

保護されていない、または暗号化されていないローミングクライアントモードの解決

内容

[はじめに](#)

[非保護および非暗号化状態](#)

[通信の要件](#)

[ネットワーク接続のテスト](#)

[非暗号化状態のみ](#)

はじめに

このドキュメントでは、Umbrellaローミングクライアントの保護されていない状態と暗号化されていない状態の意味と、そのトラブルシューティング方法について説明します。

非保護および非暗号化状態

Umbrella Roaming Clientが保護モードまたは非暗号化モードの場合、トレイアイコン (Windows) またはメニューバー (OS X) に黄色の状態が表示されます。ステータスには、UnprotectedとUnencryptedの両方が表示されます。

通信の要件

セキュリティとコンテンツのフィルタリングを提供するために、Umbrella Roamingクライアントは、「[Roamingクライアントの前提条件](#)」の記事に記載されているHTTPの宛先に加えて、提供されているポートと宛先でUDPとTCPの両方を使用してUmbrellaと通信する必要があります。

ポート	プロトコル	IPv4	IPv6
53	UDP	208.67.222.222, 208.67.220.220	2620:119:53::53, 2620:119:35::35
53	TCP	208.67.222.222, 208.67.220.220	2620:119:53::53, 2620:119:35::35
443	UDP	208.67.222.222, 208.67.220.220	2620:119:53::53, 2620:119:35::35
443	TCP	208.67.222.222, 208.67.220.220	2620:119:53::53, 2620:119:35::35

Umbrella Roamingクライアントは、次の条件の両方が存在する場合、コンピュータを保護できません。

- サードパーティのDNS要求を許可しない接続の背後にコンピューターがあります。
- コンピューターは、既定の送信拒否ファイアウォールポリシーを持つ接続の背後にあります。

これらの条件が満たされると、Umbrella Roaming ClientはDHCPに委任されたDNSサーバをネットワーク接続プロパティに復元し、Umbrella DNSサーバに接続してセキュリティとコンテンツフィルタリングの提供を再開できるようになるまでテストを続行します。Umbrella DNSサーバとの通信が不可能な期間は、ポリシーの適用とレポートを使用できません。

ネットワーク接続のテスト

ネットワークがUmbrella DNSサーバとの通信を許可しているかどうかを確認するには、DNSクエリを手動で実行します。ネットワークがクエリをブロックする場合、出力は次のようになります。

```
$ nslookup opendns.com 208.67.222.222
;; connection timed out; no servers could be reached
```

テストは成功したが、Umbrella Roaming Clientで「Unprotected/Unencrypted」と表示される場合は、サポートチケットをオープンし、診断テストの結果を提供します。正常なクエリは次のように表示されます。

```
$ nslookup opendns.com 208.67.222.222
Server: 208.67.222.222
Address: 208.67.222.222#53

Non-authoritative answer:
Name: opendns.com
```

非暗号化状態のみ

Umbrellaローミングクライアントで「Unencrypted」と表示される場合、ポート443/UDPで通信できません。セキュリティを確保するために、ファイアウォールでこのポートを許可することをお勧めしますが、クライアントは暗号化されたDNSクエリなしで機能し続けます。詳細については、「[クライアントのローミングの前提条件](#)」の記事を参照してください。

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。