



Umbrella ローミング セキュリティ

Umbrella ローミング セキュリティ モジュールには、Professional、Insights、Platform、MSP のいずれかのパッケージでの Cisco Umbrella ローミング サービスのサブスクリプションが必要です。Cisco Umbrella ローミングはアクティブな VPN がないときに DNS レイヤセキュリティを提供し、Cisco Umbrella サブスクリプションはインテリジェントプロキシを追加します。さらに、Cisco Umbrella サブスクリプションはコンテンツ フィルタリング、複数ポリシー、強力なレポート、Active Directory の統合などの機能を提供します。サブスクリプションに関係なく、同じ Umbrella ローミング セキュリティ モジュールが使用されます。

Umbrella ローミング モジュールのプロファイル (OrgInfo.json) は、各展開を対応するサービスに関連付け、対応する保護機能は自動的に有効化されます。

Umbrella ダッシュボードは、ローミング セキュリティ モジュールから発信されるすべてのインターネットアクティビティについてリアルタイムの可視性を提供します。ポリシーおよびレポートの精度のレベルは Umbrella サブスクリプションによって異なります。

サービス レベル サブスクリプションごとに含まれる機能の詳細な比較については、<https://umbrella.cisco.com/products/packages> を参照してください。

- [Android Windows または OS 用の AnyConnect Umbrella モジュール \(1 ページ\)](#)

Android Windows または OS 用の AnyConnect Umbrella モジュール

Umbrella ローミングクライアントと Umbrella ローミングセキュリティモジュールの非互換性

Umbrella ローミングセキュリティモジュールと Umbrella ローミングクライアントは互換性がありません。Umbrella ローミングセキュリティモジュールを展開している場合は、ローミングセキュリティモジュールのインストール中に Umbrella ローミングクライアントのすべての既存のインストールが検出され、競合を防ぐために自動的に削除されます。Umbrella ローミングクライアントの既存インストールを Umbrella サービス サブスクリプションに関連付けてい

る場合は、OrgInfo.json ファイルを AnyConnect インストーラと同じ場所に配置して Umbrella モジュールのディレクトリで Web 展開または事前展開を設定していない限り、Umbrella ローミングセキュリティ モジュールに自動的に移行されます。Umbrella ローミングセキュリティ モジュールを展開する前に、手動で Umbrella ローミング クライアントをアンインストールすることもできます。

Cisco Umbrella アカウントの取得

Umbrella ダッシュボード (<http://dashboard.umbrella.com/>) は、展開に含める AnyConnect Umbrella ローミングセキュリティ モジュールのプロファイル (OrgInfo.json) を取得できるログイン ページです。このページでは、ローミングクライアントのアクティビティのポリシーとレポートを制御することもできます。

ダッシュボードからの OrgInfo ファイルのダウンロード

OrgInfo.json ファイルは、ローミングセキュリティ モジュールにレポートの送信先と適用するポリシーを知らせる、Umbrella ダッシュボード インスタンスについての詳細情報です。

Umbrella ローミングセキュリティ モジュールの導入準備を行うには、Umbrella ダッシュボード (<https://dashboard.umbrella.com>) から、OrgInfo.json ファイルを取得する必要があります。

[ID (Identities)] メニュー ストラクチャで [ローミング コンピュータ (Roaming Computers)] をクリックし、続いて、ページ左上隅の [+] 記号をクリックします。AnyConnect Umbrella ローミングセキュリティモジュールまでスクロールし、[モジュールプロファイル (Module Profile)] をクリックします。特定のインストール/展開手順と特定のパッケージおよびファイルについては、「[AnyConnect 展開の概要](#)」を参照してください。



- (注) OrgInfo.json ファイルを初めて展開すると、データサブディレクトリ (/umbrella/data) にコピーされて、他のいくつかの登録ファイルも作成されます。したがって、OrgInfo.json 置換ファイルを展開する必要がある場合は、このデータサブディレクトリを削除する必要があります。または、Umbrella ローミングセキュリティ モジュールをアンインストールし (データサブディレクトリが削除されます) 、新しい OrgInfo.json ファイルを再インストールすることもできます。

Umbrella ローミングセキュリティの起動と実行

AnyConnect を展開するとき、Umbrella ローミングセキュリティ モジュールは、追加機能を有効にするために含めることができるオプション モジュールの 1 つです。



- (注) Umbrella ローミングセキュリティ モジュールと Web セキュリティ モジュールを展開している場合は、「Web セキュリティとローミングセキュリティの互換性に必須のホスト例外」と「Web セキュリティと Umbrella ローミングセキュリティ モジュールの互換性に必須の静的な例外」を参照して静的な例外の除外とホスト例外を設定する必要があります。

Windows 7 SP1 ユーザは、インストールまたは初回使用前に、Microsoft .NET Framework 4.0 をインストールすることを推奨します。起動時に、Umbrella サービスは .NET Framework 4.0（または以上）がインストールされているかどうかを確認します。検出されない場合は、Umbrella ローミングセキュリティモジュールはアクティブにならず、メッセージが表示されます。.NET Framework にアクセスし、これをインストールするには、再起動して Umbrella ローミングセキュリティモジュールを有効にする必要があります。

OrgInfo.json ファイルの設定

OrgInfo.json ファイルには、Umbrella サービスのサブスクリプションについての固有の情報が格納されており、レポート先や適用するポリシーに関する情報をセキュリティ ローミングモジュールに通知します。OrgInfo.json ファイルを展開し、CLI または GUI を使用して ASA または ISE から Umbrella ローミングセキュリティモジュールを有効にすることができます。次の手順では、最初に ASA から有効にする方法、次に ISE から有効にする方法を示します。

ASA CLI

1. Umbrella ダッシュボード (<https://dashboard.umbrella.com>) から ASA ファイルシステムに取得した OrgInfo.json をアップロードします。
2. 設定に応じてグループ ポリシー名を適切に調整して、次のコマンドを実行します。

```
webvpn
  anyconnect profiles OrgInfo disk0:/OrgInfo.json

group-policy DfltGrpPolicy attribute
  webvpn
    anyconnect profiles value OrgInfo type umbrella
```

ASDM GUI

1. [設定 (Configuration)] > [リモート アクセス VPN (Remote Access VPN)] > [ネットワーク (クライアント) アクセス (Network (Client) Access)] > [AnyConnect クライアント プロファイル (AnyConnect Client Profile)] の順に移動します。
2. [追加 (Add)] を選択します。
3. プロファイルの名前を入力します。
4. [プロファイルの使用 (Profile Usage)] ドロップダウンメニューから Umbrella セキュリティ ローミングクライアントタイプを選択します。OrgInfo.json ファイルが、[プロファイルの場所 (Profile Location)] フィールドに入力されます。
5. [アップロード (Upload)] をクリックして、ダッシュボードからダウンロードした OrgInfo.json ファイルの場所を参照します。

6. [グループポリシー (Group Policy)] ドロップダウンメニューで DfltGrpPolicy に関連付けます。グループポリシーで新しいモジュール名を指定するには、「追加の AnyConnect モジュールの有効化」を参照してください。

ISE

ISE からイネーブルにするには、以下の手順に従います。

1. Umbrella ダッシュボード (<https://dashboard.umbrella.com>) から OrgInfo.json をアップロードします。
2. ファイル OrgInfo.xml の名前を変更します。
3. 「AnyConnect を展開するための ISE の設定」の手順に従います。

クラウド最新情報

Umbrella ローミングセキュリティ モジュールは、Umbrella クラウドインフラストラクチャからインストールされたすべての AnyConnect モジュールの自動更新を提供できます。クラウド更新では、ソフトウェアアップグレードは Umbrella クラウドインフラストラクチャから自動的に得られます。更新トラックは管理者のアクションではなくこれによって決まります。

デフォルトでは、クラウド更新からの自動更新は無効です。Umbrella ローミングセキュリティとその他の AnyConnect のクラウド更新を有効にするには、Umbrella ダッシュボードにログインします。[ID (Identities)] > [ローミング コンピュータ (Roaming Computers)] > 設定アイコン (歯車アイコン) の下で、[新しいバージョンがリリースされたら常に、VPN モジュールを含む AnyConnect を自動的に更新する (Automatically update AnyConnect, including VPN module, whenever new versions are released)] をオンにします。更新は VPN が有効である間は実行されません。デフォルトでは、このオプションは選択されていません。

クラウド更新に関して以下を検討してください。

- 現在インストールされているソフトウェア モジュールのみが更新されます。
- カスタマイズ、ローカリゼーション、およびその他の展開タイプはサポートされません。
- 更新は、デスクトップにログインしたときにのみ実行され、VPN が確立されているときは実行されません。
- 更新を無効にすると、最新のソフトウェア機能と更新を利用できません。
- クラウド更新を無効にしても、他の更新メカニズムや設定 (Web 展開、遅延更新など) には影響しません。
- クラウド更新は、AnyConnect のより新しいバージョンや未公開バージョン (暫定リリース、修繕公開されたバージョンなど) を持つデバイスを無視します。

セキュリティポリシーの設定とレポートの確認

保護を受信し、レポート情報を表示し、ポリシーを設定するには、Cisco Umbrella ローミングアカウントが必要です。詳細な説明については、<https://docs.umbrella.com/product/umbrella/> または <https://support.umbrella.com> にアクセスして追加情報を参照してください。

インストール後 90 分から 2 時間以内に、ローミングコンピュータが Umbrella ダッシュボードに表示されます。<https://dashboard.umbrella.com> に移動して認証し、**[ID (Identities)] > [ローミングコンピュータ (Roaming Computers)]** の順にアクセスすると、ローミングクライアントのリスト（アクティブクライアントと非アクティブクライアントの両方）とインストールされている各クライアントの詳細が表示されます。

最初は、セキュリティフィルタリングが基本レベルのデフォルトのポリシーがローミングコンピュータに適用されています。このデフォルトのポリシーは、ダッシュボードの **[ポリシー (Policies)]** セクション（または **[設定 (Configuration)] > [Cisco Umbrella アカウントのポリシー (Policy for Cisco Umbrella accounts)]**）にあります。

ローミングクライアントのレポートは、**[レポート (Reports)]** セクションにあります。Umbrella ローミングセキュリティモジュールがインストールされ VPN がオフにされているコンピュータからの DNS トラフィックを確認するには、アクティビティ検索レポートをチェックします。

エンドポイントに表示される UI の変更内容解説

AnyConnect UI では、Umbrella ローミングセキュリティモジュールのタイルに現在のステータスが表示されます。

状態	アイコンの色	説明	条件
予約済 (Reserved)	オレンジ (Orange)	接続状況をチェック中です。Umbrella モジュールは保護状態をまだ確認していません。	この動作ステータスは次の条件で発生します。 <ul style="list-style-type: none"> モジュールが最初にアクティブにされたとき。 ネットワーク インターフェイスの変更（新しいネットワークアダプタの検出、既存アダプタの IP の変更、新しい VPN トンネルの確立または中断）が発生したとき。

状態	アイコンの色	説明	条件
オープン (Open)	黄	<p>現在、<i>Umbrella</i> によって保護されていません。<i>Umbrella</i> リゾルバとの接続の問題が原因で、ローカル <i>Umbrella</i> モジュールの DNS 保護がアクティブになっていません。少なくとも 1 つのアクティブなネットワーク接続が存在します。ただし、ローミングクライアントは、アクティブな接続の <i>Umbrella</i> サービスに接続できません。</p> <p>システムの DNS 設定は元の設定 (DHCP または固定) に戻ります。</p>	<p>この動作ステータスは次の条件で発生します。</p> <ul style="list-style-type: none"> • UDP ポート 443 または UDP ポート 53 は、<i>Umbrella</i> リゾルバ (209.67.222.222) に接続していない。 • <i>Umbrella</i> DNS VA がローカルネットワークで設定されていない。 • VPN トンネルが一時的に中断または確立状態になっている可能性がある。
保護済み (Protected)	グリーン	<p><i>Umbrella</i> によって保護されています。DNS クエリーが暗号化されていません。ローカル <i>Umbrella</i> モジュールの DNS 保護がアクティブで、DNS 要求は暗号化されずに <i>Umbrella</i> リゾルバに送信されます。</p>	<p>このステータスは、モジュールが最初にアクティブ化されたときか、ネットワーク インターフェイスの変更があるときに発生する可能性があります。</p>
暗号化	グリーン	<p><i>Umbrella</i> によって保護されています。DNS クエリーが暗号化されています。ローカル <i>Umbrella</i> モジュールの DNS 保護がアクティブで、DNS 要求は暗号化されて <i>Umbrella</i> リゾルバに送信されます。</p>	<p>この動作ステータスは次の条件で発生します。</p> <ul style="list-style-type: none"> • <i>Umbrella</i> リゾルバ (209.67.222.222) に UDP ポート 443 で接続している。 • <i>Umbrella</i> リゾルバ (208.67.222.222) に TCP ポート 443 および TCP ポート 53 で接続している。

状態	アイコンの色	説明	条件
保護されたネットワーク (Protected Network)	グリーン	<i>Umbrella</i> によってネットワークが保護されています。現在のエンドポイントネットワークが <i>Umbrella</i> リゾルバを使用して保護されているため、ローカル <i>Umbrella</i> モジュール DNS 保護はアクティブではありません。ローミングクライアントにより、DNS 設定が DHCP 経由または固定設定で設定されていた内容に戻されました。接続は暗号化されていません。	この動作ステータスは次の条件で発生します。 <ul style="list-style-type: none"> 現在のエンドポイント ネットワーク出力 IP アドレスが、エンドポイントと同じ <i>Umbrella</i> アカウントに登録されている。 使用されるリゾルバが <i>Umbrella</i> クラウド リゾルバ (208.67.222.222、208.67.220.220) である。 <i>Umbrella</i> ダッシュボード ([保護されたネットワークでは無効にする (Disable Behind Protected Networks)]) で設定されたポリシーで、保護されたネットワークでは <i>Umbrella</i> モジュールを無効にすることが指定されている。 <p>(注) ネットワーク レベルの保護がないため、すべての <i>Cisco Umbrella</i> ローミング パッケージのお客様がこのステータスになることはありません。</p>
仮想アプライアンスの背後 (Behind Virtual Appliance)	グリーン	<i>Umbrella</i> 仮想アプライアンスによって保護されています。 <i>Umbrella</i> 仮想アプライアンスはオンプレミスの DNS リゾルバとして設定されているため、ローカル <i>Umbrella</i> モジュールの DNS 保護はアクティブではありません。ローミングクライアントは無効になり、DNS 設定が DHCP 経由または固定設定で設定されていた内容に戻されました。接続は暗号化されていません。	この動作ステータスは、エンドポイントで設定された DNS アドレス (DHCP 経由または固定) が <i>Umbrella</i> VA アドレスであるときに発生します。

状態	アイコンの色	説明	条件
Umbrella 信頼ネットワークステータス (Umbrella Trusted Network State)	グレー	信頼済みのネットワーク上では無効。現在のエンドポイントネットワークが Umbrella 信頼ネットワークとして設定されているため、ローカル Umbrella モジュールの DNS 保護はアクティブではありません。	この動作ステータスは次の条件で発生します。 <ul style="list-style-type: none"> • Umbrella ダッシュボードがマジックドメイン名で設定されている。 • 対応するマジックドメイン名またはレコードがローカルDNSリゾルバで設定されている。
VPN 信頼ネットワークステータス (VPN Trusted Network State)	グレー	信頼済みのネットワーク上では無効。現在のエンドポイントネットワークが AnyConnect VPN 信頼ネットワークとして設定されているため、ローカル Umbrella モジュールの DNS 保護はアクティブではありません。	この動作ステータスは次の条件で発生します。 <ul style="list-style-type: none"> • AnyConnect VPN モジュールが信頼ネットワーク検出の状態を信頼できると報告している。 • AnyConnect VPN トンネルが接続されていないか、完全トンネルモードで確立されていない。 • Umbrella ダッシュボードで設定されたポリシーで、AnyConnect VPN 信頼ネットワークにあるときは Umbrella モジュールを無効にすると指定されている。 <p>(注) この設定は、すべてのローミングパッケージのお客様に対して適用され、管理者が変更することはできません。</p>

状態	アイコンの色	説明	条件
VPN 状態が原因で無効 (Disabled Due to VPN State)	グレー	VPN がアクティブな間は無効。現在エンドポイントでアクティブな AnyConnect VPN トンネルが確立されているため、ローカル Umbrella モジュールの DNS 保護はアクティブではありません。	この動作ステータスは次の条件で発生します。 <ul style="list-style-type: none"> AnyConnect VPN モジュールが信頼ネットワーク検出の状態を信頼できないと報告している。 AnyConnect VPN トンネルが完全トンネルモードで確立されている。 Umbrella ダッシュボードで設定されたポリシーで、AnyConnect VPN トンネルが確立されているときは Umbrella モジュールを無効にすると指定されている。 <p>(注) この設定は、すべてのローミングパッケージのお客様に対して適用され、管理者が変更することはできません。</p>
OrgInfo.json ステートなし (No OrgInfo.json State)	赤	現在、Umbrella によって保護されていません。プロファイルが見つかりません。現在エンドポイントでアクティブな AnyConnect VPN トンネルが確立されているため、ローカル Umbrella モジュールの DNS 保護はアクティブではありません。	この動作ステータスは、OrgInfo.json ファイルが次の適切なディレクトリに配置されていない場合に発生します。 <p>Windows : %ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\Umbrella</p> <p>macOS : opt/cisco/anyconnect/umbrella</p>
エージェント利用不可ステート (Agent Unavailable State)	赤	現在、Umbrella によって保護されていません。サービスは利用できません。Umbrella エージェントが実行されていないため、ローカル Umbrella モジュールの DNS 保護はアクティブではありません。	この動作ステータスは、Umbrella エージェント サービスが現在実行していないとき (クラッシュまたは手動によるサービス停止のため) に発生します。

状態	アイコンの色	説明	条件
.NET 依存ステータスが見つからない (Missing .NET Dependency State) (Windows のみ)	赤	現在、 <i>Umbrella</i> によって保護されていません。Microsoft 4.0 NET Framework がインストールされていません。ローカルの <i>Umbrella</i> モジュールの DNS 保護がアクティブではありません。 <i>Umbrella</i> エージェントが実行されていないためです。.NET ランタイムフレームワークが見つかりません。	この動作ステータスは、.NET 4.0 ランタイムが見つからないために <i>Umbrella</i> エージェントサービスが実行していないときに発生します。

AnyConnect UI は、*Umbrella* ローミングセキュリティモジュールの統計とメッセージ履歴を表示します。

診断の解釈

Cisco *Umbrella* ローミングセキュリティモジュールの問題を診断するには、DART レポートを実行する必要があります。*Umbrella* の問題とトラブルシューティングの詳細については、docs.umbrella.com を参照してください。