

# RV34xシリーズルータによるネットワーク上でのCisco Umbrellaの設定

## 概要

ファームウェアバージョン1.0.0.2.16以降、RV34xシリーズルータはCisco Umbrellaをサポートするようになりました。Umbrellaは、マルウェアやデータの侵入に対する防御のベクトルまたはシールドとしてDNSを使用します。

## 該当するデバイス

- RV34xシリーズルータ

## [Software Version]

- 1.0.02.16

## 要件

- アクティブなUmbrellaアカウント(持っていない? [見積もりを依頼する](#)か、[無料トライアルを開始します](#))

## 目的

このガイドでは、Umbrellaのセキュリティプラットフォームをネットワークに統合するための手順を説明します。詳細を説明する前に、Umbrellaに関する質問にお答えします。

## 傘とは何ですか。

Umbrellaは、シスコが提供するシンプルでありながら非常に効果的なクラウドセキュリティプラットフォームです。Umbrellaはクラウドで動作し、多くのセキュリティ関連サービスを実行します。新たな脅威からイベント後の調査まで。Umbrellaは、すべてのポートとプロトコルに対する攻撃を検出して防止します。

## この仕組みを説明しましょう

Umbrellaは防御のメインベクトルとしてDNSを使用します。ユーザがブラウザバーにURLを入力してEnterキーを押すと、Umbrellaが転送に参加します。このURLはUmbrellaのDNSリゾルバに渡され、セキュリティ警告がドメインに関連付けられている場合、要求はブロックされます。このテレメトリデータはマイクロ秒単位で転送および分析されるため、遅延はほとんど発生しません。テレメトリデータは、世界中の何十億ものDNS要求を追跡するログと機器を使用します。このデータが世界中に広がっている場合、世界中でデータに関連付けることで、攻撃の開始時に迅速に対応できます。[完全なポリシー](#)、[概要バージョン](#)の詳細については、シスコのプライバシーポリシーを参照してください。テレメトリデータ

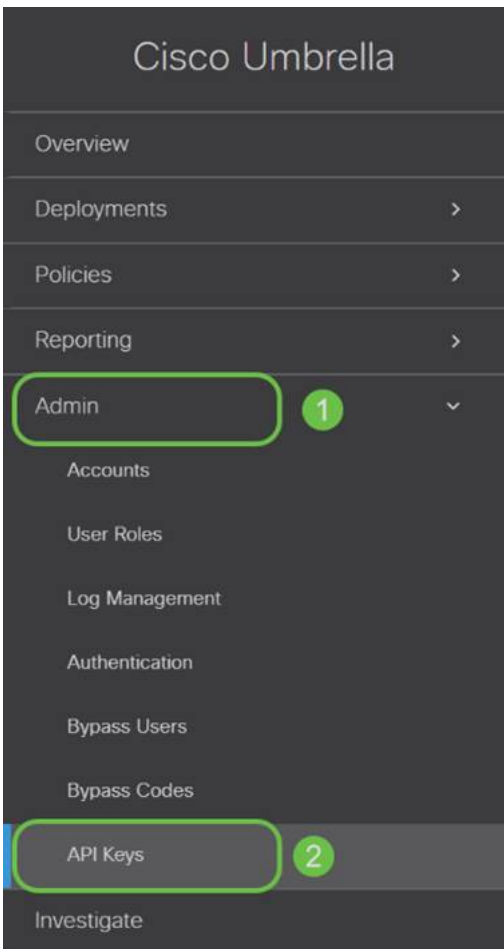
は、ツールやログから得られるデータと考えてください。

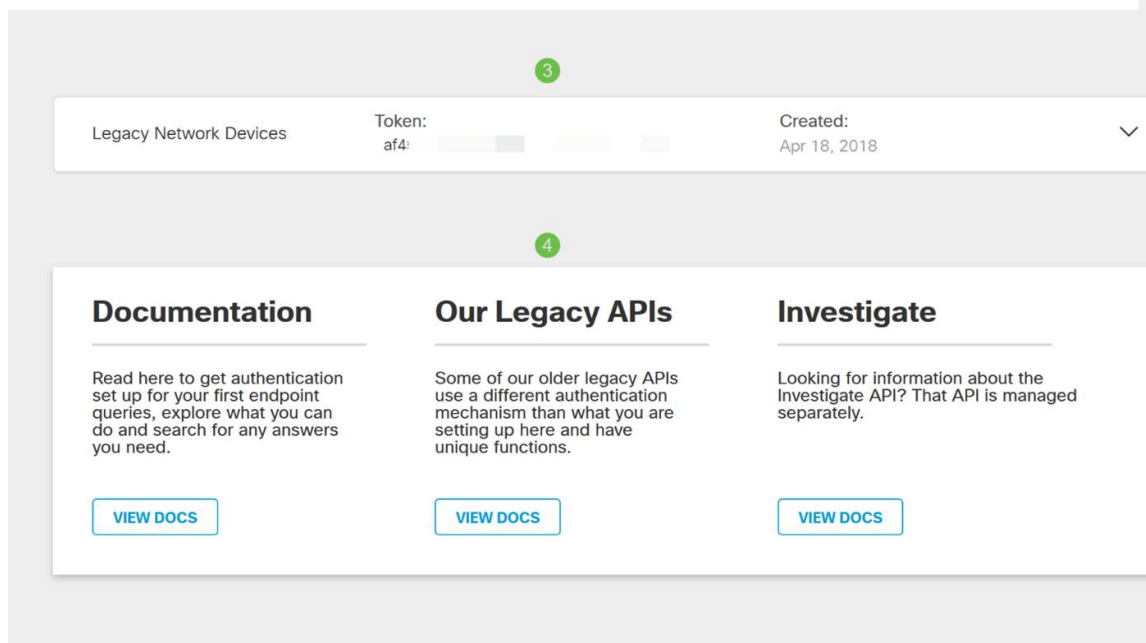
メタファーでまとめると、あなたがパーティーにいと想像してください。このパーティーでは、誰もが電話でWebを閲覧しています。静かなグループの沈黙は、パーティー参加者が画面をタップして離れることで中断されます。[それは素晴らしいパーティーではないが](#)、自分の携帯電話では魅力的に思える子猫GIFへのハイパーリンクが表示されます。しかし、URLが疑わしいので、タップすべきかどうか分からない。ハイパーリンクをタップする前に、「このリンクは悪いですか？」と相手に叫びます。もし他の人がリンクに行って、それが詐欺だと分かったら、彼らは叫んで叫ぶだろう「うん、私がやったし、それは詐欺だ！かわいい動物の写真を探し続け、あなたを救ってくれたその人に感謝します。もちろん、シスコの規模では、このタイプの要求およびコールバックセキュリティチェックは1秒間に何百万回も行われています。これは、ネットワーク上のセキュリティのメリットです。

## いいねどうやって始める？

このガイドのナビゲーションでは、まずUmbrellaアカウントダッシュボードからAPIキーとシークレットキーを取得します。その後、ルータデバイスにログインして、APIと秘密キーを追加します。問題が発生した場合は、[ドキュメント](#)を確認し、[Umbrellaサポート](#)オプションを確認してください。

ステップ1:Umbrellaアカウントにログインした後、[Dashboard] 画面で[Admin] > [API Keys] をクリックします。

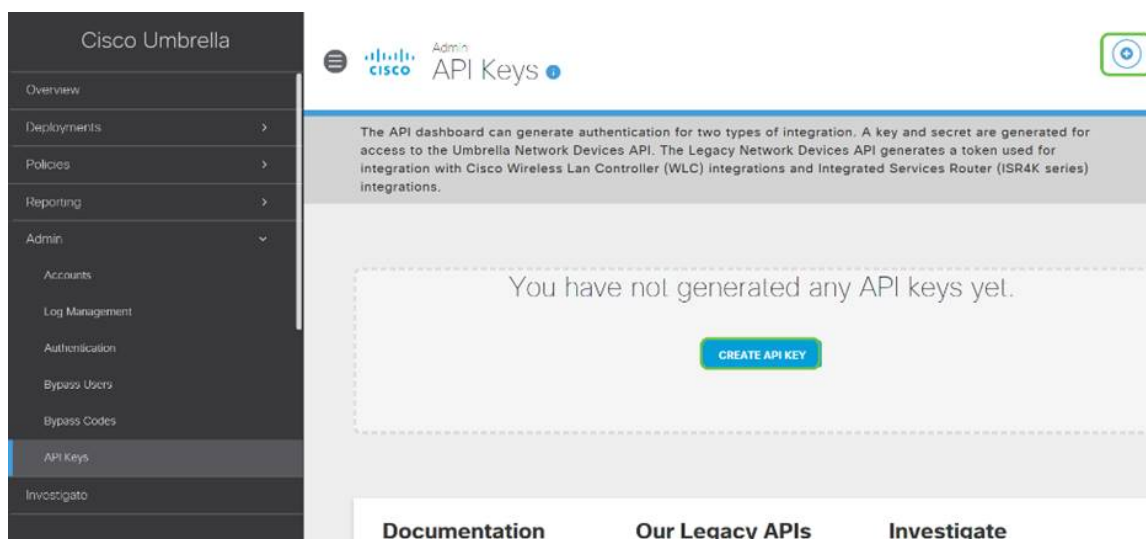




## APIキー画面の構造 ( 既存のAPIキーを使用 ) :

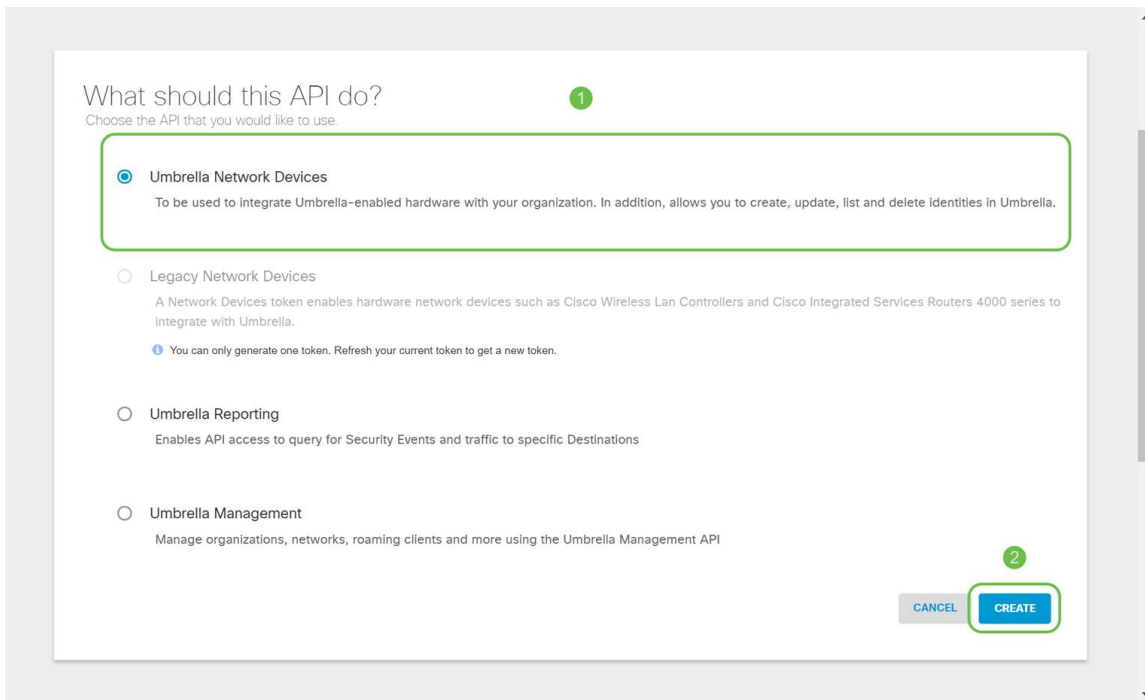
1. APIキーの追加 : Umbrella APIで使用する新しいキーの作成を開始します。
2. 追加情報 – この画面の説明文を上下にスライドします。
3. Token Well : このアカウントによって作成されたすべてのキーとトークンが含まれます。  
( キーが作成されると入力されます )
4. サポートドキュメント – 各セクションのトピックに関連するUmbrellaサイトのドキュメントへのリンク。

ステップ2 : 右上隅の[Add API Key] ボタンをクリックするか、[Create API Key] ボタンをクリックします。両方とも同じように機能します。

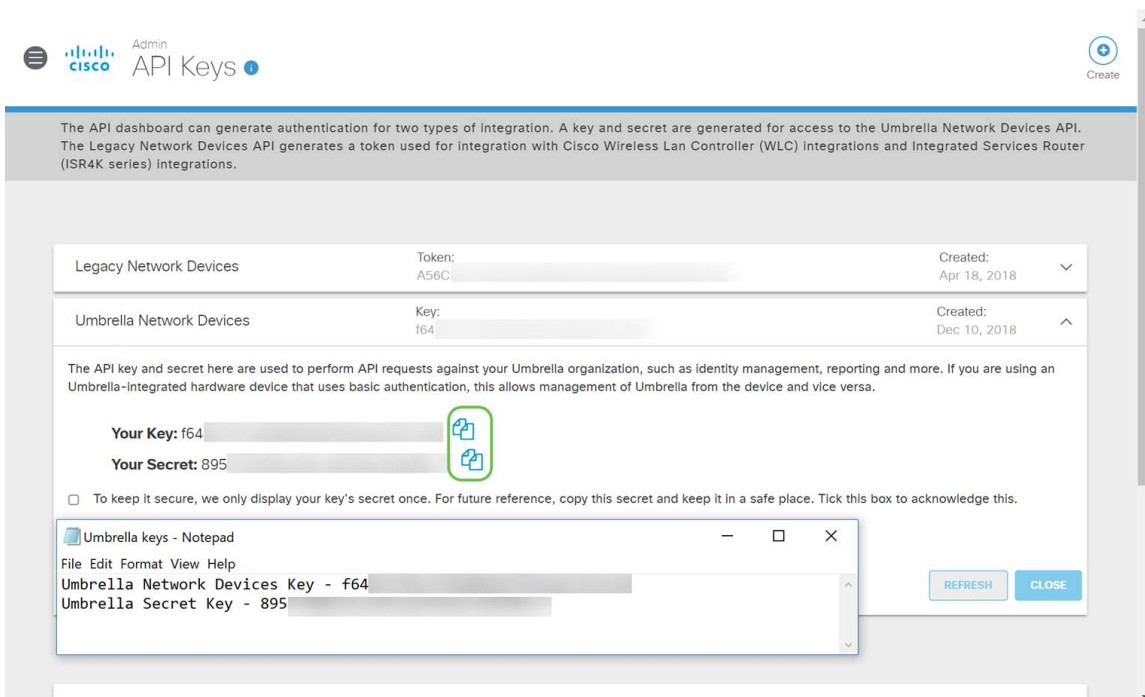


注 : 上のスクリーンショットは、このメニューを初めて開く場合と同様です。

ステップ3:[Umbrella Network Devices] を選択し、[Create] ボタンをクリックします。



ステップ4：メモ帳などのテキストエディタを開き、APIとAPIの秘密キーの右側にある [Copy] ボタンをクリックします。キーがクリップボードにコピーされたことを確認するポップアップ通知が表示されます。一度に1つずつ、秘密キーとAPIキーをドキュメントに貼り付け、後で参照できるようにラベルを付けます。この場合、ラベルは「Umbrella network devices key」です。その後、後でアクセスしやすい安全な場所にテキストファイルを保存します。



ステップ5：キーと秘密キーを安全な場所にコピーしたら、[Umbrella API] 画面でチェックボックスをクリックして秘密キーの一時的な表示の確認を完了したことを確認し、[Close] ボタンをクリックします。

To keep it secure, we only display your key's secret once. For future reference, copy this secret and keep it in a safe place. Tick this box to acknowledge this.

1 Check out the [documentation](#) for step by step instructions.

DELETE

REFRESH CLOSE

**重要事項：秘密キーを紛失したり、誤って削除した場合、このキーを取得するために呼び出す機能やサポート番号はありません。秘密を守り、安全を守れ。**紛失した場合は、キーを削

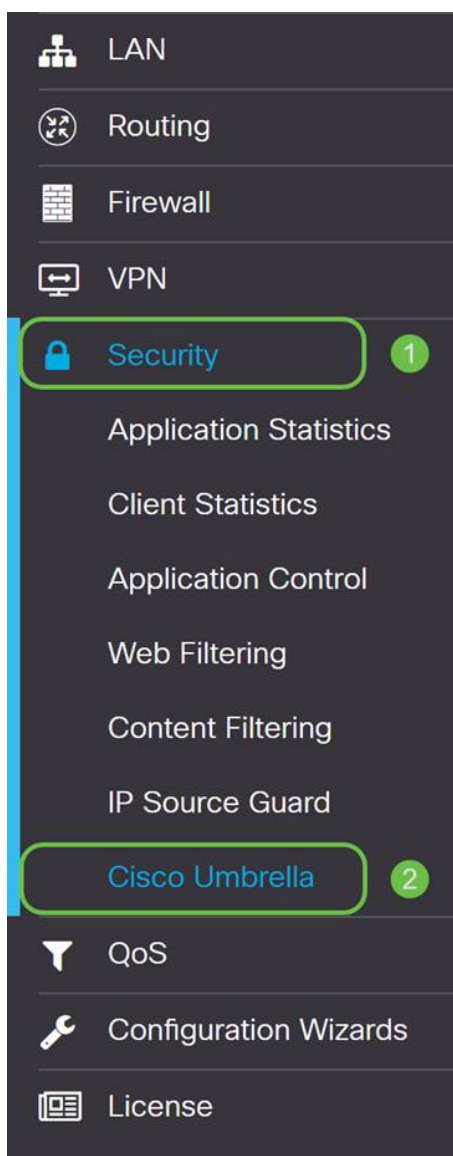
除し、Umbrellaで保護する各デバイスで新しいAPIキーを再認証する必要があります。

**ベストプラクティス:**このドキュメントのコピーをUSBサムドライブなどのデバイスに保存し、ネットワークからアクセスできないようにします。

## RV34xデバイスでのUmbrellaの設定

Umbrella内でAPIキーを作成したので、これらのキーを取得してRV34xデバイスにインストールします。この例では、RV340を使用しています。

ステップ1:RV34xデバイスにログインしたら、サイドバーメニューで[Security] > [Umbrella]をクリックします。



ステップ2:[Umbrella API]画面にはさまざまなオプションがあります。[Enable] チェックボックスをクリックして、Umbrellaの有効化を開始します。



## Cisco Umbrella

Cisco Umbrella is a cloud security platform that provides the first line of defense against threats on the internet. With an [Umbrella account](#), this integration will transparently intercept DNS queries and redirect them to Umbrella.

- Enable
- Block LAN DNS query

In [Umbrella Dashboard](#), you can create policies for different identities:

- If you use "Network" as this router's identity.
  - Go to [DNS-O-MATIC](#) website, create an account and add your OpenDNS account to it.
  - Go to [DNS-O-MATIC Settings](#) to enable DNS-O-MATIC so your WAN IP change can be propagated to O

### Advanced Configuration

Local Domain To Bypass  
(Optional):



DNSECrypt:

Enable

Public Key:

B735:1140:206F:225D:3E2B:D822:D7FD:691E:A1C3:3CC8:D666:8

- If you use "Network Device" as this router's identity. (Preferred, if available in your Umbrella subscription)

ステップ3: ( オプション ) デフォルトでは[Block LAN DNS Queries]ボックスが選択されています。この機能により、ルータ上にアクセスコントロールリストが自動的に作成され、DNSトラフィックがインターネットに送信されなくなります。この機能は、すべてのドメイン変換要求をRV34x経由で転送することを強制するため、ほとんどのユーザに適しています。

ステップ4: 次のステップでは、2つの異なる方法で再生されます。どちらもネットワークのセットアップに依存します。DynDNSやNoIPなどのサービスを使用する場合は、デフォルトの命名方式「Network」のままにしておきます。次に、これらのアカウントにログインして、Umbrellaが保護を提供するサービスとインターフェイスしていることを確認する必要があります。私たちの目的では、「ネットワークデバイス」を使用しています。下部のラジアルボタンをクリックしてください。

## Cisco Umbrella

Apply

Cancel

Cisco Umbrella is a cloud security platform that provides the first line of defense against threats on the internet wherever users go. With an [Umbrella account](#), this integration will transparently intercept DNS queries and redirect them to Umbrella.

- Enable
- Block LAN DNS query

In [Umbrella Dashboard](#), you can create policies for different identities:

- If you use "Network" as this router's identity.
- If you use "Network Device" as this router's identity. (Preferred, if available in your Umbrella subscription)

Getting Started

ステップ5:[Getting Started] をクリックして、ミニウィザードを開始します。

## Cisco Umbrella

Apply

Cancel

Cisco Umbrella is a cloud security platform that provides the first line of defense against threats on the internet wherever users go. With an [Umbrella account](#), this integration will transparently intercept DNS queries and redirect them to Umbrella.

- Enable
- Block LAN DNS query

In [Umbrella Dashboard](#), you can create policies for different identities:

- If you use "Network" as this router's identity.
- If you use "Network Device" as this router's identity. (Preferred, if available in your Umbrella subscription)

Getting Started

ステップ6 : 次に、テキストボックスにAPI KeyとSecret Keyを入力します。

### Enter Credentials

Key:

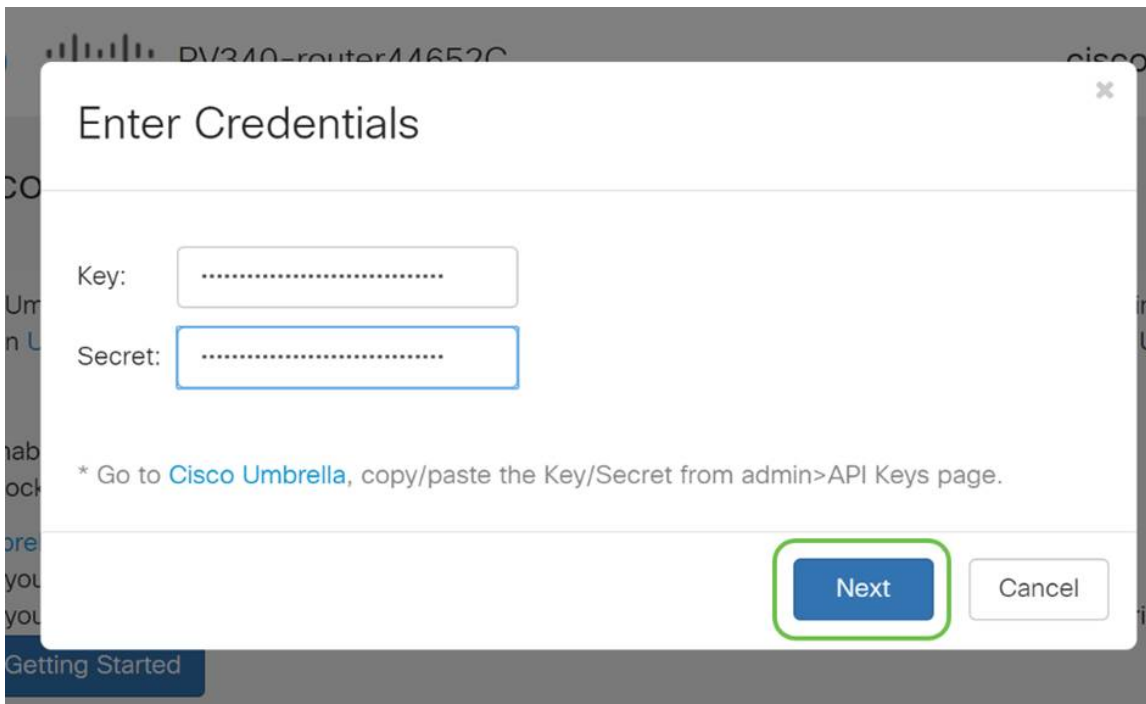
Secret:

\* Go to [Cisco Umbrella](#), copy/paste the Key/Secret from admin>API Keys page.

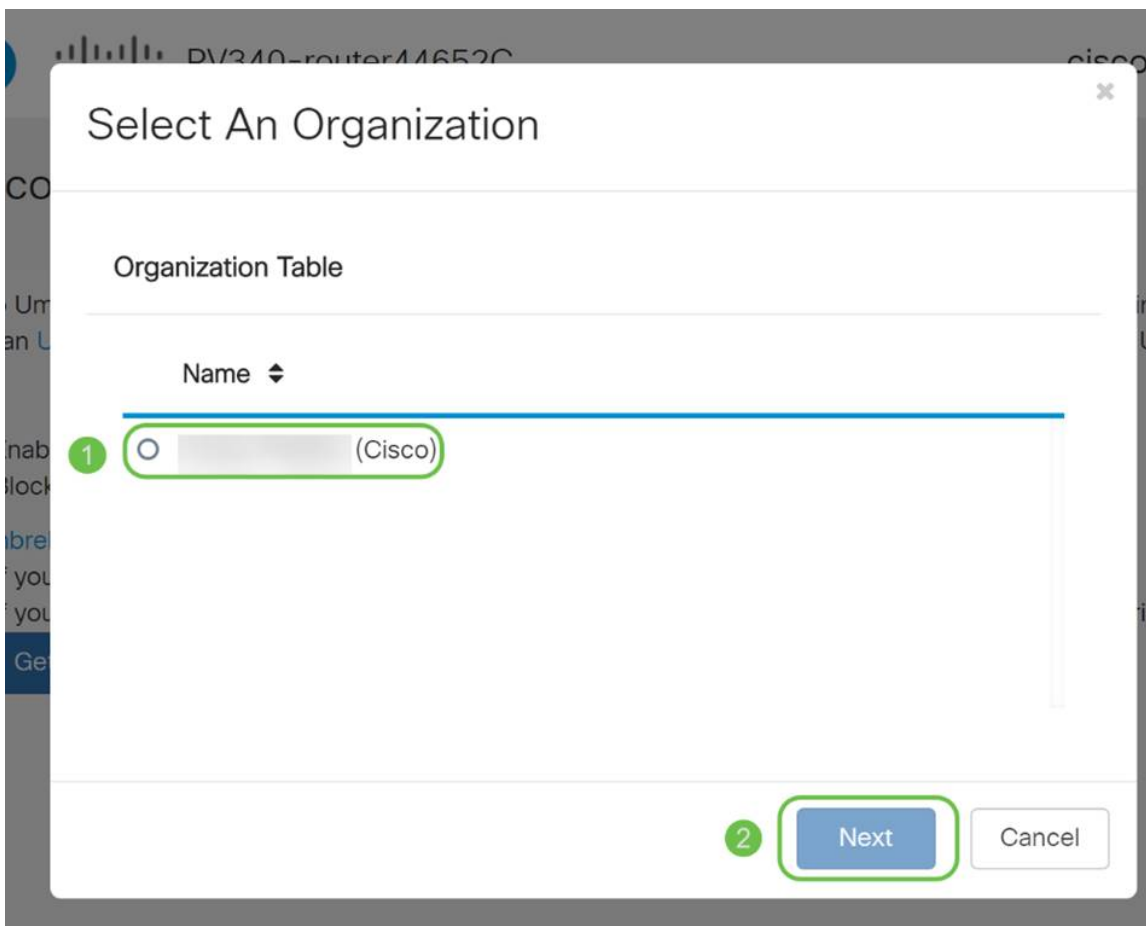
Next

Cancel

ステップ7:APIと秘密キーを入力したら、[Next] ボタンをクリックします。

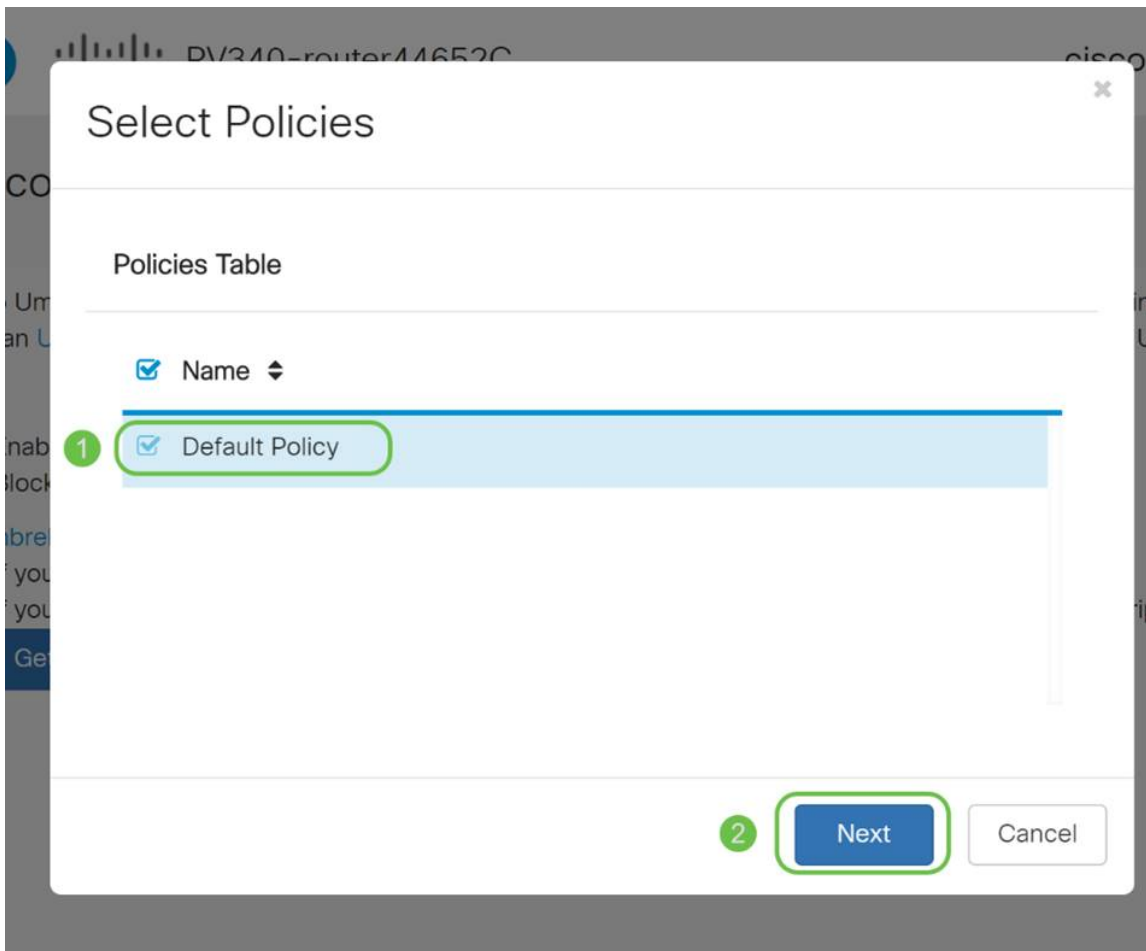


ステップ8：次の画面で、ルータに関連付ける組織を選択し、[Next] をクリックします。

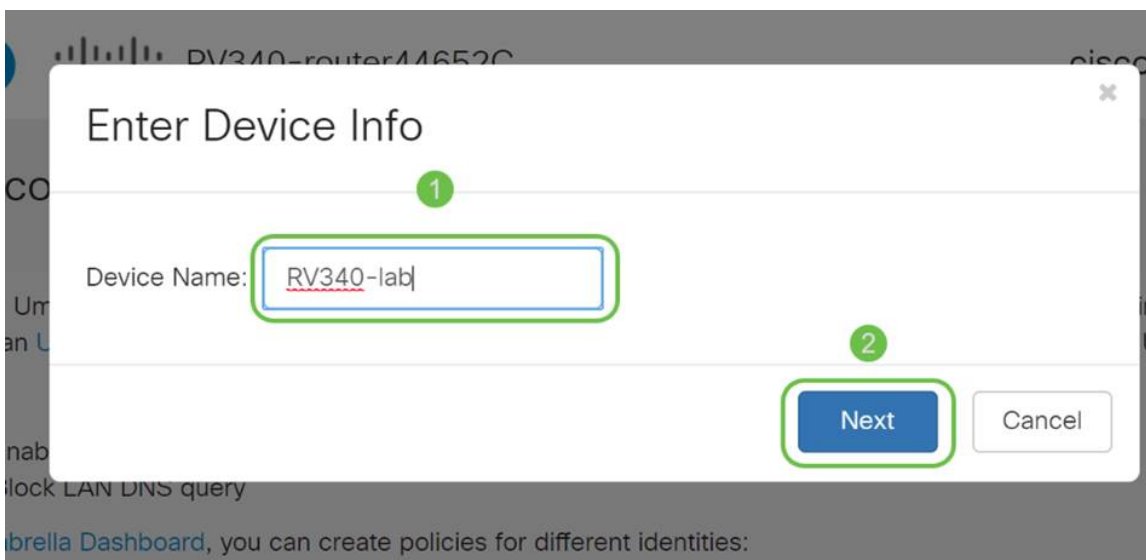


ステップ9：ここで、RV34xによってルーティングされるトラフィックに適用するポリシーを選択します。ほとんどのユーザには、デフォルトポリシーで十分なカバレッジが提供されます。

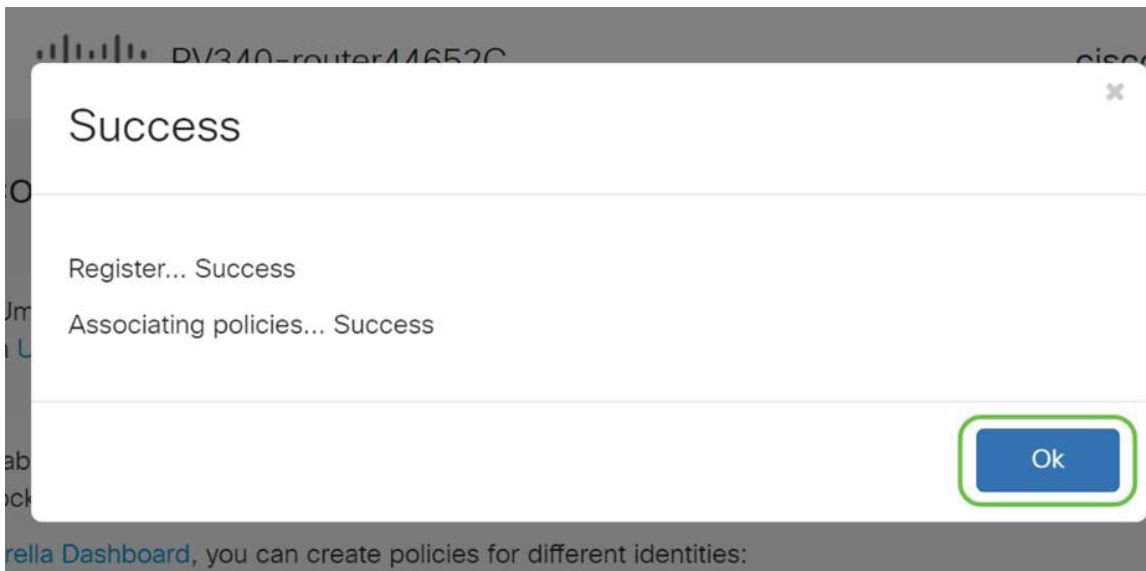




ステップ10: Umbrellaレポートで指定できるように、デバイスに名前を割り当てます。この設定では、「RV340-lab」を割り当てました。



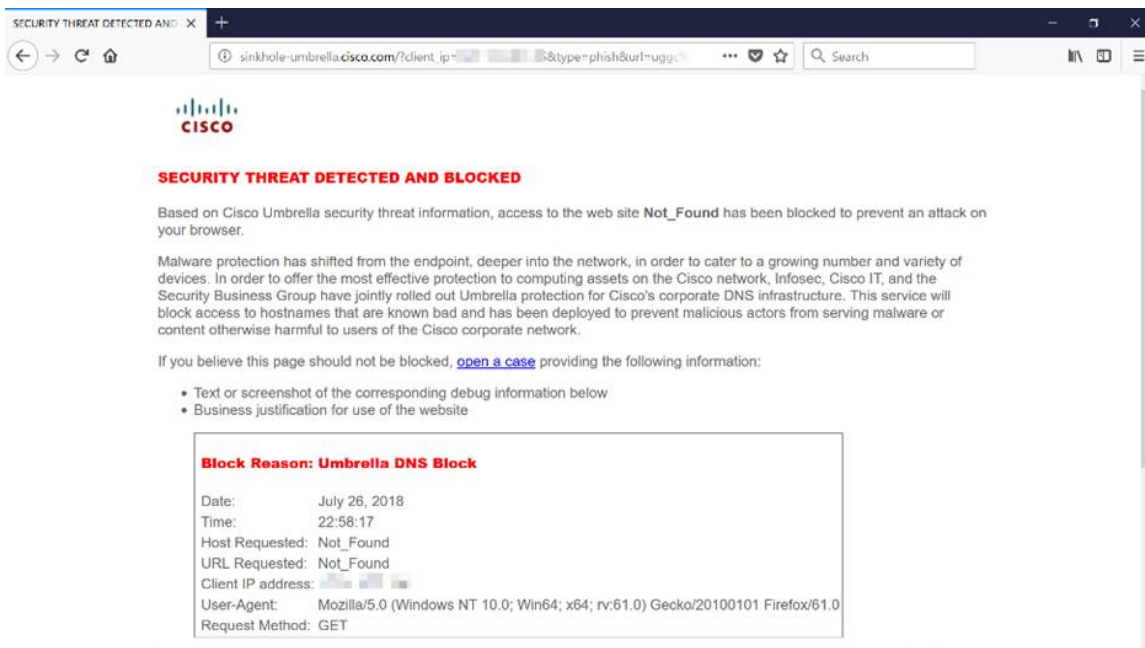
ステップ11: 次の画面で選択した設定が検証され、更新が行われます。関連付けが正常に完了したら、[OK] をクリックします。



## すべてが正しい場所にあることを確認する

おめでとうございます。これでシスコの傘が保護されました。それともお前なのか？実際の例を使って再確認してみましょう。シスコは、ページがロードされるとすぐに確認できる専用のWebサイトを作成しました。[ここをクリック](#)するか、ブラウザバーに <https://InternetBadGuys.com> と入力します。

Umbrellaが正しく設定されていれば、次のような画面が表示されます。



## この記事に関連するビデオを見る...

[シスコのその他の技術に関する講演を表示するには、ここをクリックしてください。](#)

## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。