Procedura: Estensione di Cisco Umbrella per la protezione della rete wireless

Introduzione

La sicurezza dei dati è un impegno di gruppo in ogni organizzazione. I dipendenti hanno almeno una parte di responsabilità nell'evitare di cadere vittime di truffe. In pratica, la sicurezza è difficile e non c'è da meravigliarsi. Mentre gli strumenti della tecnologia si espandono lo stesso vale per i progressi degli hacker, tutte le barche salgono con la marea, per così dire. Continua a leggere per scoprire come integrare la protezione Umbrella sulla tua LAN.

Obiettivo

Questa guida illustra i passaggi necessari per integrare la piattaforma di sicurezza Umbrella nella rete wireless. Prima di entrare nei dettagli grintosi risponderemo ad alcune domande che potresti porti riguardo Umbrella.

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)

Cos'è Umbrella?

Umbrella è una piattaforma Cisco semplice ma molto efficace per la sicurezza cloud. Umbrella opera nel cloud ed esegue molti servizi correlati alla sicurezza. Dalla minaccia emergente all'indagine post-evento. Umbrella individua e previene gli attacchi attraverso tutte le porte e i protocolli.

Come funziona?

Umbrella utilizza il DNS come vettore principale per la difesa. Quando gli utenti immettono un URL nella barra del browser e premendo Invio, Umbrella partecipa al trasferimento. L'URL viene passato al resolver DNS di Umbrella e, se al dominio viene associato un avviso di protezione, la richiesta viene bloccata. Questi dati di telemetria vengono trasferiti e analizzati in microsecondi, senza aggiungere alcuna latenza. I dati di telemetria utilizzano registri e strumenti che tracciano miliardi di richieste DNS in tutto il mondo. Quando questi dati sono diffusi, la correlazione a livello globale consente una risposta rapida agli attacchi non appena si verificano. Per ulteriori

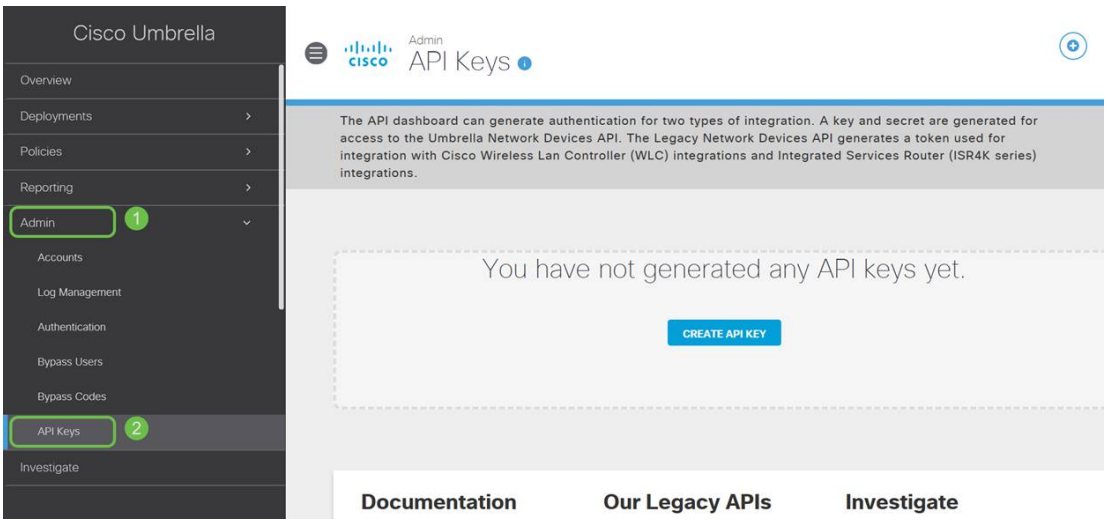
informazioni - politica completa, versione riepilogativa, vedere l'informativa sulla privacy di Cisco qui. I dati di telemetria possono essere paragonati ai dati derivati da strumenti e registri.

Per riassumere, immaginate di essere ad una festa. A questa festa tutti sono al telefono navigando in rete. Il silenzioso silenzio di gruppo è punteggiato dai partecipanti che filmano i loro schermi. Non è una grande festa, ma mentre sul vostro telefono vedete un collegamento ipertestuale a un gattino GIF che sembra irresistibile. Non si è certi, tuttavia, se toccare o meno, in quanto l'URL appare dubbio. Quindi prima di toccare il collegamento ipertestuale, si urla al resto della festa "Questo collegamento è cattivo?" Se un'altra persona alla festa fosse stata al link e avesse scoperto che era una truffa, avrebbe gridato "Si, l'ho fatto, ed è una truffa!" Ringraziate quella persona per avervi salvato, continuando la vostra ricerca di foto di animali carini in silenzio. Naturalmente, nelle dimensioni di Cisco, questo tipo di richieste e di controlli di sicurezza di callback si verificano milioni di volte al secondo.

Fantastico, come facciamo?

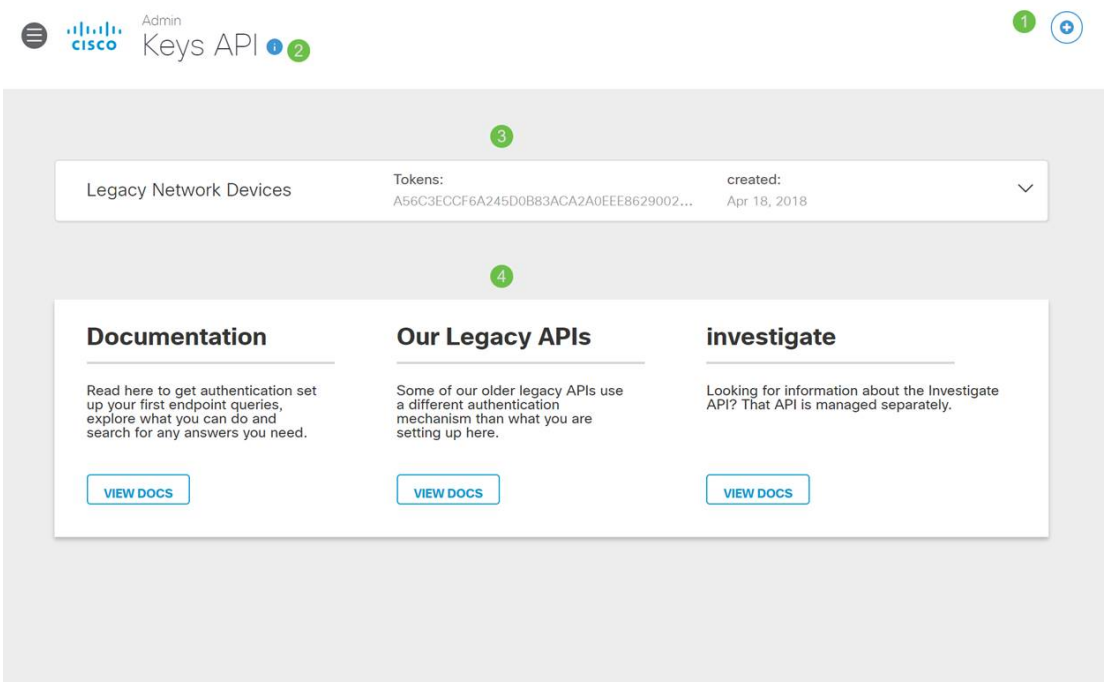
Dove si trova questa guida, inizia con l'acquisizione della chiave API e della chiave privata dal dashboard dell'account Umbrella. Dopo, accederò al tuo dispositivo WAP per aggiungere l'API e la chiave privata. In caso di problemi, consultare la documentazione e qui le opzioni di supporto Umbrella.

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

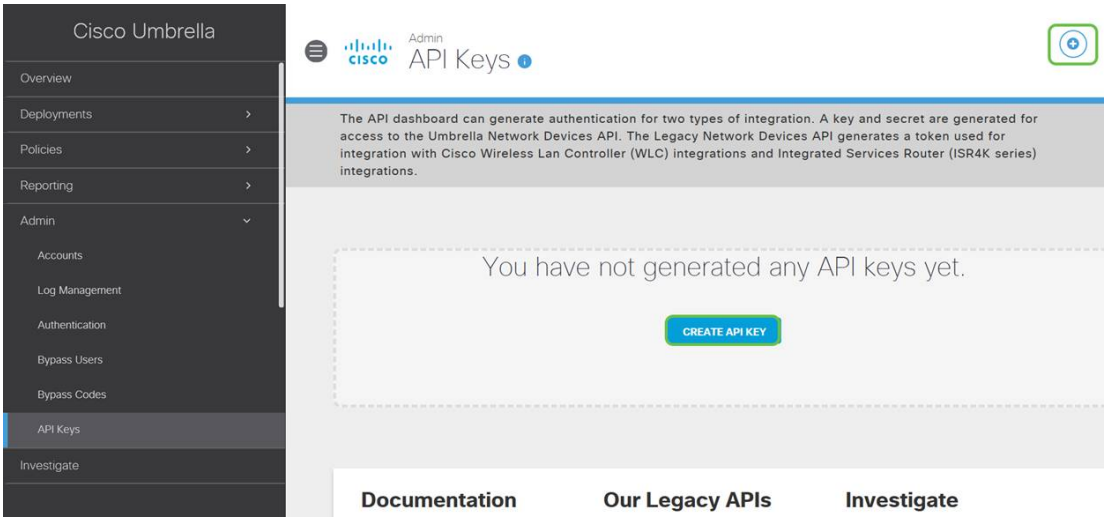


Anatomia della schermata delle chiavi API -

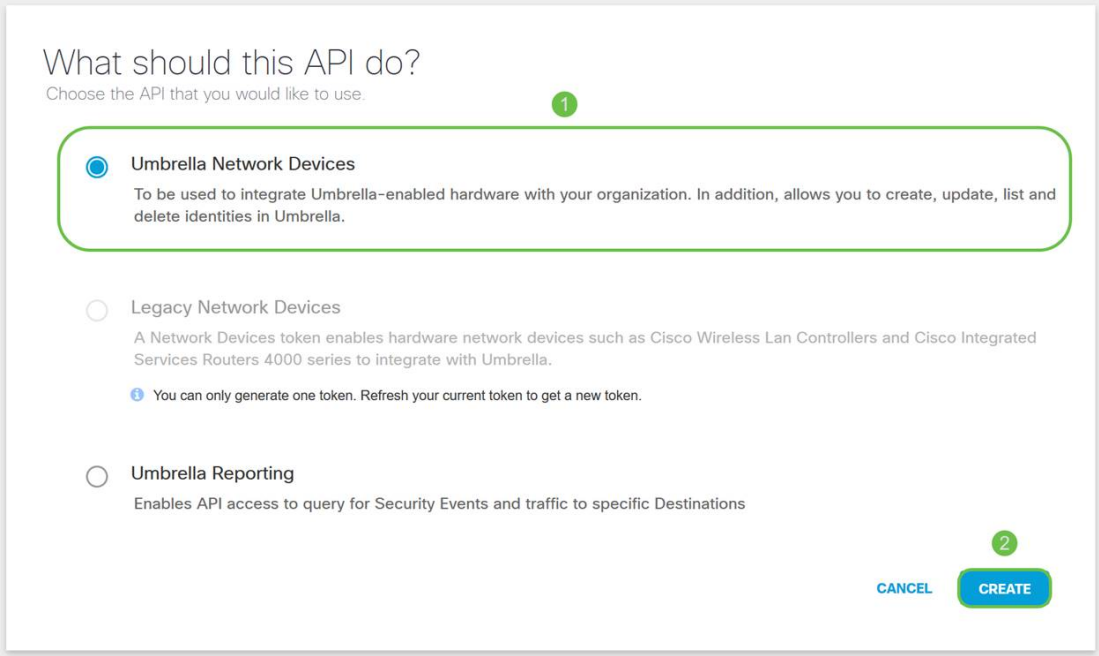
1. *Add API Key* - Avvia la creazione di una nuova chiave da utilizzare con l'API Umbrella.
2. *Ulteriori informazioni* - Visualizza le diapositive in basso/in alto con una spiegazione per questa schermata.
3. *Finestra Token* - Contiene tutte le chiavi e i token creati da questo account. (Esegue la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



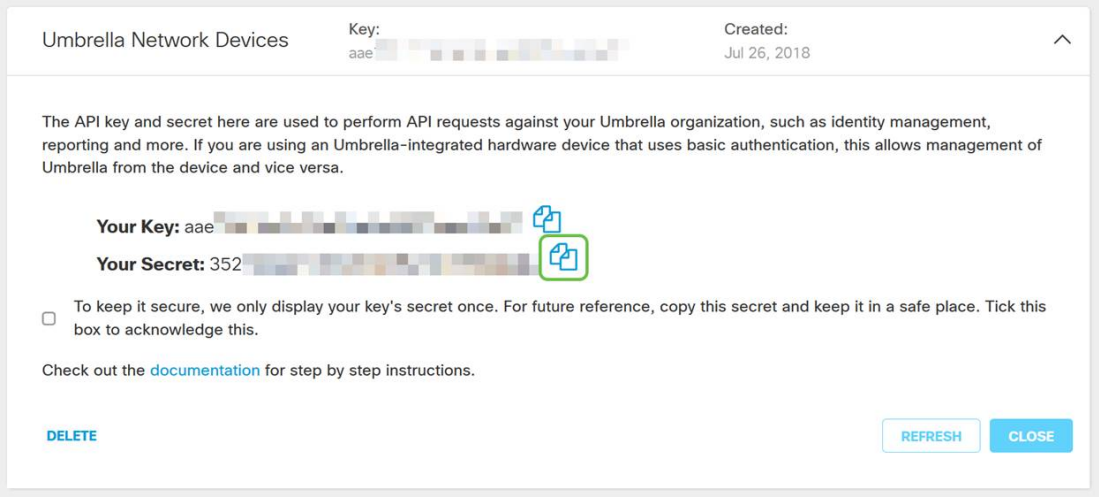
Passaggio 2. Fare clic sul pulsante **Add API Key** nell'angolo in alto a destra oppure fare clic sul pulsante **Create API Key**. Funzionano entrambi allo stesso modo.



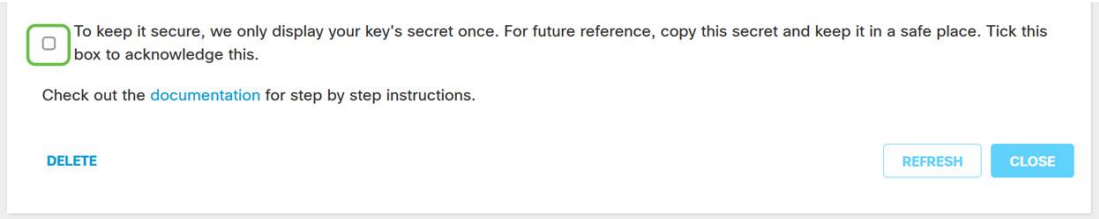
Passaggio 3. Selezionare **Umbrella Network Devices** e fare clic sul pulsante **Create**.



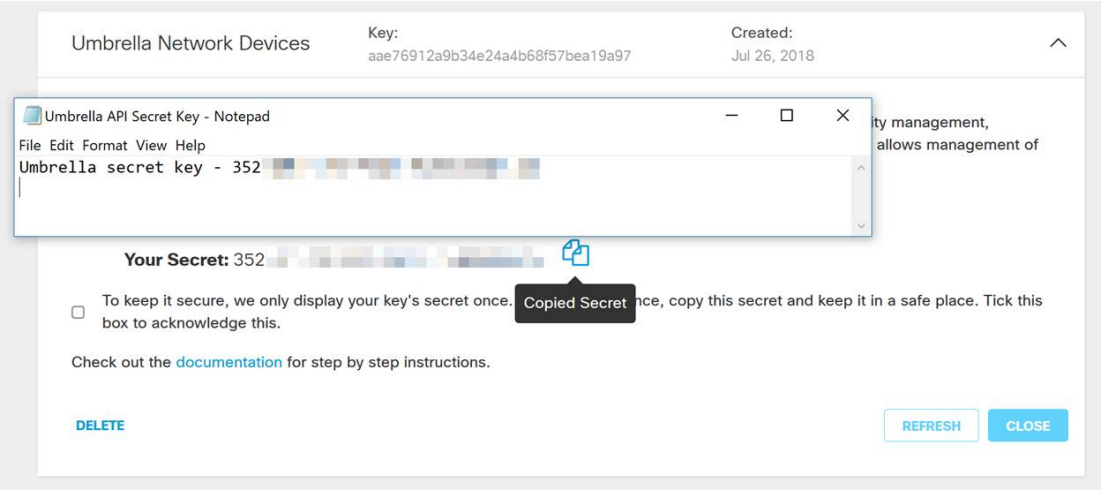
Passaggio 4. Fare clic sul pulsante **Copia** a destra della *chiave segreta.* Una notifica a comparsa confermerà che la chiave è stata copiata negli Appunti.



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 5. 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.



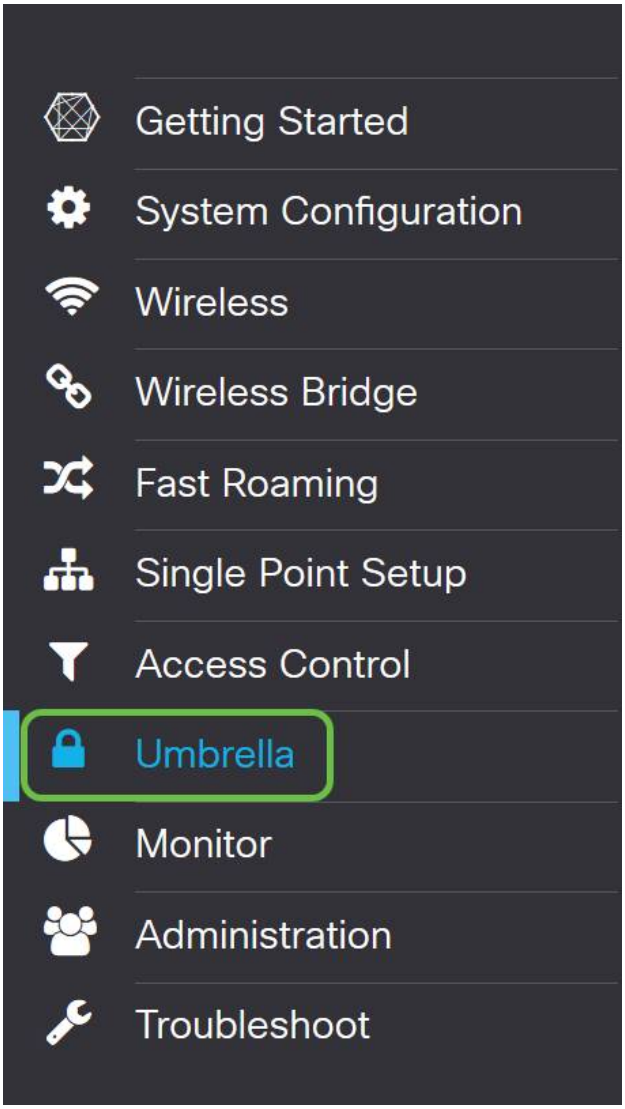
Nota importante: Se si perde o si elimina accidentalmente la chiave segreta, non sarà disponibile alcuna funzione o numero di supporto da chiamare per recuperare la chiave. Tienilo segreto, tienilo al sicuro. In caso di perdita, sarà necessario eliminare la chiave e autorizzare nuovamente la chiave API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

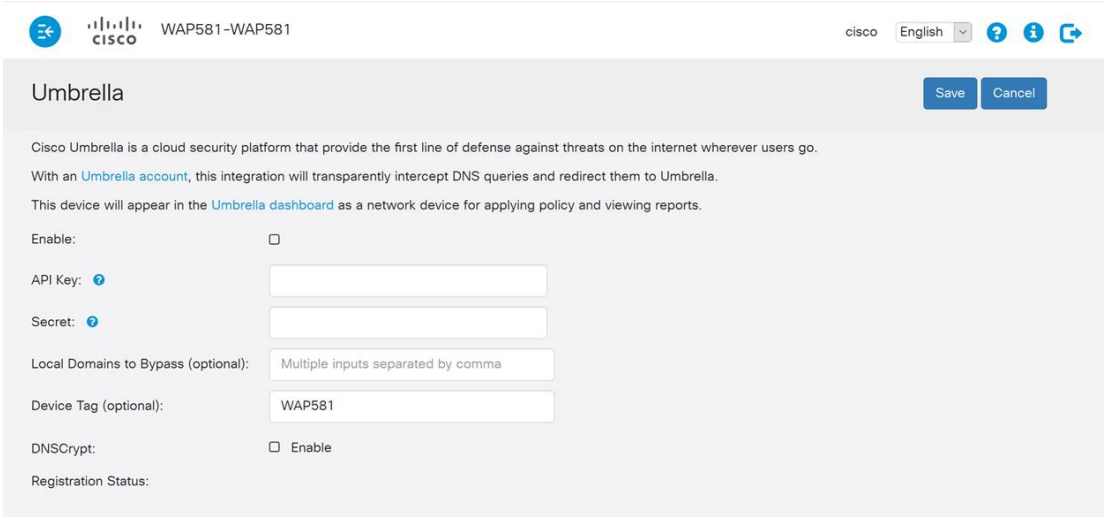
Ora che abbiamo creato le chiavi API in Umbrella, le prenderemo e le installeremo sui nostri dispositivi WAP. Nel nostro caso stiamo utilizzando un WAP581.

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

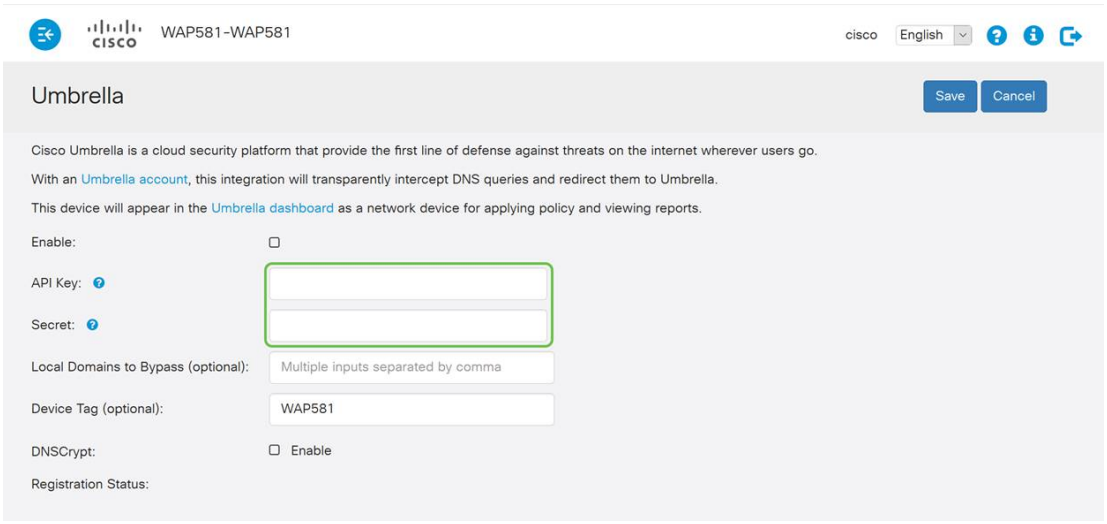


Passo 2. La schermata Umbrella è semplice, ma ci sono due campi che vale la pena definire qui:

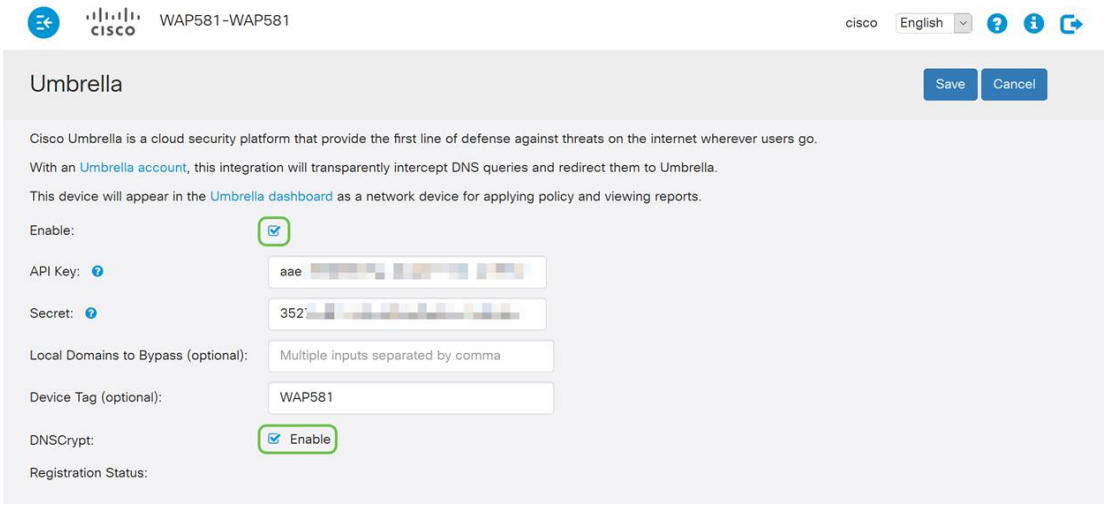
- *Domini locali da ignorare*: questo campo contiene i domini interni che si desidera escludere dal servizio Umbrella.
- *DNSCrypt:* protegge il trasferimento di pacchetti tra il client DNS e il resolver DNS. Questa funzionalità è attiva per impostazione predefinita. Se la si disattiva, la rete sarà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



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

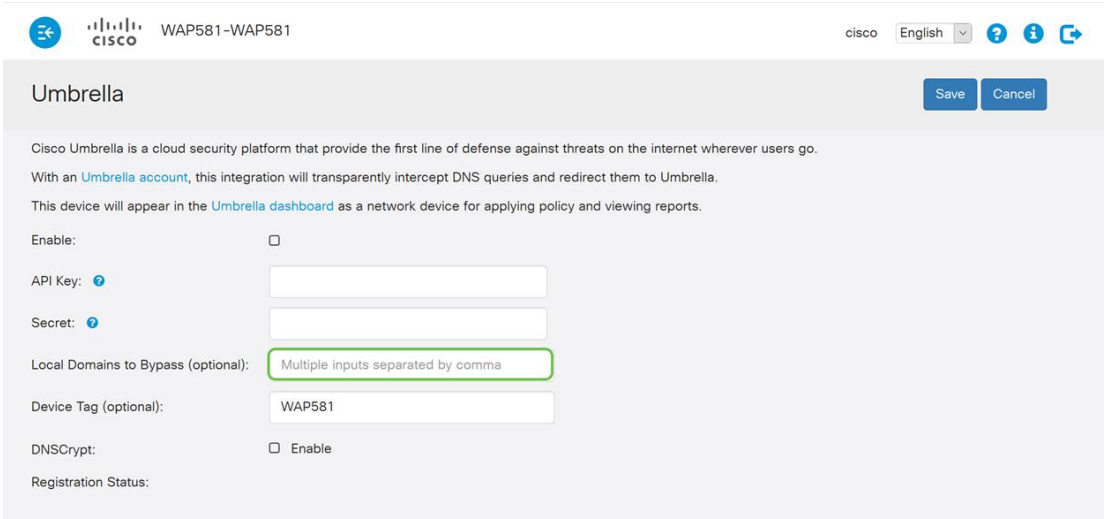


Passaggio 4. Verificare che le caselle di controllo **Enable** e **DNSCrypt** siano attivate o disattivate.



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

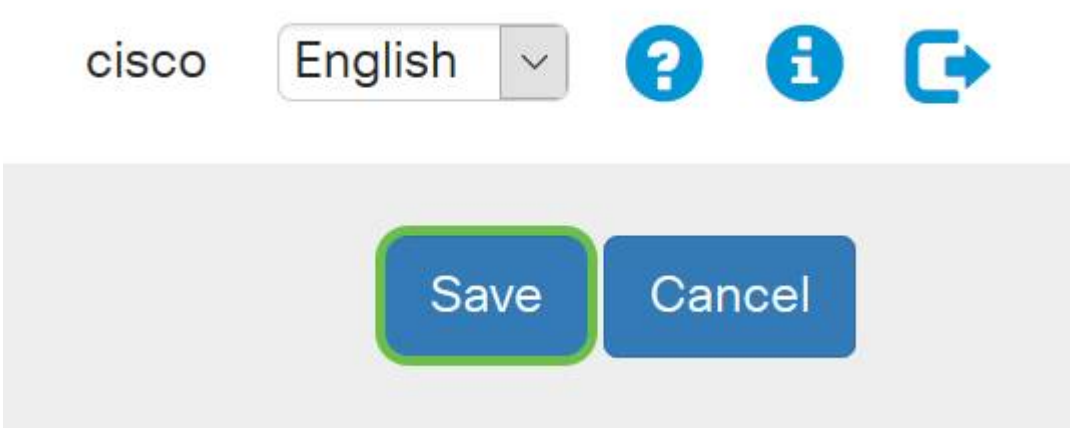
Passaggio 5. (Facoltativo) Immettere i domini locali che Umbrella deve consentire tramite il processo di risoluzione DNS.



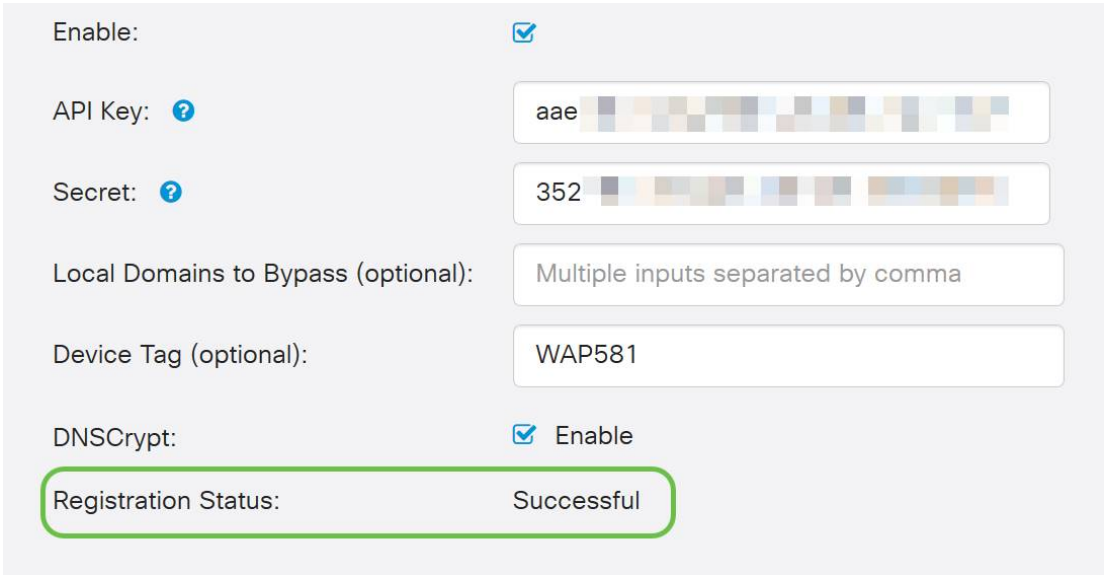
Nota: Questa operazione è obbligatoria per tutti i domini Intranet e per i domini DNS divisi. Se la rete richiede l'utilizzo di domini locali per il routing, sarà necessario contattare il supporto Umbrella per rendere operativa questa funzionalità. La maggior parte degli utenti non deve utilizzare questa

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.



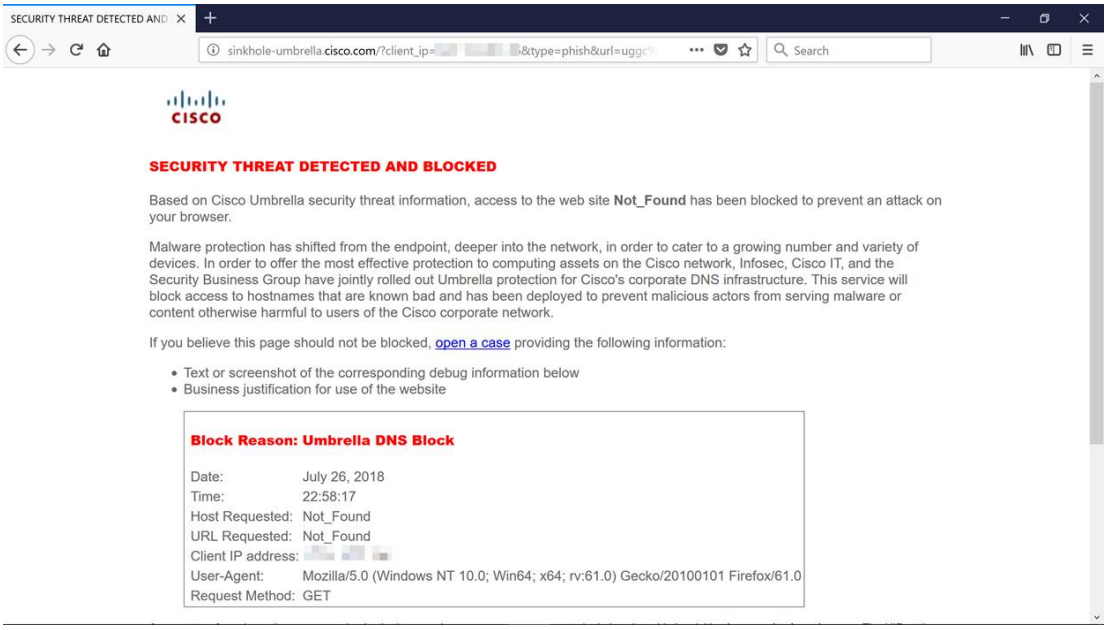
Passaggio 7. Al termine delle modifiche, nel campo *Stato registrazione* verrà visualizzato "Operazione riuscita".



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!



Qui è disponibile un video relativo a questo articolo...

[Fare clic qui per visualizzare altre Tech Talks di Cisco]