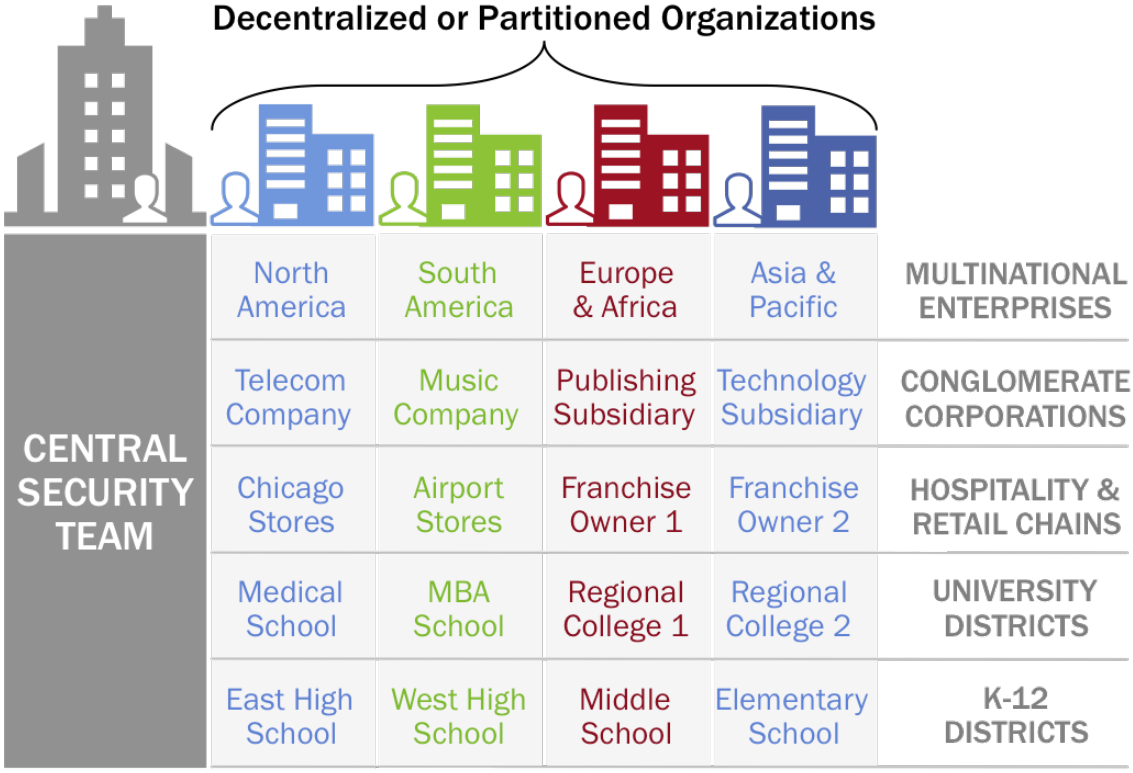
Cisco Umbrella Multi-Org Console の概要

はじめに

Cisco Umbrella Multi-Org Console により、管理者は Umbrella ダッシュボードの 1 つのインスタンス内で、複数の組織（Org）を管理できます。各組織は独立してそれぞれ固有の Umbrella ダッシュボードを使用しますが、組織間で共有できる設定もあるため、管理がシンプルになっています。また共有レポートにより、グローバル管理者は必要な処置を効率的に決定することができます。各「サブ組織」内では、それぞれの Umbrella ダッシュボードだけにアクセスできるローカル管理ユーザを設定できます。

Multi-Org Console は、広範に分散されながら、共通の IT グループまたはネットワーク セキュリティ チームを共有している組織に適しています。例としては、複数の物理的な拠点を持ちながらも、それぞれの拠点がネットワークとして接続されていない大学や、複数の事業部門を展開する一方で、全体的な IT 部門がセキュリティを管理している企業などが挙げられます。Multi-Org Console は、複数の Active Directory（AD）ドメイン（AD フォレスト内のドメイン、または論理的に分割されたドメイン）が存在するネットワークにも適しています。Umbrella の個々のダッシュボードでは単一のドメインだけがサポートされていますが、Multi-Org Console では、複数のドメインまたは論理的に分割されたネットワーク セグメントを一度に表示し、管理できます。

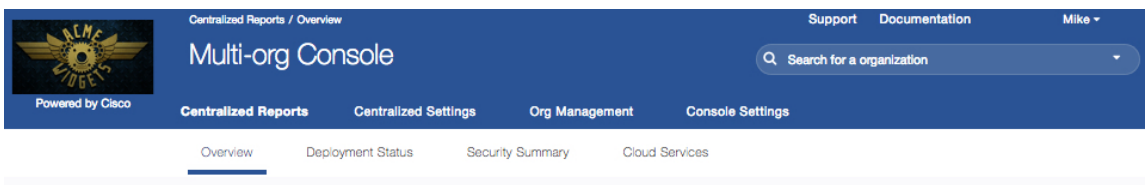
Multi-Org Console は、一元化されたセキュリティ チームが、分割されたあらゆる領域のコンプライアンスを確保しているタイプの組織に最適です。



Multi-Org Console では設定の共有が可能であるため、1 つの接続先リストまたは一連のセキュリティ設定を汎用的に適用することができます。グローバル レポートによって、対処が必要なセキュリティ インシデントをすばやく確認でき、グローバル管理者は任意の社内用ソフトウェア プロビジョニング ツールを使用して、Umbrella ローミング クライアントをすばやく導入することができます。

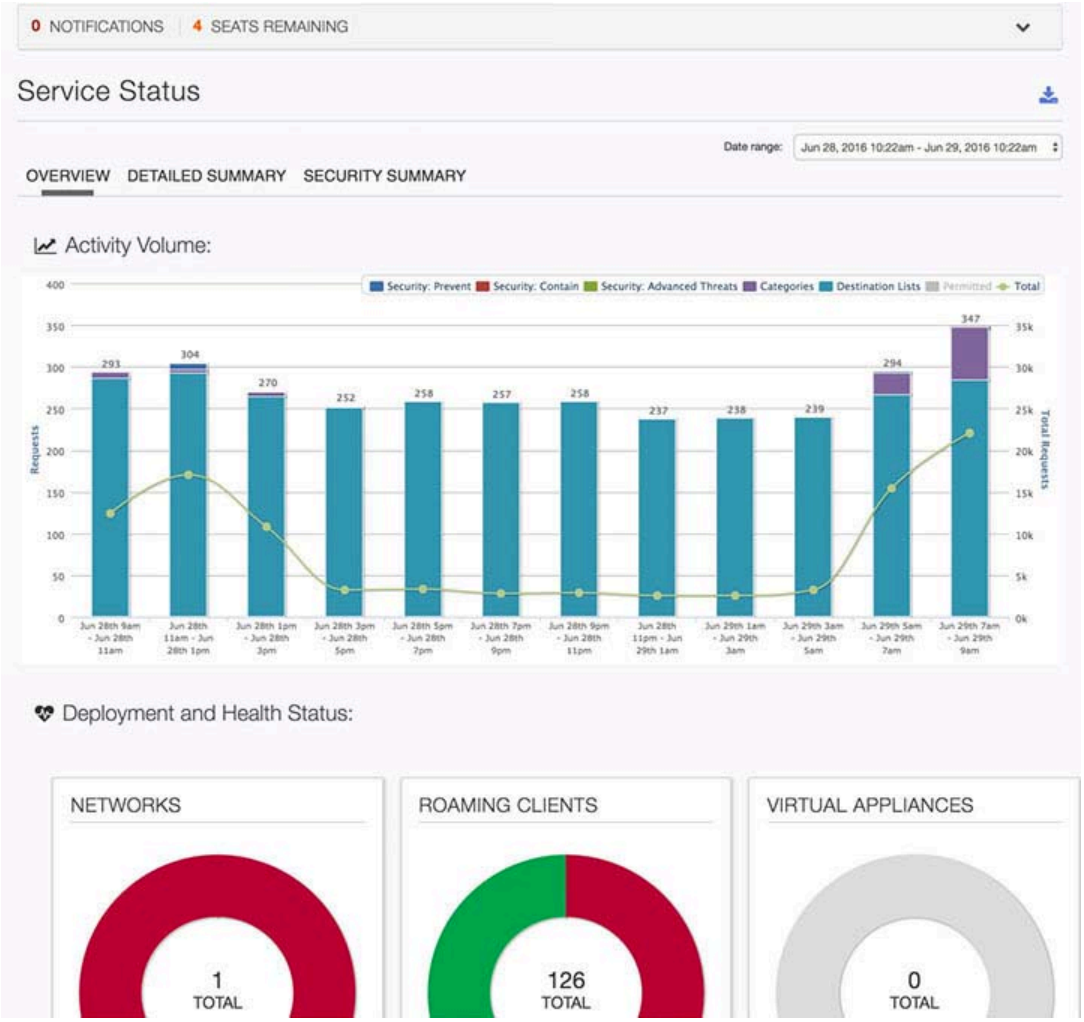
Multi-Org Console では、Umbrella の全シート（またはユーザ）を、グローバル組織内の個々の部署に割り当てることが可能です。そのため、企業のある部署が成長している場合には、その部署に適切なレベルのライセンスを動的に割り当てることができます。

Multi-Org Console は、[集中型レポート（Centralized Reports）]、[集中型設定（Centralized Settings）]、[組織管理（Org Management）]、[コンソール設定（Console Settings）] というコンポーネントで構成されています。



集中型レポート

集中型レポートは、組織全体を一括管理できる画面です。環境の状態をすばやく評価し、組織全体のセキュリティ アクティビティの量を把握し、注意が必要な問題を迅速に特定することができます。このトップ レベルのレポートで組織内の問題の評価と優先順位付けを行うことで、注意を要する問題をドリル ダウンし、その結果、必要に応じてポリシーの変更、感染したワークステーションの修復、ネットワークの変更、ソフトウェアの再導入などを行うことが可能になります。



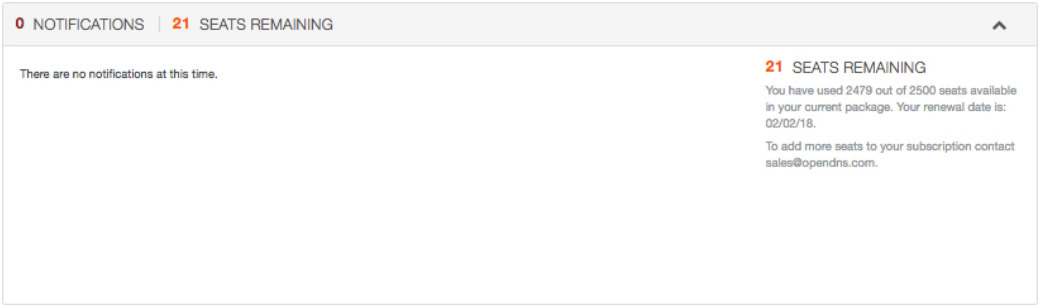
使用可能な集中型レポートは、次のとおりです。

- [概要（Overview）]：すべての顧客が利用できる 2 つの主要な機能である、[アクティビティ ボリューム（Activity Volume）] と [導入/ヘルス ステータス（Deployment and Health Status）] について、概要のスナップショットが得られます。
- [導入ステータス（Deployment Status）]：ネットワーク、Umbrella ローミング クライアント、およびカスタマー ベースの VA の合計数の概要が得られます。
- [セキュリティ サマリー（Security Summary）]：すべての顧客のトラフィックとセキュリティ イベントの概要が得られます。
- **[クラウド サービス（Cloud Services）]：このレポートでは、カスタマー ベース全体について、DNS トラフィックと既知のクラウド サービスの Umbrella リストを照合することで、クラウド ベースの SaaS サービスの使用率が示されます。それによって、シャドー IT や、未承認のツールの使用によるセキュリティ脅威の発生に対応するとともに、クラウド サービスのユーザのニーズに応じたソリューションの販売も可能になります。

Multi-org Message Center

集中型レポートの上部には、Umbrella の Multi-org Message Center があります。新機能の発表や定期メンテナンスに関する情報など、Umbrella からの通知が表示されます。

1. 右上隅の**展開**アイコンをクリックすると、Message Center が開きます。



集中型設定

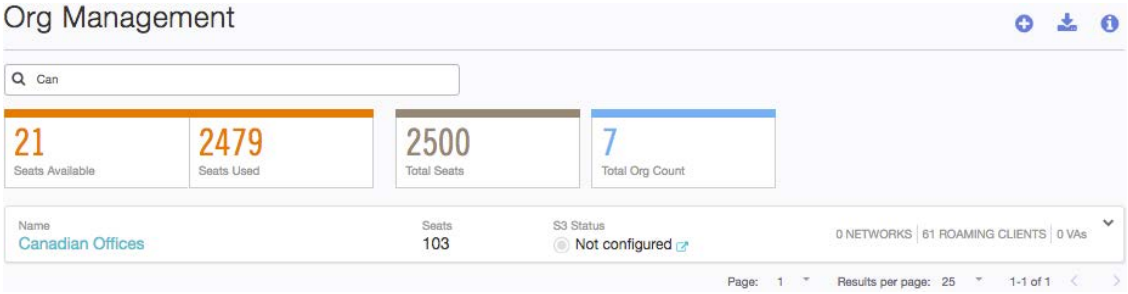
集中型設定は、複数の組織間で共有されるポリシー設定です。集中型設定には、[接続先リスト（Destination Lists）]、[ブロック ページ（Block Pages）]、[カテゴリ設定（Category Settings）]、[セキュリティ設定（Security Settings）]、[カスタム統合（Custom Integrations）] があります。集中型設定の詳細については、集中型設定を参照してください。

組織管理

[組織管理（Org Management）] を選択すると、組織管理の概要が表示されます。このページでは、新しいシートのプロビジョニングや既存の組織の変更が可能で、全組織の概要を表示することもできます。ここでは、Umbrella から購入したシート数、すでに使用しているシート数、使用可能なシート数、組織数なども確認できます。

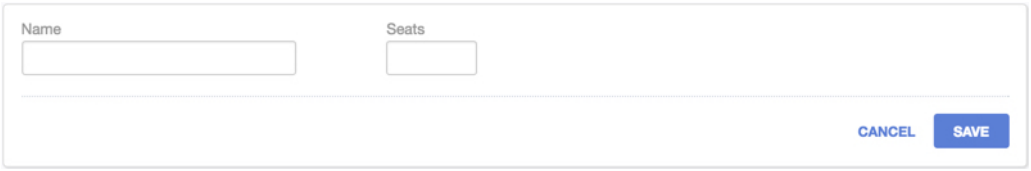
ページの右側には、コンソール内の組織に関する一般的な情報を .CSV 形式のファイルにエクスポートできるボタンがあります。この情報には、フィンガープリントと orgID、Umbrella ローミング クライアントのインストールに必要なコマンドなども含まれます。

また入力予測に基づく検索も利用できます。特定の組織を探す場合は、検索フィールドに組織名を入力すると、関心のある組織だけが表示されます。



最初の組織または新しい組織の追加

1. [組織管理（Org Management）] に移動し、[+]（**追加**）アイコンをクリックします。
2. 最初に、組織に割り当てる組織名とシート数を入力します。シート数は、組織の個々のダッシュボードでプロビジョニングに使用できます。

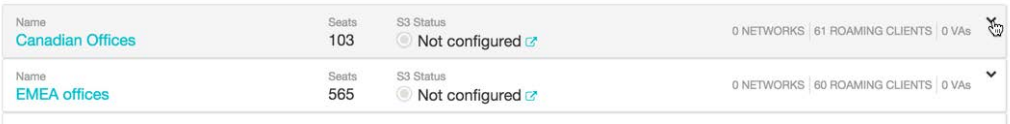


3. [保存（Save）] をクリックして変更を確定すると、新しい組織が表示されます。

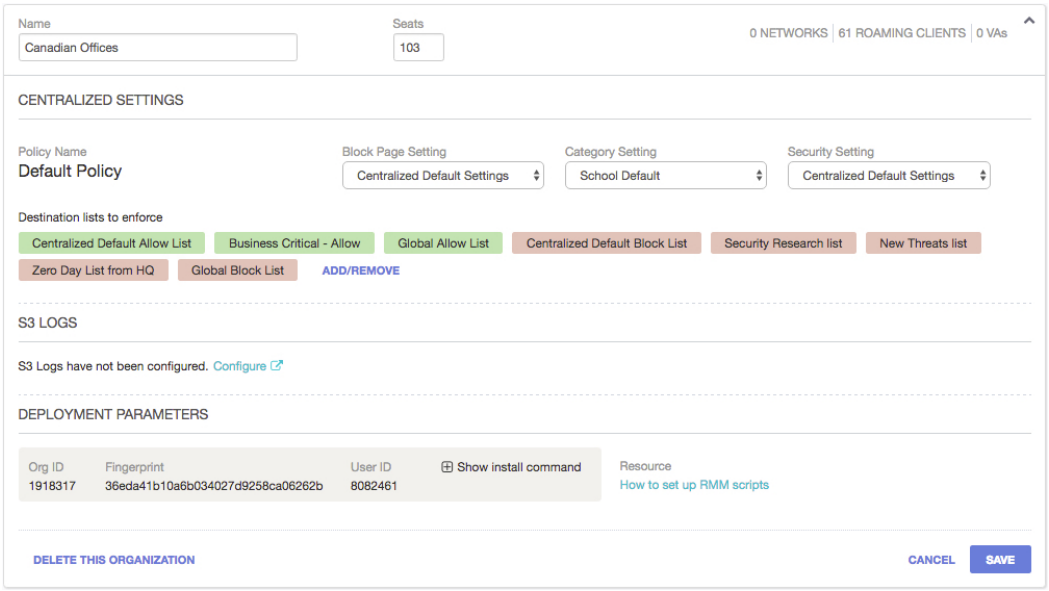
組織名をクリックすると、個々の組織の Umbrella ダッシュボードが新しいタブで開きます。

既存の組織の管理

1. **展開**アイコンをクリックすると、新しく設定した組織に関する情報が表示されます。顧客名をクリックすると、顧客の Umbrella ダッシュボードが表示されます。



展開すると、組織に関する基本情報を確認できるほか、[集中型設定（Centralized Settings）] を設定したり、組織に適用されたデフォルト ポリシーを表示したり、Umbrella ローミング クライアントの導入パラメータをすばやく取得したりできます。



2. 必要に応じて組織名とシート数を更新します。

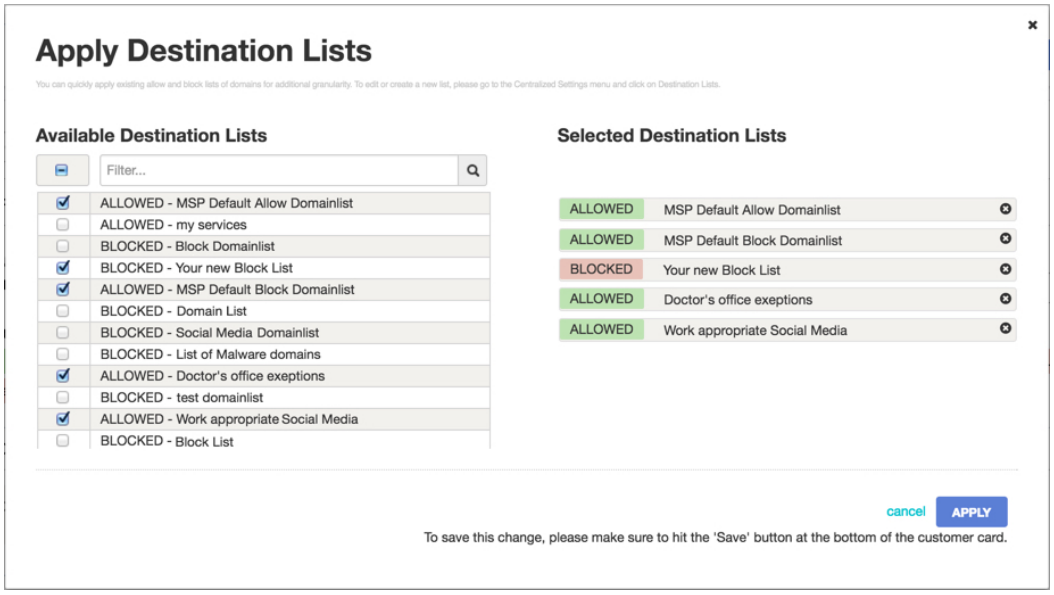
3. 必要に応じて [集中型設定（Centralized Settings）] を更新します。[集中型設定（Centralized Settings）] 領域には、[集中型設定（Centralized Settings）] コンポーネントで設定した内容が表示されます。ここで行った変更は、[集中型設定（Centralized Settings）] > [セキュリティ設定（Security Settings）] ページに反映されます。[集中型設定（Centralized Settings）] には、[ブロック ページ（Block Page）]、[カテゴリ（Category）]、[セキュリティ設定（Security Settings）] が含まれています。デフォルトに設定した集中型設定が自動的に選択されます。

集中型設定が複数ある場合は、ドロップダウン リストから別の設定を選択できます。

接続先リストの追加または削除

特に重要な集中型設定は、接続先リストです。最初は、グローバル ブロック リストとグローバル許可リストの 2 つの接続先リストだけが適用されています。ただし、デフォルトとマークされている接続先リストも適用されます。これは、[新しく作成する組織にこの設定をデフォルトで適用（Apply this setting by default when creating new organizations）] オプションを選択した接続先リストです。

1. [追加/削除（Add/Remove）] をクリックします。
   モーダル ウィンドウにすべての接続先リストのリストが表示されます。表示されるリストは顧客にすぐに追加できます。

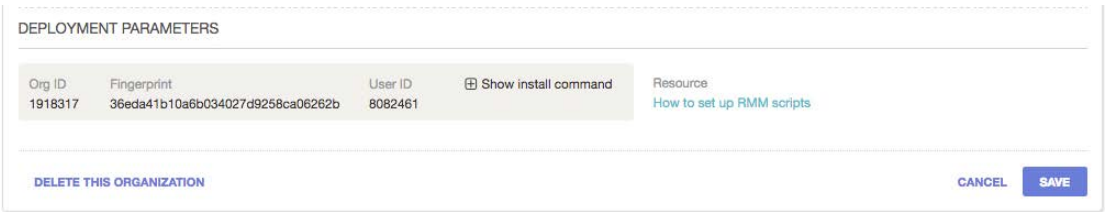


2. 適切な [使用可能な接続先リスト（Available Destination List）] チェックボックスをオンにします。
   ウィンドウの右側に選択した接続先リストが表示されます。

3. [適用（Apply）] をクリックし、[保存（Save）] をクリックして更新を確定します。

Umbrella ローミング クライアントのパラメータ

[集中型設定（Centralized Settings）] の下にある [導入パラメータ（Deployment Parameter）] 領域には、Umbrella ローミング クライアントの導入に必要な情報が表示されます。[組織 ID（Org ID）]、[フィンガープリント（Fingerprint）]、[ユーザ ID（User ID）] の値は、Umbrella ローミング クライアントをまとめて導入するときにインストーラに渡す値になります。スクリプトを含む共通 RMM の手順は、リソースとしてリンクされています。



コンソール設定

コンソール設定には、[管理者（Admins）]、[監査ログ（AuditLog）]、[請求（Billing）]、[ダッシュボードのブランド提携（Dashboard Co-branding）] があります。

管理者と委任管理者

Multi-Org Console のこのセクションでは、新しいスタッフ管理者をコンソールに追加することができます。Multi-Org Console で作成された管理者は、すべてのサブ組織に対して、完全な管理者レベルの制御を行うことができます。新しいユーザを 1 つの組織に制限する場合は、個々の組織に移動して、その組織に限定された新しいログインを作成することをお勧めします。これは、サブ組織が自身の組織内のレポートデータへのアクセスを希望する場合に使用することができる手段です。管理アカウントに対して 2 段階認証を有効にすることもできます。

委任管理

Multi-Org Console の委任管理は、コンソール管理者が、5 つのうちいずれかのロールを、コンソールを確認できる組織内の他のユーザに割り当てることができる機能です。これにより、組織を管理できるがコンソールに対する完全なアクセス権を持たないロール、サブ組織に新しいソフトウェアをプロビジョニングできるが、変更はできないロール、集中型設定を変更できるが、その他の設定にはアクセスできないロールをユーザに割り当てることができます。

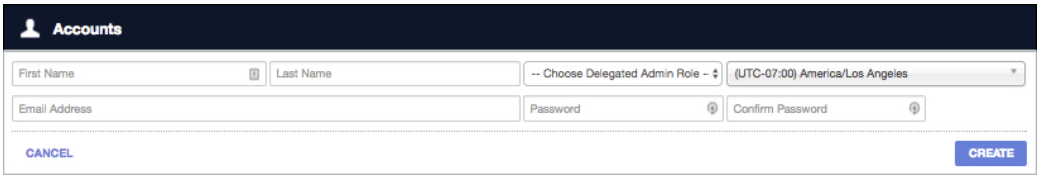
また、コンソールに対しては「読み取り専用」であるものの、複数のサブ組織のダッシュボードへの完全な管理アクセス権を持つユーザを作成することもできます。これにより、Multi-Org Console へのアクセスが制限しながら、個々の組織を扱う責任をユーザに委任することができます。

新しいユーザ アカウントのロールの選択

新しいユーザ アカウントを作成していずれかの委任管理ロールを適用するには、次の手順を実行します。

1. [コンソール設定（Console Settings）] > [管理者（Admins）] に移動し、[**+**]（**追加**）アイコンをクリックするか、既存のアカウントを選択します。

2. [委任管理ロールの選択（Choose Delegated Admin Role）] ドロップダウンリストからいずれかの管理者ロールを選択します。



- [完全な管理者（FullAdmin）]：このロールは、Multi-Org Console のすべての要素と、すべてのサブ組織の Umbrella ダッシュボードに対して、完全な管理者権限を持ちます。
- [プロビジョニング管理者（ProvisioningAdmin）]：このロールは集中型設定については読み取り専用ですが、すべてのサブ組織の Umbrella ダッシュボードに対する管理者権限を含め、組織の追加、削除、および管理について完全な管理者権限を持ちます。
- [サポート エンジニア（SupportEngineer）]：このロールは、集中型設定、組織管理（サブ組織の追加と削除）に対する読み取り専用権限と、その他すべてのコンソール管理権限を持ちます。ただしこのロールは、すべてのサブ組織の Umbrella ダッシュボードに対する完全な管理制御権限を持ちます。
- [制限付き管理（LimitedAdmin）]：このロールは、集中型設定とすべてのサブ組織の Umbrella ダッシュボードに対する完全な管理者権限を持ちますが、組織の追加と削除を含む組織管理については読み取り専用に制限されています。
- [グローバル読み取り専用（Global ReadOnly）]：このロールは、Multi-Org Console のすべての要素とすべてのサブ組織の Umbrella ダッシュボードについて読み取り専用権限を持ちます。

サブ組織の管理でのグローバル読み取り専用の作成

Multi-Org Console に対しては読み取り専用権限を持ち、特定のサブ組織に関してはそれ以上の権限を持つユーザを作成するには、最初にコンソール内で、グローバル読み取り専用としてユーザ アカウントを作成します。

1. [コンソール設定（Console Settings）] > [アカウント（Accounts）] に移動し、[+]（**追加**）アイコンをクリックします。

2. [委任管理ロールの選択（Choose Delegated Admin Role）] ドロップダウン リストから、[グローバル読み取り専用（Global Read Only）] を選択します。

3. 必要に応じてその他のボックスに入力します。

4. [作成（Create）] をクリックします。

ユーザを作成したら、サブ組織の Umbrella ダッシュボードに移動し、そのダッシュボードでそのユーザを管理者として招待します。

1. [設定（Settings）] > [アカウント（Accounts）] に移動します。

2. [既存のアカウントを招待（Invite an existing Account）] アイコンをクリックします。

3. ユーザの電子メール アドレスを入力し、[委任管理ロールの選択（Choose Delegated Admin Role）] ドロップダウン リストからいずれかの管理者ロールを選択します。

4. [招待（Invite）] をクリックします。
それにより、そのユーザは Multi-Org Console とその他すべてのサブ組織内では読み取り専用権限を持ちますが、この特定のサブ組織については完全な管理者権限を持ちます。

委任管理の制限事項

- 読み取り専用ロールは、特定の顧客に関する情報など、Mult-Org Console の特定の部分に表示を限定されるものではありません。
- そのユーザは Mult-Org Console で管理者になることはできず、個々のサブ組織の Umbrella ダッシュボードに対する管理アクセス権を持つことはできません。

監査ログ

Multi-Org Console 設定に対して管理者が行った変更を記録します。このログは個々の組織の管理者監査ログと同様に使用できますが、Multi-Org Console 固有のログです。管理者には、Multi-Org Console 内で生成されたイベントに関連するエントリが表示されます。記録される一般的なアクションとしては、組織に割り当てられている組織やシートの追加または削除などがあります。

課金

請求先担当者情報を更新できます。

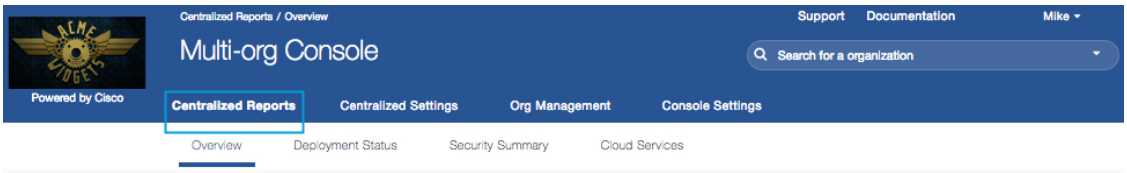
ダッシュボードのブランド提携

ダッシュボードとコンソールに、企業ロゴなどのグラフィックを追加できます。ブランド提携されたログ ページを作成することもできます。

Cisco Umbrella Multi-Org Console の概要 > 集中型設定

集中型レポート

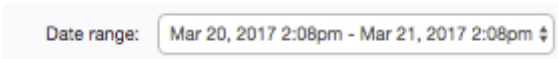
集中型レポートは、組織ベース全体を一括管理できる画面です。導入の状態をすばやく評価し、組織ベース全体のセキュリティ アクティビティの量を把握し、注意が必要な問題を迅速に特定することができます。このトップ レベルのレポートにより、組織内の問題の評価と優先順位付けが可能になります。ポリシー変更、ネットワーク変更、感染したワークステーションの修復、ソフトウェアの再導入など、注意が必要な事項にドリル ダウンできます。



集中型レポートは、次のサブレポートに分割されます。

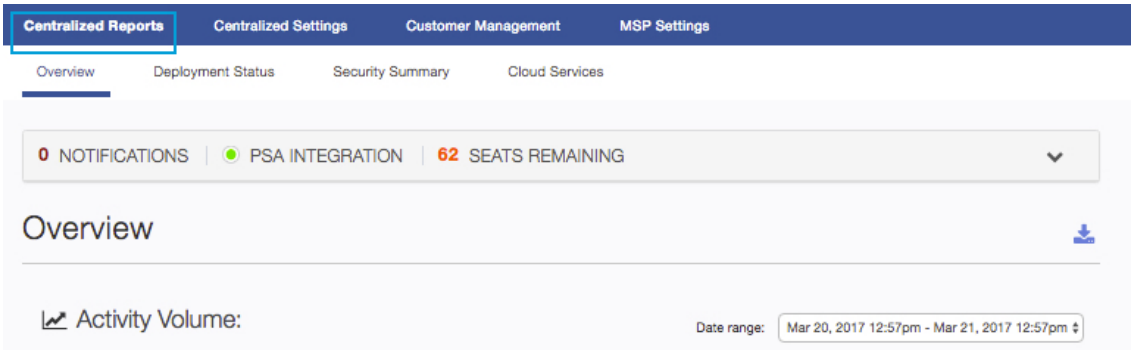
- 概要レポート
- 導入ステータス レポート
- セキュリティ サマリー レポート
- クラウド サービス レポート

これらのレポートは、対象となる期間を変更することができます。直近のレポート（最近 24 時間または今日）、またはカスタマイズした範囲の日単位または週単位のレポートを設定できます。



集中型レポート > 概要レポート

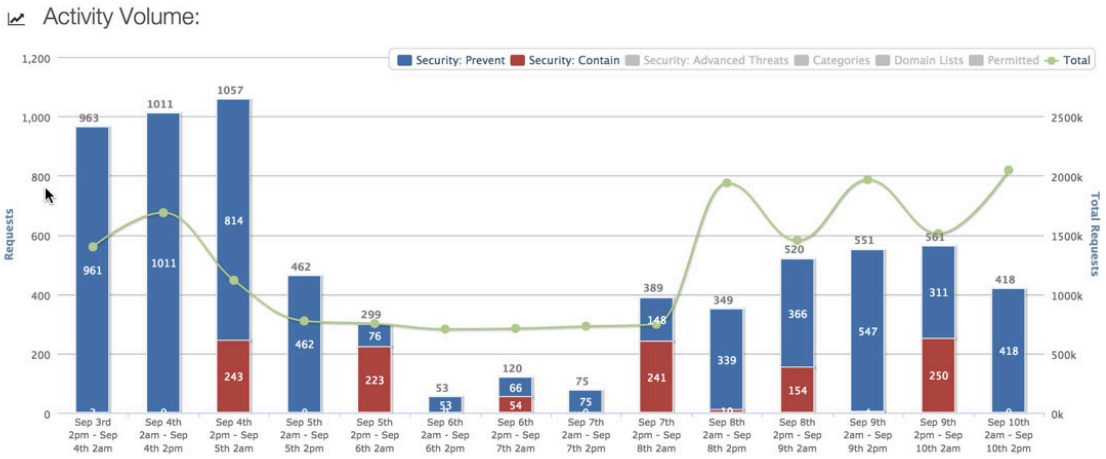
[集中型レポート（Centralized Reports）] > [概要レポート（Overview Report）] を選択することで、すべての顧客が利用できる 2 つの主要な機能である、[アクティビティ ボリューム（Activity Volume）] と [導入/ヘルス ステータス（Deployment and Health Status）] について、概要のスナップショットが得られます。



アクティビティ ボリューム

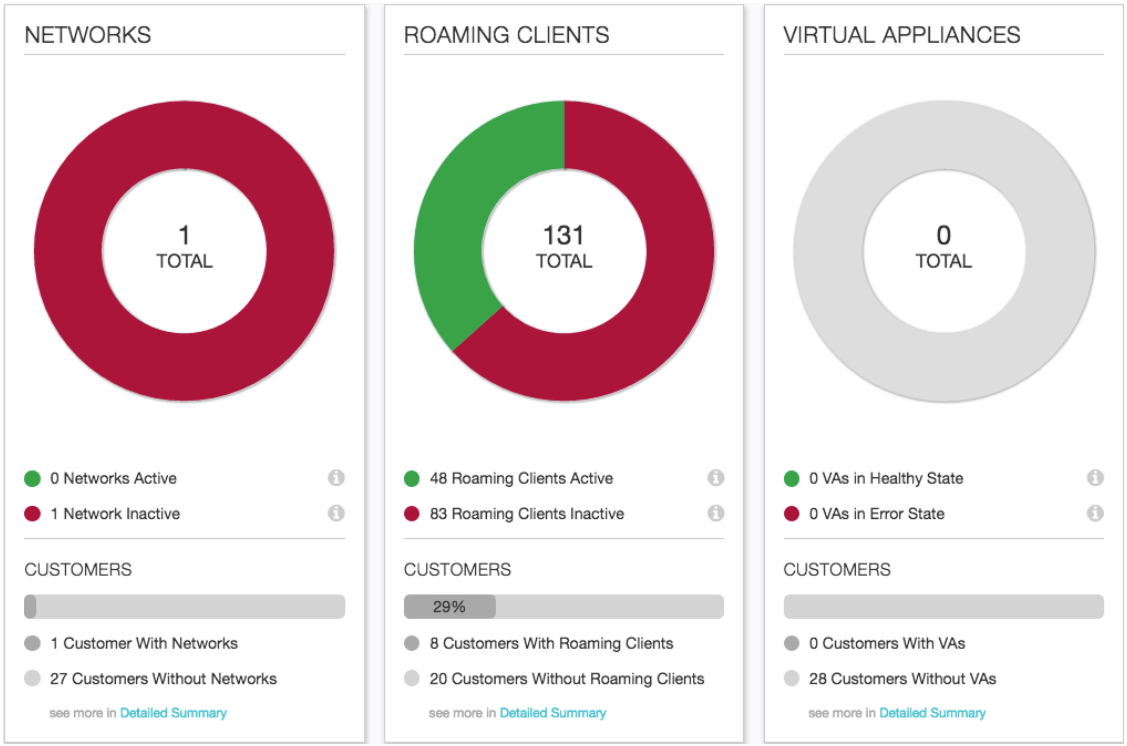
[アクティビティ ボリューム（Activity Volume）] は、個々の組織の Umbrella ダッシュボードに表示されるアクティビティ ボリューム レポートに類似していますが、このレポートには、すべての顧客からのすべてのトラフィックに関する情報が示されます。特定のタイプのトラフィックに関連するボタンをクリックすることで、そのタイプでのフィルタリングができます。トラフィック タイプの表示/非表示を切り替えるには、凡例のラベルをクリックします。

次に、[セキュリティ：防止（Security: Prevent）] および [セキュリティ：封じ込め（Security: Contain）] カテゴリに限定した、7 日間のトラフィック合計の例を示します。

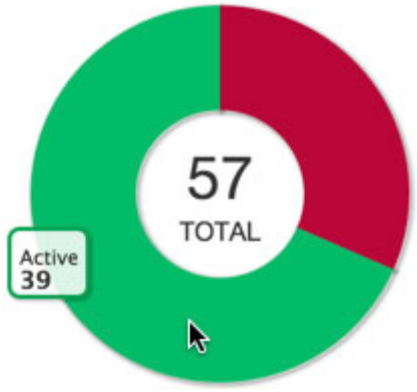


導入およびヘルス ステータス

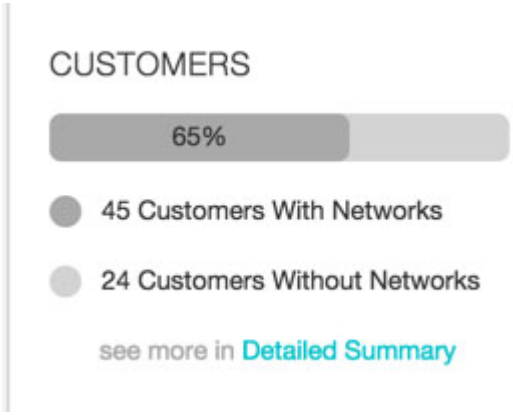
アクティビティ ボリュームのグラフの下に、導入およびヘルス ステータスのセクションがあります。これは、顧客の環境全体に導入されたネットワーク、Umbrella ローミング クライアント、仮想アプライアンス（VA）を対象とする、円グラフ スタイルのレポートです。



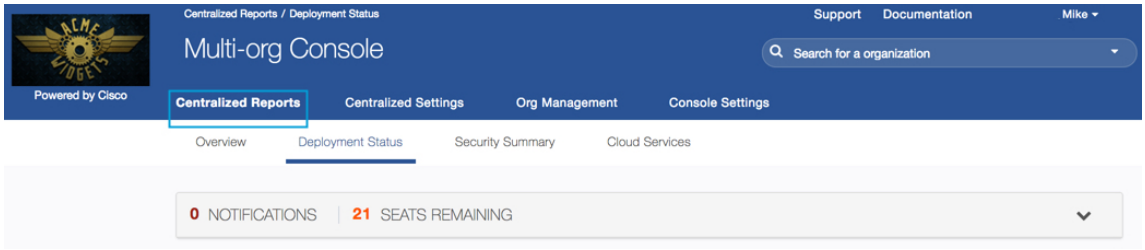
円グラフの緑色の部分は、指定された日付範囲内に 1 つ以上の DNS クエリを生成したアイデンティティ数を示しています。赤色の部分は、非アクティブなアイデンティティ数、つまり指定された日付範囲内に DNS クエリを生成していないアイデンティティ数を示しています。赤い「非アクティブ」領域にあるアイデンティティは、ネットワークに対して誤った IP アドレスが指定されていたり、Umbrella ローミング クライアントがアンインストールされていたりする可能性があります。円グラフまたは情報アイコンにカーソルを置くと、全組織のアクティブまたは非アクティブなコンポーネントの数が表示されます。



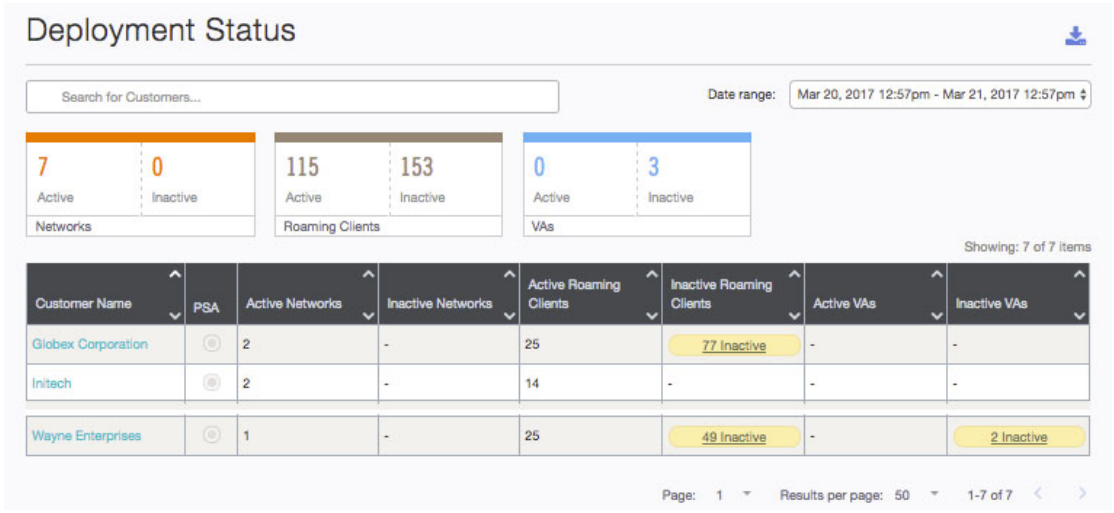
さらに [顧客（Customers）] 領域では、特定のタイプのアイデンティティ タイプを導入している顧客の割合を確認できます。また [詳細サマリー（Detailed Summary）] にジャンプして、統計で特定された顧客の詳細をドリル ダウンし、問題の修復または追加シートのインストールを行うことが可能です。



集中型レポート > 導入ステータス レポート



[集中型レポート(Centralized Reports)] > [導入ステータス レポート(Deployment Status Report)] では、ネットワーク、Umbrella ローミング クライアント、およびカスタマー ベースの VA の合計数の概要が得られます。また**特定の顧客を検索**し、その顧客の最新情報を確認することができます。列をソートすれば、関心に応じて重要な統計情報を見つけることがもできます。

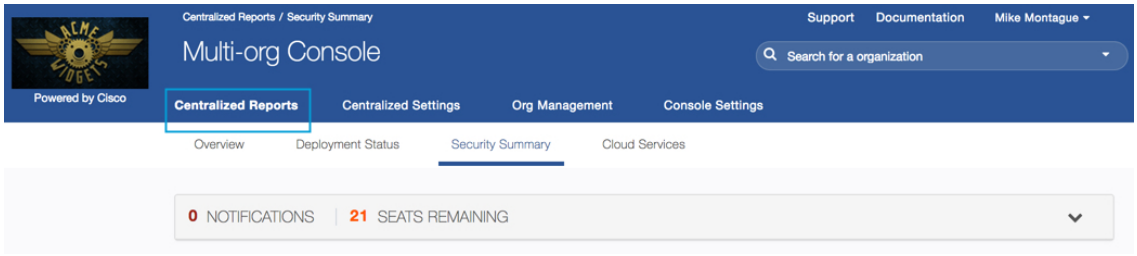


それぞれの顧客について、非アクティブな項目は黄色で強調表示されます。それを選択すると顧客の Umbrella ダッシュボードにジャンプし、正確にどのコンポーネントが非アクティブであるかが示されます。次の例では、5 つの非アクティブなローミング クライアントを示す黄色いリンクをクリックすると、顧客の Umbrella ダッシュボードで非アクティブになっているクライアントだけを示す画面が表示されます。

注:非アクティブ レポートは時間に依存します。非アクティブなローミング クライアントの例では、レポート対象として指定された期間内に Umbrella に DNS クエリを送信しなかった場合、Umbrella ローミング クライアントが非アクティブに設定されます。非アクティブなネットワークの例では、レポート対象として指定された期間内に Umbrella に DNS クエリを送信しなかった場合、ネットワークが非アクティブに設定されます。

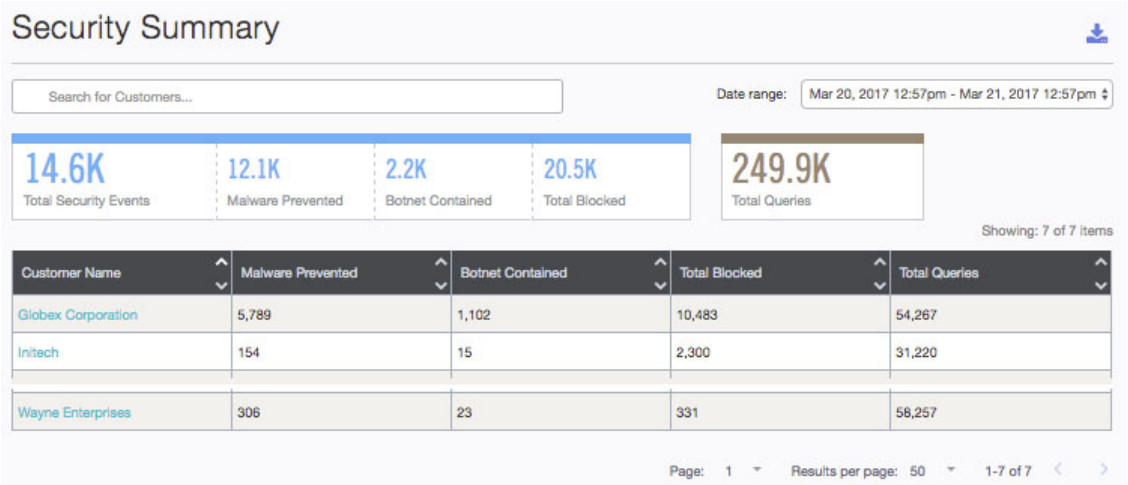
Inactive Networks	Active Roaming Clients	Inactive Roaming Clients
-	7	-
-	30	5 Inactive
-	-	-
3 Inactive	80	11 Inactive
-	14	7 Inactive

集中型レポート > セキュリティ サマリー レポート



[集中型レポート(Centralized Reports)] > [セキュリティ サマリー レポート(Security Summary Report)] を選択すると、選択した期間内について、すべての顧客のトラフィックとセキュリティ イベントの概要が表示されます。特定の顧客を検索すると、その顧客の最新情報が表示されます。

概要レポートと同様に、このセキュリティ サマリーの主な目標は、カスタマー ベースに対して期待するベンチマークを確立することにあります。それにより、感染の可能性を示すボットネット トラフィックなどの問題を特定できます。

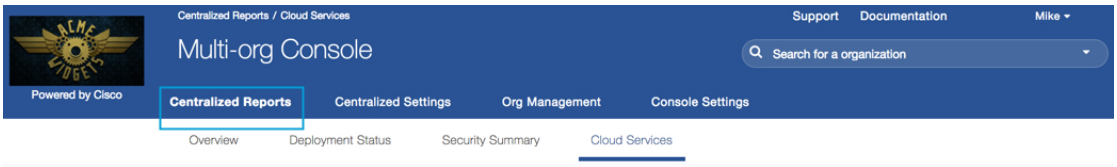


次のようなソート可能な列があります。

- [防御されたマルウェア（MalwarePrevented）]：ドメインがマルウェアを配布していると見なされてブロックされた DNS クエリ数。
- [封じ込められたボットネット（BotnetContained）]：ドメインが、感染したマシンをボットネットに参加させるために使用するコマンド/コントロール サーバと見なされ、ブロックされた DNS クエリ数。ボットネット トラフィックは、顧客のネットワーク上に感染したマシンがある可能性を示します。
- [合計ブロック数（TotalBlocked）]：カテゴリ設定、接続先リスト、およびその他のカテゴリによるブロックを含む、ブロックされたクエリの合計数。

最も重要なソートである列によるソートでは、防御された脅威の数に基づいて Umbrella から特定の値を受け取る顧客、または感染したマシンがボットネットのコマンド/コントロールにアクセスしているために特に注意を必要とする顧客を特定できます。

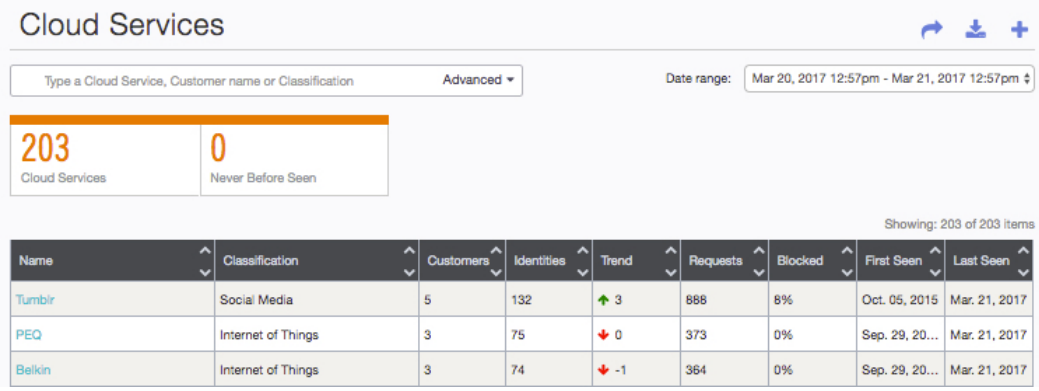
集中型レポート > クラウド サービス レポート



[集中型レポート（Centralized Reports）] > [クラウド サービス レポート（Cloud Services Report）] を選択すると、顧客が使用しているクラウド ベースのアプリケーションを把握し、その使用を緩和、制限、または補完することができます。

この情報は次のように使用できます。

- ソフトウェアに対するニーズがユーザにありながらも、正式なツールがないという状況が発生していないかを確認する。たとえば、ユーザがファイル サーバの代わりに、オンラインのストレージ システムを使用している場合、それはセキュリティを回避するためではなく、生産性を向上させるためである可能性があります。
- 従来のデータ損失の防止措置をバイパスするために使用されている、クラウドサービスを特定する。クラウド サービスが使用されていることがわかれば、個人を特定できるデータや企業の機密情報の漏洩から作業環境を保護することができます。

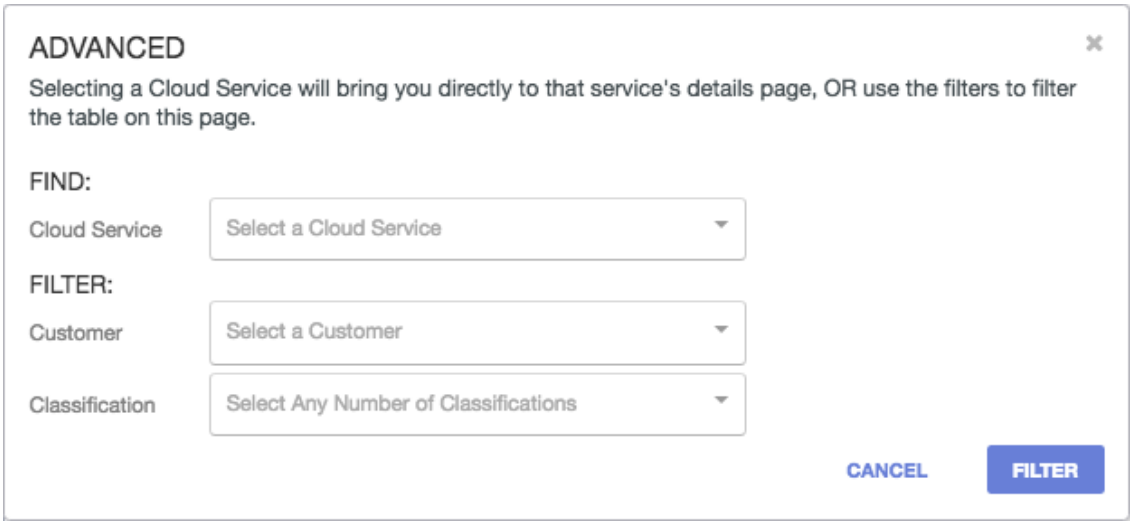


クラウド サービスのサマリーでは、指定した期間内に見つかったクラウド サービスの数も示されます。このサマリーには、その期間に見つかった新しいクラウド サービスの数も表示されます。

- [クラウド サービス(CloudServices)]:フィルタで指定した期間内に組織内のアイデンティティによってアクセスされたことが確認された個々のクラウド サービスの数。
- [過去に確認されていないサービス(Never BeforeSeen)]:フィルタで指定した期間内に確認されたが、組織での使用がそれまでに確認されていなかったクラウド サービスの数。

検索

クラウド サービス レポートには、ドロップダウン リストから検索またはフィルタ オプションを指定できる、高度なフィルタが含まれています。



クラウド サービス レポートの仕組み

クラウド サービス レポートは、顧客のユーザがクラウド内のサービスにアクセスした際の行動に関する DNS 情報を取得し、そのサービスの既知のドメインと照合します。Umbrella の「いつでも、どこでも、どんなデバイスでも」というアプローチにより、顧客がネットワーク上に存在しない時でさえ、顧客のクラウド サービスの使用を把握できます。Umbrella では、電子メール、ファイル共有、SaaS/IaaS/PaaS サービスなどの使用中のクラウド サービスが検出され、その使用状況がレポートされます。

プロビジョニング済みのアイデンティティに対する既存の設定など、Umbrella ダッシュボードのデータが確認され、組織から特定のクラウド サービスへの DNS トラフィックと照合されます。これにより、ユーザのクラウド サービスの使用状況を示します。レポートには、新しいサービスの導入傾向も含まれます。最初の使用日や最終確認日などが含まれます。

クラウド サービスの認識方法

近年では、ほぼすべてのユーザが、業務上もしくは個人的な理由から、オンライン ストレージ、Web ベースの電子メール、コラボレーション ツール、教育用のサイト、ソーシャル メディアなどを利用しています。このレポートにおける「クラウド サービス」とは、数ある SaaS、IaaS、PaaS やその他の「クラウド」コンピューティング サービスを意味します。実際に、Umbrella 自体もクラウド サービスであり、レポートにリストされます。

Umbrella では、小規模な企業から有名ソフトウェア企業までの数千のクラウド サービスのリストを蓄積しています。組織のユーザがアクセスしたドメインが、クラウド サービスであると Umbrella が特定したドメインに一致する場合は、クラウド サービスのレポートでそれが示されます。クラウド サービス レポートでは、それぞれのクラウド サービスを構成する URL に関する詳細が示されます。

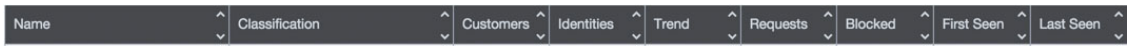
要求のロギングが有効になっていることの確認

レポートでデータが生成されるようにするには、顧客のポリシーでコンテンツ要求のロギングを有効にする必要があります。これはデフォルトで有効になっています。ただし、ロギングが無効になっている場合、クラウド サービス レポートでデータを表示させるには、ロギングを再度有効にする必要があります。顧客の組織の [ポリシー（Policies）] で、ポリシー ビルダーのステップ 4（ポリシーの詳細設定）を確認します。[要求のロギング（Request Logging）] ドロップダウン リストは、[ロギングの有効化（Logging enabled）] に設定し、[コンテンツ ロギングの無効化（Content logging disabled）] または [ロギングの無効化（Logging Disabled）] には**設定しない**ようにします。クラウド サービスへの要求に対してロギングが必要となるのは、それがセキュリティ イベント（例：マルウェア）ではなく、DNS クエリに関連したコンテンツだからです。

また、関連するすべてのアイデンティティからイベントを収集するには、ロギングを有効にしたポリシーをポリシーの階層の中で、適切な場所に位置づけることが重要です。

クラウド サービスのリスト

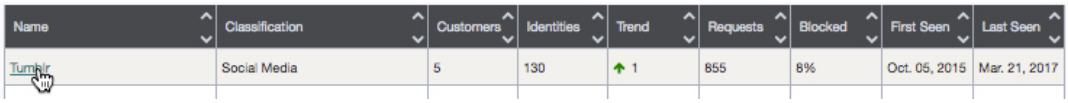
クラウド サービス レポートには、顧客が環境内でアクセスしたすべてのクラウド サービスがリストされます。これは、Umbrella でリストできるすべてのクラウド サービスを網羅したものではなく、レポートで指定した時間内にアクセスされたサービスだけのリストです。デフォルトのレポートでは、要求数が最大であるクラウド サービスが最上位に位置していますが、各列はソート可能であり、重要な機能に焦点を絞ることもできます。



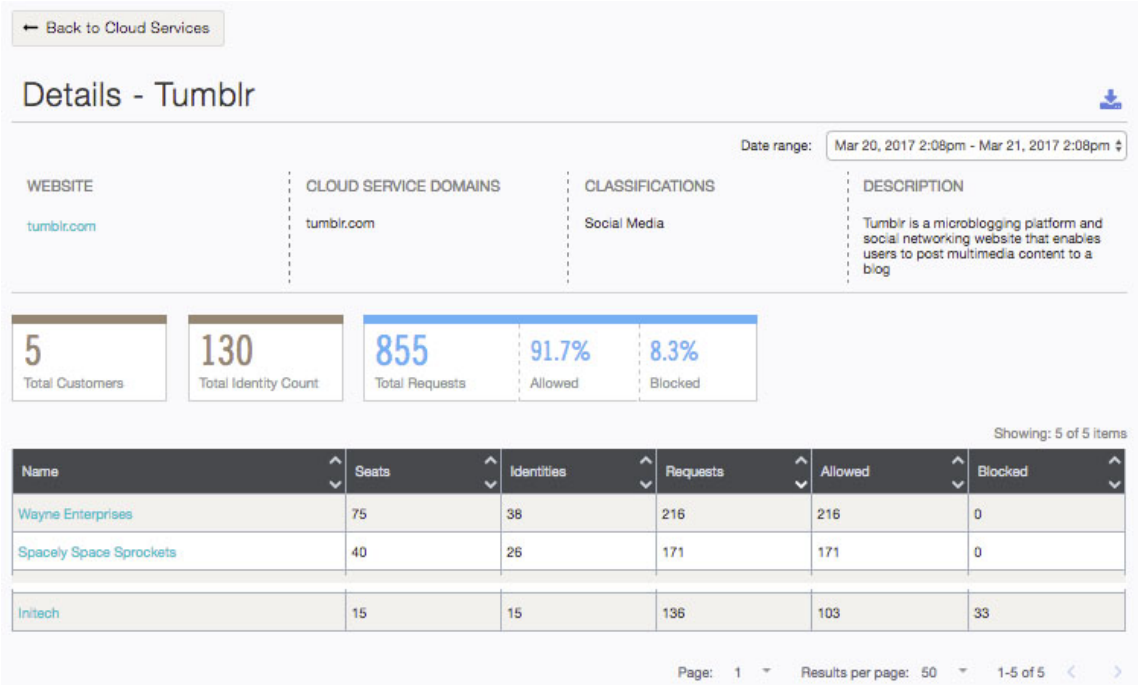
- [名前（Name）]：クラウド サービス自体の名前。 サービス内容の詳細については、サービスを選択してクリックします。
- [分類（Classification）]：分類では、サービスが一般的に何に使用されているかが説明されます。 各サービスに 1 つ以上の分類があります。クラウド サービスの分類の完全なリストに関しては、左下の [分類によるフィルタ（Filter by Classification）] をクリックします。
- [顧客（Customers）]：対象のサービスを使用している顧客の数。
- [アイデンティティ（Identities）]：対象のクラウドサービスにアクセスしている組織内のアイデンティティの数。
- [トレンド（Trend）]：指定期間内における、対象のクラウドサービスを要求するアイデンティティの数の増減。
- [要求（Requests）]：指定期間内の、組織から対象のクラウドサービスに送信された要求数の合計。
- [ブロック済み（Blocked）]：指定期間内の、ブロックされたサービスへの要求の割合。
- [最初の確認（FirstSeen）]：対象のサービスが組織内のアイデンティティによって使用されたことが最初に確認された日付。
- [最新の確認（LastSeen）]：対象のサービスへの要求が行われた最新の日付。

サービスの詳細

それぞれのクラウド サービスをドリルダウンすることで、組織による個々のサービスの使用状況に関するレポートを表示できます。レポート内のクラウド サービスの名前をクリックします。この例では Tumblr を選択しています。



クリックすると、このサービスの [サービス詳細（Service Details）] が表示されます。



各サービスについて、次のような詳細が表示されます。

- [Web サイト（Website）]：クラウドサービスを提供する企業の Web サイト。例では、クラウド サービスの名前と企業名が同じですが、異なる場合もあります。
- [クラウド サービス ドメイン（Cloud ServiceDomains）]：クラウド サービスが使用されているかを判断する際に、Umbrella が一致を発見した URL のリスト。多くのクラウド サービスでは、クラウド サービス ドメインは 1 つしかありません。ただしドメインが複数ある場合は、ユーザがリスト内のいずれかのクラウド サービス ドメインにアクセスした時点で一致と見なされます。Twitter の例では、このサービスに一致するドメインは 1 つだけです。4 つまたは 5 以上のドメインがある場合は、[+] 記号をクリックするとその他のドメインが表示されます。
- [分類（Classifications）]：サービスのタイプおよび分類が表示されます。 次の例では、分類は 1 つだけですが、クラウド サービスは複数の分類に含まれる可能性があります。
- [説明（Description）]：クラウドサービスに関する簡単な説明。クラウド サービスの内容や、サービスの使用によりユーザに提供される IT サービスの効果について説明されます。

サービスの詳細の下には、顧客とアイデンティティの合計数に特価した統計情報が表示されます。時間の経過に伴う対象のサービスのトレンドがわかるため、2 つの期間を比較する場合に役立ちます。

- [合計顧客数（TotalCustomers）]：指定した日付範囲の中で対象のクラウド サービスを利用した顧客数の合計。
- [合計アイデンティティ数（Total IdentityCount）]：指定した日付範囲の中でこのクラウド サービスを利用した顧客のアイデンティティの合計数。
- [合計要求数（TotalRequests）]：このクラウド サービスに対する要求の合計数。個々のアイデンティティごとの要求は、顧客のダッシュボード内で内訳を見ることができます。顧客の設定によって許可またはブロックされた要求の割合も示されます。

顧客名をクリックすると、それぞれの Umbrella ダッシュボードが表示され、組織のクラウド サービスのレポートを確認できます。レポートは事前にフィルタリングされ、詳細を確認していたクラウド サービスに情報が絞れらるため、それぞれの顧客の環境内の正確なアイデンティティと、サービスの利用状況を表示できます。

集中型設定

集中型設定は、新しく登録された組織を含め、複数の組織に同時に適用できる設定です。集中型設定は使いやすく強力で、時間の余裕ができるとともに、総所有コストの削減に役立ちます。多対多のリンクを作成するアプローチは、標準設定を適用しながらカスタマイズが可能である点で、従来のテンプレートに比べて利点があります。

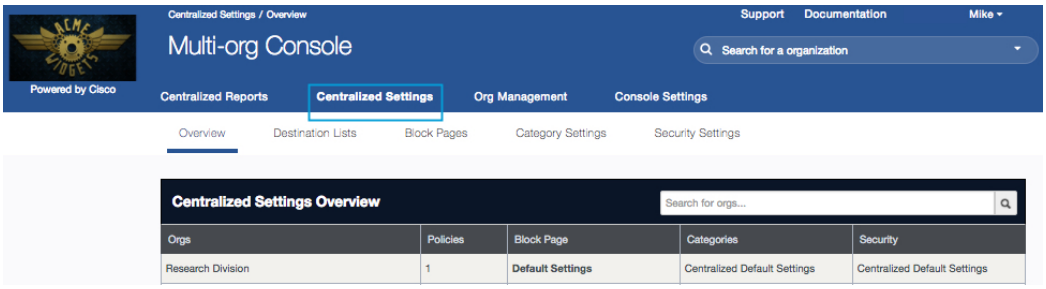
Cisco Umbrella Multi-Org Console の集中型設定は、次の領域に分割されます。

- 集中型設定の概要ページ
- 集中型接続先リストの設定
- 集中型ブロック ページの設定
- 集中型カテゴリ設定
- 集中型セキュリティ設定

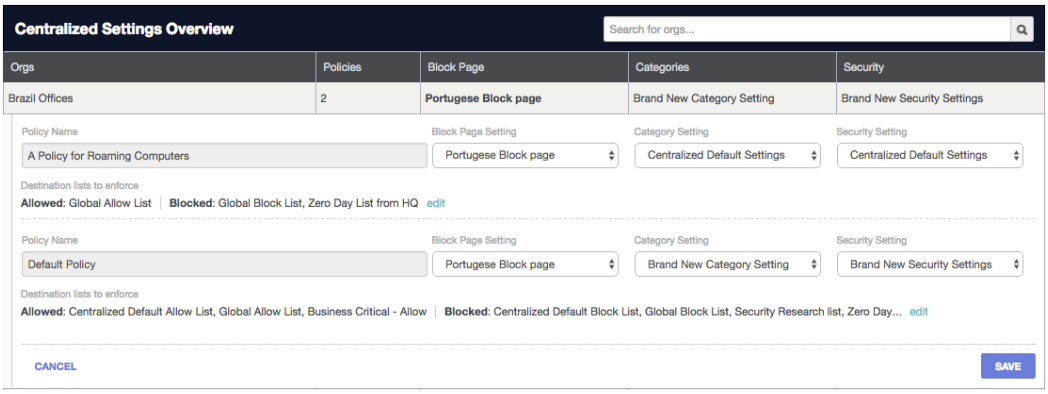
集中型設定へのアクセス

[Multi-Org 集中型設定の概要（Multi-Org Centralized Settings Overview）] ページでは、すべての組織に一括適用されたすべての接続先リスト、ブロック ページ、カテゴリ設定、およびセキュリティ設定を表示できます。[概要（Overview）] ページでは、個々の組織ポリシーの設定を変更することもできます。

1. Umbrella Mult-Org Console で、[集中型設定（Centralized Settings）] > [概要（Overview）] に移動します。すべての組織のリストと、各組織に適用されているポリシーの数が表示されます。各組織のデフォルト ポリシーに適用されている設定は、プライマリの [概要（Overview）] ページにリストされます。集中型設定はここで作成することはできませんが、Multi-Org Console の [組織管理（Org Management）] セクションから組織に適用することができます。



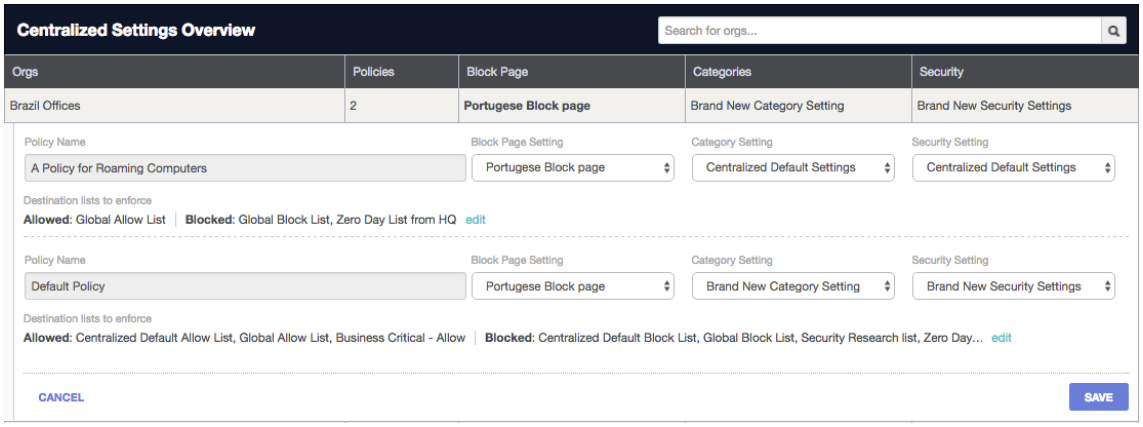
2. 組織名をクリックして組織を展開すると、組織の設定に関する詳細が表示されます。



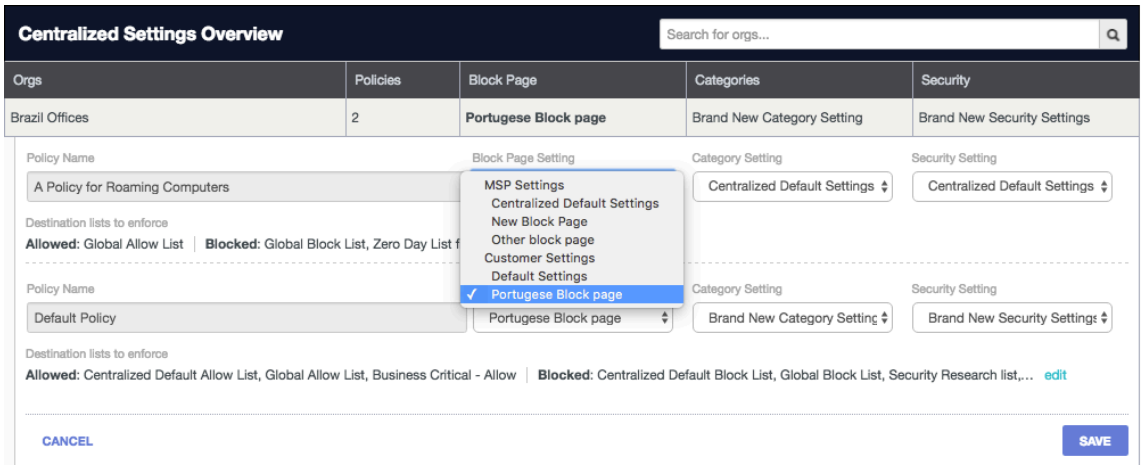
太字の設定は、Multi-Org 集中型設定**ではない**設定であり、その組織のダッシュボードで独自に設定されたものです。この例では「Portuguese Block Page」が太字であり、Brazil Offices 組織に固有のものです。

概要ページでは、両方の種類の設定（集中型設定と組織固有の設定）を変更できます。

次の例では、組織「Brazil Offices」に 2 つのポリシーが適用されています。ポリシー内には 2 つの設定（[カテゴリ（Categories）] と [セキュリティ（Security）]）があり、Multi-Org Console の [集中型設定（Centralized Settings）] から設定されています。ただし [ブロック ページ設定（Block Page Setting）] は、この組織固有のポリシー（「Portuguese Block Page」）を使用して設定されています。



設定を変更するには、個々の組織の Umbrella ダッシュボードにログインするのではなく、該当するドロップダウン リストから設定を選択します。ここでは、組織に固有の設定、またはすべての組織に共通の設定を選択できます。各ドロップダウン リストでは、個別のサブリストに Multi-Org の集中型設定と個々の組織設定が表示されます。



集中型接続先リストの設定

接続先リストは、インターネットの特定の接続先に対する顧客のアクセスを管理（ブロックまたは許可）するために使用する、インターネット要求（ドメイン名、URL、IP アドレスなど）のリストです。
集中型接続先リストは、次の手順で設定します。

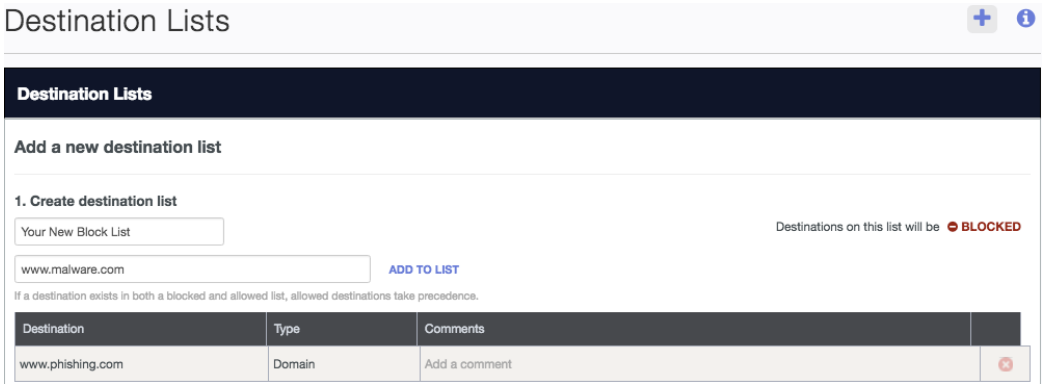
1. ブロックまたは許可する接続先リストを作成します。
2. 組織と接続先リストを共有します（オプション）。
3. 変更を確認します。

ステップ 1：ブロックまたは許可する接続先リストを作成する

1. [集中型設定（Centralized Settings）] > [接続先リスト（Destination Lists）] に移動します。
2. [+]（**追加**）アイコンをクリックし、[ブロック リストの追加（Add Block List）] または [許可リストの追加（Add Allow List）] を選択します。

3. 新しい接続先リストに、目的を示す名前を付けます。ここでは、接続先リストに「Your New Block List」という名前を付けます。

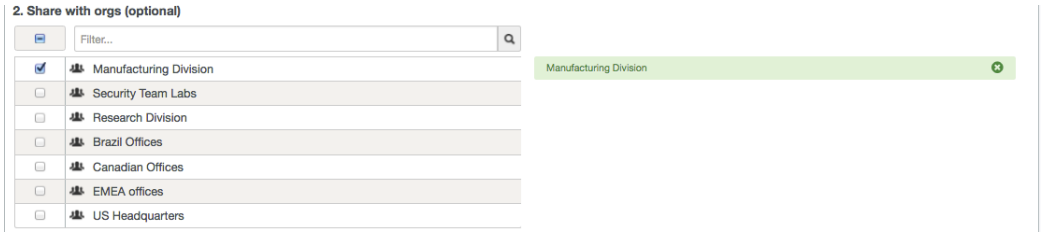
4. [リストに追加（Add to List）] をクリックして、接続先リストにドメインを追加します。



注：「domain.com」などのエントリには、「mail.domain.com」や「www.domain.com」など、すべてのサブドメインが含まれます。
ブロックされる接続先リストと許可される接続先リストの両方にドメインが存在する場合は、許可リストが優先されます。

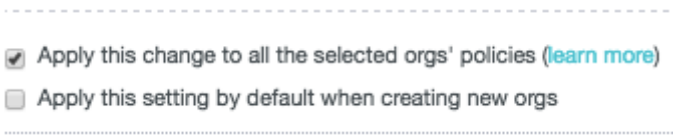
ステップ 2：組織と接続先リストを共有する（オプション）

1. [組織と共有（オプション）（Share with orgs (optional)）] で、接続先リストを共有する組織のチェックボックスをオンにします。
   接続先リストは、1 つ以上の組織に適用できます。[接続先リスト（Destination Lists）] ページには、管理するすべての組織がリストされます。それらすべてを選択することも、フィルタ オプションを使用して特定の組織を検索することもできます。



2. 接続先リストを組織と共有しないことを選択することもできます。組織を選択せずに、[保存（Save）] をクリックします。
   必要に応じて、後で組織を共有接続先リストに追加することもできます。

3. ページの下部には、新しい設定を適用する方法を決定する、2 つの重要な設定があります。



1 つ目のオプションでは、選択した組織のすべてのポリシーに、この集中型設定を適用することができます。ここで重要なことは、[選択したすべての組織のポリシーにこの変更を適用する（Apply this change to all the selected orgs' policies）] のチェックマークが、このステップで追加された組織に対してのみ実行されるということです。対象の組織は右側の列で緑色で強調表示されます。

この設定をその組織に再適用するには、その組織から設定を削除し、[選択したすべての組織のポリシーにこの変更を適用する（Apply this change to all the selected orgs' policies）] をオンにして設定を再度保存します。

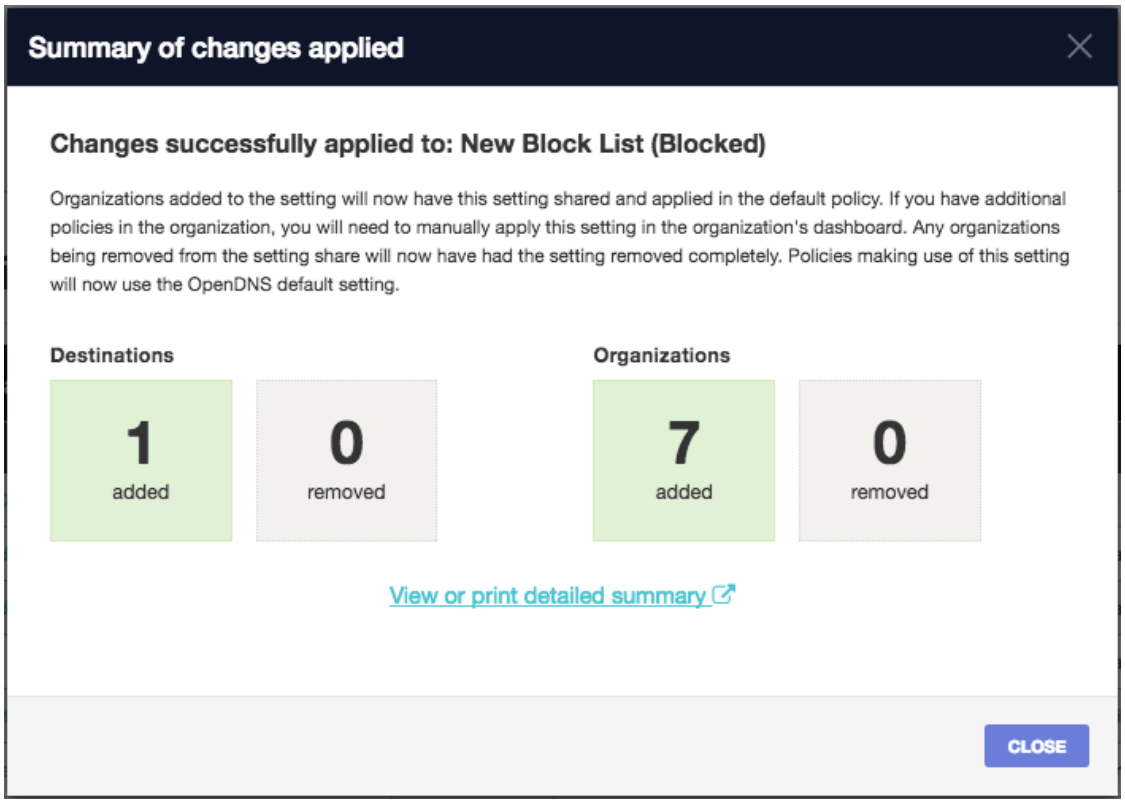
2 つ目のオプションは、[新しい組織を作成する場合にデフォルトでこの設定を適用する（Apply this setting by default when creating new orgs）] オプションです。Multi-Org Console に新しい組織を追加すると、このチェックマークが付いた接続先リストが、その組織のデフォルト ポリシーに自動的に適用されます。後で接続先リストの一覧を確認すると、このオプションを選択した集中型設定が「デフォルト」としてマークされていることがわかります。

デフォルトに設定できるポリシーは 1 つだけです。デフォルトを変更するには、ウィザードを再実行して、別のデフォルトを選択します。デフォルトのポリシーは必ず設定する必要があり、デフォルトとして別のポリシーを設定するまでは、デフォルト設定を削除することはできません。ただし、複数の接続先リストをデフォルトとして適用し、新しい組織が作成されたときにすべてが適用されるようにすることができます。

4. [保存（Save）] をクリックします。

ステップ 3: 変更を確認する

最後のステップでは、行った変更を確認します。[保存（Save）] をクリックすると、変更のサマリーが表示されたモーダル ウィンドウが表示されます。この例では、1 つの接続先リストが 7 つの組織に追加されています。またこのポリシーが新しい組織のデフォルトになります。



[詳細なサマリーの表示または印刷（View or print detailed summary）] をクリックすると、ブラウザで新しいタブが開き、行った変更の詳細なリストが表示されます。

- 変更された組織や、追加または削除された接続先など、適用された変更のリスト
- 接続先リストの接続先と、リストを共有している組織の詳細を示す、「現在の状態」

集中型ブロック ページの設定

ブロック ページは、Umbrella サービスのユーザが、そのユーザが属すアイデンティティのポリシーによってブロックされている Web サイトにアクセスを試みた場合に表示されるページです。集中型ブロック ページは、次の手順で設定します。

1. 新しいブロック ページを追加するか、デフォルトのブロック ページを編集します。

2. ブロック ページを組織と共有します。

3. ブロック ページを組織のすべてのポリシーに適用します。

4. 新しい組織を作成すると、設定が自動的に適用されます。

5. 変更を確認します。

最初のステップでは、ブロック ページ自体を作成します。このプロセスは、Multi-Org Console のいずれかのサブ組織内（個々の組織内の [ブロック ページ設定（Block Page Settings）] >[ブロック ページの外観（Block Page Appearance）]）でブロック ページを作成する場合とほぼ同じです。

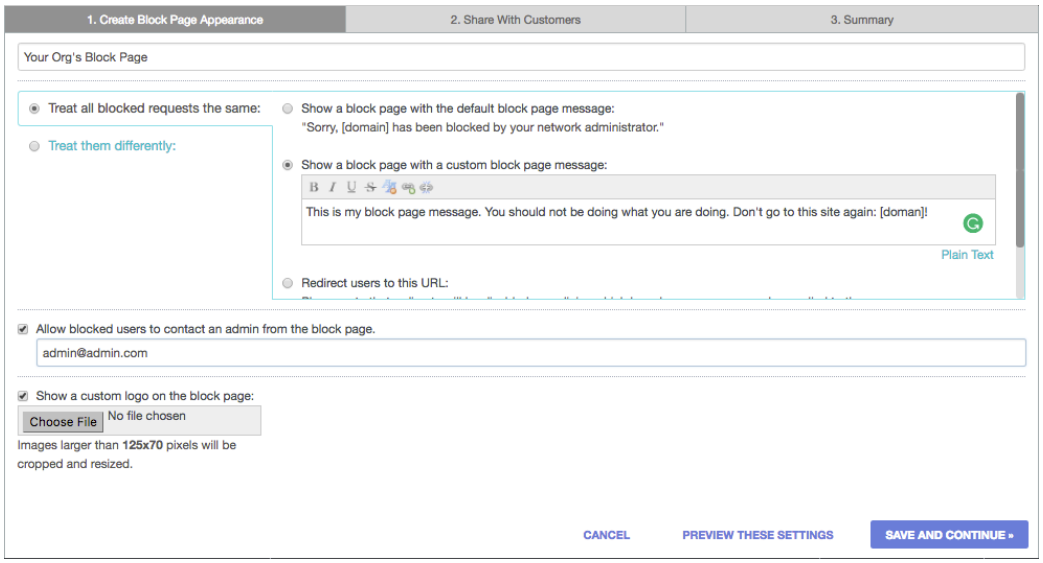
ステップ 1: 新しいブロック ページを追加するか、デフォルトのブロック ページを編集する

1. [集中型設定（Centralized Settings）] > [ブロック ページ（Block Pages）] に移動します。

2. [新しいブロック ページの追加（Add a New Block Page）] をクリックして、最初の集中型ブロック ページを作成し、カスタマイズを開始します。または、[ブロック ページ（Block Pages）] テーブルにリストされているデフォルトを選択して編集します。
   集中型ブロック ページ設定を行うことができる、簡単な 3 ステップのウィザードが開きます。

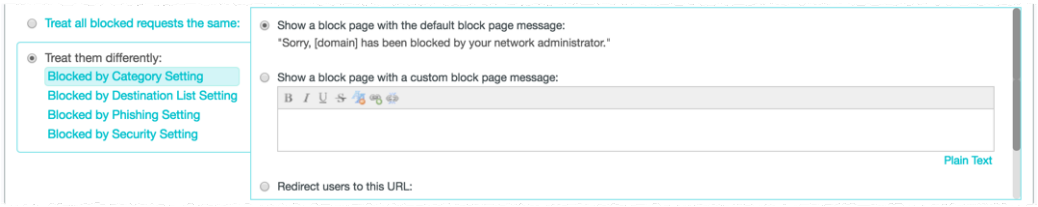
3. ブロック ページのタイトルを設定します。これは、同僚やスタッフに表示される名前です。



注

Umbrella ダッシュボードで単一のサブ組織にアクセスできるユーザは、誰でも集中型設定名を見ることができますが、変更することはできません。

4. ブロック ページの処理方法を選択します。[すべてのブロック要求を同じ方法で処理する（Treat all block requests the same）] または [異なる方法で処理する（Treat them differently）] を選択します。
   [異なる方法で処理する（Treat them differently）] を選択すると、[カテゴリ設定（Category Setting）]、[接続先リスト設定（Destination List Setting）]、[フィッシング設定（Phishing Setting）]、[セキュリティ設定（Security Settings）] など各種のブロックについて、コンテキスト ブロック ページを作成できます。



5. ユーザ用にカスタム メッセージを設定するか、デフォルトのメッセージのままにします。
   ブロック ページでは、ユーザがアクセスを試みたドメインのコンテキストに応じてメッセージを表示できます。これはカスタム メッセージとして、[domain] 変数を使用して追加できます。

6. 必要に応じて、自分宛てまたは組織内の管理者グループ宛ての電子メールアドレスを設定します。このアドレスは、ユーザがアクセスしたいブロック ページについてバイパスの許可を要求する場合に使用できます。

7. [ブロック ページにカスタム ロゴを表示する（Show a custom logo on the block page）] をオンにして、ブロック ページにカスタム ロゴとして表示するファイルを選択します。
   これでブロック ページにブランドが表示され、ブロックの作成元が明確になります。これは多くの場合、大学、企業、公的ブランドなどのロゴになります。

8. 変更を確定する前に、[これらの設定をプレビュー（Preview These Settings）] をクリックして、ブロック ページの外観を確認します。

9. [保存して続行（Save and Continue）] をクリックします。

ステップ 2a：ブロック ページを組織と共有する

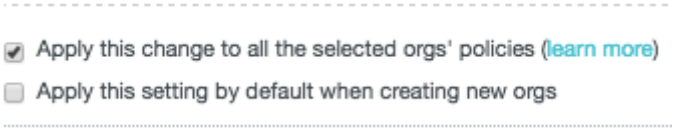
ウィザードの次のステップでは、1 つ以上の組織とブロック ページを共有します。ここには管理しているすべての組織がリストされます。

1. ブロック ページを共有する組織のチェックボックスをオンにします。

2. ブロック リストを組織と共有しないことを選択することもできます。組織を選択せずに [スキップ（Skip）] をクリックします。
   必要に応じて、後で組織をブロック ページに追加することができます。

ステップ 2b：ブロック ページを組織のすべてのポリシーに適用する

ウィザードの第 2 段階の下部には、新しい設定を組織内の特定のポリシーに適用するための、2 つの重要な設定があります。



1 つ目のオプションは、この設定を選択した組織のすべてのポリシーに適用することができます。ここで重要なことは、[選択したすべての組織のポリシーにこの変更を適用する（Apply this change to all the selected orgs' policies）] のチェックマークが、このステップで追加された組織に対してのみ実行されるということです。対象の組織は右側の列で緑色で強調表示されます。

この設定を特定の組織に再適用するには、その組織から設定を削除し、[選択したすべての組織のポリシーにこの変更を適用する（Apply this change to all the selected orgs' policies）] をオンにして設定を再度保存します。

ステップ 2c：新しい組織を作成したら設定を自動的に適用する

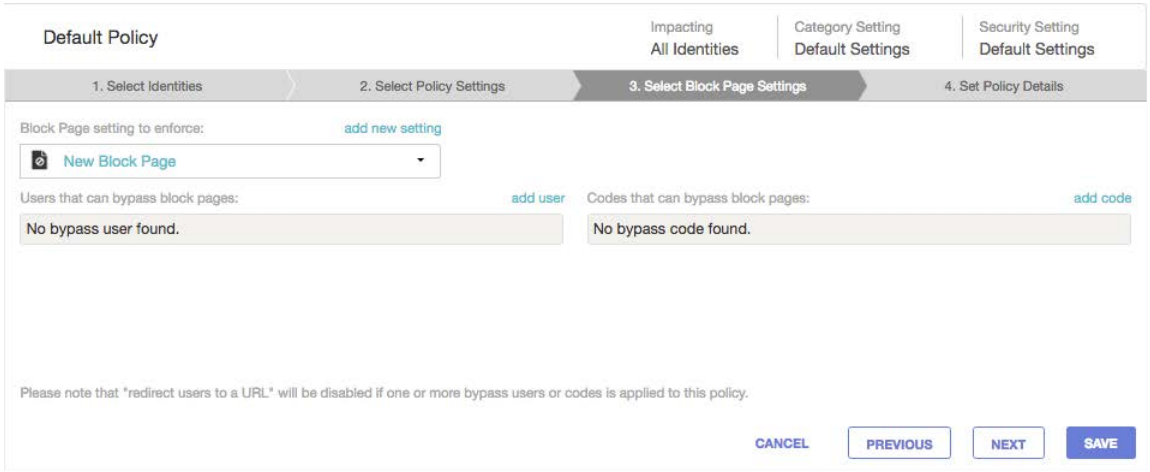
2 つ目のオプションは、[新しい組織を作成する場合にデフォルトでこの設定を適用する（Apply this setting by default when creating new orgs）] オプションです。Multi-Org Console に新しい組織を追加すると、このチェックマークが付いたブロックページ設定が、その組織のデフォルト ポリシーに自動的に適用されます。後で集中型設定ブロック ページのリストを確認すると、このオプションを選択した集中型設定が「デフォルト」としてマークされていることがわかります。

デフォルトに設定できるポリシーは 1 つだけです。これを変更したい場合は、ウィザードを再実行して、別の集中型設定ブロック ページのチェックボックスをオンにします。デフォルトの設定は必ず設定する必要があり、デフォルトとして別のポリシーを設定するまでは、デフォルト設定を削除することはできません。

たとえば上記の例では、「US Headquarters」という組織にブロック ページ「New Block Page」を設定しました。「US Headquarters」のダッシュボードで移動すると、デフォルト ポリシーで新しいブロック リストが有効になっています。

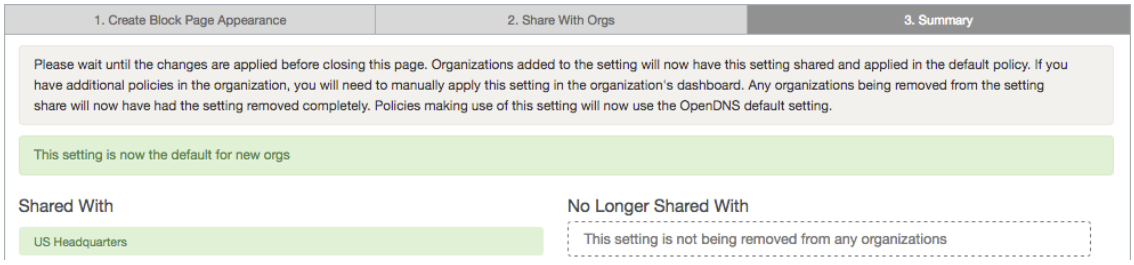
最初は「デフォルト」として表示されます。

そしてデフォルト ポリシーで自動選択されます。



ステップ 3: 変更を確認する

最後のステップでは、行った変更を確認します。確認ページには、集中型設定ブロックページがデフォルトであるか、どのサブ組織に適用されたか、このブロック ページが適用されなくなった組織があるかどうかなど、行ったすべての変更が表示されます。



集中型カテゴリ設定

集中型カテゴリ設定は、次の手順で設定します。

1. カテゴリ設定を追加するか、デフォルトの設定を編集します。
2. カテゴリ設定を共有して、組織のデフォルト ポリシーに適用します。
3. 組織の特定のポリシーにカテゴリ設定を適用します。
4. 新しい組織を作成すると、設定が自動的に適用されます。
5. 変更を確認します。

ステップ 1:カテゴリ設定を追加するか、デフォルトの設定を編集する

1. [集中型設定(Centralized Settings)] > [カテゴリ設定(Category Settings)] に移動します。すでに設定されている集中型カテゴリ設定がリストされます。デフォルト設定から開始します。

2. [新しいカテゴリ設定の追加(Add A New Category Setting)] をクリックして最初の設定を作成し、カスタマイズを開始します。または、組織のデフォルトのカテゴリを選択します。
   集中型カテゴリの設定を行うことができる、簡単な 3 ステップのウィザードが開きます。

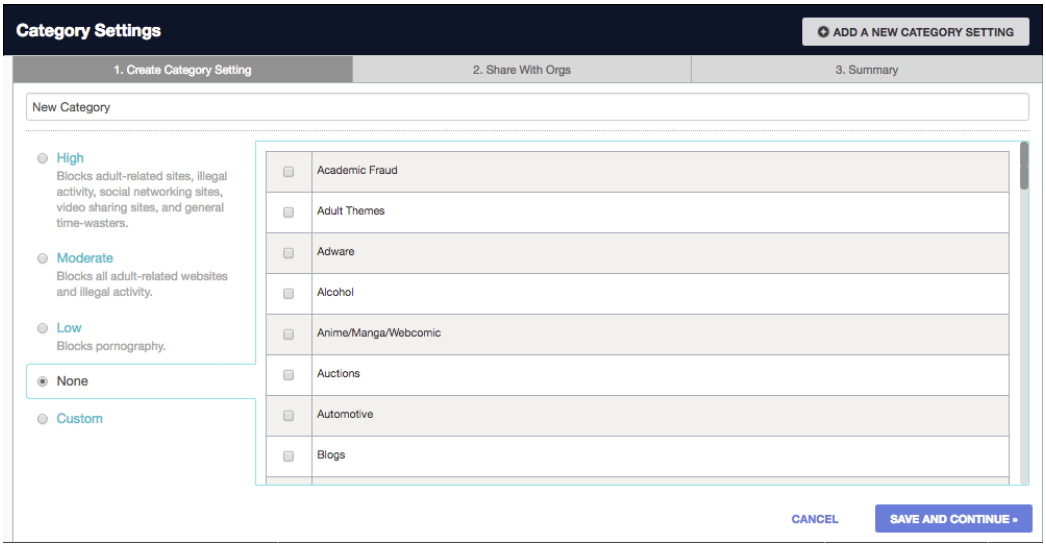
3. 新しいカテゴリ設定に意味のある名前を付けます。次に、有効にするカテゴリ設定を選択します。各カテゴリ設定とコンテンツ カテゴリの説明については、こちらを参照してください。これは、個々の組織のカテゴリ設定を作成する方法と同様です(Umbrella ダッシュボードのサブ組織内で、[ポリシー(Policies)] > [コンテンツ カテゴリ(Content Categories)]を選択します)。

デフォルトでは、ブロック対象は選択されません。[高（High）]、[中（Moderate）]、[低（Low）] の設定についてはこちらを参照してください。設定を選択して、ブロックされる関連コンテンツ設定を表示することもできます。または、自身のカテゴリ設定のカスタム セットを選択します。

注

Umbrella ダッシュボードのアクセス権を持つサブ組織の管理者は、集中型設定を見ることができますが、変更することはできません。

4. [保存して実行（Save and Continue）]をクリックします。

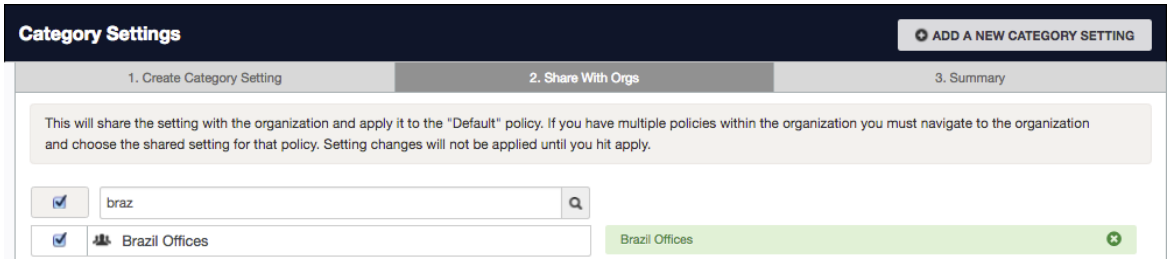


ステップ 2a：設定を共有し、組織のデフォルト ポリシーに適用する

ウィザードの次のステップでは、1 つ以上の組織とカテゴリ設定を共有します。ここには管理しているすべての組織がリストされます。この設定を適用する組織を選択します。

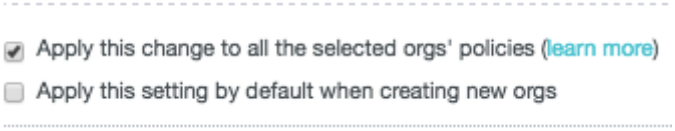
この設定の適用をスキップするには、組織を選択せずに [適用（Apply）] をクリックします。後で組織を追加することもできます。

次の例では、新しいコンテンツ設定を新しい組織のみと共有します。リスト内の特定の組織を検索することもできます。この例では、「Brazil」で検索して組織「Brazil Offices」を選択します。



ステップ 2b：組織の特定のポリシーにカテゴリ設定を適用する

ウィザードの第 2 段階の下部には、新しい設定を組織内の特定のポリシーに適用するための、2 つの重要な設定があります。



1 つ目のオプションは、この集中型設定を選択した組織のすべてのポリシーに適用することができます。ここで重要なことは、[選択したすべての組織のポリシーにこの変更を適用する（Apply this change to all the selected orgs' policies）] のチェックマークが、このステップで追加された組織に対してのみ実行されるということです。対象の組織は右側の列で緑色で強調表示されます。

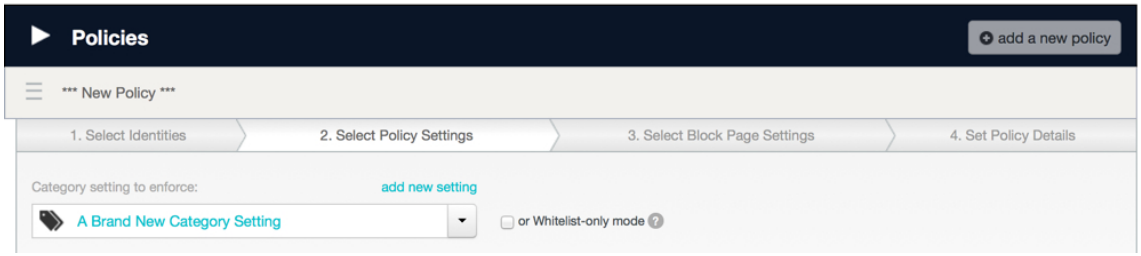
この設定をその組織に再適用するには、その組織から設定を削除し、[選択したすべての組織のポリシーにこの変更を適用する（Apply this change to all the selected orgs' policies）] をオンにして設定を再度保存します。

ステップ 2c：新しい組織を作成したら設定を自動的に適用する

2 つ目のオプションは、[新しい組織を作成する場合にデフォルトでこの設定を適用する（Apply this setting by default when creating new orgs）] オプションです。Umbrella Multi-Org Console に新しい組織を追加すると、このチェックマークが付いたカテゴリ設定が、デフォルト ポリシーに自動的に適用されます。後で集中型カテゴリ設定のリストを確認すると、このオプションを選択した集中型設定が「デフォルト」としてマークされていることがわかります。

デフォルトには 1 つのポリシーのみ設定できますが、デフォルト ポリシーを変更するには、ウィザードを再実行して、別の集中型カテゴリ設定をオンにします。デフォルトの設定は必ず設定する必要があり、デフォルトとして別のポリシーを設定するまでは、デフォルト設定を削除することはできません。

上記の例では、「Brazil Offices」という組織に、カテゴリ設定 [新しいカテゴリ設定（Brand New Category Setting）] を作成しました。「Brazil Offices」の Umbrella ダッシュボード内を移動すると、デフォルト ポリシーで新しいカテゴリ設定が有効になります。



ステップ 3: 変更を確認する

最後のステップでは、行った変更を確認します。確認ページには、集中型設定がデフォルトであるか、どの組織に適用されたか、この設定が適用されなくなった組織があるかどうかなど、行ったすべての変更が表示されます。

集中型セキュリティ設定

集中型セキュリティ設定は、次の手順で設定します。

1. セキュリティ設定を追加するか、デフォルトの設定を編集します。
2. セキュリティ設定を共有し、組織のデフォルト ポリシーに適用します。
3. セキュリティ設定を組織のポリシーに適用します。
4. 新しい組織を作成すると、設定が自動的に適用されます。
5. 変更を確認します。

ステップ 1: セキュリティ設定を追加するか、デフォルトの設定を編集する

1. [集中型設定（Centralized Settings）] > [セキュリティ設定（Security Settings）] に移動します。すでに設定されている集中型セキュリティ設定がリストされます。デフォルト設定から開始します。

2. [新しいセキュリティ設定の追加（Add A New Security Setting）] をクリックして最初の集中型セキュリティ設定を作成し、カスタマイズを開始します。または、すでに存在するデフォルトのセキュリティ設定を選択します。

集中型セキュリティ設定を行うことができる、簡単な 3 ステップのウィザードが開きます。

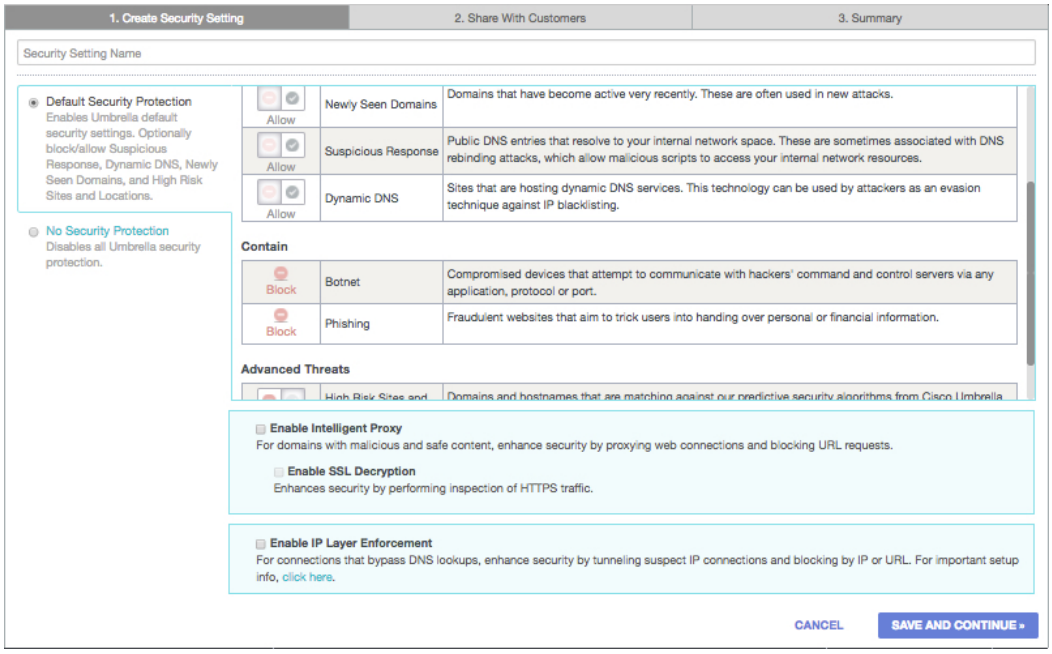
3. 新しいセキュリティ設定に意味のある名前を付けます。

4. 次に、有効にするセキュリティ設定を選択します。各セキュリティの優先順位の説明については、こちらを参照してください。これは、個々の組織のセキュリティ設定を作成する方法と同様です（Umbrella ダッシュボードの個々の組織内で、[ポリシー（Policies）] > [セキュリティ設定（Security Settings）] を選択します）。

デフォルトでは、これらの設定をそのままにすることをお勧めします。ただし、組織ごとに異なる設定を作成する場合は、マルウェア、フィッシング、ボットネット、およびその他セキュリティ上の脅威の防御を目的とした組織のニーズに応じて、中央から設定を変更することもできます。次のイメージは、デフォルトのセキュリティ防御を示しています。[新しく検出されたドメイン（Newly Seen Domains）]、[疑わしい応答（Suspicious Response）]、[ダイナミック DNS（Dynamic DNS）]、[高リスクのサイトおよびロケーション（High Risk Sites and Locations）] を変更できます。

注

Umbrella ダッシュボードのアクセス権を持つサブ組織の管理者は、集中型設定を見ることができますが、変更することはできません。



5. ページの下部で、これらのセキュリティ強化から 1 つ以上選択できます。
    - [インテリジェント プロキシの有効化（Enable IntelligentProxy）]：Web 接続のプロキシを行い、URL 要求をブロックします。
    - [SSL 復号化の有効化（Enable SSLDecryption）]：HTTPS トラフィックを検査します。
    - [IP レイヤ適用の有効化（Enable IP LayerEnforcement）]：疑わしい IP 接続をトンネルし、IP または URL によってブロックします。

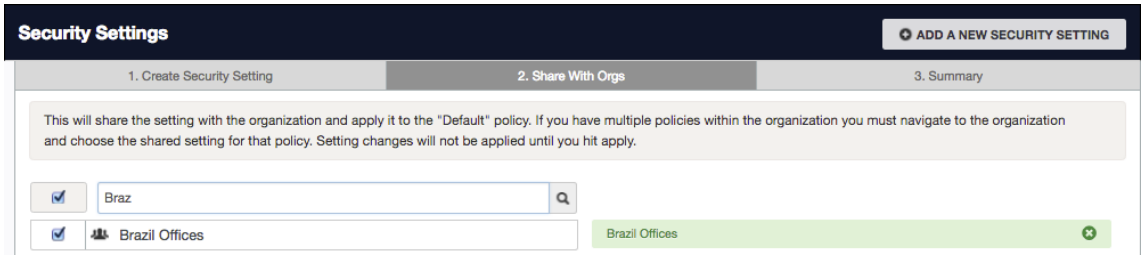
6. [保存して続行（Save and Continue）] をクリックします。

ステップ 2a：セキュリティ設定を共有し、組織のデフォルト ポリシーに適用する

ウィザードの次のステップでは、1 つ以上の組織とセキュリティ設定を共有します。ここには管理しているすべての組織がリストされます。このセキュリティ設定を適用する組織を選択します。

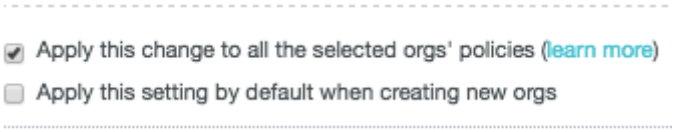
このセキュリティ設定の適用をスキップするには、組織を選択せずに [適用して続行（Apply And Continue）] をクリックします。後で組織を追加することもできます。

次の例では、新しいセキュリティ設定を新しい組織のみと共有します。リスト内の特定の組織を検索することもできます。この例では、「Braz」で検索して組織「Brazil Offices」が得られました。



ステップ 2b：セキュリティ設定を組織のポリシーに適用する

ウィザードの第 2 ステップの下部には、新しい設定を組織内の特定のポリシーに適用するための、2 つの重要な設定があります。



1 つ目のオプションは、この集中型設定を選択した組織のすべてのポリシーに適用することができます。ここで重要なことは、[選択したすべての組織のポリシーにこの変更を適用する（Apply this change to all the selected orgs' policies）] のチェックマークが、このステップで追加された組織に対してのみ実行されるということです。対象の組織は右側の列で緑色で強調表示されます。

この設定をその組織に再適用するには、その組織から設定を削除し、[選択したすべての組織のポリシーにこの変更を適用する（Apply this change to all the selected orgs' policies）] をオンにして設定を再度共有します。

ステップ 2c：新しい組織を作成したら設定を自動的に適用する

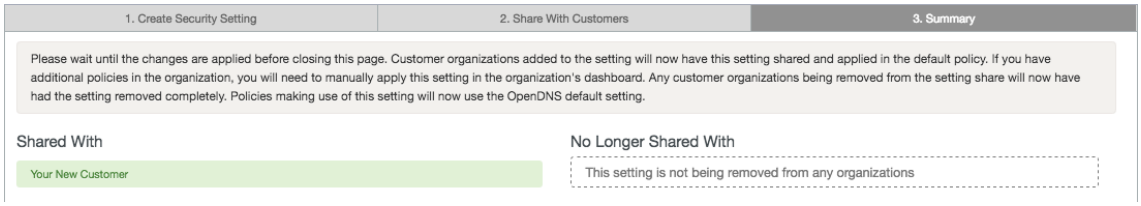
2 つ目のオプションは、[新しい組織を作成する場合にデフォルトでこの設定を適用する（Apply this setting by default when creating new orgs）] オプションです。新しい組織を追加すると、このチェックマークが付いたセキュリティ設定が、デフォルト ポリシーに自動的に適用されます。後で集中型セキュリティ設定のリストを確認すると、このオプションを選択した集中型設定が「デフォルト」としてマークされていることがわかります。

デフォルトには 1 つのポリシーのみ設定できますが、デフォルト ポリシーを変更するには、ウィザードを再実行して、別の集中型セキュリティ設定をオンにします。デフォルトのポリシーは必ず設定する必要があり、デフォルトとして別のポリシーを設定するまでは、デフォルト設定を削除することはできません。

たとえば上記の例では、「Brazil Offices」という組織に、セキュリティ設定 [新しいセキュリティ設定（Brand New Security Setting）] を作成しました。「Brazil Offices」のダッシュボード内を移動すると、デフォルト ポリシーで新しいセキュリティ設定が有効になります。

ステップ 3: 変更を確認する

最後のステップでは、行った変更を確認します。確認ページには、集中型設定がデフォルトであるか、どの組織に適用されたか、この設定が適用されなくなった組織があるかどうかなど、行ったすべての変更が表示されます。



Cisco Umbrella Multi-Org Console の概要 > **集中型設定** > 集中型レポート