Configuración del filtrado de contenido web mediante Cisco Umbrella en WAP571 o WAP571E

Objetivo

El objetivo de este artículo es mostrarle cómo configurar el filtrado de contenido web usando Cisco Umbrella en un WAP571 o WAP571E.

Introducción

Ha trabajado duro para poner en marcha su red. Por supuesto, uno quiere que siga así, pero los hackers son implacables. ¿Qué se puede hacer para mantener la seguridad de su red? Una solución es configurar el filtrado de contenido web. La función de filtrado de contenido web permite proporcionar acceso controlado a Internet mediante la configuración de políticas y filtros. Ayuda a proteger la red bloqueando sitios web malintencionados o no deseados.

Cisco Umbrella es una plataforma de seguridad en la nube que proporciona la primera línea de defensa contra las amenazas en Internet. Actúa como un gateway entre Internet y sus sistemas y datos para bloquear malware, botnets y phishing en cualquier puerto, protocolo o aplicación.

Mediante una cuenta Cisco Umbrella, la integración interceptará de forma transparente (informes a nivel de URL) las consultas del Sistema de nombres de dominio (DNS) y las redirigirá a Umbrella. El dispositivo aparecerá en el panel de Umbrella como un dispositivo de red para aplicar políticas y ver informes.

Para obtener más información sobre Cisco Umbrella, consulte los siguientes enlaces:

- Guía rápida de Cisco Umbrella
- Guía del usuario de Cisco Umbrella
- CÓMO: Ampliación de Cisco Umbrella para proteger su red inalámbrica

Dispositivos aplicables

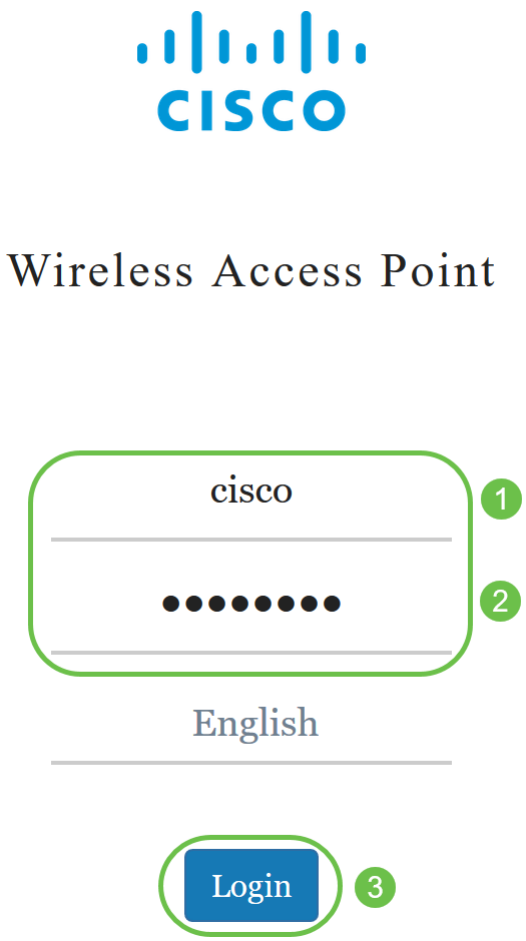
- WAP571
- WAP571E

Versión del software

- 1.1.0.3

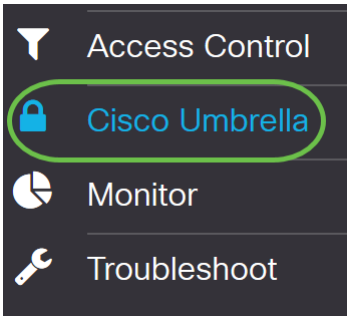
Configure Cisco Umbrella en su WAP

Paso 1. Inicie sesión en la utilidad de configuración web del WAP ingresando el nombre de usuario y la contraseña. El nombre de usuario y la contraseña predeterminados son *cisco/cisco.* Si ha configurado un nuevo nombre de usuario o contraseña, introduzca esas credenciales en su lugar. Haga clic en Login (Conexión).

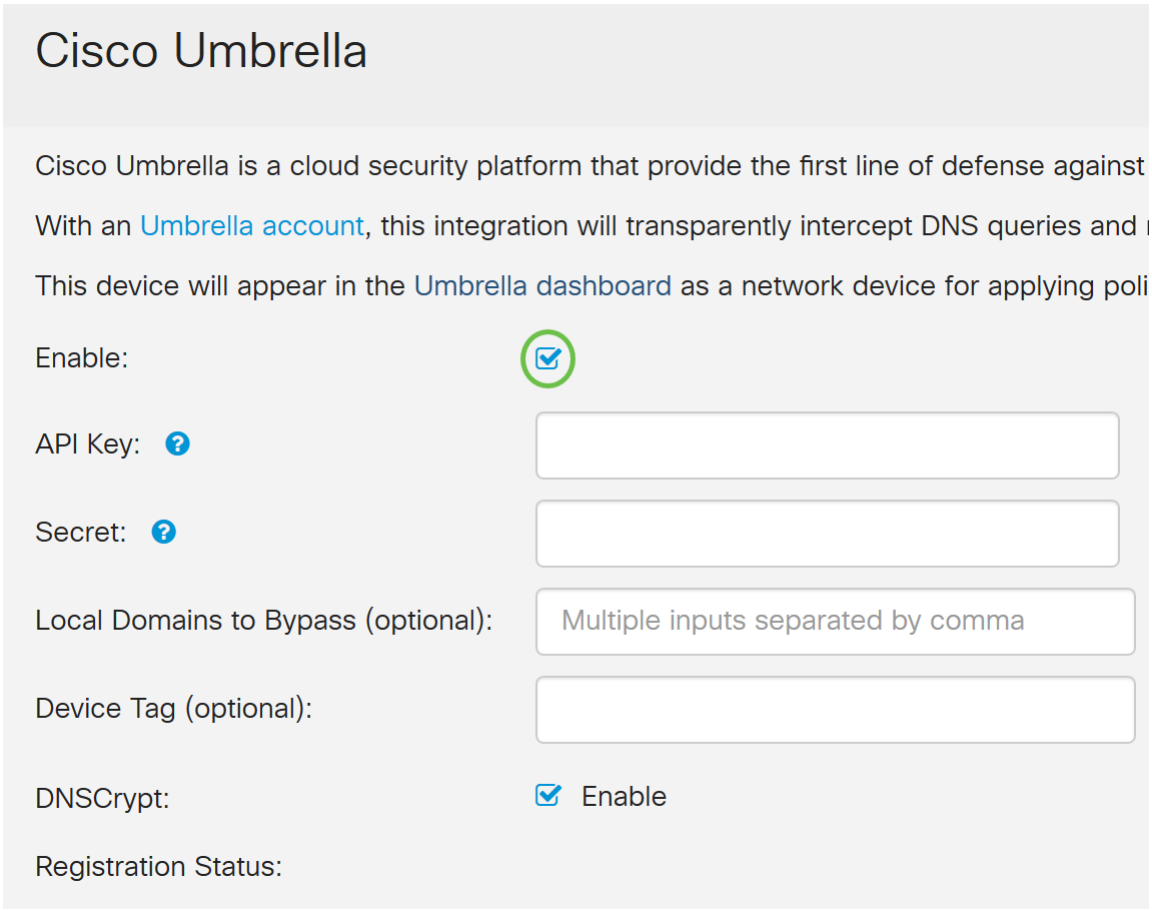


Nota: En este artículo, el WAP571E se utiliza para demostrar la configuración de Cisco Umbrella. Las opciones de menú pueden variar ligeramente según el modelo del dispositivo.

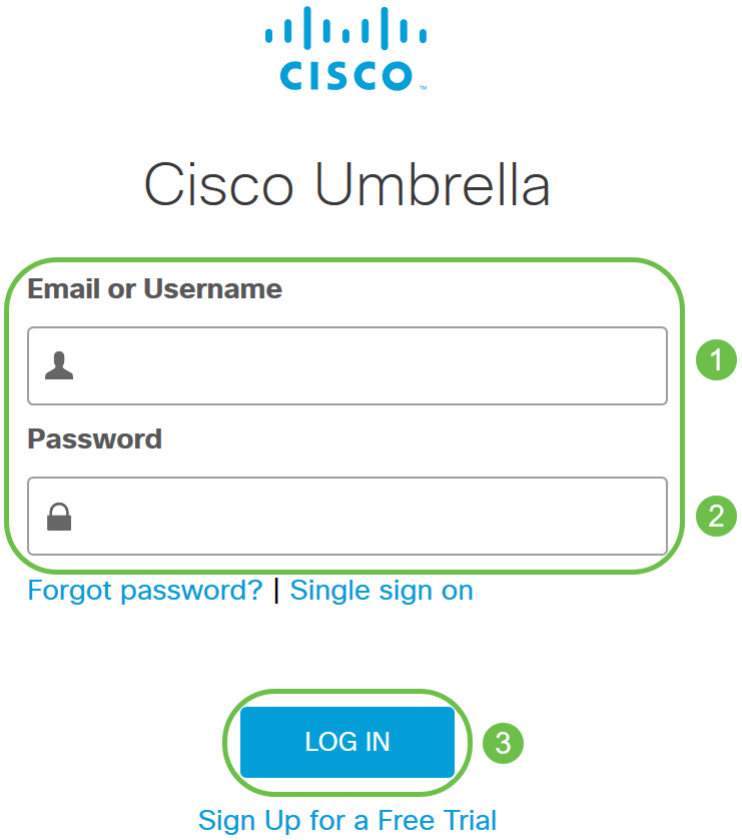
Paso 2. Elija **Cisco Umbrella**.



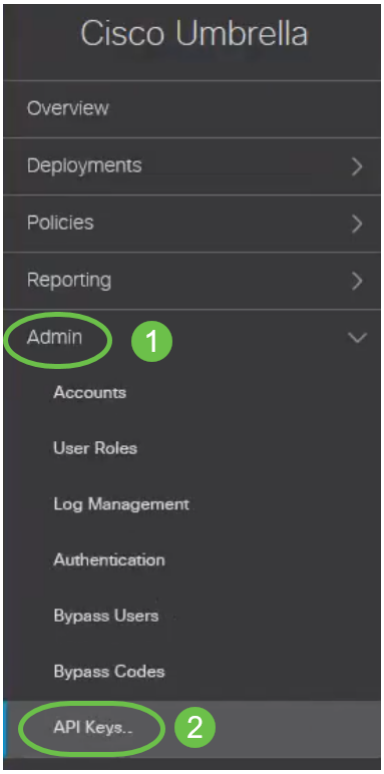
Paso 3. *Active* Cisco Umbrella haciendo clic en la casilla de verificación.



Paso 4. Para obtener la clave de la API y el *secreto*, inicie sesión en su cuenta de Cisco Umbrella usando el correo electrónico o el nombre de usuario y la contraseña. Haga clic en **INICIAR SESIÓN**.



Paso 5. Navegue hasta **Admin** y solicite una clave API eligiendo **API Keys...**en el menú.

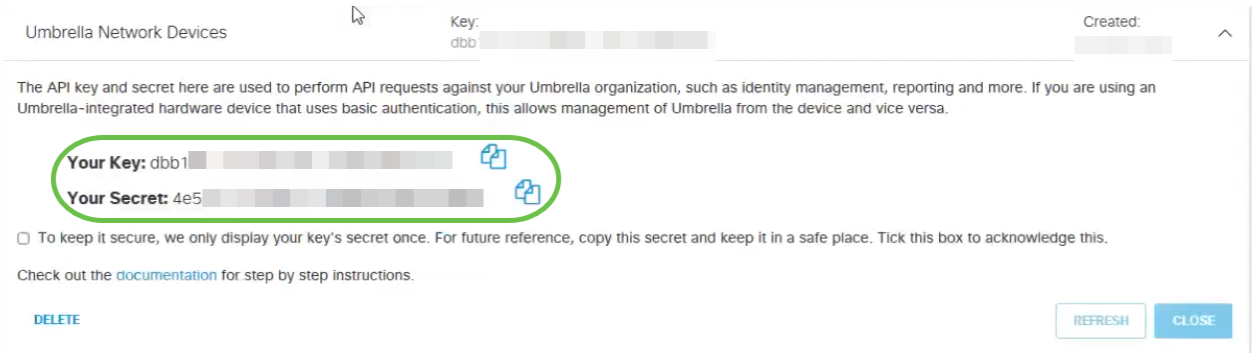


Nota: La primera vez que solicite una clave API, sólo se mostrará la clave como se muestra a continuación.

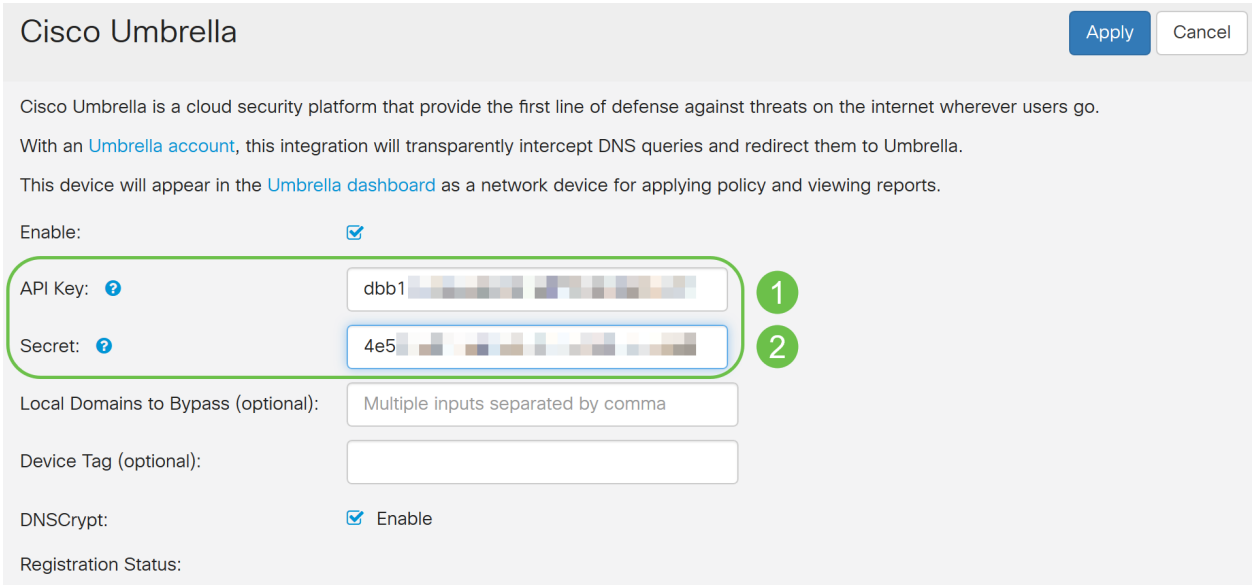
Paso 6. Haga clic en **Actualizar** para obtener la clave API y la clave Secreta.

Nota: Al hacer clic en *Actualizar*, la clave de la API cambiará.

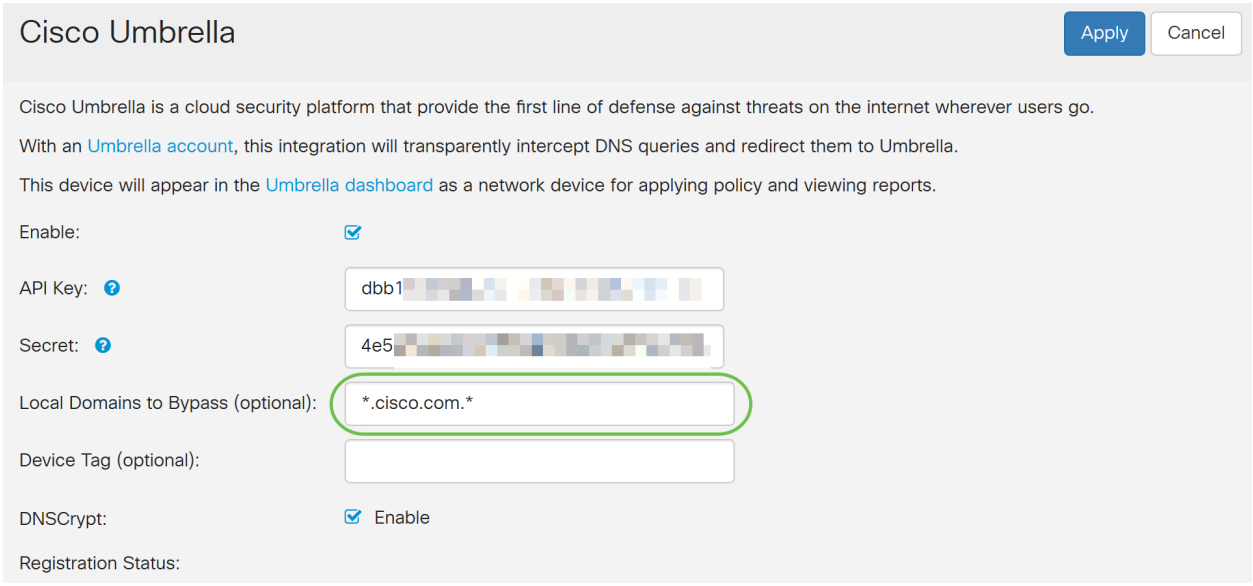
Paso 7. Copie la *clave* y *secreto* que se genera.



Paso 8. Pegue la *clave* y *secreto* copiados del paso 7 en los campos proporcionados bajo la configuración de *Cisco Umbrella* del WAP.



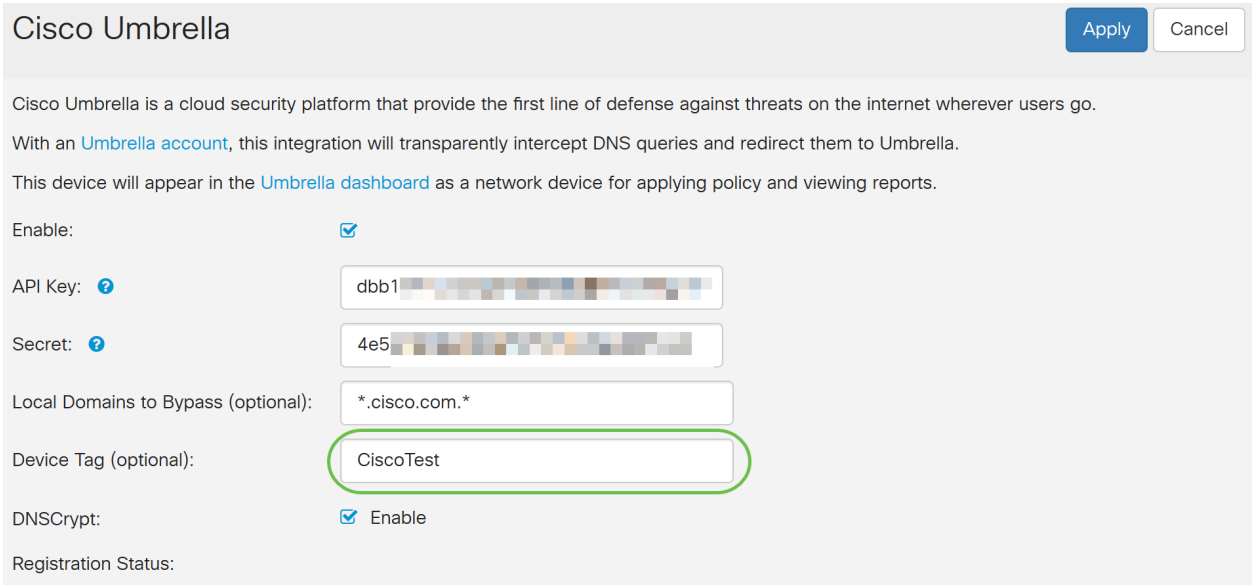
Paso 9. (Opcional) Introduzca el nombre de dominio en el campo **Dominios locales para omitir (opcional)** y los paquetes alcanzarán el destino sin pasar por Cisco Umbrella. Los elementos de la lista deben estar separados por una coma, mientras que los dominios pueden incluir caracteres comodín en forma de asterisco (*). Por ejemplo: *.cisco.com.*.



Nota: Esto es necesario para todos los dominios de Intranet y dominios DNS divididos donde existen servidores separados para redes internas y externas.

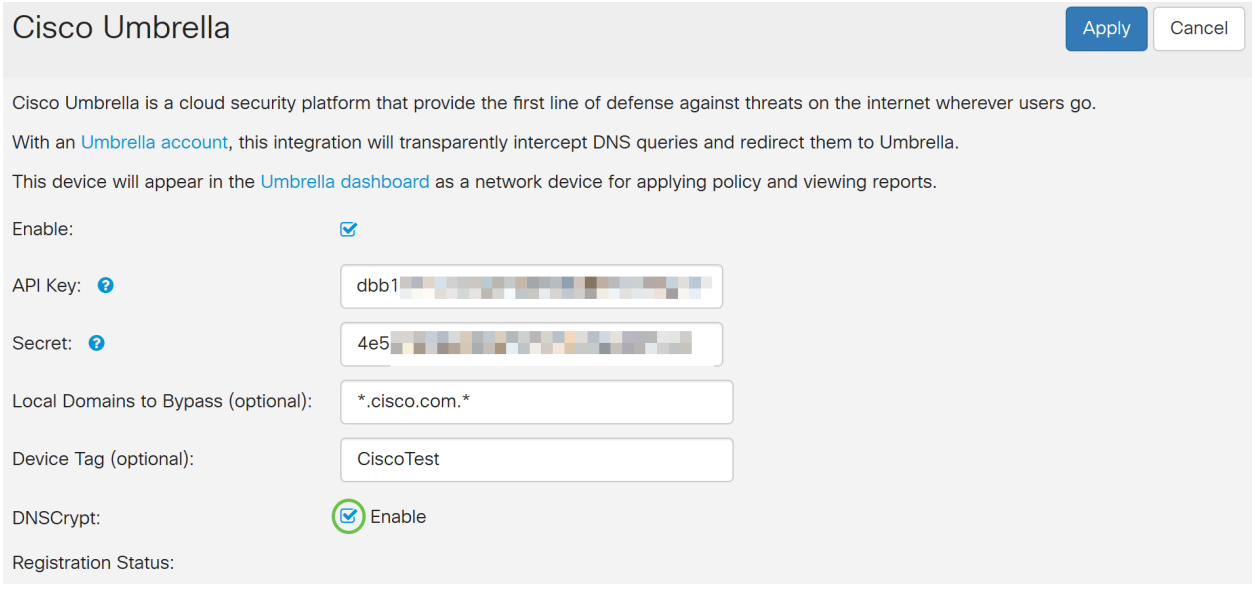
Paso 10. (Opcional) Introduzca un nombre de etiqueta en el campo **Device Tag (etiqueta de**

dispositivo) (opcional) para etiquetar el dispositivo. *Device Tag* describe el dispositivo o un origen particular asignado al dispositivo. Asegúrese de que es exclusivo para su organización.

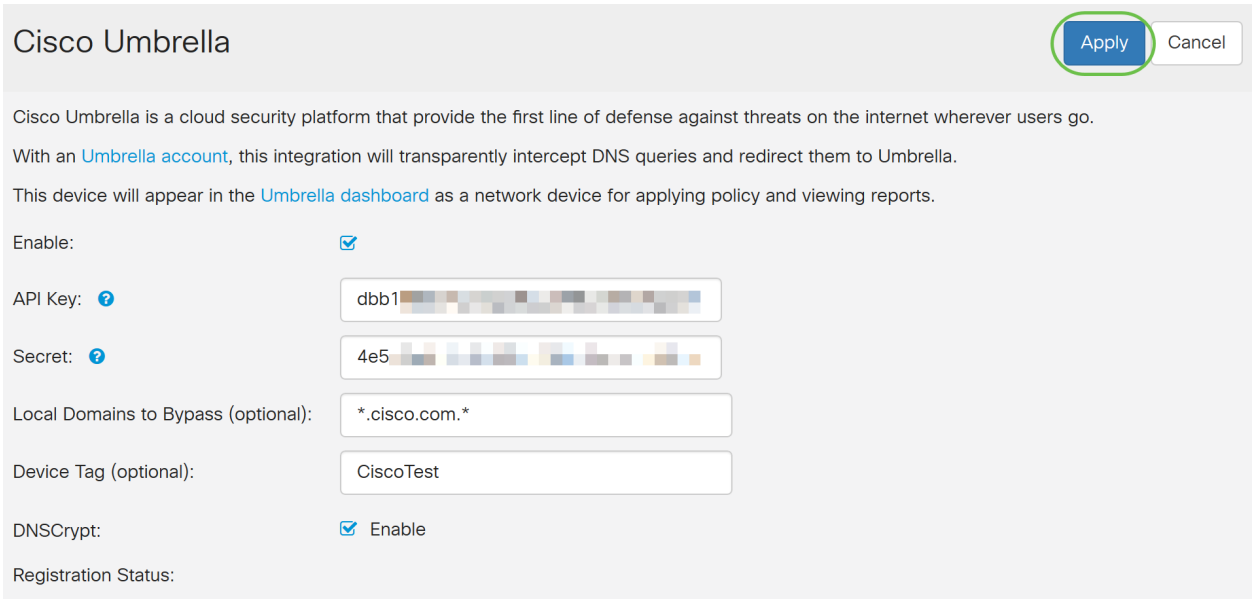


Nota: Cualquier cambio en *Secret*, *API Key* y la *Device Tag* activará el reregistro para crear un dispositivo de red.

Paso 11. **DNSCrypt** se utiliza para proteger (a través del cifrado) la comunicación DNS entre un cliente DNS y una resolución DNS. Previene varios tipos de ataques DNS y snooping. Está habilitado de forma predeterminada.

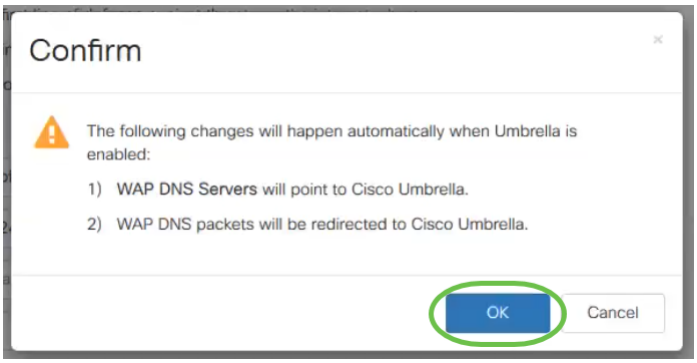


Paso 12. Haga clic en **Aplicar** para aplicar estas configuraciones.



Nota: El estado del registro se indica en el campo *Registration Status* . El estado puede ser *Satisfactorio*, *Registro* o *Error*.

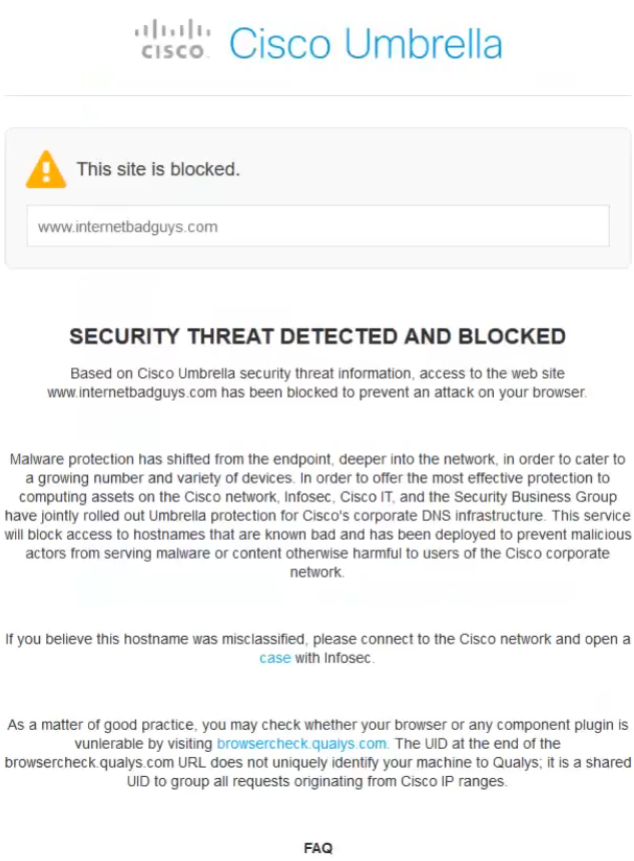
Paso 13. Aparecerá una pantalla emergente como se muestra a continuación. Haga clic en **Aceptar** para confirmar.



Verificación

Hay una manera divertida de verificar si el filtrado de sitios web está habilitado. Solo tiene que abrir un navegador web e introducir la siguiente url: www.internetbadguys.com. No se preocupe, se trata de un sitio propiedad de Cisco con fines de prueba y verificación.

Dado que el filtrado de sitios web está habilitado en WAP a través de Cisco Umbrella, recibirá la siguiente notificación. La red inalámbrica redirigirá la consulta DNS a Cisco Umbrella. A su vez, Cisco Umbrella actúa como servidor DNS, protegiendo la red y sus usuarios.



Conclusión

Ahora ha configurado y activado el filtrado de sitios web en un punto de acceso WAP571 o WAP571E mediante Cisco Umbrella.

¿Desea obtener más información? Vea estos vídeos relacionados con Cisco Umbrella:

Charla técnica de Cisco: Protección de una red empresarial mediante el uso de puntos de acceso de Cisco Small Business y Umbrella

Charla técnica de Cisco: Cómo obtener una cuenta de paraguas

Charla técnica de Cisco: Configuración de una Política de Paraguas