CÓMO: Recuperación de una clave secreta del paraguas perdida

Objetivo

Si alguna vez perdiste una llave irrecuperable, sabes lo rápido que la sangre puede empezar a bombear a través de tu cuerpo. En este artículo se explica cómo recuperarse de la pérdida de la clave secreta de la interfaz de programación de aplicaciones (API). Esta clave secreta sólo se muestra una vez cuando se genera y no se vuelve a mostrar. Si desplaza el explorador lejos de la pantalla de la clave de la API, puede perder esa información.

Dispositivos aplicables

- WAP125
- WAP581

Versión del software

- 1.0.1

Requirements

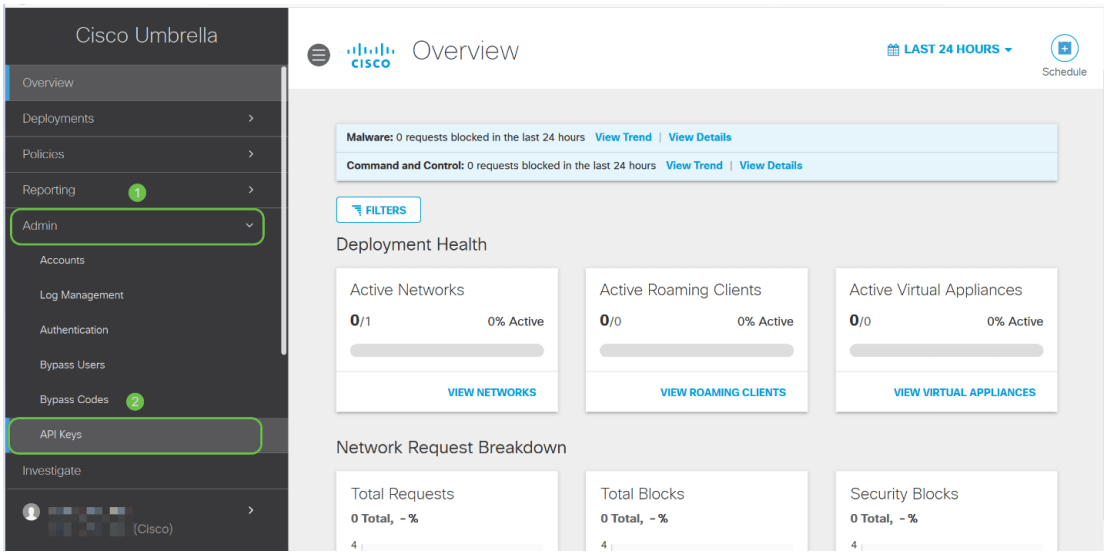
- Una cuenta de Umbrella activa (¿No tiene una? Solicitar un presupuesto o iniciar una prueba gratuita)

¡Ayuda, he perdido mi clave secreta!

Aquí están las noticias difíciles, su clave secreta, se perdió en la red éter, se fue. Donde esto se convierte en una mejor noticia, es que el proceso de recuperación no es tan doloroso. Al generar una nueva clave API, se genera una nueva clave secreta. Por lo tanto, el proceso de recuperación implica eliminar la clave API asociada a la clave perdida y generar el nuevo conjunto de claves API.

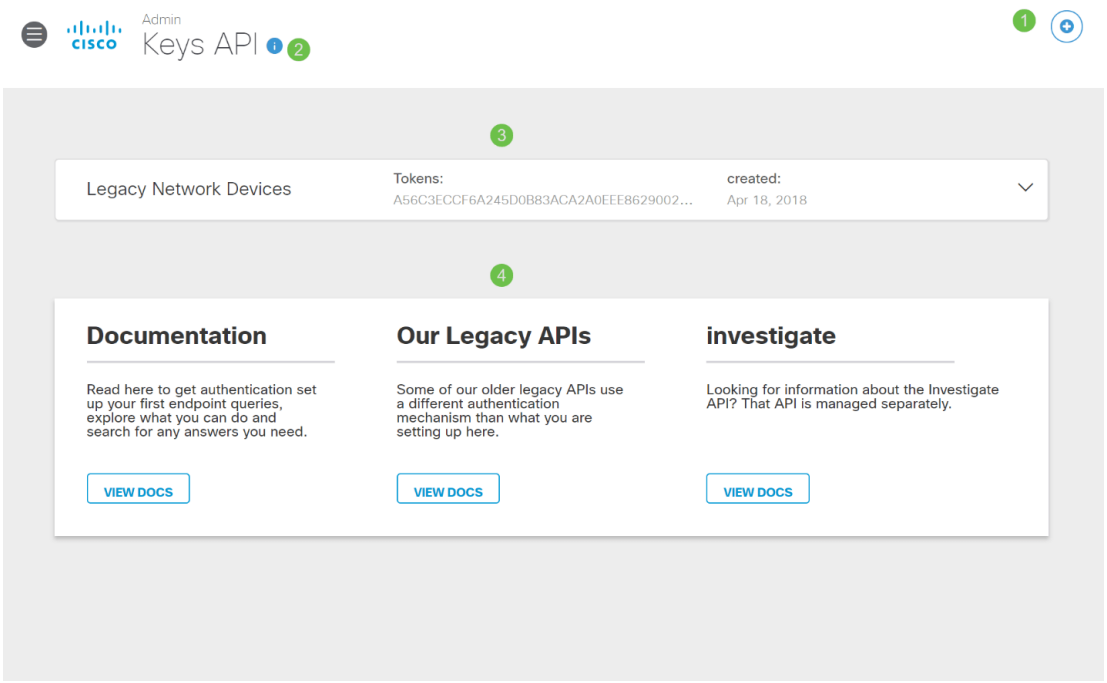
Cuando se desplaza por esta guía, comienza por la clave API y la clave secreta del panel de su cuenta principal. Después, iniciaremos sesión en su dispositivo WAP para agregar la API y la clave secreta. Si tiene algún problema, consulte aquí la documentación y aquí las opciones de Soporte de Umbrella.

Paso 1. Después de iniciar sesión en su cuenta principal, desde la pantalla *Panel* haga clic en **Admin > API Keys**.

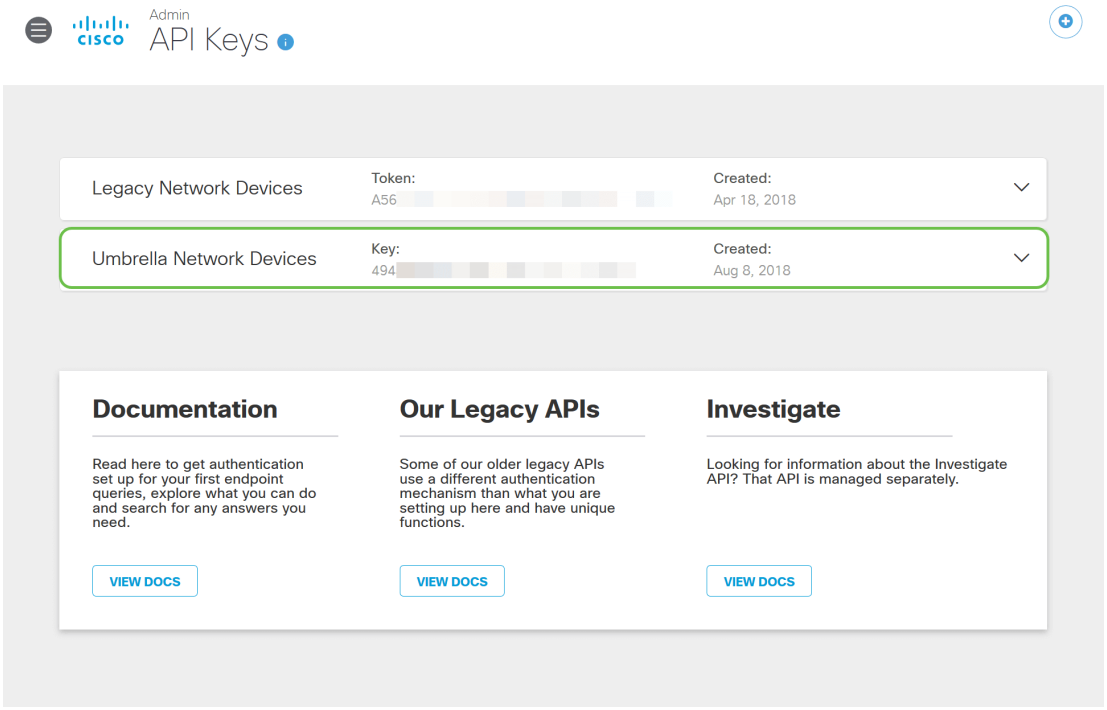


Anatomía de la pantalla API Keys (Claves de API):

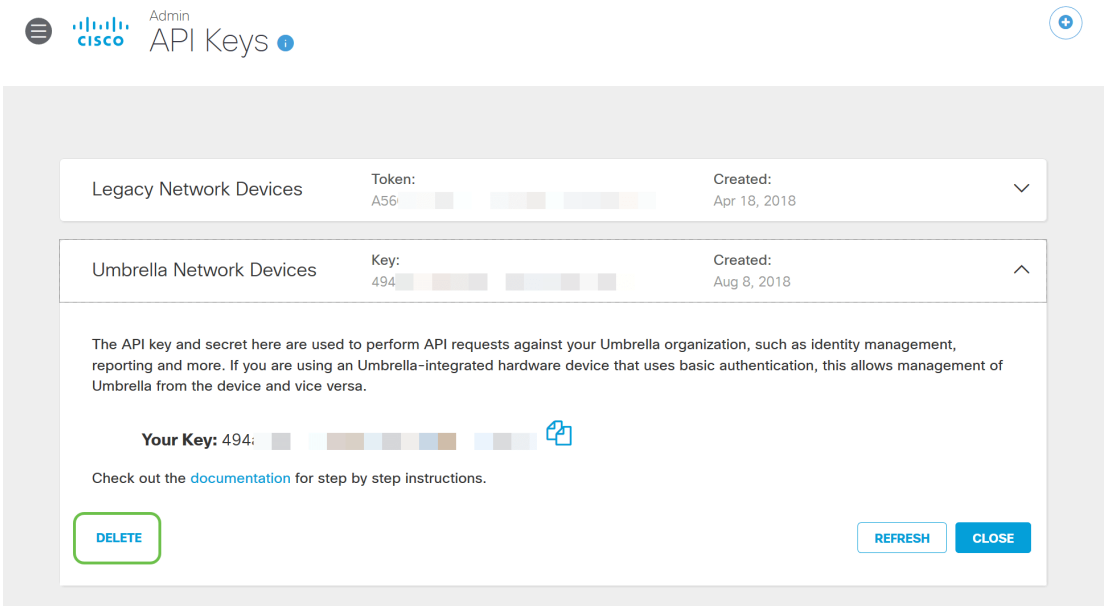
1. *Agregar clave API*: inicia la creación de una nueva clave para su uso con la API Umbrella.
2. *Información adicional*: se desliza hacia abajo/hacia arriba con un explicador para esta pantalla.
3. *Token Well*: contiene todas las claves y fichas creadas por esta cuenta. (Rellena una vez que se ha creado una clave)
4. *Documentos de soporte* - Enlaces a la documentación del sitio de Umbrella relativa a los temas de cada sección.



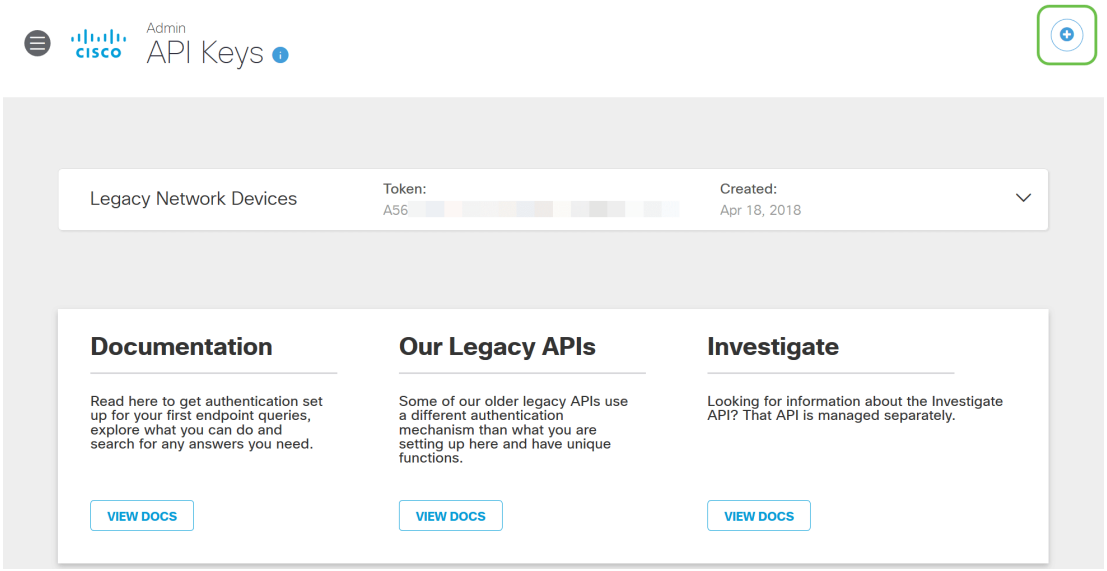
Paso 2. Haga clic en el botón **Umbrella Network Devices** en el *pozo Token*.



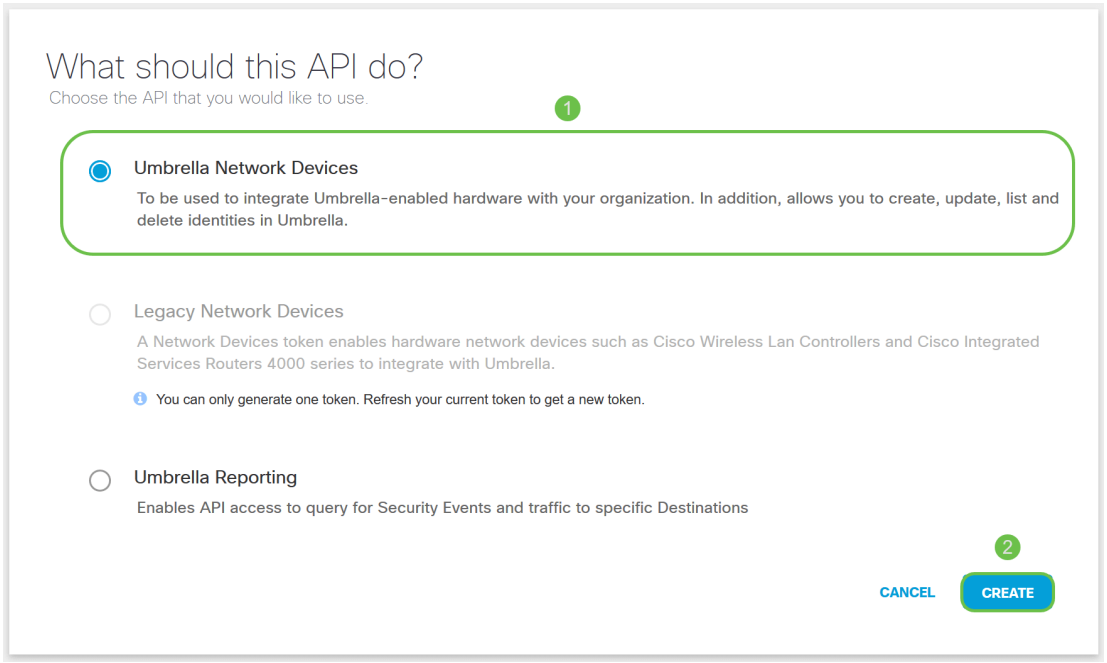
Paso 3. Seleccione **Umbrella Network Devices** y luego haga clic en el **botón Create**.



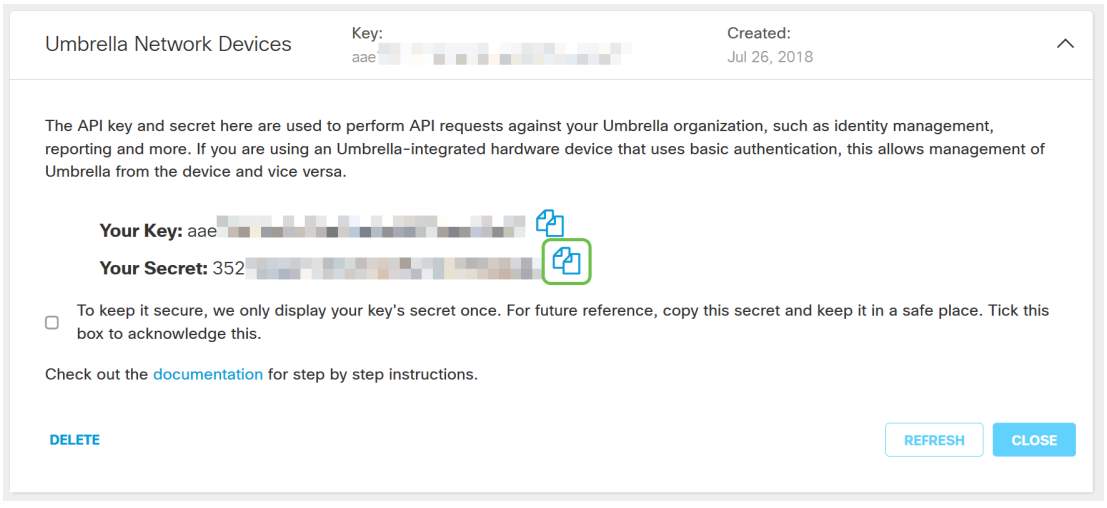
Paso 4. La clave se eliminará instantáneamente. Haga clic en el botón **Add API Key** en la esquina superior derecha o haga clic en el botón **Create API Key**. Ambos funcionan igual.



Paso 5. Seleccione **Umbrella Network Devices** y luego haga clic en el **botón Create**.

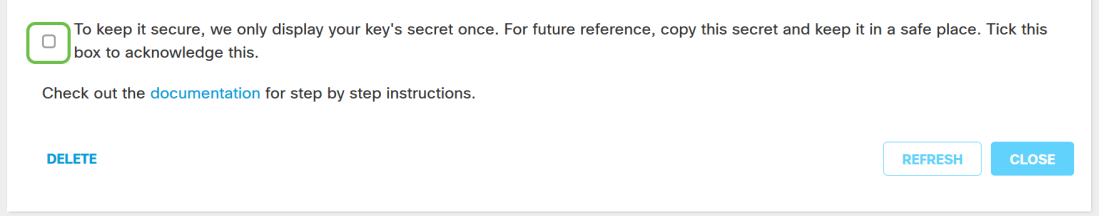


Paso 6. Haga clic en el botón **Copiar** situado a la derecha de la *clave secreta,* una notificación emergente confirmará que la clave se ha copiado en el portapapeles.

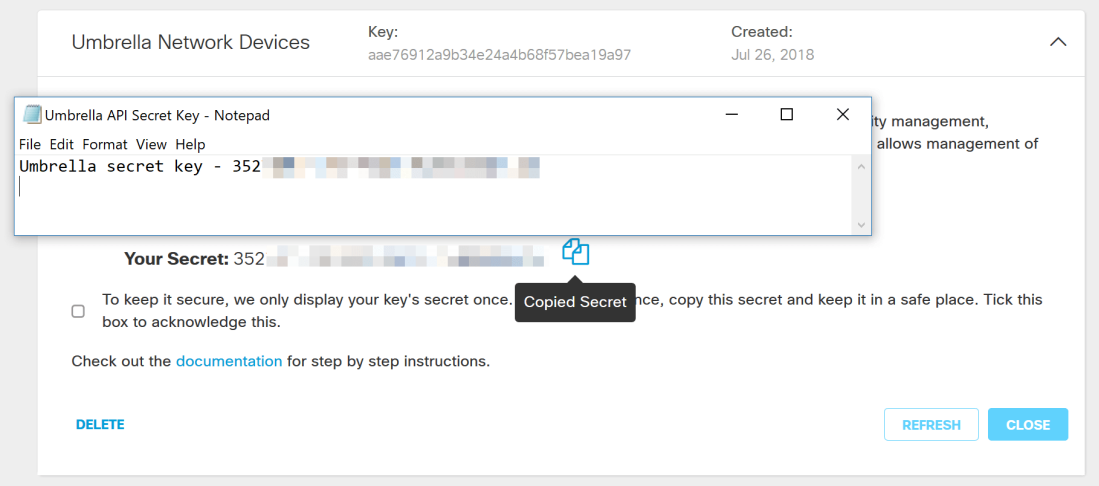


Después de copiar la clave y la clave secreta en una ubicación segura, haga clic en la ***casilla de***

verificación para confirmar que se ha completado el reconocimiento y, a continuación, haga clic en el **botón Cerrar**.



Paso 7. Abra un editor de texto como el bloc de notas y pegue su clave secreta y API en el documento, etiquételos para futuras referencias. En este caso, su etiqueta es "Clave secreta de paraguas". Incluya la clave API con su clave secreta junto con una breve descripción de su uso en este mismo archivo de texto. A continuación, guarde el archivo de texto en una ubicación segura a la que sea fácil acceder más adelante si lo necesita.



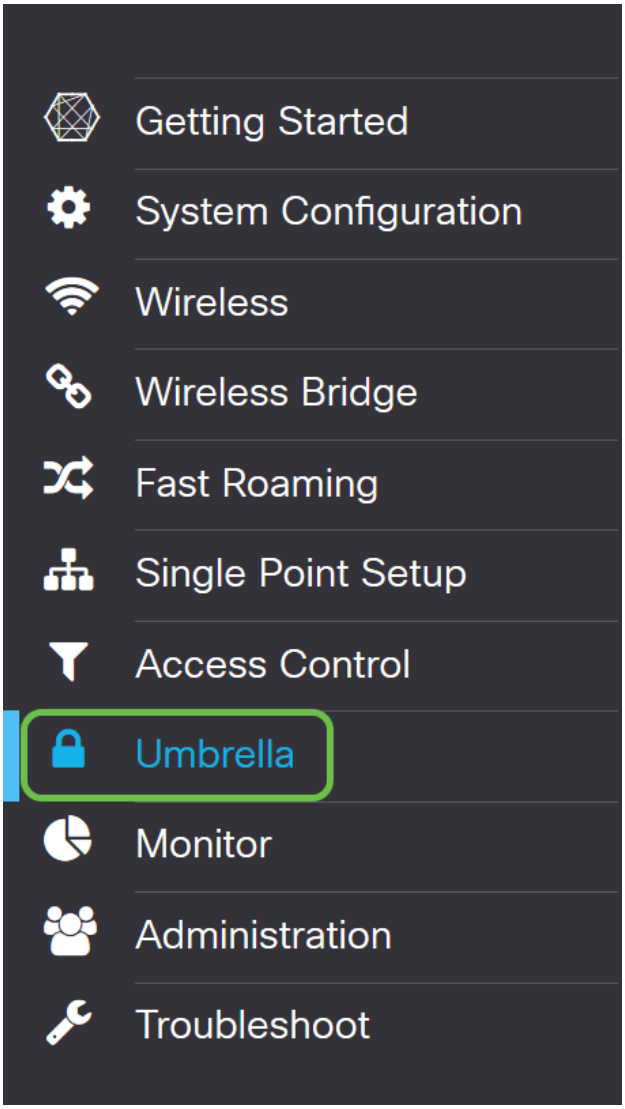
Nota importante: Si pierde o elimina accidentalmente la clave secreta, no hay ninguna función o número de soporte al que llamar para recuperar esta clave. Manténgalo en secreto, manténgalo a salvo. Si se pierde, deberá eliminar la clave y volver a autorizar la clave de API con cada dispositivo WAP que desee proteger con Umbrella.

Práctica recomendada: Mantenga sólo una *única* copia de este documento en un dispositivo, como una unidad de almacenamiento en miniatura USB, inaccesible desde cualquier red.

Configuración del paraguas en su dispositivo WAP

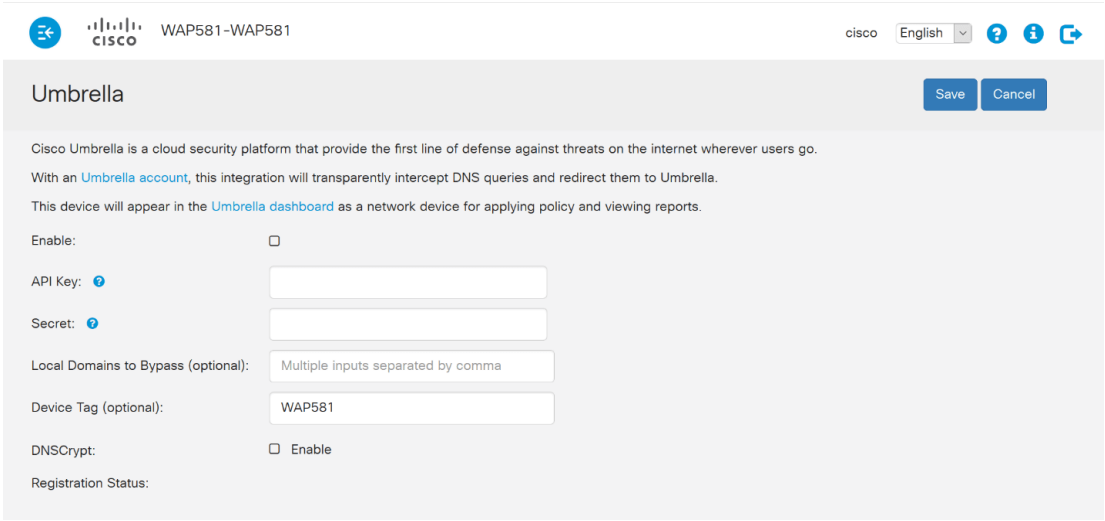
Ahora que hemos creado claves API dentro de Umbrella, tomaremos esas claves e las instalaremos en nuestros dispositivos WAP. En nuestro caso, utilizamos un WAP581.

Paso 1. Después de iniciar sesión en su dispositivo WAP, haga clic en **Umbrella** en el menú de la barra lateral.

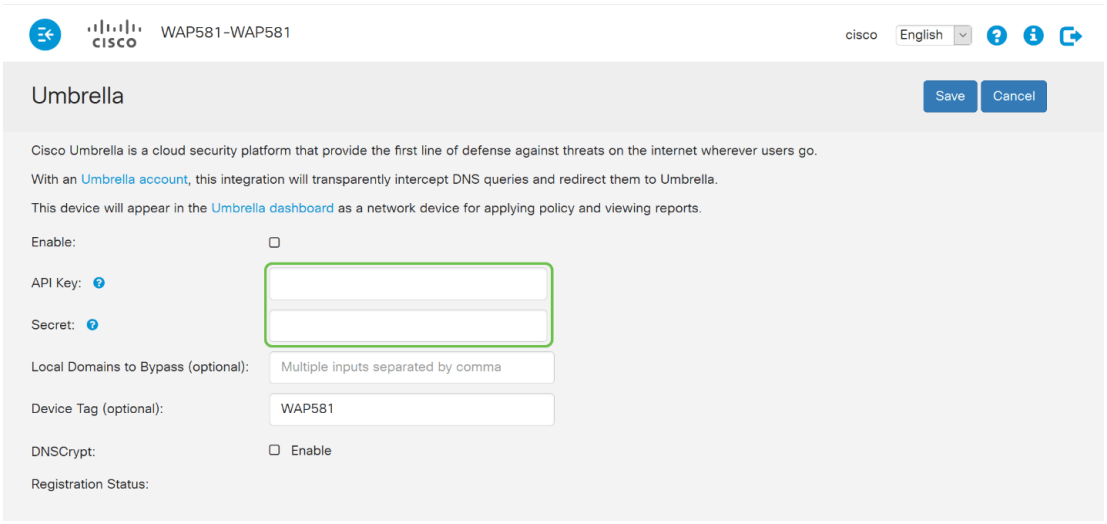


Paso 2. La pantalla del paraguas es sencilla, pero hay dos campos que vale la pena definir:

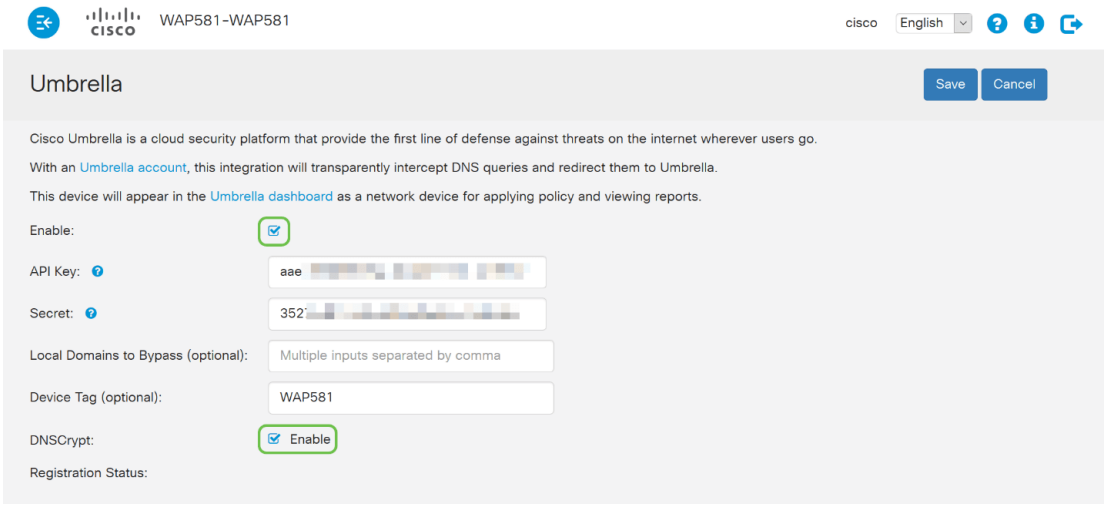
- *Dominios locales que se deben omitir*: este campo contiene los dominios internos que desea excluir del servicio Umbrella.
- *DNSCrypt:* Protege la transferencia de paquetes entre el cliente DNS y el Resolver DNS. Esta función está activada de forma predeterminada; si desactiva esta función, la red será menos segura.



Paso 3. Pegue la API y la clave secreta en los campos correspondientes

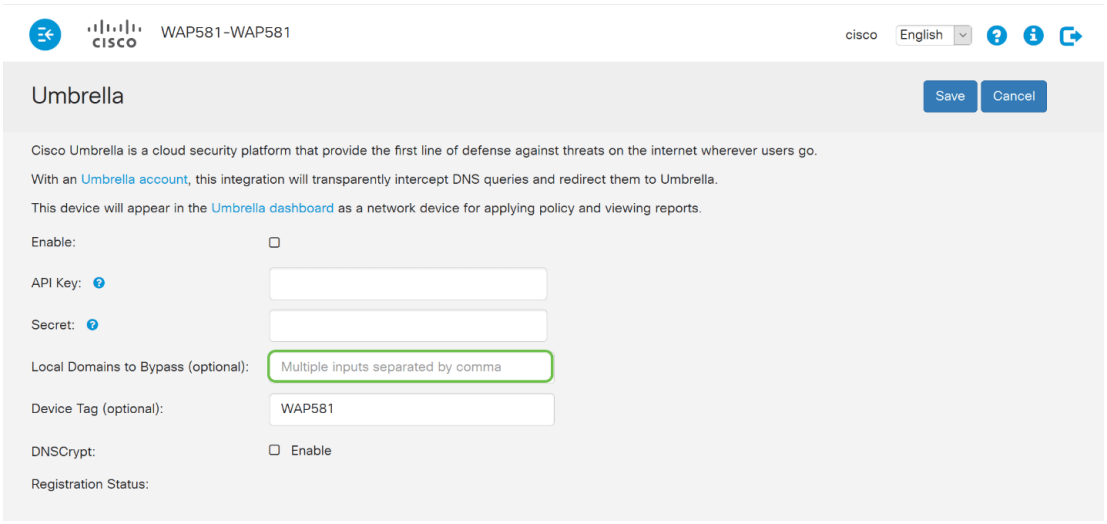


Paso 4. Asegúrese de que las casillas de verificación **Enable** y **DNSCrypt** se conmuten al estado de verificación.



Nota: DNSCrypt protege la comunicación DNS entre un cliente DNS y una resolución DNS. El valor predeterminado está habilitado.

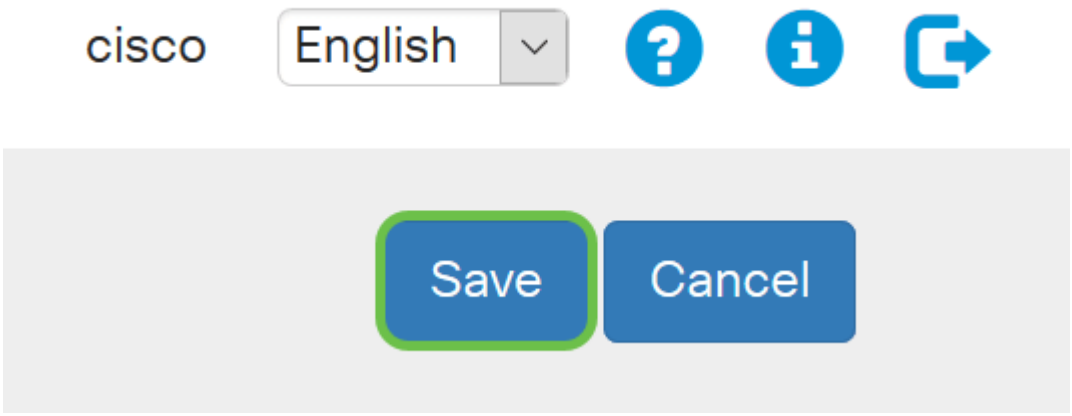
Paso 5. (Opcional) Introduzca los dominios locales que desea que Umbrella permita a través del proceso de resolución de DNS.



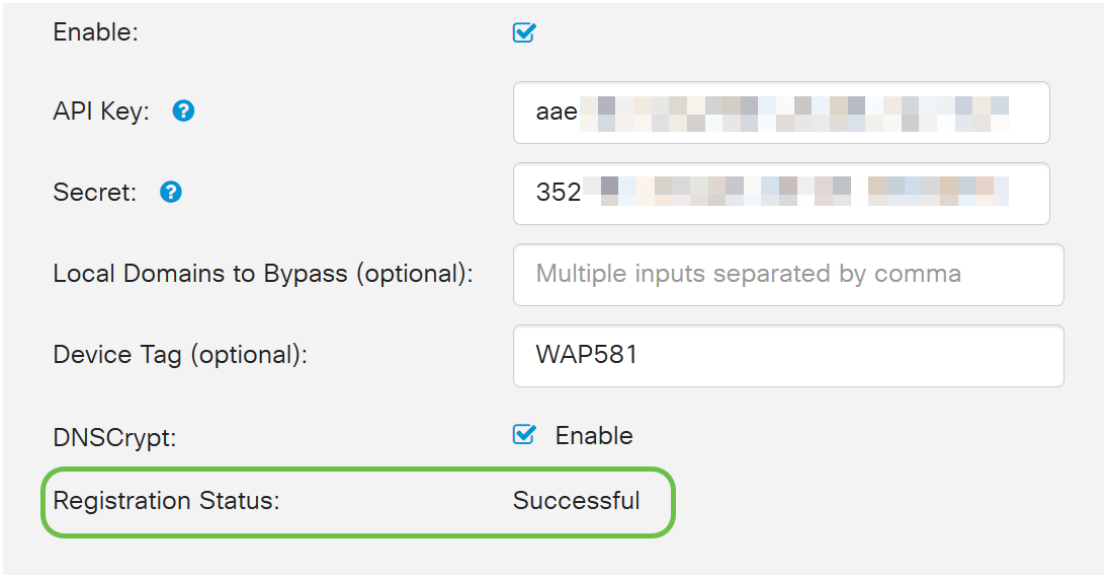
Nota: Esto es necesario para todos los dominios de intranet y dominios DNS divididos. Si su red requiere el uso de dominios de área local para el ruteo, deberá ponerse en contacto con el

soporte técnico de Umbrella para activar y ejecutar esta función. La mayoría de los usuarios no necesitarán utilizar esta opción.

Paso 6. Cuando esté satisfecho con los cambios o haya agregado sus propios *dominios locales para omitir*, haga clic en el **botón Guardar** de la esquina superior derecha.



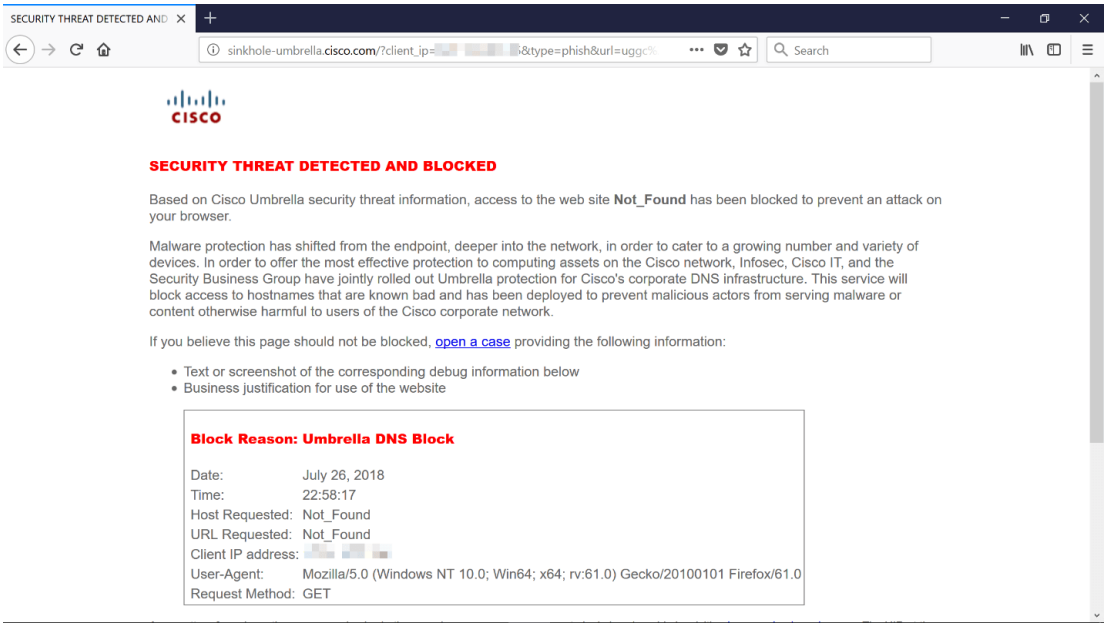
Paso 7. Cuando se completen los cambios, el campo *Estado de registro* será "Satisfactorio".



Confirmación de que todo está en el lugar adecuado

Enhorabuena, ahora está protegido el paraguas de Cisco. ¿O sí? No olvidemos que Cisco ha creado un sitio web dedicado a determinar esto tan rápido como se carga la página. Haga clic aquí o escriba https://InternetBadGuys.com en la barra del explorador.

Si Umbrella está configurado correctamente, recibirá una pantalla similar a esta.


SECURITY THREAT DETECTED AND
sinkhole-umbrella.cisco.com/?client_ip=
&type=phish&url=ugg
Search
CISCO
SECURITY THREAT DETECTED AND BLOCKED
Based on Cisco Umbrella security threat information, access to the web site Not_Found has been blocked to prevent an attack on your browser.
Malware protection has shifted from the endpoint, deeper into the network, in order to cater to a growing number and variety of devices. In order to offer the most effective protection to computing assets on the Cisco network, Infosec, Cisco IT, and the Security Business Group have jointly rolled out Umbrella protection for Cisco's corporate DNS infrastructure. This service will block access to hostnames that are known bad and has been deployed to prevent malicious actors from serving malware or content otherwise harmful to users of the Cisco corporate network.
If you believe this page should not be blocked, open a case providing the following information:
Text or screenshot of the corresponding debug information below
Business justification for use of the website
Block Reason: Umbrella DNS Block
Date: July 26, 2018
Time: 22:58:17
Host Requested: Not_Found
URL Requested: Not_Found
Client IP address:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:61.0) Gecko/20100101 Firefox/61.0
Request Method: GET