Hoe: Uitbreiding van Cisco Umbrella om uw draadloze netwerk te beschermen

Inleiding

Gegevensbeveiliging is een groepsinspanning bij elke organisatie. Werknemers zijn ten minste gedeeltelijk verantwoordelijk om ervoor te zorgen dat ze niet ten prooi vallen aan oplichterij. In de praktijk is veiligheid zwaar en het is geen wonder waarom. Terwijl de hulpmiddelen van de technologie hetzelfde doen voor de vooruitgang van hackers, stijgen alle boten met het getij om zo te spreken. Lees ook door om te leren hoe u Umbrella-bescherming op uw LAN kunt integreren.

Doel

Deze manier om u te begeleiden zal u de stappen tonen die bij het integreren van Umbrella's veiligheidsplatform in uw draadloos netwerk betrokken zijn. Voordat we in de details komen, zullen we een paar vragen beantwoorden die je jezelf kunt stellen over Umbrella.

Toepasselijke apparaten

- WAP125
- WAP581

Softwareversie

- 1.0.1

Vereisten

Een actieve Umbrella-account (heb je er geen? Offerte aanvragen of een gratis proces starten)

Wat is Umbrella?

Umbrella is een eenvoudig maar zeer effectief cloudbeveiligingsplatform van Cisco. Umbrella is actief in de cloud en voert veel beveiligingsgerelateerde services uit. Van opkomende dreiging tot onderzoek na een gebeurtenis. Umbrella ontdekt en voorkomt aanvallen in alle havens en protocollen.

Hoe werkt het?

Umbrella gebruikt DNS als hoofdvector voor defensie. Wanneer gebruikers een URL in hun browser bar invoeren en op ENTER klikken, neemt Umbrella deel aan de overdracht. Die URL gaat over naar de DNS-oplossing van Umbrella en als een veiligheidswaarschuwing aan het domein gekoppeld is, wordt het verzoek geblokkeerd. Deze telemetrie gegevensoverdracht en wordt geanalyseerd in microseconden, wat bijna geen latentie toevoegt. Telemetrie-gegevens gebruiken logbestanden en instrumenten om miljarden DNS-verzoeken overal ter wereld te volgen. Als deze gegevens alomtegenwoordig zijn, kan correlatie ermee over de hele wereld een snelle reactie op aanvallen mogelijk maken vanaf het moment dat ze beginnen. Zie het

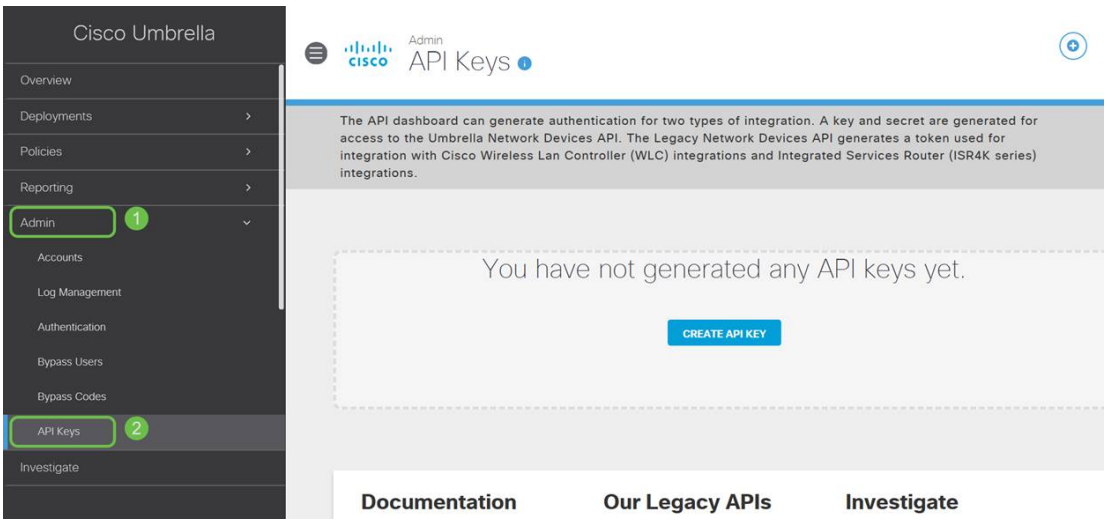
privacybeleid van Cisco hier voor meer informatie - het volledige beleid, samenvattende versie. Denk aan telemetrie data als data afgeleid van tools en logs.

Om samen te vatten in een metafoor, stel je voor dat je op een feestje bent. Op dit feestje is iedereen aan de telefoon die op het web surft. De rust in de groep wordt gekenmerkt door de aanwezigheid van partijbezoekers die op hun schermen aftapen. Het is geen geweldig feest, maar terwijl je aan je eigen telefoon een hyperlink naar een katje GIF ziet die onweerstaanbaar lijkt. U weet echter niet of u wel of niet moet tikken, omdat de URL betwistbaar lijkt. Dus voordat je de hyperlink aanspreekt, schreeuwde je naar de rest van het feest "Is deze link slecht?" Als een andere persoon op het feestje naar de link was geweest en ontdekte dat het een oplichterij was, dan schreeuwden ze terug "Ja, dat heb ik gedaan en het is oplichterij!" Bedankt dat hij je gered heeft, door te gaan met je zoektocht naar foto's van schattige dieren in stilte. Natuurlijk, op de schaal van Cisco dit type van verzoek en de controles van de callback veiligheid komen miljoenen keren per seconde voor.

Klinkt geweldig, hoe doen we dit af?

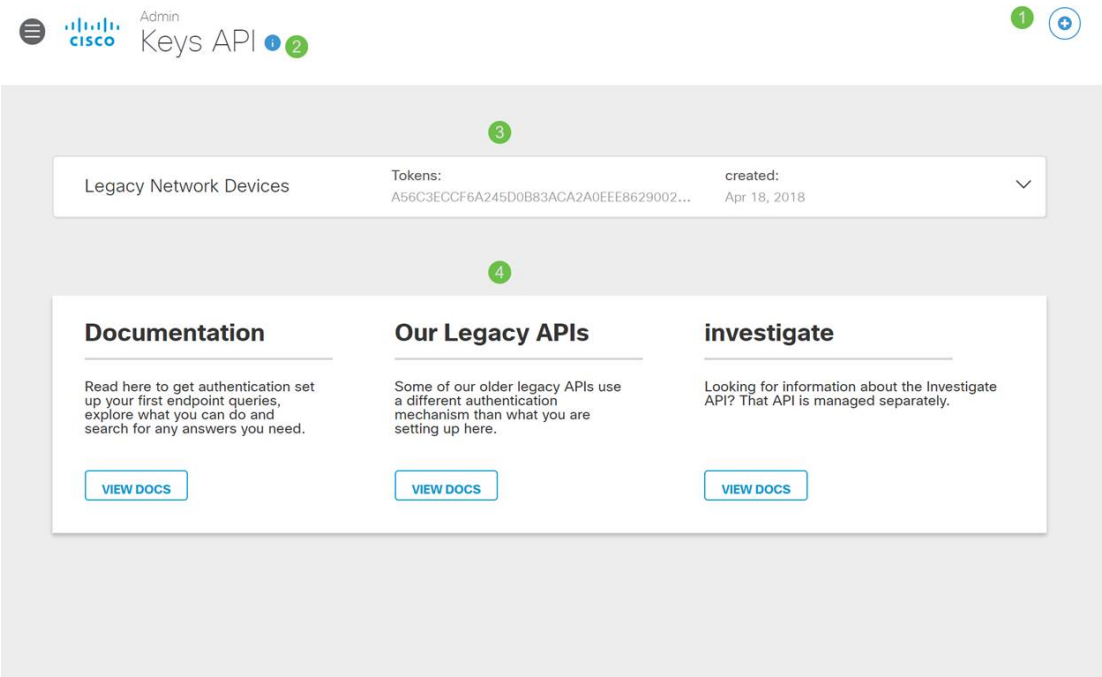
Waar deze handleiding navigeert, begint door de API-toets en de geheime toets van uw Umbrella-accountdashboard te grepen. Na, zullen we inloggen op uw WAP apparaat om de API en de Secret-toets toe te voegen. Als u problemen hebt, controleert u hier op documentatie en hier op de opties voor Umbrella Support.

Stap 1. Na het loggen in uw Umbrella-account klikt u op **Admin > API-toetsen** op het *Dashboard*.

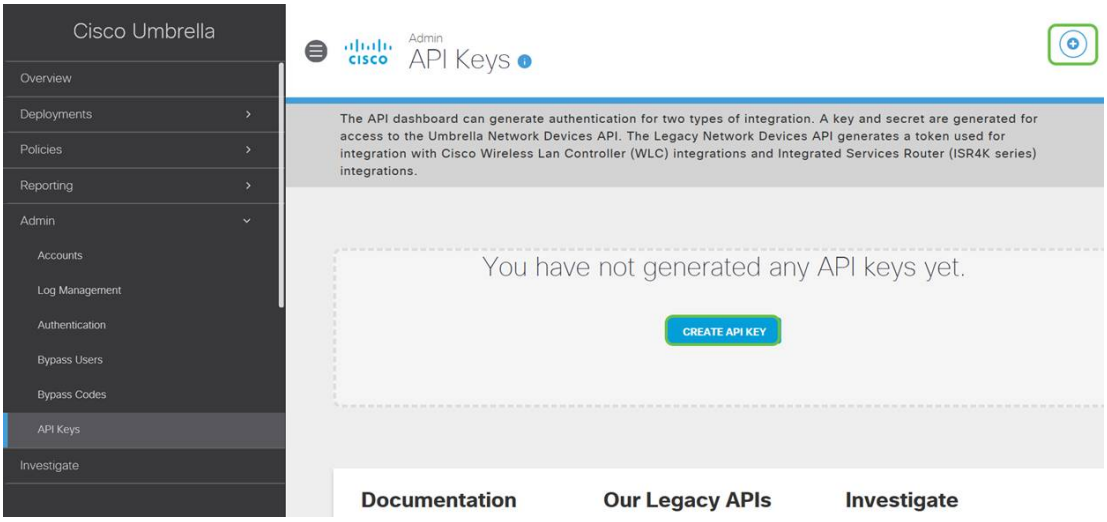


Anatomie van het API-toetsenbord -

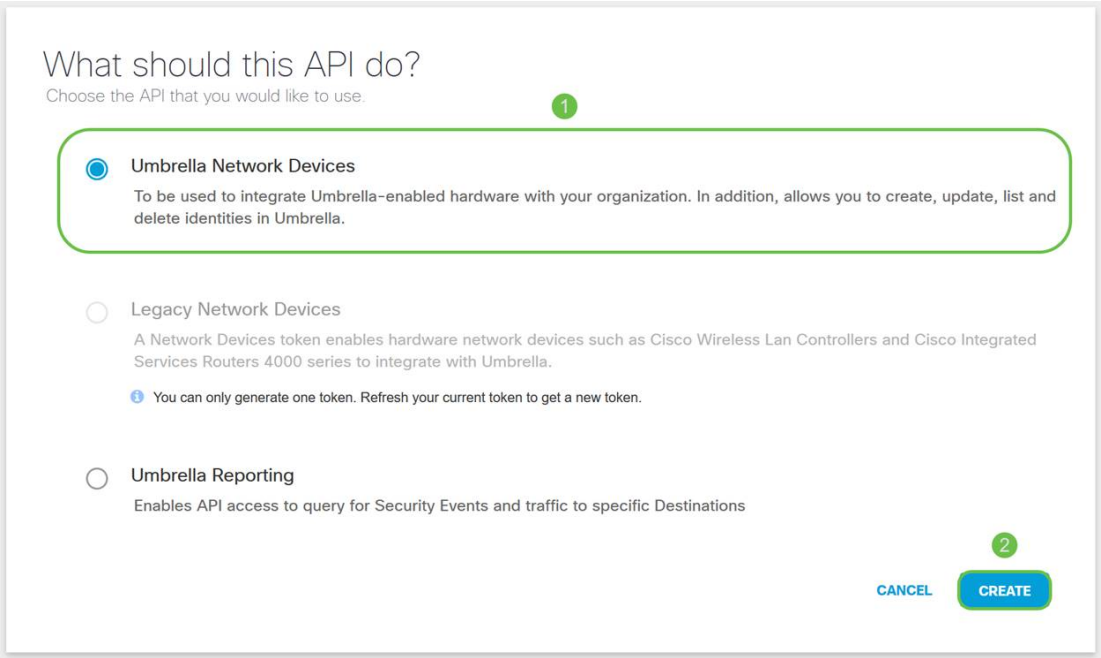
1. *Add API Key* - Hiermee wordt de creatie van een nieuwe toets voor gebruik met de Umbrella API gestart.
2. *Aanvullende informatie* - Gaat omlaag/omhoog met een toelichting op dit scherm.
3. *Token Well* - Bevat alle sleutels en penningen die door deze account zijn gemaakt. (Populaten zodra een sleutel is gecreëerd)
4. *Ondersteunende documenten* - links naar documentatie op de Umbrella-site met betrekking tot de onderwerpen in elke sectie.



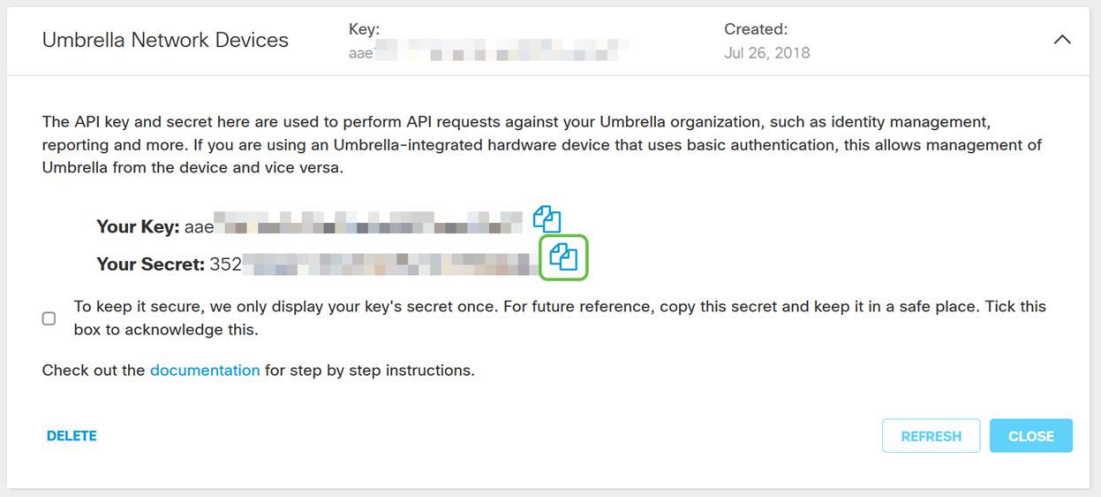
Stap 2. Klik op de knop **API-**sleutel **toevoegen** in de rechterbovenhoek of klik op de knop **API-**toets **maken**. Ze functioneren allebei hetzelfde.



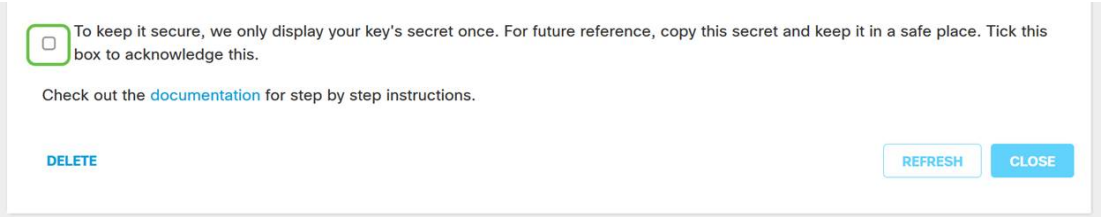
Stap 3. Selecteer **Umbrella Network Devices** en klik vervolgens op de knop **Create**.



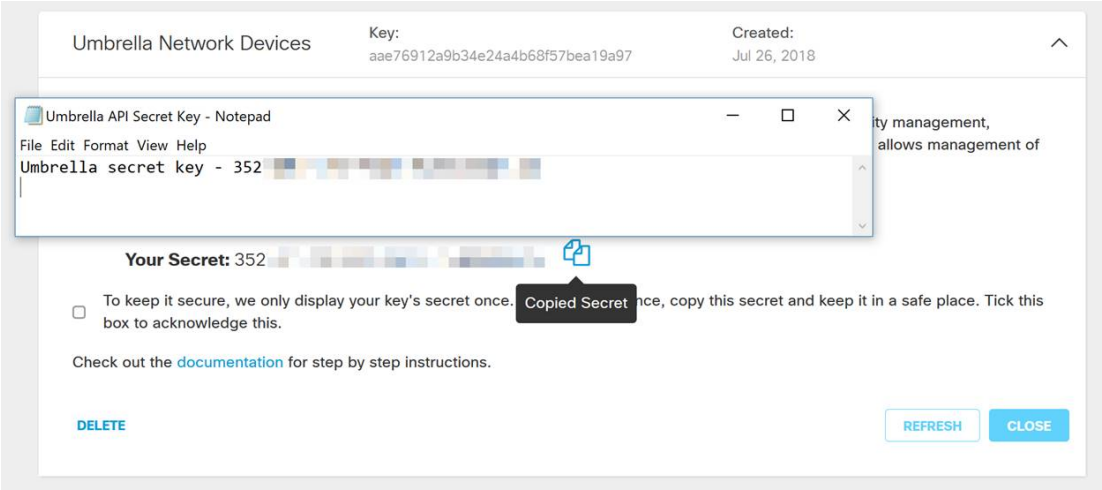
Stap 4. Klik op de knop **Kopie** rechts van uw *beveiligingssleutel.* Een pop-upbericht zal bevestigen dat de toets naar uw klembord is gekopieerd.



Nadat u de sleutel en de geheime sleutel naar een veilige plaats hebt gekopieerd, klikt u op het ***selectieteken*** om te bevestigen dat u de herkenning wilt voltooien en vervolgens klikt u op de knop **Sluiten**.



Stap 5. Open een teksteditor zoals een schrijfblok en plak uw geheime en API-toets in het document, label ze voor raadpleging in de toekomst. In dit geval is het label "Umbrella gehesen sleutel". Voeg de API-toets met uw geheime sleutel toe samen met een korte beschrijving van het gebruik ervan in hetzelfde tekstbestand. Sla het tekstbestand vervolgens op een beveiligde locatie die makkelijk toegankelijk is, indien u dit nodig hebt.



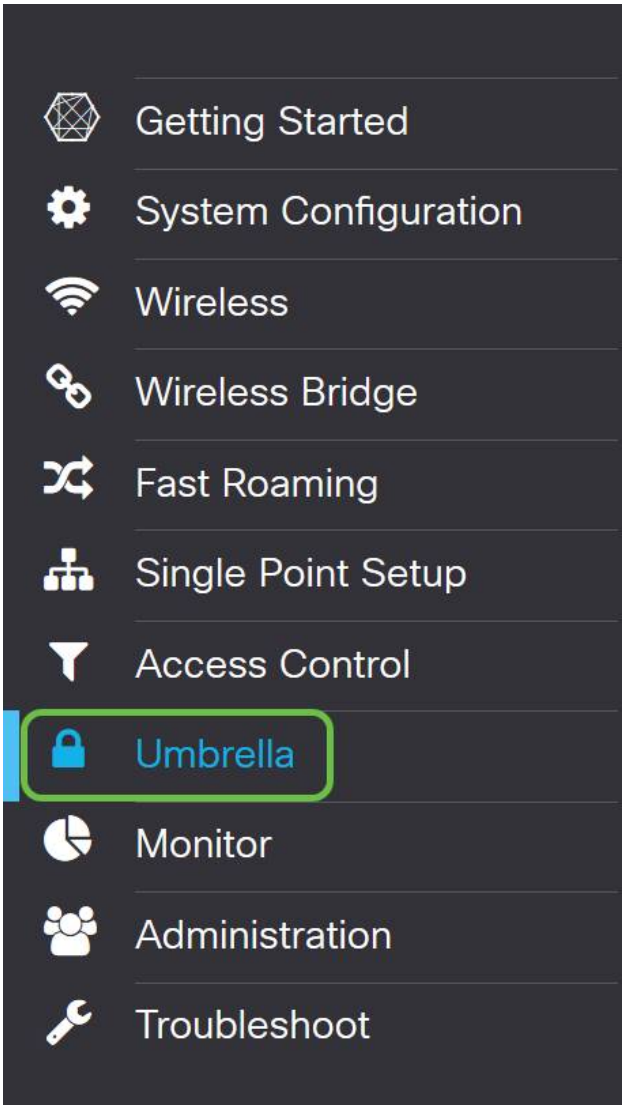
Belangrijke opmerking: Als u de geheime toets kwijtraakt of per ongeluk verwijdert, is er geen functie of ondersteuningsnummer om deze toets te bellen. Houd het geheim, hou het veilig. Indien verloren, moet u de toets verwijderen en de API-toets opnieuw autoriseren met elk WAP-apparaat dat u met Umbrella wilt beveiligen.

Best Practice: Bewaar slechts *één* exemplaar van dit document op een apparaat, zoals een USB-duimschijf, ontoegankelijk vanaf een netwerk.

Umbrella op uw WAP-apparaat configureren

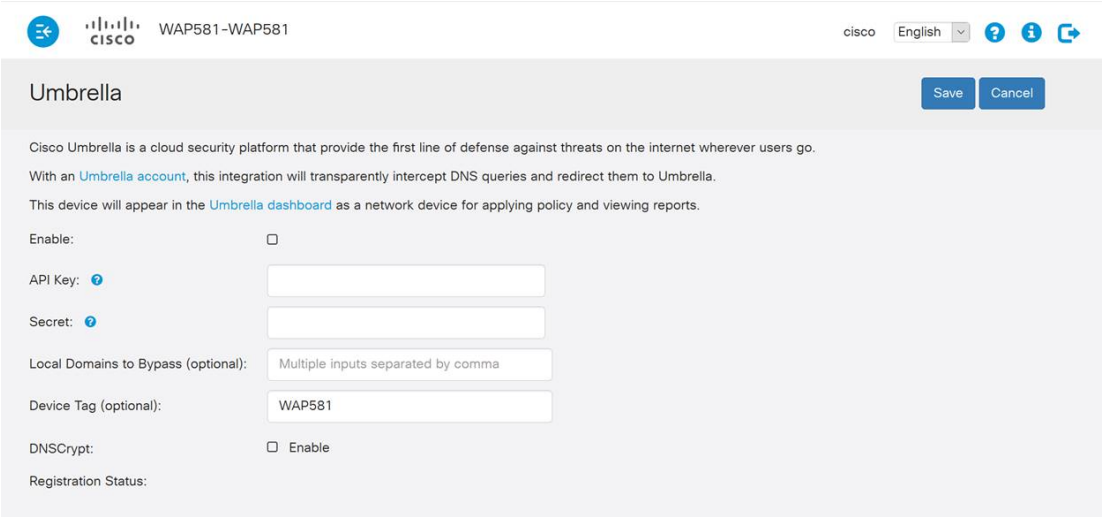
Nu we API-toetsen hebben gemaakt in Umbrella, nemen we deze toetsen en installeren ze op onze WAP-apparaten. In ons geval gebruiken we een WAP581.

Stap 1. Klik na het loggen in uw WAP-apparaat op **Umbrella** in het menu Sidebar.

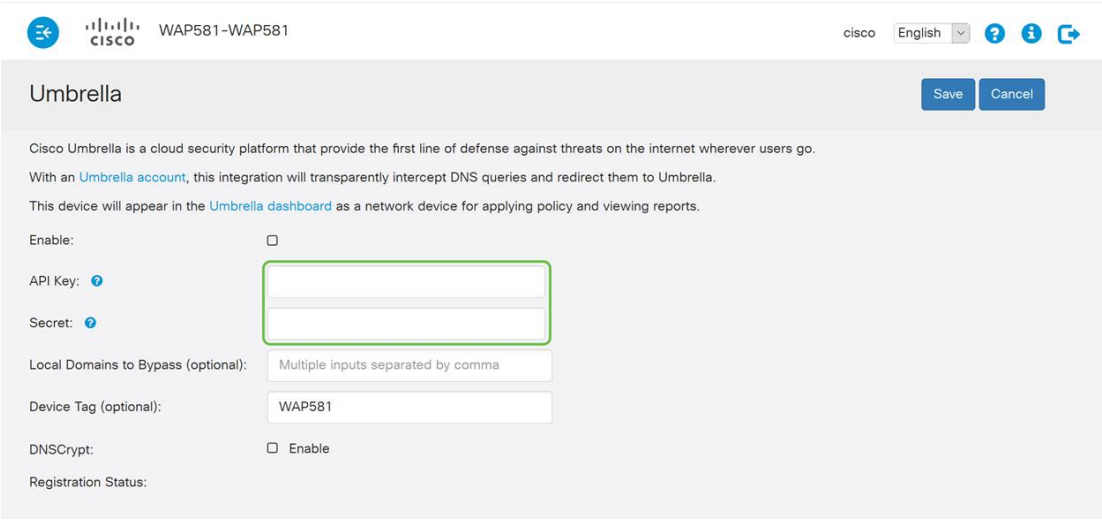


Stap 2. Het Umbrella-scherm is duidelijk, maar er zijn twee velden die het waard zijn om hier te definiëren:

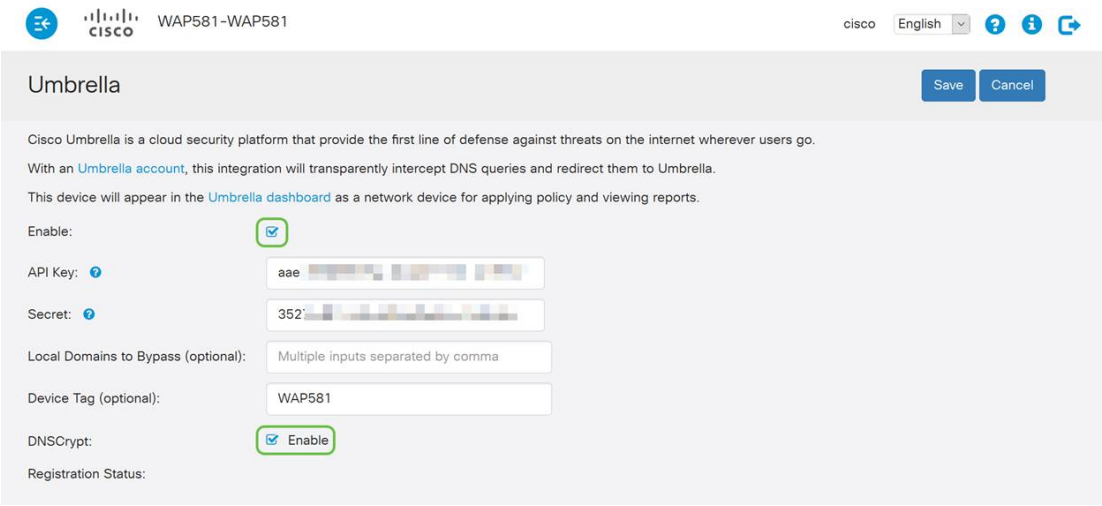
- *Local Domein to Bypass* - Dit veld bevat uw interne domeinen die u wilt uitsluiten van de Umbrella-service.
- *DNSCrypt* - Beveiliging van de overdracht van pakketten tussen de DNS-client en de DNS-oplossing. Deze optie is standaard ingeschakeld door deze optie uit te schakelen. Dit maakt uw netwerk minder veilig.



Stap 3. Plakt uw API- en geheime sleutel in de corresponderende velden.

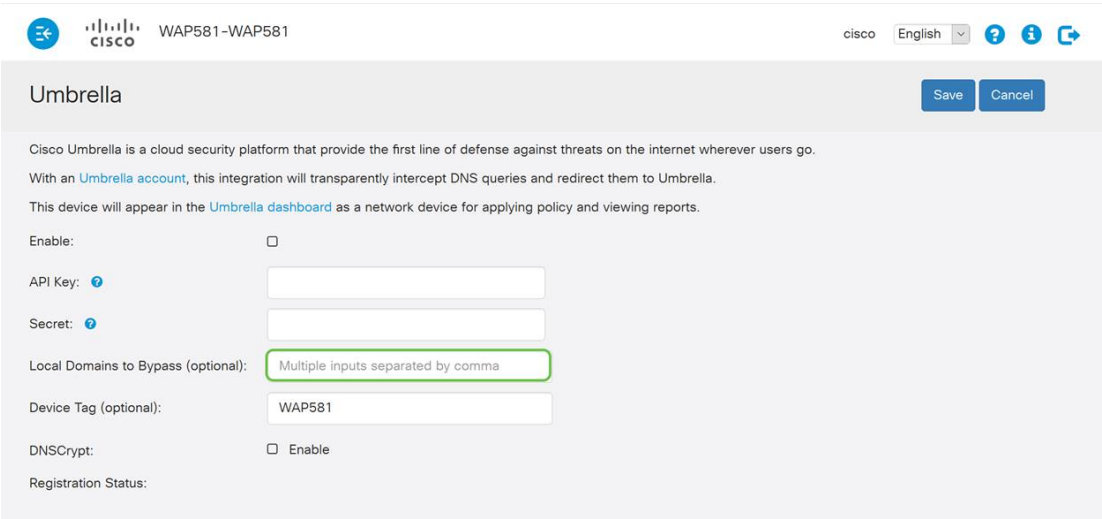


Stap 4. Verzeker u dat de selectietekens voor **Enable** and **DNSCrypt** de controlestaat zijn ingedrukt.



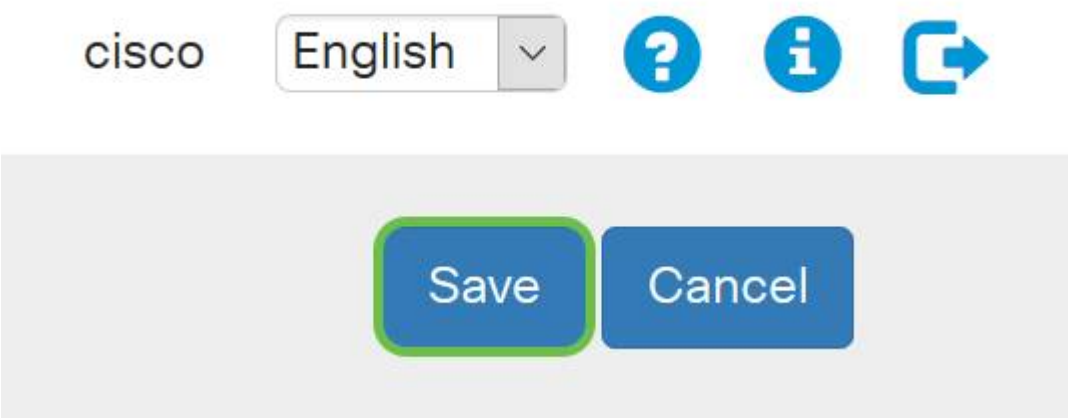
Opmerking: DNSCrypt waarborgt DNS communicatie tussen een DNS client en een DNS resolutie. Standaard is ingeschakeld.

Stap 5. (Optioneel) Voer de lokale domeinen in die u wilt dat Umbrella doorheen het DNS-resolutieproces toestaat.

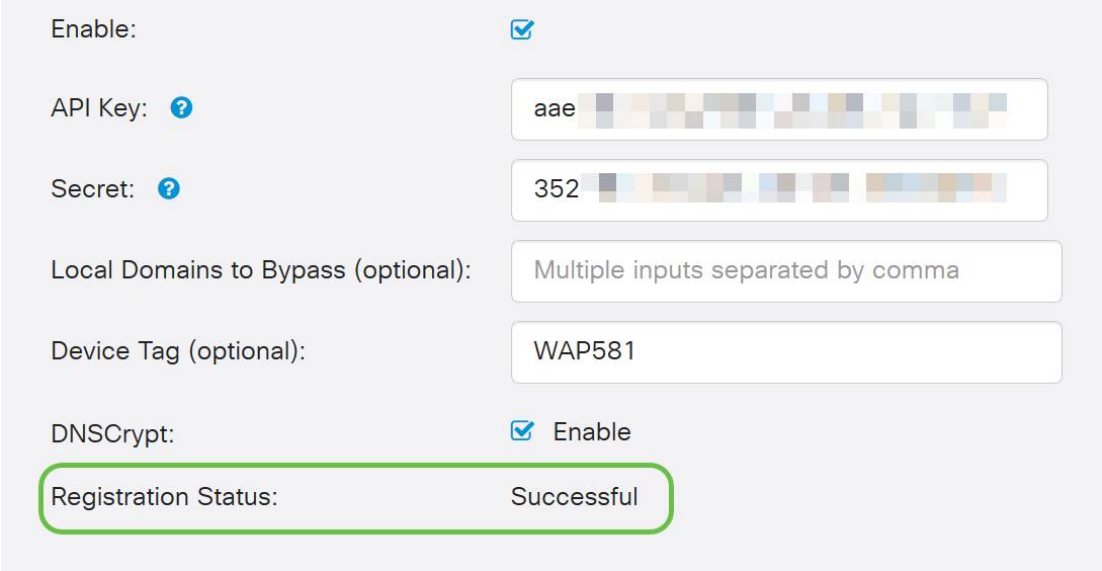


Opmerking: Dit is vereist voor alle intranet domeinen en gesplitste DNS-domeinen. Als uw netwerk het gebruik van lokale gebiedsdomeinen voor het routing nodig heeft, moet u contact opnemen met de ondersteuning van Umbrella om deze functie in bedrijf te stellen. De meeste gebruikers hoeven deze optie niet te gebruiken.

Stap 6. Nadat u tevreden bent met de wijzigingen of uw eigen *lokale domein aan* Bypass hebt toegevoegd, klikt u in de rechterbovenhoek op de knop **Opslaan**.



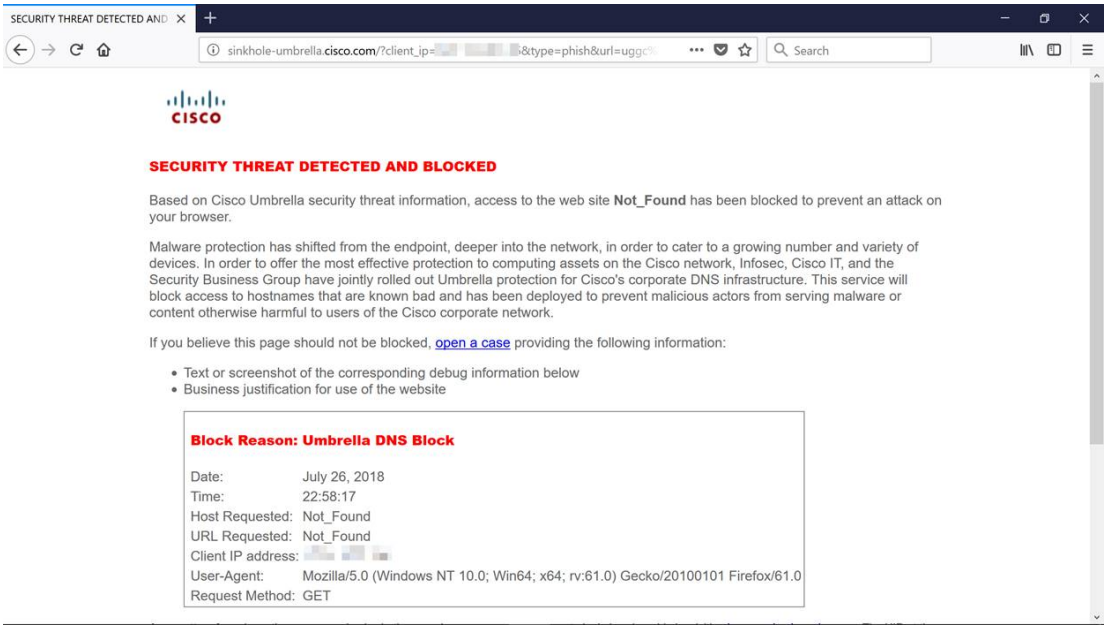
Stap 7. Wanneer de wijzigingen zijn voltooid, wordt de *Registratiestatus* van het veld "Succesvol" gelezen.



Alles bevestigen is op zijn juiste plaats

Gefeliciteerd, u bent nu beschermd de Umbrella van Cisco. Of ben jij? Zeker, Cisco heeft een website gemaakt die dit zo snel mogelijk moet bepalen als de pagina oplaadt. Klik hier of type https://InternetBadGuys.com in de browser bar.

Als Umbrella goed is ingesteld, wordt u op dezelfde manier begroet door een scherm!



Bekijk een video gerelateerd aan dit artikel...

Klik hier om andere Tech Talks uit Cisco te bekijken