1. Umbrella ローミング クライアントの概要

はじめに

このドキュメントでは、Cisco Umbrella ローミング クライアントの概要を示し、組織の Windows および Mac ラップトップ（さらに必要に応じてデスクトップ システム）にクライアントを導入し、正常に動作していることを確認できるようにすることを目的としています。

注：このドキュメントに含まれているいくつかのリンクは、セットアップ ガイド内の認証が必要な領域にアクセスします。Umbrella のログイン アカウントを持っていない場合は、無料トライアルにサインアップすることでアクセスできるようになります。

Umbrella ローミング クライアントとは

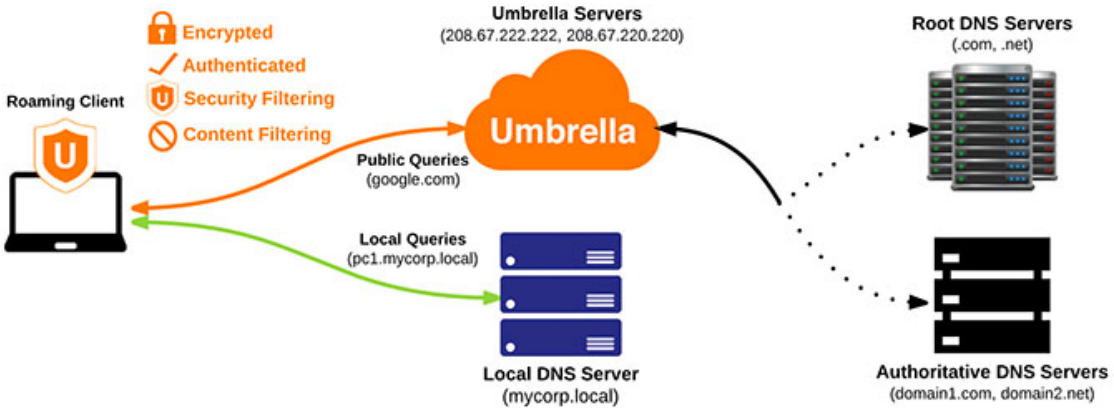
Umbrella ローミング クライアントは、Windows または Mac OSX コンピュータで動作する***非常に軽量な*** DNS クライアントです。これは、VPN クライアントまたはローカルのウイルス対策エンジン***ではありません***。ローミング クライアントは、**インテリジェント プロキシ**を含む Umbrella のセキュリティおよびポリシー ベースの保護を、接続しているネットワークを問わずに適用することを可能にします。オフィス、ホテル、コーヒー ショップなどにいても、モバイル ホットスポットを使用している場合でも、Umbrella ローミング クライアントにより、Umbrella で設定したポリシーが適用されます。

ローミング クライアントについて、またはその機能については、Umbrella のプロダクト マネージャ、Adam Winn による次のブログ記事をご覧ください。
https://blog.opendns.com/2016/11/30/ten-things-didnt-know-umbrella-roaming-client/

Umbrella ローミング クライアントの仕組み

Umbrella ローミング クライアントは 127.0.0.1:53（ローカルホスト）にバインドされ、コンピュータ上のすべてのネットワーク接続で排他的に DNS サーバとして設定されます。それによってすべての DNS 要求が最も近い Umbrella データセンターにリダイレクトされ、また、ローカル ネットワーク リソースに関しては、また内部ドメインを使用して正常に処理されます。

Umbrella を通じて送信される DNS クエリは、暗号化されて認証され、組織の管理者の指示に従い、セキュリティとコンテンツ フィルタリングの対象になります。コンピュータから、Umbrella または自社の管理者が安全でないと判断するドメイン名へのアクセスを試みると、コンピュータのブラウザが安全なブロック ページにリダイレクトされます。



Umbrella ローミング クライアントはコンピュータのネットワーク環境に応じて、運用に適した状態を複数の選択肢から適切に選択します。

重要な点として、Umbrella ローミング クライアントには、キャッシュされた DNS レコードまたは DNS 応答は保存されません。Umbrella ローミング クライアントは、通常の（Umbrella ローミング クライアントがない）コンピュータと同様に、ドメインの DNS プロパティによって設定された TTL に従います。

Umbrella ローミング クライアントの利点

従来のネットワーク ベースのサービス、または従来のほとんどのアプライアンス ベースのネットワーク境界ゲートウェイに存在した次の 2 つの制約が、Umbrella ローミング クライアントによって解決されます。

- **ローミング/ネットワーク非接続**：ラップトップをオフィスから持ち出し、フルトンネル VPN を常時使用しない場合（低速になるため）、ネットワーク外部でのローミング時に、ラップトップは脅威や望ましくないコンテンツから保護されません。
- **詳細なレポートとフィルタリング**：ネットワーク ベースのサービスだけを使用する場合、単一のネットワーク ID のみしか表示されませんが、Umbrella レポートでは、すべての DNS トラフィックが表示されます。**Umbrella Insights** がなければ、どのコンピュータまたは IP アドレスが望ましくないコンテンツや悪意のあるコンテンツを要求しているか、特定できません。Umbrella ローミング クライアントでは、Umbrella で設定したポリシーをコンピュータ単位で設定できます。コンピュータ単位で各種のセキュリティおよびコンテンツ フィルタリング設定を適用できるだけでなく、コンピュータ レベルのレポートを確認することもできます。

VPN との連動

Umbrella ローミング クライアントは、VPN と連動可能です。ほとんどのスプリット トンネルおよびフルトンネル VPN と連動します。

Cisco スプリット トンネル VPN については、特別な考慮事項があります。詳細については **Umbrella ローミング クライアント：VPN、VPN の互換性** を参照してください。

また Umbrella ローミング クライアントと**互換性がない** VPN クライアントの簡単なリストもあります。このリストは互換性がない VPN クライアントにあります。

ウイルス対策ソフトウェアやエンドポイント セキュリティ ソフトウェアとの同時実行

同時に実行できます。DNS 要求を処理することが Umbrella ローミング クライアントの唯一の機能であるため、サードパーティ製セキュリティ ソフトウェアが Umbrella ローミング クライアントを妨げることはありません。大量の処理はすべて Umbrella データセンターとクラウドで行われるため、従来のウイルス対策のような遅さもありません。

Umbrella ローミング クライアントの詳細

一般的な FAQ からさらに踏み込んだ内容のビデオが用意されています。Umbrella ローミング クライアントの機能と利点について詳しく知りたい場合は、このビデオをご覧ください。https://www.youtube.com/watch?v=6pCjDlTeXrY

次のステップ

- 前提条件

ご質問がある場合

- **Umbrella ローミング クライアント ナレッジ ベース**をご覧ください。一般的なさまざまな質問や状況について回答しています。

---

2. 前提条件

概要：前提条件

Cisco Umbrella ローミング クライアントを適切に使用するには、次の前提条件を満たしている必要があります。競合や問題の発生を回避するために、リスト全体を読んで前提条件を満たしていることを確認してください。

サポートされるオペレーティング システム

- .NET 4.5 搭載 Windows 10
- .NET 4.5 搭載 Windows 8（8.1 を含む）（64 ビット）
- .NET 3.5 搭載 Windows 7（64 ビット/32 ビット）
- Mac OS X 10.9 以降

サポートされていないオペレーティング システム

- Windows Server（全バージョン）
- Windows RT（ARM プロセッサは未サポート）
- Mac OS X 10.8 以降

ネットワークアクセス

DNS

Umbrella ローミング クライアントでは、Umbrella との通信に標準の DNS ポート 53/UDP および 53/TCP を使用しています。社内ネットワークやホーム ネットワークでサードパーティ製 DNS サーバへのアクセスを明示的にブロックする場合は、ファイアウォールに次の許可ルールを追加する必要があります。

ポート	プロトコル	接続先
53	UDP	208.67.222.222/208.67.220.220
53	TCP	208.67.222.222/208.67.220.220

サードパーティ製 DNS サーバがブロックされている場合、Umbrella ローミング クライアントは、一時的に DHCP に委任された DNS サーバを使用して解決する状態に移行します。

暗号化（オプション）

Umbrella ローミング クライアントでは、オプションで、443/UDP を使用して Umbrella に送信されたすべてのクエリを暗号化することができます。暗号化を確実に有効にし、ファイアウォールでデフォルトの拒否ルールセットを使用するには、ファイアウォールに次の許可ルールを追加します。

ポート	プロトコル	接続先
443	UDP	208.67.222.222/208.67.220.220

Umbrella ローミング クライアントでは、443/UDP が開いていることが認識されると、DNS クエリが自動的に暗号化されます。

HTTP と HTTPS

Umbrella ローミング クライアントでは、HTTP（80/TCP）と HTTPS（443/TCP）を使用して、次の用途でシスコの API と通信します。

- インストール時の初回登録
- Umbrella ローミング クライアントの新バージョンのチェック
- Umbrella ローミング クライアントのステータスを Umbrella に報告
- 新しい内部ドメインのチェック（後述）

Windows のみ：ユーザ レベル（通常は GPO を使用）で設定された HTTP プロキシを使用する場合は、「SYSTEM」ユーザもプロキシを使用するように設定する必要があります。

その他の場合は、ファイアウォールに次のルールを追加して、ローミング クライアントが API に到達できるようにします。

ポート	プロトコル	接続先
80	TCP	crl3.digicert.com、crl4.digicert.com
443	TCP	67.215.92.201、67.215.92.210、sync.hydra.opendns.com、crl3.digicert.com、crl4.digicert.com

上の表で、IP アドレス 67.215.92.201 と 67.215.92.210 は次のように解決されます。

- api.opendns.com
- disthost.opendns.com

Digicert のドメインは、CDN に基づいて複数の IP アドレスに解決されており、変更される場合があります。現在これらのドメインは、次の IP に解決されます。

- 72.21.91.29、117.18.237.29
- 93.184.220.29、205.234.175.175

注：sync.hydra.opendns.com は、146.112.63.0/24 IP 範囲の複数の IP アドレスに解決されます。この範囲全体を sync.hydra.opendns.com の IP アドレスとして追加することをお勧めします。Anycast は変更される場合があります。現在、このドメインは次の IP アドレスに解決されます。

146.112.63.3 ～ 146.112.63.9 および 146.112.63.11 ～ 146.112.63.13

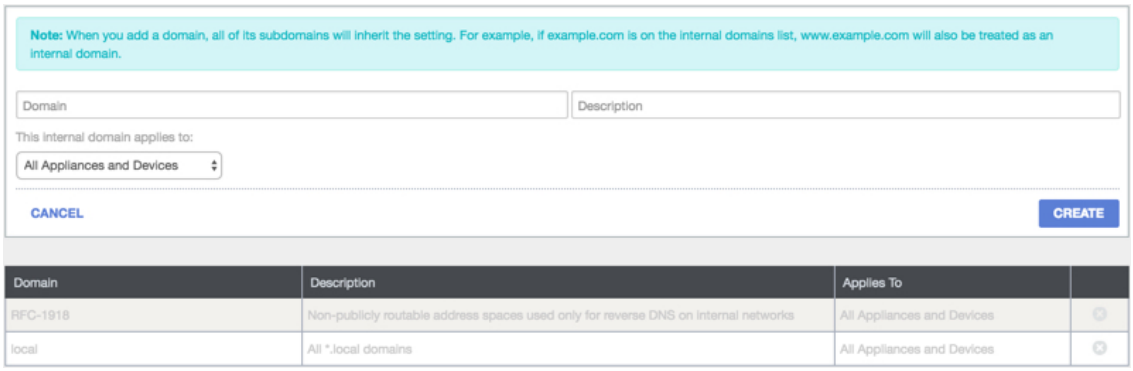
ソフトウェア

- Umbrella ローミング クライアントは DNS を提供する他のソフトウェアと**互換性がない**ため、DNS 要求に対応するマシンにはインストールしないでください。
- Umbrella ローミング クライアントをインストールする前に、**DNSCrypt** をアンインストールする必要があります。インストーラによってインストールされている DNSCrypt が自動的に検出され、インストールを続行する前にアンインストールするように、管理者にプロンプトが表示されます。

IPv6：現在 Umbrella ローミング クライアントは、IPv6 またはデュアル スタックの IPv4/IPv6 をサポートしていません。詳細については、次の URL を参照してください。
https://support.umbrella.com/hc/en-us/articles/230901268-Umbrella-Roaming-Client-IPv6-Support

内部ドメイン

Umbrella ローミング クライアントを使用すると、すべての DNS ルックアップが、コンピュータから Umbrella グローバル ネットワーク リゾルバに直接送信されます。ただし、Umbrella ローミング クライアントが内部 DNS 要求を内部 DNS サーバに送信して解決するようにするには、次に示すように、Umbrella ダッシュボードの [内部ドメイン（Internal Domains）] セクション（[設定（Settings）] > [内部ドメイン（Internal Domains）] ）にローカル ドメイン名を追加する必要があります。Umbrella ローミング クライアントは、10 分ごとにシスコの API と同期し、新しい**内部ドメイン**の有無をチェックします。これは設定プロセスの**重要な**部分であり、このリストには、Umbrella ローミング クライアントを導入する前に入力する必要があります。



この機能の技術的な詳細を含む内部ドメインの詳細については、「付録 D：内部ドメイン」を参照してください。

次に、Umbrella ローミング クライアントをダウンロードしてインストールします。

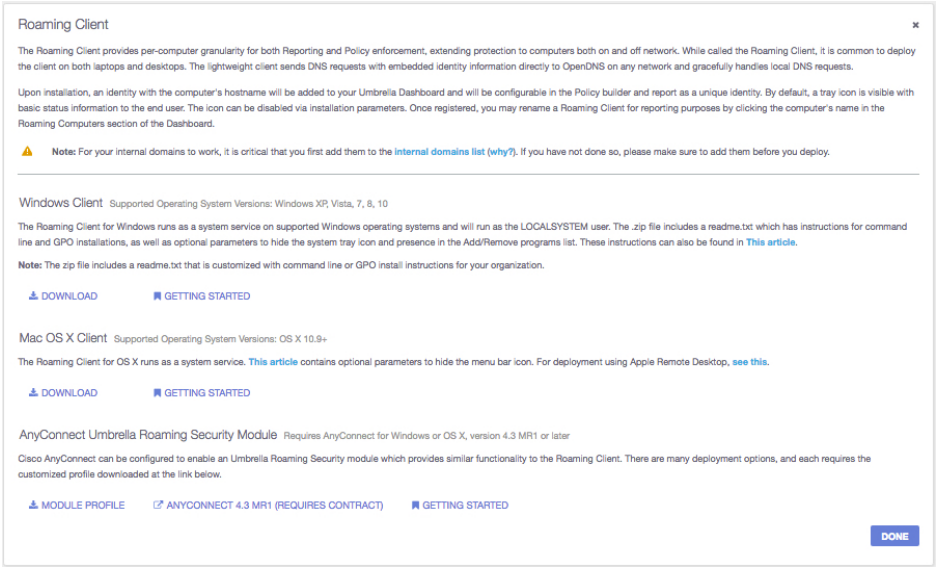
---

1. Umbrella ローミング クライアントの概要 <**2. 前提条件**> 3. ダウンロードとインストール

3. ダウンロードとインストール

Umbrella ローミング クライアントのダウンロード

1. [アイデンティティ(Identities)] > [ローミング コンピュータ(Roaming Computers)] に移動します。
2. [+] (**追加**)アイコンをクリックします。
3. [ダウンロード(Download)] をクリックします。



このセクションには、**Mac** と **Windows** 両方のバージョンのダウンロード リンクに加え、ドキュメントと**内部ドメイン**情報のリンクがあります。

重要

ダウンロードしたインストーラはお客様の組織専用です。**外部に配布しないでください。**

Umbrella ローミング クライアントのインストール

インストールする前に、**前提条件**の記事を読むことをお勧めします。

Umbrella ローミング クライアントのインストール中に、トレイ アイコン（Windows + Mac）を非表示にしたり、削除可能なアプリケーション（Windows のプログラムの追加/削除）に Umbrella ローミング クライアントが表示されないように設定したりできます。それにより、Umbrella ローミング クライアントの存在をわかりにくくして、エンドユーザのマシンで管理者権限によって簡単に削除されるのを防ぐことができます。この方法の詳細については、「Umbrella ローミング クライアント：インストールのコマンド ラインおよびカスタマイズ」をお読みください。

単一マシンへのインストールまたは手動インストール

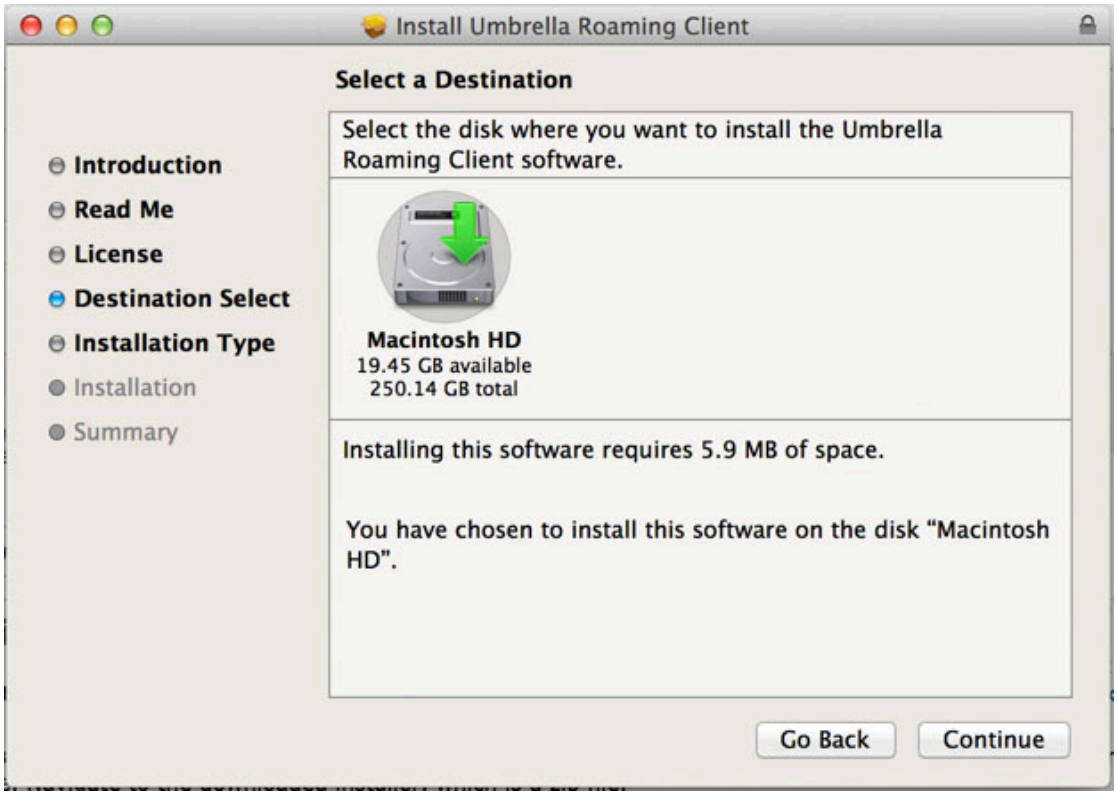
単一のマシンに手動でインストールする方法は、限られた数のコンピュータにローミング クライアントをインストールする小規模の組織に最適です。ローミング クライアントをシンプルに手動でインストールするほうが、インストールを自動化するよりも効率的であるためです。単一のマシンにインストールする方法は、他のアプリケーションのインストールと同様に非常に簡単です。

この方法は、大規模な自動導入に先立って特定のワークステーションに試験的に導入する際にも役立ちます。

ステップ 1：ローミング クライアントをダウンロードする

1. [アイデンティティ（Identities）] > [ローミング コンピュータ（Roaming Computers）] に移動します。
2. [**+**]（**追加**アイコン）をクリックします。
3. [ダウンロード（Download）] をクリックします。

ステップ 2:インストーラを展開し、ウィザードに従う



ステップ 3:トレイ アイコンでインストールを確認する

分散インストールまたは自動インストール

分散インストールは、Group Policy Objects、Apple Remote Desktop などの導入ツールや、自動ソフトウェア インストール用のその他のツールを使用した、大規模な導入に適しています。

シスコでは、ほとんどのソフトウェア導入ツールで使用されているコマンド ライン インストールによる導入について、詳細なガイドを用意しています。

- インストールに使用できるコマンド ライン パラメータとカスタマイズ

シスコでは、一般的なソフトウェア導入ツール別のガイドを提供しています。

- **Windows 2003 での GPO を使用した導入**
- **Windows 2008 R2 および Windows 2012 での GPO を使用した導入**
- **SuperORCA を使用したアプリケーション インストールによる導入**
- **Apple Remote Desktop を使用した導入**
- **標準イメージを使用した導入**

---

2. 前提条件 **<3. ダウンロードとインストール>** 4. 動作の確認

4. 動作の確認

Cisco Umbrella ローミング クライアントをインストールしたら、正常にインストールされているか、そして正常に動作しているかを確認します。

この記事で説明するように、Umbrella ダッシュボードまたはトレイ アイコンでインジケータが緑色である場合は、Umbrella ローミング クライアントが正常に動作しています。ステータス インジケータが緑色以外の場合については、***付録 A*** を参照してください。

ターゲット コンピュータでの確認

デフォルトでは、Mac と Windows 両方のインストールで、トレイ アイコンがインストールされて表示されます。

コマンド ライン/分散インストールでフラグを使用してトレイ アイコンを***インストールしない***ことを選択しないかぎり、インストールが完了した時点でトレイ アイコンが表示されます。

Umbrella ローミング クライアントをインストールしたマシンでこのことを確認します。

Umbrella ダッシュボードでの確認

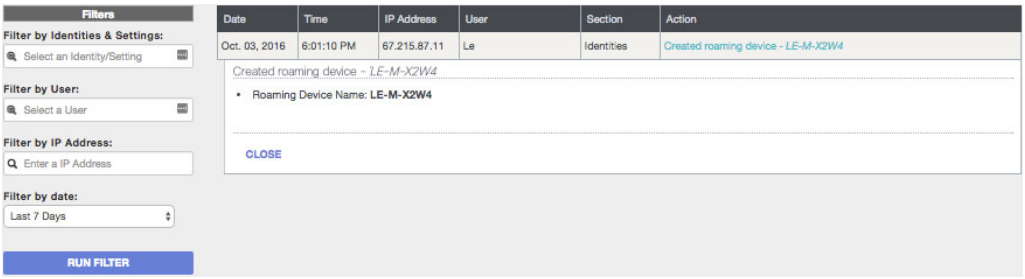
Umbrella ローミング クライアントがインストールされたことをダッシュボードで確認するには、2 つの方法があります。

管理者監査ログ

1. Umbrella にログインし、[レポート（Reporting）] > [管理者監査ログ（Admin Audit Log）] に移動します。

2. [フィルタ（Filters）] の [アイデンティティと設定によってフィルタ（Filter by Identities & Settings）] に、コンピュータのホスト名を入力します。

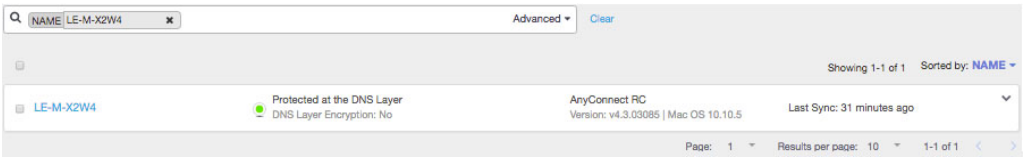
3. [フィルタの実行（Run Filter）] をクリックします。



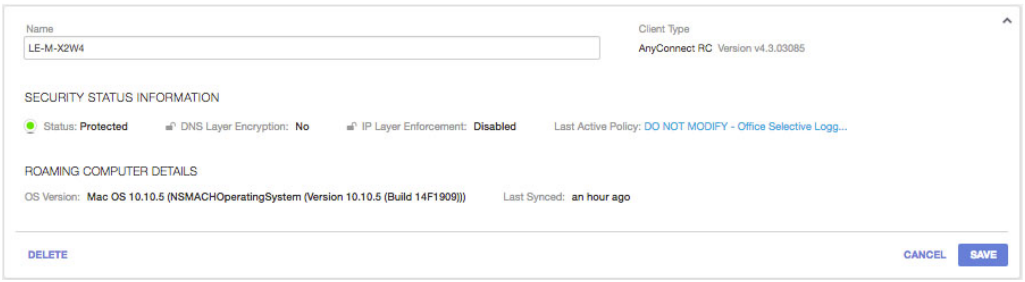
4. 特定のタイムラインを見て、Umbrella ローミング クライアントのインストールがログに記録されていることを確認することもできます。

ローミング コンピュータ ページ

1. Umbrella にログインし、[アイデンティティ（Identities）] > [ローミング コンピュータ（Roaming Computers）] に移動します。Umbrella ローミング クライアントをインストールした各マシンのホスト名と、ステータスおよびポリシー情報が表示されます。管理者監査ログと同じ方法でホスト名を検索することもできます。



2. 名前をクリックして展開します。



---

3. ダウンロードとインストール < **4. 動作の確認** > 5. ポリシーの設定

5. ポリシーの設定

概要

ポリシーを設定して Cisco Umbrella でポリシーの順序を設定する方法がわからない場合は、先に進む前に**ポリシーの作成と管理のためのセットアップ ガイド**をお読みください。

この記事では、ローミング コンピュータにおけるオンネットワークのポリシーとオフネットワークのポリシーの作成について説明しています。コンテンツ フィルタリングとセキュリティに関して、Umbrella ローミング クライアント、ネットワーク、および Umbrella のその他のアイデンティティに対して単一の統合ポリシーを適用する必要であり、オンネットワークにおける許可とオフネットワークにおける許可を異なるものにしたくない場合、この記事をスキップして標準の『*Setup Guide（セットアップ ガイド）*』を参照してください。

組織の IT ポリシーによっては、***オフネットワーク***と***オンネットワーク***のコンテンツ フィルタリング ポリシーを別個に設定できます。「コンテンツ ロギング」を無効にして、セキュリティ関連イベントだけをレポートに記録することもできます。その際、リモート ロケーションでの接続時にも、エンド ユーザのプライバシーは保持されます。

Umbrella では、これを簡単に行うことができます。ネットワーク使用時のポリシーを作成し、ローミング用の類似するポリシーに優先させるだけで実現します。

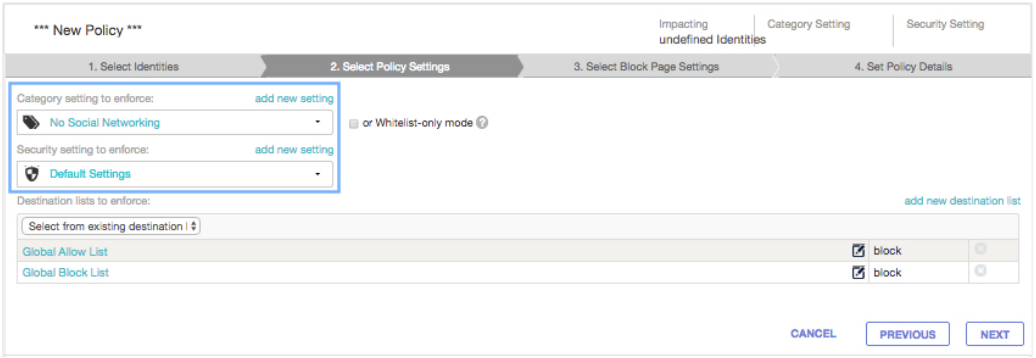
ステップ 1：オンネットワーク ポリシーを作成する

最初に、ローカル ネットワーク上のすべてのユーザ（Umbrella ローミング クライアントがインストールされているかを問わない）に適用するポリシーを作成します。

1. [ポリシー（Policies）] > [ポリシー リスト（Policy List）] の順に移動します。
2. [**+**]（**追加**アイコン）をクリックします。

3. ポリシー ウィザードのステップ 1 で、すべてのネットワーク(または個々のネットワーク)を選択し、ローミング コンピュータは選択しません。

4. [次へ(Next)] をクリックし、ポリシー ウィザードのステップ 2 で、オンネットワークで適用する [コンテンツ設定(Content Settings)] と [セキュリティ設定(Security Settings)] を選択します。



6. [次へ(Next)] をクリックし、ポリシー ウィザードのステップ 3 で、適切な [ブロック ページ設定(Block Page Settings)] と [ポリシー詳細(Policy Details)] を選択します。

7. [次へ(Next)] をクリックし、ポリシー ウィザードの最終ステップで、ポリシーに名前を付けて [保存(Save)] をクリックします。
ローミング コンピュータにポリシーが適用されるまで、最大 90 秒かかります。

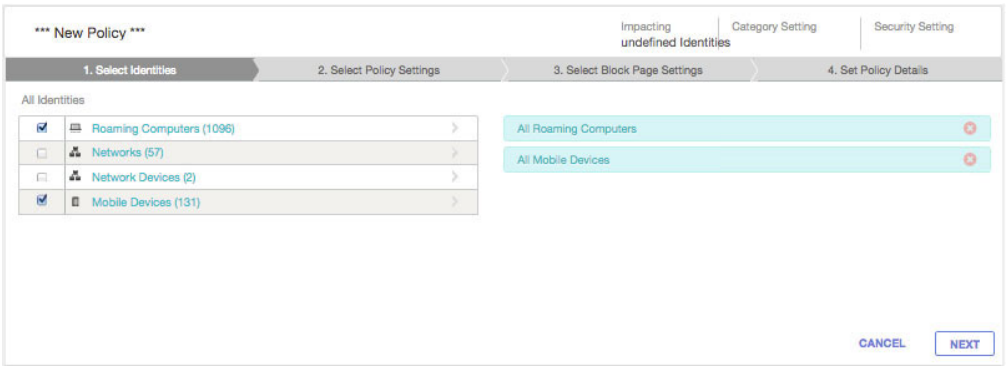
ステップ 2:オフネットワーク ポリシーを作成する

次に、ネットワーク外で接続しているときに、すべてのローミング コンピュータのユーザに適用するポリシーを作成します。

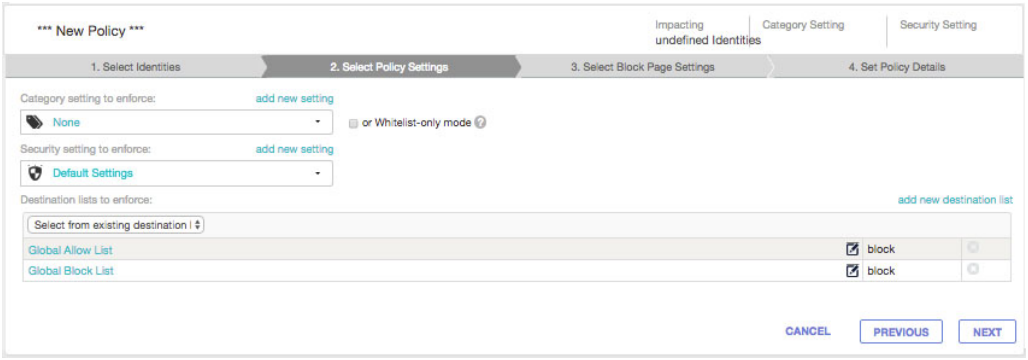
1. [ポリシー(Policies)] > [ポリシー リスト(Policy List)] の順に移動します。

2. [+] (**追加**アイコン)をクリックします。
注:VPN 経由でいずれかのネットワークに再度接続したユーザには、オンネットワーク ポリシーが適用され、コンピュータが再度ネットワークの一部になります。

3. 次に示すように、すべて、または複数のローミング コンピュータを選択します（ただしネットワークは選択しない）。



4. [次へ（Next）] をクリックし、ポリシー ウィザードのステップ 2 で、ネットワーク外にいるときに適用する [コンテンツ設定（Content Settings）] と [セキュリティ設定（Security Settings）] を選択します。ビジネスでの一般的な使用では、デフォルトのセキュリティ設定を有効にし、コンテンツ フィルタリングを無効にしてユーザのプライバシーを保持します。



5. [次へ（Next）] をクリックし、ポリシー ウィザードのステップ 3 で、適切な [ブロック ページ設定（Block Page Settings）] と [ポリシー詳細（Policy Details）] を選択します。

6. [次へ（Next）] をクリックし、ポリシー ウィザードの最終ステップで、ポリシーに名前を付けて [保存（Save）] をクリックします。
ローミング コンピュータにポリシーが適用されるまで、最大 90 秒かかります。

ステップ 3:ポリシーの順序を適切に設定する

最も重要なこととして、ネットワークのポリシーがローミング コンピュータのポリシーよりも上位になるように設定します。ポリシーの順序を変更するには、横線のアイコンを使用してポリシーをドラッグ アンド ドロップします。

ユーザがネットワーク上にいる場合は、ネットワーク ポリシーが優先します。ただしローミング コンピュータがオフネットワークである場合は、ローミング ポリシーが有効になります。

注:

ユーザがネットワーク上にいる場合は、ネットワーク ポリシーが優先します。ただしローミング コンピュータがオフネットワークである場合は、ローミング ポリシーが有効になります。

---

4. 動作の確認 <**5. ポリシー設定**> 6. IP レイヤ適用の追加

6. IP レイヤ適用の追加

Umbrella ローミング クライアントによる IP レイヤ適用

このドキュメントでは、IP レイヤ適用機能の設定方法を説明します。またこの機能の動作とテスト方法、さらにソフトウェアやハードウェアを追加する必要なく機能を実現した方法について、詳細を示します。

注:この機能は、Umbrella Insights または Umbrella Platform パッケージを購入したお客様か、Umbrella for MSP を使用するお客様のみ使用できます。

組織の Mac と Windows の両方で IP レイヤ適用を有効にするには、バージョン 2.0.1 以降の Umbrella ローミング クライアントが必要になります。Umbrella ローミング クライアントがこのバージョンに自動的にアップグレードされない場合は、オフラインになっているか、インストールが破損している可能性があります。

デスクトップの場合でも、必ず Umbrella ローミング クライアントを導入して、この追加保護機能を利用することをお勧めします。

目次

IP レイヤ適用の概要

Cisco Umbrella はすでに世界中に最高度の脅威保護と予測型セキュリティを提供していますが、マルウェア作成者は完全修飾ドメイン名ではなく IP アドレスを使用して、マルウェアをホストする場合があります。Umbrella では主に悪意のあるドメインと URL に対する防御を提供しているため、こうした攻撃に対応する必要性も認識しています。

マルウェアの作成者は、脅威の作成時に DNS ルックアップをバイパスする IP アドレスを使用する可能性があります。たとえば、ユーザがオフィス外でファイアウォールで保護されていない状態で、http://x.x.x.x/malware.exe のように IP アドレスが含まれた URL が記載されたフィッシング メールを受信することがあります。あるいはユーザが自宅に帰り、感染している USB スティックをコンピュータに挿入して子供の宿題を確認し、http://x.x.x.x:3000/malicious/bad.exe にアクセスするマルウェアを実行する可能性があります。

通常マルウェアの作者は、IP アドレスではなくドメイン名を使用します。それには理由があります。マルウェアをホストする IP アドレスは直ちにブロックされるか、その IP アドレスを認識している ISP によって削除されますが、ドメイン名は常に新しい IP アドレスに解決されるためです。ただし例外もあるため、シスコではセキュリティ適用範囲を最大にするために、特定の状況で IP をブロックする必要性を認識しています。不正であることが認知されている IP アドレスもあります。その他にも、HTTP ポート以外のポートで有効なコンテンツをホストしながら、Web ポートで悪意のあるコンテンツをホストしている IP アドレスもあります。その逆も同様です。正当な HTTP Web サイトをホストしながら、非標準ポートで悪意のあるコマンド/コントロール ホストをホストしている IP アドレスも存在します。IP レイヤ適用では、これらすべてのシナリオに対応できます。

開始する

前提条件

注:現在この機能は、Windows ではバージョン 1.7.320 およびバージョン 2.0.1 以降の Umbrella ローミング クライアント、Mac OS X ではバージョン 1.7.30 およびバージョン 2.0.1 以降の Umbrella ローミング クライアントでのみ使用できます。この機能は、ポリシーで有効になっていても、それ以前のバージョンの Umbrella ローミング クライアントでは使用できません。

- Windows または Mac 用の Umbrella ローミング クライアントをインストールして有効にし、Windows と Mac OS X の両方でバージョン 2.0.1+ を実行するローカル UI と Umbrella ダッシュボードで、暗号化および保護された状態として表示される必要があります。

- 互換性のある Windows のバージョン：7、8、8.1、10
    - 注：Umbrella IP レイヤ適用は、Windows 10 バージョン 10.0.10586.14 以降と互換性があると考えられます。ただし広範かつ長期的なテストを実施していないため、サポートまたは正常な動作は保証していません。IP レイヤ適用が機能しない場合、正常にシャットダウンされるため、ネットワーク接続や DNS レイヤの保護に影響することはありません。
- 互換性のない Windows のバージョン：Windows XP、Vista
- サポートされる Mac OS X のバージョン：10.7 以降 Umbrella ローミング クライアントでは、ベータ版の Mac OS X の「El Capitan 10.11」リリースはサポートされていませんが、メインラインのリリースはサポートされています。
    - Mac OS X の既知の問題：Mac OS X デバイスの場合のみ、「信頼ネットワーク」に接続されている顧客の既存の VPN クライアント（AnyConnect や JunOS/Pulse Secure など）を、非アクティブなトンネルを使用して実行したときに問題が発生しています。このシナリオでは、エンド ユーザに対してエラー ポップアップが表示されます。サポートはこの問題を認識しており、トラブルシューティングを支援できます。この問題が発生した場合は、チケットをオープンしてください。

IPv6：現在 Umbrella ローミング クライアントは、IPv6 またはデュアル スタックの IPv4/IPv6 をサポートしていません。詳細については、次の URL を参照してください。
https://support.umbrella.com/hc/en-us/articles/230901268-Umbrella-Roaming-Client-IPv6-Support

- Umbrella ローミング クライアントが仮想アプライアンス（VA）の背後にある場合、Umbrella ローミング クライアントに適用されるポリシーは、Umbrella ローミング クライアントのアイデンティティ用ではなく VA のアイデンティティ用のポリシーになるため、テストが困難になります。詳細については、このガイドの次のセクションを参照してください。
- インターネット プロトコル セキュリティ（IPSec）トラフィックは、ファイアウォールを通過できるようにする必要があります。次のポートとプロトコルを許可する必要があります。
    - プロトコル 50（ESP）
    - プロトコル 51（AH）
    - UDP ポート 500
    - UDP ポート 4500

IPSec では、カプセル化セキュリティ プロトコル（ESP）に IP プロトコル 50、認証ヘッダー（AH）に IP プロトコル 51、IKE フェーズ 1 ネゴシエーションおよびフェーズ 2 ネゴシエーションに UDP ポート 500 を使用します。UDP ポート 4500 も使用されます。

悪意のある IP のブロックを提供している Umbrella サーバだけに IPSec を制限するには、次の IP 範囲についてのみ、ESP、AH、UDP ポート 500、および UDP ポート 4500 を許可します。

67.215.82.0/23 67.215.84.0/23 67.215.86.0/24 204.194.237.0/24 204.194.238.0/23 208.67.216.0/23 204.194.239.0/24 208.69.32.0/22 208.69.36.0/23

使用されているすべての Umbrella 範囲へのアクセスを許可する場合は、次の IP を指定します。

67.215.64.0/19 204.194.232.0/21 208.67.216.0/21 208.69.32.0/21

注：範囲だけでなく、正確な IP アドレスの完全なリストは、この記事の最後に添付されているテキスト ファイルで確認できます。

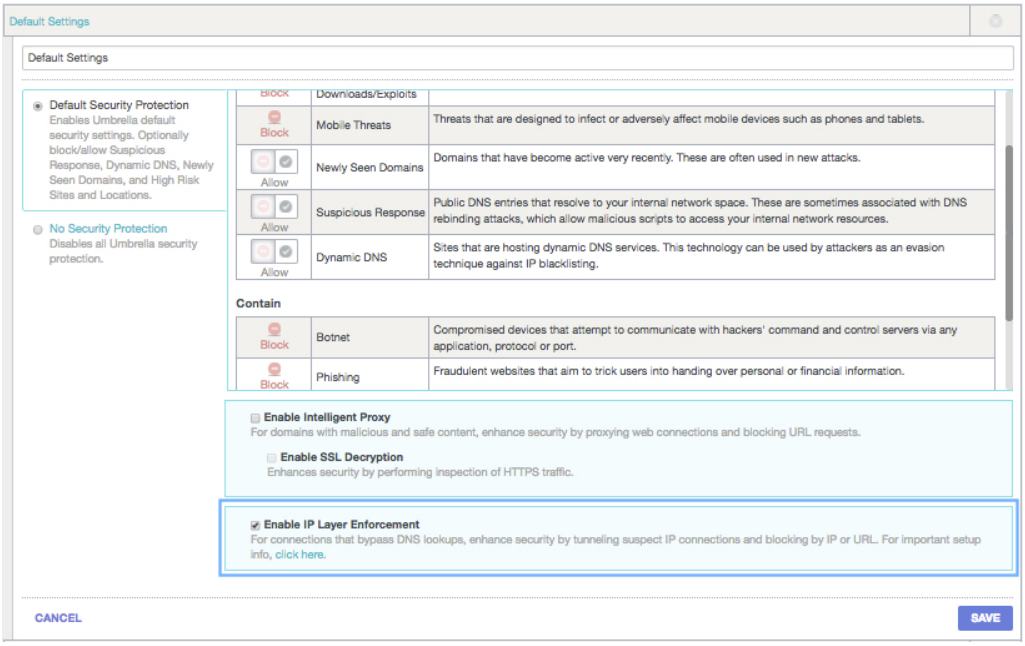
Umbrella ローミング クライアントでの IP レイヤ適用の有効化

この機能をポリシーで有効にするには、次の手順を実行します。

1. [ポリシー（Policies）] > [セキュリティ カテゴリ（Security Categories）] に移動します。

2. 既存のセキュリティ設定を編集するか、新しいセキュリティ設定を追加します。

3. セキュリティ設定の最後で、[IP レイヤ適用を有効にする（Enable IP Layer Enforcement）] をオンにします。

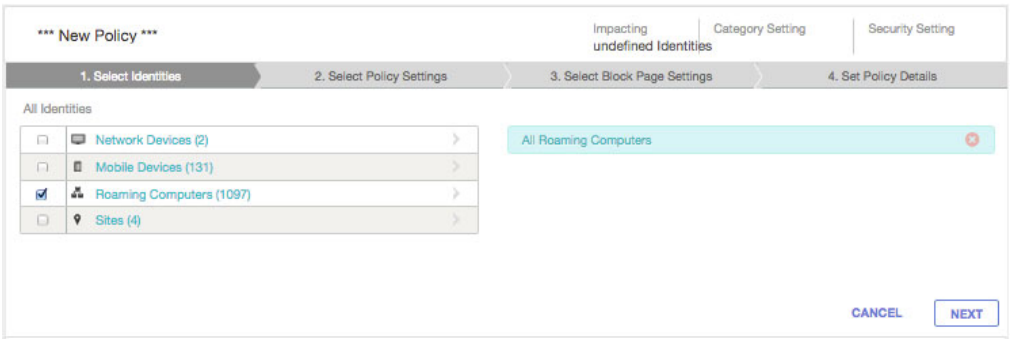


4. [保存（Save）] をクリックします。

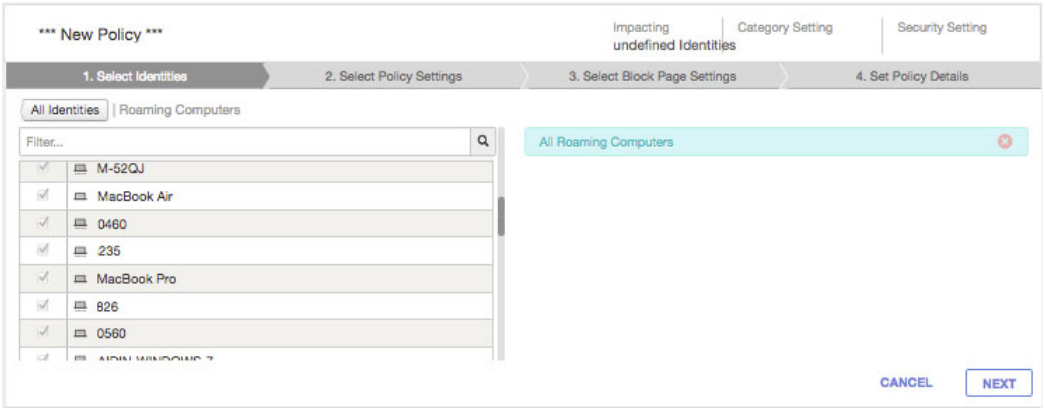
評価グループの一部である Umbrella ローミング クライアントだけに IP レイヤ適用ポリシーを適用するには、セキュリティ設定を有効にして IP レイヤ適用する前に、新しいポリシーを作成することをお勧めします。次の手順を実行します。

1. [ポリシー（Policies）] > [ポリシー リスト（Policy List）] の順に移動します。

2. [+]（**追加**アイコン）をクリックします。



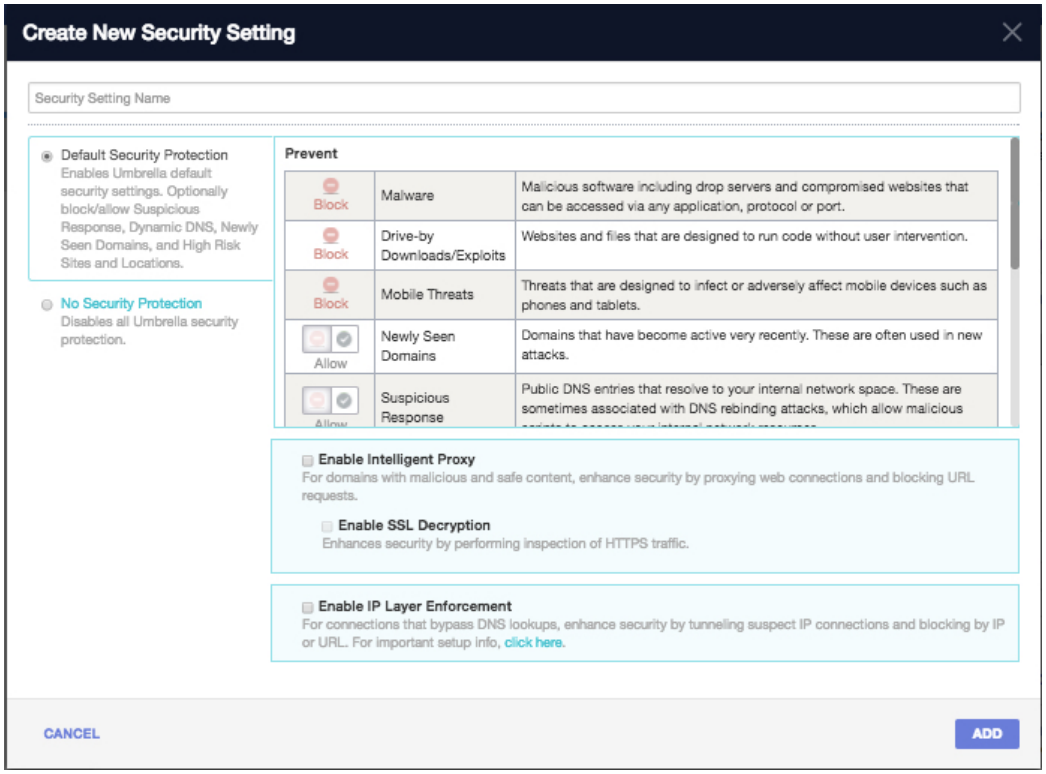
3. ポリシー ウィザードのステップ 1 で、ローミング コンピュータの [>]（**展開**アイコン）をクリックし、評価に含めるローミング コンピュータのみを選択します。



4. [次へ（Next）] をクリックします。

5. ポリシー ウィザードのステップ 3 の [適用するカテゴリ設定（Category setting to enforce）] で [新しい設定の追加（add new setting）] をクリックします。

6. [新しいセキュリティ設定の作成（Create New Security Setting）] モードで、設定にわかりやすい名前を付け、[デフォルトのセキュリティ保護（Default Security Protection）] を（設定はそのままで）選択し、[IP レイヤ適用を有効にする（Enable IP Layer Enforcement）] をオンにして [追加（Add）] をクリックします。

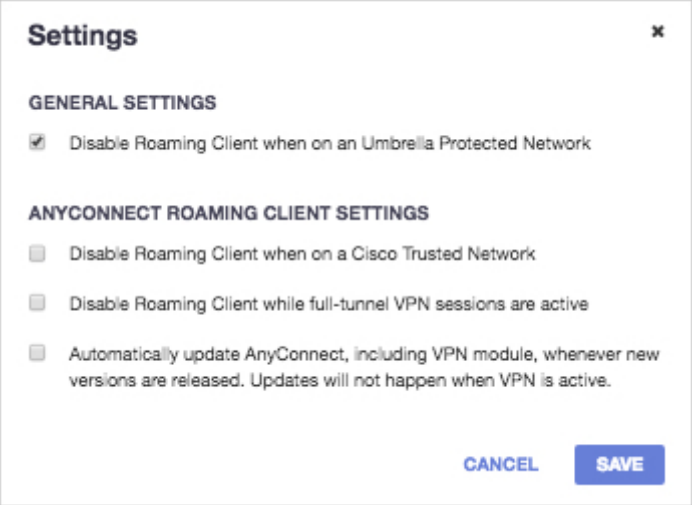


7. [次へ（Next）] をクリックし、ポリシー ウィザードのステップ 3 で、適切な [ブロック ページ設定（Block Page Settings）] と [ポリシー詳細（Policy Details）] を選択します。

8. [次へ（Next）] をクリックし、ポリシー ウィザードの最終ステップで、ポリシーに名前を付けて [保存（Save）] をクリックします。
   ローミング コンピュータにポリシーが適用されるまで、最大 90 秒かかります。

IP レイヤ適用は、Umbrella ローミング クライアントがインストールされている Windows または Mac のローミング コンピュータだけに適用されます。ただし IP レイヤ適用は、Umbrella ローミング クライアントが VA の背後にある場合でも引き続きアクティブになります。その場合、Umbrella ローミング クライアントのその他のセキュリティ機能（およびフィルタリング設定）はインスタンス内でバックオフされ、設定に応じて、代わりにネットワーク、内部ネットワーク、または Active Directory ユーザ/コンピュータのポリシーが適用されます。

Umbrella ローミング クライアントが、Umbrella ダッシュボードに追加されたネットワークによって保護され、ローミング コンピュータ設定（[アイデンティティ（Identities）] > [ローミング コンピュータ（Roaming Computer）] >（設定アイコン））が [Umbrella で保護されているネットワークではローミング クライアントを無効にする（Disable Roaming Client when on an Umbrella Protected Network）] に設定されている場合、Umbrella ローミング クライアントは基本的に無効になり、IP レイヤ適用以外のすべての機能がネットワークの保護に依存するようになります。

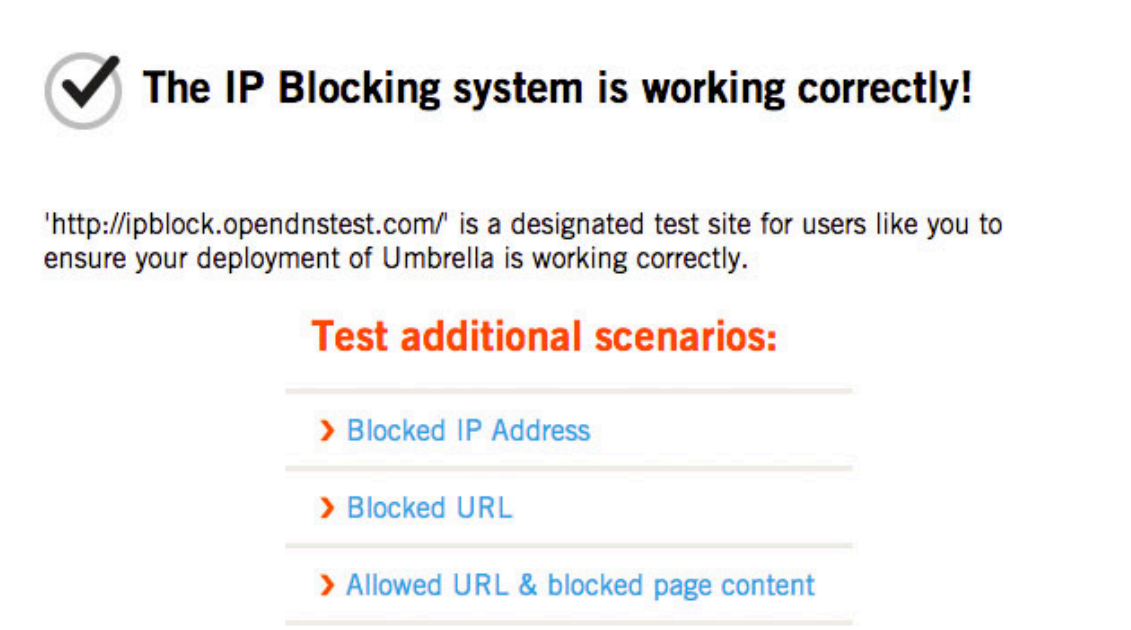


IP レイヤ適用は Umbrella ローミング クライアントとは別個になっているため、ネットワークの背後にいる場合には、その他の Umbrella ローミング クライアントと動作が異なります。これは、ほとんどの機能がネットワークまたは VA の機能と重複する一方で、IP レイヤ適用は Umbrella ローミング クライアント固有の機能であるためです。

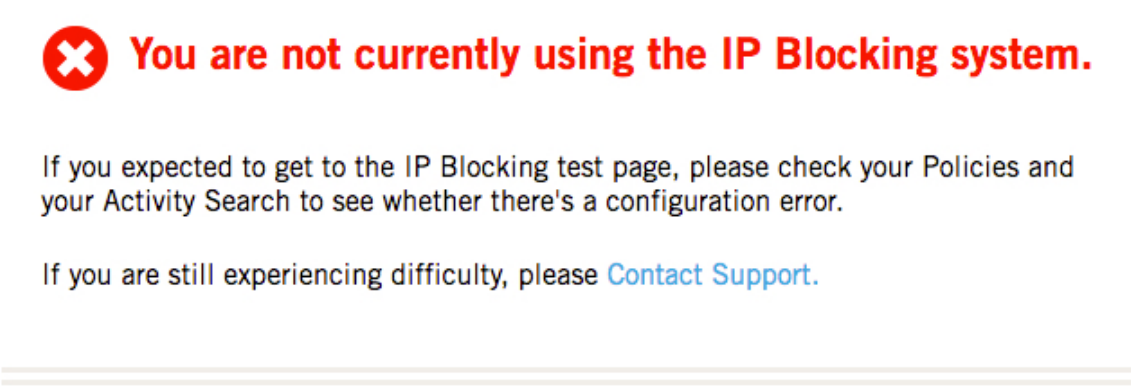
IP レイヤ適用のテスト

IP レイヤ適用によって悪意のある IP がブロックされていることをテストするために、http://ipblock.opendnstest.com/ にテスト ページが設定されています。

このページは、コンピュータにインストールされている Umbrella ローミング クライアントに対して IP レイヤ適用が有効に機能している場合に正しく表示されます。その他のシナリオを自由にテストして、悪意のある IP アドレスをブロックする際の動作を確認してください。



予期したとおりに機能していない場合、またはテスト対象のローミング コンピュータで機能が有効になっていない場合には、次のように表示されます。



ポリシーを可能なかぎり適切に設定しても、テスト ページに IP レイヤ適用の有効化が反映されない場合は、このローミング コンピュータに適用されているポリシーで IP レイヤ適用機能が有効になっていない可能性があります。ダッシュボードで、該当するアイデンティティのポリシーの優先順位を再度チェックしてください。

トラブルシューティングを開始する場合は、次の発信ポートで、暗号化された DNS 要求が Umbrella グローバル ネットワークを通じてルーティングされるように設定されていることを確認してください。

- Umbrella へのポート 53 TCP/UDP
- Umbrella へのポート 443 TCP

この機能のシステム要件が満たされていることを再度チェックしてください。

問題が解決されない場合、または IP レイヤ適用機能を有効にしたときに予期しないまたは異常な動作があった場合は、サポートまでご連絡ください。電子メールでのお問い合わせ先：umbrella-support@cisco.com

FAQ

Q：Umbrella ローミング クライアントが IP レイヤ適用のためにサーバに接続できない場合はどうなりますか？
A：VPN が接続できない場合は、引き続き接続が試行されますが、バックオフされるため、他のサービスを妨げることはありません。VPN サーバが使用できない場合、VPN はフェール クローズして他のトラフィックをブロックすることはなく、フェール オープンになります。

Q：Umbrella ローミング クライアントは利用中の Umbrella サービスにどのように影響しますか？
A：オンネットワークとオフネットワークのセキュリティ機能のギャップを改善する他には、変更はありません。疑わしくないと見なされる IP アドレスに対するダイレクトな要求は影響を受けません。Umbrella ローミング クライアントに配信されるルーティング テーブルにリストされている IP アドレスまたは特定の範囲の IP に対する直接接続のみ影響を受け、それらの IP に対する接続試行にのみ IP レイヤ適用が機能します。

Q：IP レイヤ適用のための VPN は保護されますか？
A：IP レイヤ適用のためのセキュア トンネルは IPSec に基づいているため、Umbrella ローミング クライアントがインストールされているコンピュータと Umbrella サービス間のトラフィックが暗号化され、エンドツーエンドの整合性と機密性が確保されます。

Q：IP レイヤ適用は、インストールされている別の VPN とどのように連動しますか?
A：AnyConnect や JunOS/Pulse Secure など別のアクティブな VPN が検出されると、IP レイヤ適用機能は自動的に「バックオフ」して無効になります。IP レイヤ適用は、VPN が接続されていない場合に有効になります。詳細については、この記事を参照してください。他の VPN ソフトウェアに関する問題があれば、サポートまでご連絡ください。

Q：許可またはブロックする IP のリストを独自に追加することはできますか?
A：この機能の初期のリリースでは、すべてのユーザに対して単一の悪意のある/疑わしい IP リストが使用されます。Umbrella のセキュリティ研究者は、最新の脅威から保護するためにリストを維持し、更新します。ただし、お客様が指定した IP アドレスも積極的に追加する予定であり、このことは「接続先リスト」のロードマップに含まれています。現時点では、限定提供のバージョンで特定の IP または CIDR を許可する機能を利用でき、今後さらに広範なお客様に対してこの機能をリリースしていく予定です。

Q：この VPN アプローチは、既存のポリシー適用とどのように組み合わせることができますか?
A：ポリシー適用はクラウド内で他のポリシーと同じポイントで実行されるため、ポリシーに対して定義した内容も適用されます。たとえばカスタム ブロック ページを設定していて、ブラウザを通じてポート 80 で悪意のある IP にアクセスを試みると、ブロック ページが表示されます。

IP レイヤ適用：高度な詳細

Q：IP レイヤ適用では、ブロックされる IP アドレスはどのように決定されますか?
A：Umbrella ローミング クライアントは疑わしい IP アドレスのリストを Umbrella から取得し、Umbrella API から、新しい IP アドレスの追加を 5 分ごとに自動的にチェックします。バックエンドでの更新は最短 45 分ごとに行われますが、Umbrella ローミング クライアントは 5 分ごとにチェックを行い、可能な限り最新の状態を維持します。

情報はローカル クライアントにダウンロードされ、Umbrella ローミング クライアントが実行されていれば、メモリにロードされます。どの IP アドレスがルーティングされるかの情報は、ディスクには保存されず、メモリだけに保持されます。

IP レイヤ適用機能は Umbrella ローミング クライアント ソフトウェアにバンドルされていますが、実際には別のプロセスとして、Umbrella ローミング クライアントと平行して実行されます。クライアント側プロセスの主な目的は、OS 用の組み込みの VPN クライアントを使用して、IPSec VPN トンネルを作成することにあります。OS X では組み込みの VPN は Raccoon と呼ばれるもので、Windows では RASClient(または RRAS Client)と呼ばれるものです。

Q:Umbrella ローミング クライアントが疑わしい IP アドレスのリストを取得すると、次はどうなりますか?

A:この機能が Umbrella ローミング クライアントのアイデンティティのポリシーで有効になると、ローミング クライアントは、セットアップ記事にある前提条件でリストされている IP アドレスを使用して、IPSec トンネルを確立します。IPSec トンネルはトラフィックが送信される前に確立されるため、トンネルを通じてトラフィックがルーティングされるように準備が完了します。ただし必要になるまでトラフィック フローは確立されません。

リストのいずれかの IP に対して、クライアントのネットワーク スタックからの要求(アプリケーションからの要求またはユーザがコンピュータ上で生成したインターネット要求)があると、Umbrella ローミング クライアントはそのトラフィックに IP レイヤ適用を機能させて、IPSec トンネルを通じてプロキシします。この処理は、Windows と OS X 用の Umbrella ローミング クライアントのバージョンによって多少異なります。

OS X では、IP レイヤ適用プロセスにより、リスト内の各 IP に対するルートが追加されます。ルートが設定されると、それらの IP アドレスに対するトラフィックは、すべて VPN を通じてサーバに送信されます。

Windows の場合はこのプロセスが多少異なります。すべての IP を(OS X のように)ルートとして追加する代わりに、Windows Filtering Platform(https://msdn.microsoft.com/en-us/library/windows/desktop/aa366510(v=vs.85).aspx)を使用して、リスト内のブロック対象の IP アドレスに対する発信パケットを監視します。これらの IP のいずれかに要求が送信されると、ルートがその場で動的に作成され、それ以降、接続先がその IP であるすべてのパケットが、トンネルを通じてサーバに送信されます。その結果、最初の接続試行は失敗する可能性がありますが、TCP の再試行はトンネルを通じて Umbrella に正常に送信されます。

Q：疑わしいトラフィックが Umbrella サーバに到達した場合には、直ちにブロックされますか?

トラフィックが VPN を通じて Umbrella IP レイヤ適用サーバに到達しても、必ずしも直ちに要求がブロックされるわけではありません。代わりに、トラフィックが Umbrella サーバに到達した時点で接続先が検査されます。その IP アドレスについて Umbrella が持っている情報量に応じて、Umbrella は接続先またはトラフィックの代わりにブロック ページの IP を返信するか、特定のコンテンツをブロックできるインテリジェント プロキシに送信します。

まず、基本的なプロセスとして、ブロックされたページの応答を返すかどうかが決定されます。接続先の疑わしい IP に悪意があることがわかっている場合は、ブロックされたページ応答を返します。それ以外の場合は、IP アドレスがグレーリスト（適切または不適切なドメイン/IP のリスト）内に見つかると、トラフィックをインテリジェント プロキシに渡し、その IP を接続先とするトラフィックを引き続きプロキシします。さらにその IP に悪意のある URL が 1 つだけ含まれている場合はブロックし、その IP でホストされているその他すべてのリソースへのアクセスは許可します。

たとえば、完全に正常な Web データを示す IP に、侵害された URL（たとえば http://x.x.x.x/malware.exe）が存在する場合は、その URL をインテリジェント プロキシを使用してブロックします。

別の例としては、無料ダウンロード可能なソフトウェアをホストするファイル配信 Web サイトなどがあります。ドメインのサーバ y.y.y.y には多数のファイルが保存されていて、ほとんどのファイルが安全です。ブラックリストのエントリは y.y.y.y および y.y.y.y/* 接続をブロックし、グレーリストのエントリはインテリジェント プロキシによって http://y.y.y.y/software/windows/malware.exe だけをブロックし、その他の良好なファイルがユーザに送信されるのは許可します。

Q：IP レイヤ適用のための VPN はどこに接続されますか?

IPSec VPN トンネルは、IP レイヤ適用サーバ インフラストラクチャに接続されます。その時点で、インテリジェント プロキシへのトラフィックの送信が可能になり、特定の URL をブロックできます。IP レイヤ適用サーバでは、サーバ自体にセカンダリの完全なバージョンのインテリジェント プロキシが含まれているため、別のサーバ セットに転送して URL を解析する必要はありません。

トンネルが Umbrella サーバに接続されると、ブロックされたページの応答を返すべきかどうかを決定するプロセスが実行されます。接続先の疑わしい IP に悪意があることがわかっている場合は、ブロックされたページ応答を返します。それ以外の場合は、IP がグレーリスト（適切または不適切なドメイン/IP のリスト）内に見つかると、トラフィックをインテリジェント プロキシに渡し、その IP を接続先とするトラフィックを引き続きプロキシします。さらにその IP に悪意のある URL が 1 つだけ含まれている場合はブロックし、その IP でホストされているその他すべてのリソースへのアクセスは許可します。

Q：IP レイヤ適用では、IPSec VPN トンネルが他のセキュリティ チェックのバイパスに使用されないことをどのように保証していますか?
高い技術的知識を持ったユーザや、特殊なマルウェアは、ローミング クライアントがネットワーク外の IP アドレスへのトラフィックをトンネリングさせていることを認識し、そのトンネルを使用してファイアウォールや IDS など、境界線防御をバイパスできると考える可能性があります。Umbrella でそのようなトラフィックが検出されると、ルーティング先のいずれかの IP アドレスを接続先としないトラフィックはドロップされます。将来的には、そのような要求はログに記録され、後で確認できるようになります。

Q：IP レイヤ適用は、エンドポイント上の Umbrella ローミング クライアントにある既存の機能にどのように適合しますか?
IP レイヤ適用とインテリジェント プロキシは、Umbrella ローミング クライアントの機能を拡張し、DNS だけでなく境界を超える保護を可能にする大きな戦略の一部になっています。それにより、よりきめ細かいフィルタリングが可能になり、最新のファイアウォールに近い機能が実現します。

Q：IP レイヤ適用はどのようにトラブルシューティングできますか?
この機能について何らかの問題が発生した場合、またはサポートの協力の下でこの機能を問題として除外する場合は、次の情報が役に立ちます。

- 詳細をロギングするための診断テスト
- 何らかの VPN クライアント（Umbrella ローミング クライアント機能以外）を使用しているか
- ネットワークの上流に、必要なポートでトラフィックをブロックできるネットワークデバイスが他にあるか
  IP レイヤ適用が機能していることを迅速にテストするには、http://ipblock.opendnstest.com/ を確認します。トンネルが設定されて有効になっていると、正常な処理がここに記録されます。

信頼できない接続が見つかったか、他の VPN ソフトウェアで問題が発生した場合は、VPN を確立していない状態で、IP レイヤ適用システムが機能していることを（上記のテストによって）確認します。システムが機能していれば、IP レイヤ適用機能を無効にし、VPN に再接続することで、その問題が VPN の互換性の競合によるものかどうかを確認します。

IP レイヤ適用機能を無効にすると VPN が問題なく機能し、有効にすると問題が発生する場合は、サポートまでご連絡ください。

Q：互換性のないプログラムはありますか?
既知の互換性のないプログラムを次に示します。

- Peerblock：このソフトウェアは、ルーティング テーブルにエントリがある IP をブロックします。受信した IP レイヤ適用の IP（キャリアグレード NAT 範囲で使用する 100.64.0.0/10 内）が PeerBlock によってブロックされると、IP レイヤ適用機能が動作しなくなります。

---

5. ポリシー設定 <**6. IP レイヤ適用の追加**> 付録 A：ステータスおよび機能

付録 A: ステータス、状態、機能

概要

Cisco Umbrella ローミング クライアントのステータス(Umbrella ローミング クライアントの現在の状態)は、Umbrella ダッシュボードの [アイデンティティ(Identities)] > [ローミング コンピュータ(Roaming Computers)] と、ローカル マシンの Umbrella ローミング クライアントのトレイ アイコンの両方で確認できます。

注:インストール時にトレイ アイコンを非表示に設定することができます。

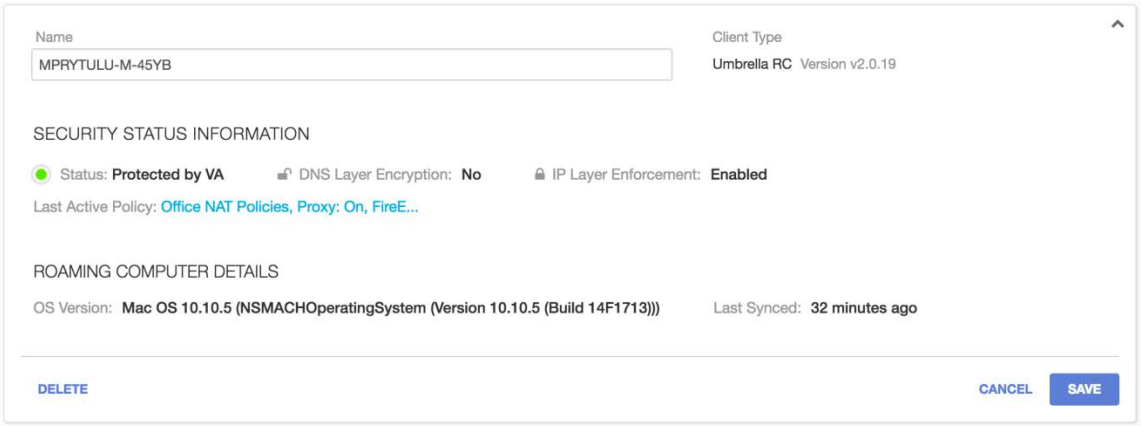
Umbrella ローミング クライアントが動作する状態は、現行のネットワーク環境によって異なります。この状態により、Umbrella ローミング クライアントの動作と、Cisco Umbrella のどのポリシーを適用すべきかを把握できます。Umbrella ローミング クライアントの状態によって、次のことを把握できます。

- 適用する Umbrella ポリシー
- DNS 設定
- DNS 暗号化が可能かどうか

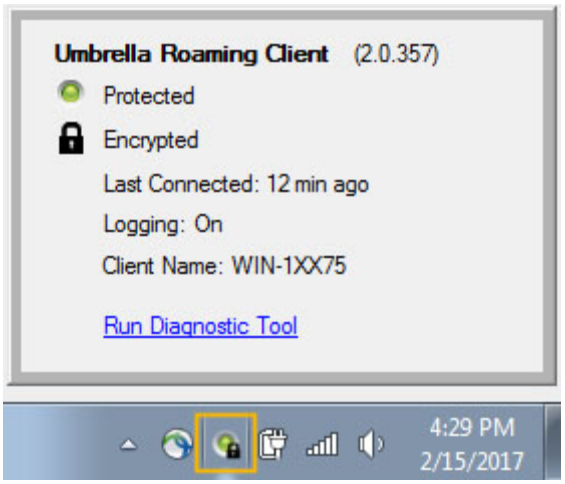
Umbrella ダッシュボード内のステータス

[アイデンティティ(Identities)] > [ローミング コンピュータ(Roaming Computers)] に移動します。

各ローミング コンピュータを展開して、追加情報を確認することもできます。



トレイのステータス



Umbrella ダッシュボードに表示される Umbrella ローミング クライアントのステータス

Umbrella ダッシュボードでは、Umbrella ローミング クライアントの現在の動作モードを示す、ステータスやその他の情報を確認できます。

[クライアント名（Client Name）]

コンピュータのホスト名

[ステータス（Status）]

Umbrella ローミング クライアントの現在の状態を表示します。

緑色の状態（保護）:

- [保護（Protected）] :Umbrella ダッシュボードの適切なポリシー設定が適用されており、コンピュータが DNS サーバと通信できます。ポリシーによっては、IP レイヤ適用の有効/無効も表示されます。
- [保護および暗号化（Protected &Encrypted）] :保護状態と基本的に同じですが、送信時に DNS クエリが暗号化されます。ポリシーによっては、IP レイヤ適用の有効/無効も表示されます。
- [VA による保護（Protected byVA）] :Umbrella ローミング クライアントがネットワーク上で VA を検出し、VA が優先されています（DNS と IP レイヤの両方を含む）。
- [ネットワークによる保護（Protected byNetwork）] : Umbrella ローミング クライアントが、現在のネットワークに Umbrella ネットワーク保護ポリシーが適用されていることを検出しています。ローカル DNS サーバとコンピュータが同じ登録済みダッシュボード ネットワークに登録されていて、保護されたネットワーク上では Umbrella ローミング クライアントが無効になるように設定されています。これは設定可能なオプションです。
- **黄色（非保護）**:ポリシーが適用されていません。コンピュータがシスコの DNS サーバと通信できません。
- **グレー（オフライン）**:コンピュータの電源がオフになっており、アクティブなインターネット接続がないか、Umbrella ローミング クライアントが適切にインストールされていないか、インターネットから切断されたときにアンインストールされました。
- **グレー（アンインストール）**:Umbrella ローミング クライアントがエンドポイントからアンインストールされましたが、ダッシュボードからは削除されていません。エンドポイントに再インストールするか、ダッシュボードから削除することができます。

	• **グレー（無効）**：ユーザが Umbrella ローミング クライアントを手動で無効にしました。これは OSX 専用の機能です。この機能に関するドキュメント • *赤色（未登録）*：Umbrella ローミング クライアントが HTTPS 経由でシステムへの初期登録を行うことができません。
[前回の同期（Last Sync）]	コンピュータがシスコの API と前回同期してから経過した時間。API は最大 10 分ごとに同期して更新をチェックし、内部ドメインリストが最新であることを確認します。
[前回の Active Policy（Last Active Policy）]	Umbrella API と前回同期したときに、コンピュータに割り当てられていたポリシー。
[DNS レイヤ暗号化（DNS Layer Encryption）]	ダッシュボードで「ロック アイコン」または「ロック解除アイコン」を表示し、コンピュータと Umbrella 間の DNS 要求が暗号化されているかどうかを示します。 *注：*仮想アプライアンス（VA）の背後にある Umbrella ローミング クライアントは暗号化されません。
[IP レイヤ適用（IP Layer Enforcement）]	ダッシュボードで「ロック アイコン」または「ロック解除アイコン」を表示し、IP レイヤ適用がポリシーで有効になっているか、また Umbrella ローミング クライアント自体で有効かどうかを示します。 *注：*VA の背後にある Umbrella ローミング クライアントでも、IP レイヤ適用は有効のままです。
[クライアント タイプ（Client Type）]	現在インストールされている Umbrella ローミング クライアントのバージョン。通常は「Umbrella RC」にバージョンが続きます。 **注：**バージョンが表示されていない場合、そのマシンは Umbrella と正常に同期されていません。
[OS のバージョン（OS Version）]	Umbrella ローミング クライアントのインストール時に記録される OS のバージョン。 わかりやすい名前と「高度な」名前があり、後者は、Umbrella ローミング クライアントが読み取るシステムに対して OS の製造元が実際に付けた名前です。

[削除（Delete）]	[削除（Delete）] をクリックすると、組織が管理するマシンのリストから、そのマシンが削除されます。エンド ユーザのマシンに Umbrella ローミング クライアントがインストールされている状態で、ダッシュボードから Umbrella ローミング クライアントを削除すると、そのユーザはすべてのセキュリティ機能と内部ドメイン機能を使用できなくなります。先にマシンから Umbrella ローミング クライアントをアンインストールしてください。

トレイ アイコンで表示される Umbrella ローミング クライアントのステータス

トレイ アイコンに表示される Umbrella ローミング クライアントのステータスは、6 つの状態のいずれかになります。このステータスは一連の DNS クエリに基づいて決定され、正しい状態を判断するテストとして使用されます。

Umbrella ローミング クライアントが使用するポートとプロトコルの詳細については、前提条件の記事の「**ネットワーク アクセス**」セクションを参照してください。

状態 アイコンの色	説明
予約済み グレー	アクティブなネットワーク接続がありません。Umbrella ローミング クライアントはアクティブなネットワーク接続が発生するまで待機しています。
オープン イエロー	アクティブなネットワーク接続が少なくとも 1 つあります。しかしそのアクティブな接続において、Umbrella ローミング クライアントはポート 53/UDP を通じて 208.67.222.222 / 208.67.220.220 に接続できていません。ユーザは Umbrella によって保護されていません。もしくは、Umbrella にレポート送信されていません。 システムの DNS 設定は元の設定（DHCP または静的）に戻っています。

透過	グリーンとグレーのロックアイコン	ネットワーク接続がアクティブで、Umbrella ローミング クライアントが 208.67.222.222 / 208.67.220.220 に、ポート 443/UDP ではなく、ポート 53/UDP で接続できています。ユーザは Umbrella によって保護されており、Umbrella にレポートが行われています。ただし、接続は暗号化されていません。
暗号化	グリーンとブラックのロックアイコン	Umbrella ローミング クライアントが、208.67.222.222 / 208.67.220.220 への接続をポート 443/UDP で確立しています。ユーザは保護されており、Umbrella にレポートが送信されています。また、DNS クエリが暗号化されます。内部ドメインについては、DHCP により委任された DNS サーバまたはスタティックに設定された DNS サーバに転送されます。そのため、暗号化はされません。
保護されたネットワーク	グリーンとグレーのロックアイコン	コンピュータが保護されたネットワークの範囲内にあり、組織のダッシュボードで「保護されたネットワーク内では無効」が有効にされています。Umbrella ローミング クライアントにより、DNS 設定が DHCP による設定、もしくはスタティックな設定に戻されています。接続は暗号化されていません。
仮想アプライアンスの範囲内	グリーンとグレーのロックアイコン	コンピュータが、DNS サーバに設定された VA が存在するネットワークに接続されています。Umbrella ローミング クライアントは自身を無効にし、DNS 設定を DHCP による設定、もしくはスタティックな設定に戻しています。接続は暗号化されていません。

プローブ

プローブは、Umbrella ローミング クライアントが高頻度で行う DNS 要求です。ネットワーキング環境のヘルス チェックと分析を行います。Cisco Umbrella ローミング クライアントの動作はこのプローブによって異なり、このプローブによって Umbrella ローミング クライアントの状態が判断されます。

プローブには次のタイプがあります。

- 暗号化
- 非暗号化
- 仮想アプライアンス + 保護されたネットワーク

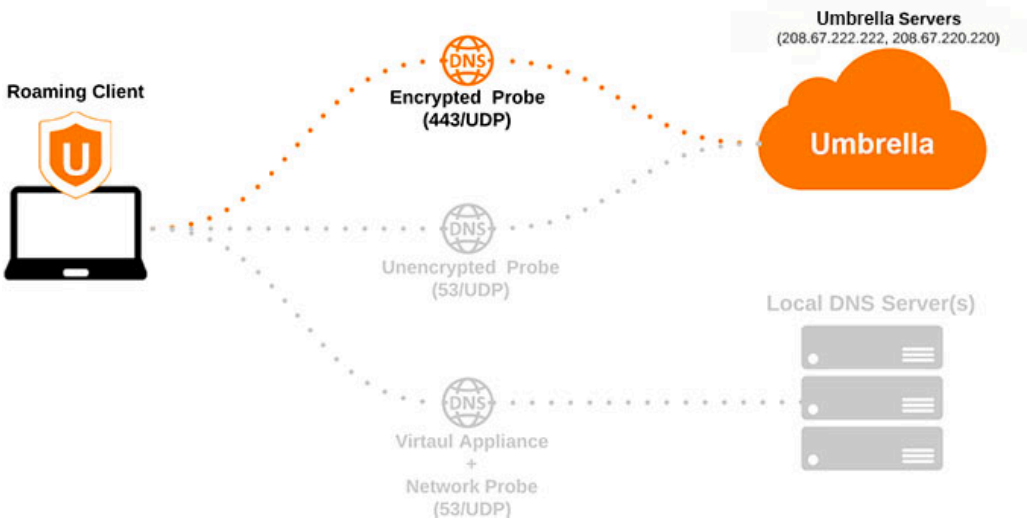
プローブは 208.67.222.222 に送信される DNS クエリであり、debug.opendns.com ドメインに対する TXT タイプのクエリです。これは、ネットワークまたは DNS ログで一般的に見られるクエリです。プローブは約 10 秒ごとに実行され、ネットワーク環境の変化を検知します。2 つのローカル DNS サーバがある一般的なネットワーキング環境では、Umbrella ローミング クライアントは次のプローブを送信します。

- 1 X 暗号化されたプローブ
- 1 X 暗号化されていないプローブ
- 2 X 仮想アプライアンス + 保護されたネットワーク プローブ（ローカル DNS ごとに 1 つ）

暗号化されたプローブ

53/UDP 経由でローカル DNS サーバに DNS 要求を送信します。

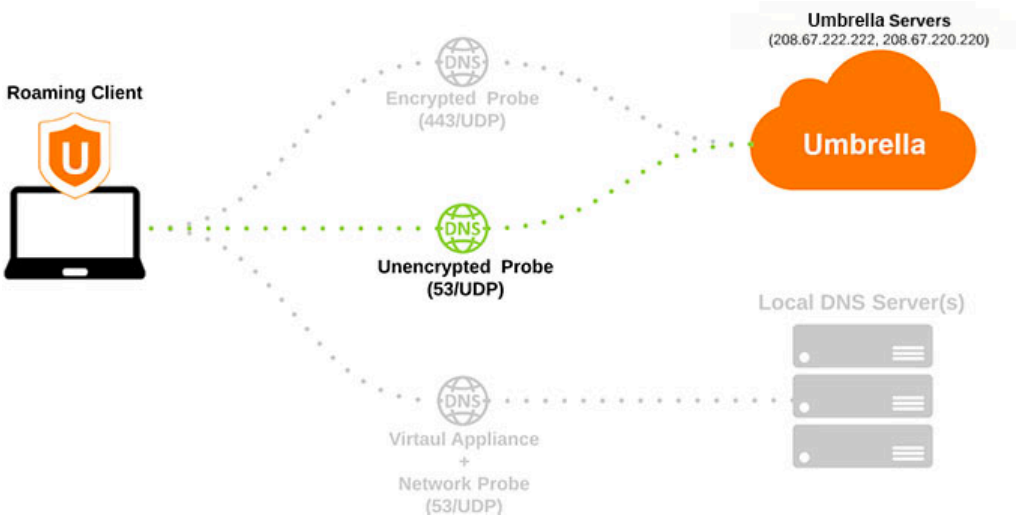
- **成功**：応答。仮想アプライアンス + 保護されたネットワーク プローブが成功しないかぎり暗号化状態で動作します。プローブが成功した場合は、そのどちらかの状態に切り替わります。
- **失敗**：応答なし。非暗号化状態で動作するように試み、確認のために暗号化されていないプローブを送信します。



暗号化されていないプローブ

53/UDP 経由で 208.67.222.222 に DNS 要求を送信します。

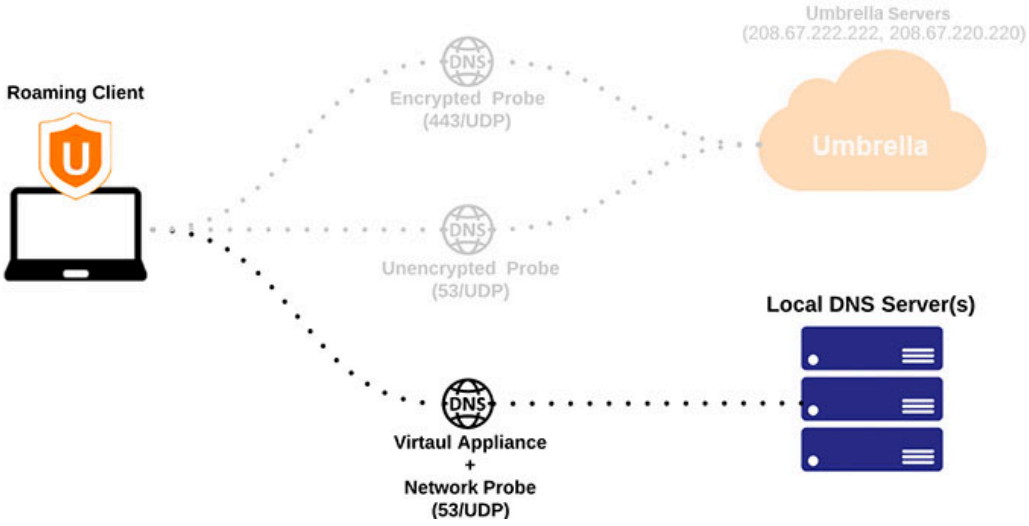
- **成功**:応答。仮想アプライアンス + 保護されたネットワーク プローブが成功しないかぎり非暗号化状態で動作します。プローブが成功した場合は、そのどちらかの状態に切り替わります。
- **失敗**:応答なし。オープン状態に移行します。



仮想アプライアンス + 保護されたネットワーク プローブ

53/UDP 経由でローカル DNS サーバに DNS 要求を送信します。

- **成功**:ローカル DNS サーバは仮想アプライアンスまたは保護されたネットワークであり、暗号化されたプローブまたは暗号化されていないプローブも成功しています。それぞれ VA の背後または保護されたネットワーク状態で動作します。
- **失敗**:ローカル DNS サーバは VA でも保護されたネットワークでもありません。VA の背後または保護されたネットワーク状態では動作しません。



高度：サービスごとのネットワーク アクセス

実行ファイル（バイナリ）単位でネットワーク リストによるアクセスを許可する必要がある防御手段（エンドポイント クライアント ファイアウォール/ウイルス対策）を使用する場合は、次のプロセスでアクセスを許可します。

ERCService.exe（Windows）

dns-updater（Mac OS X）

これらの実行ファイルは、同じネットワーク ベースのタスクを実行します。

- 内部ドメインに対して DNS ルックアップを行う
- ヘルス チェックを実行する（ステータスと機能に関する記事を参照）
- シスコの API と通信する（更新、ダッシュボードの同期ステータス）
- ロギングおよび診断インフラストラクチャと通信する

ポート	プロトコル	接続先
53	UDP	任意
80	TCP	67.215.92.201、67.215.92.210、ocsp.digicert.com、crl4.digicert.com
443	TCP	67.215.92.201、67.215.92.210、ocsp.digicert.com、crl4.digicert.com

注:67.215.92.201、67.215.92.210 IP アドレスは、api.opendns.com および disthost.opendns.com に解決されます。Digicert のドメインは、CDN に基づいて複数の IP アドレスに解決されており、変更される場合があります。現在これらのドメインは、次の IP に解決されます。

- 72.21.91.29
- 117.18.237.29
- 93.184.220.29
- 205.234.175.175

dnscrypt-proxy

暗号化されたおよび暗号化されていない DNS クエリを Umbrella に直接送信します。

Port	プロトコル	接続先
53	UDP	208.67.222.222、208.67.220.220
53	TCP	208.67.222.222、208.67.220.220
443	UDP	208.67.222.222、208.67.220.220

高度:Umbrella ローミング クライアントの状態の変化

コンピュータの電源をオンにするか、ハイバネーションから起動されるか、新しいネットワーク接続が確立されると、Umbrella ローミング クライアントは一連のテストを実行して、適切な状態を決定します。各テストの結果には成功と失敗があります。次のアクションが実行されます(実行順)。

初期の待機段階

Umbrella ローミング クライアントがアクティブなネットワーク接続を検出しなかった場合は、**予約済み**状態で動作し、第 1 段階に入る前にアクティブなネットワーク接続を待機します。

第 1 段階

Umbrella ローミング クライアントが、すべてのインターフェイスで DHCP により委任された DNS サーバまたはスタティックに設定された DNS サーバ経由で、通常の EDNS 要求を送信します。いずれかの DNS 要求が VA を経由したことが検出

されると、成功と見なされ、[VA の背後（Behind VA）] 状態で動作します。VA が検出されなかった場合は失敗と見なされ、第 2 段階に進みます。

第 2 段階

Umbrella ローミング クライアントが、特別に暗号化された EDNS 要求を 443/UDP 経由で 208.67.222.222/208.67.220.220 に送信します。要求によって有効な応答を受信した場合は**成功**と見なされ、Umbrella ローミング クライアントは**暗号化**状態で動作します。要求がタイムアウトになるか拒否された場合は失敗と見なされ、第 3 段階に進みます。

第 3 段階

ローミング クライアントが、ポート 53/UDP 経由で 208.67.222.222/208.67.220.220 に通常の EDNS 要求を送信します。要求によって有効な応答を受信した場合は成功と見なされ、ローミング クライアントは**透過**状態で動作し、**保護されたネットワーク**状態で動作するかを決定する追加テストを送信します。要求がタイムアウトになるか拒否された場合は失敗と見なされ、第 4 段階に進みます。

第 4 段階

Umbrella ローミング クライアントで**すべての**テストが失敗した場合は、すべての DNS 設定が元の DHCP または静的な値に戻され、**オープン**状態で動作します。**オープン**状態への移行には最大 6 秒かかるため、ネットワークでサードパーティ製 DNS がブロックされている場合には、Umbrella ローミング クライアントがこの状態に移行するまで DNS は解決されません。

[非保護（Unprotected ）] ステータス（黄色）

Umbrella ローミング クライアントの*ステータス*（状態ではない）が [非保護（Unprotected）] である場合、Umbrella ローミング クライアントではすべての段階のテストが積極的に行われるため、[保護（Protected）] 状態に可能な限り早く移行します。これは、管理者が突然ファイアウォール ポートを開いたり、あるユーザがパブリック WiFi ネットワークに参加し、WiFi ネットワークのサービス条件の認証または同意が必要になった場合などに、Umbrella ローミング クライアントを再起動する必要がないようにするためです。WiFi 認証またはファイアウォールの変更が行われてから数秒以内に、Umbrella ローミング クライアントは [保護（Protected）] *ステータス*に戻り、適切な状態が選択されます。

付録 B: 仮想アプライアンス

仮想アプライアンスと Umbrella ローミング クライアント

内部ネットワークまたは Active Directory の可視性と粒度のために仮想アプライアンス（VA）を使用している場合、Cisco Umbrella ローミング クライアントの動作は変化します。VA は DNS フォワーダとして機能し、すべてのパブリック DNS 要求を Umbrella に送信し、内部 DNS 要求をネットワークの内部 DNS サーバに送信します。

動作

Umbrella ローミング クライアントを実行しているコンピュータが、DHCP の DNS 設定で VA が設定されているネットワークに接続すると、Umbrella ローミング クライアントは次のことを実行します。

- 無効になります。Umbrella ローミング クライアントが実行中のまま「スタンバイ」状態になります。
- DNS サーバが VA の設定に戻ります。
- Umbrella ダッシュボードのレポートが、Umbrella ローミング クライアントのホスト名としてではなく、ユーザまたはコンピュータの内部ネットワーク IP または Active Directory のアイデンティティとして表示されます。

Umbrella ローミング クライアント固有のポリシーは、VA がないネットワークにローミングするまで適用されません。

この状態は、ダッシュボードの [アイデンティティ（Identities）] > [ローミング コンピュータ（Roaming Computers）] ページに反映されます。VA に保護されたローミング コンピュータは、VA で保護された緑色の状態になります。

付録 A: ステータスおよび機能 <付録 B: 仮想アプライアンス> 付録 C: トラブルシューティング

付録 C: トラブルシューティング

一般的な問題とトラブルシューティング

この付録は、Cisco Umbrella ローミング クライアントで発生した一般的な問題を、サポートに連絡する前に、またはナレッジ ベースを検索する前に解決するために、コンテキストと実用的なステップを示すことを目的としています。以下に示すほとんどのコマンドは、トラブルシューティングを行うためにコンピュータへの管理アクセス権を必要とします。これらのタスクを実行する場合は、管理者アカウントにログインすることをお勧めします。

Umbrella ローミング クライアントをインストールできない場合

Umbrella ローミング クライアントが正しくインストールされない場合は、いくつかの原因が考えられます。

シナリオ 1: GPO、Apple Remote Desktop、標準のイメージなど、分散/大規模導入の方法によって Umbrella ローミング クライアントをインストールした場合。

その場合は、手動インストール方法で Umbrella ローミング クライアントをマシンにインストールしてみてください。Umbrella ローミング クライアントが正常にインストールされたら、大規模導入に関する記事（標準のイメージの使用および OS X で Apple Remote Desktop を使用する）を再度確認して、各ステップを正確に実行したかどうかを確認してください。Umbrella ローミング クライアントがインストールされなかった場合は、**シナリオ 2** に進みます。

シナリオ 2: 手動インストール方法による単一のインストールで Umbrella ローミング クライアントをインストールした場合。

配信の**最小要件**を満たしていることを確認します。

最小要件を満たした上で Umbrella ローミング クライアントが正しくインストールされない場合は、サポート チケットをオープンしてください。

内部リソースを解決できない

内部リソース(ドメイン)を解決できない場合は、ローカル リソースをホストするすべてのドメインを内部ドメインリストに追加したことを確認してください。

対象のドメインが内部ドメイン リストに追加されている場合は、次のコマンドを(端末またはコマンド プロンプトで)実行して、すべての DHCP に委任された DNS サーバがプライベート IP を返していることを確認し、結果を比較します。次のコマンドは、Umbrella ローミング クライアントのインストールについて問題が発生しているマシンで実行します。必要に応じて、内部ドメイン名とローカル DNS サーバを置き換えます。

nslookup resource.internal-domain.com 127.0.0.1
nslookup resource.internal-domain.com $LOCAL_DNS_SERVER_1
nslookup resource.internal-domain.com $LOCAL_DNS_SERVER_2

いずれかのローカル DNS サーバがパブリック IP アドレスを返した場合は、Umbrella ローミング クライアントが内部ドメイン DNS ルックアップをそのサーバに渡し、結果としてその応答を使用する可能性があるため、修正が必要です。

Umbrella ローミング クライアント(127.0.0.1)がパブリック IP を返し、ローカル DNS サーバに対するクエリによってプライベート IP が返される場合は、サポートまでご連絡ください。

インストールの失敗

Umbrella ローミング クライアントのインストーラが突然終了するか(エラー コードあり/なし)、インストール中にクラッシュすると、インストールが失敗します。Umbrella ローミング クライアントが正常にインストールされても、登録に失敗するか「保護」状態にならない場合は、別の問題であるため、このセクションはスキップしてください。

Umbrella ローミング クライアントのインストーラが失敗することはあまりありませんが、失敗した場合は、いくつかの一般的な原因が考えられます。追加のアクションを実行する前に、これらのチェックを行ってください。

- コマンド ラインまたは導入システムによってインストールする場合は、**手動/単一インストール方法**でのインストールを試してください。単一のインストールが成功して、コマンド ラインまたは導入システムによるインストールが失敗した場合は、**コマンド ライン パラメータ** 、または関連する**大規模導入**の記事を確認してください。一般的に、「OrgInfo」情報などのパラメータが正しく渡されていないか、インストールに必要なソース ファイルが欠落しているなどの原因が考えられます。
- ウイルス対策ソフトウェアまたはその他のセキュリティ ベースのソフトウェア製品を実行している場合は、セキュリティ ログをチェックして、インストールがセキュリティ ソフトウェアによってブロックされていないことを確認します。

Windows の場合

Windows 用の Umbrella ローミング クライアントで必要なソフトウェアは .NET Framework 3.5（Windows 8/8.1 の場合は 4.5）だけであるため、.NET Framework がないことが原因として考えられます。適切なバージョンの .NET Framework がインストールされていることを確認してください。

実際にインストーラがクラッシュしたか、Umbrella ローミング クライアントがインストールされずにインストーラが終了し、エラーが表示されない場合は、次の手順を実行してインストーラ エラーを生成します。

1. 管理者としてコマンド プロンプトを開きます。

2. Setup.msi ファイルと OrgInfo.json ファイルがあるフォルダ（一般にはダウンロードして展開したフォルダ）にディレクトリを変更します。

3. 次のコマンドを実行します。

msiexec /i Setup.msi /L*v install.log

4. インストールが完了したら、サポート チケットをオープンし、Setup.msi と同じフォルダにある install.log を添付します。

未登録の Umbrella ローミング クライアント

インストールが完了すると、Umbrella ローミング クライアントのトレイ アイコンがグレーまたは赤色になります。また、Umbrella ローミング クライアントが登録済みとしてダッシュボードに表示されない場合もあります。これは「未登録」の Umbrella ローミング クライアントであると考えられます。

Umbrella ローミング クライアントが未登録であるのは、ほとんどの場合次のいずれかの理由によります。

HTTP プロキシ（Windows の場合）：ローカル コンピュータ レベルに HTTP/HTTPS プロキシがあるか、以前のプロキシ設定による古い設定が残っています。**Umbrella ローミング クライアントの前提条件**の記事の「ネットワーキング」セクションで HTTP/HTTPS のスニペットを確認し、詳細について **Umbrella ローミング クライアントと HTTP プロキシ**の記事を参照してください。

コマンド ライン/大規模導入：GPO、Apple Remote Desktop、Kaseya などの配信ツールを使用して Umbrella ローミング クライアントを導入した場合は、OrgInfo.json/.plist からの情報が正しくコピーされていない可能性があります。Umbrella ローミング クライアントは特定の方法で導入する必要があるため、大規模導入の記事で説明されている方法を使用していることを確認してください。

- **Windows 2003 での GPO を使用した導入**
- **Windows 2008 R2 および Windows 2012 での GPO を使用した導入**
- **SuperORCA を使用したアプリケーション インストールによる導入**
- **Apple Remote Desktop を使用した導入**
- **標準イメージを使用した導入**

非保護/非暗号化

Umbrella ローミング クライアントのトレイ/メニュー バー アイコン、または Umbrella ダッシュボードで、ステータスが黄色で、[非保護/非暗号化（Unprotected/Unencrypted）] と示されています。

この状態について詳細に説明している、**Umbrella ローミング クライアントが非保護/非暗号化になる原因**の記事を参照してください。テストと実施可能な修正方法も記載されています。

状態またはステータスの頻繁な変化（フラッピング）

ローカルのエンドポイントで、Umbrella ローミング クライアントの状態が常時変化し続ける場合があります（フラッピング）。これはトレイ/メニュー バー アイコンのメッセージで確認できます。フラッピングが発生するときは、ネットワーク接続の問題の可能性があります。Umbrella ローミング クライアントの状態が急速に変化し、インターネット接続の問題が発生している場合は、**一時的に Umbrella ローミング クライアントを無効に**して、サポートに連絡することを検討してください。

接続上の問題がなく、ユーザのトレイ/メニュー バー アイコンでフラッピングや状態の変化を確認できる場合は、原因として次のいずれかのシナリオが考えられます。

シナリオ #1：**互換性のない VPN クライアント リスト**に含まれている VPN クライアントを使用しています。その場合は、現時点では特に解決方法がありません。別の **VPN クライアント**を使用する必要があります。

シナリオ #2：ネットワーク上で多量のパケット損失があり、それによって Umbrella ローミング クライアントのヘルス チェックが失敗しています。ping または MTR/WinMTR を使用して、208.67.222.222/208.67.220.220 とクライアント コンピュータ間でのパケット損失の有無を確認することをお勧めします。パケット損失が多量である場合、または集中している場合（2 % を超えると過大）には、Umbrella ローミング クライアントは一時的に別の状態に移行し、異常時での保護が行われます。パケット損失がない場合、またはパケット損失の問題を解決できない場合は、サポートにご連絡ください。

ログ

現在、Umbrella ローミング クライアントのログは、非常に詳細であるため読みにくく、高度なトラブルシューティングが必要になっています。Umbrella では、サポート チケットで問題が報告されるとログが自動的に収集されますが、エンド ユーザが診断ツールを手動で実行しなければならない場合があります。診断ツールの詳細については、以下を参照してください。

現時点では、ログを解釈してトラブルシューティングを行うことはお勧めしません。近い将来、サポートと開発者向けの高度なログと、ユーザが自分でトラブルシューティングを行うための詳細度を下げたログの、2 種類のログを提供する予定です。

Umbrella ローミング クライアントのサービス ログは、次の場所にあります。

- **Windows**：テキスト エディタで次のファイルを開きます。**C:¥ProgramData¥OpenDNS¥ERC¥OpenDNS_ERC_Service.log**
- **Mac**：端末アプリケーションで次のコマンドを実行して、システムからローミング クライアント ログを抽出します。**grep dns-updater /var/log/system.log**

診断ツール

Umbrella ローミング クライアントには診断ツールが組み込まれています。ほとんどの場合、サポートではこのツールを実行することで、Umbrella ローミング クライアントのログを自動的に取得できます。場合によっては、サポートに代わり、またはサポートの指示に従って、ユーザが診断ツールを実行する場合もあります。

サポート要求を最初に行うときに診断出力を提出すれば、サポートによるトラブルシューティングの効率が大幅に向上します。診断ツールには複数の実行方法があります。それについては、サポートにローミング クライアントの診断上を提供する方法に関する記事で説明されています。

Umbrella が収集する情報については、次を参照してください。

- **ログの収集と診断の自動化**

付録 B：仮想アプライアンス <**付録 C：トラブルシューティング**> 付録 D：内部ドメイン

付録 D: 内部ドメイン

概要: 内部ドメイン

内部ドメイン機能により、Umbrella ローミング クライアントの使用時に、ドメインの DNS クエリが Cisco Umbrella サーバではなく、ローカル ネットワークの DNS サーバへクエリされるようになります。

内部ドメインを指定しない場合、すべての DNS クエリが Umbrella に直接送信されます。その結果、ローカル DNS サーバを使用する内部ホスト ドメインのネットワーク リソース(コンピュータ、サーバ、プリンタなど)に到達できなくなります。

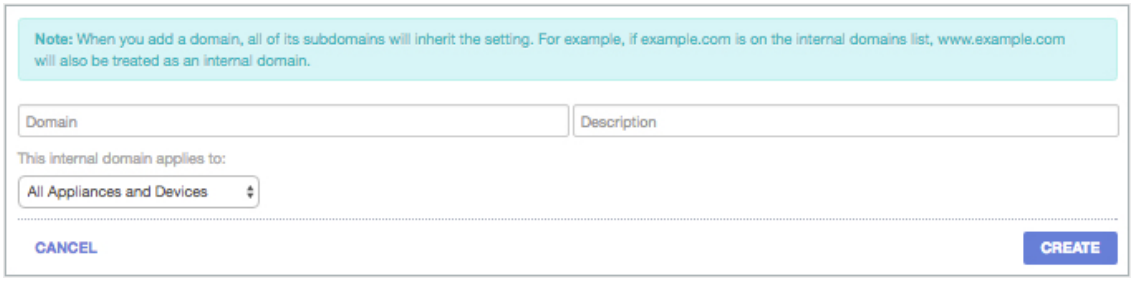
これらのリソースに対する中断のないアクセスを確保するには、管理者はダッシュボードの [内部ドメイン(Internal Domains)] セクション([設定(Settings)] > [内部ドメイン(Internal Domains)])に、適切なドメインを追加する必要があります。これにより、内部ドメインの許可リストが作成され、ローミング ユーザと同期されます。基本的に、内部ドメイン リストに追加されたすべてのドメインは、Umbrella ローミング クライアントがコンピュータにインストールされていないときと同じように DNS レコードを解決できます。

Umbrella ローミング クライアントは、どのドメインを内部ドメインとして処理するか判断する際に、ダッシュボードと DNS サフィックスの 2 つのソースに基づきます。

ダッシュボード: [内部ドメイン(Internal Domains)] セクション

Umbrella ダッシュボードの [内部ドメイン(Internal Domains)] 領域([設定(Settings)] > [内部ドメイン(Internal Domains)])には、組織のネットワーク内(物理ネットワークおよび VPN 接続)にいるときに組織がローカル リソースへのアクセスに使用するドメインをすべて入力する必要があります。内部ドメインには、**.local の TLD**、**RFC-1918(プライベート ネットワーク)**の逆引き DNS アドレス空間のすべてがあらかじめ入力されています。新しく追加したドメインは、約 10 分以内に Umbrella ローミング クライアントと同期されます。

[この内部ドメインの適用先（This internal domain applies to:）] では、内部ドメインを Umbrella ローミング クライアントと仮想アプライアンス（VA）のどちらかまたは両方に適用するように指定できます。



DNS サフィックス

コンピュータのアダプタの DNS サフィックス設定、およびグローバル ネットワーク設定に含まれているドメインは、Umbrella ローミング クライアントを起動するか、新しいネットワーク アダプタ（VPN またはワイヤレス接続）を開始するたびに、個々の Umbrella ローミング クライアントの内部ドメイン リストに自動的にインポートされます。それにより、Umbrella ローミング クライアントは、ダッシュボードを通じてドメインを追加することなくローカル リソースにアクセスできると同時に、外部ネットワークに接続することができます。

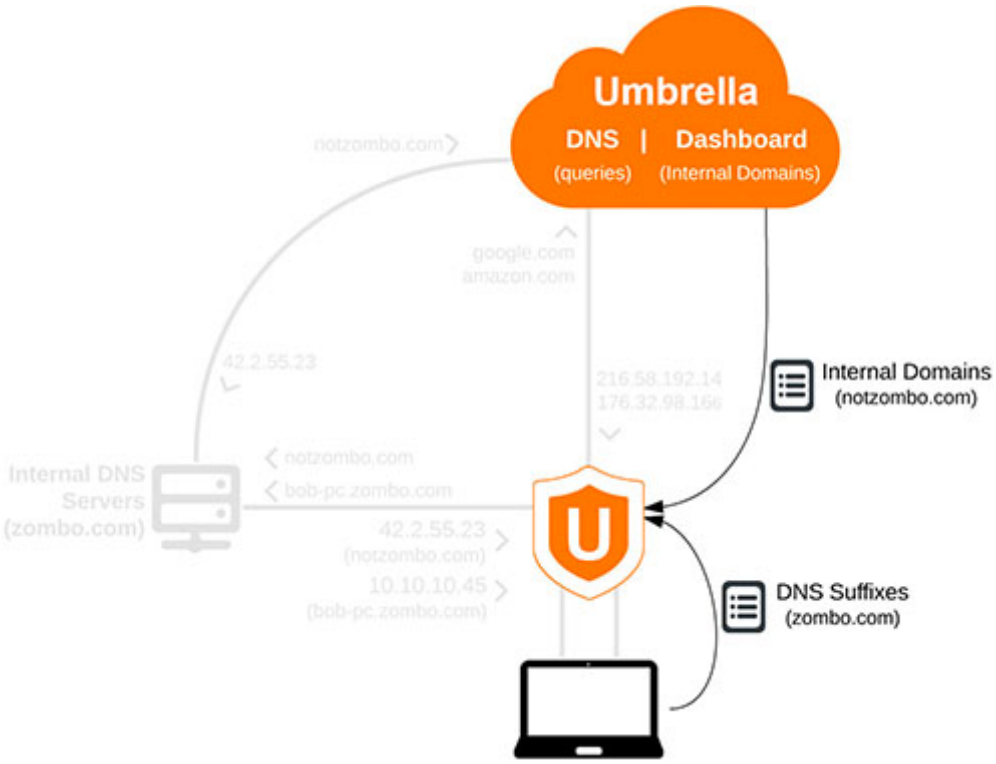
操作のフローチャート

次のフローチャートは、ローミング クライアントが内部および外部 DNS クエリを正常に処理する方法を示しています。

1. 内部ドメイン

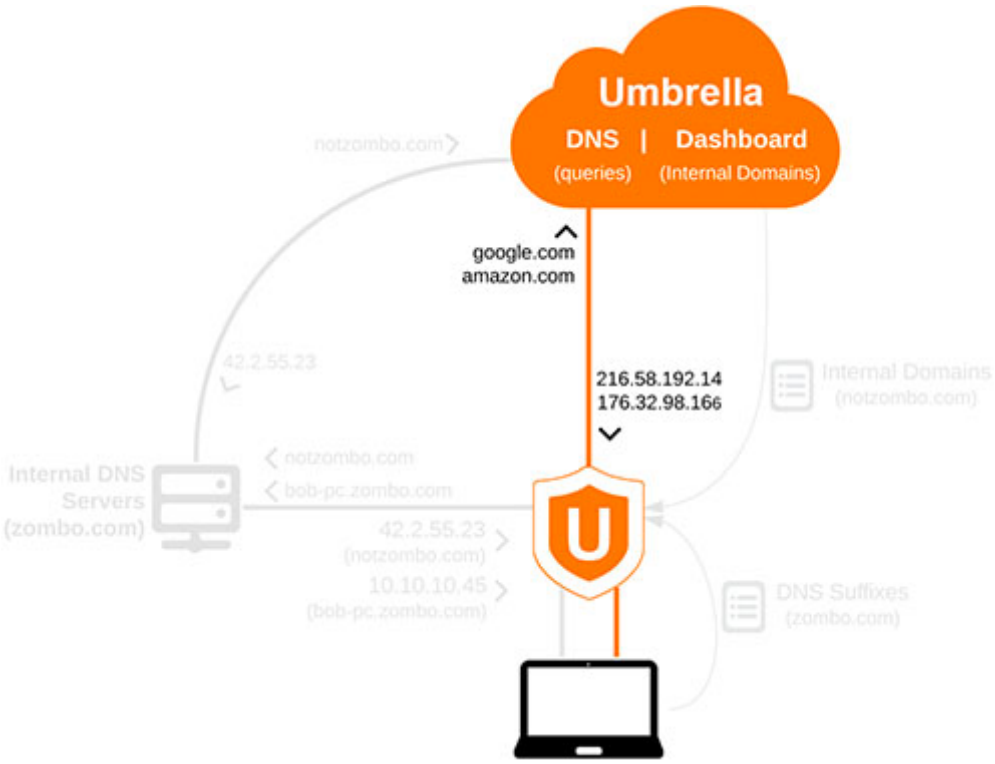
Umbrella ローミング クライアントの内部ドメイン リストには、2 つのソースから入力されます。

- Umbrella ダッシュボードの内部ドメイン リストを同期する
- ローカル コンピュータのネットワーキング設定の DNS サフィックス リスト



2. 外部クエリ

どの内部ドメイン リストにあるドメインにも一致しない外部 DNS クエリは、Umbrella に直接送信されます。

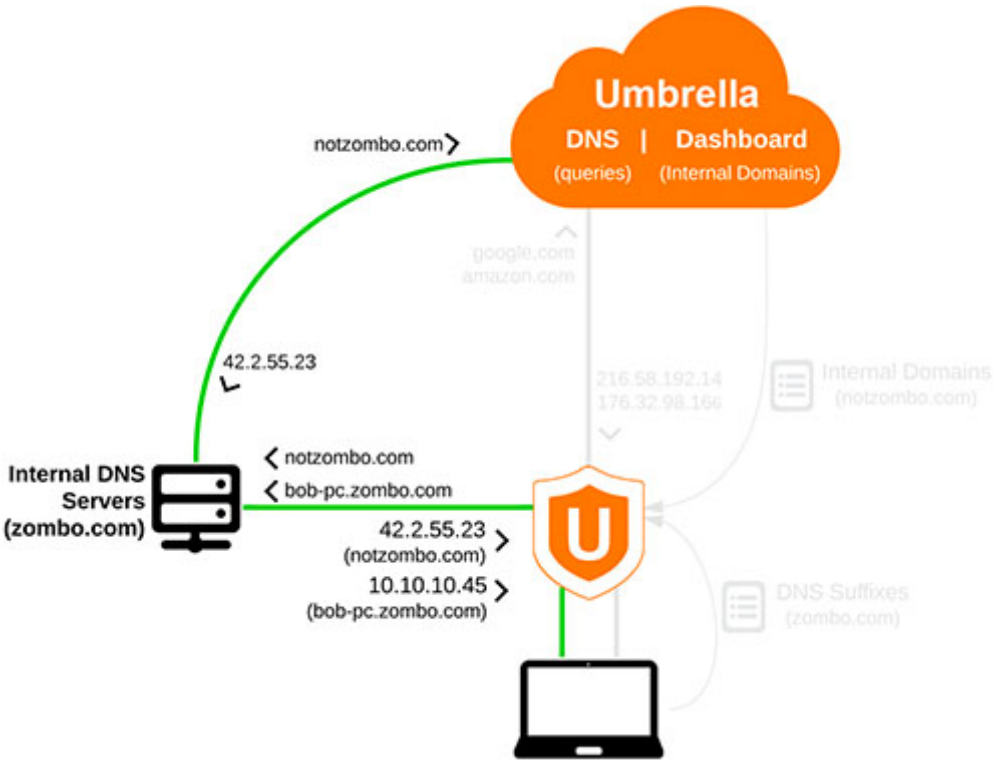


3. 内部クエリ

内部ドメイン リストに含まれるドメインに対する DNS クエリは、ローカル ネットワークの DNS サーバを通じて送信されます。

ローカル ネットワークで*ホストされている*内部ドメインは、内部 DNS サーバによって直接解決されます（bob-pc.zombo.com を参照）。

ローカル ネットワークで*ホストされていない*内部ドメインは、Umbrella によって、または解決用に使用されているパブリック DNS サーバによって解決されます（notzombo.com を参照）。



高度なトピック

次のセクションでは、内部ドメインとその動作について、さらに詳細な情報とロジックを示します。

非暗号化

Umbrella ローミング クライアントは、暗号化状態にある場合、暗号化された DNS クエリを Umbrella に送信できますが、内部ドメイン リストに含まれているドメインは、Umbrella には送信されないため、送信時に暗号化されません。

仮想アプライアンス

注: 仮想アプライアンス(VA)を使用しない場合は、このセクションをスキップできます。

VA を組織内の 1 つまたは複数の環境に導入している場合、Umbrella ローミング クライアントがその環境に物理的または VPN 経由で接続すると、Umbrella ローミング クライアントは無効になり、DNS 設定が VA に戻ります。VA を使用している場合の Umbrella ローミング クライアントの動作の詳細については、付録 B:仮想アプライアンスと Umbrella ローミング クライアントを参照してください。

組織内のすべて環境で VA を使用している場合は、内部ドメイン リストをアプライアンスにのみ設定（アプリケーションとデバイス以外）するだけで十分です。Umbrella ローミング クライアントが対象のネットワークに接続していない場合は、「アプライアンスのみ」に設定されている内部ドメインは使用されず、ドメインに対する DNS クエリは（暗号化された）パブリック クエリとして処理されます。

DHCP/静的 DNS サーバ

コンピュータが起動するか、新しいネットワーク接続がアクティブになると、Umbrella ローミング クライアントでは、DNS サーバが各ネットワーク アダプタで 127.0.0.1 に設定されます。

ネットワーク アダプタ上の既存の DNS サーバ設定を置き換えると、各アダプタの既存の DNS アドレスが、システム上の次のローカル ファイルに保存されます。

Mac OS X	/var/lib/data/opendns/resolv_orig.conf
Windows	C:¥ProgramData¥OpenDNS¥ERC¥Resolver#-Name-of-Network Adaptor.conf

内部ドメイン許可リスト内のドメインが送信されるアドレスが、Umbrella ローミング クライアントが存在しない環境をエミュレートします。

Umbrella ローミング クライアントでは DNS がキャッシュされないため、ローカルの DNS サーバで行われたローカル DNS の変更は直ちに有効になります。Umbrella ローミング クライアントが存在してもこの動作は変わりません。

Umbrella ローミング クライアントは、次の条件の下で、DHCP によって設定された DNS サーバまたは静的に設定された DNS サーバを元の状態に戻します。

- **手動で停止された**
- **アンインストールされた**
- **「オープン」状態にある**：Umbrella に接続できない
- **「VA の背後」にある**：ネットワーク上に VA がある
- **「保護されたネットワーク」状態にある**：Umbrella ローミング クライアントは、組織のネットワークに接続している間は無効になるように設定されます。

DNS サフィックス（続き）

DNS サフィックスについては、次の 2 つの状態を考慮する必要があります。

1. それにより組織は、ダッシュボードの内部ドメイン リストにドメインを**追加する必要がなくなります**。ドメインを DNS サフィックスとして使用するように DHCP が設定されている場合、Umbrella ローミング クライアントでは、ダッシュボードに追加しなくても、そのドメインが自動的にローカルとして処理されます。

2. すでに説明したように、ダッシュボードのリストに入力する代わりに、DNS サフィックスを使用して内部ドメインを解決すれば、セキュリティが向上します。内部ドメイン リスト内のドメインに送信される DNS クエリは暗号化されないため、ダッシュボードに追加されているドメインに対して DNS クエリを実行するマシンは、常に *すべて*のネットワークで暗号化されずに送信されることになります。

DNS サフィックス リストに含まれているドメインを追加する動作は、インストール中に**特別なコマンドライン パラメータ**を使用して無効にすることができます。
