AnyConnect：Cisco Umbrella ローミング セキュリティ クライアント管理者ガイド

はじめに

Cisco Umbrella ローミング セキュリティ モジュールは、VPN がアクティブでない場合にも、常にセキュリティを提供します。ローミング セキュリティ モジュールは、DNS 層と IP 層 * でセキュリティを強化し、すべてのポート上でマルウェア、フィッシング、コマンド アンド コントロール コールバックをブロックします。Umbrella は、コンピュータがネットワークや VPN の外にあるときでも、すべてのインターネット アクティビティをホスト名ごとにリアルタイムで可視化します。

ローミング セキュリティ モジュールでは、すでに AnyConnect が設定されている場合に、既存の Umbrella ローミング クライアントの代わりとなることができます。

このソリューションの詳細については、2 つのビデオで確認できます。

1 つ目のビデオは、シスコの製品マネージャである Adam Winn がソリューションについて説明しています：https://www.youtube.com/watch?v=31tGpnAyV5g

2 つ目のビデオは、エンジニアリング ディレクタの Dan Hubbard が TechWise TV でトークを繰り広げています：http://www.cisco.com/c/m/en_us/training-events/events-webinars/webinars/techwise-tv/196-anyconnect-opendns.html

ローミング セキュリティ モジュールでは、Cisco Umbrella ローミング サービス、もしくは Cisco Umbrella サービス（Professional、Insights、Platform、MSP）のサブスクリプションが必要になります。ローミング セキュリティ モジュールでは、VPN がアクティブでない場合に、DNS 層でのセキュリティを提供します。一方、Cisco Umbrella サブスクリプションでは、インテリジェント プロキシや IP 層の適用機能が、ネットワークのオン/オフに関わらず追加されます。さらに、Cisco Umbrella サブスクリプションでは、コンテンツ フィルタリング、複数のポリシー、強力なレポート、Active Directory 統合などが提供されます。なお、サブスクリプションに関わらず、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。

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）により、各環境が対応するサービスと関連付けられ、対応する保護機能が自動で有効になります。

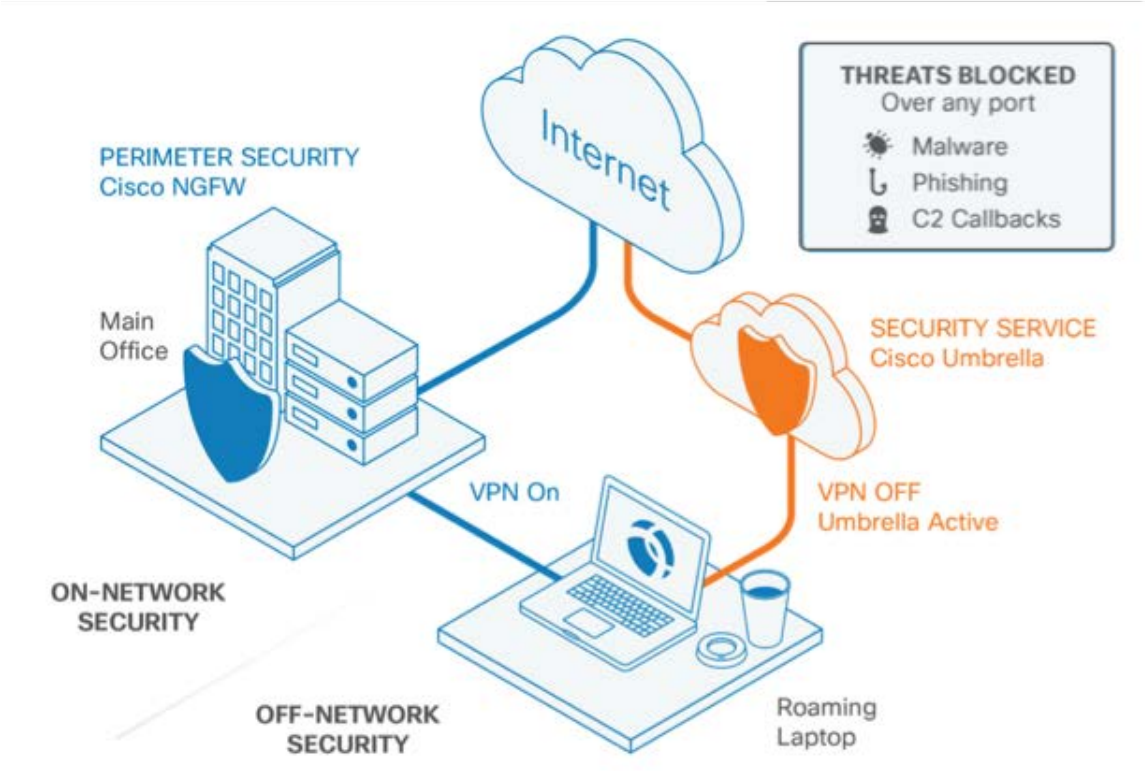
Umbrella ダッシュボードでは、ローミング セキュリティ モジュールから発信されるすべてのインターネット アクティビティがリアルタイムに可視化されます。ポリシーやレポートの精度は、Umbrella サブスクリプションにより異なります。

それぞれのサービス レベルのサブスクリプションに含まれる機能の詳細な比較については、https://www.opendns.com/enterprise-security/threat-enforcement/package-comparison/ 参照してください。

注:

IP 層の適用については、すべての Umbrella パッケージで利用できません。

ネットワークから離れているときに DNS 層のセキュリティを適用したり、単一のセキュリティ ポリシーと基本的なレポート（ホスト名単位）を利用したりするだけでなく、Umbrella ローミング セキュリティのすべての機能を利用するには、Insight か Platform の Cisco Umbrella パッケージが必要です。これらのパッケージの詳細については、こちらを参照してください。



目次

本ガイドは、主に 3 つのエリアで構成されており、各エリアはサブセクションに分かれています。

クイック スタート ガイド

すでに Umbrella ローミング クライアントや AnyConnect に習熟している場合は、アップグレードの実行に必要な手順を大きく短縮することができます。完全な導入の場合は複数の手順を考慮する必要がありますが、クイック スタート ガイドでは、テスト インストール用に手動で導入する手順について紹介しています。Umbrella ローミング セキュリティ モジュールは、ASA を通じて導入されるため、サードパーティ製ツールや GPO の設定を使用することなく、容易に導入し、シンプルに管理することができます。

Umbrella ローミング クライアントがすでに組織に導入されている場合:

既存のローミング クライアント(スタンドアロン)の導入から、Umbrella ローミング セキュリティ モジュールに移行するには、特別な配慮が必要となります。既存の Umbrella ローミング クライアントのインストールの上に導入を行うには、次の手順に従います。

1. Umbrella ローミング セキュリティ モジュールが有効な状態で、AnyConnect 4.3 MR1 にアップグレードします。これにより、Umbrella ローミング クライアントが自動的に検出され、登録されている内容がコピーされたうえで、アンインストールされます。

2. 終了すれば、手順も終了です。

複数のテスト マシンにテストもしくはトライアルとしてのみ導入する場合:

Umbrella ローミング クライアントをまだインストールしていない場合

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、[+] ([追加(Add)] アイコン)をクリックします。

2. [モジュール プロファイル(Module Profile)] をクリックし、OrgInfo.json ファイルをダウンロードします。Windows:%ProgramData%¥Cisco¥Cisco AnyConnect Secure Mobility Client¥Umbrella¥
もしくは
Mac:/opt/cisco/anyconnect/Umbrella/
にファイルをドロップします。この手順を行う場合には、事前に必要なフォルダ構造を作成しておく必要があります。

4. Umbrella ローミング セキュリティ モジュールが有効な状態で、AnyConnect 4.3 MR1 にアップグレードします。

5. 終了すれば、手順も終了です。

システム要件

- Windows 7 以降の x86（32 bit）/x64（64 bit）オペレーティング システム

  VPN モジュールには、Visual Studio 2015 の 32 ビット ランタイムが必要です。これはインストール パッケージに付属しています。
  ローミング セキュリティ モジュールには、.NET Framework（3.5 以上）が必要です。
  注：IP 層での適用には追加の要件があります。こちらを参照ください。

- Mac OS X 10.9 以降のオペレーティング システム
- 追加のシステム要件やライセンスの依存関係の詳細については、『AnyConnect Secure Mobility Client Features, Licenses, and OS（AnyConnect Secure Mobility Client の機能、ライセンス、OS）』の機能ガイドを参照してください。

重要

AnyConnect 用の Umbrella ローミング セキュリティ モジュールは、フル機能を備えた Umbrella ダッシュボードと Cisco Umbrella ローミング パッケージの購入時に付属する機能制限版のダッシュボードのどちらとも連携します。本ドキュメントのこのセクションでは、制限版のローミング パッケージ ダッシュボードに関して説明します。フル機能の Umbrella ダッシュボードに関するドキュメントについては、docs.umbrella.com の他のセクションで確認できます。

ローミング セキュリティ モジュールの AnyConnect クライアントへの導入手順や、モジュールから送信される OrgInfo.json ファイルの収集手順は、使用されるダッシュボードにより異なります。

はじめる前に

1. ローミング クライアントと AnyConnect ローミング セキュリティ モジュールの非互換性。

2. Umbrella アカウントの取得。

3. Umbrella ダッシュボードからのローミング セキュリティ モジュールのプロファイル ファイルのダウンロード。

ローミング クライアントと AnyConnect 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 クライアントの間には互換性がありません。Umbrella ローミング セキュリティ モジュールを導入している場合、Umbrella ローミング クライアントの既存のインストールが、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自動的に検出され、削除されます。Umbrella ローミング クライアントの既存のインストールが、Umbrella サービスのサブスクリプションに関連付けられている場合、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。ただし、OrgInfo.json ファイルが AnyConnect のインストーラと同じ場所に配置されている場合、ネットワーク導入用に設定されている場合、Umbrella モジュールのディレクトリに事前導入されている場合には自動的に移行されません。また、Umbrella ローミング セキュリティ モジュールを導入する前に、Umbrella ローミング クライアントを手動でアンインストールすることもできます。

Umbrella アカウントの取得

Umbrella ダッシュボード（http://dashboard.umbrella.com）は、AnyConnect の 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。このプロファイルにより、Umbrella ローミング セキュリティ モジュールを導入に追加できます。また、Umbrella ダッシュボードのログインにも使われます。このダッシュボードで、ローミング クライアント用のポリシーとアクティビティのレポートを管理します。ダッシュボードのログインの際にサポートが必要な場合は、シスコのアカウント担当者までお問い合わせください。

導入時に使用する必要がある AnyConnect ファイル

ASA から導入する場合：
完全イントール パッケージ：Linux 64 ビット/ヘッドエンド導入（PKG）
完全イントール パッケージ：Windows/ヘッドエンド導入（PKG）
完全イントール パッケージ：Mac OS X/ヘッドエンド導入（PKG）

テスト目的で手動で導入する場合：
完全イントール パッケージ：Linux 64 ビット（tar.gz）
完全イントール パッケージ：Mac OS X/スタンドアロン インストーラ（DMG）
完全イントール パッケージ：Windows/スタンドアロン インストーラ（ISO）。DART、NAM、Core/VPN、Phone Home、Hostscan、ISE ポスチャ、WebSecurity コンポーネント用のインストール パッケージが含まれています。

Umbrella ダッシュボードからの AnyConnect ローミング セキュリティのプロファイルのダウンロード

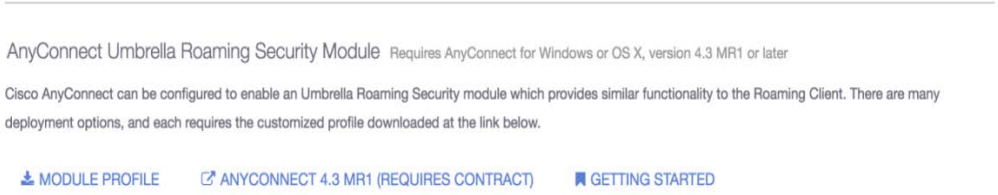
OrgInfo.json ファイルには、Umbrella ダッシュボードのインスタンスについての固有の情報が記録されており、レポート先や適用するポリシーに関する情報をローミング セキュリティ モジュールに通知します。

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（http://dashboard.umbrella.com）から、OrgInfo.json ファイルを取得する必要があります。

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、[+]（[追加（Add）] アイコン）をクリックします。

2. [AnyConnect Umbrella ローミング セキュリティ モジュール（AnyConnect Umbrella Roaming Security Module）] のセクションまでスクロールして、[ダウンロード（Download）] をクリックします。インストール/導入に関する個別の手順、パッケージ、ファイルの詳細については、『AnyConnect Deployment Overview（AnyConnect の導入と概要）』を参照してください。

3. [AnyConnect Umbrella ローミング セキュリティ モジュール（AnyConnect Umbrella Roaming Security Module）] のセクションまでスクロールして、[モジュール プロファイル（Module Profile）] をクリックし、OrgInfo.json ファイルをダウンロードします。



重要

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、他の登録ファイルもいくつか作成されます。したがって、OrgInfo.json ファイルを展開して置きかえる必要がある場合は、データ サブディレクトリを削除する必要があります。もしくは、Umbrella ローミング セキュリティ モジュールをアンイン

ストールして（データ サブディレクトリが削除される）、新しい OrgInfo.json ファイルで再インストールすることもできます。

OrgInfo.json には、Umbrella ダッシュボードのインスタンスについての固有の情報が記録されており、レポート先や適用するポリシーに関する情報をローミング セキュリティ モジュールに通知します。別のダッシュボードの OrgInfo.json ファイルを使用して、ローミング セキュリティ モジュールをインストールすると、クライアント コンピュータは、その別のダッシュボードに表示されます。

ローミング セキュリティ モジュールの稼動

AnyConnect を導入する場合、追加機能を有効にするオプション モジュールを含めたり、VPN やオプション機能を設定するクライアント プロファイルを設定したりすることができます。

ローミング セキュリティは、現在、これらのオプション モジュールの 1 つとなっています。

Web セキュリティ モジュールの互換性に関する情報

Umbrella ローミング セキュリティ モジュールを Web セキュリティ モジュールと同時に導入する場合は、スタティック IP での除外とホスト名での除外を設定する必要があります。詳細については、『Required Host Exception for Web Security and Roaming Security Compatibility（Web セキュリティとローミング セキュリティの互換の上で必要となるホストの除外）』と『Required Static Exception for Web Security and Umbrella Roaming Security Modules Compatibility（Web セキュリティと Umbrella ローミング セキュリティの互換の上で必要となるスタティック IP の除外）』を参照してください：

Windows 7 SP1 を使用している場合は、インストールもしくは最初の使用の前に、Microsoft .NET Framework 4.0 のインストールを推奨します。起動の際、Umbrella のサービスは .NET Framework 4.0 以降がインストールされているかを確認します。検出されない場合、Umbrella ローミング セキュリティ モジュールがアクティブにならず、メッセージが表示されます。先に進むためには、.NET Framework をインストールし、再起動して Umbrella ローミング セキュリティ モジュールをアクティブ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、Cisco 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 や 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、ASA から有効にする方法と、ISE から有効にする方法について、順次説明します。

ASA CLI

1. Umbrella ダッシュボードから取得した OrgInfo.json を、ASA ファイル システムにアップロードします。

2. 次のコマンドを実行します。グループ ポリシー名は、設定に応じて変更してください。

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

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

ASDM GUI

注:

ASDM 7.6.2 では、Umbrella ローミング セキュリティ モジュールを GUI から設定する必要がありますが、当該バージョンはまだリリースされていません。ASDM 7.6.2 がリリースされるまでは、CLI からの設定が唯一のオプションになります。

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）] に移動します。

2. [追加（Add）] を選択します。

3. プロファイルに名前を付けます。

4. [プロファイルの使用（Profile Usage）] ドロップダウン リストから、Umbrella セキュリティ ローミング クライアントのタイプを選択します。[プロファイルの場所（Profile Location）] フィールドに、OrgInfo.json ファイルが入力されます。

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 ファイルの場所を指定してください。

6. [グループ ポリシー（Group Policy）] ドロップダウン リストで、DfltGrpPolicy と関連付けます。グループ ポリシーで新しいモジュール名を指定する場合は、『Enable Additional AnyConnect Modules（追加の AnyConnect モジュールの有効化）』を参照してください。

ISE

ISE から有効化する場合は、次の手順に従います。

1. Umbrella ダッシュボードから OrgInfo.json をアップロードします。

2. OrgInfo.xml のファイル名を変更します。

3. 『Configure ISE to Deploy AnyConnect（ISE の設定による AnyConnect の導入）』の手順に従います。

クラウド更新

Umbrella ローミング セキュリティ モジュールでは、インストール済みのすべての AnyConnect モジュールを、Umbrella のクラウド インフラストラクチャから自動更新できます。クラウド更新によって、ソフトウェアの更新が Umbrella のクラウド インフラストラクチャから自動的に行われるようになります。更新のトラッキングも行われ、管理作業も一切不要です。

デフォルトでは、クラウド更新による自動更新は無効になっています。Umbrella ローミング セキュリティとその他の AnyConnect に対する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。[設定（Settings）] アイコン（歯車型のアイコン）の下にある、[新しいバージョンがリリースされた場合に VPN モジュールを含めた AnyConnect を自動更新する。VPN がアクティブの場合は更新しない。（Automatically update AnyConnect, including VPN module, whenever new versions are released.Updates will not occur while VPN is active.）] にチェックを入れます。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は、次の内容を考慮してください:

- 更新されるのは、現在インストールされているソフトウェア モジュールのみです。
- カスタマイズ、ローカリゼーション、その他の導入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ている際にだけ実行され、VPN が確立されている場合には実行されません。
- 更新が無効の場合は、最新のソフトウェア機能とアップデートは利用できません。
- クラウド更新を無効にしても、他の更新機能には影響しません。たとえば、Web での導入や遅延更新などには影響しません。
- クラウド更新では、AnyConnect の今後のバージョンやまだリリースされていないバージョン(暫定リリースやパッチ適用バージョン)をインストールしたデバイスは無視されます。

シスコの証明書のインポート

ネットワーク外の場合または VPN が無効になっている場合にローミング セキュリティ モジュールを使用するコンピュータにおいて、エンド ユーザ エクスペリエンスに重要なのは、シスコの証明書をインストールすることです。これは、HTTPS ドメインにアクセスした際のブロック ページにのみ影響を及ぼすものであるため、必須ではありませんが、推奨されます。HTTPS が有効化されたドメインがポリシーでブロックされた場合、Umbrella ローミング セキュリティ モジュールによりブロック ページが表示されますが、そのページも HTTPS により提供されます。このブロック ページは、シスコのルート CA で署名された証明書で暗号化されています。ブロック ページへのアクセスの際に、証明書のエラーが発生することを避けるには、シスコのルート CA をユーザのブラウザにインストールする必要があります。

これを実行するための手順は、オペレーティング システムやブラウザのタイプによって異なります。こちらに概要を示します。

クラウド Web セキュリティ(CWS)モジュールの互換性

Umbrella ローミング セキュリティ モジュールと、クラウド Web セキュリティ モジュールを連携させて使用するには、CWS による Umbrella ローミング モジュールの上書きを回避するために、2 つの設定変更が必要です。変更が必要な項目は、次に示すスタティック IP の除外とホスト名の除外です。

1. 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のために必要となる、スタティック IP での除外

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 モジュールとの相互互換性を確保するうえで、AnyConnect にプロビジョニングされる Web セキュリティのプロファイルで、次の例外を設定する必要があります。

67.215.64.0/19 204.194.232.0/21

208.67.216.0/21 208.69.32.0/21

185.60.84.0/22 146.112.61.0/24

146.112.128.0/18 146.112.192.0/18

2. Web セキュリティとローミング セキュリティの互換性のために必要となる、ホスト名の除外

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 モジュールを同時に導入する場合は、ホスト名の例外に *.opendns.com を設定する必要があります。そうしない場合、Umbrella ローミング セキュリティの DNS 保護が完全にバイパスされます。

エンドポイントでの UI の変化について

Umbrella ローミング セキュリティをインストールすると、AnyConnect エンドポイントの状態が新たに変化するのを確認できます。

AnyConnect のユーザ インターフェイス内では、ローミング セキュリティの現在のステータスがタイル表示されます。

注:ステータスが表示されない場合は、ローミング セキュリティ モジュールはインストールされていますが、OrgInfo ファイルが導入されていません。

状態	アイコンの色	説明	条件
			この動作状態は、次の条件で生じます。
予約済み	オレンジ	*接続状況をチェック中です。* アクティブなネットワーク接続がありません。ローミング モジュール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。	モジュールが最初にアクティブになった場合。 ネットワーク インターフェイスが変更された場合（新しいネットワーク アダプタの検出、既存のアダプタの IP の変更、新しい VPN トンネルの確立もしくは中断）。
オープン	イエロー	*現在、Umbrella によって保護されていません。* 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、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 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、元の設定に戻ります：DHCP またはスタティック。	この動作状態は、次の条件で生じます。 UDP 443 番ポートまたは UDP 53 番ポートでの Umbrella リゾルバ（208.67.222.222）への接続が確立していない場合。 ローカル ネットワークで、VA に Umbrella の DNS が設定されていない場合。 VPN トンネルが一時的に中断している、もしくは確立中である場合。

保護済み	グリーン	*Umbrella によって保護されています。*ネットワーク接続がアクティブで、ローミングモジュールが 208.67.222.222 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。	この状態は、モジュールが最初にアクティブ化された時、またはネットワーク インターフェイスに変更があった場合に発生する可能性があります。
暗号化済み	グリーン	*Umbrella によって保護されています。* Umbrella ローミング クライアントが、208.67.222.222 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。	この動作状態は、次の条件で生じます。 UDP 443 番ポートでの Umbrella リゾルバ（209.67.222.222）への接続が確立している場合。 TCP 443 番ポートおよび TCP 53 番ポートでの Umbrella リゾルバ（208.67.222.222）への接続が確立している場合。

保護されたネットワーク	グリーン	*Umbrella によってネットワークが保護されています。* 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。	この動作状態は、次の条件で生じます。 現在のエンドポイント ネットワークの出力 IP アドレスが、エンドポイントとして同じ Umbrella アカウントで登録されている場合。 使用されるリゾルバが、Umbrella クラウドのリゾルバ（208.67.222.222、208.67.220.220）である場合。 Umbrella ダッシュボードで設定されたポリシー（「保護されたネットワーク内では無効」）により、保護されたネットワークにある場合は、Umbrella モジュールが無効化されるようになっている場合。 **注**：ネットワーク レベルの保護のないパッケージもあるため、この状態はすべての Umbrella ローミング パッケージで発生するわけではありません。

仮想アプライアンスの範囲内	グリーン	*Umbrella 仮想アプライアンスによって保護されています。* コンピュータが、DNS サーバに設定された仮想アプライアンスが存在するネットワークに接続されています。ローミング モジュールは自身を無効にし、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。	この動作状態は、エンドポイントに設定された DNS アドレス（DHCP による設定もしくはスタティックな設定）が、Umbrella の VA のアドレスである場合に発生します。
VPN ネットワークが信頼済みの状態	グレー	*信頼済みのネットワーク上では無効。*ローカルの Umbrella モジュールの DNS 保護がアクティブではありません。現在のエンドポイントのネットワークが、AnyConnect VPN の信頼済みネットワークとして設定されているためです。	この動作状態は、次の条件で生じます。 AnyConnect VPN モジュールが、信頼ネットワーク検出の状態を、信頼済みとしてレポートしている場合。 AnyConnect VPN トンネルが、フル トンネル モードで確立もしくは接続されていない場合。 Umbrella ダッシュボードで設定されたポリシーにより、AnyConnect VPN の信頼済みネットワークにある場合は、Umbrella モジュールが無効化されるようになっている場合。 **注**：この設定は、すべてのローミング パッケージのお客様で有効になっており、管理者によって変更することはできません。

			この動作状態は、次の条件で生じます。 AnyConnect VPN モジュールが、信頼ネットワーク検出の状態を、信頼されていないとしてレポートしている場合。
VPN の状態による無効	グレー	*VPN がアクティブな間は無効。*ローカルの Umbrella モジュールの DNS 保護がアクティブではありません。現在、エンドポイントにアクティブな AnyConnect VPN トンネルが確立されているためです。	AnyConnect VPN トンネルが、フル トンネル モードで確立されている場合。 Umbrella ダッシュボードで設定されたポリシーにより、AnyConnect VPN トンネルが確立している場合は、Umbrella モジュールが無効化されるようになっている場合。 **注**:この設定は、すべてのローミング パッケージのお客様で有効になっており、管理者によって変更することはできません。
OrgInfo.json のステータスが不明	レッド	*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。ローカルの Umbrella モジュールの DNS 保護がアクティブではありません。現在、エンドポイントにアクティブな AnyConnect VPN トンネルが確立されているためです。	この動作状態は、OrgInfo.json ファイルが適切なディレクトリに配置されていないときに発生します。 Windows:%ProgramData%¥Cisco¥Cisco AnyConnect Secure Mobility Client¥Umbrella Mac:opt/cisco/anyconnect/umbrella

エージェントが使用不可な状態	レッド	*現在、Umbrella によって保護されていません。* サービスが使用できません。ローカルの Umbrella モジュールの DNS 保護がアクティブではありません。Umbrella エージェントが実行されていないためです。	この動作状態は、Umbrella エージェント サービスが、その時点で実行されていない場合に発生します（クラッシュまたは手動でのサービス停止）。
.NET の依存関係のステータスが不明（Windows のみ）	レッド	*現在、Umbrella 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 Umbrella モジュールの DNS 保護がアクティブではありません。Umbrella エージェントが実行されていないためです。.NET Framework のランタイムがありません。	この動作状態は、.NET 4.0 のランタイムがなく、Umbrella エージェント サービスが実行されていない場合に発生します。

診断の解釈

AnyConnect、またはローミング セキュリティ モジュールの一般的な問題については、『Cisco AnyConnect Secure Mobility Client Administrator Guide（Cisco AnyConnect セキュア モビリティ クライアント管理者ガイド）』を参照してください。また、診断に利用するために、DART レポートの実行を依頼することがあります。

ローミング セキュリティ モジュールにも同様に、独自のトラブルシューティング用診断ツールがあります。次の場所に、実行可能ファイルがあります。

Windows：
%Program Files (x86)%¥Cisco¥Cisco AnyConnect Secure Mobility Client¥UmbrellaDiagnostic.exe

Mac OS X：
/opt/cisco/anyconnect/bin/UmbrellaDiagnostic.app/

実行可能ファイルを実行すると、診断からのフィードバックをサポートに送信する方法が表示されます。

次に、**Cisco Umbrella のセキュリティ ポリシーの設定とレポートの確認**の設定を行います。

Cisco Umbrella ダッシュボードの設定

Cisco Umbrella のセキュリティ ポリシーの設定、レポートの確認、システム設定の確認

本ドキュメントのこの項目では、Cisco Umbrella ローミング セキュリティ モジュール（および AnyConnect）のみを所有しているお客様が利用できる独自のダッシュボードについて一通り説明します。従来の Umbrella ダッシュボードをご利用のお客様の場合には、ここに記載された概要よりもさらに多くの機能が利用可能です。こちらのサイトの各ドキュメントを参照ください。

レポート情報、ポリシー設定、システム設定の変更を確認するには、Cisco Umbrella のアカウントが必要です。

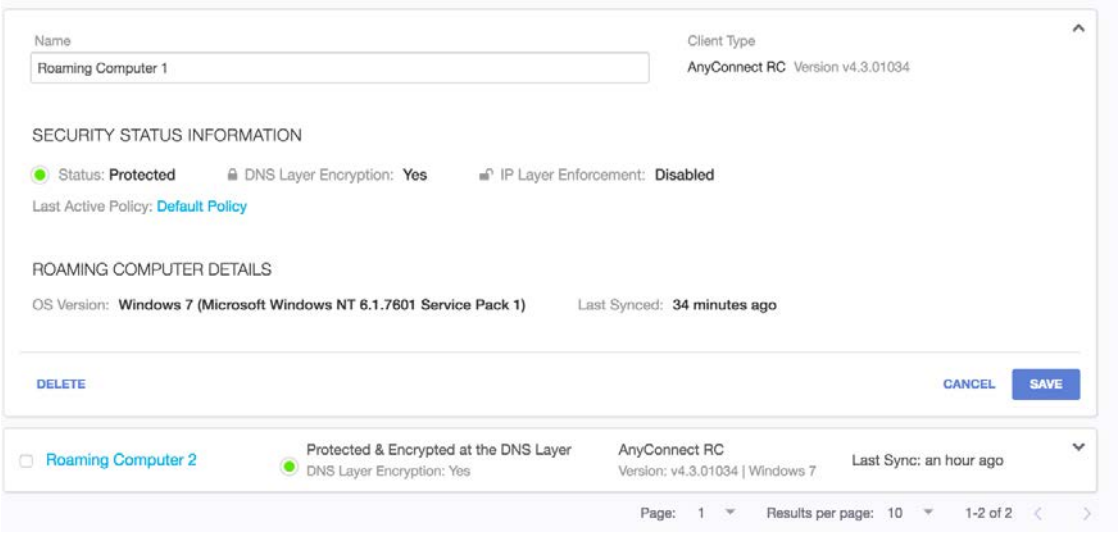
重要

ローミング コンピュータは、インストール後、ダッシュボードに自動的には表示されません。登録にしばらく時間がかかります。ローミング コンピュータが Umbrella のダッシュボードに表示されるのは、インストール後、90 分から 2 時間ほどしてからです。

Umbrella ローミング コンピュータのリスト

認証を行い、Umbrella ダッシュボードに移動します。そして、[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 クライアントのリストには、アクティブなものとアクティブでないものの両方が含まれ、インストールされたクライアントについての詳細が表示されます。ローミング コンピュータ名をクリックすると、次のように詳細が表示されます。



ダッシュボードのステータスには、次のものがあります。

- *オフライン*
- *保護されていない*
- *保護済み*
- *保護済みおよび暗号化済み*
- *VA 仮想アプライアンスによって保護済み*
- *ネットワークによって保護済み*
- *無効*
- *アンインストール済み*
- *一時停止中*

詳細

これらのステータスの詳細については、本ドキュメントの Umbrella ローミング セキュリティのセクションを参照してください。

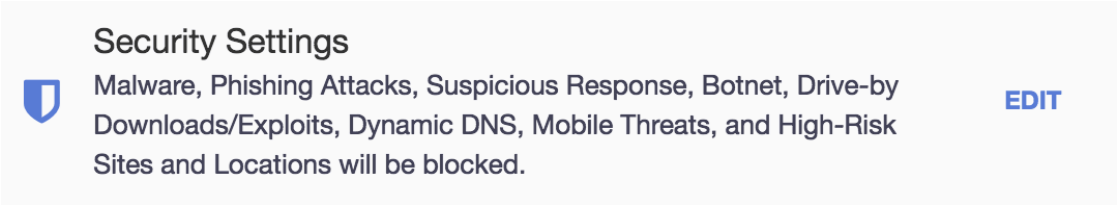
DNS 層の適用:ローミング セキュリティのベースラインが、DNS プロトコルで使用可能かどうか
IP 層の適用:セキュリティ層の追加が、IP 層適用トンネルで使用可能かどうか。

注:Cisco Umbrella ローミング セキュリティ モジュールの初回リリースでは、IP 層の適用機能は使用できません。なお、ごく短期間のうちに次のリリースが出され、使用可能となる予定です。その際には、これらのドキュメントも更新されます。

Umbrella ポリシーの詳細

最初に、ローミング コンピュータには、基本レベルのセキュリティ フィルタリングを備えたデフォルトのポリシーが適用されます。このポリシーの詳細については、ダッシュボードの [ポリシー（Policies）] セクションで確認できます。

1. *セキュリティ設定*

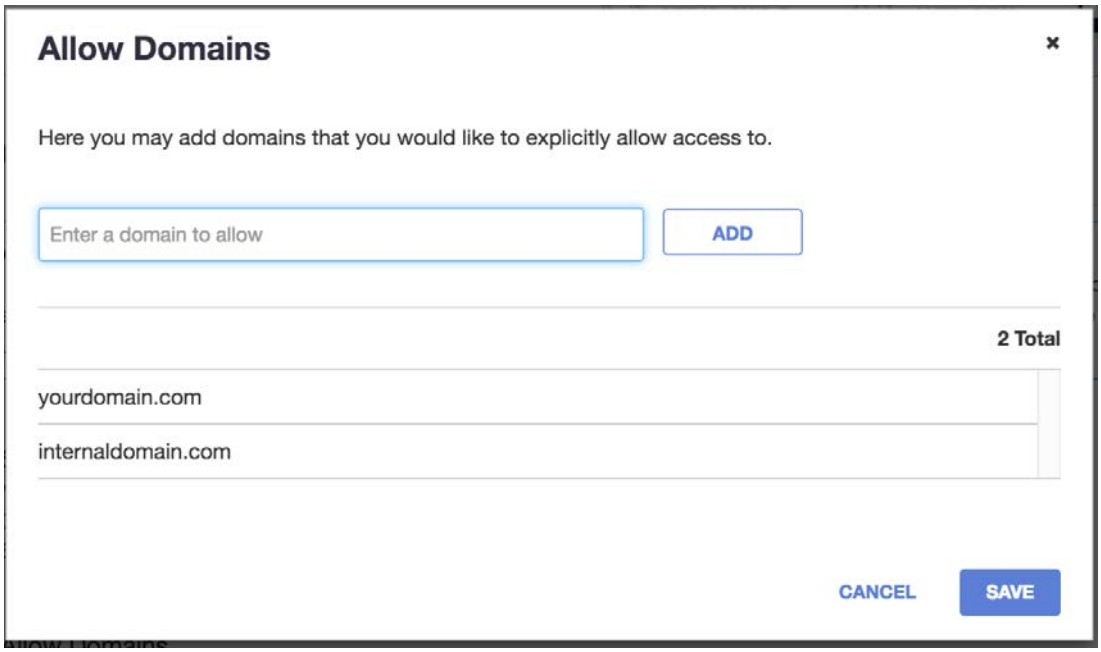


設定可能なセキュリティ設定を以下に示します。通常、大半のお客様には、デフォルトで有効になっている設定を使用するようにお勧めします。デフォルトでない設定を有効にする場合は、慎重に検証いただくようお願いします。

設定	機能	デフォルトで有効
マルウェア	サーバの障害や Web サイトの侵害を引き起こす悪意のあるソフトウェア。	○
ドライブ バイ ダウンロード/エクスプロイト	ユーザの介入なしにコードを実行するように設計された Web サイトやファイル。	○
ダイナミック DNS	ダイナミック DNS コンテンツをホストしているサイトのブロック。	×
モバイルの脅威	電話、タブレット、その他のローミング デバイスに特化した脅威。	×
疑わしい応答	内部ネットワーク空間に解決されるパブリック DNS エントリ。DNS 再バインディング攻撃に使われる手法。	×
フィッシング	ユーザに誤認させ、個人情報や財務情報の取得を狙う Web サイト。	○
ボットネット（コマンド アンド コントロール）	侵害されたデバイスが、ハッカーのコマンド アンド コントロール サーバと通信することを防ぐ。	○
高リスク サイトおよびロケーション	シスコのいくつかの統計モデルにより特定されたドメイン。	×

2. *ドメインの許可*

将来の時点で Cisco Umbrella によってブロックされたくないドメインを許可することは重要です。ドメインを許可リストに追加する場合、サブドメインもすべて潜在的に許可されることになります。つまり、「domain.com」を追加すると、「subdomain.domain.com」やその他のすべてのサブドメインも対象となります。Umbrella ローミング セキュリティにより意図しない検出が行われた場合は、このセクションでドメインを追加してブロックされないようにできます。変更した内容は、数分でプッシュされます。



3. *ブロック ページの表示*

この設定により、ブロック ページを個別に設定して、ページが組織のセキュリティ ポリシーによってブロックされたことを、ユーザに理解できるようにパーソナライズすることができます。

任意の画像を追加してブロックページをカスタマイズしたり、アクセスがブロックされた際にユーザが連絡を取るための電子メール アドレスを追加したりします。

Umbrella のレポート

Umbrella ローミング クライアントのレポートは、[レポート（Reporting）] の下にあります。アクティビティ検索レポートをチェックすると、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ていて VPN がオフになっているコンピュータから送信される DNS トラフィックが示されます。

これは、テスト設定に最適です。テストには、「internetbadguys.com」が利用できます。エンドポイントで Umbrella ローミング セキュリティのプロセスが正常に実行されていれば、フィッシングのアラートがトリガーされます。エンド ユーザにはブロック ページが表示され、レポートにそれが反映されます。

レポートのセクションには、次の内容が含まれます。

- セキュリティ アクティビティ
- クラウド サービス
- 総要求数
- アクティビティ ボリューム
- 上位ドメイン
- 上位カテゴリ
- 上位アイデンティティ
- オン/オフのネットワーク比較

Umbrella の設定

システム設定には、主要なものが 4 つあります。

アカウント: ここでは、アカウントの追加や削除ができます。新しいアカウントを追加する場合は、対象者の電子メール アドレスに招待メールが送信され、招待されたユーザはパスワードを設定することができます。新規ユーザには、3 つのロールを割り当てることができます。フル管理者ロール、読み取り専用ロールには名称どおりの権限が付与されます。レポート専用ロールの場合は、レポートへのアクセスはできますが設定はできません。

内部ドメイン:この項目は、Umbrella ローミング セキュリティ製品がネットワーク内に物理的に存在するとき、また VPN を経由して存在するときの動作を定義するうえで重要です。内部ドメイン機能により、特定のドメインの 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 Cisco 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。

こうしたリソースへのアクセスが中断されないことを確保するには、内部ドメインのセクションに適切なドメインを追加します。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 セキュリティ モジュール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。

ドメインの追加はシンプルです。必要に応じて、特定のサブドメインを追加するだけです、それ以外の場合は TLD を追加します。

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。

ダッシュボードの内部ドメインのセクションには、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。新しく追加されたドメインは、Umbrella ローミング セキュリティ クライアントと 10 分以内に同期します。

認証:ダッシュボードのこの項目では、Umbrella の 2 つの重要な項目、つまり二段階検証(二要素認証:2FA)と Security Assertion Markup Language(SAML)を使用するための機能について規定します。これらの設定は、セキュリティ上不可欠なものですが、より高度な設定になります。

SAML に関する詳細については、こちらを参照ください。

二段階検証の詳細については、こちらを参照ください。

ルート証明書:この部分の設定に関しては、本ドキュメントの次のセクションで詳しく説明します。こちらを参照してください。

シスコの証明書のインポートに関する情報

概要：シスコのルート CA をインストールする理由と方法

HTTPS が有効なドメインがポリシーでブロックされた場合、Cisco Umbrella によりブロック ページが表示されますが、そのページも HTTPS により提供されます。このブロック ページは、シスコのルート CA で署名された証明書で暗号化されています。ブロック ページへのアクセスの際に、証明書のエラーが発生することを避けるには、シスコのルート CA をブラウザにインストールする必要があります。また、コンピュータのネットワークがある場合には、ユーザのブラウザにインストールする必要があります。

これらの手順の理由

Umbrella のブロック ページと、ブロック ページのバイパス機能では、HTTPS サイトとの接続を確立するブラウザに SSL 証明書が提示されます。証明書は、要求を送信したサイトと照合されますが、シスコのルート認証局（CA）によって署名されます。そのため、シスコのルート CA がブラウザで信頼されていない場合、エラーが表示される可能性があります。一般的なエラーは次のようなものとなります。「この Web サイトで提示されたセキュリティ証明書は、信頼された証明機関から発行されたものではありません。（The security certificate presented by this website was not issued by a trusted certificate authority）」（Internet Explorer）、「このサイトのセキュリティ証明書は信頼されていません（The site's security certificate is not trusted!）」（Google Chrome）、「この接続は信頼されません」（Mozilla Firefox）。このエラーは想定内のエラーですが、表示されるメッセージは混乱を招き、余計な負担となる可能性もあることから、表示させないようにすることもできます。

これらのエラーを完全に回避するには、ブラウザもしくはユーザのブラウザ（ネットワーク管理者の場合）に、シスコのルート CA をインストールします。個人使用や小規模な環境の場合は、ブラウザごと、マシンごとに対処します。大規模な導入の場合は、グループ ポリシー（GPO）による自動インストールが可能です。なお、GPO による自動インストールが有効なのは、Windows システム上で Internet Explorer か

Chrome を使用しているユーザだけであることに留意ください。ネットワークに、Firefox ブラウザや Safari ブラウザを使用するユーザがいたり、Windows 以外のオペレーティング システムを使用するユーザがいたりする場合は、手動でのインストール手順を実施する必要があります。

本ドキュメントでは、ブラウザにシスコのルート CA を手動でインストールする際に必要な手順について説明します。

また、高度なスキルを持つユーザや大規模ネットワークのシステム管理者向けに、Microsoft Windows Active Directory のユーザ グループに対してシスコのルート CA を自動インストールする方法（Active Directory のグループ ポリシー オブジェクトを使用）についても、本ドキュメントで説明しています。なお、シスコのルート CA の自動インストールが有効なのは、Windows システム上で Internet Explorer や Chrome を使用しているユーザに対してのみです。したがって、ネットワークに、Firefox ブラウザや Safari ブラウザを使用するユーザがいたり、Windows 以外のオペレーティング システムを使用するユーザがいたりする場合は、手動でのインストール手順を実施する必要があります。

*重要:*これらの手順を実行するには、コンピュータのローカル管理者（または、ネットワークのネットワーク管理者）である必要があります。

概要：シスコのルート CA をインストールする理由と方法

この説明に含まれている手順は次のとおりです。

シスコのルート CA の自動インストール（Active Directory ネットワーク用）*

- Microsoft 管理コンソール（MMC）を使用したグループ ポリシーでの CA のインストール
- グループ ポリシー管理コンソール（GPMC）を使用したグループ ポリシーでの CA のインストール
- グループ ポリシーを使用した Firefox での CA のインストール

シスコのルート CA の手動インストール（単一のコンピュータ）

- Windows 上の Internet Explorer での CA のインストール
- Windows 上の Firefox 2 での CA のインストール

- Mac OS X 上の Safari での CA のインストール
- Mac OS X のコマンドラインでの CA のインストール
- Linux 上の Chromium または Chrome での CA のインストール

証明書のダウンロード

シスコのルート CA の自動インストール

Active Directory ネットワーク環境のネットワーク管理者の場合は、Active Directory サーバでグループ ポリシー オブジェクト（GPO）を作成することで、すべてのユーザのブラウザに自動的にルート CA をインストールできます。これは、Microsoft 管理コンソール（MMC）や、グループ ポリシー管理コンソール（GPMC）を使用して作成することができます。

Microsoft 管理コンソール（MMC）を使用したグループ ポリシーでの CA のインストール

- このドキュメントの最後のリンクからシスコのルート CA をダウンロードします。
- ドメインの管理者アカウントを使用して、Active Directory サーバにログインします。
- [スタート（Start）] > [すべてのプログラム（All Programs）] > [管理ツール（Administrative Tools）] > [Active Directory のユーザおよびコンピュータ（Active Directory Users and Computers）] を選択します。Microsoft 管理コンソール（MMC）が表示されます。
- ドメイン全体を対象とするポリシーを作成するには、ドメイン名として表示されるドメインのルートの組織単位（OU）を右クリックし、コンテキスト メニューから [プロパティ（Properties）] を選択します。
- [<OU 名>プロパティ（<OU_Name> Properties）] ダイアログ ボックスで、[グループ ポリシー（Group Policy）] タブをクリックします。
- [新規（New）] をクリックして、ポリシーに「Umbrella Certificate Installer（Umbrella 証明書インストーラ）」という名前をつけ、Enter を押します。
- 新しいグループ ポリシー オブジェクトを選択し、[編集（Edit）] をクリックします。グループ ポリシー オブジェクト エディタが表示されます。

- 左側の設定オプション サイドバーで、[コンピュータ設定（Computer Configuration）] > [Windows 設定（Windows Settings）] > [セキュリティ設定（Security Settings）] > [パブリック キー ポリシー（Public Key Policies）] と展開します。[信頼済みルート認証局（Trusted Root Certification Authorities）] を右クリックし、コンテキスト メニューから [インポート（Import）] を選択します。
- 証明書のインポート ウィザードで、[次（Next）] をクリックします。[インポートするファイル（File to Import）] のページで、[参照（Browse）] をクリックし、証明書がダウンロードされたローカル システムの場所に移動したうえで、Cisco_Umbrella_Root_CA.cer ファイルをダブルクリックします。
- [ファイル名（File name）] フィールドに証明書の完全パスが表示された状態で、[次へ（NEXT）] をクリックします。
- デフォルト オプションを受け入れ、すべての証明書を次のストア（信頼済みルート認証局）に置き、[次へ（Next）] 、[完了（Finish）] 、[OK] の順にクリックします。

これで、ドメインのすべてのコンピュータに証明書をインストールするグループ ポリシー オブジェクトが作成されました。新しいポリシーは、すべてのクライアント コンピュータにすぐには反映されません。デフォルトでは、バックグラウンドでの同期プロセスは 90 分から 120 分ごとにランダムなタイミングで行われます。クライアント マシンを再起動すると、同期が実行されます。

ワークステーション端末の Internet Explorer で、[ツール（Tools）] > [インターネット オプション（Internet Options）] > [コンテンツ（Content）] > [証明書（Certificates）] > [信頼済みルート認証局（Trusted Root Certification Authorities）] を開いて、シスコのルート CA 証明書が表示されていることを確認することで、ドメインのすべてのコンピュータにグループ ポリシーが伝播しているかチェックできます。

グループ ポリシー管理コンソール（GPMC）を使用したグループ ポリシーでの CA のインストール

Microsoft のグループ ポリシー管理コンソール（GPMC）サービス パック 1（SP1）は、企業全体のグループ ポリシーの管理を統合します。GPMC は、MMC のスナップインとグループ ポリシー管理用のプログラム可能なインターフェイスで構成されています。

- このドキュメントの最後のリンクからシスコのルート CA をダウンロードします。
- ドメインの管理者アカウントを使用して、Active Directory サーバにログインします。

- [スタート（Start）] > [プログラム（Programs）] > [管理ツール（Administrative Tools）] > [グループ ポリシー管理（Group Policy Management）] を選択します。グループ ポリシー管理コンソール（GPMC）が表示されます。
- ドメイン全体を対象とするポリシーを作成するには、ドメイン名として表示されるドメインのルートの組織単位（OU）を右クリックし、コンテキスト メニューから [ここに GPO を作成してリンクする（Create and Link a GPO Here）] を選択します。* [新しい GPO（New GPO）] ダイアログ ボックスが表示されます。
- [新しい GPO（New GPO）] ダイアログ ボックスの[名前（Name）] フィールドで、「Umbrella Certificate Installer（Umbrella 証明書インストーラ）」のようなわかりやすい名前をポリシー オブジェクトに入力します。
- ウィンドウの右側の新しいグループ ポリシー オブジェクト、「Umbrella Certificate Installer（Umbrella 証明書インストーラ）」を右クリックし、コンテキスト メニューから [編集（Edit）] を選択します。グループ ポリシー オブジェクト エディタが表示されます。
- 左側の設定オプション サイドバーで、[コンピュータ設定（Computer Configuration）] > [ポリシー（Policies）] > [Windows 設定（Windows Settings）] > [セキュリティ設定（Security Settings）] > [パブリック キー ポリシー（Public Key Policies）] を展開します。[信頼済みルート認証局（Trusted Root Certification Authorities）] を右クリックし、コンテキスト メニューから [インポート（Import）] を選択します。
- 証明書のインポート ウィザードで、[次（Next）] をクリックします。[インポートするファイル（File to Import）] のページで、[参照（Browse）] をクリックし、証明書がダウンロードされたローカル システムの場所に移動したうえで、Cisco_Umbrella_Root_CA.cer ファイルをダブルクリックします。
- [ファイル名（File name）] フィールドに証明書の完全パスが表示された状態で、[次へ（NEXT）] をクリックします。
- デフォルト オプションを受け入れ、すべての証明書を次のストア（信頼済みルート認証局）に置き、[次へ（Next）] 、[完了（Finish）] 、[OK] の順にクリックします。

これで、ドメインのすべてのコンピュータに証明書をインストールするグループ ポリシー オブジェクトが作成されました。新しいポリシーは、すべてのクライアント コンピュータにすぐには反映されません。デフォルトでは、バックグラウンドでの同期プロセスは 90 分から 120 分ごとにランダムなタイミングでのみ行われます。クライアント マシンを再起動すると、同期が実行されます。

ワークステーション端末の Internet Explorer で、[ツール（Tools）] > [インターネット オプション（Internet Options）] > [コンテンツ（Content）] > [証明書（Certificates）] > [信頼済みルート認証局（Trusted Root Certification Authorities）] を開いて、シスコのルート CA 証明書が表示されていることを確認することで、ドメインのすべてのコンピュータにグループ ポリシーが伝播しているかチェックできます。

グループ ポリシーを使用した Firefox での CA のインストール

デフォルトでは、グループ ポリシーで Firefox を設定することはできません。そうするためには、Firefox 用の設定オプションが含まれるようにグループ ポリシーを拡張する必要があります。Firefox ADMX を使用することで、グループ ポリシーや Active Directory の管理テンプレートを通じて、Firefox のデフォルト設定やロックされた設定が一元管理できるようになります。Firefox ADMX は、Firefox ADM の後継で、Mark Sammons 氏によって開発されています。

FirefoxADMX の Web サイトで、インストール方法が確認できます。

単一マシンでのシスコのルート CA の手動インストール

次の 3 つの手順では、個々のコンピュータ上の Internet Explorer、Firefox、Safari の各ブラウザで、シスコのルート CA を手動でインストールする方法について説明します。

Windows 上の Internet Explorer または Chrome での CA のインストール

Internet Explorer のブラウザに、シスコのルート CA を手動でインストールするには、次の手順を使用します。Chrome は、Internet Explorer の証明書ストアを使用するため、同じ手順で Chrome も設定できます。

- このドキュメントの最後のリンクからシスコのルート CA ファイルをダウンロードします。注：[ファイルを開く：セキュリティ警告（Open File - Security Warning）] のダイアログが表示される場合は、[開く（Open）] をクリックします。
- [証明書のインストール（Install Certificate）] をクリックします。
- [証明書のインポート ウィザード（Certificate Import Wizard）] ウィンドウで、[次へ（Next）] をクリックします。
- [証明書ストア（Certificate Store）] ウィンドウで、[すべての証明書を次のストアに置く（Place all certificates in the following store）] を選択し、[参照（Browse）] をクリックします。

- [証明書ストアの選択（Select Certificate Store）] ウィンドウで、[信頼済みルート認証局（Trusted Root Certification Authorities）] を選択し、[OK] をクリックします。
- [証明書ストア（Certificate Store）] ウィンドウで、証明書ストアに、信頼済みルート認証局が表示されます。[次へ（Next）] をクリックし、さらに [完了（Finish）] をクリックします。
- [セキュリティ警告（Security Warning）] ウィンドウで、[はい（Yes）] をクリックし、証明書をインストールします。
- [証明書のインポート（Certificate Import）] ウィザードで、[インポートが成功しました（The import was successful）] と表示されます。[OK] をクリックして終了します。
- Internet Explorer を終了し、再起動します。

Windows 上の Firefox での CA のインストール

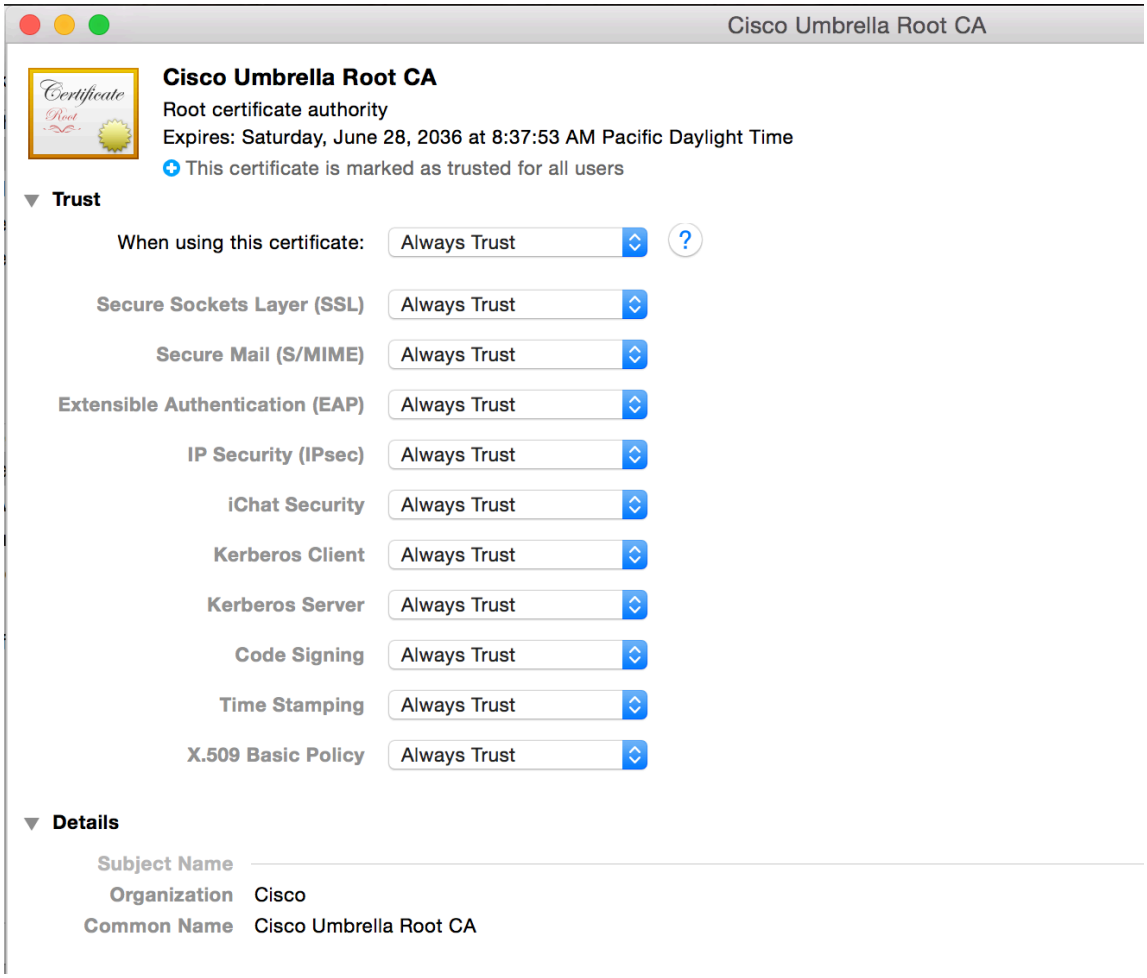
Windows 上の Firefox ブラウザに、シスコのルート CA を手動でインストールするには、次の手順を使用します。この手順では、コンピュータの管理者がすでにシスコのルート CA をダウンロードしており、ローカル システムに証明書をインストールするための適切なアクセス権限を持っているものとします。

- シスコのルート CA ファイル、Cisco_Umbrella_Root_CA.cer をダウンロードします。
- ブラウザ ウィンドウの右上隅の [メニューを開く（Open Menu）] アイコンをクリックします。
- [オプション（Options）] > [詳細（Advanced）] > [証明書（Certificates）] > [証明書の閲覧（View Certificates）] > [認証局（Authorities）] > [インポート（Import）] をクリックします。
- 最初の手順でダウンロードした、シスコのルート証明書を参照して選択します。
- [この CA を信頼して Web サイトを識別する（Trust this CA to identify websites）] を選択します。[OK] をクリックし、もう一度 [OK] をクリックします。
- Firefox ブラウザを再起動します。
- Firefox の証明書ストアは、NSS ツール パッケージの certutil ツールを使用して、コマンドラインから処理することもできます。詳細については、次の Mozilla のドキュメントを参照ください。 https://developer.mozilla.org/en-US/docs/Mozilla/Projects/NSS/tools/NSS_Tools_certutil

Mac OS X 上の Safari での CA のインストール

Mac OS X 上の Safari ブラウザに、シスコのルート CA を手動でインストールするには、次の手順を使用します。この操作を実行するには、コンピュータの管理者である必要があります。

- シスコのルート CA ファイル、Cisco_Umbrella_Root_CA.cer をダウンロードします。
- ファイルをダブルクリックするか、[アプリケーション（Applications）] > [ユーティリティ（Utilities）] フォルダの [キーチェーン アクセス（Keychain Access）] アイコンの上にドラッグ アンド ドロップします。[証明書の追加（Add Certificate）] ウィンドウが表示されます。[常に信頼（Always Trust）] をクリックします。
- シスコのルート CA をダブルクリックして、プロパティ ウィンドウを開きます。[この証明書の使用時（When using this certificate）] のプルダウンを [常に信頼（Always Trust）] に変更します。



Mac OS X のコマンドラインでの CA のインストール

OS X のコマンドラインで CA をインストールするには、CA をダウンロードして、次のコマンドを実行します。
注:この操作を実行するには、コンピュータの管理者である必要があります。

テキスト
sudo /usr/bin/security add-trusted-cert -d -r trustRoot -p ssl -p basic -k /Library/Keychains/System.keychain /path/to/Cisco_Umbrella_Root_CA.cer

Linux 上の Chromium または Chrome での CA のインストール

Linux の Chromium ベースのブラウザに、シスコのルート CA を手動でインストールするには、次の手順を使用します。

1. シスコのルート CA ファイル、Cisco_Umbrella_Root_CA.cer をダウンロードします。
2. Chromium の設定を開きます。
3. [HTTPS/SSL] までスクロールします。
4. [証明書の管理（Manage certificates）] をクリックします。
5. [認証局（Authorities）] をクリックします。
6. [インポート（Import）] をクリックします。
7. Cisco_Umbrella_Root_CA.cer を選択し、[開く（Open）] をクリックします。
8. [この CA を信頼して Web サイトを識別する（Trust this CA to identify websites）] を選択します。
9. [OK] をクリックします。

証明書のダウンロード

証明書をダウンロードするには、https://dashboard.umbrella.com に移動し、[ポリシー（Policies）] > [ルート証明書（Root Certificate）] に移動します。

証明書のダウンロード リンクはこちらです。