Cisco Umbrella へようこそ

このガイドでは、Cisco Umbrella の使用を開始するために必要な情報を提供します。基本的な設定を順を追って示すことで、新しいセットアップを設定する方法を示します。各種のコンポーネントに関する詳細なサポート記事のリンクも記載されています。

このガイドには次のセクションがあります。

- Umbrella のクイック スタート ガイド（このセクション）：ネットワークを保護し、DNS サービスの接続先が Umbrella になるようにします。またポリシーのカスタマイズ方法と、Intelligent Proxy を有効にしてさらに保護を強化する方法を説明します。
- ローミング クライアント セットアップ ガイド：Umbrella ローミング クライアントをラップトップやデスクトップに展開し、機能を追加する方法を示します。
- 仮想アプライアンス セットアップ ガイド：仮想アプライアンス（VA）を設定して導入し、ネットワーク内の詳細な情報を取得して、レポートとポリシー適用に利用する方法を説明します。
- Active Directory セットアップ ガイド：AD ユーザのコンピュータおよびグループと DNS アクティビティを関連付ける方法を説明します。
  開始するには、まずはダッシュボードにサインインするのが最も簡単です。http://dashboard.umbrella.com にアクセスしてください。ログインすると、新規アカウントの場合は [セットアップ ガイド（Setup Guide）] が表示されます。この統合されたインタラクティブなガイドでは、Umbrella ダッシュボードの基本的な要素を確認することができます。

今お読みのガイドには、ダッシュボードの [セットアップ ガイド（Setup Guide）] よりもさらに詳細な説明が記載されています。またダッシュボードのオンプレミスまたは高度なコンポーネントをセットアップする手順も確認できます。ただし最初の段階では、組み込みの [セットアップ ガイド（Setup Guide）] を参照することで、すばやく使い始めることができます。

これらのガイドが表示されなくなった場合は、こちらをクリックしてセットアップ ガイドにアクセスするか、https://dashboard.umbrella.com/#setupguide にアクセスしてください。

Umbrella ダッシュボードを使用するには、最初にアイデンティティを追加します。アイデンティティは、ポリシーを適用し、レポートの対象になるものです。組み込みの [セットアップ ガイド（Setup Guide）] による導入では、次の 2 つタイプのアイデンティティを使用できます。

- ネットワーク
- ローミング クライアント

このガイドでは、次にネットワークで Umbrella を使用するように設定します。ただし、特にまだ評価中のお客様の場合は、1 台のコンピュータをローミング クライアントで保護するほうが簡単です。ローミング クライアントの詳細については、こちらをクリックしてください。

その他の場合は、次のセクション「ネットワークを保護する」から始めましょう。

ネットワークを保護する

ネットワークは Umbrella ではアイデンティティとして扱われ、ネットワーク自体のパブリック IP スペースによって定義されます。IP スペースから発信されたトラフィックは、すべて Umbrella のネットワークから発信されたものとして認識されます。したがって、Umbrella にネットワークを追加するには、パブリック IP スペースまたは IP 範囲を追加してアイデンティティを定義します。アイデンティティを追加したら、ポリシーを作成して、そのネットワーク内からインターネットに接続するデバイスに Umbrella の保護を展開する必要があります。

ステップ 1：適切なネットワークを選択する

最初に、使用中のコンピュータが接続するネットワークを設定します。そのネットワークのパブリック IP が不明である場合は、http://www.whatismyip.com を参照してください。

注：

Umbrella ダッシュボードへのアクセスに現在使用しているネットワークとは別のネットワークを追加する場合は、手動による確認について、サポートまでお問い合わせください。また、IP 範囲が /29 ネットワークをよりも大きなネットワークに関しても、サポートによる手動の確認が必要になります。確認のためのケースは自動的に作成され、確認が終了次第、直ちに更新を受信できます。

ステップ 2：ネットワーク アイデンティティを設定する

開始する前に、動的 IP アドレスを使用しているかどうかを確認してください。ほとんどの家庭、小規模の学校、小規模のビジネスのネットワークは、それぞれのインターネット ネットワークの定義に動的 IP アドレスを使用するインターネット サービス プロバイダー（ISP）によってプロビジョニングされています。静的 IP アドレスを使用しているかわからない場合は、ほとんどの場合では静的 IP アドレスはありません。

動的 IP アドレスの場合は、その IP アドレスの「リース」が変更されると、ネットワークのパブリック IP も変更されます。IP は数週間は変わらないとしても、いずれリースは期限切れになり、ISP の別の顧客にそのリースが付与されることになります。

Umbrella に登録した IP アドレスが変更された場合、Umbrella のセキュリティ設定は適用されなくなります。これらの設定はアカウント情報と一致しなくなるため、更新が必要になります。

この情報を手動で更新しなくてもすむように、Umbrella に登録したネットワーク内の 1 台以上のコンピュータに、Umbrella Dynamic IP Updater をインストールすることをお勧めします。

注

ほとんどのダイナミック DNS（DDNS）クライアントには、ネットワークを最新に維持する機能があります。ただし、サードパーティ製 DDNS クライアントはサポート対象ではありません。

ネットワークを追加するには、次の手順を実行します。

1. [アイデンティティ（Identities）] > [ネットワーク（Network）] に移動します。
2. [+]（**追加**アイコン）をクリックします。

3. 新しいアイデンティティにわかりやすい名前を付け、IP アドレスとサブネットマスク（通常は単一の IP アドレスである /32 サブネット）を追加します。
4. これが動的 IP アドレスである場合は、[動的（Dynamic）] をオンにして、Umbrella Dynamic IP Updater をダウンロードします。
   Umbrella Dynamic IP Updater では、動的 IP アドレスが変更されると、ネットワークの IP アドレスが自動的に検出され、Umbrella アカウントに登録されます。Dynamic IP Updater を使用しない場合は、IP アドレスが変更されるたびに、手動で再入力する必要があります。

5. 日次ステータス レポートを受信するには、[日次ステータス メールを有効にする（Enable a daily stats email）] をオンにして、電子メール アドレスを指定します。このレポートには、[合計要求数（Total Requests）]、[固有ドメイン（Unique Domains）]、[ドメイン（Domains）]、[ブロックされたドメイン（Blocked Domains）]、[要求タイプ（Request Types）] が記載されます。最初の電子メールは、有効にしてから 24 ～ 48 時間以内に届きます。

6. [保存（Save）] をクリックします。

注

可能であれば、登録されている IP からネットワークを追加します。それ以外の場合は、登録されているネットワークの IP アドレスからリンク先にアクセスすることを要求する電子メールが届きます。

ステップ 3：関連するネットワーク デバイスの DNS 設定を変更する

これは、エッジ DNS 機器（一般的に DNS または DHCP サーバ）で、またはルータ（DSL ルータまたはケーブル モデム（ネットワーク内の唯一のルータである場合））でのみ行う必要があります。

モバイル デバイス、コンピュータ（ラップトップを含む）、またはルータの設定方法については、この記事を参照してください。

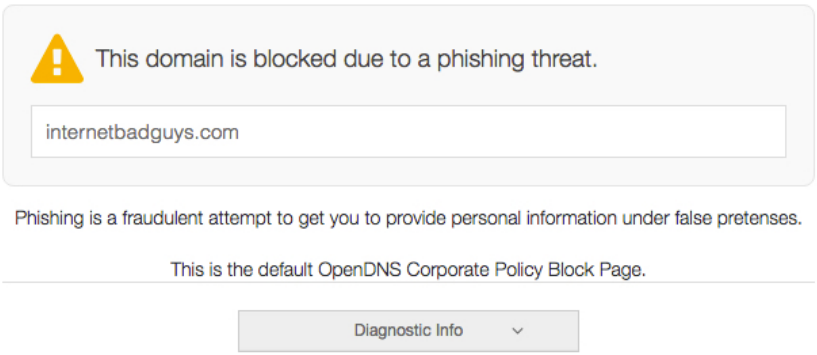
注

テストを実行するクライアントでは、確認を正常に行うために、DNS/DHCP サーバまたはルータから新たに一連の DNS サーバを取得しているか、DNS 設定を手動で変更している必要があります。

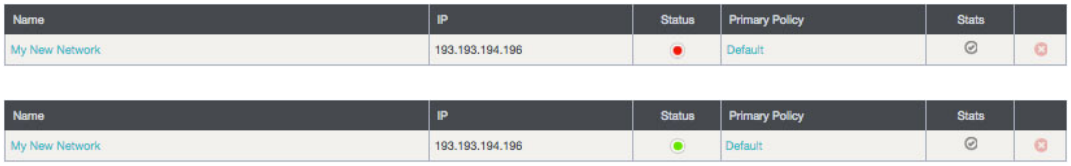
ステップ 4：ネットワークをテストする

以上です。この時点でクライアントのネットワーク インターフェイスを再起動（またはコンピュータを再起動）すると、クライアントのブラウザで http://internetbadguys.com にアクセスすることで、Cisco Umbrella グローバル ネットワークを通じて DNS 接続がルーティングされていることを確認できます。

次のページが表示されます。



サービスによって IP アドレスが検証されると、[アイデンティティ(Identities)] > [ネットワーク(Networks)] のリストにネットワークが表示されます。最初は、ネットワークステータスが赤く表示されます。ネットワーク ステータスは、DNS トラフィックがそのネットワークから Umbrella に送信された場合のみ緑色に変わります。



ステップ 5:次のステップ

ネットワーク アイデンティティが設定され、ネットワークから DNS トラフィックを受信できるようになりました。次に、DNS の接続先を Cisco Umbrella に設定します。

Cisco Umbrella へようこそ <**ネットワークを保護する**> DNS の接続先を Cisco Umbrella に設定する

DNS の接続先を Cisco Umbrella に設定する

DNS を設定することで、ネットワークからのトラフィックの接続先を Cisco Umbrella グローバル ネットワークにすることができます。インターネット上のホスト名を解決する要求が、シスコの DNS アドレスを接続先としてネットワークから送信されると、Umbrella がポリシーに応じたセキュリティ設定を適用します。

Umbrella に切り替えるには、オペレーティング システムまたはハードウェアのファイアウォール/ルータ内の DNS 設定を明示的に変更して、Umbrella のネーム サーバの IP アドレスを使用するように設定し、ISP から提供された自動 DNS サーバをオフにするように設定する必要があります。

Umbrella の IP アドレス（IPv4）は次のとおりです。

- 208.67.222.222
- 208.67.220.220

複数のシステムを使用している場合は、複数の DNS サーバを指定できます。その場合も、Cisco Umbrella サーバだけを使用して、他の DNS サーバをリストに含めないようにすることをお勧めします。

注

この手順を最後まで実行するには、ルータ、DNS サーバ、または自身のコンピュータに対する管理アクセス権が必要になるため、その権限を持つユーザだけがこの手順を実行することをお勧めします。

ステップ 1：パブリック DNS サーバのアドレスが設定されているマシンを見つける

パブリック DNS サーバのアドレスが設定されている、ネットワーク内のデバイスまたはサーバを判別します。これは多くの場合、ルータまたは DNS サーバになります。一般的に、ルーティング不可能な内部 IP アドレス（DHCP）を提供するデバイス、ま

たはデフォルト ゲートウェイとして機能するデバイスにも、パブリック DNS サーバが設定されています。

ステップ 2：DNS が設定されているサーバまたはルータにログインする

ログインしたら、このデバイスの DNS 設定を見つけます。これらの設定の場所がわからない場合は、こちらをクリックして設定ガイドにアクセスし、サーバとルータの設定に関するガイダンスを参照してください。

ステップ 3：DNS サーバのアドレスを変更する

Cisco Umbrella を使用するように DNS 設定を変更する前に、現在の DNS サーバのアドレスまたは設定を記録してください（たとえば紙に書き留めるなど）。後日必要になった場合に備えて、これらの数字をバックアップ目的で保存しておくことが重要です。

注

ISP によっては、DNS サーバが提供されている機器にハード コードされている場合があります。そのようなデバイスを使用している場合は、Umbrella を使用するように設定することはできません。代わりに、Umbrella のローミング クライアントをインストールして各コンピュータを設定するか、各コンピュータ上で DNS サーバのアドレスを設定できます。一般的な Windows または Macintosh コンピュータの設定方法については、https://support.opendns.com/forums/21618384 を参照してください。

DNS 設定を変更するプロセスは、オペレーティング システムとバージョン（Windows、Mac、または Linux）、またはデバイス（DNS サーバ、ルータ、またはモバイル デバイス）によって異なります。OS、ルータ、またはデバイスによっては、この手順を適用できない場合があります。確実な情報については、ベンダーのドキュメントを参照してください。また、シスコの『Router Configuration（ルータ設定）』、『Computer Configuration（コンピュータ設定）』、『Mobile Device Configuration（モバイル デバイス設定）』、または『Server Configuration（サーバ設定）』の各ガイドも参照してください。

一般的なルータで設定を変更するには、次の手順を実行します。

1. ブラウザで IP アドレスを入力して、ルータのユーザ インターフェイスにアクセスし、パスワードを入力します。

2. DNS サーバの設定が指定されている設定領域を特定し、それらのアドレスを Cisco Umbrella の IP アドレスに置き換えます。
    - 208.67.222.222
    - 208.67.220.220
      どちらの DNS アドレスもプライマリまたはセカンダリ DNS サーバとして使用できますが、必ず両方の数字を使用し、同じ IP アドレスを 2 回使用しないようにしてください。ルータで 3 つ目または 4 つ目の DNS サーバ設定を必要とする場合は、208.67.220.222 と 208.67.222.220 を、それぞれ 3 つ目と 4 つ目のアドレスとして入力してください。

4. 変更を保存し、ルータのユーザ インターフェイスを終了します。

5. DNS キャッシュを消去します。

6. 設定が正しく動作しているかどうかをテストします。以下の「新しい DNS 設定のテスト」を参照してください。

DNS は、必ず静的アドレスとして設定してください。

注:

DNS を変更すると、サービスに影響する結果をキャッシュする可能性があります。DNS の最新の結果だけを受け取るようにするには、DNS キャッシュを消去します。DNS キャッシュを消去する方法については、こちらをクリックしてください。

ステップ 4:新しい DNS 設定をテストする

DNS 設定が完了したところで、http://welcome.opendns.com にアクセスします。DNS の接続先を Cisco Umbrella サーバに設定できていると、次の確認ページが表示されます。

注:

知識が豊富なユーザは、Umbrella を回避するように DNS 設定を変更しようとする可能性があります。これはファイアウォール ルールによって防止できます。詳細についてはこちらをクリックしてください。

Cisco Umbrella のようこそページにアクセスできない場合、または Web ページを読み込めない場合は、次の方法をお試しください。

1. ブラウザで、アドレス バーに固定 IP アドレスを入力します。http://18.62.0.96/（http://www.eecs.mit.edu/ をポイント）と入力します。それでも Umbrella のようこそページにアクセスできない場合は、DNS の設定に問題があります。すべてを正しく設定しているかどうか、上記の手順を再度確認してください。それでも解決できない場合は、ステップ 2 に進みます。

2. 実行した DNS 変更を元に戻し、再度テストを実施します。テストが失敗する場合は、ネットワーク設定または ISP に問題があります。

3. Umbrella ダッシュボードの [サポート（Support）] タブ、または https://support.umbrella.com/tickets/new から、サポートにお問い合わせください。

次に固有の Umbrella ポリシーを作成して、保護とフィルタリングをカスタマイズします。

ポリシーのカスタマイズ

これですべての作業は完了しました。保護が設定されました。

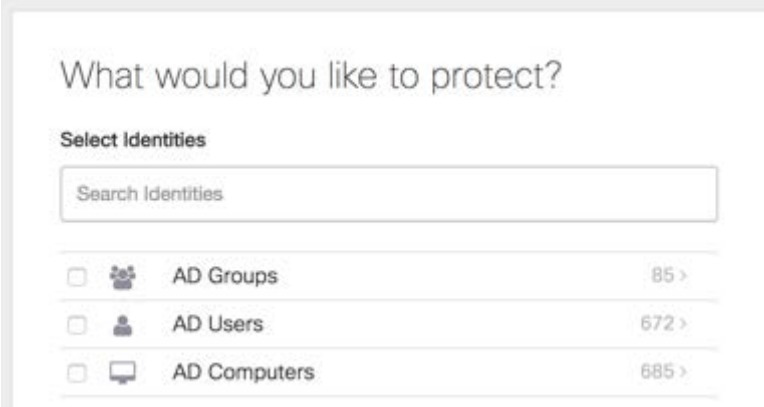
前の手順に従ってネットワークを保護し、DNS の接続先を Umbrella に設定すれば、ネットワークまたはデバイスは保護されています。簡単な手順で保護が確保されました。

このページでは、ポリシー マネージャの概要を示します。ここではポリシーの各要素を段階的なプロセスに分解します。

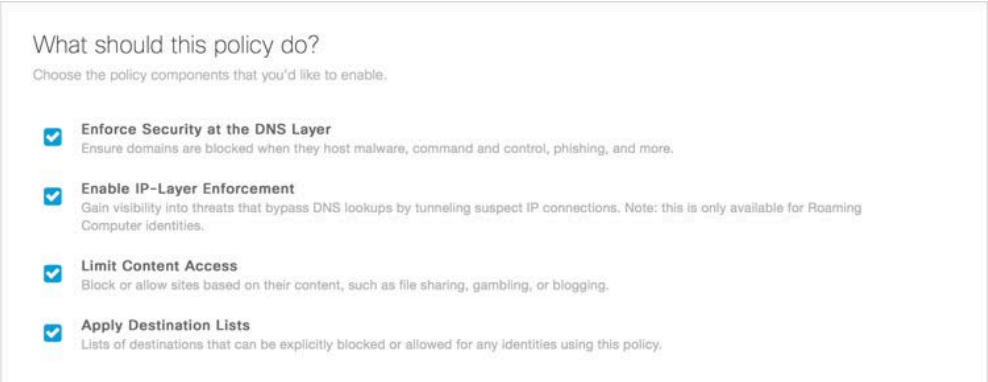
ポリシーは、フィルタリングするサイトのタイプを含め、保護とロギングのレベルを制御します。ポリシー ウィザードを使用すれば、作成したアイデンティティにポリシーを効率的に適用できます。ポリシー ウィザードでは、「このポリシーの目的は何か」というような問いに対して答えながら、段階的なプロセスで設定できるように設計されています。

ポリシーの設定を開始する

最初に、ポリシーによって保護するアイデンティティを選択します。



次のステップでは、[このポリシーの目的は何か（What should this policy do?）] という問いに答えます。



選択肢は複数あり、どの選択肢を選択したかに応じて、Umbrella の機能とサービスを最大限に活用するための設定手順が変わります。ポリシーの設定を進める過程では、セットアップ フローから離れることなく、ウィザードで設定を簡単に編集できるようになっています。

設定が完了すると、確認画面が表示されます。どのような変更を行ったかがわかり、ポリシーを保存する前に修正することが可能です。

注：

ポリシーは追加されていくものではなく、最初の一致に基づいてアイデンティティに適用されます。最上位に最も近い位置で一致したポリシーが適用されます。ドラッグ アンド ドロップでポリシーの順番を変更することができます。これに関するベスト プラクティスを示すガイドも用意されています。ポリシー定義のベスト プラクティスを参照してください。

デフォルトでは、ポリシーは常に 1 つ（デフォルトポリシー）です。アイデンティティに対応するポリシーが他に設定されていなければ、デフォルト ポリシーがすべてのアイデンティティに適用されます。つまり Umbrella のデフォルト ポリシーは、組織内のすべてのアイデンティティが基本レベルの保護を受けられるようにするための汎用的なポリシーです。

ステップ 1：最初の新しいポリシーを作成する

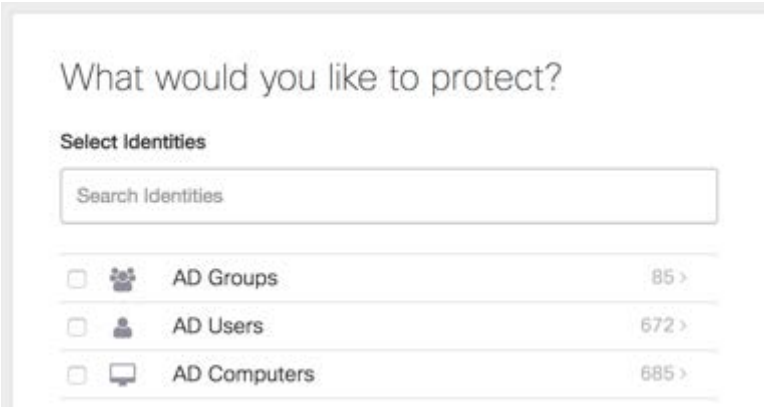
1. [ポリシー（Policies）] > [ポリシー リスト（Policy List）] を選択すると、デフォルトポリシーが表示されます。このポリシーを選択するか、[+] アイコンをクリックすると、新しいポリシーの作成が開始され、最初に保護対象が尋ねられます。

2. 設定したいずれかまたはすべてのアイデンティティを選択します。[デフォルトポリシー（Default Policy）] を選択するとすべてのアイデンティティが選択され、サマリー画面が表示されます。これは、デフォルトのポリシーがすでに設定されていて、作成されたアイデンティティに適用されているためです。

アイデンティティの選択

ポリシーの編集では、最初にポリシーを適用するアイデンティティを選択します。それにより、設定が適用される対象が決定されます。アカウントで使用できるアイデンティティから任意の組み合わせで選択できます。カテゴリ（[AD コンピュータ（AD Computers）] や [ローミング コンピュータ（Roaming Computers）] など）をドリルダウンすることで、ポリシーを適用するアイデンティティをさらに詳細に選択できます。アイデンティティが 1 つだけ（ネットワーク）である場合は、そのアイデンティティを選択します。

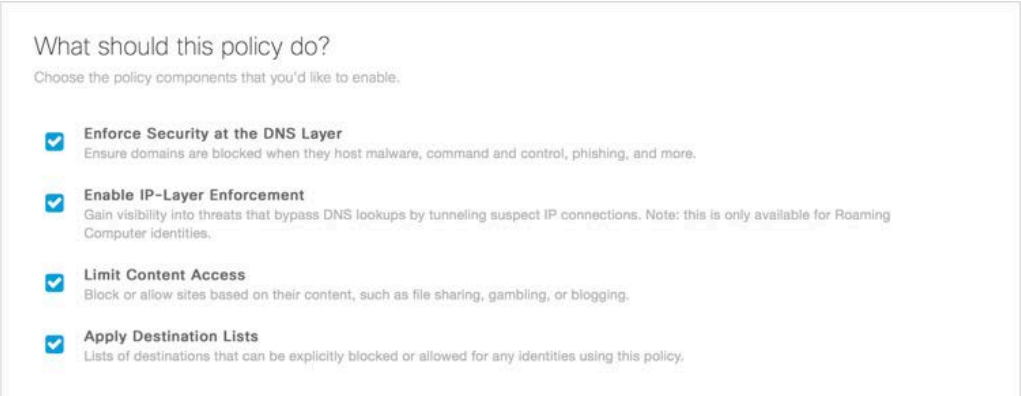
注：デフォルト ポリシーはすべてのアイデンティティに適用されるため、サマリー画面からデフォルト ポリシーを編集する場合は、アイデンティティの編集機能が制限されます。



ポリシーを適用するアイデンティティを選択し、[次へ（Next）]をクリックします。

ステップ 2：ポリシーの目的を選択する

次にポリシーの目的を尋ねられます。次のようなオプションがあります。使用できないオプションがある場合は、アカウント担当者にお問い合わせください。

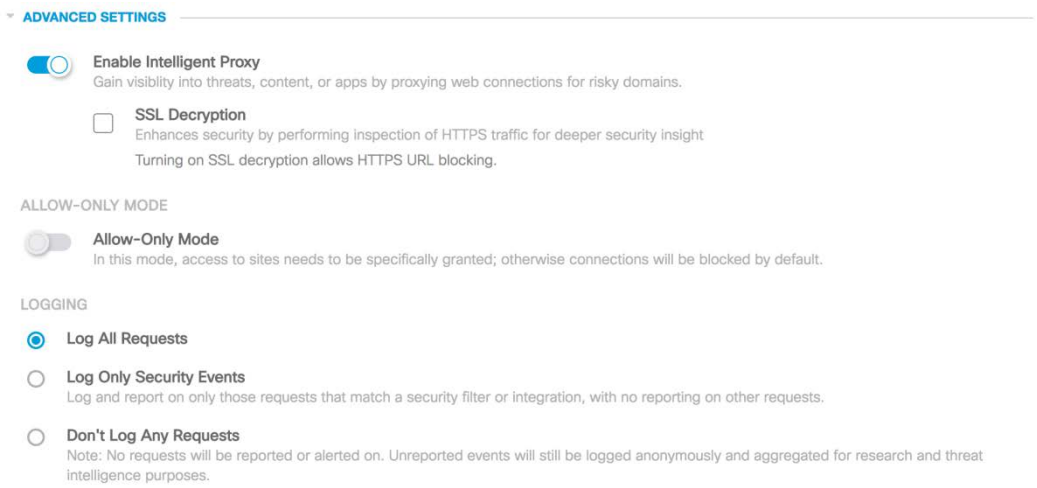


表示されている 4 つのオプションは、セキュリティ設定、IP レイヤ適用、コンテンツ カテゴリ ブロック、カスタム接続先リストという 4 つのポリシー機能に対応しています。

- [DNS レイヤにセキュリティを適用する（Enforce Security at the DNSLayer）]：悪意の有無に基づくドメインのブロックに直接関係する設定であり、基本レベルのセキュリティ保護が得られます。このオプションは必ず選択することをお勧めします。
- [IP レイヤ適用を有効にする（Enable IP LayerEnforcement）]：IP レイヤ適用は、シンプルなドメインのみのセキュリティを超えてドメインをブロックします（ローミング クライアントのアイデンティティのみ）
- [コンテンツのアクセスを制限する（Limit ContentAccess）]：組織のアクセプタブル ユース ポリシーに基づいてコンテンツ タイプのフィルタリングを行います。
- [接続先リストの適用（Apply DestinationLists）]：許可またはブロックする必要がある特定のドメインがある場合は、それらのドメインを接続先リストに追加します。デフォルトでは、2 つのリスト（[ブロック（Block）] と[許可（Allow）]）があります。接続先リストは、ドメインのグループを整理するために追加作成できます。2 つのデフォルトは「グローバルな」リストであり、*すべて*のポリシーに適用されます。

注:グローバル接続先リストは、[ブロック(Block)] の場合も [許可(Allow)] の場合も、*すべてのポリシーとすべてのアイデンティティ*に適用されます。つまり、組織全体の設定に対してグローバルに適用されます。さらに詳細なリストを定義するには、新しいリストを作成してドメインを追加し、そのリストを個々のアイデンティティのセットに適用します。

ポリシーの目的を示すオプションの下に、[詳細設定(Advanced Settings)] があります。



これにはインテリジェント プロキシ、SSL 復号化、許可限定モード(従来の「ホワイトリスト モード」)、およびロギング オプションがあります。

インテリジェント プロキシは、選択したパッケージに対してアクティブにすることもできます。それにより、正当なコンテンツの一部に悪意のあるファイルが含まれたドメインに対する、URL ベースのマルウェア フィルタリングが可能になります。
ただし、インテリジェント プロキシを有効にしない場合は、プロキシを使用できなくなるため、ポリシーの目的のオプションで一部が使用できなくなります。ポリシーでインテリジェント プロキシを使用しない場合でも、試してみることをお勧めします。
インテリジェント プロキシとその機能の詳細、および HTTPS 検査の有効化に関する重要な情報については、インテリジェント プロキシの有効化を参照してください。

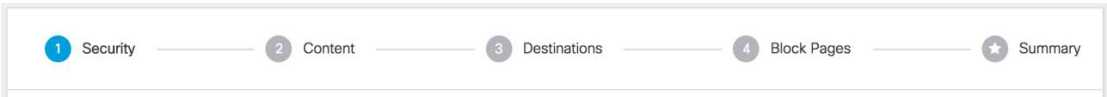
許可限定モードは、少数のドメインにアクセスを限定し、*その他すべて*のドメインをブロックする場合のみ使用します。この機能を有効にすると、許可することを定義したドメインを除いてインターネットがブロックされるため、注意して使用してください。

ロギング設定には次のものがあります。

- [すべての要求をロギング（Log All Requests）]：コンテンツ、セキュリティなどを問わず、すべてをロギングします。
- [セキュリティ イベントのみロギング（Log Only Security Events）]：セキュリティ ロギングのみをロギングし、ユーザのプライバシーが向上します（個人用のデバイスにローミング クライアントがインストールされている場合に適しています）。
- [要求をロギングしない（Don't Log Any Requests）]：すべてのロギングを無効にします。このオプションを選択すると、レポートの対象となる情報がロギングされないため、このポリシーが適用されたアイデンティティに関するほとんどのレポートが無効になります。

ポリシーの目的を選択したら、[次へ（Next）] をクリックします。このドキュメントでは、[このポリシーの目的は何か（What should this policy do?）] にあるすべてのオプションを選択します。

[次へ（Next）] をクリックすると、選択した項目に応じて、進行状況のメーターと、ポリシーを完全に設定するまでの残りのステップ数が表示されます。これを使用して、必要に応じて任意の部分に変更を加えることができます。

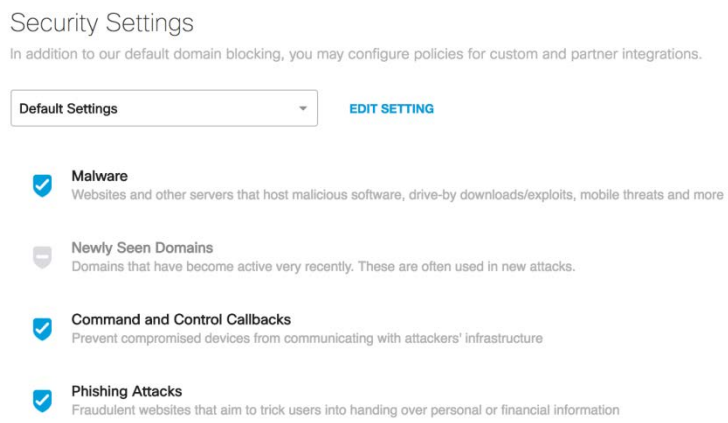


ステップ 3：設定の詳細の設定

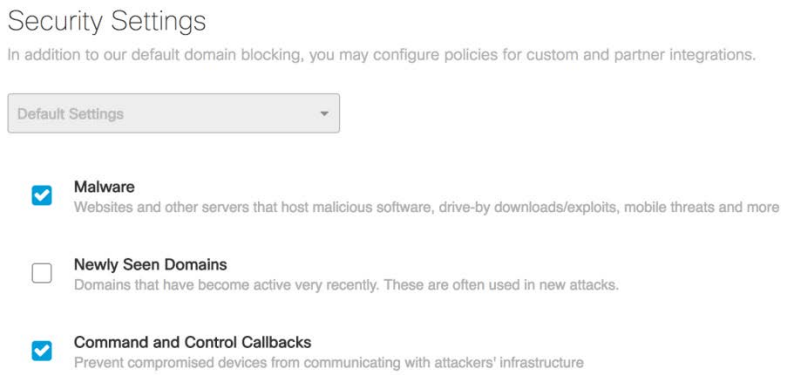
セキュリティ設定

これらの設定により、ブロックされる脅威のセキュリティ タイプが決定されます。カテゴリの内容の詳細については、https://docs.umbrella.com/product/umbrella/understanding-the-security-categories/ を参照してください。

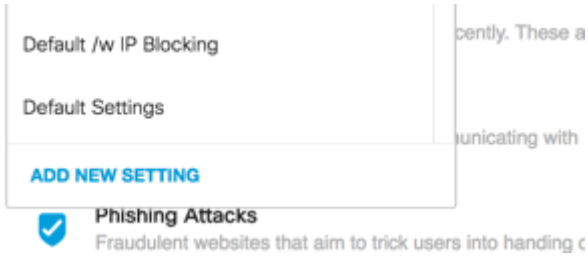
デフォルトでは、チェックマーク付きのシールド アイコンが表示された設定が、すべて有効になっています。



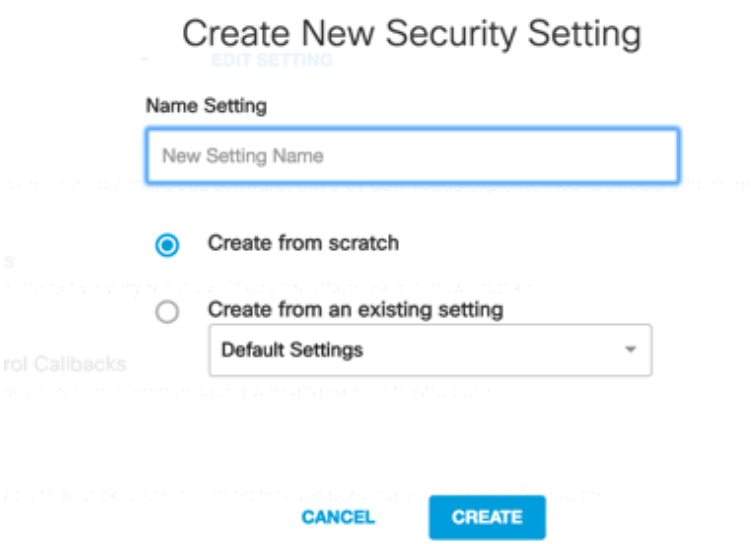
設定を編集するには、[設定の編集（Edit Settings）] をクリックして個々の設定を有効または無効にします。チェックマークが有効または無効に切り替わります。



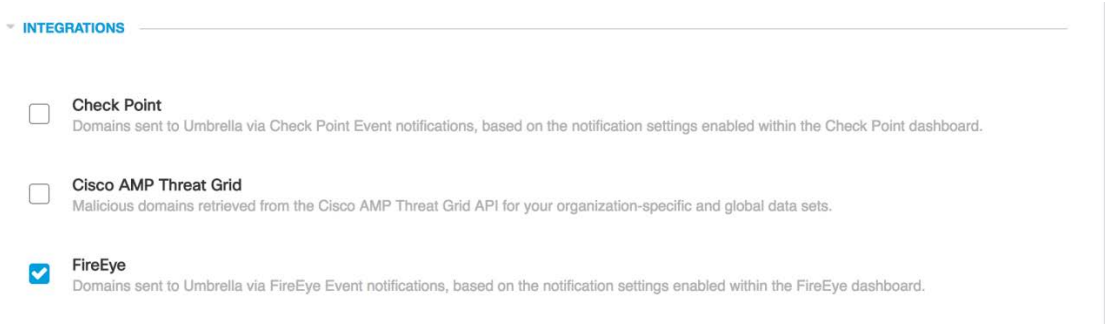
デフォルト設定がすでに選択されています。別の設定を追加または選択したい場合は、ドロップダウン リストを使用します（次の図を参照）。



[新しい設定の追加（Add New Setting）] をクリックすれば、セキュリティ設定セクションのウィンドウを表示せずに、選択した設定を直接編集することもできます。新しい設定を直接追加できるウィンドウが表示されます。



カスタム統合がある場合は、セキュリティ セクションの下部にリストされます。ここでは、自分のアカウントで有効にして設定したカスタム統合だけが表示されます。

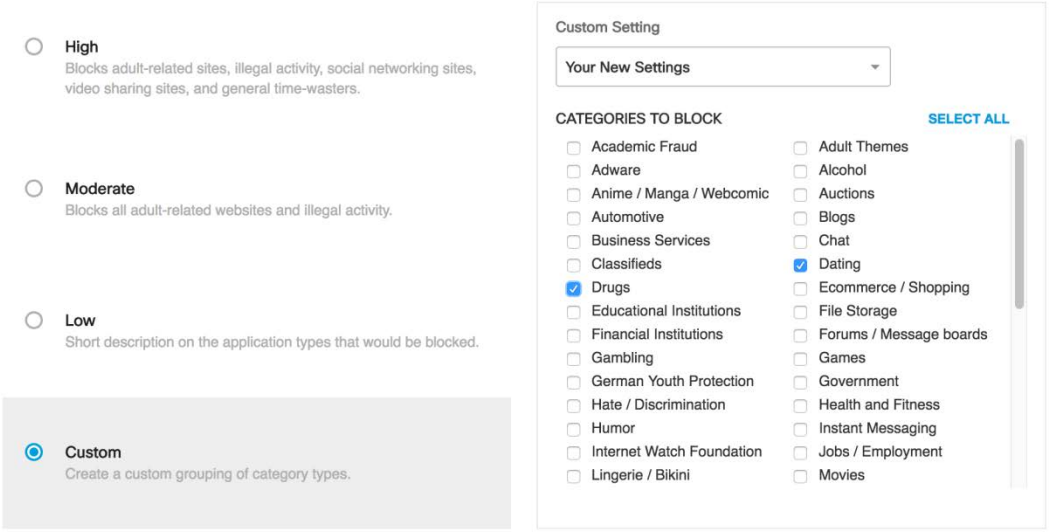


目的の項目を選択したら、[次へ（Next）] をクリックします。

コンテンツの設定

この設定では、ポリシー エディタのステップ 1 で選択したアイデンティティについてブロックするコンテンツ カテゴリを選択できます。デフォルトではブロックされるコンテンツ カテゴリがないため、必要に応じて調整し、設定に適切な名前を付けます。[高（High）]、[中（Moderate）]、[低（Low）] から選択するか、コンテンツ カテゴリのカスタム設定を作成するか、既存のカスタム リストを選択します。

新しい設定を作成するには、[カスタム（Custom）] ドロップダウンを選択し、[新しい設定を作成（Create New Setting）] をクリックして、ウィザード内で定義します。



すべてのカテゴリのリストとそれぞれの詳細については、こちらを参照してください。

セキュリティ設定と同様に、新しいコンテンツ設定の追加と、既存のコンテンツ設定の変更は、ウィザードから直接行うことができます。

接続先リストの適用

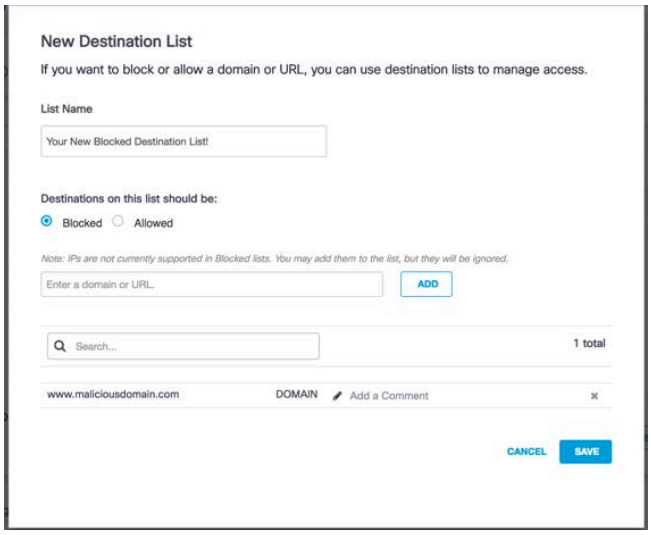
接続先リストにより、明示的にブロックまたは許可するドメインのリストを作成して、フィルタリングをカスタマイズすることができます。各接続先リストは、ブロック リスト（デフォルト）または許可リストのどちらかに設定できます。

許可リスト エントリは、常にブロック リスト エントリよりも優先されます。次に例を示します。

- domain.com をブロックして、許可リストに mail.domain.com を追加した場合は、mail.domain.com が許可されます。
- 許可リストに domain.com を追加して、sub.domain.com をブロックした場合は、sub.domain.com が許可されます。
- セキュリティ設定またはカテゴリ設定によってブロックされていたドメインを許可した場合も、それらの許可リストが優先されます。

*.domain.com が含まれるように、www.domain.com ではなく「domain.com」の形式でドメインを追加することをお勧めします（ワイルドカードは暗黙的）。ただし subdomain.domain.com だけをブロックする場合は、ここでさらに詳細に入力する必要があります。

接続先リストの作成は簡単です。まずリストのタイプを選択し、許可またはブロックするドメインを追加して、リストに名前を付けます。



注：

接続先リストに入力するとリスト ビューに表示されますが、[保存（Save）] をクリックするまでは保存されません。

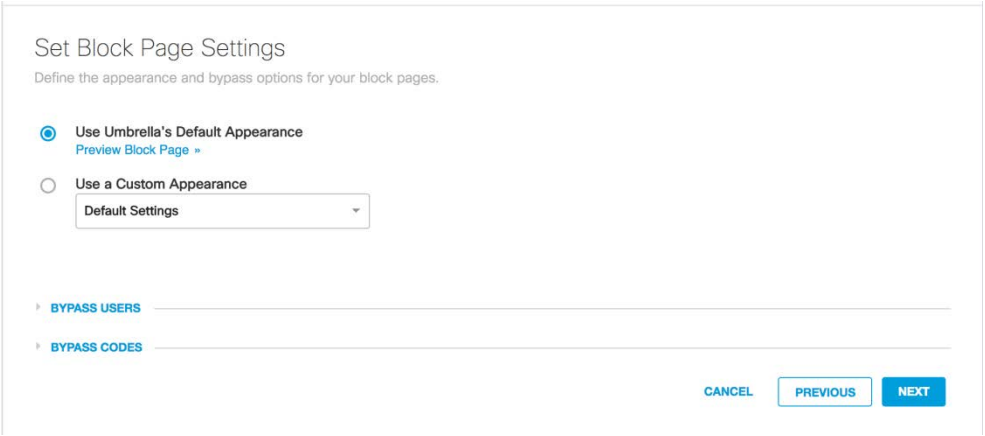
詳細については、接続先リストで接続先を追加/削除するを参照してください。

注：

これらのポリシー設定は、すべて左側のメニューの [ポリシー設定（Policy Settings）] で編集することができます。

ブロック ページ

[ブロック ページの設定（Block Page Settings）] では、ユーザ向けの独自のブロック ページや、必要時にブロック ページをバイパスする方法を設定します。各設定の内容を以下に示します。



- [ブロック ページの設定（Block PageSettings）]：ブロック ページの外観のカスタマイズ、カスタム ドメインへのリダイレクトなどを設定できます。
- [バイパス ユーザ（Bypass Users）]：ログインしてこのポリシーのブロック ページをバイパスできるユーザアクティブにするには、ポリシーで [バイパス ユーザ（Bypass Users）] を**オンにする**必要があります。
- [バイパス コード（BypassCodes）]：このポリシーのブロック ページをバイパスするために使用するコード。アクティブにするには、ポリシーで [バイパス コード（Bypass Codes）] を**オンにする**必要があります（上記を参照）。

ブロック ページ設定

変更を行わない場合は Umbrella のデフォルトの外観を使用できますが、この設定により、ブロック ページをカスタマイズすることもできます。

名前にカーソルを合わせて小さな「編集」ペン アイコンをクリックすることで、既存のブロック ページを編集できます。

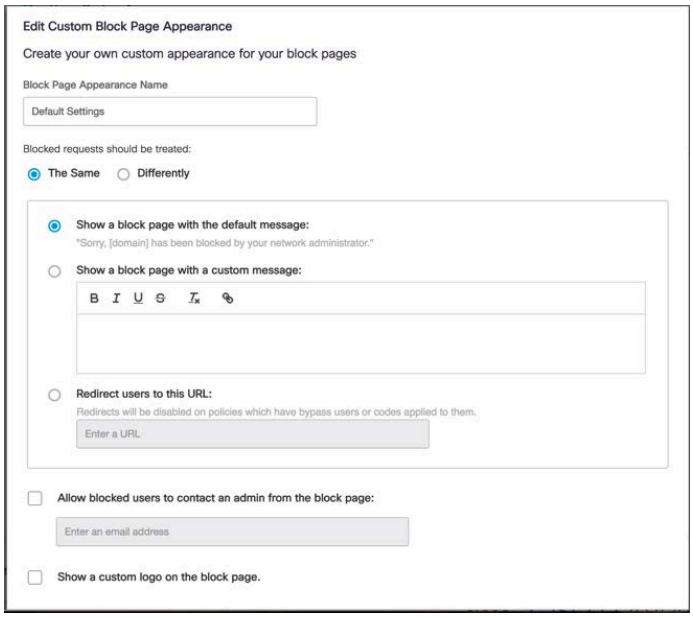
[カスタム外観を使用（Use a Custom Appearance）] を選択して、ドロップダウンから [新しい外観を作成（Create new Appearance）] を選択します。

ページ設定を作成または初めて編集するときには、設定に [企業ブロック ポリシー（Corporate Block Policy）] などの覚えやすい名前を付けてください。

ブロックされた要求の処理方法を同じにするか変更するかを選択して、すべてのブロック ページで汎用のメッセージを使用するか、ブロック ページのタイプごとにメッセージをカスタマイズします。
ブロックはカスタム URL にリダイレクトすることもできます。

カスタム URL にリダイレクトしない場合は、連絡フォームを追加して、ブロックされたユーザが指定された電子メールで管理者に連絡できるようにすることができます。

最後に、ブロック ページの Umbrella ロゴの場所に表示させる、カスタム ロゴをアップロードすることができます。



バイパス ユーザ

バイパス ユーザは（ポリシーに追加された場合）、ログイン後に、選択したタイプのブロック ページをバイパスすることができます。ブロック ページをバイパスするオプションは、ブロック ページが表示されたときに選択できます。ユーザは認証を受けてブロック ページをバイパスできます。このようなクレデンシャルがない場合は、ブロックはその状態で保持されます。
[新規作成（Create New）] をクリックして、新しいバイパス ユーザを作成します。

注：バイパス ユーザとして追加されるためには、ユーザがすでに Umbrella ダッシュボードに追加されていなければなりません。

ユーザを追加するには、[設定（Settings）] > [アカウント（Accounts）] に移動します。

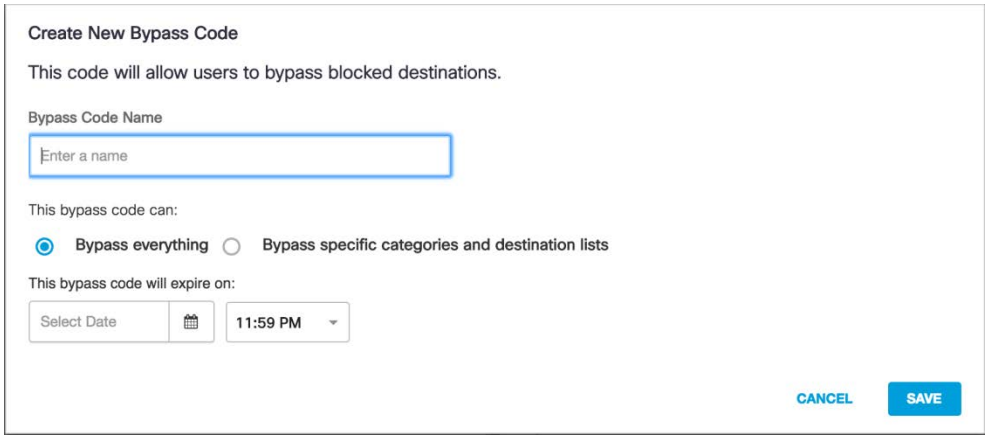
必要に応じて、特定のカテゴリ フィルタまたは接続先リストだけにバイパスが適用されるようにすることができます。バイパス ユーザは、セキュリティ ブロックをバイパスすることはできません。

この場合も、ブロック ページにアイデンティティを誘導するポリシーと同じポリシーにバイパス ユーザが適用されることが重要です。

[バイパス コード(Bypass Codes)]
バイパス コードを作成することで、ブロックされたユーザがブロック ページをバイパスすることが可能になります。バイパス コードは指定された期間にわたって使用できます。

ポリシーに対して有効(チェックマーク付き)にすると、選択したカテゴリまたはドメインをバイパスできます。コードの有効期限を設定しない場合、デフォルトの有効期限は 1 時間です。

この場合も、ブロック ページにアイデンティティを誘導するポリシーと同じポリシーにコードが適用されることが重要です。



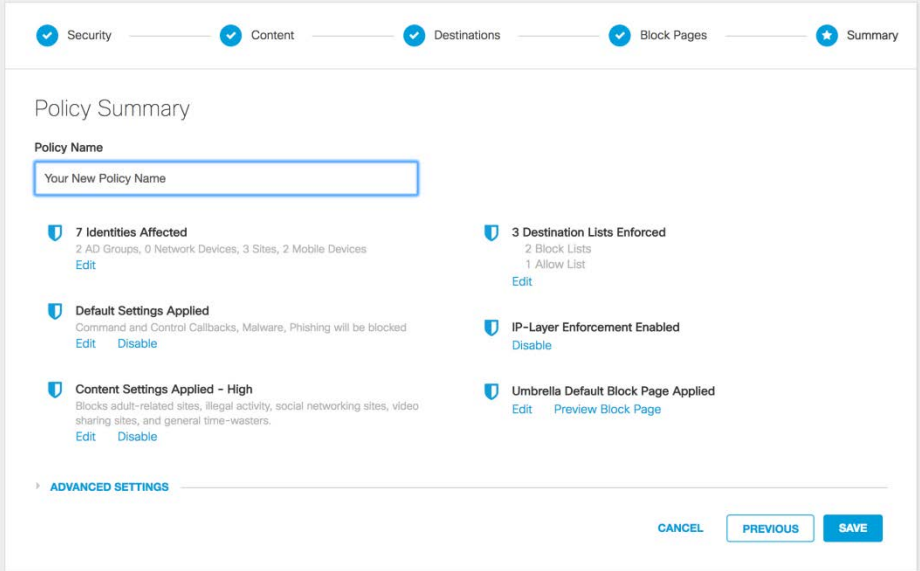
ブロック ページとバイパスを設定したら、[次へ(Next)] をクリックします。

ステップ 4:ポリシーの詳細設定

最後にポリシーのサマリーが表示されます。ここには、ポリシーに対して行ったすべての変更が示されます。何らかの変更を行う場合は、該当する [編集(Edit)] ボタンを

クリックすると、その手順に戻ります。またサマリー画面で機能を直接無効にすることもできます。変更を行ったら、クリックして他の手順をたどることなく、サマリーに直接戻ることができます。

ポリシーは、名前を付けてから保存してください。この画面では、詳細設定を直接変更することもできます。必要な変更を行ったら、[保存（Save）] をクリックします。



以上です。最初のポリシーの設定がすべて完了しました。Umbrella 用にアイデンティティや設定を追加する場合は、ポリシーの調整が必要になることがあります。既存のポリシーを開くと、サマリー画面に直接移動できます。またウィザード全体をやり直さなくても、ステップ間を自由に移動して、必要な変更を直ちに行うことができます。

DNS の接続先を Cisco Umbrella に設定する <**ポリシーのカスタマイズ**> インテリジェント プロキシの有効化

インテリジェント プロキシの有効化

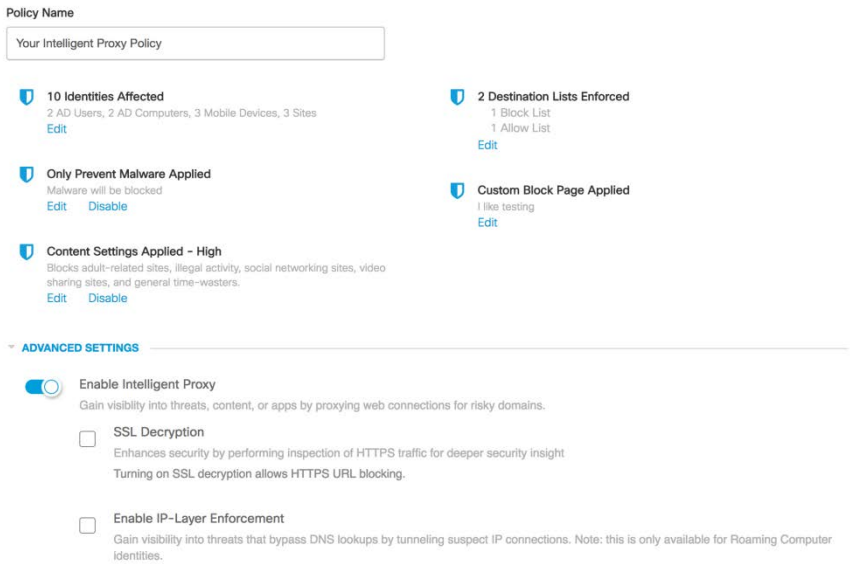
インテリジェント プロキシを有効または無効にする手順は、ウィザードで新しいポリシーを設定する際に制御することができます。すでに設定されている場合は、ポリシー サマリー ページで変更できます。この章では、インテリジェント プロキシを正しく設定する方法を示します。

インテリジェント プロキシとその機能に関する FAQ も含まれています。

ポリシー ウィザード

1. [ポリシー（Policies）] > [ポリシー リスト（Policies List）] に移動し、新しいポリシーを追加するか、既存のポリシーを開きます。

2. 新しいポリシーを作成した場合には [このポリシーの目的は何か（What should this policy do?）] 手順、既存のポリシーを開いた場合にはサマリー画面の [詳細設定（Advanced Settings）] でインテリジェント プロキシを有効にするオプションを利用できます。新しいポリシー設定の最後に変更することもできます。



[詳細設定（Advanced Settings）] の下部を展開すると、セキュリティ設定の下部にインテリジェント プロキシに関するチェックボックスが表示されます。オプションを切り替えれば、既存のセキュリティ設定にインテリジェント プロキシを追加することができます。

有効にしたら、期待したように機能しているかを確認してください。インテリジェント プロキシのテストについては、こちらをクリックしてください。

テスト用に、またはユーザのグループ用にインテリジェント プロキシを無効にするには、オプションをオフにしてそれらの変更を適用します。

ここにはさらに、インテリジェント プロキシの SSL 復号化と IP レイヤ適用の 2 つの機能があります。IP レイヤ適用（ローミング クライアントのアイデンティティのみ）の詳細については、https://docs.umbrella.com/product/umbrella/6-adding-ip-layer-enforcement/ を参照してください。

SSL 復号化の詳細については、https://support.umbrella.com/hc/en-us/articles/231246508-SSL-Decryption-in-the-Intelligent-Proxy を参照してください。

Umbrella インテリジェント プロキシとは何ですか。

インテリジェント プロキシは、要求をインターセプトしてプロキシし、「グレー」ドメインに埋め込まれた悪意のあるファイルを調べる機能です。

特に大規模なユーザ コミュニティがあったり、ファイルのアップロードと共有が可能な Web サイトには、ほとんどのユーザがアクセスしても問題ないコンテンツがある一方で、マルウェアのホスティングの可能性によるリスクも存在します。管理者は「グレー」なドメイン全体へのアクセスをブロックしたくない場合でも、コンピュータに損害を与え、企業データを侵害するようなファイルにアクセスしてほしくはありません。

インテリジェント プロキシはこのギャップを解消するために、既知の問題のないサイトへのアクセスを許可しながら、リスクの可能性があるサイトへのアクセスだけがプロキシされるようにします。プロキシによって、マルウェアをホスティングしている特定の URL をフィルタリングしてブロックしながら、その他の URL へのアクセスを許可できます。

プロキシとは何ですか。

プロキシとは、コンピュータまたはモバイル デバイスとインターネットの間のステップです。インターネット上のコンピュータに対する要求をインターセプトして検査し、問題がない場合にアクセスを許可します。コンピュータまたはモバイル デバイスがアクセスしようとするコンテンツにセキュリティ脅威がある場合は、プロキシがブロックします。それにより、脅威による損害が発生する前に、すばやく簡単に保護が行われます。

インテリジェント プロキシはどのように機能しますか。

通常は、Umbrella DNS リゾルバに DNS 要求を送信すると、悪意のあるサイトかどうか、また接続先リストやコンテンツ設定によってブロックされていないかどうかがチェックされます。ブロックされている場合は、要求に対してブロック ページが返されます。ブロックされていない場合は、ドメインの IP アドレスが返され、そのサイトに直接アクセスできるようになります。

インテリジェント プロキシがあれば、疑わしいコンテンツか、悪意のあるコンテンツをホスティングしている可能性があるサイトに対しては、インテリジェント プロキシの IP アドレスが返されます。そのドメインに対する要求は、クラウド ベースのセキュアなゲートウェイを通じてルーティングされ、悪意のあるコンテンツは、ユーザに送信される前に検出されてブロックされます。

Umbrella のインテリジェント プロキシにはどのような利点がありますか。

従来のプロキシの問題は、インターネットの規模に応じた拡張ができない点にありました。インターネットは日々拡大しており、大量のストリーミング ビデオ フィード、ビデオ会議、Voice over IP などさまざまな形で利用されるため、プロキシ ハードウェアの製造元もそれに備えることができません。かつてはすべてのトラフィックについてプロキシとスキャンが必要であったため、ゲートウェイ プロキシでトラフィックの速度が低下し、ゲートウェイの外部にあるデバイスは保護されていませんでした。

インテリジェント プロキシには、3 つの大きな利点があり、セキュアなだけでなく速度も向上します。

- Umbrella のサービスはクラウド ベースであり、あらゆる量のインターネット トラフィックを処理できるように拡張できます。他のプロキシ サービス（特に完全なプロキシ ソリューション）では速度が低下しますが、Umbrella のサービスではそのようなことはありません。
- ラップトップやモバイル デバイスを持って社内ネットワークを離れる場合でも、インテリジェント プロキシがあればどこにいても、24 時間 365 日保護されます。
- 予測型のインテリジェンスによって、プロキシが必要な対象を特定できるため、すべてのトラフィックをプロキシする必要がありません。悪意があることがわかっているドメインは、DNS サービスによって直ちにブロックされます。問題がないことがわかっているドメインは、DNS サービスによって常に許可されます。グレー リストに含まれるドメインについては、デバイスから送受信される HTTP トラフィックをプロキシすることで、悪意のあるファイルにアクセスしないように保護されます。

インテリジェント プロキシを利用するために Umbrella を再度学習する必要はありますか。

いいえ。ソフトウェアやハードウェアを追加する必要はなく、コストもかかりません。インテリジェント プロキシは 1 つのセキュリティ カテゴリにすぎず、Umbrella ダッシュボードで作成したポリシーの一部として選択できます。一般的にはサマリー画面の詳細設定で、また [このポリシーの目的は何か（What should this policy do?）] セクションでも選択できます。詳細については、このドキュメントの冒頭を参照してください。

インテリジェント プロキシに関心があります。どうすれば使用できますか。

ポリシー内のボタンをクリックして、ポリシー内のアイデンティティに対して有効にするだけです。変更を行う場合は、最初にユーザ ベースの一部に対して行い、互換性を確認することをお勧めします。その後必要に応じて許可リストを拡張します。

有効にした後で、どのように機能をテストできますか。

ラップトップやモバイル デバイスなどのアイデンティティにポリシーを適用したら、テスト サイトに移動します。

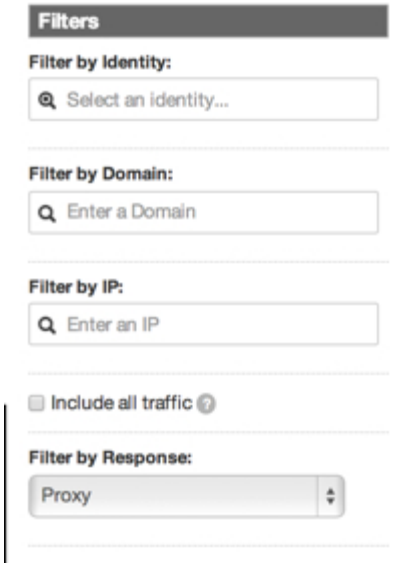
http://proxy.opendnstest.com/

ページの指示に従って、インテリジェント プロキシを使用して他に問題のない Web サイトで特定のイメージをブロックできるか、また Web サイト全体をブロックできるかをテストします。

テスト サイトでインテリジェント プロキシを使用していないことが示された場合は、使用しているアイデンティティに適用されているポリシーで、インテリジェント プロキシが有効になっているかをチェックします。

インテリジェント プロキシを使用した要求のレポートは作成されますか。

作成されます。アクティビティ検索およびその他のレポートに含まれているインテリジェント プロキシのアクティビティに絞り込むことができるフィルタが用意されています。フィルタリングされたトラフィックに限定したフィルタリングが可能です。



インテリジェント プロキシは HTTPS トラフィックを処理できますか。

はい。簡単に設定できますが、さらにいくつかの設定を行うことで、エンド ユーザに不要なエラーが表示されないようにすることができます。詳細については、こちらを参照してください。

インテリジェント プロキシでプロキシされるドメインをリクエストまたは追加することはできますか。

現在、特定のドメインをプロキシの対象とするかどうかは、Umbrella の脅威インテリジェンスに基づいて、Umbrella のセキュリティ研究者が判断しています。ただし近い将来に向けて、ユーザが設定可能な、インテリジェント プロキシを使用する機能を増やす予定です。ご注目ください。

ポリシーのカスタマイズ <インテリジェント プロキシの有効化> Umbrella Policy Tester

Umbrella Policy Tester

Umbrella Policy Tester の概要

Umbrella Policy Tester は、ポリシーが適用されている実際のコンピュータ、ネットワーク、または Cisco Umbrella アイデンティティからテストすることなく、意図したようにポリシーが機能しているかを確認できる、シンプルで使いやすいツールです。アイデンティティとさまざまな接続先に正しい順序でポリシーが適用され、問題なくテスターが実行されていく様子を一度ご覧下さい。

ユーザが以下に説明する機能を使用してブロック ページからフィードバックを送信することを許可した場合、ブロック ページからのフィードバックでは、ブロックされたアイデンティティ、接続先、ブロックしたポリシーが示されるため、それに応じた対応が可能です。

注: Policy Tester では、接続先になっているドメインに対してのみテストが可能です。IP アドレスと CIDR 範囲はサポートされていないため、結果が返されません。

Policy Tester は、Umbrella ダッシュボードの [ポリシー（Policies）] ページの上部にあります。[Policy Tester] をクリックすると開きます。

Policy Tester には基本的な使用方法が記載されており、それだけで使用することができますが、いくつかポイントを示します。テスト対象のアイデンティティと接続先の 2 つのフィールドが必須です。Policy Tester は基本的に、ポリシーの設定に基づいて、選択されたアイデンティティが、定義されている接続先に到達可能かどうかを判定します。特定のアイデンティティが特定の接続先に到達すべきかどうかまたは到達すべきでないかに応じて、得られた結果の理由を理解するための情報が提供されます。

この 2 つのフィールドはどちらも必須です。

アイデンティティを入力すると、入力の予測に基づいた検索が行われます。たとえば「A」と入力すると、「A」が含まれるすべてのアイデンティティのリストが表示されます。

重要:接続先には完全修飾ドメイン名を指定する必要があります。IP アドレスと URL はサポートされていません。

どのアイデンティティが優先されるかを確認する場合は、複数のアイデンティティを入力します。たとえば、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にポリシーが適用されていて、1 つ以上のネットワーク アイデンティティによって保護されている場合は、どのポリシーが有効になるかが明確でないことがあります。Policy Tester では、どのアイデンティティがどのポリシーによって最初にトリガーされるかを判定できます。

必要な 1 つ以上のアイデンティティを選択し、[テストを実行(Run Test)] をクリックすると、結果が表示されます。

[リセット(Reset)] をクリックすると、アイデンティティと接続先の両方のフィールドがクリアされます。

Policy Tester の結果

テストの結果には次の情報が含まれています。

- [トリガーされたアイデンティティ(TriggeredIdentity)]:トリガーされたアイデンティティを示します。これは複数のアイデンティティが指定されている場合に重要です。
- [接続先(Destination)]:テスト対象とする接続先
- [結果(Result)]:接続先が許可されたかブロックされたか、またブロックされた理由を示します。理由としては、セキュリティ設定、カテゴリ設定、ドメイン リストなどがあります。またブロックのタイプが記録されます。さらに、設定の実際の名前やドメイン リストが示されます。

- [接続先リスト/セキュリティ設定/カテゴリ設定（Destination List/Security Settings/Category Settings）]：ブロックタイプに応じて、適用された設定/リストの名前が示されます。一致がない場合、この情報は表示されません。
- [分類（Categorization）]：Umbrellaが接続先をどのように分類したかを示します。カテゴリは、接続先がブロックされたかどうかに関わらず表示されます。ここで接続先がどのように分類されているかを確認することで、そのカテゴリをブロック対象とするかを決定できるため、この情報は役に立ちます。一致がない場合、この情報は表示されません。
- [適用されたポリシー（PolicyApplied）]：適用されたポリシーを示します。適用されたポリシーは、下に赤色で強調表示されます。デフォルト ポリシー意外に適用されたポリシーがない場合は、すべてに適用されるデフォルト ポリシーが表示されます。

さらに、結果に関する説明が表示されます。次に例を示します。

「このアイデンティティは 2 つのポリシーで見つかりました。その中で「Your First Policy」が最上位のポリシーであるため、アイデンティティに適用されました。このアイデンティティに低いランクのポリシーを適用するには、ポリシーをクリックして「Your First Policy」よりも上にドラッグします。」

適用されたポリシーは強調表示されます。接続先がブロックされた場合、ポリシーは赤色で強調表示され、接続先が許可された場合、ポリシーは緑色で強調表示されます。

重要：接続先には完全修飾ドメイン名を指定する必要があります。IP アドレスと URL はサポートされていません。

Policy Tester の制限

限られた状況で、特定の接続先について、Policy Tester が正確な情報を返さない、またはまったく情報を返さない場合があります。詳細については、Umbrella Policy Tester の制限事項を参照してください。

インテリジェント プロキシの有効化 < **Umbrella Policy Tester** > ポリシーの優先順位

ポリシーの優先順位

Umbrella ダッシュボードのポリシーの順序：ポリシーの優先順位

Cisco Umbrella ダッシュボードには、アイデンティティ全体の設定を管理するための強力なツールが用意されています。Policy Editor は、アイデンティティごとのフィルタリングとセキュリティ設定をカスタマイズできるツールです。任意のアイデンティティを任意のポリシーに追加することもできますが、エンド ユーザに適用される設定は、ポリシーの優先順位ルールに基づいて決定されます。

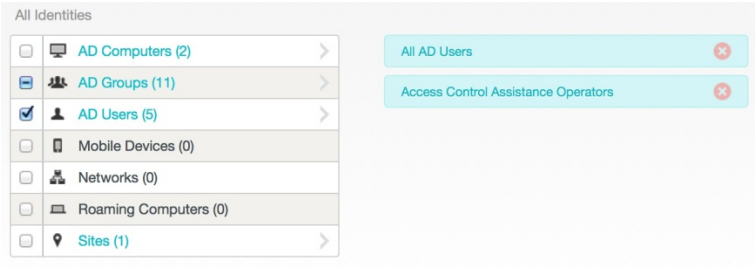
一般的に、エンド ユーザに追加されるリストの最上位のポリシーが適用されます。ただしこれは、Umbrella ローミング クライアントや Active Directory（AD）アイデンティティなど、ユーザが複数のアイデンティティを持っている場合には複雑になります。

アイデンティティがどのカスタム ポリシーにも一致しない場合、アイデンティティはデフォルト ポリシーに適用されます。特定のアイデンティティがどのポリシーに一致するかを確認するには、Umbrella Policy Tester（ダッシュボードのポリシー エディタの上にある）の記事を参照してください。

ポリシーの優先順位：アイデンティティ

どのアイデンティティがどのポリシーに属するかを選択する際には、追加されたアイデンティティのリストが、Identity Chooser の右側に表示されます。すべてのカテゴリ（[AD ユーザ（AD Users）]、[AD グループ（AD Groups）]、[ネットワーク（Networks）]など）を選択した場合は、チェックマークが表示されます。一部のカテゴリ（特定の[AD ユーザ（AD Users）]、[AD グループ（AD Groups）]、[ローミング クライアント（Roaming Client）] など）だけを選択した場合は、ダッシュが表示されます。

ネストされたアイデンティティ セットが表示され、そのチェックマークがグレー表示されている場合、サブグループを変更するには、1 レベル上に青色のチェックマークが表示されていないことを確認します。



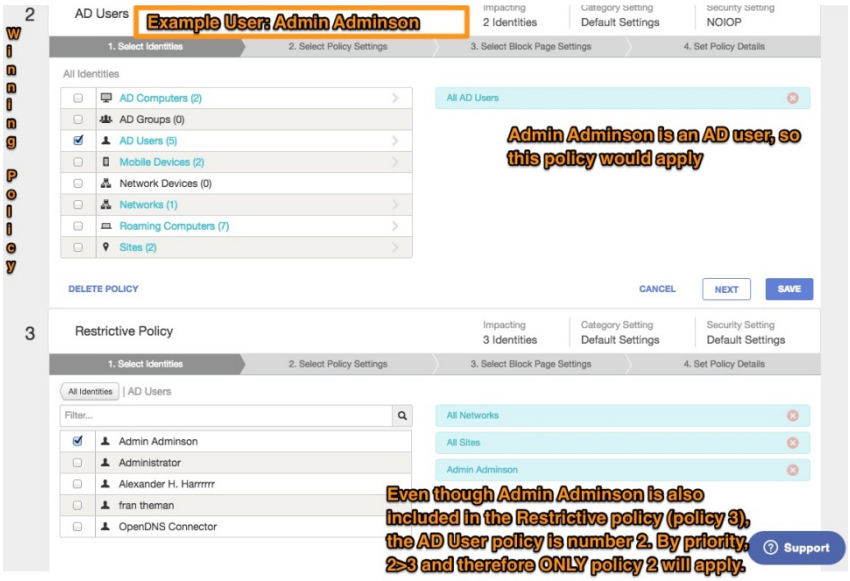
各ポリシーでは、任意の組み合わせのアイデンティティを選択することができます。

たとえば Active Directory 内のユーザ「Joe」は、異なる複数のポリシーに 1 人のユーザとして追加することも、「すべての AD ユーザ」が対象のポリシーに含めることもできます。

「Joe」は複数のポリシーに含めることができるため、それらのポリシーが「Joe」に適用される順序が重要になります。一般的にポリシーは追加されていくものであるという誤解があり、「YouTube ポリシー」と「Facebook ポリシー」を作成してアイデンティティを追加すると、チェックされたすべてのアイデンティティがこれらのサイトにアクセスできると考えられています。それは誤りです。

ポリシーは「最初の一致」に基づいて適用されるもので、上位から下位へ実行順序に従ったランク（各ポリシーの左に示される数字）の順に適用されます。したがって、ユーザのアイデンティティに一致する最高ランクのポリシーが適用され、それ以下のすべてのランクの一致は無視されます。

以下に示す例では、AD ユーザであるサンプル アイデンティティ「Admin Adminson」を設定しています。ここでは 2 つのポリシーがあります。すべての AD ユーザ（AD ユーザ）に適用されるランク 2 のポリシーと、特定のユーザ「Admin Adminson」だけに適用される制限的な 2 番目のポリシー（ランク 3）です。AD ユーザ ポリシーは、2 つのポリシーのうち上位のランクにあるポリシーであるため、実行順序で最初に一致します。制限的なポリシーの一致は無視されます。



上の例の制限的なポリシーの目的は、「Admin Adminson」のアイデンティティに他のユーザよりも厳格なフィルタリングを設定することにありますが、正しい順序が設定されませんでした。これは「ローミング クライアント」と「ネットワーク」にも適用されます。このユーザに特定のポリシーを適用するには、ポリシーの順序を更新する必要があります。この場合は、制限的なポリシーを AD ユーザ ポリシーよりも上位に移動させる必要があります。ポリシーの順序はどのように変更できるでしょうか。次のセクションを参照してください。

ポリシー順序の設定

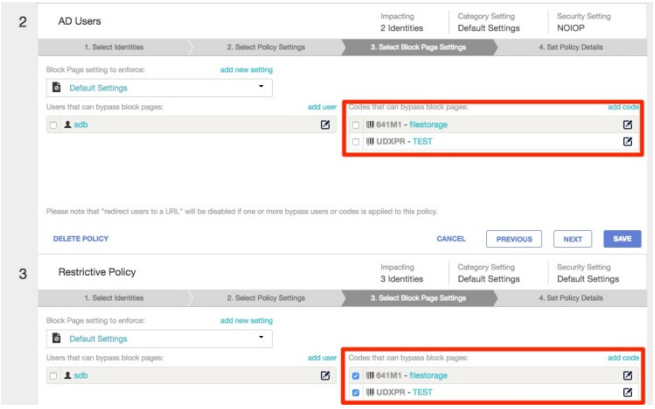
ポリシー順序は、各ポリシー バーの左側にある「ハンドル」を使用してドラッグ アンドドロップによって変更できます（以下のアニメーションを参照）。それにより、ポリシーの配列を目的の順序に変更することができます。

同じポリシー内のアイデンティティの優先順位

複数のアイデンティティが同じポリシーを共有する場合に、どのアイデンティティが最終一致のアイデンティティとして記録されるかの詳細については、ポリシー ステータスの識別ガイドを参照してください。たとえば、登録済みのネットワーク上のユーザが、Umbrella ローミング クライアントもインストールしている場合、または AD コンピュータ、AD ユーザ、および内部ネットワークがそのユーザのネットワークに適用されている場合、どちらがレポートに適用されるでしょうか。

ポリシーとブロック ページのバイパス（BPB）

ポリシーの優先順位は、バイパス コードとバイパス ユーザの使用にも影響します。BPB コードとユーザはポリシーごとに有効にするため、バイパス コードが機能しない場合、または「Admin」バイパス リンクが表示されない場合には、コード/ユーザがポリシーに対して有効になっていることを確認します（以下のスクリーンショットでは、コードの例は有効になっていません）。コードまたはユーザを有効にするには、コードまたはユーザの横にあるチェックボックスをオンにして、ポリシーを保存します。ユーザに目的のポリシーが適用されていることを確認するには、Umbrella Policy Tester（ダッシュボードのポリシー エディタの上にある）を使用して、目的のポリシーでコードがアクティブになるように設定していることを確認します。



Policy Tester を使用した確認

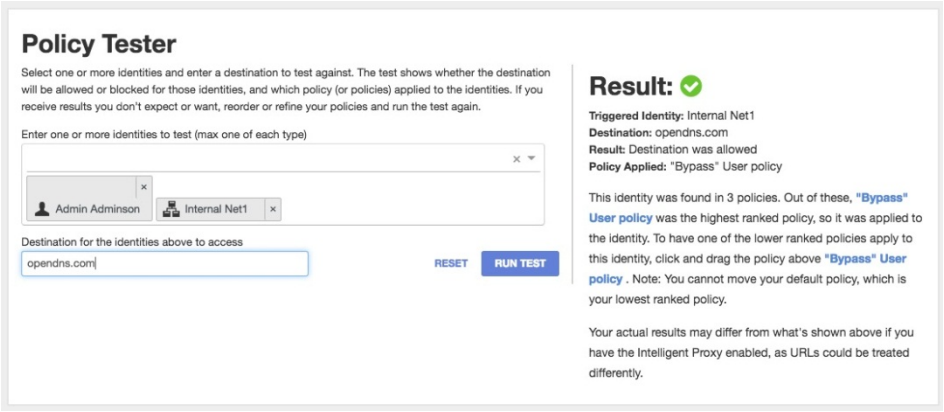
ポリシーを設定したら、実環境でのテストの前に、ダッシュボードに組み込まれている Policy Tester を使用して、ポリシーの適用をテストします。詳細については、Umbrella Policy Tester のガイドを参照してください。

次に Policy Tester の使用例を示します。

ステップ 1:対象とするアイデンティティを入力します。たとえば、AD ユーザと AD コンピュータ(VA と AD の統合を使用している場合)、内部ネットワーク、ローミングクライアント、パブリック ネットワークなどです。

ステップ 2:テスト対象のドメインを入力します。

ステップ 3:[テストの実行(Run Test)] をクリックして結果を確認します。どのポリシーが適用され、またどのポリシーが一致しながらポリシー ランクが下位であったために適用されなかったかが示されます。



Umbrella Policy Tester <**ポリシーの優先順位**> Cisco Umbrella のお客様 FAQ

Umbrella の委任管理

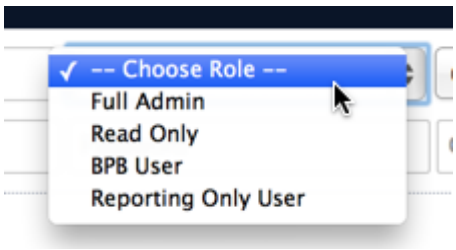
委任管理は、Umbrella ダッシュボードの特定の部分へのアクセスを管理する機能です。組織のニーズとダッシュボードで必要なアクセス レベルによって決定される、ダッシュボードへのアクセスに関連するロールを効果的に管理します。

委任管理の設定

委任管理は 2 つのシンプルなステップで設定できます。最初に適切なデフォルトのロールを選択するか、新しいロールを作成し、次にそのロールをユーザに割り当てます。委任管理は、[設定（Settings）] > [委任管理（Delegated Administration）] のダッシュボードから設定できます。

ステップ 1：デフォルトのロールを選択する、または新しいロールを作成する

デフォルトのロールは次のとおりです。

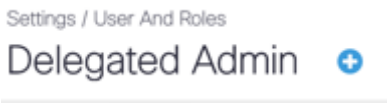


デフォルトでは 4 つのロールが用意されています。

- [完全な管理（FullAdmin）]：新しいロールの作成と割り当てを含め、Umbrella 内のすべてにアクセスできます。
- [BPB ユーザ（BPBUser）]：通常のユーザがページのバイパスを必要とする場合に使用します。詳細についてはこちらをクリックしてください。
- [レポート専用ユーザ（Reporting Onlyuser）]：レポートの表示と実行だけが可能なユーザ。詳細についてはこちらをクリックしてください。
- [読み取り専用ユーザ（Read Onlyuser）]：ダッシュボードのレイアウトを表示できるが変更することはできないユーザ。このユーザは、その他すべてのユーザの全レポートを表示できます。

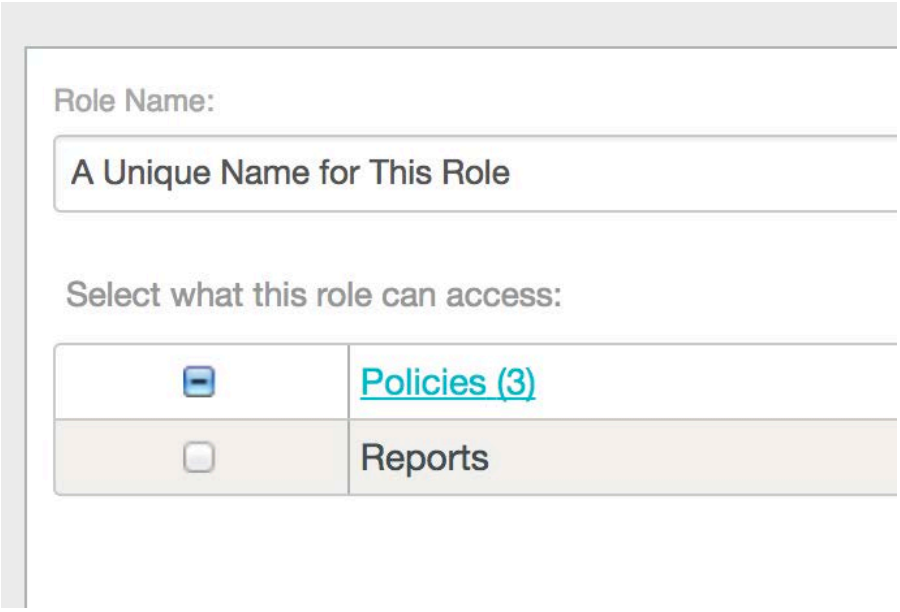
委任管理を利用するには、管理ユーザ固有のロールを作成します。

[設定（Settings）] > [委任管理（Delegated Administration）] で、「追加」ボタン（[+] 記号）をクリックします。



ロールにわかりやすい名前を付けます。

次に、新しいロールがアクセスして管理できるダッシュボードの部分を選択します。2 つの主要なセクション、[ポリシー（Policies）] と [レポート（Reports）] があります。



[ポリシー（Policies）] は 3 つの管理サブロールに分割されます。

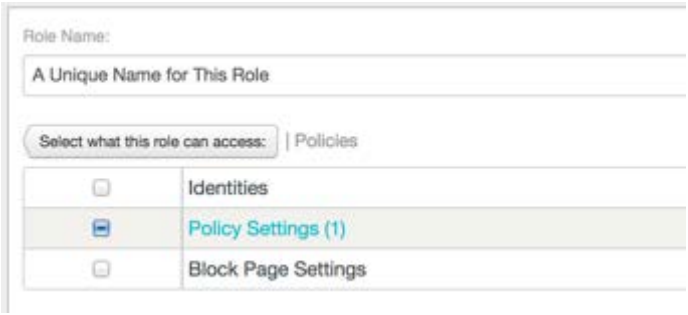
1. アイデンティティ
2. ポリシー設定
   a. ドメイン リスト
3. ブロック ページ設定

[ポリシー設定（Policy Settings）] には、ドメイン リストだけを管理するサブポリシー設定があります。

- [レポート（Reports）]は、ダッシュボードの [レポート（Reports）] セクションのすべての機能を管理します。これが設定されたロールでは、新しいレポートの作成、ブックマークされたレポートの実行、レポートのエクスポートを行うことができます。ただし単独で選択した場合は、ダッシュボードのその他の部分は使用できません。このロールは、管理職や、特定の情報を必要とする部門に適しています。
- [ポリシー（Policies）] では、すべてのアイデンティティ、ポリシー設定、ブロックページ設定を管理でき、またポリシーの追加、削除、および変更、さらにアイデンティティへのポリシー適用が可能です。ポリシーを管理するロールは、ネットワークでの日常の Umbrella ポリシーの導入および管理を担当する、上級ヘルプデスク管理者に適しています。ただしこの制限的なロールでは、ダッシュボード内の他のユーザの管理、ロールの追加または変更、ダッシュボードの [システム設定（System Settings）] 下のその他の機能の追加または変更などはできません。

ポリシーの最上位のチェックボックスをオンにした場合には、すべてのサブロールが含まれます。[ポリシー（Policies）] リンクをドリル ダウンすると、特定のサブロールを選択できます。

[ポリシー（Policies）] には 3 つのサブロール設定があります。



- [アイデンティティ（Identities）] では、[ローミング コンピュータ（Roaming Computers）]、[ネットワーク（Networks）]、[モバイル（Mobile）]、[内部ネットワーク（Internal Networks）] など、ダッシュボード左側のメニュー ペインの [アイデンティティ（Identities）] にあるすべてのアイデンティティを管理します。このロールでは、これらのアイデンティティの変更、名前変更、または削除、さ

らに新しいアイデンティティの作成が可能です。ただしこのロールを単独で選択した場合は、新しく作成したアイデンティティにポリシーを割り当てることはできません。このサブロールは、ネットワークでコンピュータを最初にオンラインにする際に、Umbrella で新しいデバイスをプロビジョニングする場合に適しています。

- [ポリシー設定（Policy Settings）] ロールでは、ダッシュボードの左側のメニュー ペインにある [ポリシー設定（Policy Settings）] のすべての設定を管理できます。このロールでは、コンテンツ設定、セキュリティ設定、およびドメイン リストの変更、名前変更、または削除が可能です。ただしこのロールを単独で選択した場合は、追加されたアイデンティティに対するポリシー設定の割り当てを変更することはできません。このサブロールは、グローバル許可リストまたはグローバル ブロック リストを更新したり、セキュリティ設定を変更したりして、ヘルプデスクに対する予期しない要求に即座に対応するのに適しています。[ポリシー設定（Policy Settings）] にはもう 1 つ、[ドメイン リスト（Domain List）] ロールの設定があります。
- [ドメイン リスト（Domain List）]* ロール（[ポリシー設定（Policy Settings）] の下）では、既存のドメイン リスト内のドメインを追加または削除できます。このロールでは複数のドメイン リストを管理することができます。一般的にこのロールは、Umbrella の従来の管理者がいない場合に、単一のドメインへの一時的なアクセスを必要とするヘルプデスク ユーザに適用されます。また、標的型の攻撃または侵害がある場合に個々のドメインをブロックする、セキュリティ責任者に適用することもできます。

リマインダ：グローバル許可リストまたはグローバル ブロック リストのいずれかを含む [ドメイン リスト（Domain List）] ロールを適用すると、組織全体でドメインを許可またはブロックできます。

- [ブロック ページ設定（Block Page Settings）] ロールでは、ダッシュボード左側のメニュー ペインにある [ブロック ページ設定（Block Page Settings）] で、すべての設定を管理できます。このロールでは、ブロック ページの外観変更、ブロック ページ ユーザの追加、変更、または削除、ブロック ページ バイパス コードの追加、変更、または削除が可能です。ただしこのロールを単独で選択した場合は、ブロック ページ ユーザに割り当てるユーザ アカウントを追加することはできません。このサブロールは、ヘルプデスク チームの一員として、エンド ユーザのためにブロック ページ バイパス コードを更新するユーザに適しています。

注:

アイデンティティのプロビジョニングが可能でポリシーの管理ができないロールの場合は、ポリシー実行矢印(ポリシー セクションにある下向き矢印)に従って、「汎用的な」ポリシーが正しい順序で配列されていることを確認してください。たとえば、アイデンティティ ロールを持つユーザが新しいローミング コンピュータだけをプロビジョニングした場合は、すべてのローミング クライアントが階層の上位にあるポリシーに対して選択されていないかぎり、そのローミング コンピュータはデフォルト ポリシーを受け取ります。

ステップ 2:ユーザにロールを割り当てる

ステップ 2a.必要に応じて新しいユーザを作成する

委任管理者が Umbrella ダッシュボードにログインするためのアカウントを持っていない場合は、[設定(Settings)] > [アカウント(Accounts)] でアカウントを作成する必要があります。アカウントの作成時に、ユーザにロールを割り当てることができます。

ステップ 2b.ユーザに新しいロールを割り当てる

この手順はシンプルです。新しく作成したロールは、[ロールの選択(Choose Role)] ドロップダウン メニューのオプションとして選択できます。

ステップ 2c.ユーザにパスワードを割り当てる

ユーザ自身は、[アカウント(Accounts)] セクションにアクセスして、パスワードなど自分の情報を変更することはできません。この段階で割り当てられるパスワードは、委任管理者ユーザが後で変更できないため、一時的なパスワードであってはなりません。

ステップ 2d.委任管理者ユーザがログインする場合

ユーザを委任管理者に設定すると、ユーザのダッシュボードは、割り当てられた要素だけに自動的に制限されます。この場合ユーザのダッシュボードは、見慣れた画面より若干小さくなります。制限された部分がグレー表示ではなくまったく表示されなくなるため、その部分の存在が認識されません。