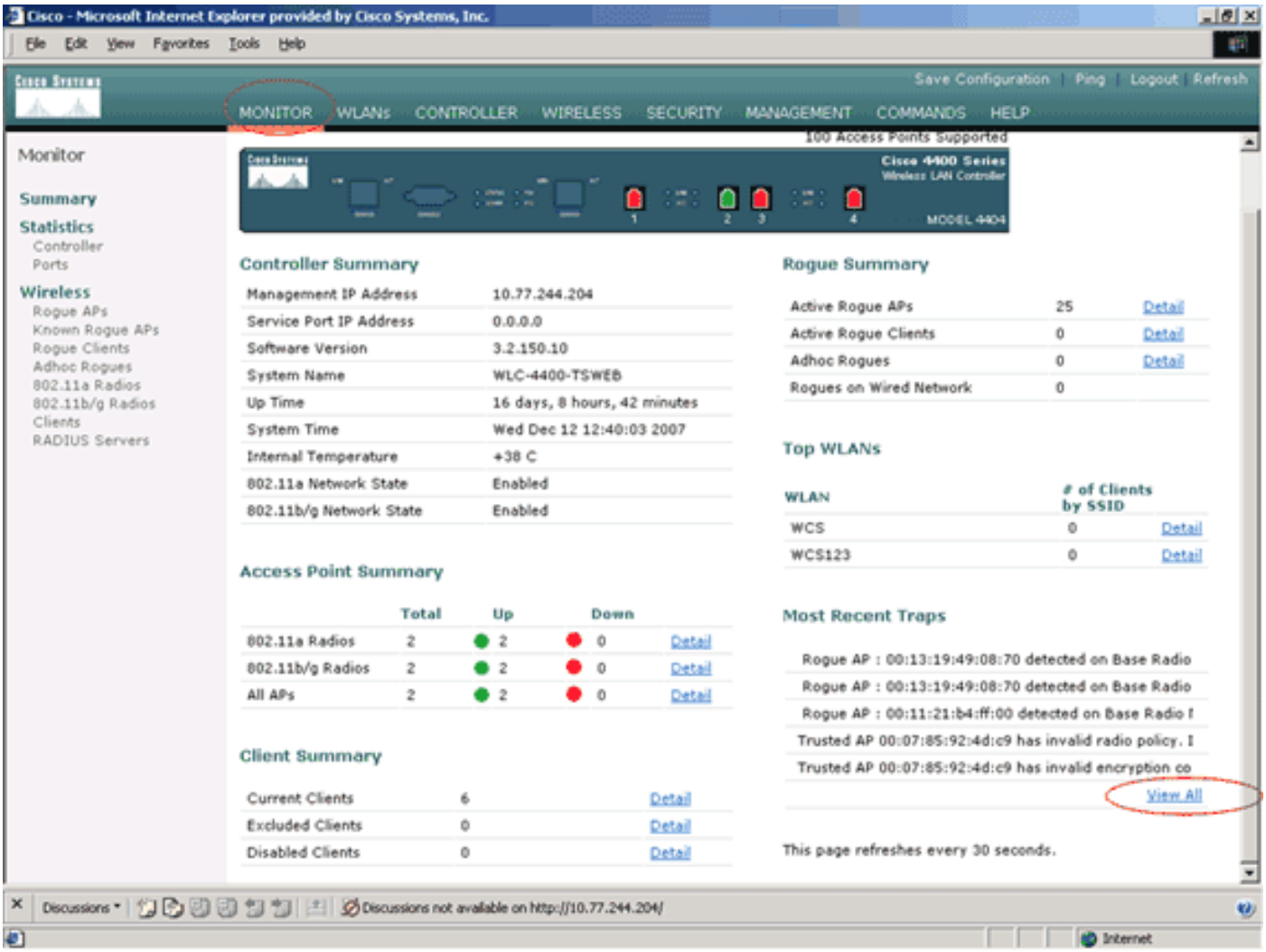
Mensaje de alerta de violación de política AP de confianza

Este es un ejemplo del mensaje de alerta de violación de política AP confiable que muestra el controlador.

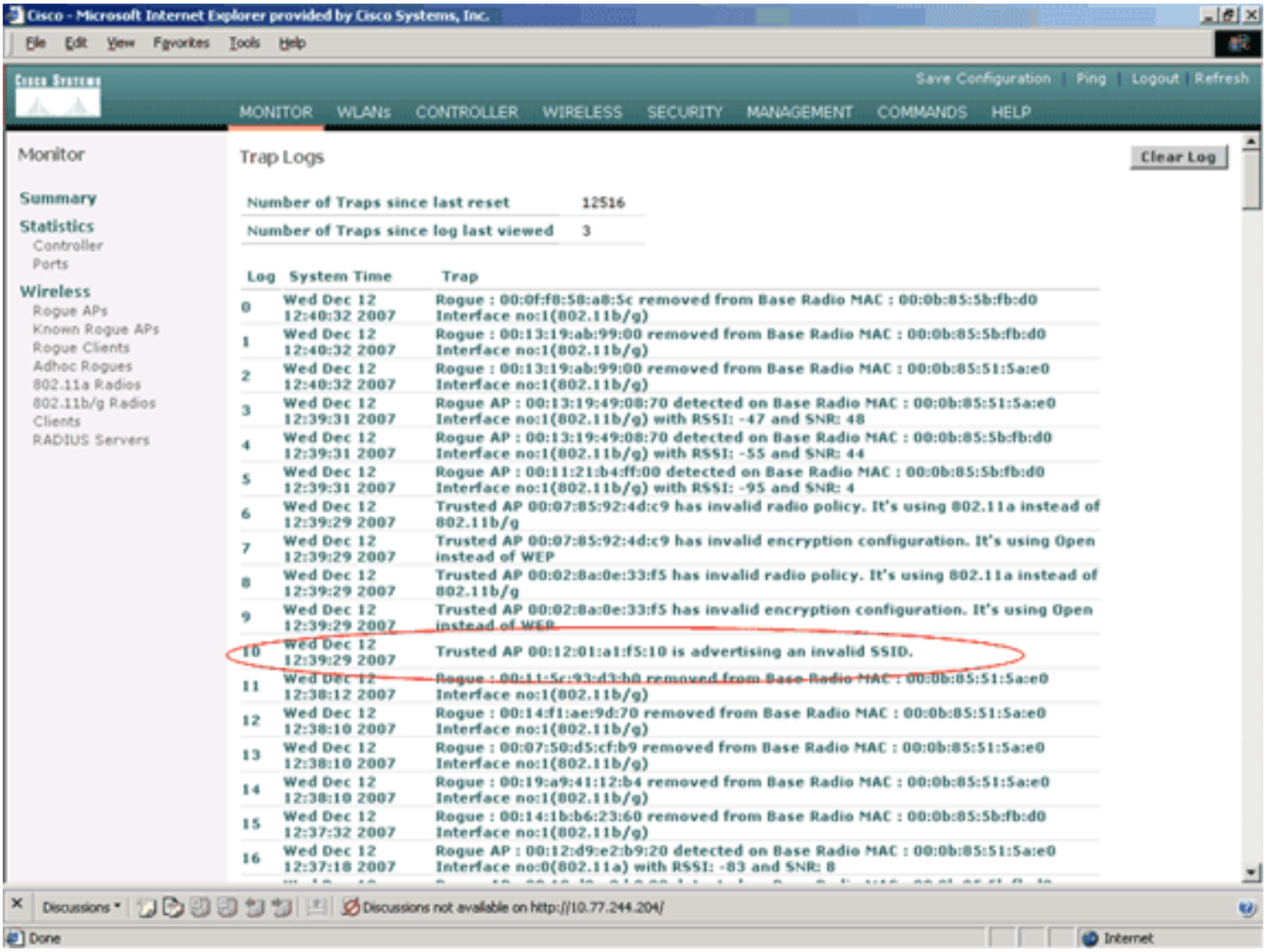
```
Thu Nov 16 12:39:12 2006  [WARNING] apf_rogue.c 1905: Possible AP
impersonation of xx:xx:xx:xx:xx:xx, using source address of
00:16:35:9e:6f:3a, detected by 00:17:df:7d:e1:70 on slot 0
 Thu Nov 16 12:39:12 2006  [SECURITY] apf_rogue.c 1490: Trusted AP Policy
failed for AP xx:xx:xx:xx:xx:xx - invalid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

Observe los mensajes de error resaltados aquí. Estos mensajes de error indican que el SSID y el tipo de encripción configurados en el AP de confianza no coinciden con la configuración de la política AP de confianza.

Se puede ver el mismo mensaje de alerta desde la GUI del WLC. Para ver este mensaje, vaya al menú principal de la GUI del WLC y haga clic en **Monitor**. En la sección Trampas más recientes de la página Monitor, haga clic en **Ver todo** para ver todas las alertas recientes en el WLC.



En la página Trampas más recientes, puede identificar el controlador que genera el mensaje de alerta de violación de la política AP confiable como se muestra en esta imagen:



Información Relacionada

- Guía de Configuración del Controlador de LAN Inalámbrica de Cisco, Versión 5.2 - Habilitación de la Detección del Punto de Acceso de Ruteo en Grupos de RF
- Guía de Configuración del Controlador de LAN Inalámbrica de Cisco, Versión 4.0 - Configuración de Soluciones de Seguridad
- Detección no autorizada en redes inalámbricas unificadas
- Guía de diseño e implementación del teléfono SpectraLink
- Ejemplo de Configuración de Conexión LAN de Elementos Básicos de Red Inalámbrica
- Resolución de problemas de conectividad en una red inalámbrica de LAN
- Ejemplos de configuración de autenticación de controladores para redes LAN inalámbricas
- Soporte Técnico y Documentación - Cisco Systems