Konfigurieren der Webinhaltsfilterung mithilfe von Cisco Umbrella in WAP571 oder WAP571E

Ziel

In diesem Artikel erfahren Sie, wie Sie die Filterung von Webinhalten mithilfe von Cisco Umbrella auf einem WAP571 oder WAP571E konfigurieren.

Einführung

Sie haben hart daran gearbeitet, Ihr Netzwerk in Betrieb zu nehmen. Natürlich wollen Sie, dass es so bleibt, aber Hacker sind unerbittlich. Wie können Sie die Sicherheit Ihres Netzwerks gewährleisten? Eine Lösung ist die Einrichtung einer Filterung von Webinhalten. Mit der Filterfunktion für Webinhalte können Sie durch die Konfiguration von Richtlinien und Filtern einen kontrollierten Zugriff auf das Internet ermöglichen. Sie trägt zum Schutz des Netzwerks bei, indem sie schädliche oder unerwünschte Websites blockiert.

Cisco Umbrella ist eine Cloud-Sicherheitsplattform, die die erste Verteidigungslinie gegen Bedrohungen aus dem Internet darstellt. Sie fungiert als Gateway zwischen dem Internet und Ihren Systemen und Daten, um Malware, Botnets und Phishing über beliebige Ports, Protokolle oder Anwendungen zu blockieren.

Bei Verwendung eines Cisco Umbrella-Kontos werden durch die Integration (Reporting auf URL-Ebene) Abfragen des Domain Name System (DNS) transparent abgefangen und an Umbrella umgeleitet. Ihr Gerät wird im Umbrella Dashboard als Netzwerkgerät angezeigt, um Richtlinien anzuwenden und Berichte anzuzeigen.

Weitere Informationen zu Cisco Umbrella finden Sie unter den folgenden Links:

Cisco Umbrella auf einen Blick

Cisco Umbrella-Benutzerhandbuch

Vorgehensweise: Erweiterung von Cisco Umbrella zum Schutz Ihres Wireless-Netzwerks

Anwendbare Geräte

WAP571

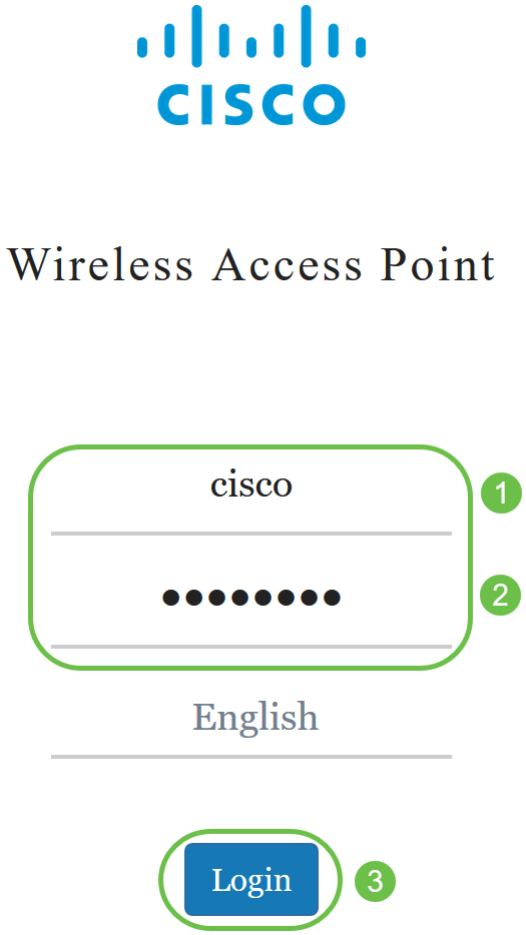
WAP571E

Softwareversion

- 1,1/0,3

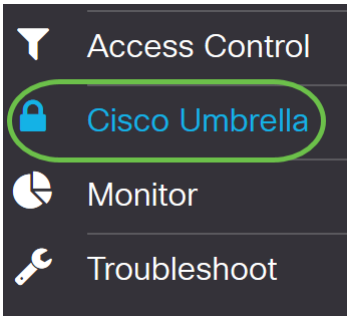
Konfigurieren von Cisco Umbrella auf dem WAP

Schritt 1: Melden Sie sich beim Webkonfigurations-Dienstprogramm des WAP an, indem Sie den Benutzernamen und das Kennwort eingeben. Der Standardbenutzername und das Standardkennwort sind *cisco/cisco.* Wenn Sie einen neuen Benutzernamen oder ein neues Kennwort konfiguriert haben, geben Sie diese stattdessen ein. Klicken Sie auf **Anmelden.**

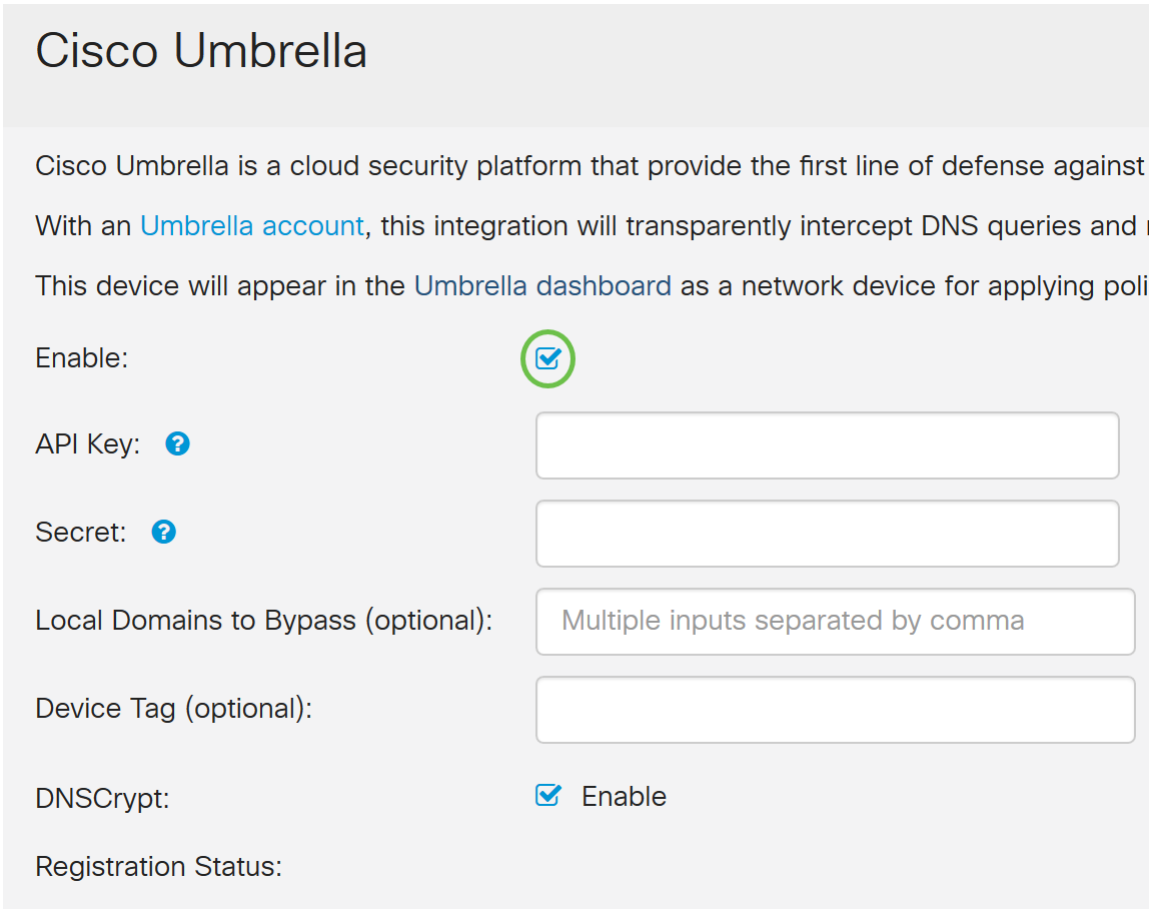


Hinweis: In diesem Artikel wird der WAP571E verwendet, um die Konfiguration von Cisco Umbrella zu demonstrieren. Die Menüoptionen können je nach Gerät leicht variieren.

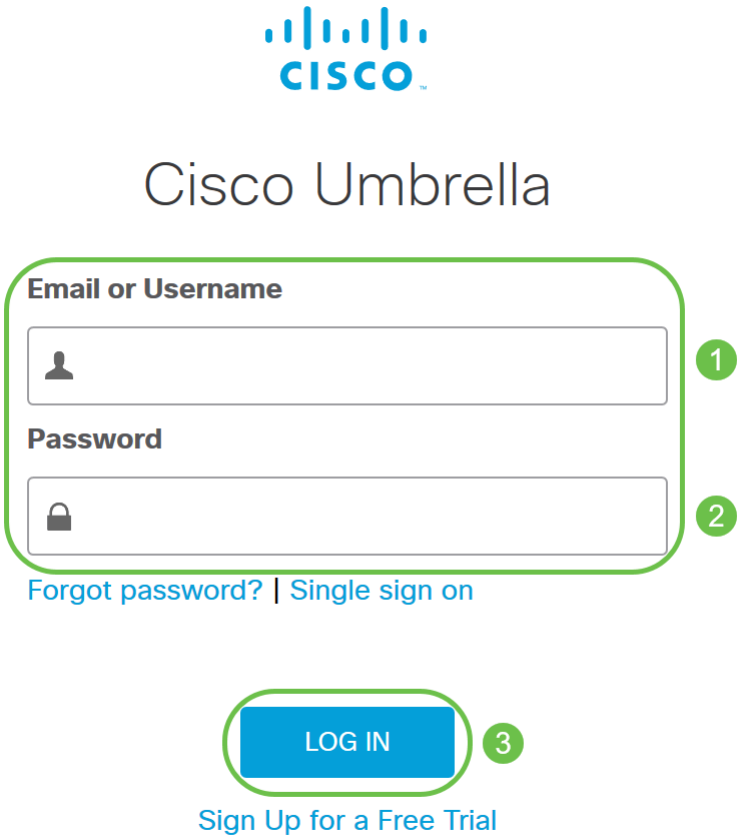
Schritt 2: Wählen Sie **Cisco Umbrella**.



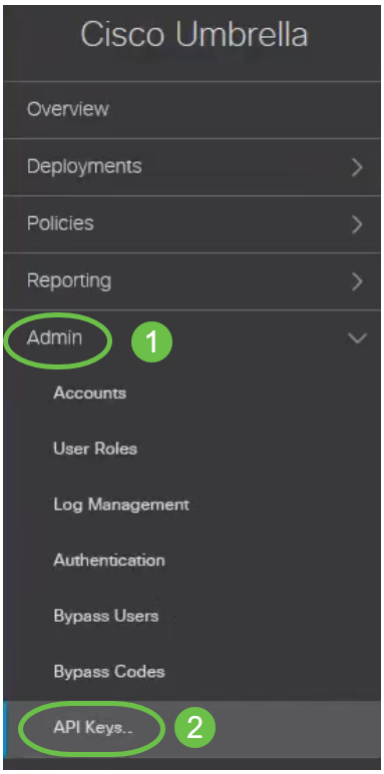
Schritt 3: *Aktivieren Sie* Cisco Umbrella, indem Sie auf das Kontrollkästchen klicken.



Schritt 4: Um den *API-Schlüssel* und den *geheimen Schlüssel* zu erhalten, melden Sie sich mit *E-Mail oder Benutzername* und *Kennwort* bei Ihrem Cisco Umbrella-Konto an. Klicken Sie auf **Anmelden**.



Schritt 5: Navigieren Sie zu **Admin**, und fordern Sie einen API-Schlüssel an, indem Sie **API-Schlüssel ...** aus dem Menü auswählen.

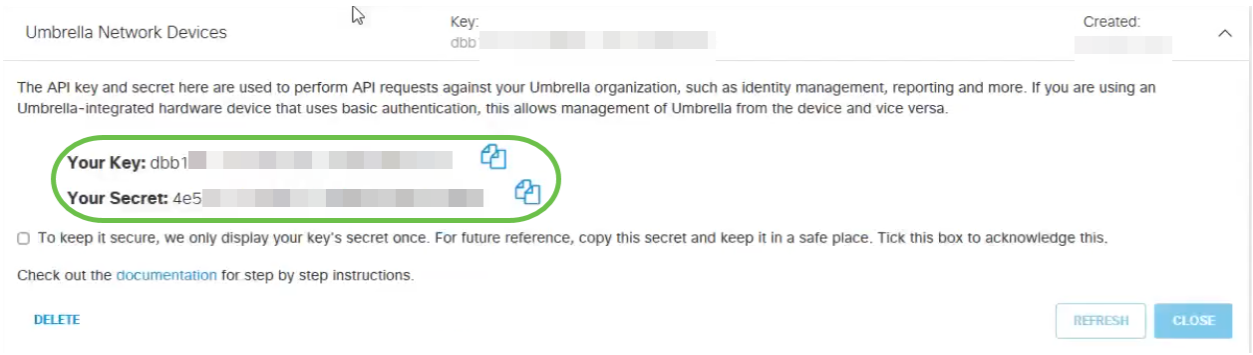


Hinweis: Wenn Sie zum ersten Mal einen API-Schlüssel anfordern, wird nur der Schlüssel wie unten gezeigt angezeigt.

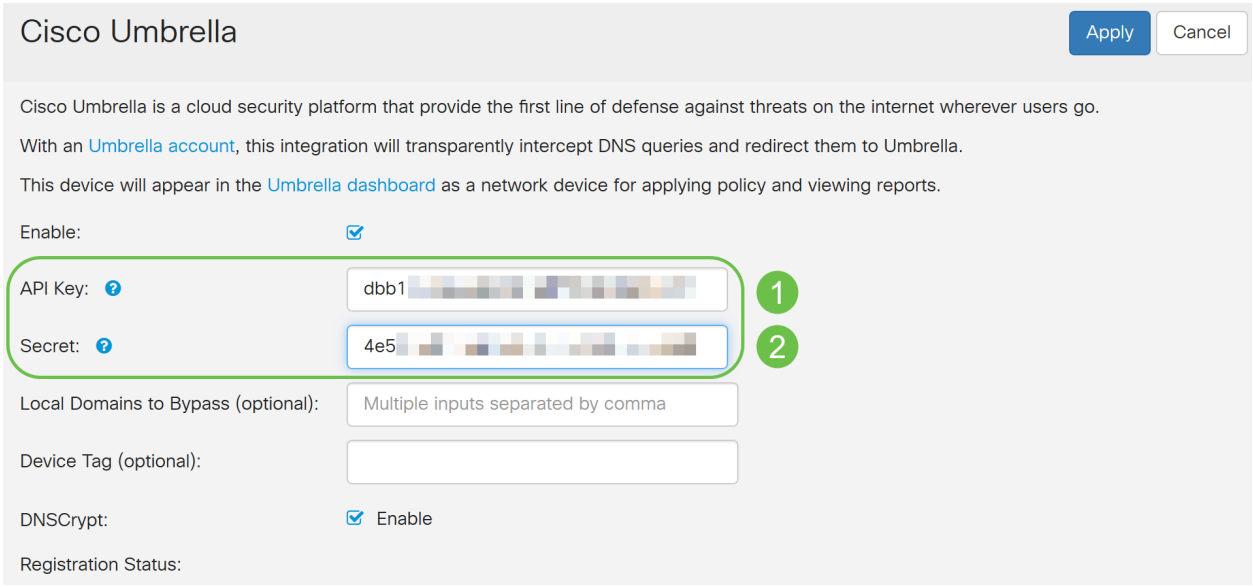
Schritt 6: Klicken Sie auf **Aktualisieren**, um sowohl den API-Schlüssel als auch Secret (Geheime Informationen) abzurufen.

Hinweis: Wenn Sie auf *Aktualisieren* klicken, ändert sich der API-Schlüssel.

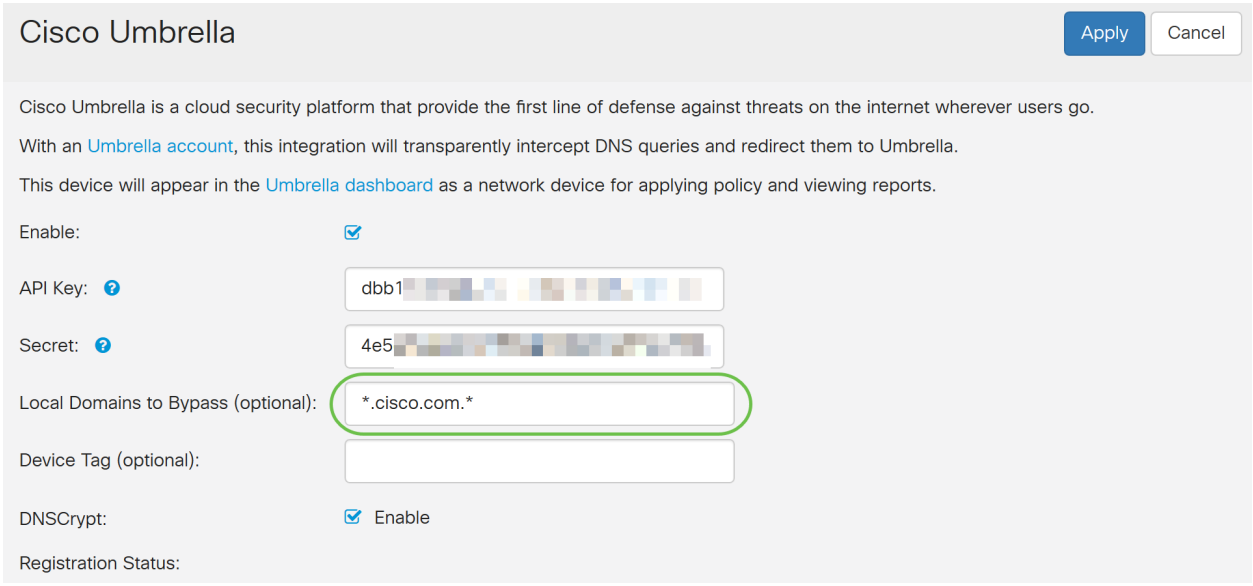
Schritt 7: Kopieren Sie den generierten *Schlüssel* und den *geheimen Schlüssel*.



Schritt 8: Fügen Sie den kopierten *Schlüssel* und *Geheimhaltungsgrad* aus Schritt 7 in die Felder ein, die unter der *Cisco Umbrella*-Konfiguration des WAP bereitgestellt werden.



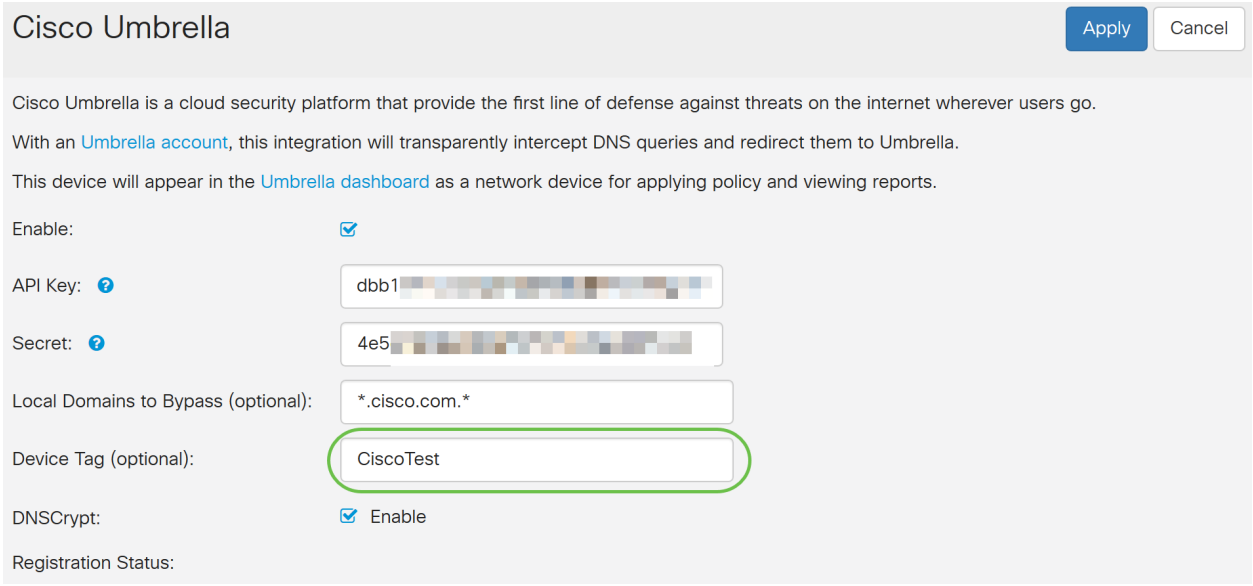
Schritt 9: (Optional) Geben Sie den Domänennamen, dem Sie vertrauen, in das **Feld Lokale Domänen zur Umgehung (optional)** ein, und die Pakete erreichen das Ziel, ohne Cisco Umbrella zu durchlaufen. Elemente in der Liste sollten durch ein Komma getrennt werden, während die Domänen Platzhalter in Form eines Sternchen (*) enthalten können. Beispiel: *.cisco.com.*



Hinweis: Dies ist für alle Intranet-Domänen und Split-DNS-Domänen erforderlich, in denen separate Server für interne und externe Netzwerke vorhanden sind.

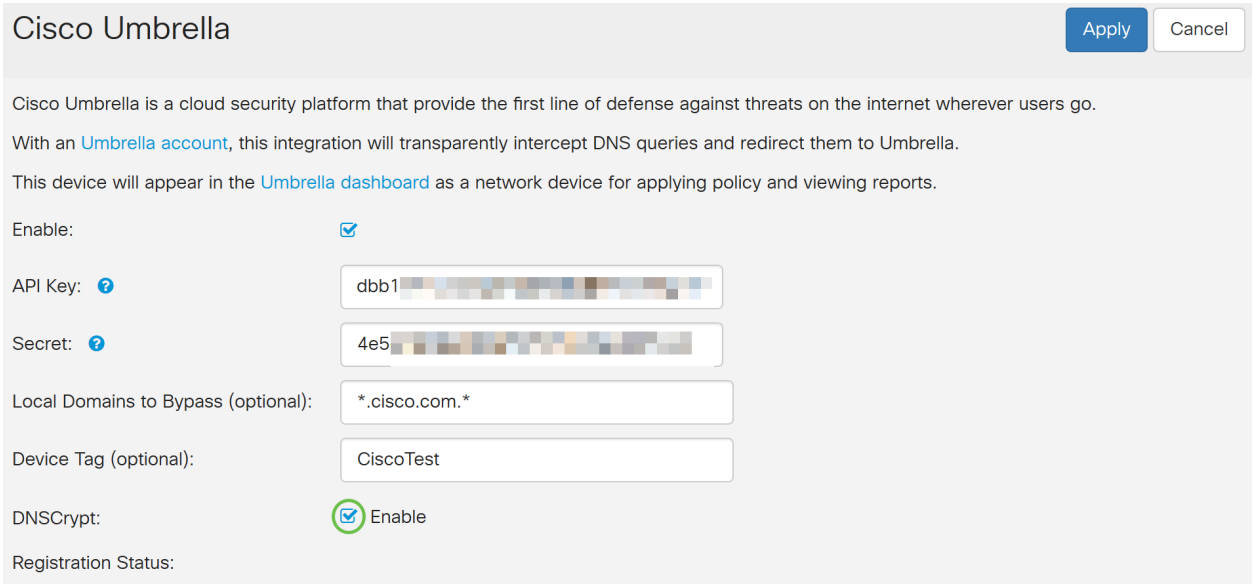
Schritt 10: (Optional) Geben Sie im **Feld Device Tag (optional)** einen Tag-Namen ein, um das

Gerät zu kennzeichnen. Die *Geräte-Tag* beschreibt das Gerät oder eine bestimmte Quelle, die dem Gerät zugewiesen ist. Stellen Sie sicher, dass die Lösung nur für Ihr Unternehmen geeignet ist.

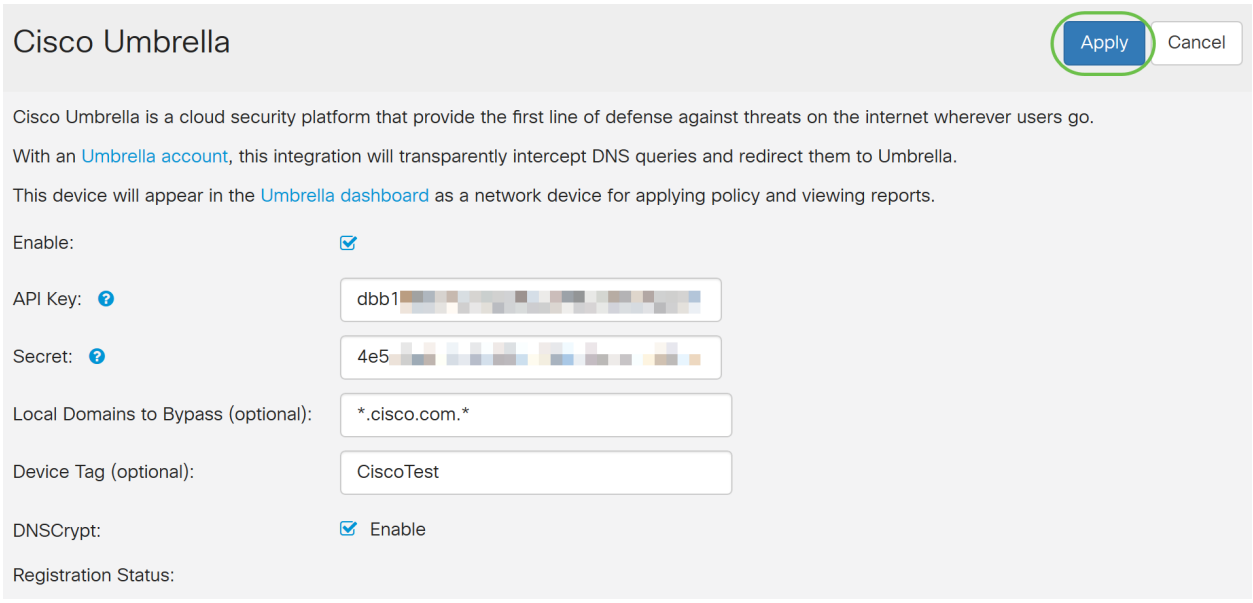


Hinweis: Jede Änderung im *geheimen*, *API-Schlüssel* und der *Geräte-Tag* löst eine erneute Registrierung aus, um ein Netzwerkgerät zu erstellen.

Schritt 11: **DNSCrypt** wird verwendet, um die DNS-Kommunikation zwischen einem DNS-Client und einem DNS-Resolver (über Verschlüsselung) zu sichern. Es verhindert mehrere Arten von DNS-Angriffen und Snooping. Es ist standardmäßig aktiviert.

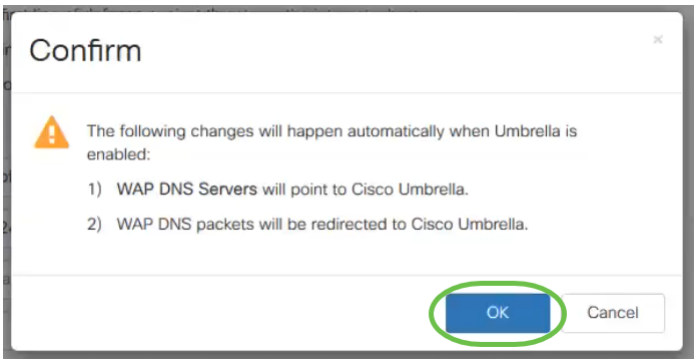


Schritt 12: Klicken Sie auf **Apply**, um diese Konfigurationen anzuwenden.



Hinweis: Der Status der Registrierung wird im Feld *Registrierungsstatus* angezeigt. Der Status kann *Successful*, *Registering* oder *Failed* sein.

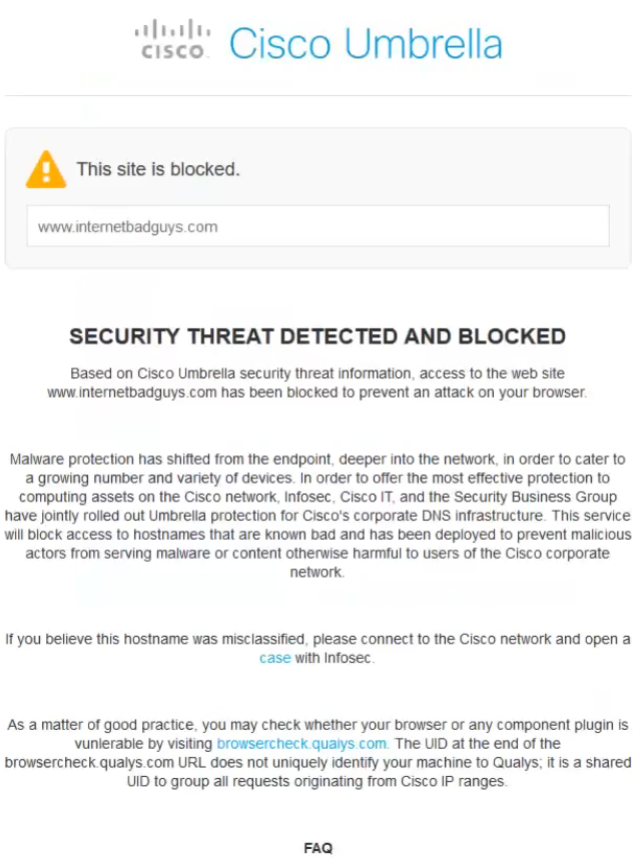
Schritt 13: Sie sehen einen Popup-Bildschirm, wie unten gezeigt. Klicken Sie zur Bestätigung auf **OK**.



Überprüfung

Es gibt eine unterhaltsame Möglichkeit, zu prüfen, ob die Filterung der Website aktiviert ist. Öffnen Sie einfach einen Webbrowser, und geben Sie die folgende URL ein: www.internetbadguys.com. Sie haben keine Angst, diese Website gehört Cisco für Test- und Verifizierungszwecke.

Da die Webseitenfilterung im WAP über Cisco Umbrella aktiviert ist, erhalten Sie die folgende Benachrichtigung. Das Wireless-Netzwerk leitet die DNS-Abfrage an Cisco Umbrella weiter. Cisco Umbrella wiederum fungiert als DNS-Server und schützt das Netzwerk und seine Benutzer.



Schlussfolgerung

Sie haben jetzt mithilfe von Cisco Umbrella die Webseitenfilterung auf einem WAP571 oder WAP571E Access Point konfiguriert und aktiviert.

Sie möchten mehr erfahren? Sehen Sie sich die folgenden Videos zu Cisco Umbrella an:

Cisco Tech Talk: Sicherung eines Unternehmensnetzwerks mit Umbrella und Cisco Small Business Access Points

Cisco Tech Talk: So erhalten Sie ein Umbrella Account

Cisco Tech Talk: Einrichten einer übergeordneten Richtlinie