Aruba WLAN管理者向けのUmbrella DNSの導入

内容

はじめに

このドキュメントでは、Aruba WLAN管理者にUmbrella DNSサービスを導入する方法について説明します。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、Cisco Umbrellaに基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

概要

Aruba Networksには、異なる市場セグメントおよび導入シナリオに対応する次の3つのワイヤレスLAN(WLAN)製品ラインとオペレーティングシステムがあります。

- ArubaOS：大規模組織および高密度環境向け
- Aruba Instant/InstantOS：中小規模の企業および分散型企業向け
- Aruba Instant On：ホームオフィスおよびスモールオフィスのユーザ向け

この記事では、Aruba WLAN管理者がUmbrella DNSサービスを採用および導入する際のガイドラインについて説明します。

導入方式

導入方法は、Arubaオペレーティングシステムと Umbrellaの使用方法によって異なります。

前述の3つのArubaオペレーティングシステムのいずれかを実行している場合は、Umbrellaユーザガイドを参照してUmbrella DNSの導入を開始できます。 ビデオチュートリアルも利用できます。

Aruba Instantを実行すると、InstantOSで利用可能なUmbrellaネットワークデバイス統合を使用する追加オプションが表示されます。ただし、このオプションを選択した場合、Umbrellaレポート(アクティビティ検索レポートなど)にWLAN上のワイヤレスクライアントの内部/プライベートIPアドレスは表示されません。クライアントからのDNSクエリは、Umbrella内のInstant APクラスタのネットワークデバイスIDにマッピングされ、個々のクライアントに関する情報は使用できません。Umbrellaクラウドの観点からは、DNSクエリはWi-Fiクライアントではなくインスタント APクラスタから送信されているように見えます。

したがって、個々のクライアントのDNSクエリをトレースする必要がある場合、またはWLAN上の個々のクライアントに合わせてDNSポリシーを調整する必要がある場合は、『Umbrella DNSユーザガイド』で説明されている標準的な方法でUmbrellaを導入し（Aruba Instantによるネットワークデバイス統合は使用しない）、導入計画にUmbrella 仮想アプライアンスを含することを検討できます。

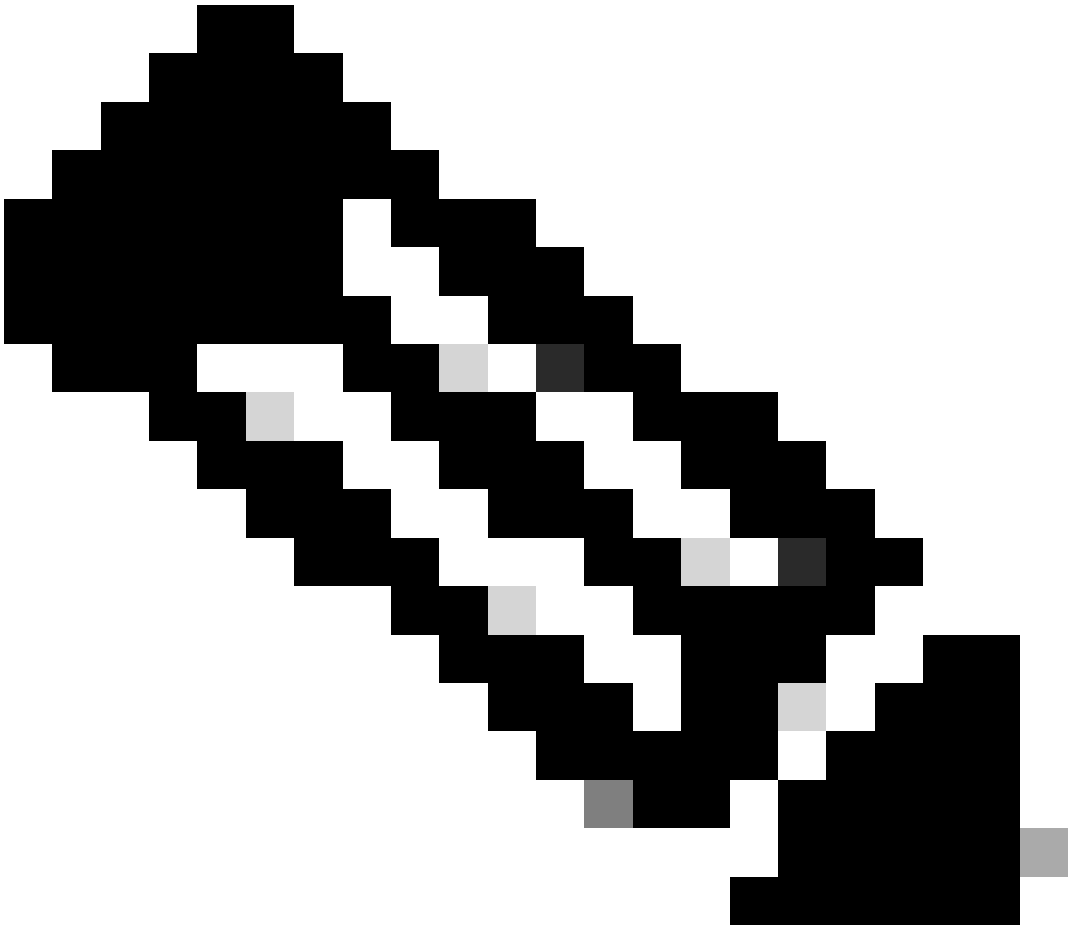
Element	Description
AD User	Identified by Virtual Appliance (VA) or Roaming Client (RC).
AD Computer	Identified by VA only.
Internal Network / Umbrella Site	Identified by VA only.
Default Umbrella Site	Traffic on VA with no other identity. Identified by VA only.
Roaming Client	Roaming Client only.
Network	Network Identity based on source IP of the DNS request.

4403300507924

Arubaのインスタント統合

Aruba InstantのUmbrella(OpenDNS)ネットワークデバイス統合は、Instant APクラスタに接続さ

れているすべてのWi-Fiクライアントが単一のUmbrella DNSポリシーの対象となり、Umbrellaレポートで個々のクライアントのDNSクエリを確認する必要がない環境で有益です。このセクションでは、統合を設定する方法について説明します。



> 注：この統合では、Umbrellaのネットワークデバイス APIのレガシーバージョンが使用されます。レガシーバージョンでは、お客様がUmbrellaダッシュボードからAPIトークンを生成する必要はありませんが、新しいバージョンでは生成します。

UmbrellaのレガシーAPIは2023-09-01年にサポート終了となり、その後は統合に対する日付サポートは提供されなくなります。2023-09-01以降の統合で問題が発生した場合は、導入ガイドの「はじめに」セクションを完了して、統合を使用せずにUmbrellaを導入してください。

統合を使用するには、次の要件を満たす必要があります。

- APは、InstantOSバージョン8.10.0.1以降（2022年5月現在）を実行する必要があります。
- 統合に使用するUmbrellaダッシュボードアカウントには、完全管理者ロールが必要です。
- アカウントのメールアドレスを複数のUmbrellaダッシュボードに関連付けることはできませ

ん。電子メールアドレスが1つのダッシュボードだけに関連付けられているかどうかがわからない場合は、Cisco Umbrellaサポートに問い合わせて確認してください。
- アカウントに対してシングルサインオン(SSO)と2要素認証(2FA)を有効にすることはできません。
- APとインターネットの間にネットワークセキュリティアプライアンス（ファイアウォールなど）がある場合、アプライアンスは208.67.220.220、208.67.222.222、67.215.92.210、および146.112.255.152/29 (.152 ~ .159)へのフィルタリングされていない接続とインスペクションされていない接続を許可する必要があります。

コンフィギュレーション

この統合を実現するには、大まかに4つの設定手順があります。

1. APクラスタの名前の設定

2. アカウントの資格情報を入力します

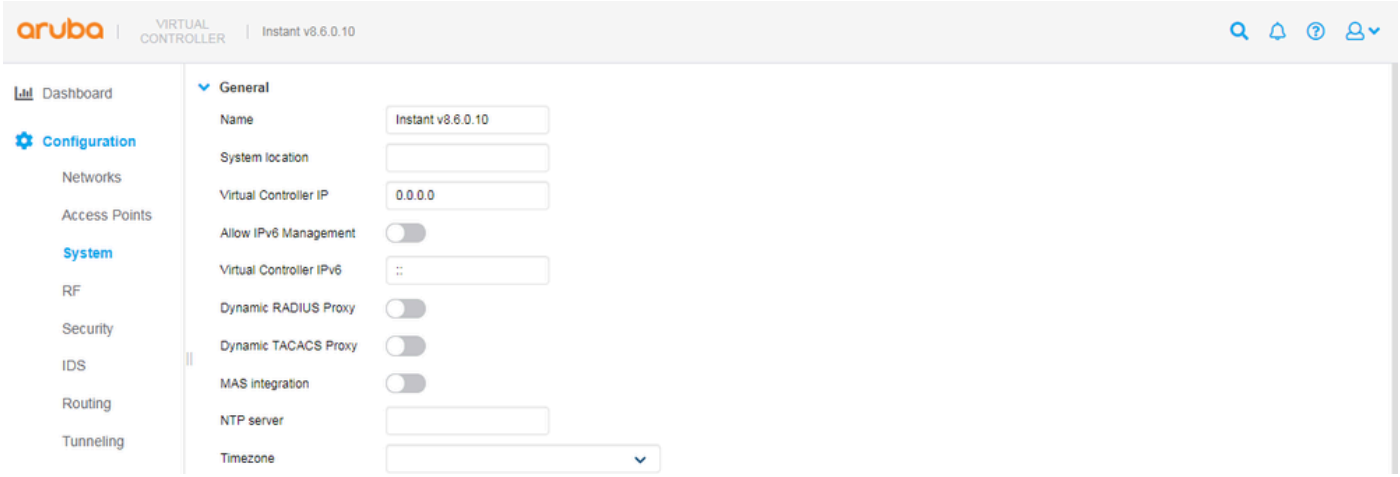
3. DNSクエリのインターセプト

4. DNSポリシーの適用

APクラスタの名前の設定

インスタントクラスタがUmbrellaダッシュボードに初めて正常に登録されると、UmbrellaダッシュボードのDeployments > Network Devicesにネットワークデバイスのエントリが追加されます。新しいエントリのデバイス名は、クラスタの仮想コントローラで設定されたシステム名から取得されます。

インスタント仮想コントローラにシステム名を設定するには、Configuration > Systemの順に選択します。



4404011628308

名前の値は、最初の登録時に1回だけコピーされることに注意してください。その後、インスタントまたはアンブレラのいずれかの側でシステム/デバイス名を変更した場合は、もう一方の側で名前を手動で更新する必要があります。

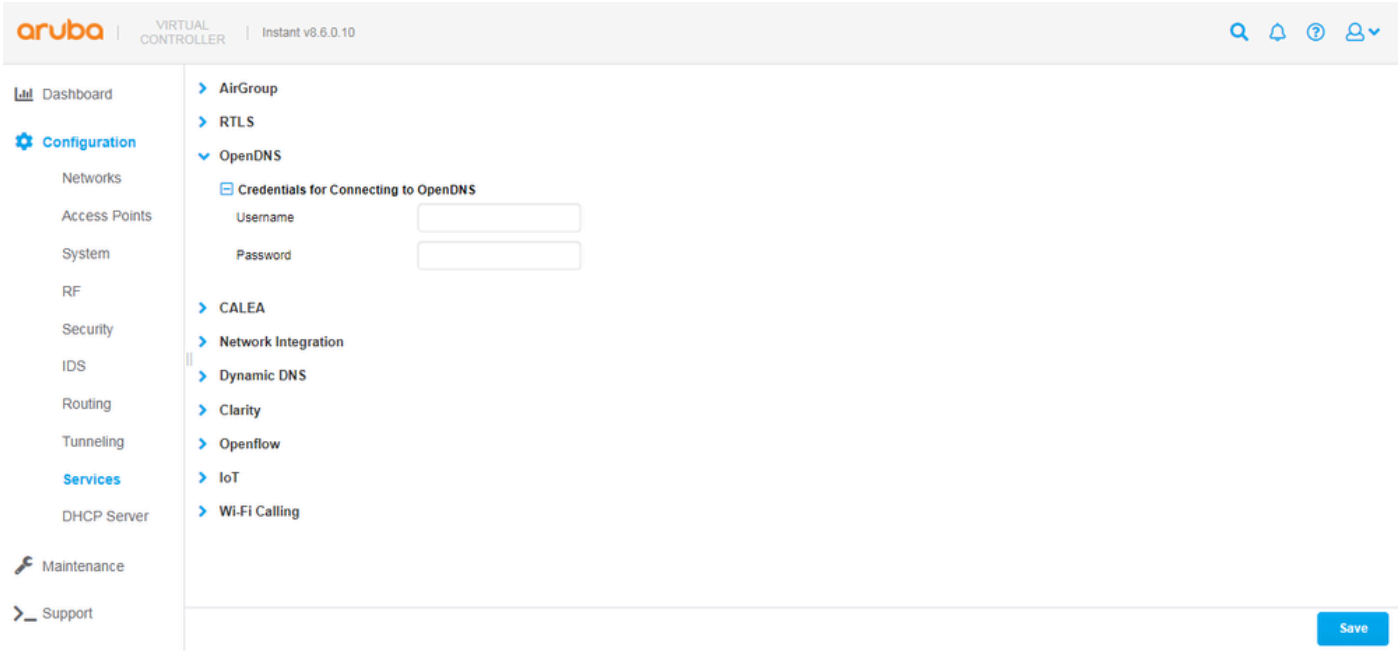
アカウント資格情報の入力

「前提条件」セクションに記載されている要件が満たされている場合は、Umbrellaダッシュボードにネットワークデバイスとしてインスタントクラスタを追加できます。クラスタの仮想コントローラから実行するには、次の手順を実行します。

1. Configuration > Services > OpenDNSの順に移動します。

2. Umbrellaアカウントのログインクレデンシャルを入力します。

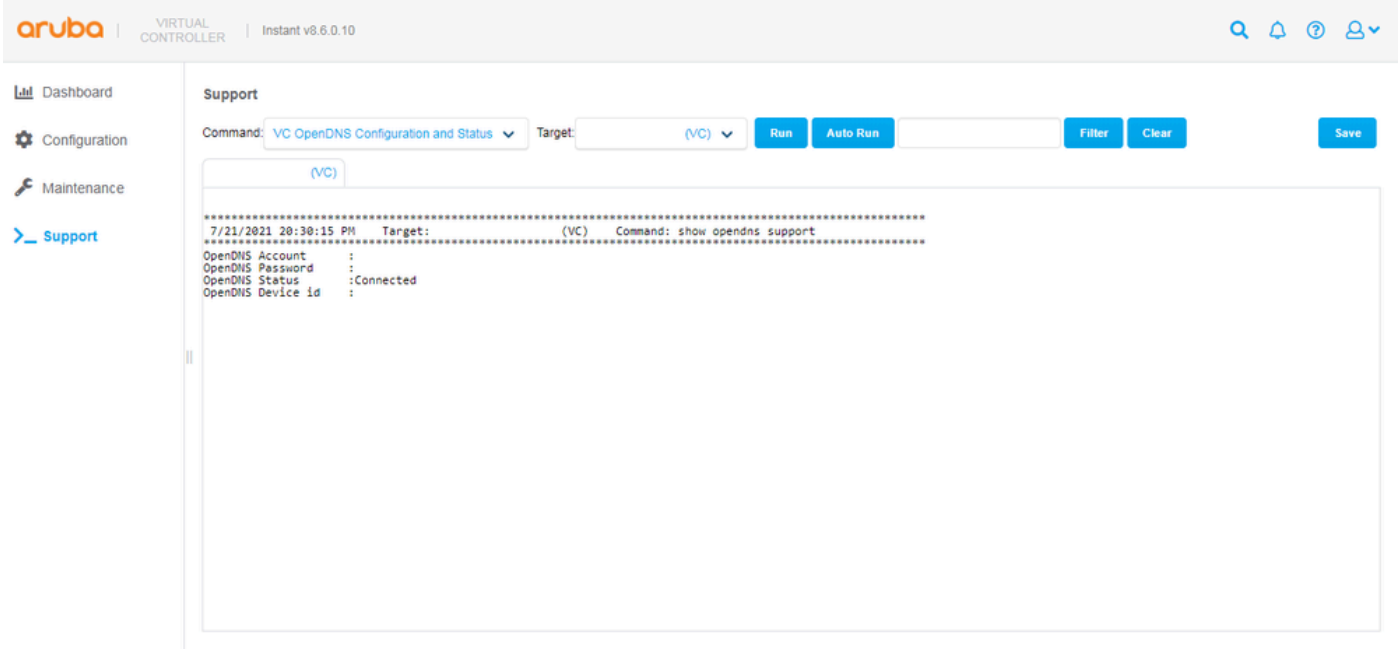
3. Saveを選択します。



4404019266196

仮想コントローラ(VC)がUmbrellaに正常に接続した場合、Supportに移動して「VC OpenDNS Configuration and Status」(show opendns support)コマンドを実行すると、Connectedステータスが表示されます。

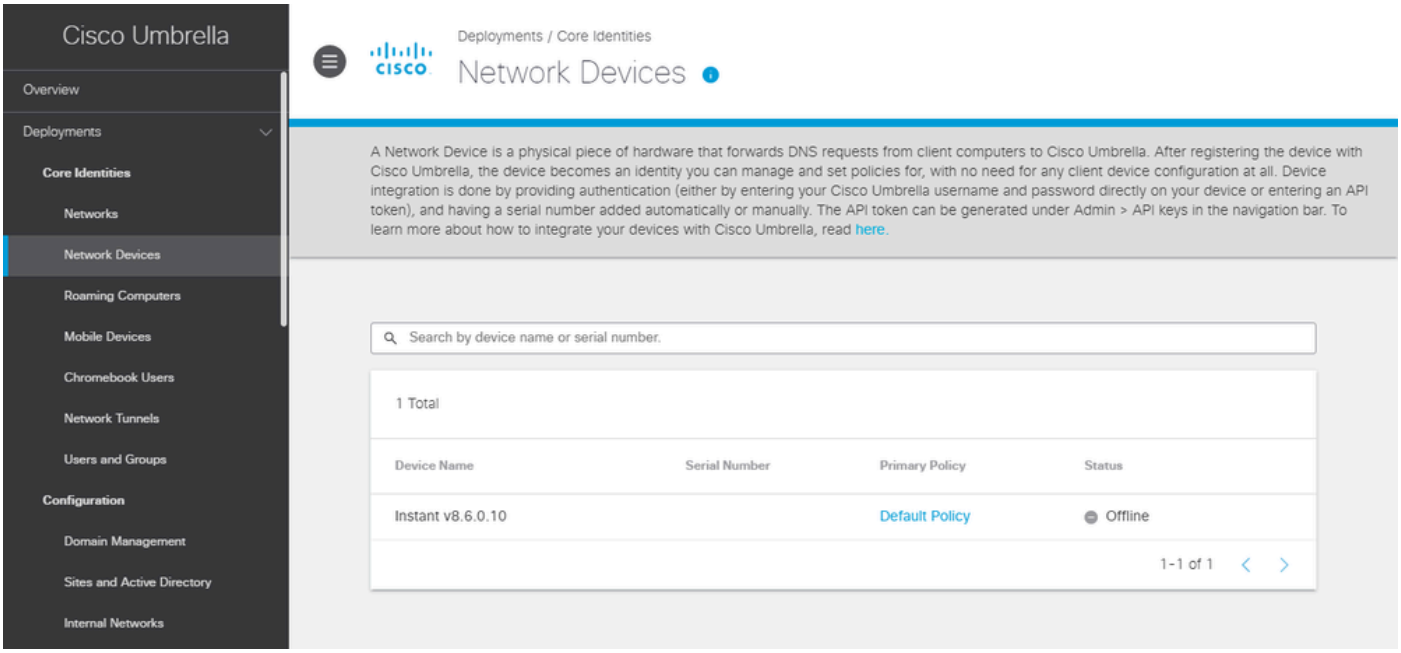
また、デバイスIDも確認できます。このIDは、新しいネットワークデバイスが作成され、インスタントVC設定に保存されたときにUmbrellaによって生成されます。後者の部分は重要です。各インスタントクラスタは一意のUmbrellaネットワークデバイスIDを持つ必要があるため、デバイスIDをクラスタの構成から別のクラスタにコピーすることはできません。有効なデバイスIDは通常16桁です。



4404019268116

コマンド出力にNot connectedステータスが表示された場合は、「AP Tech Support Dump」(`show tech-support`)コマンドと「AP Tech Support Dump Supplemental」(`show tech-support supplemental`)コマンドを実行して理由を調べてから、ログで「opendns」を検索できます。コマンド出力は、トラブルシューティングの目的でAruba TACと共有することもできます。

すべてが正しく機能している場合、UmbrellaダッシュボードのDeployments > Network Devicesに新しいエントリが表示されます。このエントリで、名前でInstant APクラスタを検索したり、新しいデバイスIDを生成したい場合に既存のエントリを削除したりできます。



4404011658516

DNSクエリのインターセプト

クラスタがネットワークデバイスとしてUmbrellaダッシュボードに正常に追加されたことを確認

したら、（クラスタ内のAPに接続されている）ワイヤレスクライアントから送信されたDNSクエリの代行受信を開始するようにクラスタを設定できます。 設定すると、ワイヤレスクライアントのNICで設定されているDNSサーバのIPアドレスに関係なく、クライアントのDNSクエリをクラスタが代行受信し、208.67.220.220および208.67.222.222のUmbrellaのエニーキャストリゾルバに転送できます。

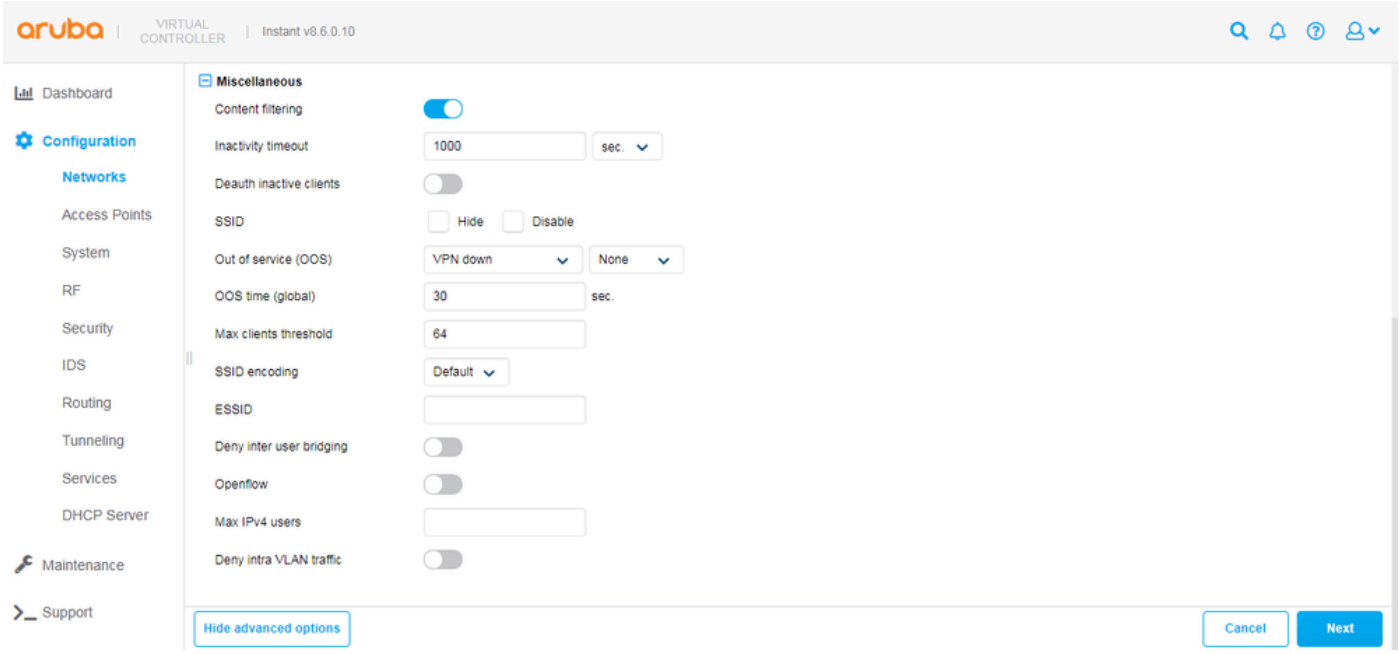
DNSクエリを代行受信するには、次の手順を実行します。

1.Configuration > Networksで、クラスタの仮想コントローラに移動します。

2. ワイヤレスネットワークを選択します。

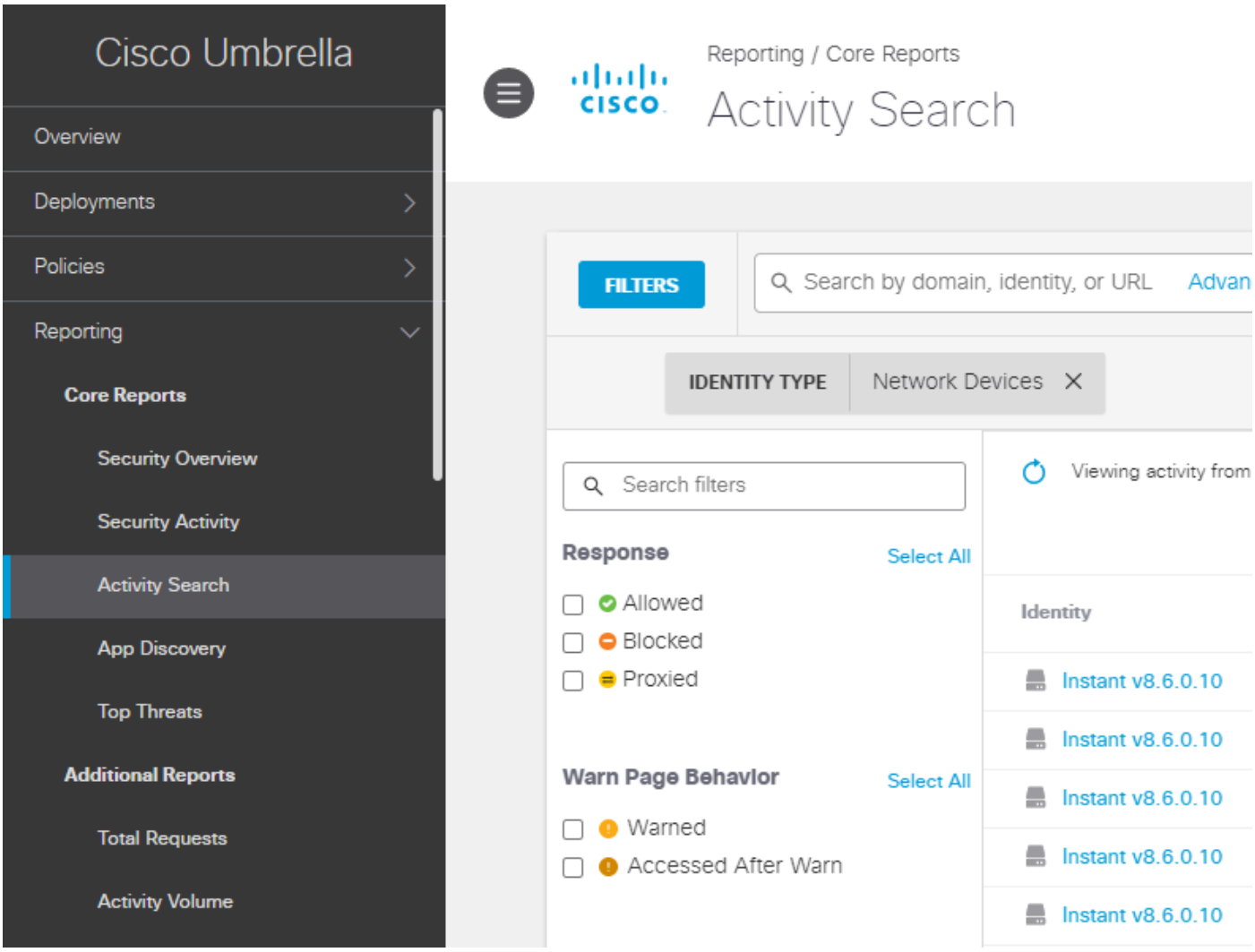
3. ネットワークを編集し、「詳細オプションの表示」を選択して、「その他」セクションまでスクロールします。

4.「コンテンツのフィルタ処理」オプションを有効にし、「終了」ボタンを選択して変更を保存できるまで「次へ」を選択し続けます。



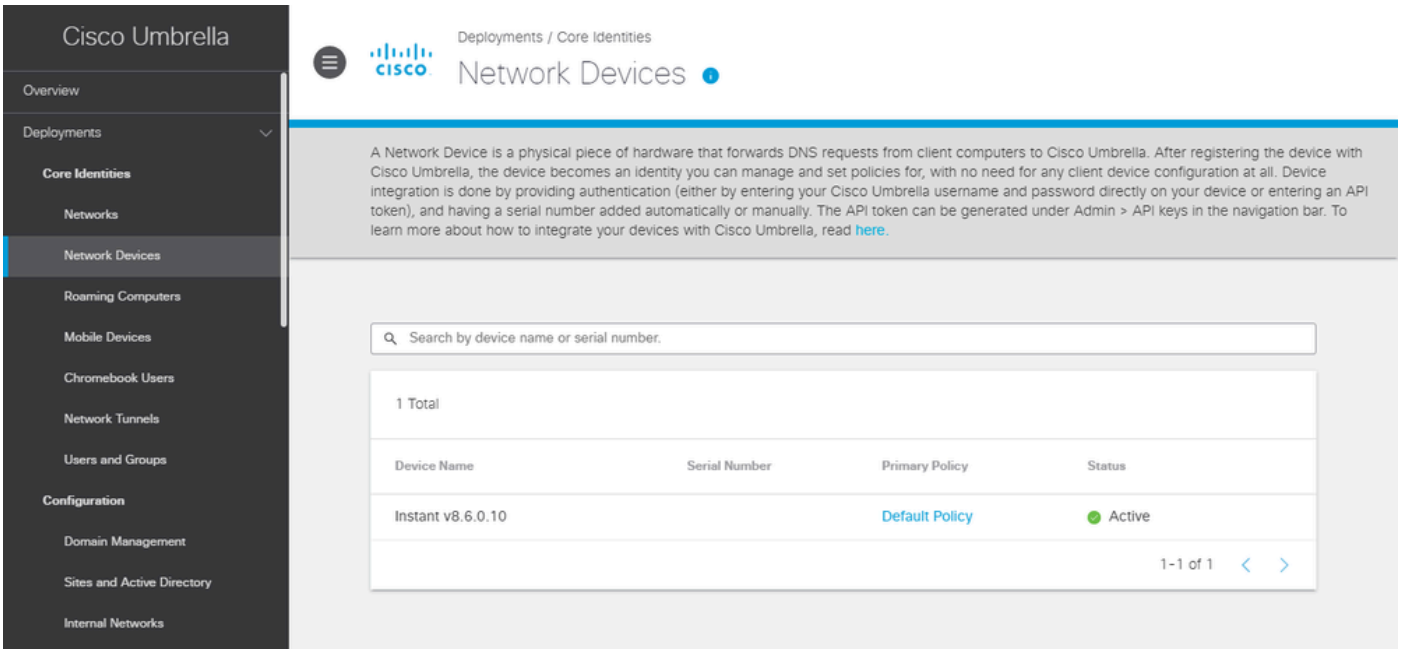
4404011668500

このオプションをオンにすると、UmbrellaダッシュボードのReporting > Activity SearchにDNSクエリが表示されるようになります。クエリのIDは、ネットワークデバイス名（通常は、APクラスタの仮想コントローラに設定されたシステム名）にマッピングできます。クエリーが処理されてダッシュボードGUIに表示されるまでに時間がかかる場合があることに注意してください（約15分）。



4404011721620

UmbrellaダッシュボードのDeployments > Network Devicesの順に選択すると、デバイスのステータスがアクティブ/オンラインステータスに変わるのに、最大で24時間かかることがあります。ネットワークデバイスのステータスは、DNSクエリがデバイスによって代行受信され、24時間前にUmbrellaに転送されたかどうかを示すだけで、デバイスがUmbrellaと通信する方法には影響を与えません。オフライン/非アクティブステータスとは、過去24時間にAPクラスタに接続されたワイヤレスクライアントがなく、クラスタによるUmbrellaサービスの利用を妨げることができないことを意味します。

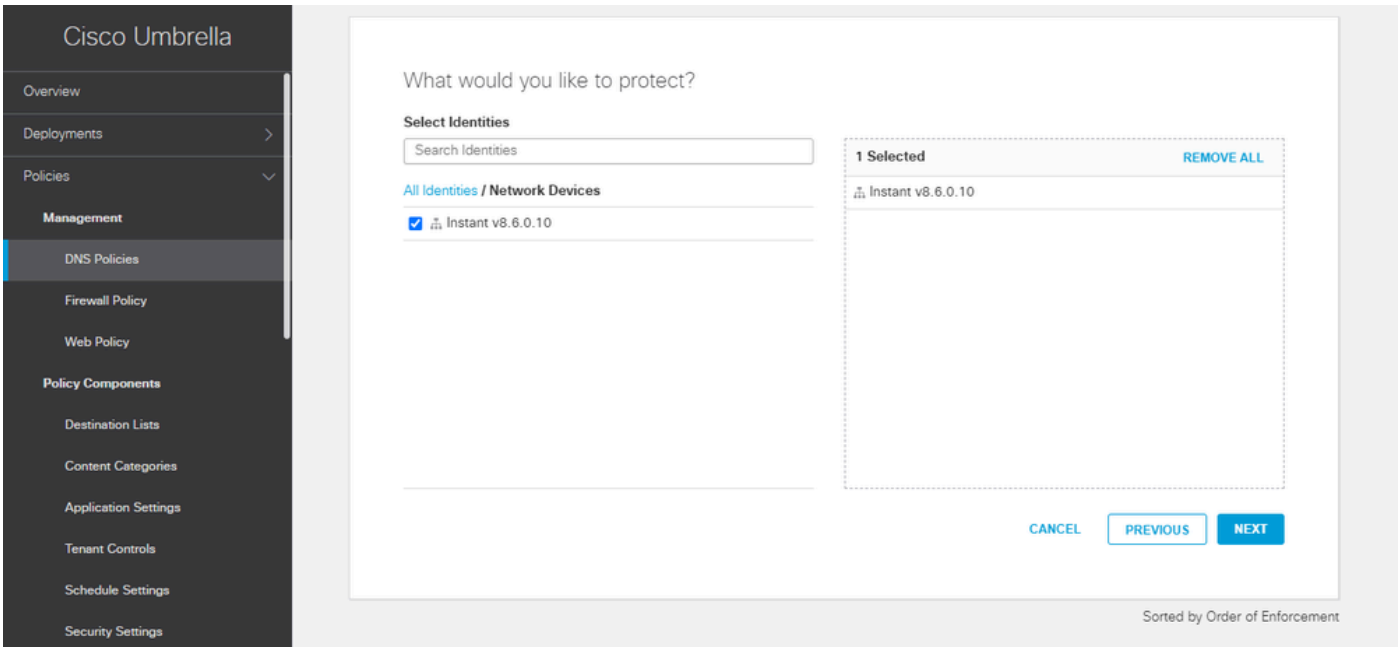


4404011756308

DNSポリシーの適用

Umbrellaでは、「デフォルトポリシー」には、ダッシュボードに追加されたすべてのID（ネットワークデバイスなど）が自動的に含まれます。展開内のすべてのAPクラスタが同じポリシーに従う場合は、追加のDNSポリシーを作成する必要はありません。その場合は、次のセクションに進んでください。

または、特定のネットワークデバイスにカスタムポリシーを適用する場合は、Umbrellaダッシュボードの**Policies > All Policies (DNS Policies)**の下に新しいポリシーを追加し、ポリシーでネットワークデバイスを選択する必要があります。



4404011773588

DNS Policies (All Policies)ページに複数のポリシーがある場合、ポリシーは最初に一致した順に

評価されます。詳細については、ポリシーの優先順位に関するドキュメント、およびポリシーを定義するためのベストプラクティスに関するドキュメントを参照してください。

内部DNS

内部DNSサーバが存在し、特定の（内部）ドメインのDNSクエリを内部DNSサーバに転送する環境では、エンタープライズドメイン機能を即座に使用できます。

この機能を有効にした後も、APクラスタはDNSクエリを代行受信できます。ただし、指定したドメインのクエリをUmbrellaに転送することはできません。代わりに、ワイヤレスクライアントのNICで最初に設定されたDNSサーバのIPアドレスに（DHCP経由などで）転送できます。 この機能は、Aruba Instant Integrationを使用しない標準のUmbrella導入方法(仮想アプライアンスを使用)で使用できる内部ドメイン機能に似ています。

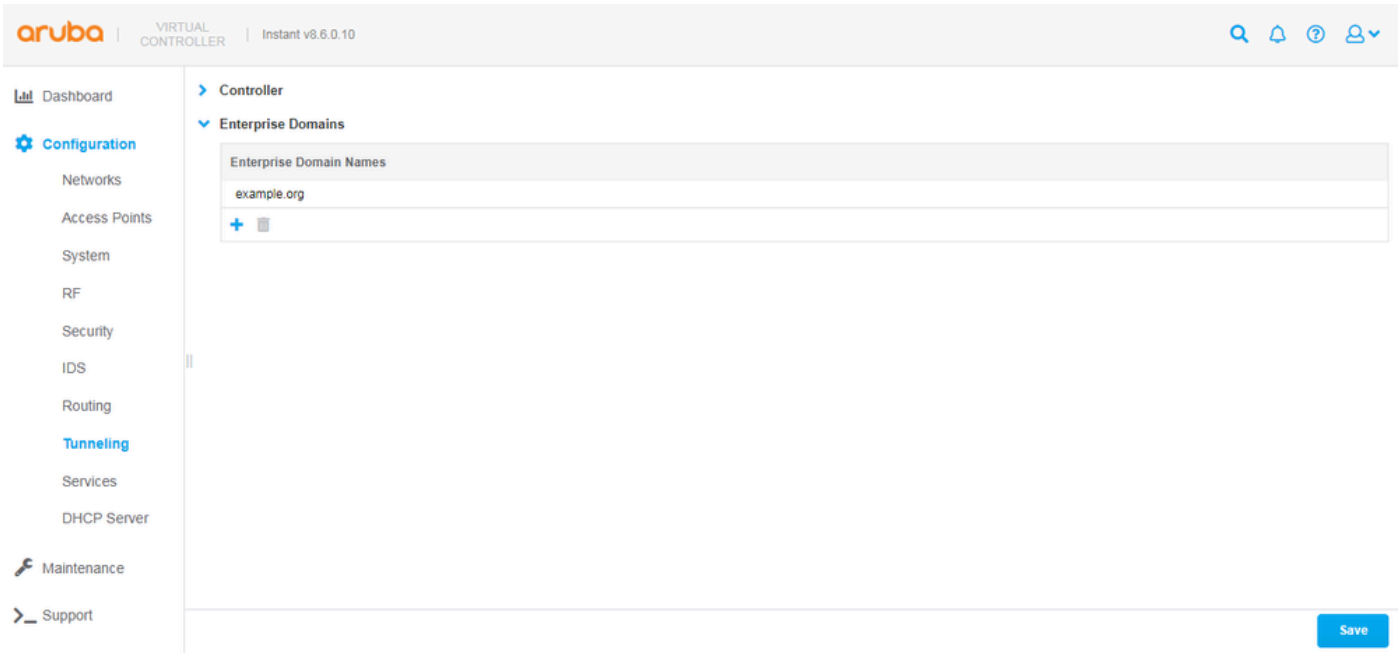
インスタント仮想コントローラで機能を設定するには、次の手順を実行します。

1. Configuration > Tunneling > Enterprise Domainsの順に移動します。

2. エンタープライズドメイン名リストにドメインを追加するか、このリストからドメインを削除します。

3. Saveを選択します。

リストに追加されたドメインには暗黙的なワイルドカードがあるため、example.orgは*.example.orgを意味します。

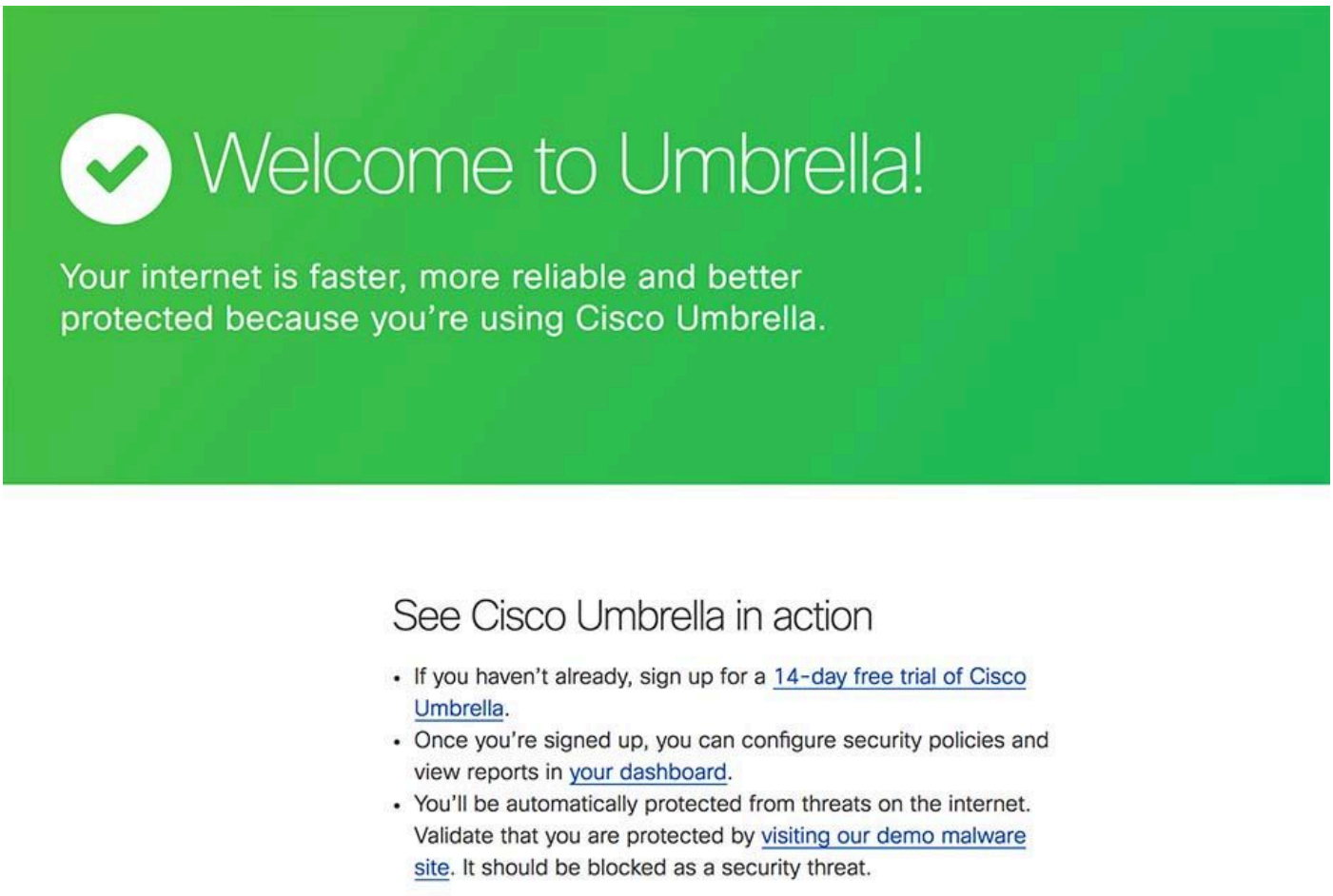


4404238114452

検証

このガイドの「導入の概要」セクションで参照されている標準方式を使用してWLANにUmbrellaを導入したか、Aruba Instant Integrationセクションで説明されている統合を導入したか

に関係なく、クライアントの1つからhttps://welcome.umbrella.com/を参照することで、ワイヤレスクライアントがUmbrella DNSを使用していることを確認できます。その後、Umbrellaのドキュメントに表示されるスクリーンショットのような緑色のチェックが表示されます。



4404011960212

または、無線クライアントのコマンドプロンプトで次のコマンドを実行して、このことを確認することもできます。

```
nslookup -type=txt debug.opendns.com.
```

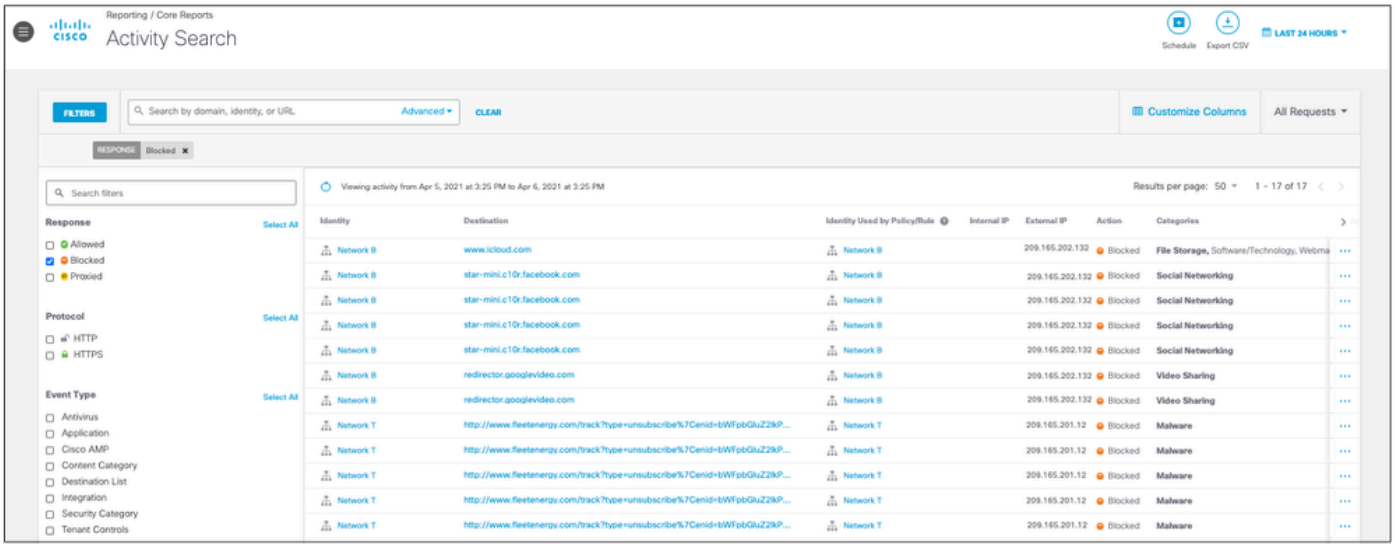
次のスクリーンショットのように、出力に多数のテキスト行が表示されます。

```
anthony@ubuntu:~/Desktop$ nslookup -type=txt debug.opendns.com.
Server:         127.0.1.1
Address:        127.0.1.1#53

Non-authoritative answer:
debug.opendns.com       text = "server 7.pao"
debug.opendns.com       text = "organization id
debug.opendns.com       text = "appliance id
debug.opendns.com       text = "host id
debug.opendns.com       text = "user id
debug.opendns.com       text = "remoteip
debug.opendns.com       text = "flags
debug.opendns.com       text = "id
debug.opendns.com       text = "source
debug.opendns.com       text = "fw: flags
debug.opendns.com       text = "fw: id
debug.opendns.com       text = "fw: source

Authoritative answers can be found from:

anthony@ubuntu:~/Desktop$
```

4404011980436

コマンド出力から、Umbrellaダッシュボードの組織IDを「orgid」行または「組織ID」行で確認できます。Instant Integrationを使用している場合は、デバイスIDを含む追加の「デバイス」行を確認できます。

UmbrellaダッシュボードのDNSクエリを確認するには、[レポート] > [アクティビティの検索] に移動します。クエリーがダッシュボードGUIに表示されるまでに時間がかかる場合があることに注意してください（約15分）。アクティビティ検索の使用方法については、Umbrellaのドキュメントを参照してください。



4404019393044

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。