Procedura: Recupera una chiave privata Umbrella persa

Obiettivo

Se avete perso una chiave irrecuperabile, sapete quanto velocemente il sangue può iniziare a pompare attraverso il vostro corpo. In questo articolo verrà spiegato come ripristinare dopo la perdita del tasto API (Application Programming Interface) segreto. Questa chiave segreta viene visualizzata una sola volta quando viene generata e non viene visualizzata di nuovo. Se ci si allontana dal browser dalla schermata della chiave API, si potrebbero perdere queste informazioni.

Dispositivi interessati

- WAP125
- WAP581

Versione del software

- 1.0.1

Requisiti

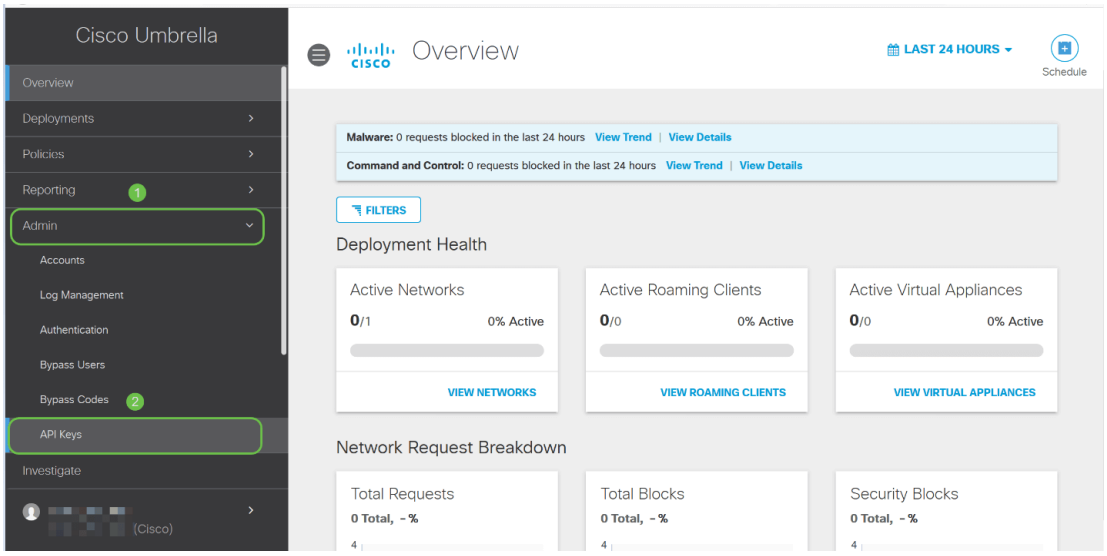
- Un account Umbrella attivo (non ne hai uno? Richiedi un preventivo o avvia una versione di valutazione gratuita)

Aiuto, ho perso la mia chiave segreta!

Ecco la dura notizia, la chiave segreta, è persa a causa dell'etere, sparita. Dove questo si trasforma in notizie migliori, è che il processo di recupero non è così doloroso. Generando una nuova chiave API, si genera una nuova chiave segreta. Il processo di ripristino comporta quindi l'eliminazione della chiave API associata alla chiave persa e la generazione della nuova serie di chiavi API.

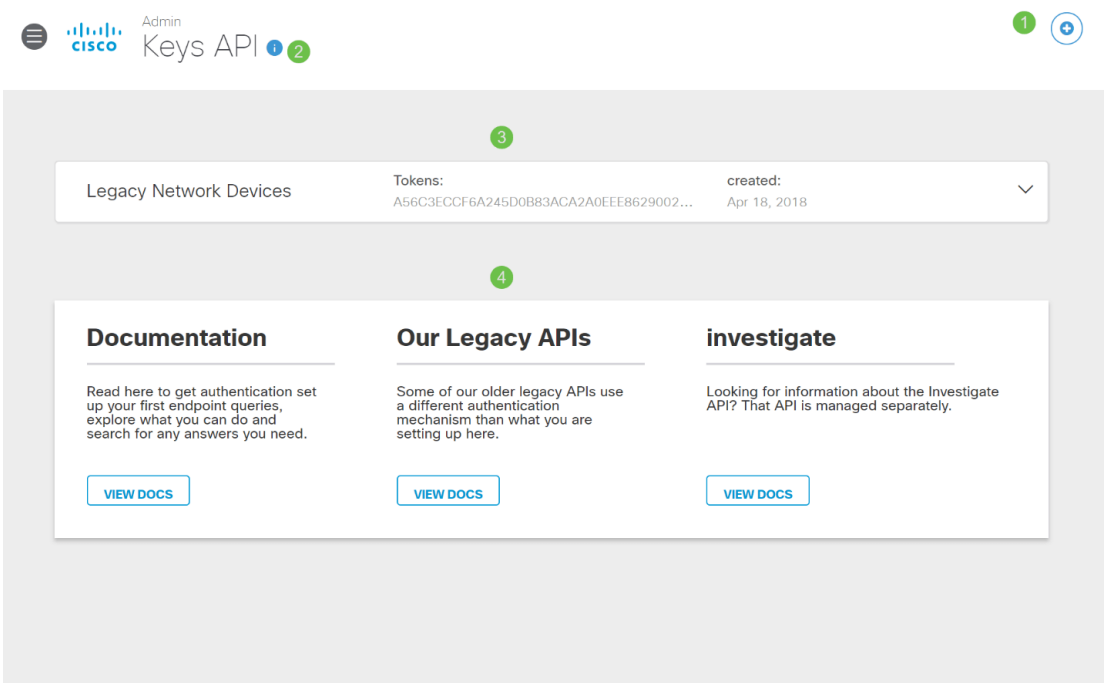
Dove si trova questa guida, inizia con l'acquisizione della chiave API e della chiave privata dal dashboard dell'account Umbrella. Dopo, accederò al tuo dispositivo WAP per aggiungere l'API e la chiave privata. In caso di problemi, consultare la documentazione e qui le opzioni di supporto Umbrella.

Passaggio 1. Dopo aver effettuato l'accesso all'account Umbrella, dalla schermata *Dashboard* fare clic su **Amministrazione > Chiavi API**.

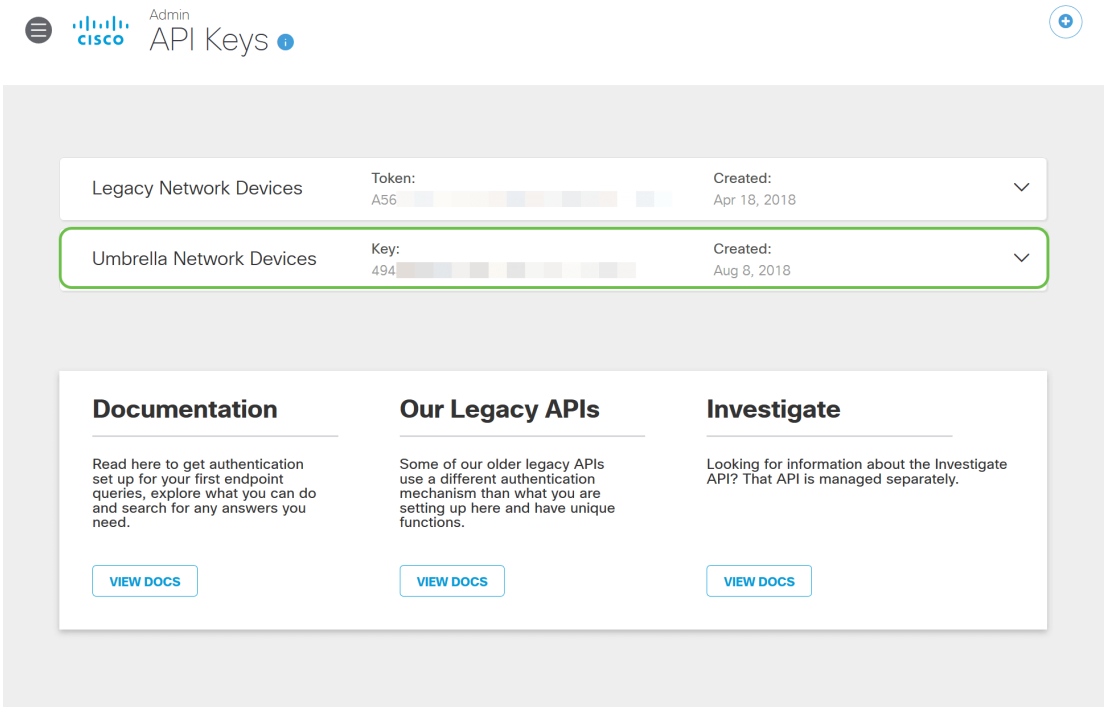


Anatomia della schermata delle chiavi API -

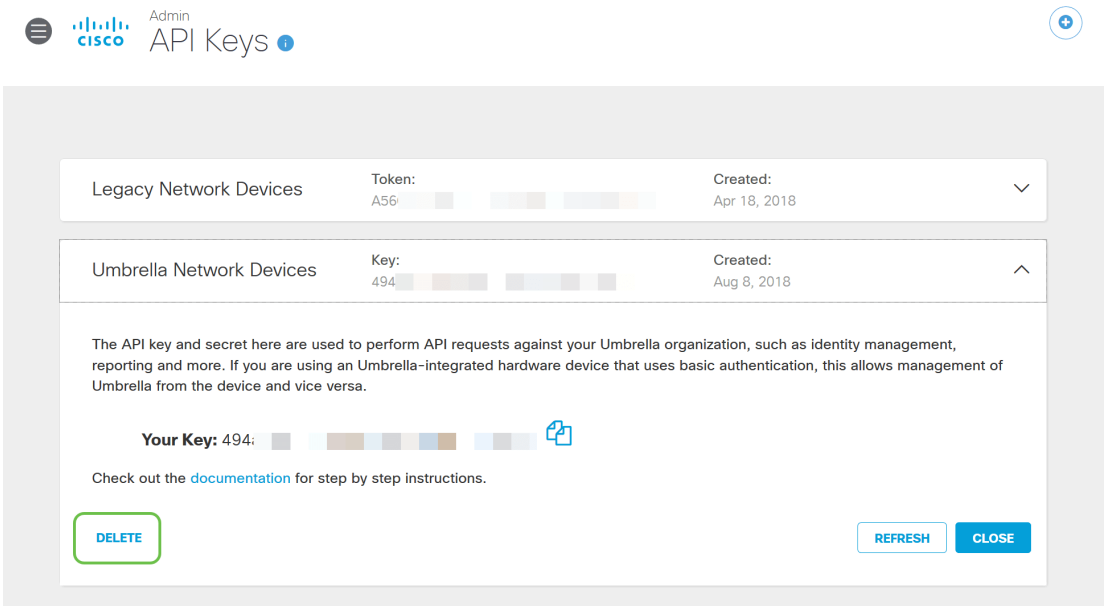
1. *Add API Key* - Avvia la creazione di una nuova chiave da utilizzare con l'API Umbrella.
2. *Informazioni aggiuntive* - Visualizza le diapositive in basso e in alto con un'illustrazione per questa schermata.
3. *Finestra Token* - Contiene tutte le chiavi e i token creati da questo account. (Esegue la compilazione dopo la creazione di una chiave)
4. *Documenti di supporto* - Collegamenti alla documentazione sul sito Umbrella relativa agli argomenti di ciascuna sezione.



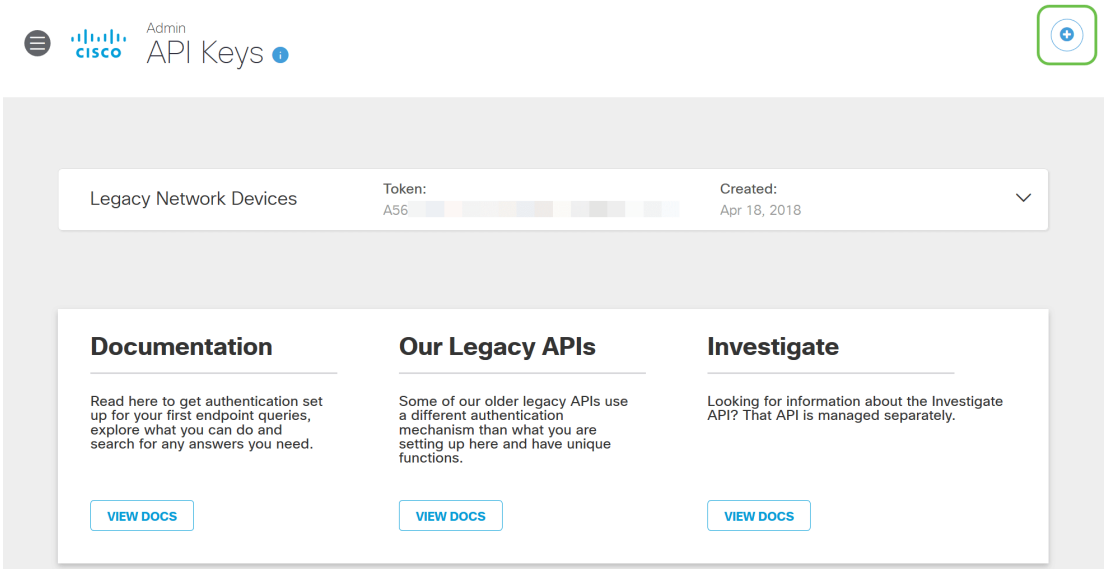
Passaggio 2. Fare clic sul pulsante **Umbrella Network Devices** nella *finestra Token*.



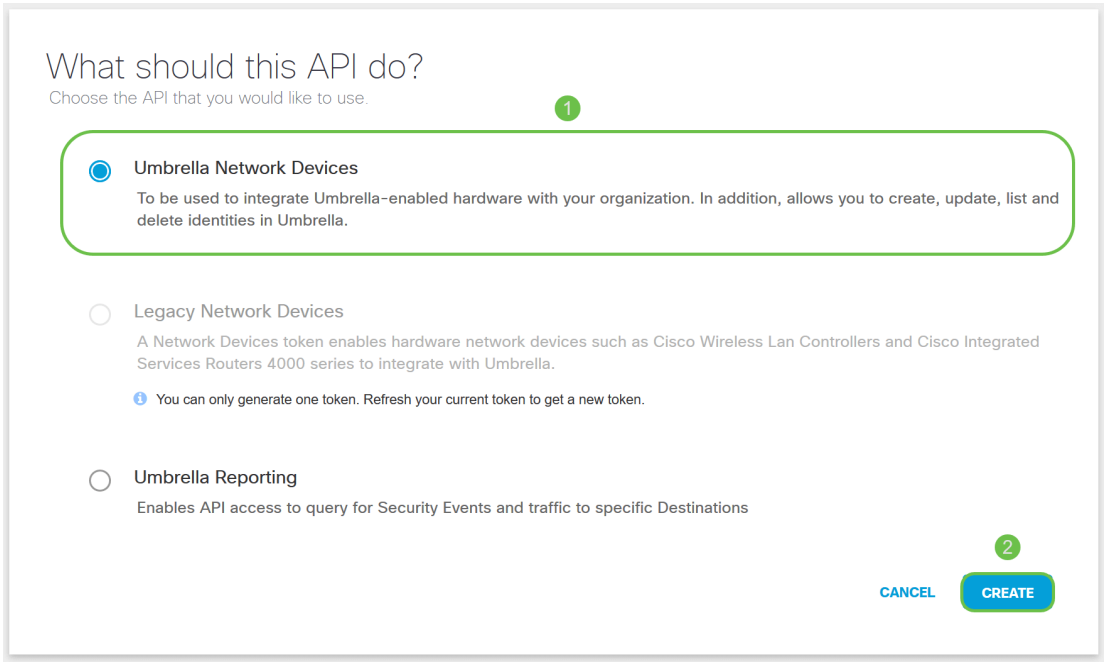
Passaggio 3. Selezionare **Umbrella Network Devices** e fare clic sul pulsante **Create**.



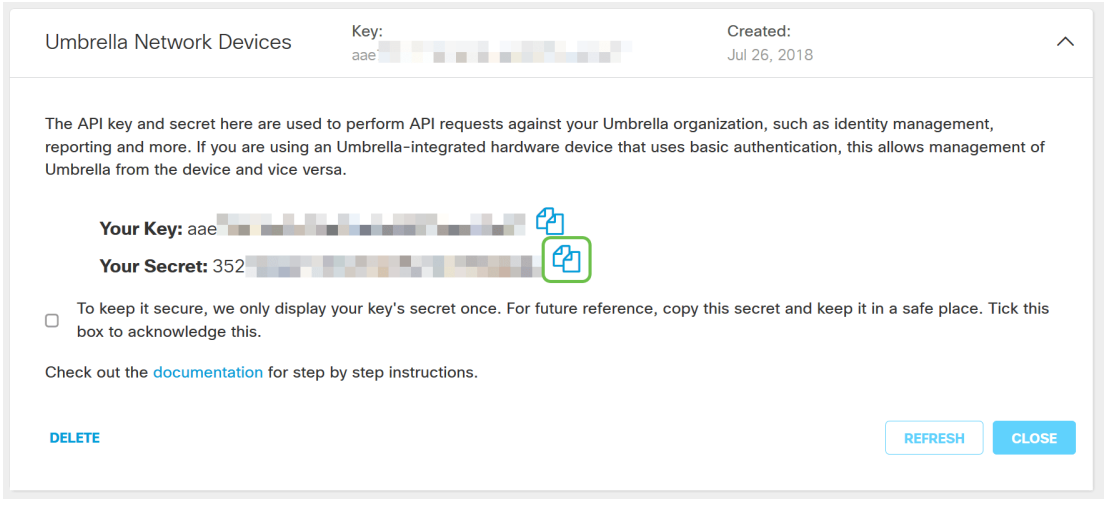
Passaggio 4. La chiave verrà eliminata immediatamente. Fare clic sul pulsante **Add API Key** (Aggiungi chiave API) nell'angolo in alto a destra oppure fare clic sul pulsante **Create API Key** (Crea chiave API). Funzionano entrambi allo stesso modo.



Passaggio 5. Selezionare **Umbrella Network Devices** e fare clic sul pulsante **Create**.

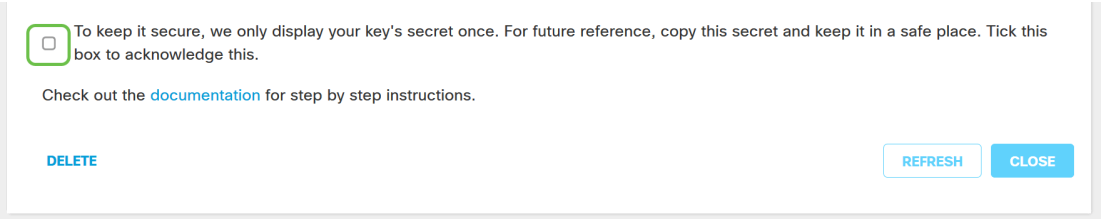


Passaggio 6. Fare clic sul pulsante **Copia** a destra della *chiave segreta.* Una notifica a comparsa confermerà che la chiave è stata copiata negli Appunti.

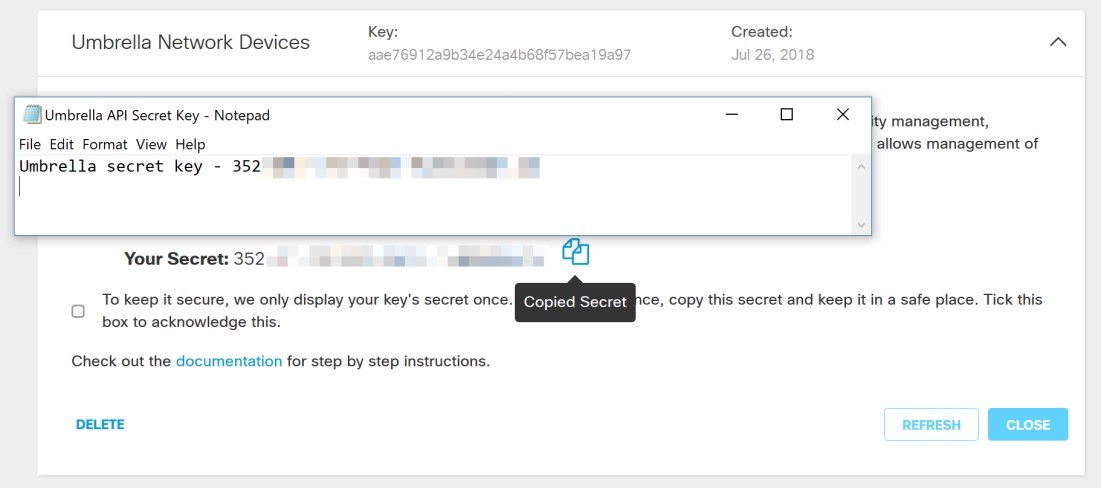


Dopo aver copiato la chiave e la chiave segreta in un percorso sicuro, fare clic sulla ***casella di***

controllo per confermare il completamento della conferma, quindi fare clic sul pulsante **Chiudi**.



Passaggio 7. Aprire un editor di testo come il Blocco note e incollare il segreto e la chiave API nel documento, etichettandoli per riferimento futuro. In questo caso la sua etichetta è "Umbrella secret key". Includere la chiave API con la chiave segreta insieme a una breve descrizione dell'utilizzo in questo stesso file di testo. Salvare quindi il file di testo in una posizione sicura, facilmente accessibile in seguito se necessario.



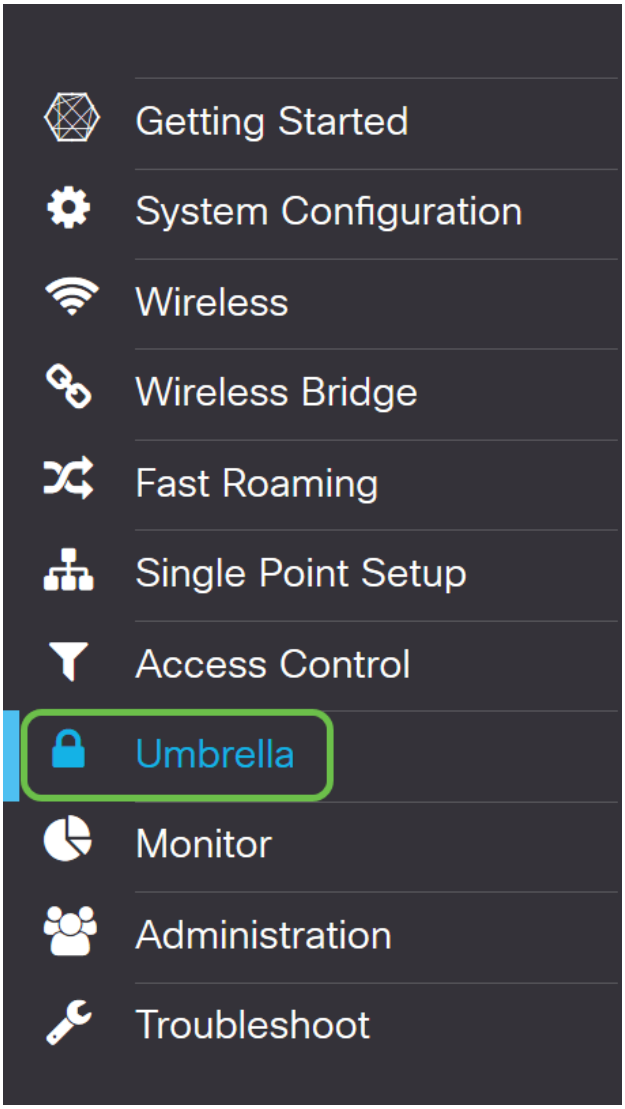
Nota importante: Se si perde o si elimina accidentalmente la chiave segreta, non sarà disponibile alcuna funzione o numero di supporto da chiamare per recuperare la chiave. Tienilo segreto, tienilo al sicuro. In caso di perdita, sarà necessario eliminare la chiave e autorizzare nuovamente la chiave API con ciascun dispositivo WAP che si desidera proteggere con Umbrella.

Procedure ottimali: Conservare una *singola* copia di questo documento su un dispositivo, come un'unità USB, inaccessibile da qualsiasi rete.

Configurazione di Umbrella sul dispositivo WAP

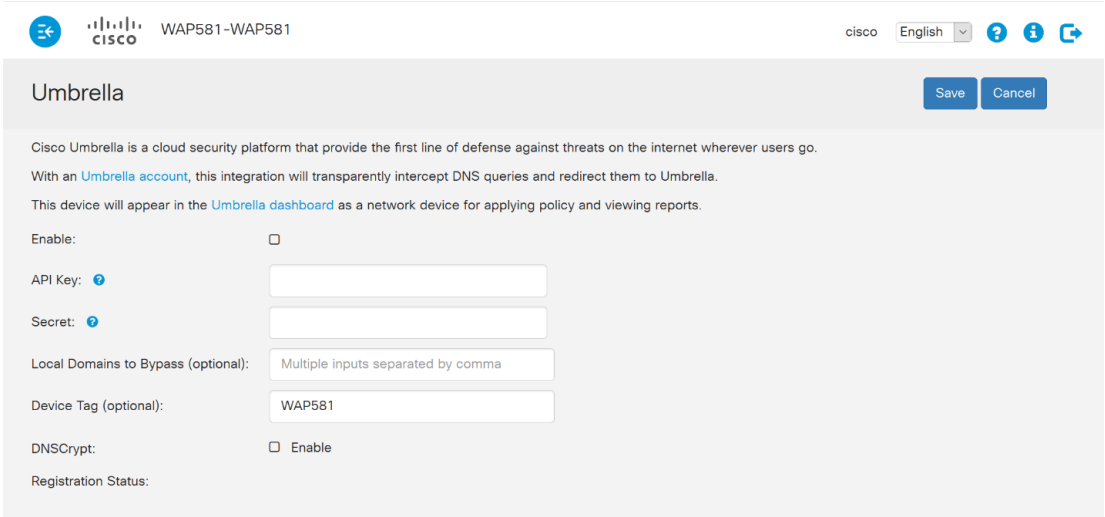
Ora che abbiamo creato le chiavi API in Umbrella, le prenderemo e le installeremo sui nostri dispositivi WAP. Nel nostro caso stiamo utilizzando un WAP581.

Passaggio 1. Dopo aver effettuato l'accesso al dispositivo WAP, fare clic su **Umbrella** nel menu della barra laterale.

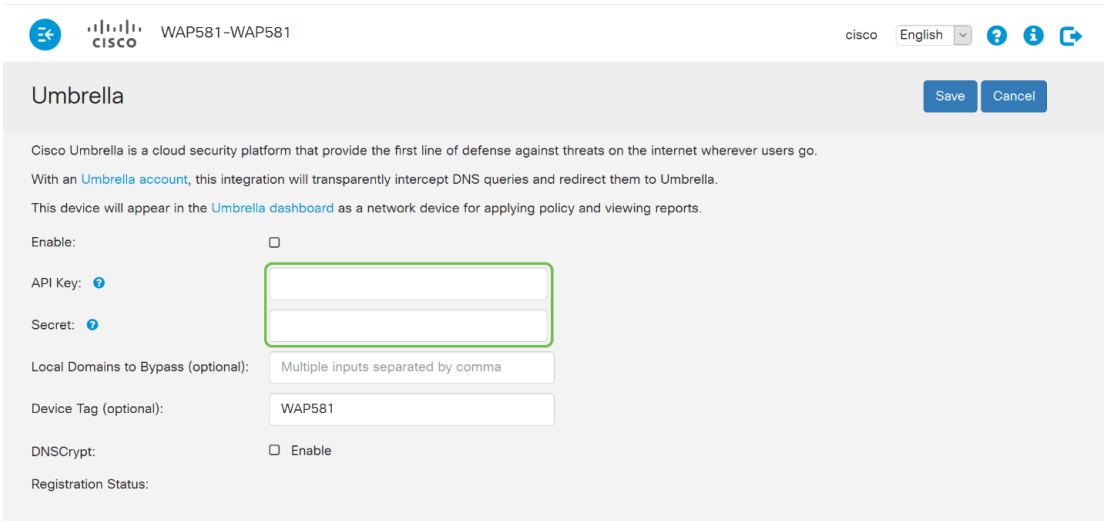


Passo 2. La schermata Umbrella è semplice, ma ci sono due campi che vale la pena definire qui:

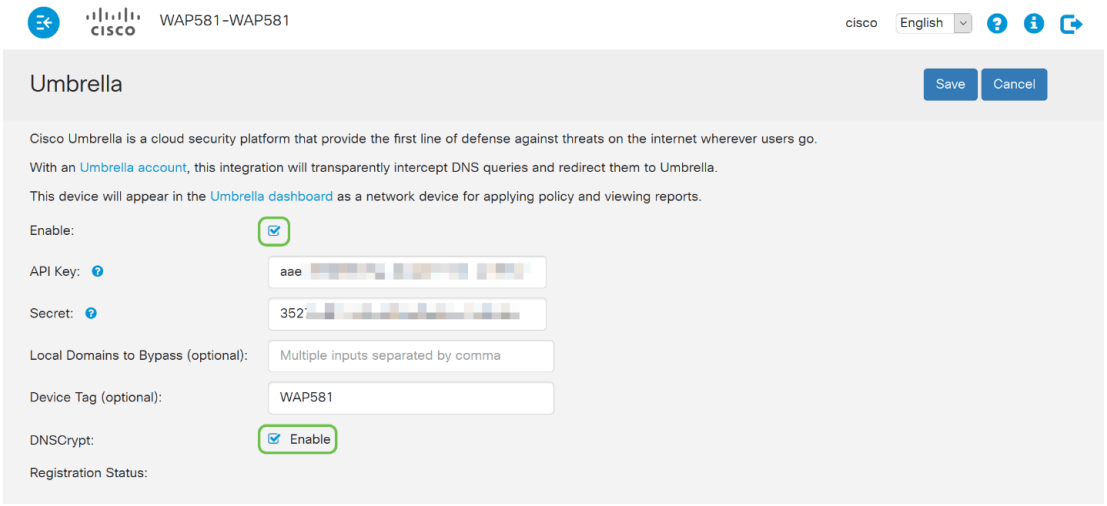
- *Domini locali da ignorare*: questo campo contiene i domini interni che si desidera escludere dal servizio Umbrella.
- *DNSCrypt:* protegge il trasferimento di pacchetti tra il client DNS e il resolver DNS. Questa funzionalità è attiva per impostazione predefinita. Se la si disattiva, la rete sarà meno sicura.



Passaggio 3. Incollare l'API e la chiave privata nei campi corrispondenti

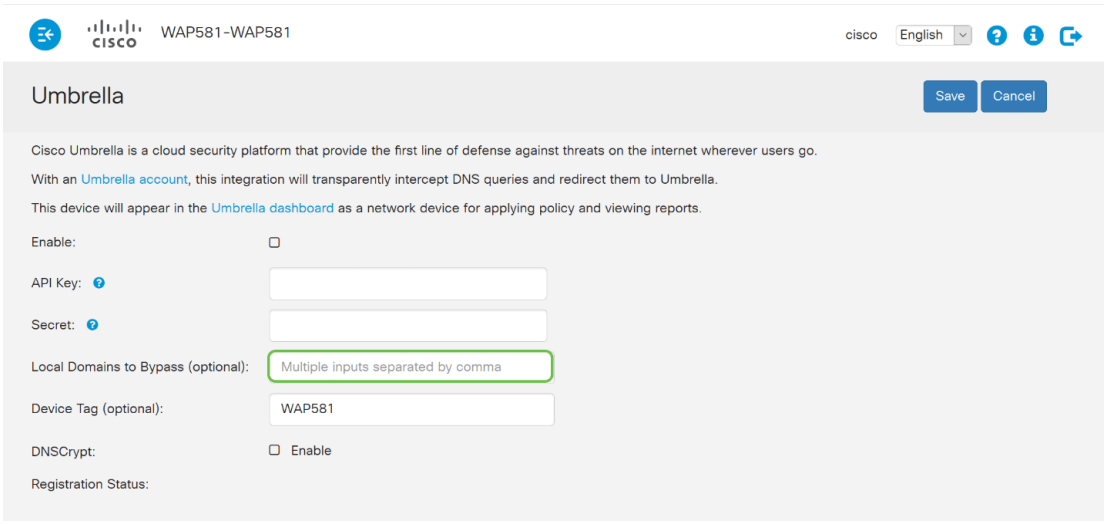


Passaggio 4. Verificare che le caselle di controllo **Enable** e **DNSCrypt** siano impostate sullo stato check.



Nota: DNSCrypt protegge la comunicazione DNS tra un client DNS e un resolver DNS. L'impostazione predefinita è attivata.

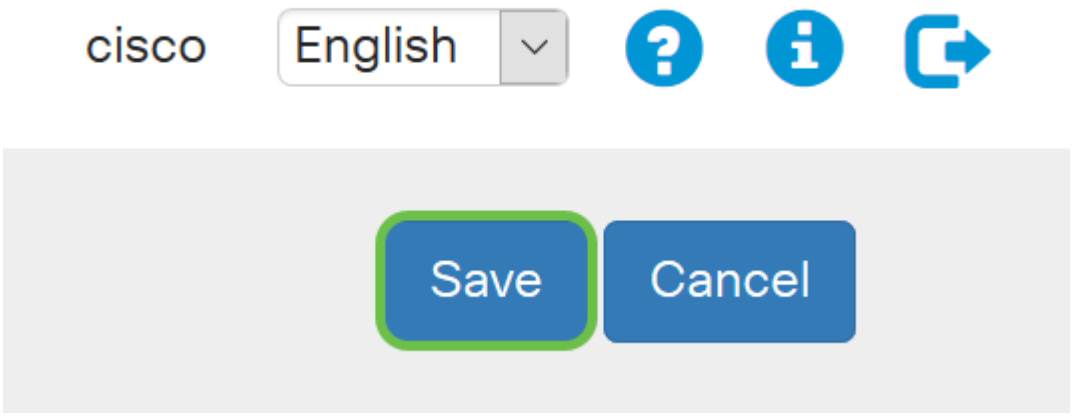
Passaggio 5. (Facoltativo) Immettere i domini locali che Umbrella deve consentire tramite il processo di risoluzione DNS.



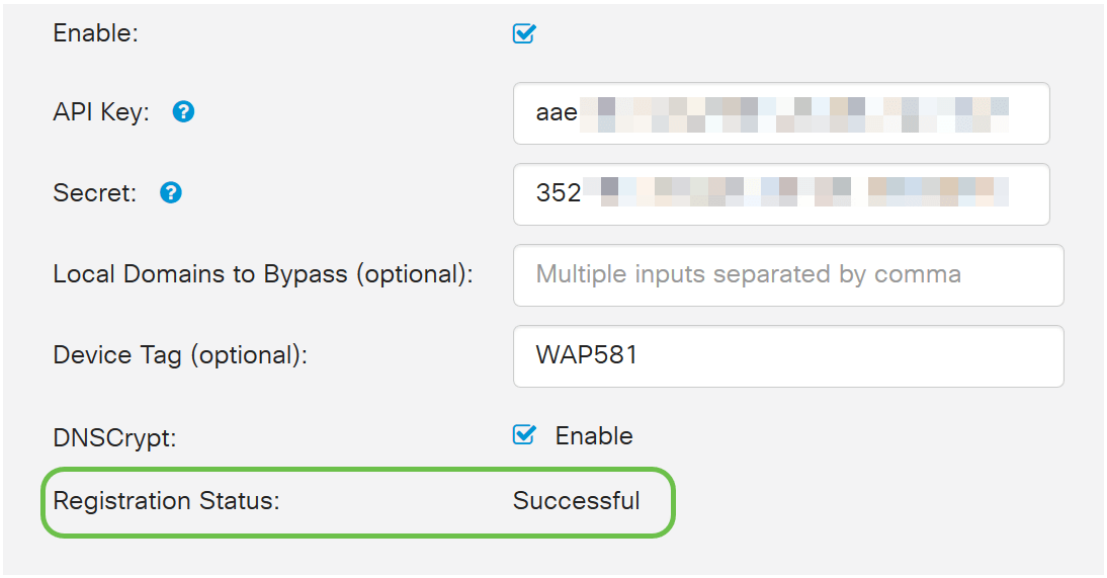
Nota: Questa operazione è obbligatoria per tutti i domini Intranet e per i domini DNS divisi. Se la rete richiede l'utilizzo di domini locali per il routing, sarà necessario contattare il supporto Umbrella

per rendere operativa questa funzionalità. La maggior parte degli utenti non deve utilizzare questa opzione.

Passaggio 6. Dopo aver apportato le modifiche desiderate o aver aggiunto i propri *domini locali da ignorare*, fare clic sul pulsante **Salva** nell'angolo superiore destro.



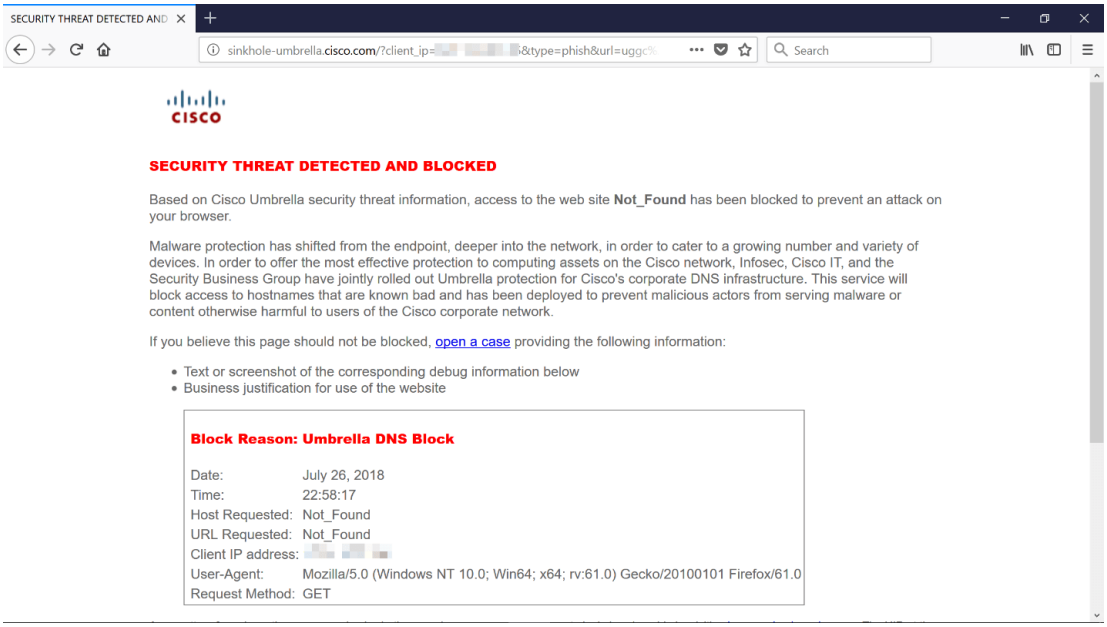
Passaggio 7. Al termine delle modifiche, nel campo *Stato registrazione* verrà visualizzato "Operazione riuscita".



Confermare che tutto è al posto giusto

Congratulazioni, ora sei protetto con Cisco's Umbrella. O lo sei? Sicuramente, Cisco ha creato un sito Web dedicato a determinare questa situazione non appena la pagina viene caricata. Fare clic qui o digitare https://InternetBadGuys.com nella barra del browser.

Se Umbrella è configurato correttamente, sarete accolti da uno schermo simile a questo!


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