Cisco Security Connector ストーリー ガイド v1

最終更新日:2018 年 1 月 24 日

このデモンストレーションについて

このストーリー ガイドは、お客様に興味を持っていただけるように、お客様の立場に立って、簡潔に作成されています。このデモを提示するために必要な時間は、対象者、その要件、および必要とされる詳細レベルに応じて異なります。さまざまなデモのシナリオが概説されており、必要に応じてさらに詳しく説明することができます。

Cisco Security Connector(CSC)はさまざまなシスコ テクノロジーを組み合わせたものですが、このデモでは、このソリューションに関連する分野にのみ焦点を当てています。各テクノロジーのより詳細な専用デモについては、以下の dCloud にあるそれぞれのインスタント デモを参照してください。

- Cisco Umbrella
- Cisco AMP for Endpoints
- Meraki Systems Manager

目標設定 – デモンストレーションの目的

このストーリー ガイドは、以下のシナリオで構成されます。

- **シナリオ 1**:危険なネットワーク アクティビティをブロックする CSC で保護されている iOS ユーザにすぐにもたらされる価値について説明します。
- **シナリオ 2**:Cisco Umbrella ダッシュボードによる、ネットワーク アクティビティの可視性について説明します。
- **シナリオ 3**:Cisco Clarity ダッシュボードによる、ネットワーク アクティビティの可視性について説明します。
- **シナリオ 4**:Umbrella ダッシュボードによる、モバイル デバイスのポリシー適用について説明します。
- **シナリオ 5**:Meraki Systems Manager ダッシュボードでの CSC のプロビジョニングについて説明します。*
- **シナリオ 6**:CSC アプリと iOS の設定について説明します。*

* シナリオ 5 と 6 には、ソリューションの導入と保守などの、より高度な分野が含まれています。対象者がこれらのシナリオのデモンストレーションを必要とするかどうかを確認します。

このデモンストレーションでは次のことができます。

- Cisco Security Connector ソリューションを構成する各種コンポーネントと、それらが全体として提供する価値をデモンストレーションします。
- お客様に関連するコンポーネントをモジュール形式で強調し、お客さまの主要なビジネス、成果、および環境と、デモとを関連付けます。
- シンプルさを心がけ、この段階では適切でない可能性がある技術的な詳細説明を避けます。
- シンプルな管理機能に重点を置いて説明します。

デモンストレーション中は、お客様のリスク削減に関する内容を中心に話し合ってください。このガイドには、一般的な課題のサンプル、利点、関連するデモンストレーション フローも記載されています。

デモンストレーション環境に関する注意

このストーリー ガイドは、販売担当者が Cisco Security Connector の主要な機能のデモンストレーションを行う場合に使用するものです。このデモンストレーション システムでは、サード パーティ製のアプリケーションや機能に対する相互作用、サポートについては扱っていません。

このソリューションは常時利用可能なデモンストレーション環境として dCloud に構築されており、次の要素で構成されています。

- CSC アプリによって保護されている iOS デバイス（iPad）のインタラクティブなシミュレーション
- Cisco Umbrella ダッシュボード
- Cisco Clarity ダッシュボード
- Meraki Systems Manager ダッシュボード

追加メモ：

- クライアント/デバイス トラフィックをシミュレーションし、ライブ環境を表現しています。
- データは変更できません。
- データは保存できません。
- これは一貫したデモンストレーション環境です。

価値提案

Cisco Security Connector（CSC）は、Apple と共に開発されたソリューションであり、企業が所有する Apple iOS デバイス上のユーザに監視モードで保護を提供します。Apple とシスコのパートナーシップは、あらゆる場所にいる iOS ユーザの可視性と制御に企業が対応できるようにするための業界初の取り組みです。

CSC 以前の既存のソリューションは、管理者とエンドユーザの両方にとって調和のとれた方法ではなく、ギャップも残されたままです。このソリューションの例として次のものがあります。

- VPN ソリューションは、エンドユーザに影響を与え、多くの場所でインターネット アクセスを中断させ、いくつかのアプリを低速化（または中断）させ、バッテリーを消耗させます。その結果、ほとんどのエンドユーザはそれをオフにしてしまい、ネットワーク アクティビティの可視性と制御ができなくなってしまいます。監視モードで常時オンの VPN を強制しても、前述の問題が原因で現在も現実的なソリューションではありません。
- グローバル HTTP プロキシでは、すべてのアプリからのクラウド サービスへの Web 専用トラフィックをプロキシできます。プロキシでは可視性にギャップが残り、非 Web アクティビティはプロキシされないため、常時例外の非プロキシ対応アプリには管理オーバーヘッドが存在します。それに加え、エンドユーザは繰り返される認証要求に多くの時間と労力をとられます。
- カスタム ブラウザ アプリはクラウド サービスへの Web 専用トラフィックをブラウズでき、これらのアプリはデフォルトで監視モードの専用ブラウザとして適用できます。アプリは MDM を介してコンテナ化することもできます。ただし、このアプローチは、管理者とエンドユーザの両方に均等に影響を与えます。すべての非 Web アクティビティはカスタム ブラウザをバイパスし、非コンテナ化アプリまたはカスタム アプリは、管理者ユーザによる可視性または制御なしで Web 要求を送信できます。

監視モードのデバイス用に Apple が作成したまったく新しい API 機能により、CSC はエンドユーザには透過的であり、管理者ユーザには包括的な機能になります。エンドユーザは繰り返し認証することを求められず、非標準ブラウザの使用を強制されることもありません。エンドユーザはアプリ使用時の遅延や中断を経験したり、外国のコンテンツが表示されたりすることもありません。

管理者ユーザは、iOS の既存のコンテンツ フィルタリング機能に基づいて構築することにより、任意のポートまたはプロトコルを経由する任意のアプリケーションを介するすべてのネットワーク アクティビティを表示できます。管理者ユーザは、すべてのネットワーク要求のトンネリング、プロキシ、および/または復号を実行しても、アプリを中断させることはありません。

CSC は、次の 2 つの拡張をサポートします。

1. Cisco Umbrella
2. Cisco Clarity

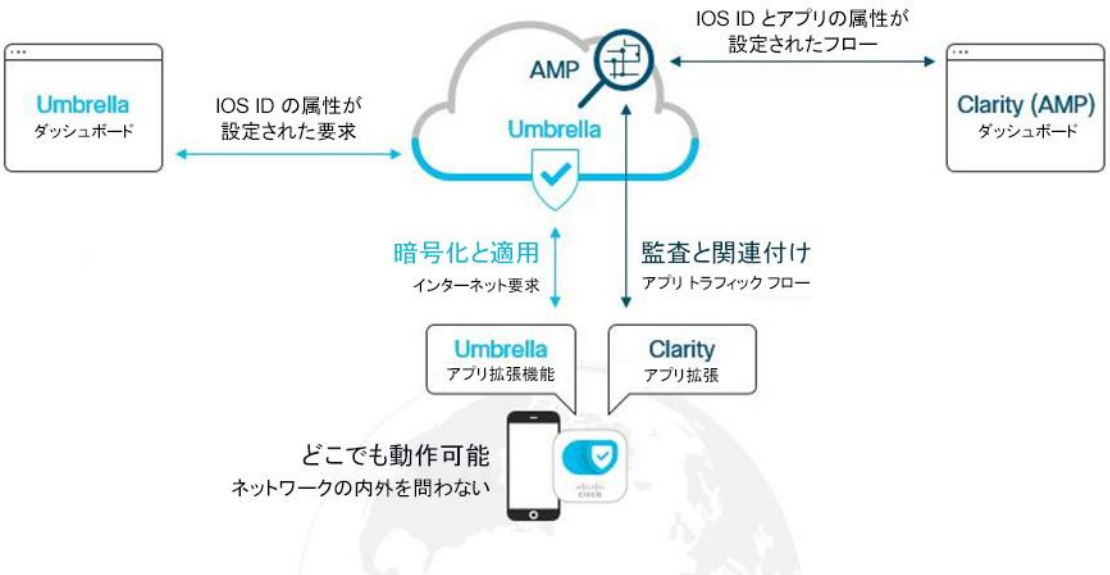
Umbrella は、ユーザがどこにいてもインターネット上の脅威を最前線で防御する、シスコのクラウド セキュリティ プラットフォームです。Umbrella は、ネットワークの内外を問わず、すべてのポートとプロトコルにわたって iOS デバイスのインターネット アクセスを保護し、どのユーザがインターネット上のどこにアクセスするかについての可視性と制御を企業に提供します。特に、Umbrella は iOS ユーザをフィッシング攻撃や悪質なサイトへの誤アクセスから保護します。逆の視点から見ると、データが悪意のある宛先へと抜き取られることを防御できます。また、インターネット要求を暗号化することでセキュリティを提供します。

このまったく新しいコネクタによって DNS 層での適用が提供され、インテリジェント プロキシを介するカスタマイズ可能な URL ブロックが可能です。管理者は Umbrella ダッシュボードでレポートを実行し、モバイル デバイス ID に基づいてポリシーを適用できます。さらに、IPv6 対応携帯電話ネットワーク経由で適用できます。

Cisco Clarity は、デバイスからのすべてのネットワーク接続への可視性を提供します。管理者は、iOS ユーザ、アプリ、およびシステム プロセスによってすべてのトラフィック フローを監査できます。特にこの可視性は、暗号化前に、iOS API を活用して SSL 復号なしで URL レベルの精度を得ることで実現します。これは証明書ピニングを使用する多くのアプリでの要件です。

加えて、Clarity はこれらのフローをアプリとデバイス トラジェクトリ ビューに関連付け、インシデント調査を容易に行えるようにします。これは他のどこにもないイノベーションです。さらに、Clarity は組織によって監視されているすべてのデバイスで使用頻度が高いアプリと低いアプリを明らかにし、管理者とセキュリティ担当者がポリシーの問題とセキュリティの異常を識別できるようにします。AMP ダッシュボードの Clarity 部分には、このまったく新しい情報を示す、iOS デバイス用の新しいアプリ トラジェクトリとレポート タブが表示されます。Umbrella と同様、可視性はすべてのポートとプロトコルに対して有効であり、IPv6 をサポートします。

図 1. Cisco Umbrella のセキュリティの適用



MDM 監視は、Apple により iOS 5 に追加され、企業所有の Windows デバイスや Mac デバイスと同じように、企業所有の iOS デバイスの制御性を大幅に向上させています。Apple はエンドユーザのプライバシーを尊重しているため、Cisco Security Connector は監視デバイス上でのみ使用できます。

Apple は、企業が現時点で監視専用機能の使用を予定していないとしても、将来、監視専用機能を利用することができるよう、デバイスのセットアップ時に監視を検討することを推奨しています。デバイスはたいていの場合、購入後すぐに、お客様の MDM にリンクされている Apple のデバイス登録プログラム（DEP）を使用して監視されます。あるいは、Apple コンフィギュレータを使用してお客様が手動で有効にすることもできます。ただし、デバイスがすでに使用中の場合、データを消去する必要があることに注意してください。

CSC の最初のリリースは Meraki Systems Manager MDM とシームレスに動作します。他については今後のリリースでサポートされる予定です。このデモンストレーションには CSC ソリューションの Umbrella、Clarity、および Meraki の各コンポーネントが含まれており、さまざまなデモンストレーション シナリオによってソリューション導入のさまざまな使用例とステージに焦点を当てています。

要約すると、CSC を使用するための前提条件は次のとおりです。

- 企業所有の Apple iOS デバイス（監視モードで iOS 11 以降を実行）。
- Apple との VPP 契約。
- モバイル デバイスを管理する MDM（Cisco Meraki Systems Manager は現在シームレスに統合されており、その他については将来統合されます）。
- 次のサブスクリプションのいずれかまたは両方。
    - Cisco Umbrella：Professional、Insights、および Platform パッケージが導入されたモバイル デバイスには追加ライセンスは不要です。
    - Cisco AMP for Endpoints：デバイスごとのライセンスと Clarity 機能のアクティベーションが必要です。

デモンストレーション プラットフォームへのアクセス

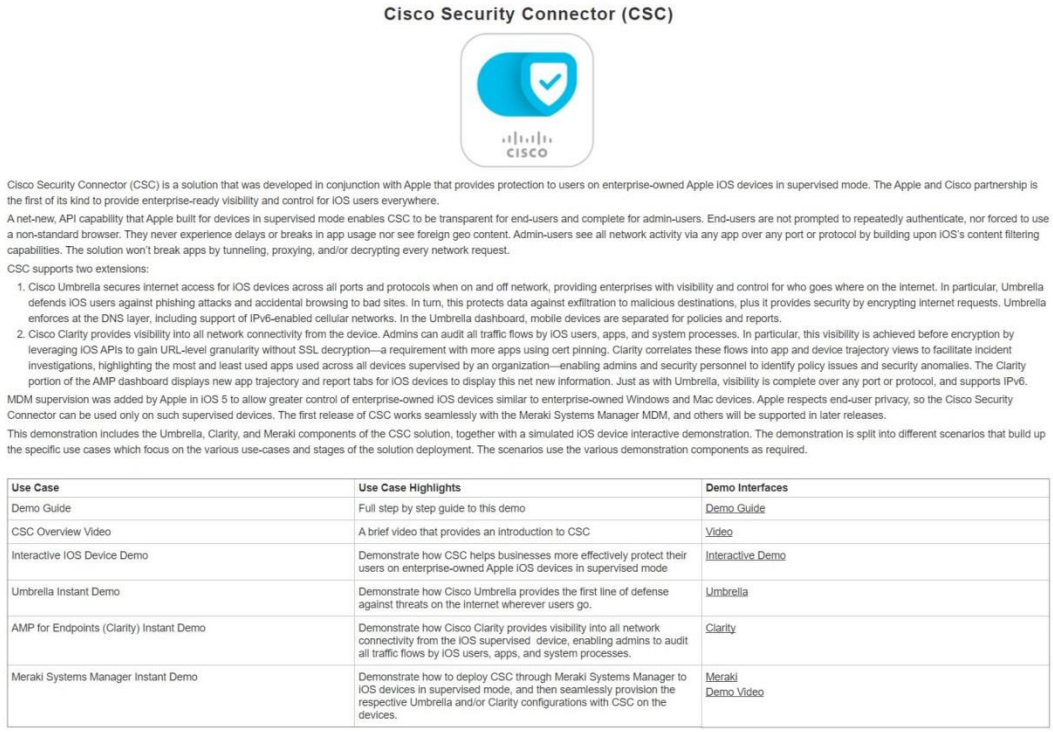
1. dCloud（dcloud.cisco.com）にログインし、自分のロケーションに最も近いデータセンターを選択します。

注：どのデータセンターも使用できますが、最寄りのデータセンターを選択することを推奨します。

注：dCloud に初めてログインする場合は、利用規約に同意する必要があります。

2. dCloud カタログから、**CSC** を検索します。結果から、[表示（View）] を選択します。CSC デモ ランディング ページが開きます。

図 2. CSC デモ ランディング ページ



Cisco Security Connector (CSC)

Cisco Security Connector (CSC) is a solution that was developed in conjunction with Apple that provides protection to users on enterprise-owned Apple iOS devices in supervised mode. The Apple and Cisco partnership is the first of its kind to provide enterprise-ready visibility and control for iOS users everywhere.

A net-new, API capability that Apple built for devices in supervised mode enables CSC to be transparent for end-users and complete for admin-users. End-users are not prompted to repeatedly authenticate, nor forced to use a non-standard browser. They never experience delays or breaks in app usage nor see foreign geo content. Admin-users see all network activity via any app over any port or protocol by building upon iOS's content filtering capabilities. The solution won't break apps by tunneling, proxying, and/or decrypting every network request.

CSC supports two extensions:

1. Cisco Umbrella secures internet access for iOS devices across all ports and protocols when on and off network, providing enterprises with visibility and control for who goes where on the internet. In particular, Umbrella defends iOS users against phishing attacks and accidental browsing to bad sites. In turn, this protects data against exfiltration to malicious destinations, plus it provides security by encrypting internet requests. Umbrella enforces at the DNS layer, including support of IPv6-enabled cellular networks. In the Umbrella dashboard, mobile devices are separated for policies and reports.
2. Cisco Clarity provides visibility into all network connectivity from the device. Admins can audit all traffic flows by iOS users, apps, and system processes. In particular, this visibility is achieved before encryption by leveraging iOS APIs to gain URL-level granularity without SSL decryption—a requirement with more apps using cert pinning. Clarity correlates these flows into app and device trajectory views to facilitate incident investigations, highlighting the most and least used apps used across all devices supervised by an organization—enabling admins and security personnel to identify policy issues and security anomalies. The Clarity portion of the AMP dashboard displays new app trajectory and report tabs for iOS devices to display this net new information. Just as with Umbrella, visibility is complete over any port or protocol, and supports IPv6.

MDM supervision was added by Apple in iOS 5 to allow greater control of enterprise-owned iOS devices similar to enterprise-owned Windows and Mac devices. Apple respects end-user privacy, so the Cisco Security Connector can be used only on such supervised devices. The first release of CSC works seamlessly with the Meraki Systems Manager MDM, and others will be supported in later releases.

This demonstration includes the Umbrella, Clarity, and Meraki components of the CSC solution, together with a simulated iOS device interactive demonstration. The demonstration is split into different scenarios that build up the specific use cases which focus on the various use-cases and stages of the solution deployment. The scenarios use the various demonstration components as required.

Use Case	Use Case Highlights	Demo Interfaces
Demo Guide	Full step by step guide to this demo	Demo Guide
CSC Overview Video	A brief video that provides an introduction to CSC	Video
Interactive IOS Device Demo	Demonstrate how CSC helps businesses more effectively protect their users on enterprise-owned Apple iOS devices in supervised mode	Interactive Demo
Umbrella Instant Demo	Demonstrate how Cisco Umbrella provides the first line of defense against threats on the internet wherever users go.	Umbrella
AMP for Endpoints (Clarity) Instant Demo	Demonstrate how Cisco Clarity provides visibility into all network connectivity from the iOS supervised device, enabling admins to audit all traffic flows by iOS users, apps, and system processes.	Clarity
Meraki Systems Manager Instant Demo	Demonstrate how to deploy CSC through Meraki Systems Manager to iOS devices in supervised mode, and then seamlessly provision the respective Umbrella and/or Clarity configurations with CSC on the devices.	Meraki Demo Video

3. これで CSC デモ環境に直接ログインしていることになります。

4. デモに進む前に、CSC ソリューションの概要を示す CSC の概要ビデオ（6 分間の情報ビデオ）を再生します。このビデオは、デモ ランディング ページの表のリンクから再生します。またはこのリンクから直接アクセスすることもできます。

図 3. CSC デモ ランディング ページからの概要ビデオの起動

Use Case	Use Case Highlights	Demo Interfaces
Demo Guide	Full step by step guide to this demo	Demo Guide
CSC Overview Video	A brief video that provides an introduction to CSC	Video
Interactive IOS Device Demo	Demonstrate how CSC helps businesses more effectively protect their users on enterprise-owned Apple iOS devices in supervised mode	Interactive Demo
Umbrella Instant Demo	Demonstrate how Cisco Umbrella provides the first line of defense against threats on the internet wherever users go.	Umbrella
AMP for Endpoints (Clarity) Instant Demo	Demonstrate how Cisco Clarity provides visibility into all network connectivity from the iOS supervised device, enabling admins to audit all traffic flows by iOS users, apps, and system processes.	Clarity
Meraki Systems Manager Instant Demo	Demonstrate how to deploy CSC through Meraki Systems Manager to iOS devices in supervised mode, and then seamlessly provision the respective Umbrella and/or Clarity configurations with CSC on the devices.	Meraki Demo Video

5. ビデオを見た後に、デモのシナリオを続行します。シナリオのリストについては、上記の目次を参照してください。

このデモは、シナリオを個別にデモンストレーションできるモジュラ方式で構築されています。すべてのシナリオのデモンストレーションを実行する場合は、このデモ ガイドの順序に従うことをお勧めします。

シナリオ 1.　CSC により保護される iOS ユーザ

このシナリオは、CSC ソリューションの高い価値をエンドユーザの視点から示します。このシナリオでは、iOS デバイス（Apple iPad）のインタラクティブ デモを利用し、エンドユーザの操作をシミュレートすることになります。このデモの 1 つの主要な目的は、CSC が提供する簡単で透過的かつ効果的なソリューションを強調することです。このインタラクティブ デモにより、Umbrella がデバイスに提供する主要なセキュリティ機能について自分自身が習熟できると同時に、このソリューションによってエンド ユーザ エクスペリエンスが影響を受けないということに焦点を当てて説明することができます。

このシナリオでは、iPad でメッセージを受け取ったエンドユーザのシミュレーションを実行することができます。また、Umbrella にブロックされる宛先へのリンク（下記）も提供されます。

- フィッシング先へのリンク：フィッシング攻撃からユーザを保護することの価値を説明します。
- 特定の URL へのリンク：別の場所から送信された可能性があるカスタム URL をブロックすることの価値を説明します。この機能は、Umbrella のインテリジェント プロキシを使用します。
- ブロック カテゴリへのリンク：デバイスでギャンブル サイトなどの望ましくないまたは不適切なコンテンツへのアクセスを防止することの価値を示します。

手順

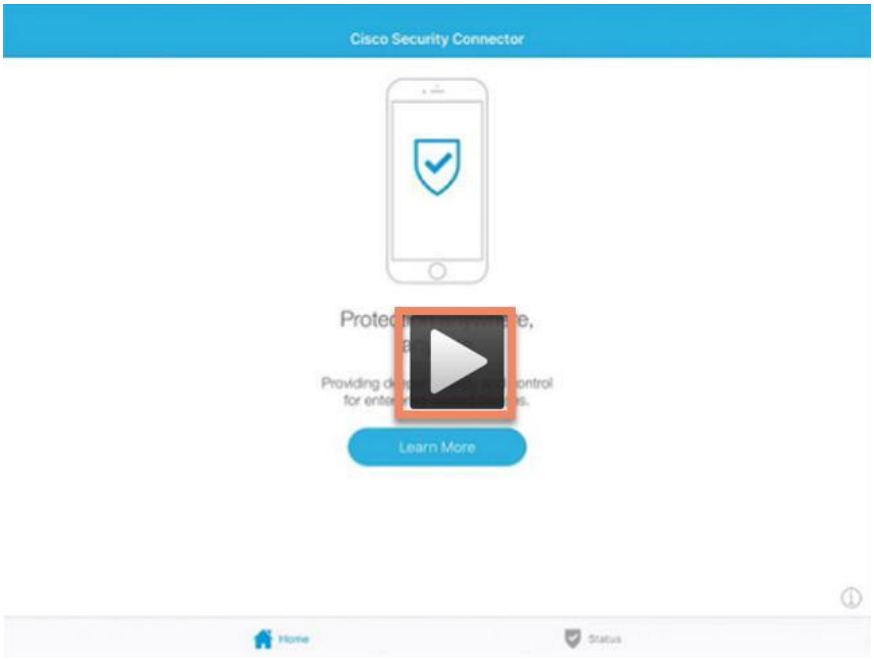
1. CSC デモ ランディング ページから、[インタラクティブ デモ（Interactive Demo）] をクリックして、インタラクティブ デモを起動します。

図 4.　CSC デモ ランディング ページ

Use Case	Use Case Highlights	Demo Interfaces
Demo Guide	Full step by step guide to this demo	Demo Guide
CSC Overview Video	A brief video that provides an introduction to CSC	Video
Interactive IOS Device Demo	Demonstrate how CSC helps businesses more effectively protect their users on enterprise-owned Apple iOS devices in supervised mode	Interactive Demo
Umbrella Instant Demo	Demonstrate how Cisco Umbrella provides the first line of defense against threats on the internet wherever users go.	Umbrella
AMP for Endpoints (Clarity) Instant Demo	Demonstrate how Cisco Clarity provides visibility into all network connectivity from the iOS supervised device, enabling admins to audit all traffic flows by iOS users, apps, and system processes.	Clarity
Meraki Systems Manager Instant Demo	Demonstrate how to deploy CSC through Meraki Systems Manager to iOS devices in supervised mode, and then seamlessly provision the respective Umbrella and/or Clarity configurations with CSC on the devices.	Meraki Demo Video

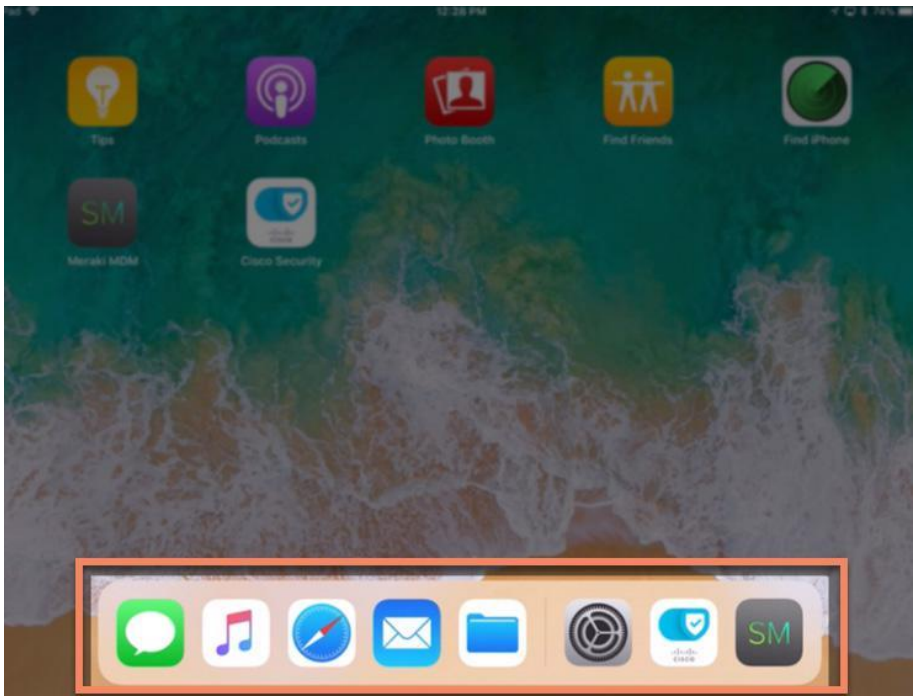
2. iOS デバイスのインタラクティブ デモが、新しいブラウザ タブで起動します。デモを開始するには、[再生（Play）] ボタンをクリックするか、またはブラウザ ウィンドウ内の任意の場所をクリックします。

図 5. インタラクティブ デモの開始ウィンドウ



3. iPad のホーム画面が表示されます。画面下部のドック領域以外はグレーアウトされます。

図 6. ドックを強調する iPad ホーム画面

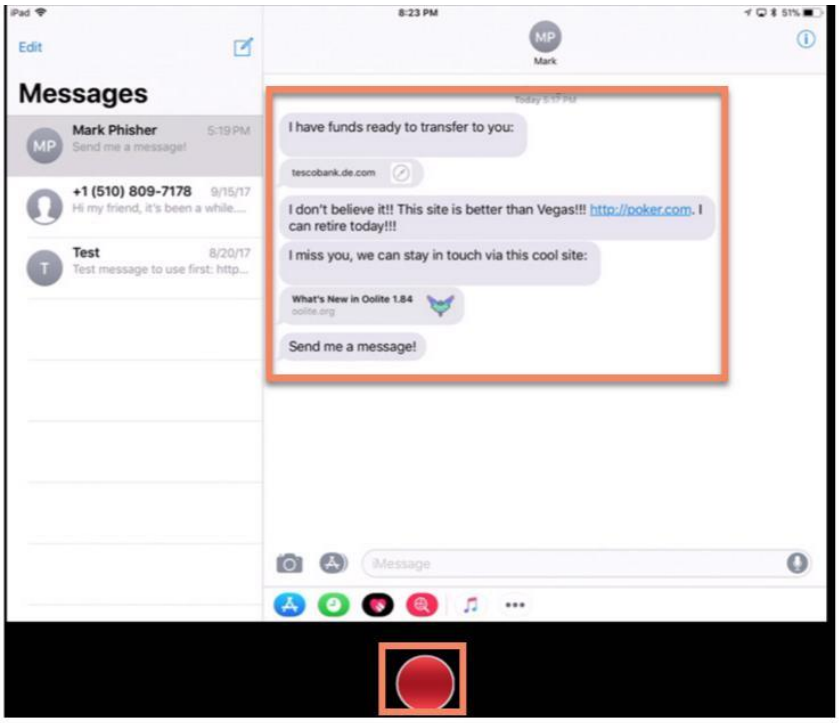


4. ドック領域から、左側の緑色の [メッセージ（Messages）] アプリ アイコンをクリックします。

図 7. メッセージ アプリ

5. メッセージ アプリが起動し、右側の領域にデモで使用されるメッセージが表示されます。

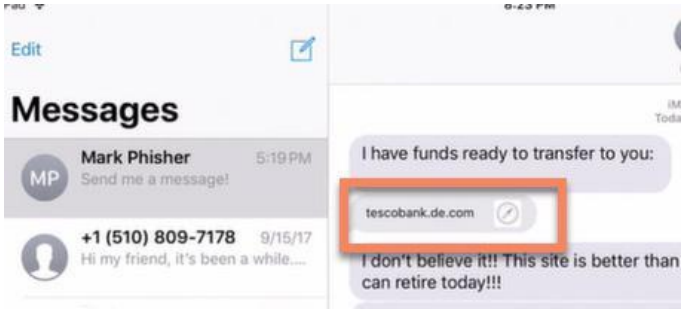
図 8. メッセージ アプリ



ヒント：インタラクティブ デモに赤のホーム ボタンが表示されるときは、クリックして iPad のホーム画面に戻ることができます。

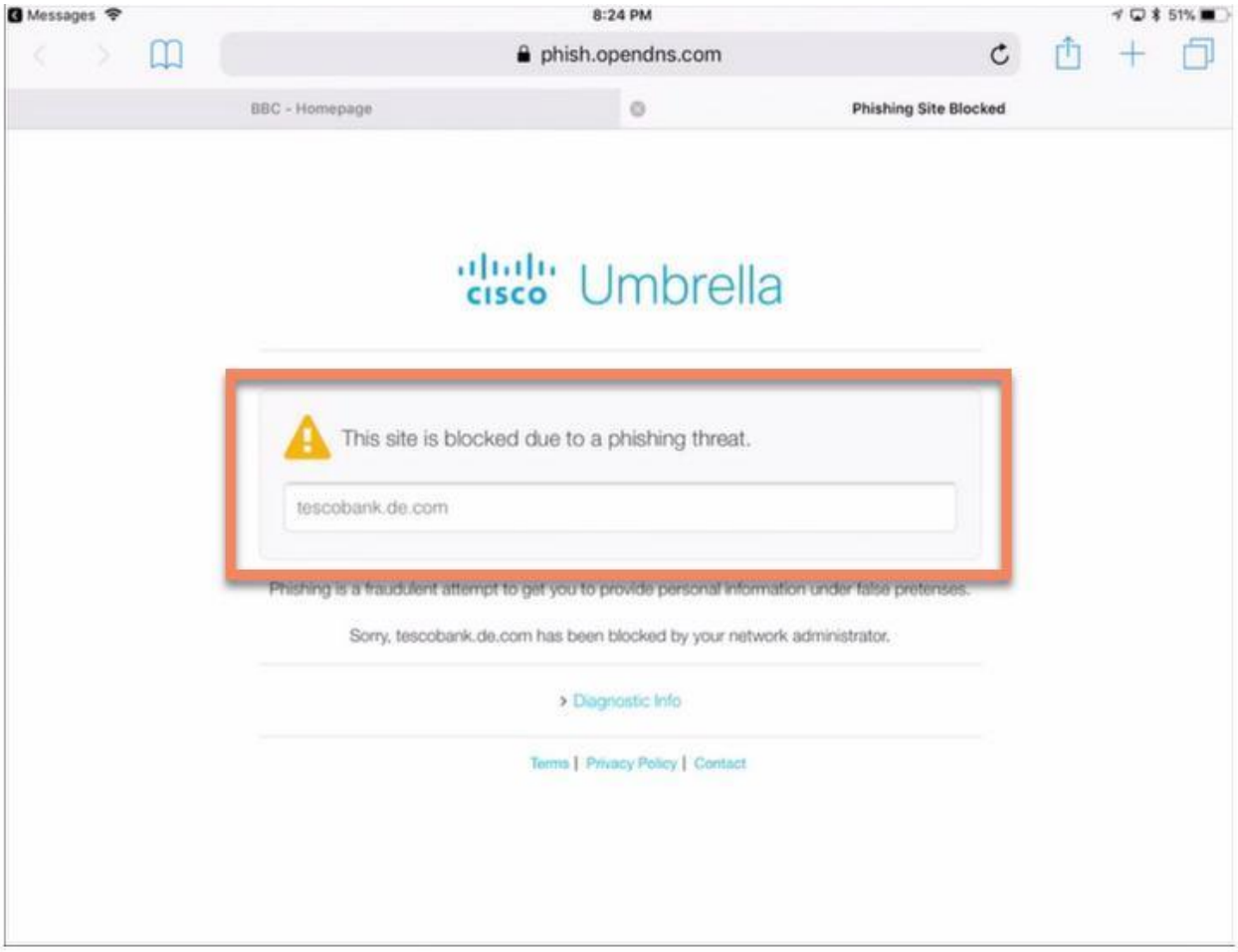
6. tescobank.de.com を指す最初のリンクをクリックします。これはフィッシング リンクです。

図 9. フィッシング リンク



7. ユーザはこのフィッシング攻撃から保護され、iPad ブラウザで Umbrella のブロック ページにリダイレクトされます。

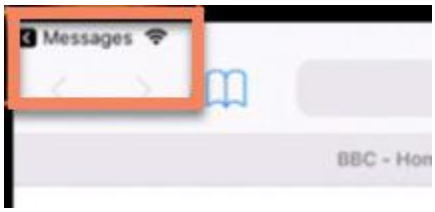
図 10. フィッシング ブロック ページ



注:エンドユーザ エクスペリエンスには(ブロック以外の)影響はなく、ページはすばやく読み込まれます。これらのブロック ページはポリシーごとにカスタマイズ可能であり、フィッシング、コンテンツ カテゴリ、およびカスタム宛先リストなどの異なるブロック タイプごとに、異なるブロック ページを表示できます。

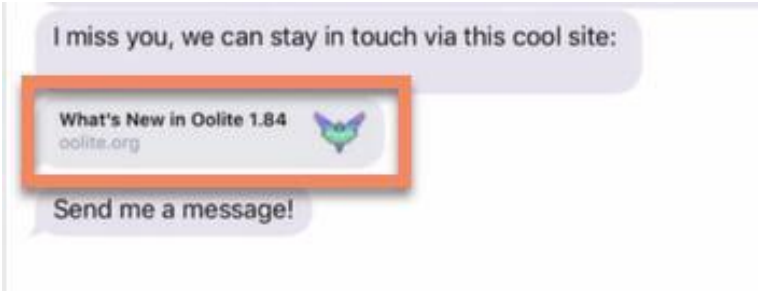
8. iPad 画面左上にあるショートカットを使用して、メッセージ ページに戻ります。

図 11. メッセージに戻るためのショートカット



9. メッセージ アプリに戻って、[Oolite 1.8.4 の新機能（What's New in Oolite 1.8.4）] リンクをクリックします。これは企業管理者によってブロック リストに追加されたカスタム URL（oolite.org/whatsnew）の例であり、たいていは悪意のある URL のリストに基づいています。

図 12. Oolite リンク



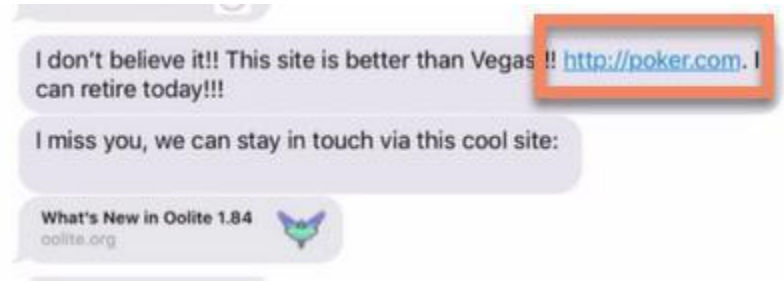
10. この要求もブロックされ、ブロック ページがデバイス上のブラウザで表示されます。

注：ブロック ページは、サイトが Umbrella のインテリジェント プロキシでブロックされたことを示します。

11. 画面左上にあるショートカットを使用して、メッセージ アプリに戻ります。

12. メッセージ アプリに戻って、**poker.com** へのリンクをクリックします。これはギャンブル サイトであり、企業によってブロックされているカテゴリです。再度、iPad ブラウザにそれぞれのブロック ページが表示されます。

図 13. Poker リンク



注：ブロック ページは、サイトがギャンブルとして分類されたためにブロックされたことを示します。

13. デモ ランディング ページに戻って、次のデモ シナリオを続行します。他のデモ シナリオのために、インタラクティブ デモが表示されたブラウザ タブは開いたままにしておきます。

シナリオ 2.　Cisco Umbrella ダッシュボードでのネットワーク アクティビティの可視性

このシナリオは、CSC がモバイル デバイスに導入されているときに、ネットワーク アクティビティがどのように Umbrella ダッシュボードに報告されるかを示します。これは、前のシナリオでデモンストレーションしたユーザ アクティビティに対応します。管理者はこれらのレポートを使用して、セキュリティ インシデントの調査を支援したり、ポリシーの適用を分析したりできます。次の概要トピックをカバーしています。

- モバイル デバイスからのすべてのネットワーク要求の検索。
- 要求されたドメインと要求の結果の詳細。
- 特定のセキュリティ イベントの詳細。
- 特定のモバイル デバイスの最近のアクティビティの詳細。

手順

14. CSC デモ ランディング ページから、[Umbrella] をクリックして Umbrella ダッシュボードを起動します。

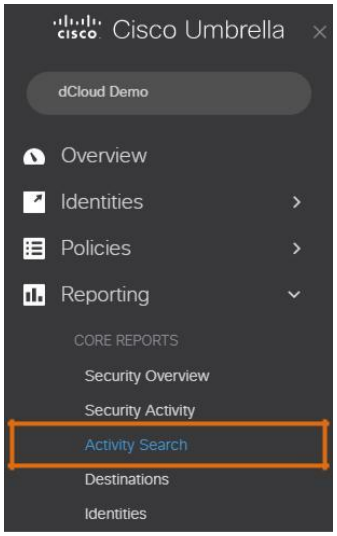
図 14. CSC デモ ランディング ページ

Use Case	Use Case Highlights	Demo Interfaces
Demo Guide	Full step by step guide to this demo	Demo Guide
CSC Overview Video	A brief video that provides an introduction to CSC	Video
Interactive IOS Device Demo	Demonstrate how CSC helps businesses more effectively protect their users on enterprise-owned Apple iOS devices in supervised mode	Interactive Demo
Umbrella Instant Demo	Demonstrate how Cisco Umbrella provides the first line of defense against threats on the internet wherever users go.	Umbrella
AMP for Endpoints (Clarity) Instant Demo	Demonstrate how Cisco Clarity provides visibility into all network connectivity from the iOS supervised device, enabling admins to audit all traffic flows by iOS users, apps, and system processes.	Clarity
Meraki Systems Manager Instant Demo	Demonstrate how to deploy CSC through Meraki Systems Manager to iOS devices in supervised mode, and then seamlessly provision the respective Umbrella and/or Clarity configurations with CSC on the devices.	Meraki Demo Video

15. Umbrella ダッシュボードが新しいブラウザ タブで起動し、[概要（Overview）] ページが表示されます。

16. 左側のナビゲーション メニューを使用して、[レポート（Reporting）] > [アクティビティ検索（Activity Search）] を選択します。

図 15. [レポート（Reporting）] > [アクティビティ検索（Activity Search）]



17. アクティビティ検索レポートが起動し、デフォルトでは直近の 24 時間のすべてのアクティビティが表示されます。モバイル デバイスのアクティビティに焦点を当てるために、左側のフィルタ領域にある [ID タイプ（Identity Type）] の下の [モバイル デバイス（Mobile Devices）] チェック ボックスを選択し、[適用（APPLY）] をクリックします。

図 16. モバイル デバイスのフィルタリング

18. それぞれの行は、モバイル デバイスからの DNS 要求を示しています。それぞれの行の次のフィールドを説明します。

    a. デバイスの ID

    b. 要求された宛先

    c. アクション（許可、ブロック、プロキシ）

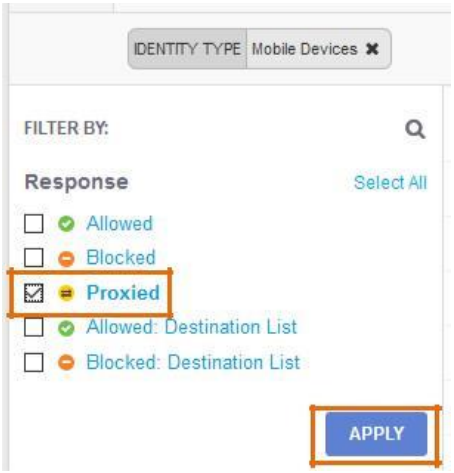
    d. カテゴリ（これは要求がブロックされた理由に関連するセキュリティ カテゴリです）

図 17. アクティビティ検索結果

Demo_iOS_1	Mobile Devices	log.umsns.com	Allowed		Jan 8, 2018 at 2:00 AM
Demo_iOS_1	Mobile Devices	ads.stickyadstv.com	Proxied		Jan 8, 2018 at 2:00 AM
Demo_iOS_1	Mobile Devices	pingma.qq.com	Allowed	Blogs, Chat, News/Media, Portals	Jan 8, 2018 at 2:00 AM
Demo_iOS_1	Mobile Devices	oolite.org	Proxied		Jan 8, 2018 at 2:00 AM
Demo_iOS_1	Mobile Devices	pingma.qq.com	Allowed	Blogs, Chat, News/Media, Portals	Jan 8, 2018 at 2:00 AM
Demo_iOS_1	Mobile Devices	oolite.org	Proxied		Jan 8, 2018 at 2:00 AM
Demo_iOS_1	Mobile Devices	cgi.connect.qq.com	Allowed	Blogs, Chat, News/Media, Portals	Jan 8, 2018 at 2:00 AM
Demo_iOS_1	Mobile Devices	assets.bounceexchange.com	Proxied		Jan 8, 2018 at 2:00 AM
Demo_iOS_1	Mobile Devices	masralarabia.com	Allowed		Jan 8, 2018 at 2:00 AM
Demo_iOS_1	Mobile Devices	wisc.edu	Allowed	Educational Institutions	Jan 8, 2018 at 2:00 AM
Demo_iOS_1	Mobile Devices	sync.search.spotxchange.com	Allowed	Business Services	Jan 8, 2018 at 2:00 AM
Demo_iOS_1	Mobile Devices	sync-jp.im-apps.net	Allowed		Jan 8, 2018 at 2:00 AM
Demo_iOS_1	Mobile Devices	t.co	Allowed	URL Shortener	Jan 8, 2018 at 2:00 AM
Demo_iOS_2	Mobile Devices	chart.apis.google.com.ref.ualibrary.org	Blocked	**Malware**	Jan 8, 2018 at 2:00 AM
Demo_iOS_2	Mobile Devices	adrta.com	Allowed	Software/Technology	Jan 8, 2018 at 2:00 AM
Demo_iOS_2	Mobile Devices	pixel.adsafeprotected.com	Allowed	Software/Technology	Jan 8, 2018 at 2:00 AM
Demo_iOS_2	Mobile Devices	insight.adsrvr.org	Proxied	Business Services	Jan 8, 2018 at 2:00 AM
Demo_iOS_2	Mobile Devices	pingma.qq.com	Allowed	Blogs, Chat, News/Media, Portals	Jan 8, 2018 at 2:00 AM
Demo_iOS_2	Mobile Devices	pingma.qq.com	Allowed	Blogs, Chat, News/Media, Portals	Jan 8, 2018 at 2:00 AM
Demo_iOS_2	Mobile Devices	www.gplexdb.com	Allowed		Jan 8, 2018 at 2:00 AM
Demo_iOS_2	Mobile Devices	use-tor.adsrvr.org	Allowed	Business Services	Jan 8, 2018 at 2:00 AM
Demo_iOS_2	Mobile Devices	timeinc.demdex.net	Allowed	Business Services	Jan 8, 2018 at 2:00 AM
Demo_iOS_1	Mobile Devices	oolite.org	Proxied		Jan 8, 2018 at 2:00 AM
Demo_iOS_1	Mobile Devices	opsen-static.dolphin-browser.com	Allowed	Software/Technology	Jan 8, 2018 at 2:00 AM
Demo_iOS_1	Mobile Devices	iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com	Blocked	**Malware, Phishing**	Jan 8, 2018 at 2:00 AM

19. [応答（Response）] の下で、左側のフィルタ領域にある [プロキシ済み（Proxied）] チェック ボックスをクリックし、[適用（APPLY）] をクリックします。

図 18. プロキシ化要求のフィルタリング

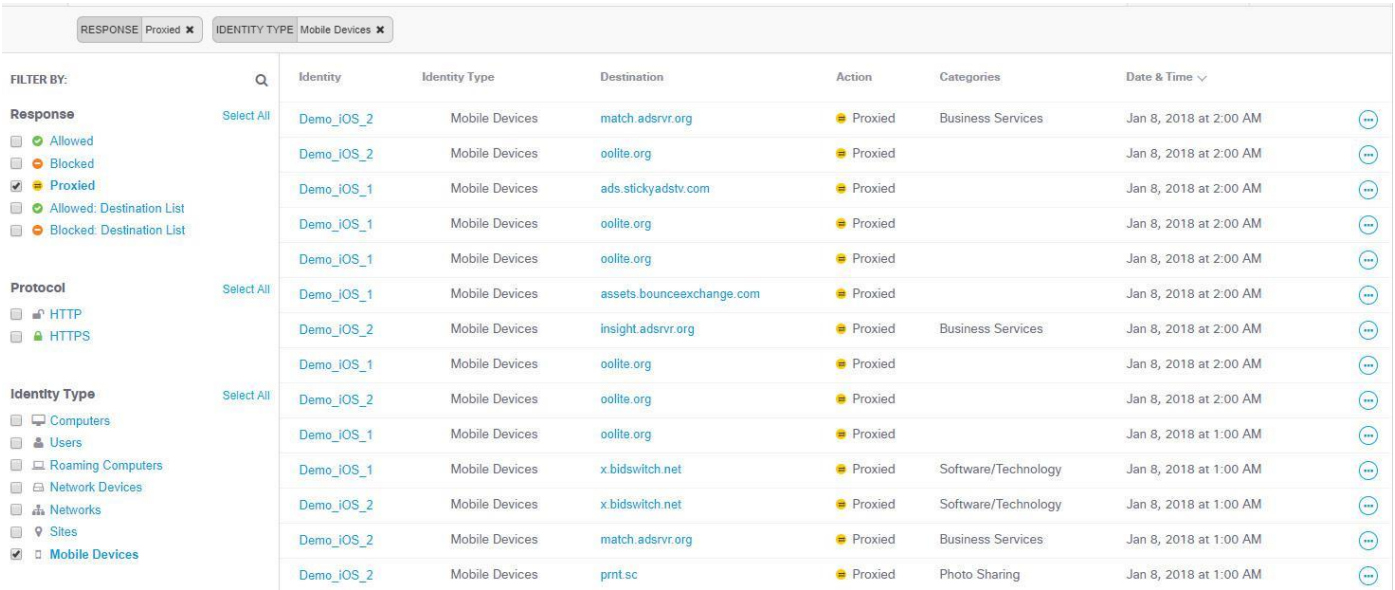


20. これで、Umbrella のインテリジェント プロキシにプロキシされた要求のみが表示されます。

ヒント：プロキシされた結果が表示されない場合は、ページ上部にあるレポートの期間を、[過去 7 日間（LAST 7 DAYS）] または [過去 30 日間（LAST 30 DAYS）] に変更します。

注：Umbrella の灰色のリスト上にあるドメインへの要求は、（URL およびファイル レベルで）さらに検査するためにプロキシされます。Umbrella のカスタム URL ブロック リストに含まれる特定の URL をホストするすべてのドメインもプロキシされます。シナリオ 1（手順 10）で oolite.org/whatsnew へのリンクをクリックすると、ブロック ページが表示され、サイトが Umbrella のインテリジェント プロキシによってブロックされたことが示されました。このアクティビティ レポートでは、これらのプロキシ化要求も表示できます。

図 19. プロキシ化要求



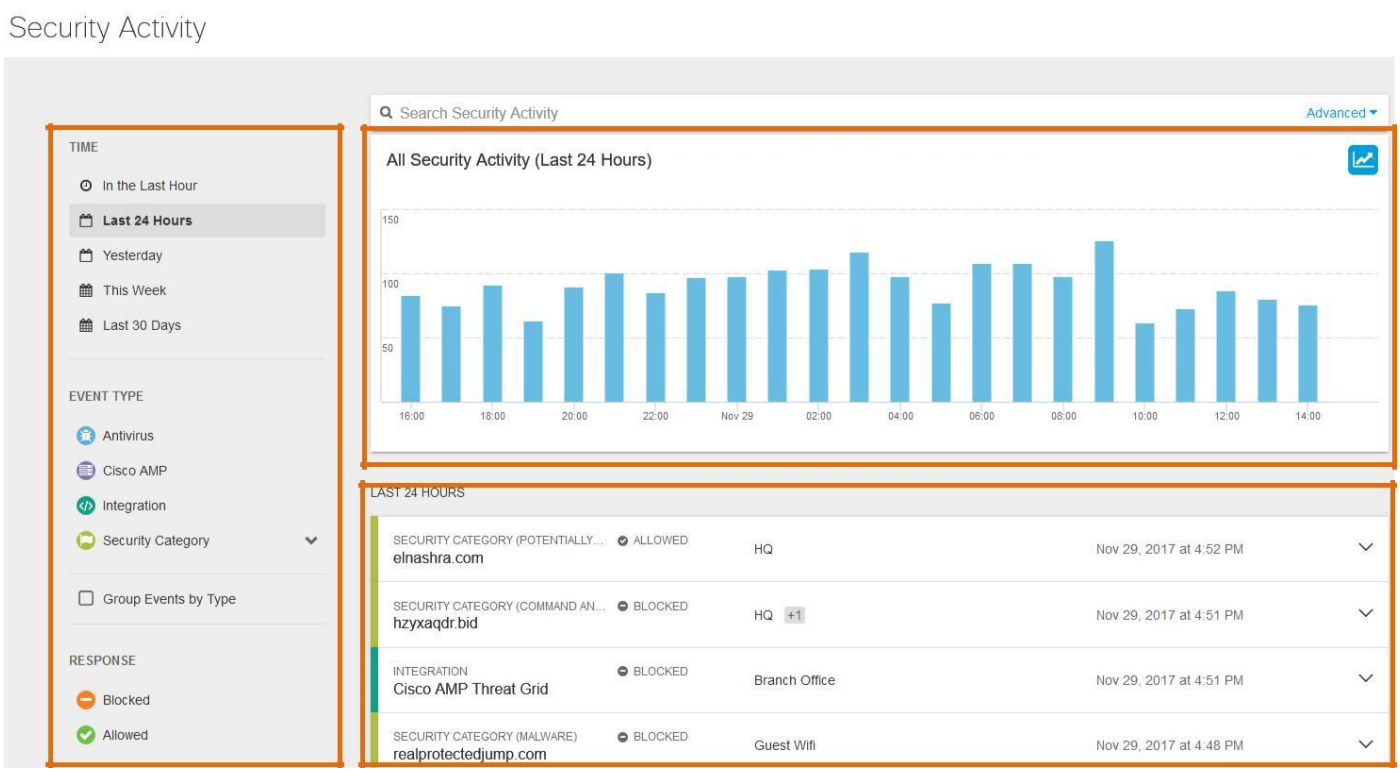
21. 要求されたドメインのいくつかのカテゴリを説明します（ある場合）。
22. ナビゲーション メニューから [レポート（Reporting）] > [セキュリティ アクティビティ（Security Activity）] を選択します。

図 20. AnyConnect Umbrella ローミング セキュリティ モジュール

23. セキュリティ アクティビティ レポートは、選択した期間に基づいて（デフォルトは直近の 24 時間）、すべてのセキュリティ関連イベントの詳細を表示します。

注：すべてのセキュリティ関連イベントがブロックされるわけではありません（ポリシーのセキュリティ カテゴリの設定に応じます）。ただし、結果に関係なくこのレポートではすべてのイベントを表示できます。

図 21. セキュリティ アクティビティ レポート



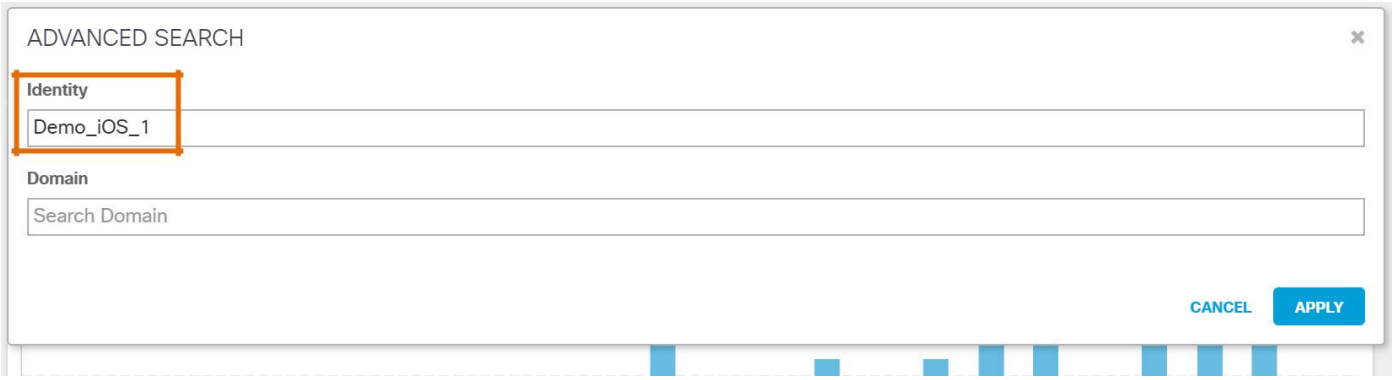
24. 上部のグラフについて説明します。これは、選択された期間にわたるセキュリティ イベントの数を示しています。直近の 24 時間に設定すると、1 時間の期間に分割されます。

25. その下に表示された領域について説明します。これは個々のイベントについて概説しています。各イベント行を展開して、イベントの完全な詳細を表示できます。
26. 左側の領域について説明します。ここでは期間を変更したり、イベント タイプまたは応答に応じてフィルタを適用できます。
27. ID タイプにはフィルタ オプションはありませんが、レポート ページ上部の [詳細（Advanced）] 領域では、特定の ID を検索できます。これはモバイル デバイスにすることもできます。[詳細（Advanced）] をクリックして、[高度な検索（ADVANCED SEARCH）] ボックスを展開します。

図 22. 高度な検索

28. [ID（Identity）] ボックスで、アクティビティ検索レポートで監視したモバイル デバイスのうち 1 つの名前の入力を開始します。たとえば **Demo_iOS_1** と入力し、[適用（APPLY）] をクリックします。

図 23. モバイル デバイスによるフィルタリング

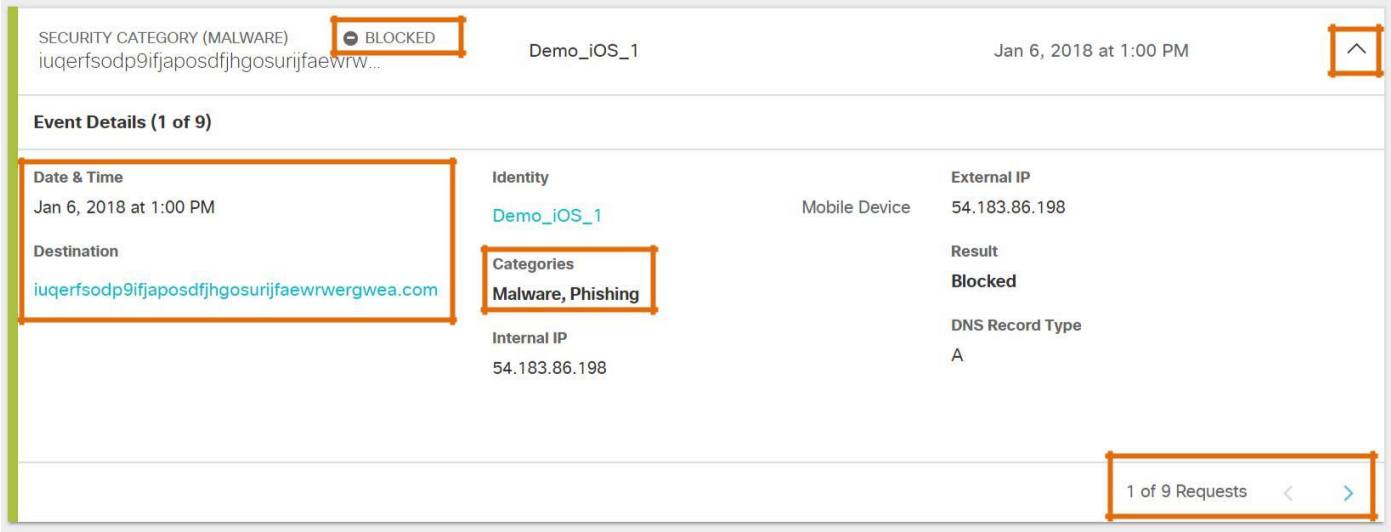


29. レポートの結果は、選択したモバイル デバイスに関連したセキュリティ イベントで更新されます。
30. 左側（フィルタ領域）のチェック ボックスを使用して、[セキュリティ カテゴリ（Security Category）] を展開します。フィッシング イベントをフィルタリングします。

図 24. フィッシング フィルタ

31. 結果の更新後に、イベントの右上の矢印から [フィッシング（Phishing）] イベントを展開します。

図 25. 展開されたフィッシング イベント



32. 展開された領域に表示されるイベントの特定の詳細を説明します。

33. このデバイスでこの宛先に複数の要求が出されている場合、右下部の領域から個々の要求をスクロールできます。各要求の日時はメイン領域に表示されます。

注：一部の宛先は、複数のセキュリティ カテゴリに分類される場合があります。上記の例では、最初に表示されたカテゴリは**マルウェア**です。そのため、フィルタリング オプションを使用せずに結果を見ただけでも、それが**フィッシング** ブロックであったと特定することはほぼありません。

34. 最後に、ナビゲーション メニューから、[レポート（Reporting）] > [ID（Identities）] をクリックします。

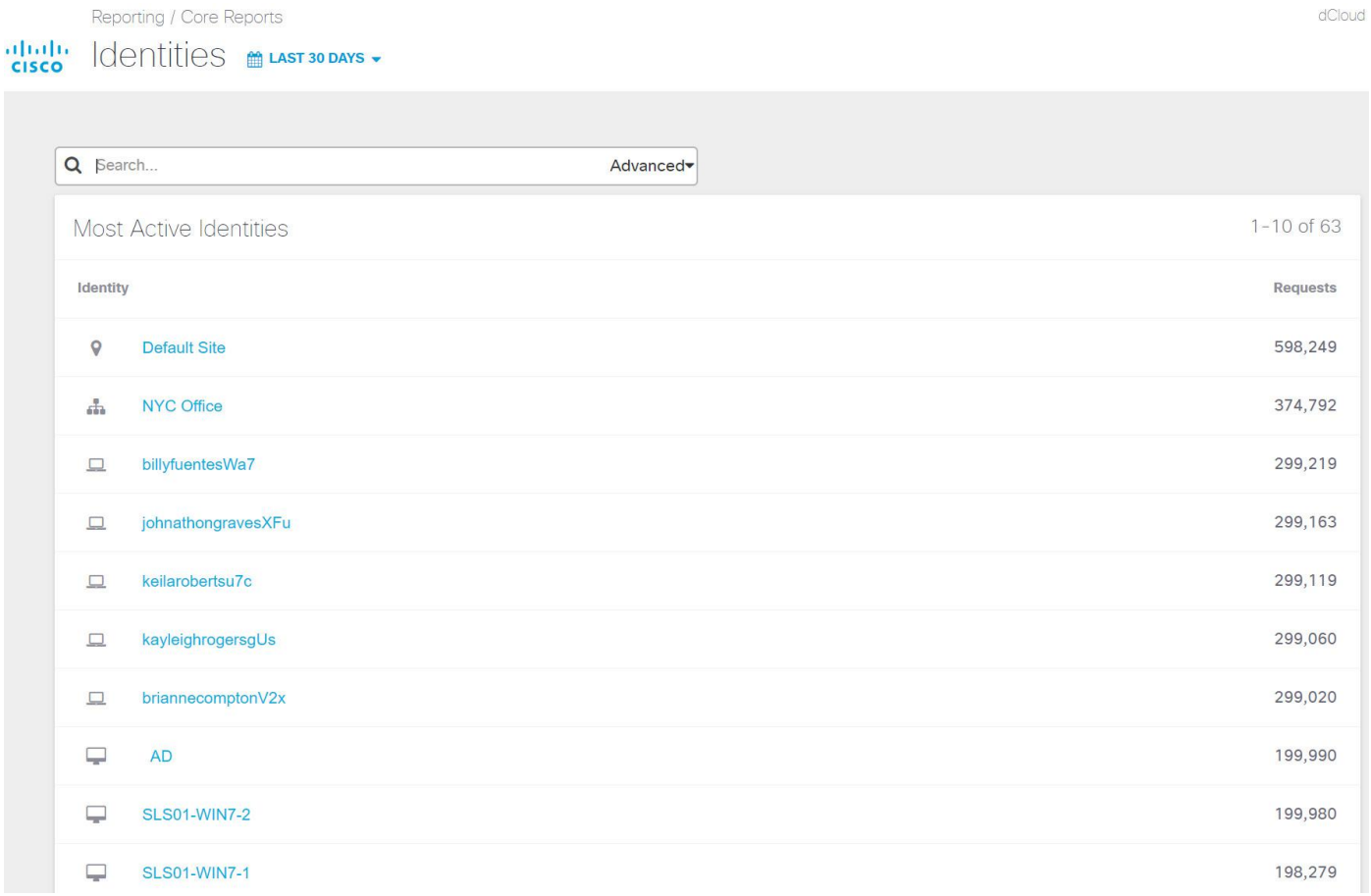
図 26. [レポート（Reporting）] > [ID（Identities）]

35. ID レポートが起動します。最近表示された ID のリストが表示されます。

注:モバイル デバイスは、初期画面に表示されていない場合があり、ページをスクロールしなければならないことがあります。

ヒント:ID のリストが長い場合、リストの上の検索ウィンドウでデバイス名の入力を開始できます。

図 27. ID レポート

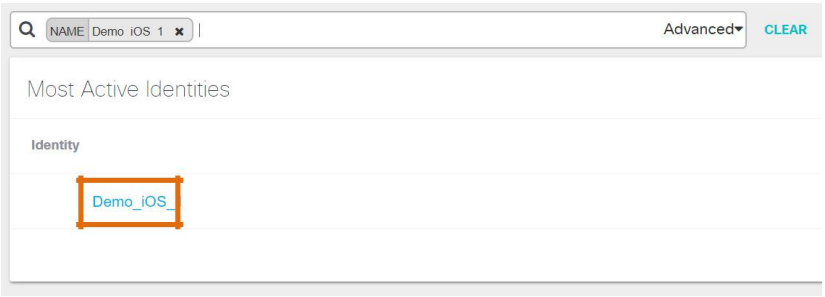


36. 前の手順ですでに使用したモバイル デバイスのいずれかの名前（demo...）の入力を開始します。これによって、最近表示された ID のリストにあるモバイル デバイスのうち 1 つがフィルタリングされます。

図 28. モバイル デバイスのフィルタリング

37. フィルタリングするモバイル デバイスの ID をクリックします。

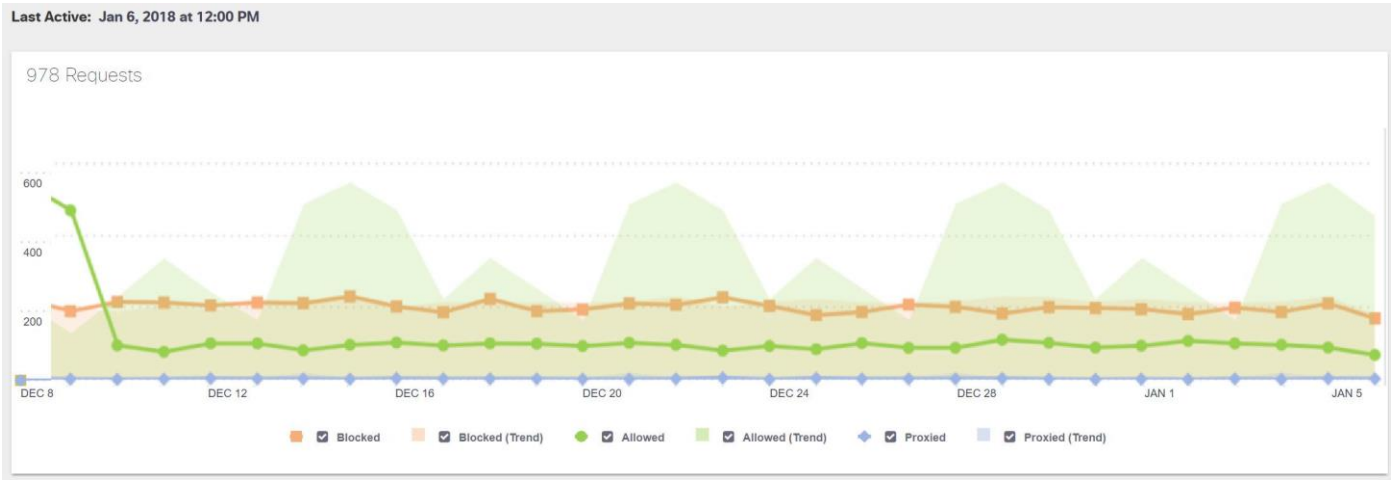
図 29. フィルタリングされたモバイル デバイス



38. モバイル デバイス用の ID レポートが起動します。以下の手順で説明されている領域について説明します。

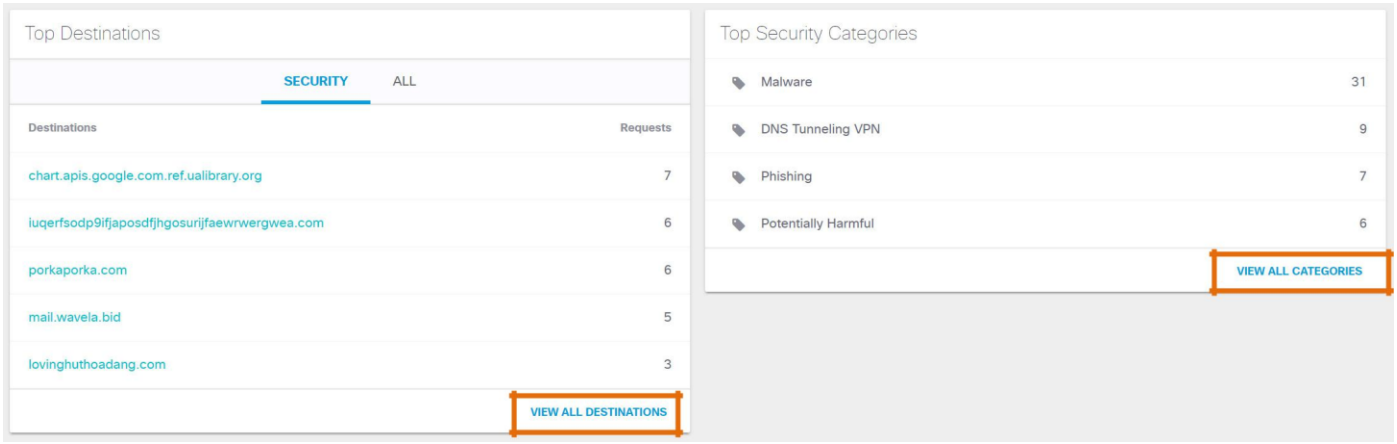
39. 上のグラフは、時間の経過に伴うすべての要求のトレンドを示し、許可、ブロック、およびプロキシ要求を区別し、それぞれのトレンドのオーバーレイを示しています。さらに、グラフ上には ID（デバイス）が最後にアクティブであった日時が示されます。

図 30. ID 要求グラフ



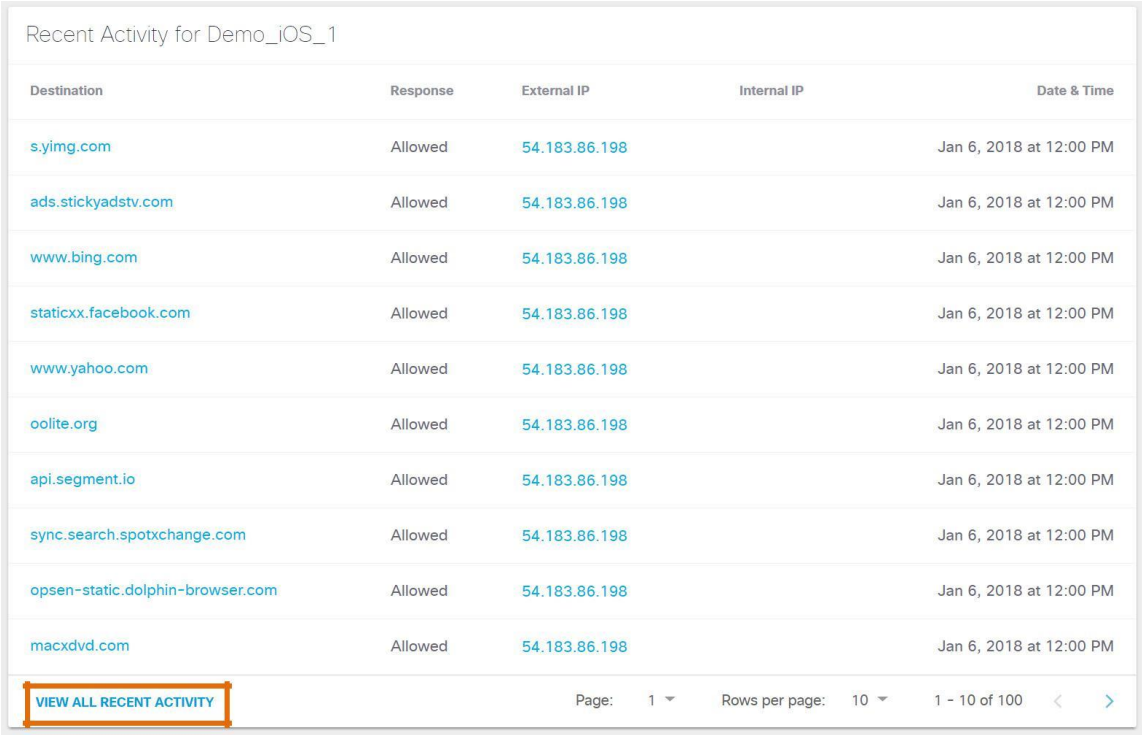
40. 次に、この ID で最近表示された上位の宛先と上位のセキュリティ カテゴリを表示します。宛先はセキュリティ関連、またはすべての宛先のいずれかにできます。宛先が宛先レポートにリンクしていることを説明します（クリックする必要はありません）。
41. これらは、「上位」の宛先とカテゴリであるに過ぎません。[すべて表示...（VIEW ALL...）] リンクでリスト全体を表示できます（クリックする必要はありません）。

図 31. 上位の宛先と上位のセキュリティ カテゴリ



42. 最後に、この ID で最近表示したすべてのアクティビティが、ID レポートの末尾にリストされます。さらに、このリストを最近のすべてのアクティビティに拡張するリンクがあります（クリックする必要はありません）。宛先をクリックすると、宛先レポートを表示できます。

図 32. ID の最近のアクティビティ



43. CSC デモ ランディング ページに戻って、次のデモ シナリオを続行します。他のデモ シナリオのために Umbrella ダッシュボードのブラウザ タブを開いたままにします。

シナリオ 3.　Cisco Clarity ダッシュボードでのネットワーク アクティビティの可視性

Cisco Security Connector（CSC）は、Umbrella と Clarity という 2 つの拡張機能に展開できます。このシナリオでは、Clarity と AMP for Endpoints ダッシュボードに対してのみ焦点を当てています。

Cisco Clarity は、AMP for Endpoints ダッシュボードの新しい部分です。これが Clarity という名前であるのは、iOS 用の Cisco Security Connector は悪意のあるファイルに焦点を当てていないためです。Cisco Clarity は、どのデバイスがアプリを使用しているか（システム プロセスを含む）、インターネット（またはイントラネット）上のどこでそれらのアプリが接続しているか、またはそれらがいつ実行されたかを把握するための可視性を提供します。

手順

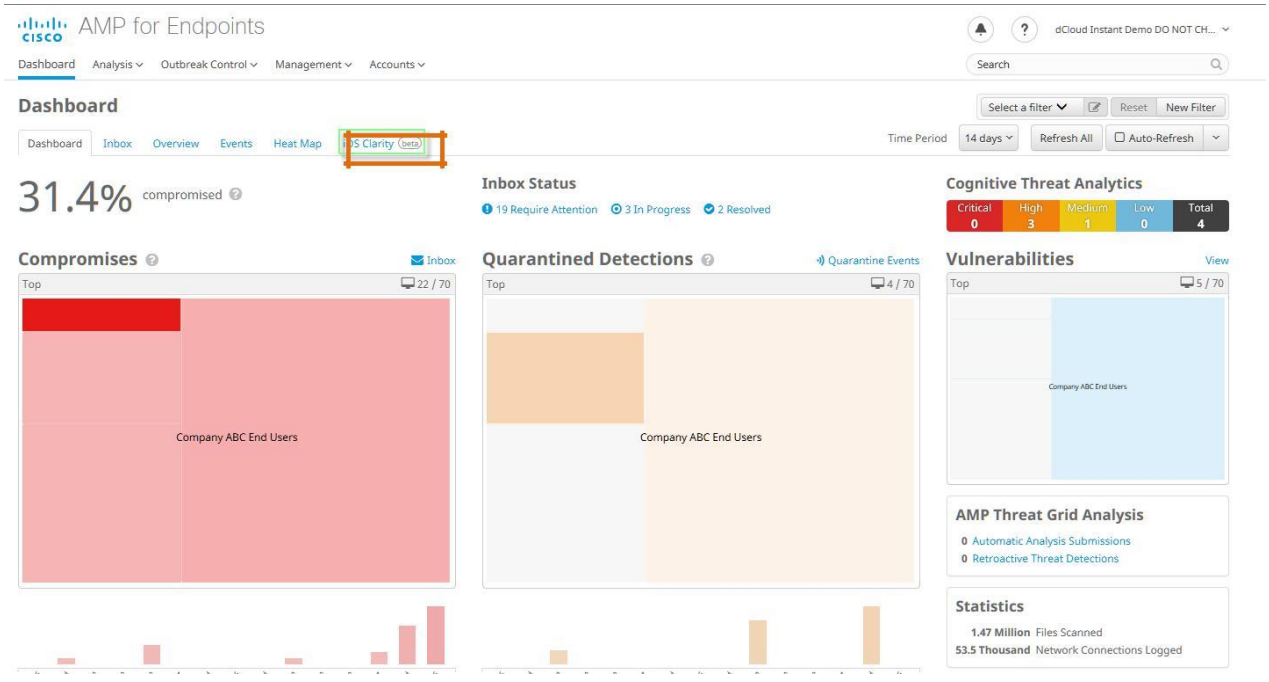
1. CSC デモ ランディング ページから、[Clarity] をクリックして Clarity ダッシュボードを起動します。

図 33. CSC デモ ランディング ページ

Use Case	Use Case Highlights	Demo Interfaces
Demo Guide	Full step by step guide to this demo	Demo Guide
CSC Overview Video	A brief video that provides an introduction to CSC	Video
Interactive IOS Device Demo	Demonstrate how CSC helps businesses more effectively protect their users on enterprise-owned Apple iOS devices in supervised mode	Interactive Demo
Umbrella Instant Demo	Demonstrate how Cisco Umbrella provides the first line of defense against threats on the internet wherever users go.	Umbrella
AMP for Endpoints (Clarity) Instant Demo	Demonstrate how Cisco Clarity provides visibility into all network connectivity from the iOS supervised device, enabling admins to audit all traffic flows by iOS users, apps, and system processes.	Clarity
Meraki Systems Manager Instant Demo	Demonstrate how to deploy CSC through Meraki Systems Manager to iOS devices in supervised mode, and then seamlessly provision the respective Umbrella and/or Clarity configurations with CSC on the devices.	Meraki Demo Video

2. AMP for Endpoints ダッシュボードが、新しいブラウザ タブで起動します。その新しい [iOS Clarity] タブをクリックします。

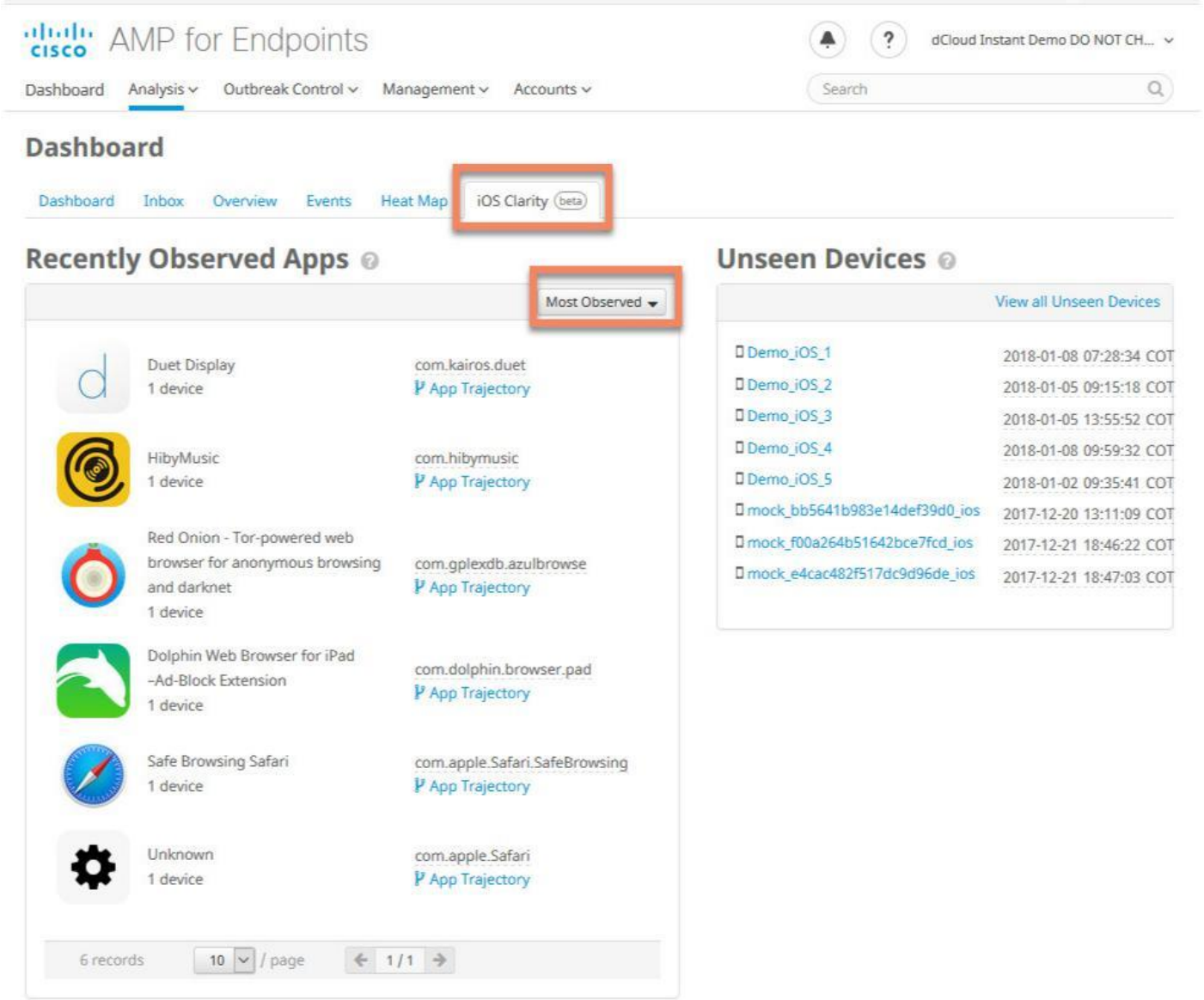
図 34. AMP ダッシュボード



3. [iOS Clarity] ページには、組織内のユーザによって最近使用された利用度の高いアプリと、ほとんど表示されることがないアプリがリストされます。ここでは、企業提供のデバイスで使用すべきでないクラウド サービスなどの未承認アプリの使用状況がわかる場合もあります。

注:上部の [iOS Clarity] タブを選択すると、デフォルトのビューは [最も監視されたアプリ(Most Observed Apps)] になります。

図 35. [最も監視されたアプリ(Most Observed Apps)]

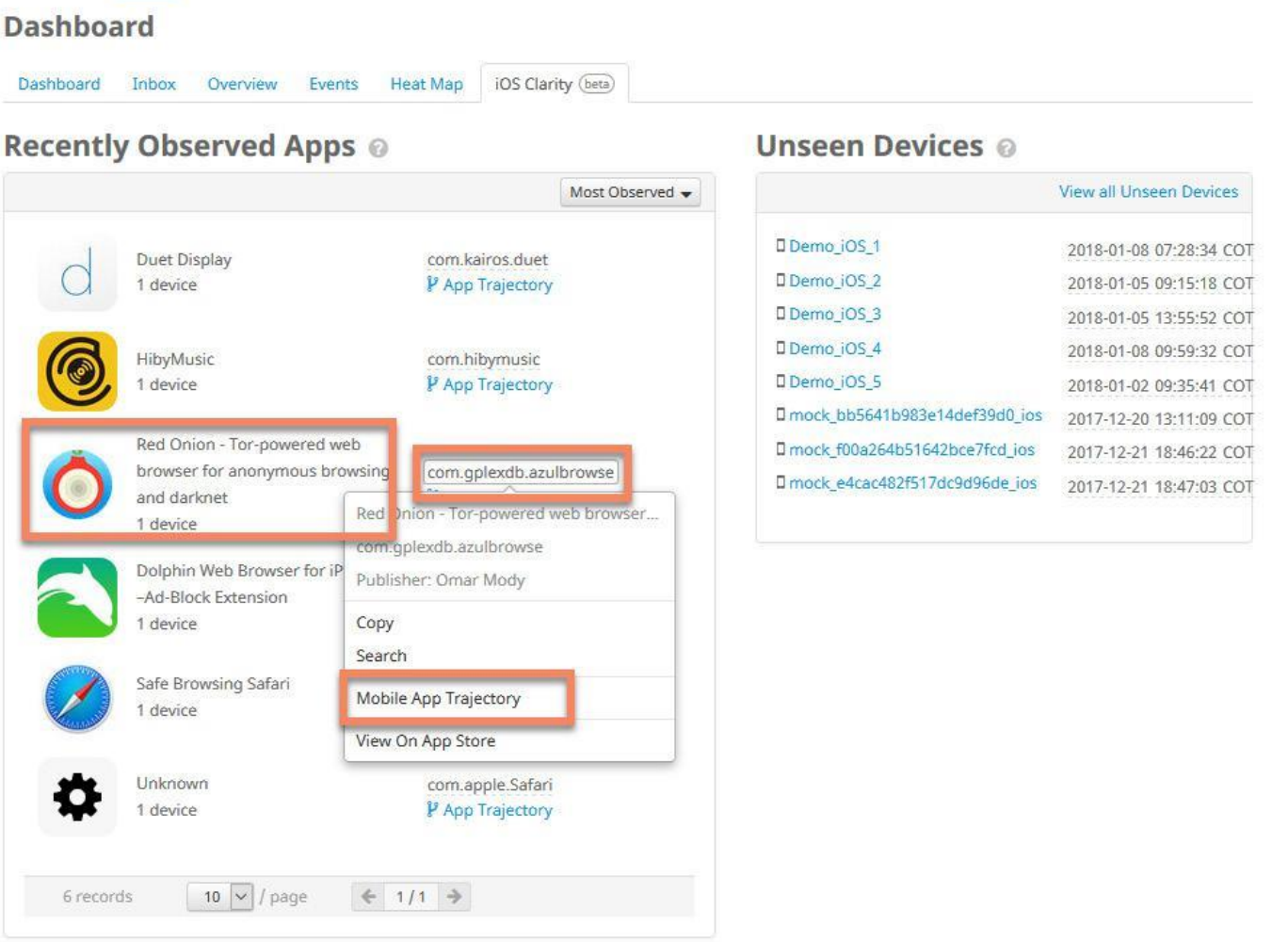


注:このデモでは、ここに表示されている 6 アプリしかありません。通常このリストはかなりの長さになり、上に強調表示されているプルダウン ボタンを切り替えて、[最も監視されていない(Least Observed)] を選択します(これらは、最も関心を向けるとともにさらに調査する必要があるアプリです)。

スクリーンショットは単なる例として表示されています。ビューは、[最近監視されたアプリ(Recently Observed Apps)] や [表示されていないデバイス(Unseen Devices)] の部分など、上記のスクリーンショットとは異なっている場合があります。

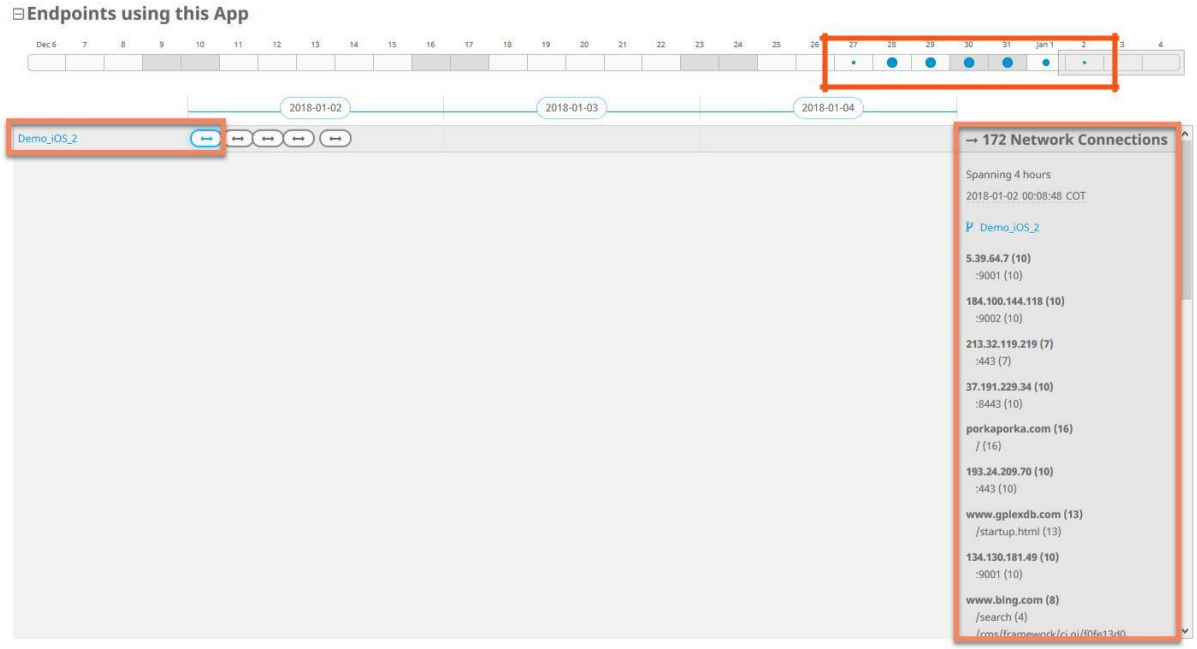
4. **Red Onion Tor** ブラウザについて説明します。これは匿名ブラウズ用で、管理対象デバイス上では企業が承認しない可能性のあるアプリです。
5. 公式アプリ名をクリックし（以下に示す **com.gplexdb.azulbrowse**）、[アプリ トラジェクトリ（App Trajectory）] をクリックして、このアプリの [モバイル アプリ トラジェクトリ（Mobile App Trajectory）] をピボットします（新しいブラウザ タブで開きます）。

図 36. 最近表示されたアプリ



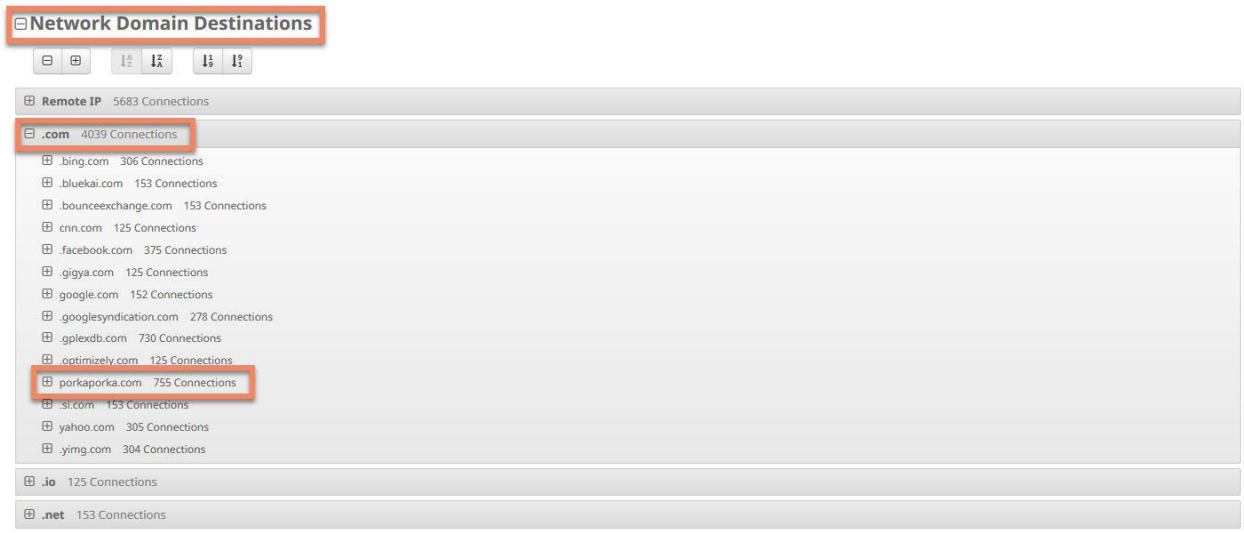
6. [モバイル アプリ トラジェクトリ（Mobile App Trajectory）] をピボットすると、そのアプリのアクティビティが可視化されます。最近このアプリを使用した iOS デバイスと、アプリによって作成された接続を表示できます。必要であれば、ポイント イン タイムをクリックして、その時点で行われている接続を表示します。青い点が含まれているポイント イン タイムをクリックします。これはその時点で行われた接続を示し、点のサイズはその時点でのネットワーク接続の量を示します。
7. **Demo_iOS_2** という名前のデバイスの横にある矢印の 1 つをクリックして、右側のペインを開きます。アプリが行った接続の概要が表示されます。スクロール ダウンして下に表示される宛先を見つけます。ない場合は、他のいずれかのデバイスを選択します。このデモンストレーションでは、疑わしいドメイン **Porkaporka.com** が強調表示されます。

図 37. モバイル アプリ トラジェクトリ：アプリを使用しているエンドポイント



8. [モバイル アプリ トラジェクトリ（Mobile App Trajectory）] ページをスクロール ダウンして、そのアプリの [ネットワーク ドメイン宛先（Network Domain Destinations）] のリストに注目します。**.com** セクションを展開し、**porkaporka.com** のエントリを見つけてクリックします。

図 38. モバイル アプリ トラジェクトリ：ネットワーク ドメイン宛先

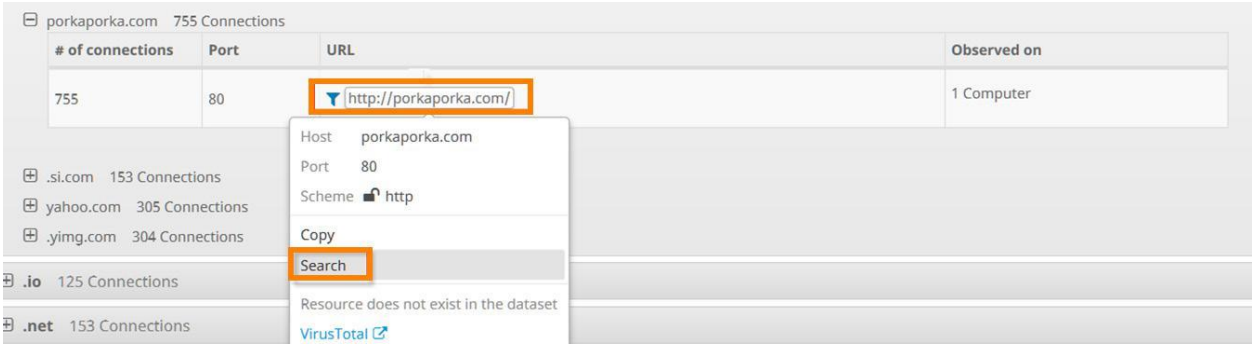


9. **porkaporka.com** のエントリ内で、詳細に調査するドメイン http://porkaporka.com をコピーします。

図 39. ネットワーク ドメイン宛先：アクセスされたドメイン

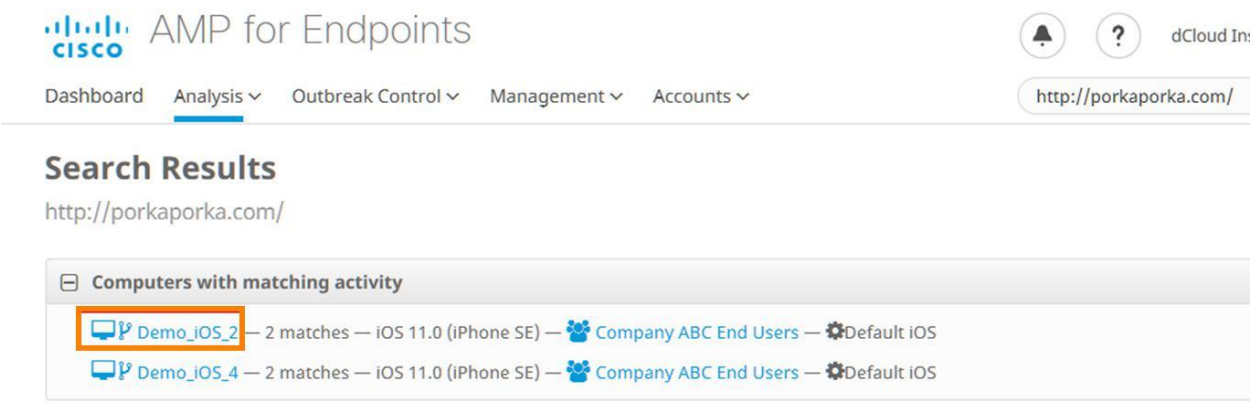
10. URL をダブルクリックして、使用されたポートやスキームなどの追加情報を表示します。この場合は HTTP ポート 80 です。URL を直接コピーすることも、このアクティビティに一致するデバイスを検索することもできます。[検索（Search）] をクリックします。

図 40. URL の検索

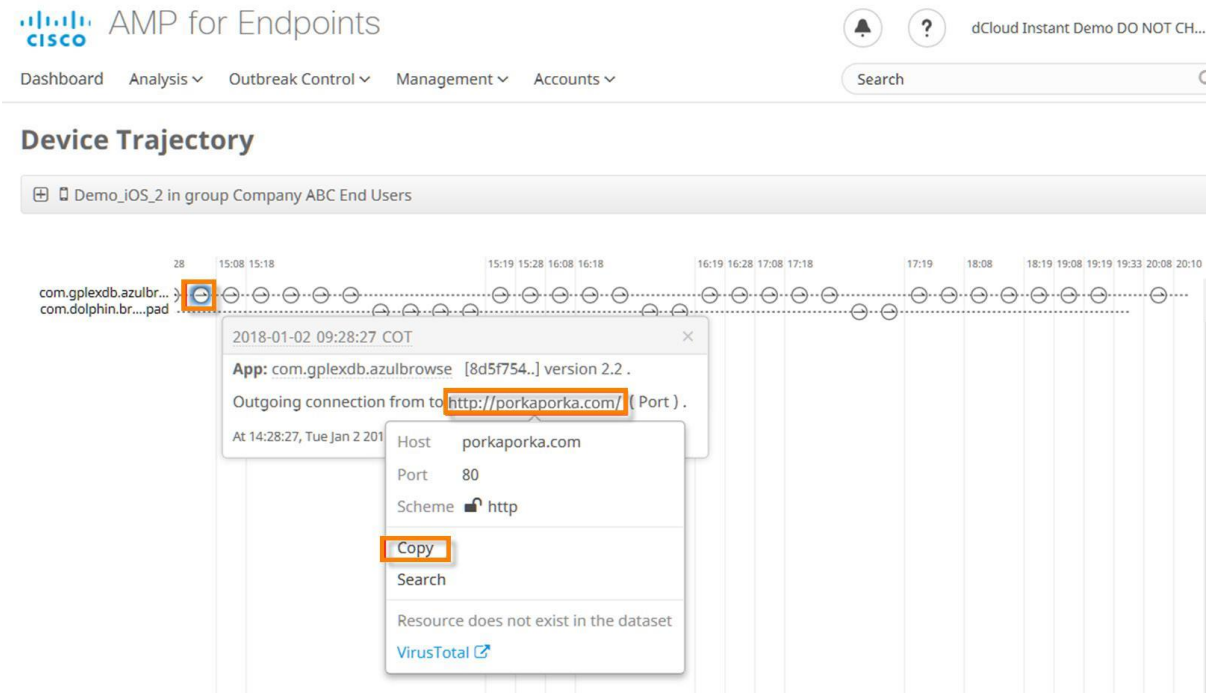


11. 検索結果には、疑わしいドメイン porkaporka.com にアクセスしたコンピュータまたはデバイスがリストされます。**Demo_iOS_2** デバイスをダブルクリックします。

図 41. Demo_iOS_2



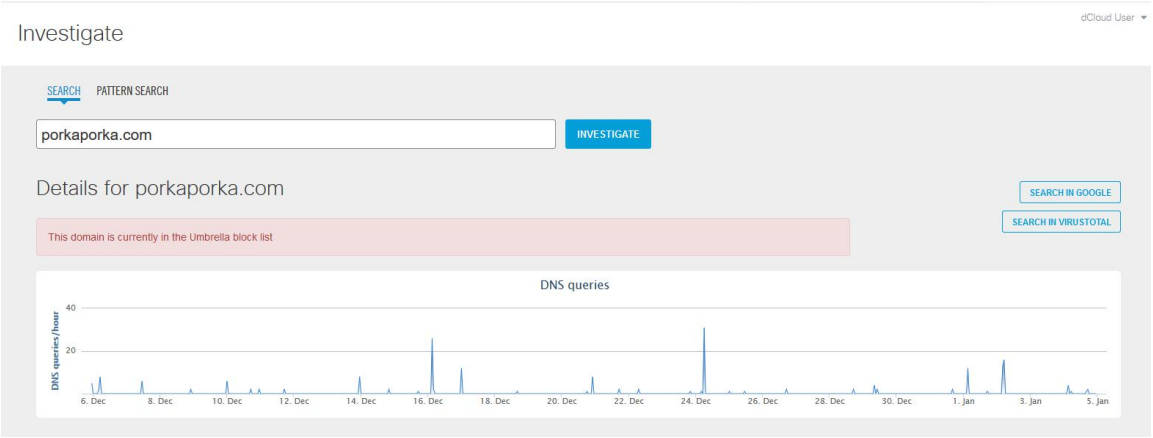
12. [デバイス トラジェクトリ（Device Trajectory）] を参照し、[Tor ブラウザ（com.gplexdb.azulbr）（Tor Browser (com.gplexdb.azulbr)）] の最初のポイント イン タイムを選択します。porkaporka.com への発信接続に注意してください。
13. URL **porkaporka.com** をクリックして、[コピー（Copy）] をクリックします。



14. シナリオ 2 で使用した Umbrella ダッシュボードに移動します。そのシナリオをまだデモンストレーションしていない場合には、シナリオ 2 の最初の手順に従ってください。
15. Umbrella ダッシュボードのメイン ナビゲーション メニュー（左側のパネル）から、[調査（Investigate）] をクリックします。
16. [調査（Investigate）] コンソールが開きます。[検索（Search）] ボックスに、（上記の手順 8 でコピーした）**porkaporka.com** を貼り付けて、[調査（Investigate）] をクリックします。

注：このドメインは、セキュリティ ポリシーを回避するように設計されたブラウザではなく企業が承認したブラウザによってアクセスされていた場合には、Umbrella によってブロックされているはずです。このサイトはマルウェアの拡散に関連付けられており、未承認のアプリを持つユーザがこのサイトにアクセスしています。このようにして、Clarity が提供する可視性の力が示されます。

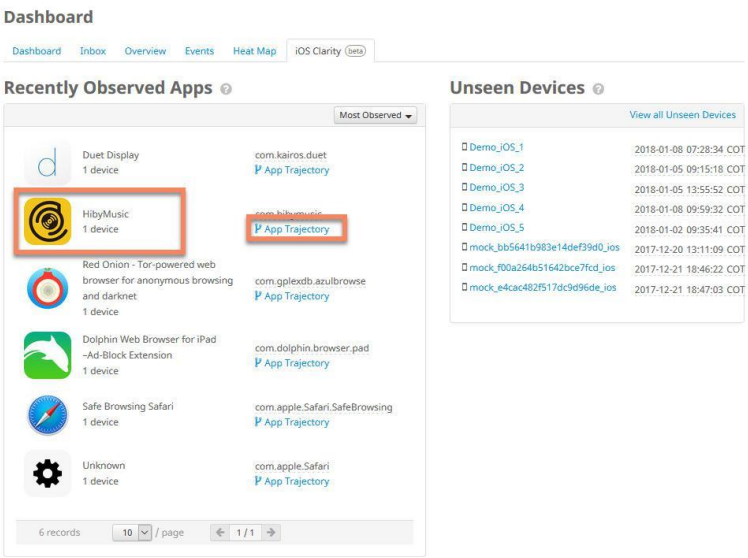
図 42. Umbrella ダッシュボードの調査



17. Clarity ダッシュボードに戻り、[iOS Clarity] タブの下にある [最近監視されたアプリ（Recently Observed Apps）] のリストに再び移動します。

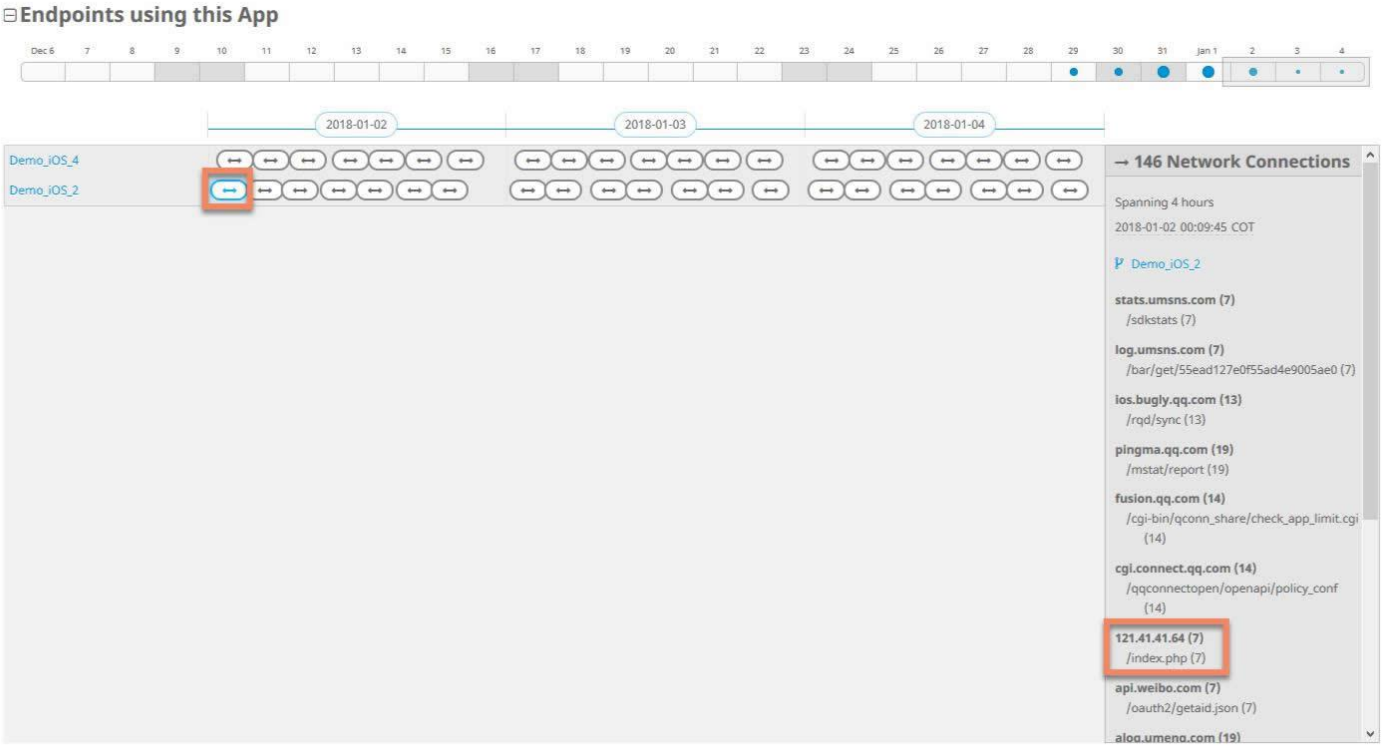
18. **HibyMusic** アプリに注目します。これは Wi-Fi ネットワーク経由で音楽を移動させることができるミュージック アプリです。このアプリの [アプリ トラジェクトリ（App Trajectory）] をクリックして、[モバイル アプリ トラジェクトリ（Mobile App Trajectory）] に再度直接ピボットします。

図 43. 最近監視されたアプリ：HiByMusic



19. このアプリを使用したモバイル デバイスにピボットした後に、ネットワーク接続があるポイント イン タイム（青い点）をクリックして、接続を監視します。多くの双方向コミュニケーションがあることを指摘します。実際に、このアプリは基本的に、接続を受信する Web サーバを作成します。発信接続の 1 つである 121.41.41.64 に注目します。

図 44. デバイス トラジェクトリ HiByMusic アプリ



20. [ネットワーク ドメイン宛先（Network Domain Destinations）] にスクロール ダウンして、宛先 http://121.41.41.64/index.php を見つけます。

図 45. アプリのネットワーク トラジェクトリ

21. ブラウザで新しいタブを開き、宛先を URL バーにコピーして、このアプリがアクセスする可能性がある場所を調査します。

図 46. http://121.41.41.64/index.php の調査

22. この Web サイトがどのようなものであるか、またなぜアプリが接続しているのかがわからないとしても、疑わしく見えるために、さらに調査が必要なことがあります。
23. Clarity ダッシュボードのブラウザ タブに戻り、[ネットワーク ドメインの宛先（Network Domain Destinations）] でスクロール ダウンし、**.com** セクションを展開します。
24. ツリーを **qq.com**、**bugly.qq.com**、および **ios.bugly.qq.com** の順に展開します。

図 47. アプリの展開されたトラジェクトリ

25. トラジェクトリに表示されるネットワーク宛先は、HTTPS 宛先です。

注：Clarity が iOS 11 で使用するネットワーク API のおかげで、何も復号しなくても HTTPS ネットワーク アクティビティへの可視性を得ることができます。Clarity には、トラフィック自体（ペイロード）ではなく、ネットワーク接続（メタデータ）への可視性があるということを覚えておくことが重要です。

26. デモ ランディング ページに戻って、次のデモ シナリオを続行します。他のデモ シナリオのために Clarity ダッシュボードのブラウザ タブを開いたままにします。

シナリオ 4.　Umbrella ダッシュボードでのモバイル ID ポリシー

このシナリオは、単純な方法でモバイル ユーザに適用される Umbrella のポリシー機能をデモンストレーションします。ポリシーは、モバイル デバイス専用にすることも、他のアイデンティティ タイプ（AD ユーザ、ネットワーク、ローミング コンピュータ）とともに適用することもできます。ポリシーには、ブロックされたセキュリティ カテゴリ、コンテンツの設定、許可およびブロック リストなど、各種設定が含まれます。

手順

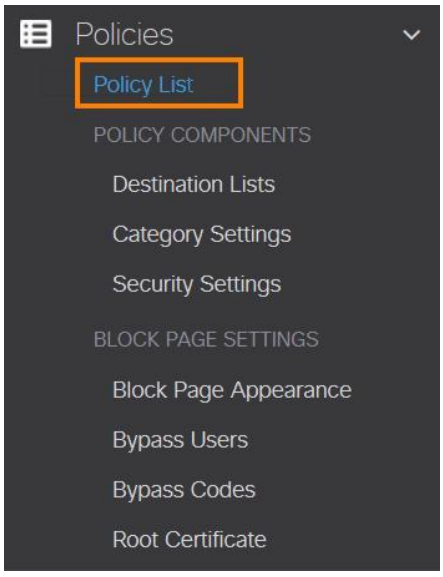
1. CSC デモ ランディング ページから、[Umbrella] をクリックして Umbrella ダッシュボードを起動します。すでに開いている場合、ブラウザのタブに戻って、下記の手順 3 に進みます。

図 48. CSC デモ ランディング ページ

Use Case	Use Case Highlights	Demo Interfaces
Demo Guide	Full step by step guide to this demo	Demo Guide
CSC Overview Video	A brief video that provides an introduction to CSC	Video
Interactive IOS Device Demo	Demonstrate how CSC helps businesses more effectively protect their users on enterprise-owned Apple iOS devices in supervised mode	Interactive Demo
Umbrella Instant Demo	Demonstrate how Cisco Umbrella provides the first line of defense against threats on the internet wherever users go.	Umbrella
AMP for Endpoints (Clarity) Instant Demo	Demonstrate how Cisco Clarity provides visibility into all network connectivity from the iOS supervised device, enabling admins to audit all traffic flows by iOS users, apps, and system processes.	Clarity
Meraki Systems Manager Instant Demo	Demonstrate how to deploy CSC through Meraki Systems Manager to iOS devices in supervised mode, and then seamlessly provision the respective Umbrella and/or Clarity configurations with CSC on the devices.	Meraki Demo Video

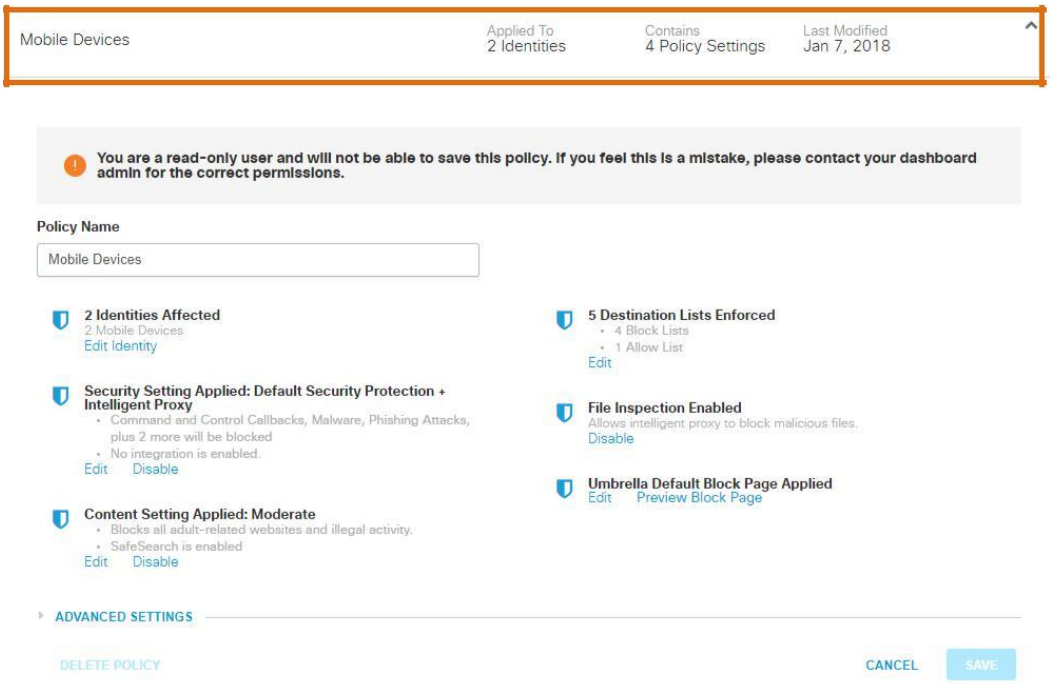
2. Umbrella ダッシュボードが新しいブラウザ タブで起動し、[概要（Overview）] ページが表示されます。
3. 左側のナビゲーション メニューを使用して、[ポリシー（Policies）] > [ポリシー リスト（Policy List）] を選択します。

図 49. [ポリシー（Policies）] > [ポリシー リスト（Policy List）]



4. [モバイル デバイス（Mobile Devices）] というポリシーをクリックして、要約ページにこのポリシーの詳細を表示します。

図 50. モバイル デバイス ポリシー

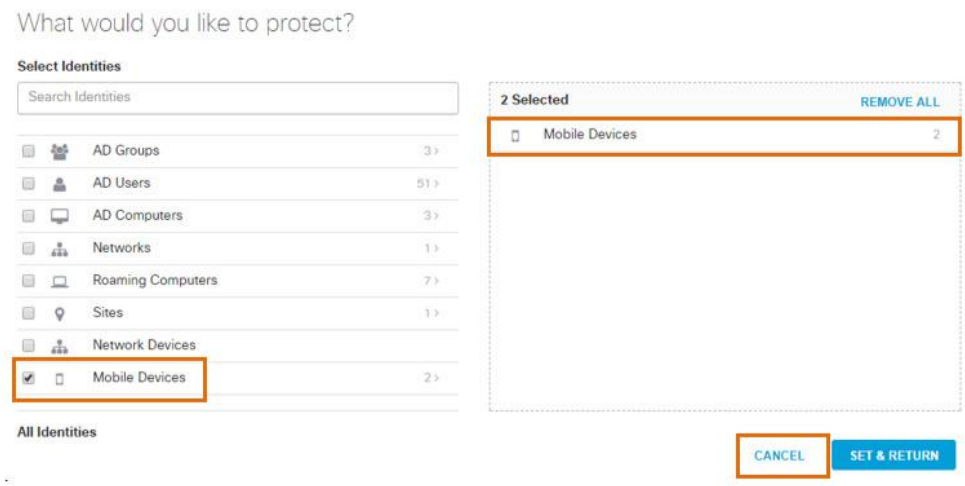


5. [影響を受ける ID（Identities Affected）] 領域で [ID の編集（Edit Identity）] をクリックします。ポリシーはモバイル デバイスのユーザ専用に（他の ID タイプとともにまたは排他的に）適用できることに注意してください。このポリシーに関連付けられているモバイル デバイスの数に注意してください。

注：Umbrella ダッシュボードに読み取り専用管理者としてログインしているため、加えたすべての変更は保存できません。

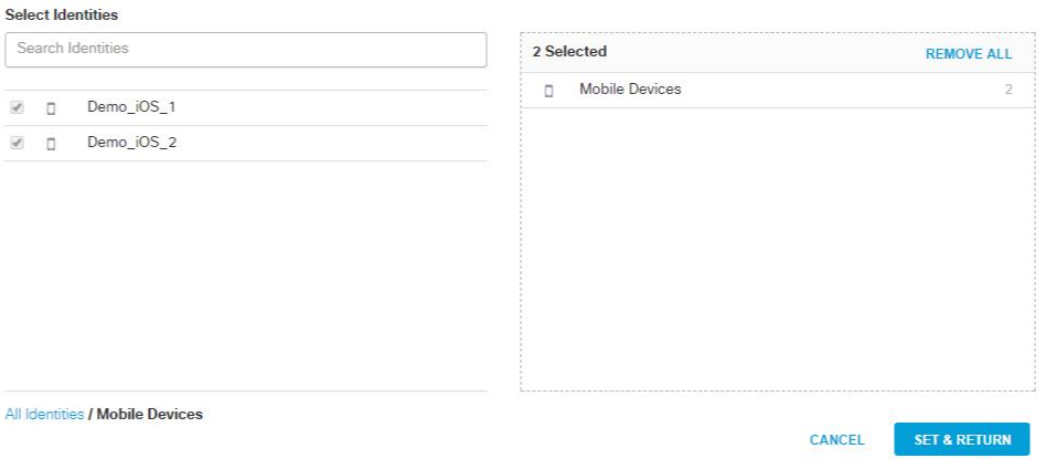
注：モバイル デバイスは MDM との統合によって同期します。リンクの手順については、CSC のプロビジョニングについて扱っているシナリオ 5 で概説されています。

図 51. ID のモバイル デバイス



6. 左側の [モバイル デバイス（Mobile Devices）] をクリックします。MDM からプロビジョニングされたプロファイルにすべてのモバイル デバイスが表示されます。

図 52. モバイル デバイス

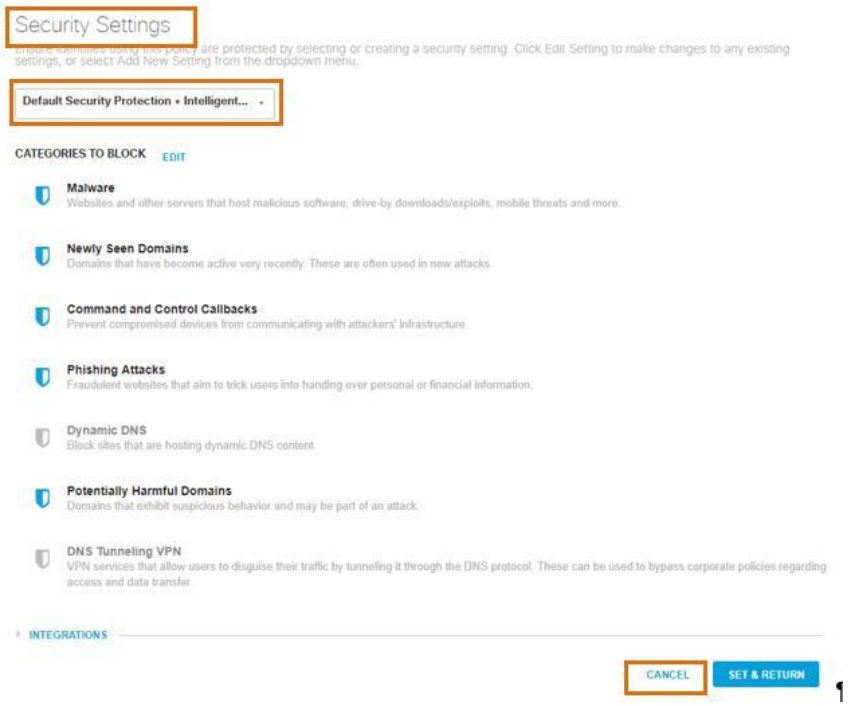


注：特定のモバイル デバイスを選択することはできません。ポリシーは選択したプロファイルで常にすべてのモバイル デバイスに適用されます。

7. [キャンセル（Cancel）] をクリックして、ポリシー要約に戻ります。

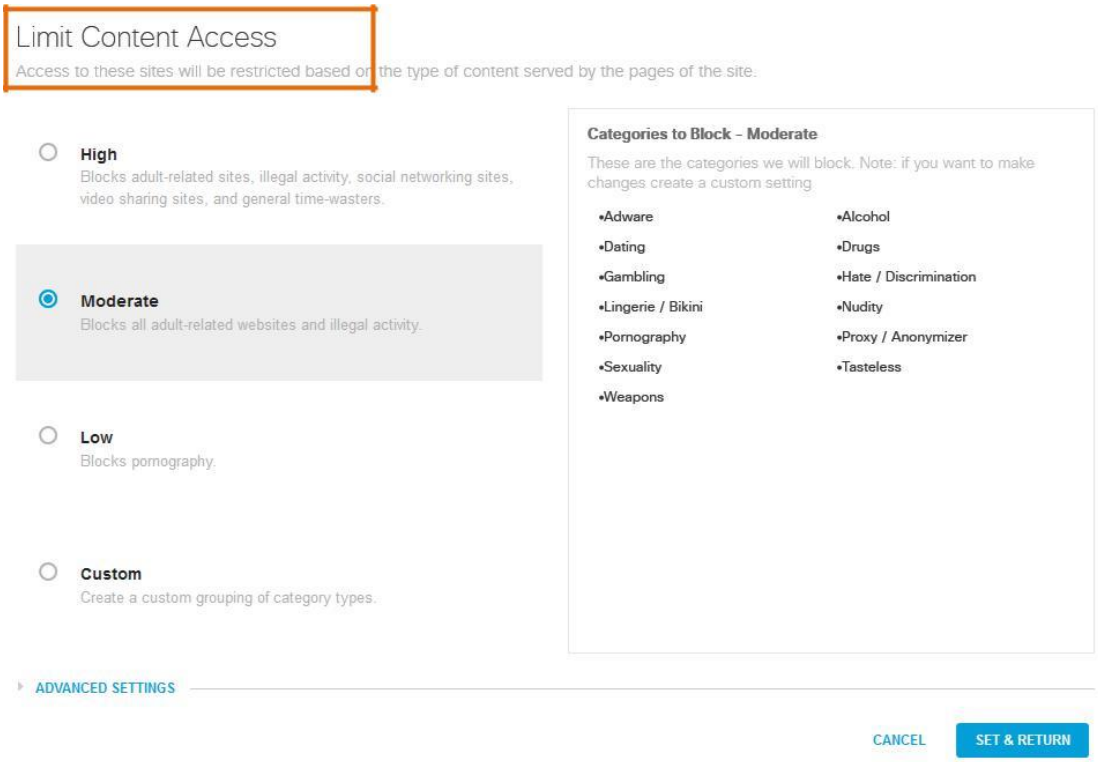
8. [セキュリティ設定適用…（Security Setting Applied…）] 領域で [編集（Edit）] をクリックします。セキュリティ設定には、特定のカテゴリを許可するかブロックするかだけでなく、定義済みのプロファイルに従ってまたは個別に適用できる多数のセキュリティ カテゴリが含まれます。この場合、特定のセキュリティ カテゴリが選択されています。つまり、このポリシーでは、モバイル デバイスのユーザにはこれらのセキュリティ カテゴリはブロックされるということです。

図 53. セキュリティ設定



9. [キャンセル（Cancel）] をクリックします。
10. [コンテンツ設定適用…（Content Settings Applied…）] 領域で [編集（Edit）] をクリックします。コンテンツ フィルタリングのカテゴリ設定は、ここのモバイル ユーザに適用されます。定義済みプロファイル（高、中、または低レベルのフィルタリング）を適用するか、またはカスタム リストを作成できます。

図 54. コンテンツ フィルタリングの設定



11. [詳細システム設定（Advanced System Settings）] をクリックします。このポリシーによって、SafeSearch がモバイル ユーザに適用されていることに注意してください。

注：SafeSearch は、Google、Bing、YouTube で検索されたコンテンツに適用されます。

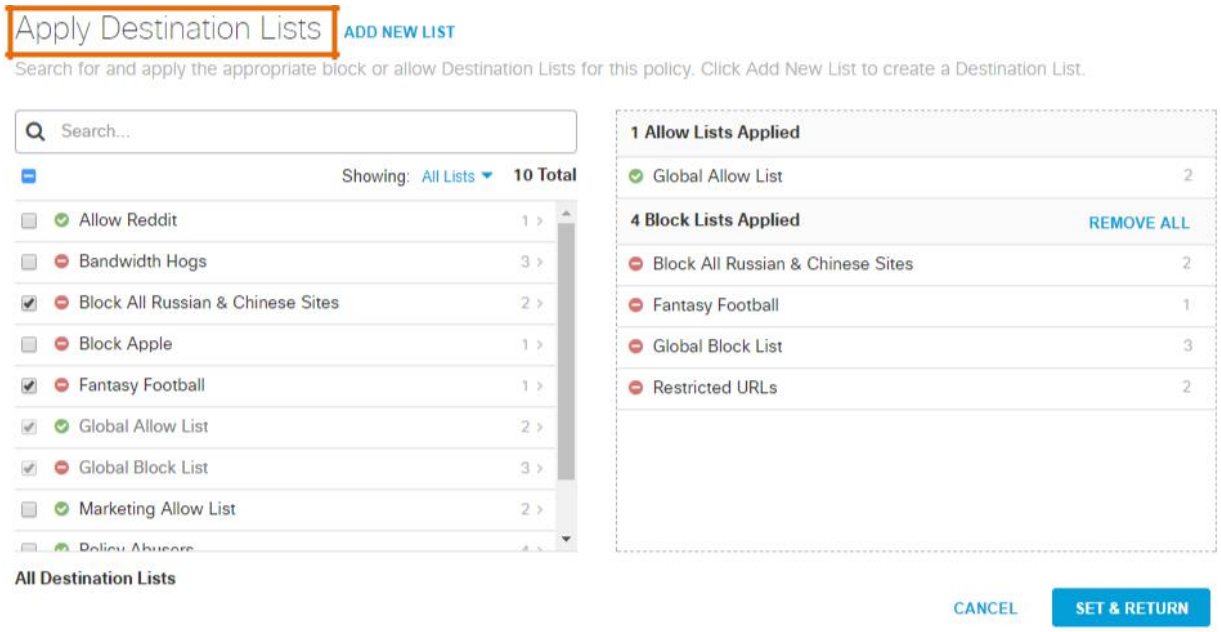
図 55. SafeSearch の設定

12. [キャンセル（Cancel）] をクリックします。

13. [適用される宛先リスト（Destination Lists Enforced）] 領域で [編集（Edit）] をクリックします。カスタムの宛先許可/ブロックのリストをこのポリシーに適用できます。既存のリストを追加するか、またはポリシーから新しいリストを直接作成します。宛先リストには、ドメイン、IP、および URL を含められることに注意してください。

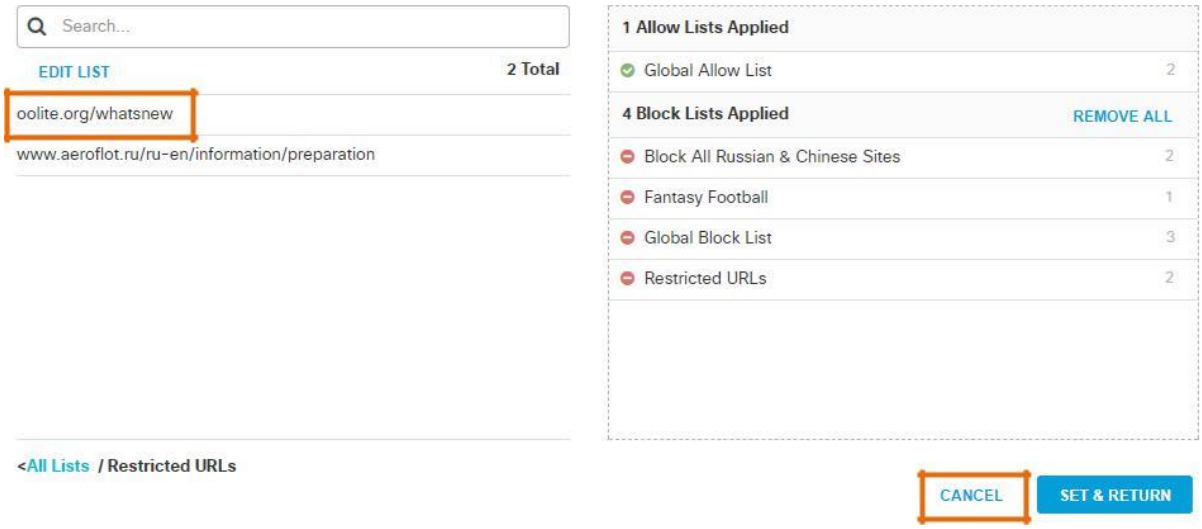
注：カスタム URL ブロック リストは、他のソースから取得できるセキュリティを適用するために役立ちます。カスタム URL ブロックの例（oolite.org/whatsnew）は、シナリオ 1 で示されています。

図 56. 宛先リストの設定



14. 左側のリストでスクロール ダウンして、[制限付き URL（Restricted URLs）] ブロック リストをクリックします。

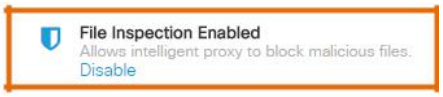
図 57. [制限付き URL（Restricted URLs）] ブロック リスト



15. [キャンセル（Cancel）] をクリックします。

16. ファイル検査を 1 回の設定で有効にします。有効にすると、ファイルはサード パーティ製の AV エンジンと Cisco AMP によって検査されます。

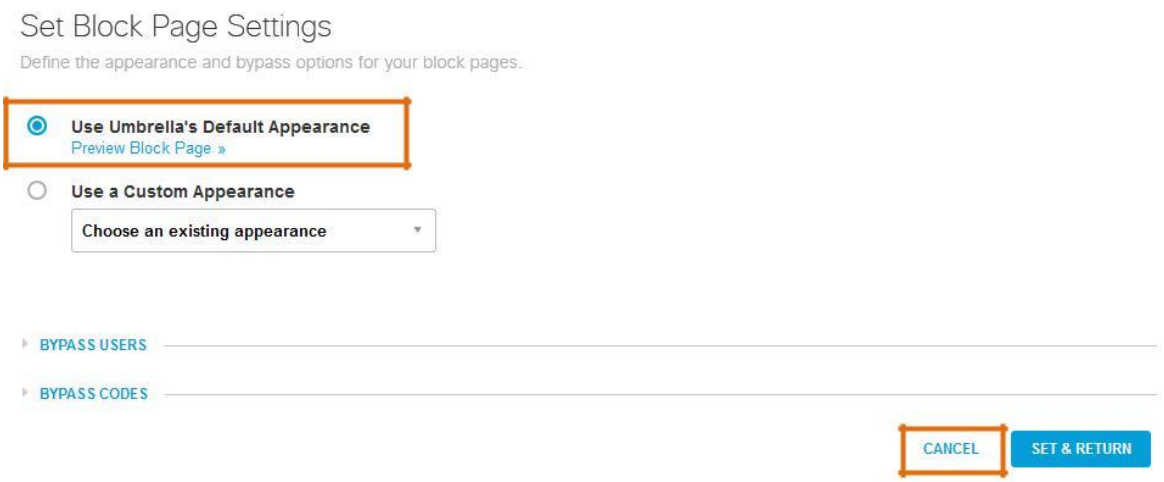
図 58. ファイル検査設定



17. [適用されるカスタム ブロック ページ（Custom Block Page Applied）] 領域で [編集（Edit）] をクリックします。デフォルトのブロック ページがこのポリシーのモバイル ユーザに対して選択されており、ここからカスタマイズされたブロック ページも（作成済みのものがあれば）選択できます。選択したブロック ページもここでプレビューできます。

注：バイパス オプションもこの領域で利用および設定できます。

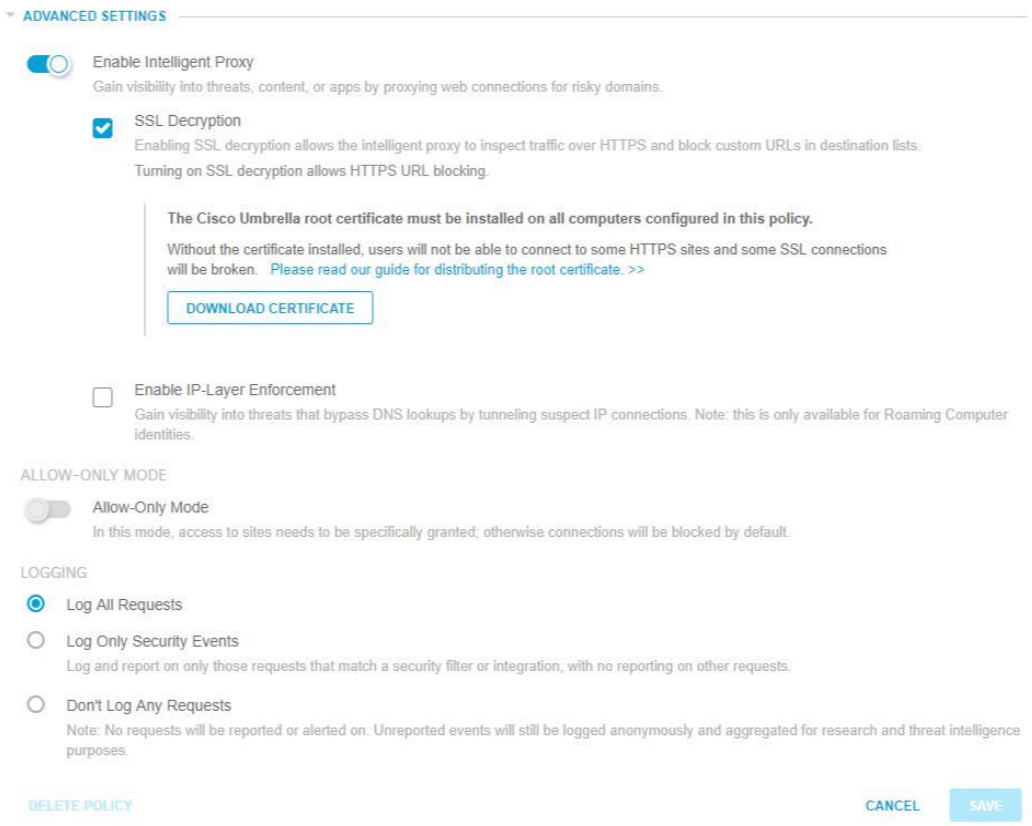
図 59. ブロック ページ設定



18. [キャンセル（Cancel）] をクリックします。
19. [Advanced Settings（詳細設定）] をクリックします。ここでインテリジェント プロキシと、関連する設定を有効または無効にできます。

注：ファイル検査と IP 層の適用などの特定のセキュリティ機能は、インテリジェント プロキシに依存し、インテリジェント プロキシを無効にすると、上記の選択は無効になります。ログ対象として、すべて、セキュリティ イベントのみ、またはこのポリシーは対象にしない、を選択することもできます。

図 60. 詳細設定



ヒント：SSL 復号を使用する場合、SSL 証明書は、プロビジョニング プロセス中に CSC アプリとともにモバイル デバイスにインストールされるため、モバイル デバイスにダウンロードまたは展開する必要はありません。

20. [キャンセル（Cancel）] をクリックして、選択したポリシーを閉じます。
21. CSC デモ ランディング ページに戻って、次のデモ シナリオを続行します。他のデモ シナリオのために Umbrella ダッシュボードのブラウザ タブを開いたままにします。

シナリオ 5.　Meraki Systems Manager ダッシュボードでの CSC のプロビジョニングと配信

Cisco Security Connector は現在有効にされており、Meraki Systems Manager から排他的に配信されます。3 つすべてのテクノロジーからの API ソリューションを活用する場合、Systems Manager による CSC の展開が、このソリューションの価値を実現する最も迅速で簡単な方法です。このシナリオでは、次の内容について説明します。

- ソリューションの接続がどの程度簡単であるか（展開のビデオを使用）
- Meraki ダッシュボードで CSC アプリを iOS 監視デバイスにプッシュする手順

手順

1. CSC デモ ランディング ページから、[デモ ビデオ（Demo Video）] をクリックして、Meraki API キーを使用して 3 つのソリューションを簡単に接続できる方法を示すデモ ビデオを起動します。

図 61.　CSC デモ ランディング ページ

Use Case	Use Case Highlights	Demo Interfaces
Demo Guide	Full step by step guide to this demo	Demo Guide
CSC Overview Video	A brief video that provides an introduction to CSC	Video
Interactive IOS Device Demo	Demonstrate how CSC helps businesses more effectively protect their users on enterprise-owned Apple iOS devices in supervised mode	Interactive Demo
Umbrella Instant Demo	Demonstrate how Cisco Umbrella provides the first line of defense against threats on the internet wherever users go.	Umbrella
AMP for Endpoints (Clarity) Instant Demo	Demonstrate how Cisco Clarity provides visibility into all network connectivity from the iOS supervised device, enabling admins to audit all traffic flows by iOS users, apps, and system processes.	Clarity
Meraki Systems Manager Instant Demo	Demonstrate how to deploy CSC through Meraki Systems Manager to iOS devices in supervised mode, and then seamlessly provision the respective Umbrella and/or Clarity configurations with CSC on the devices.	Meraki Demo Video

2. CSC デモ ランディング ページから、[Meraki] をクリックして Meraki デモ ダッシュボードを起動します。組織化された概要が表示されます。
3. [セキュリティ コネクタ（Security Connector）] ネットワークをクリックします。

注：以下のランディング ページの代わりにこのランディング ページが表示される場合は、[ネットワーク（networks）] をクリックして、以下に示している表示になるようにしてください。

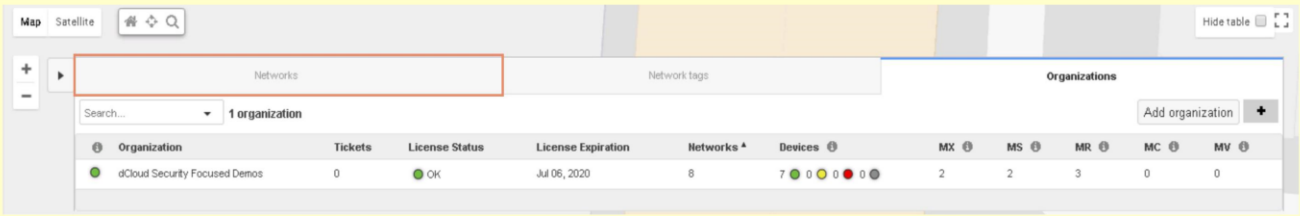
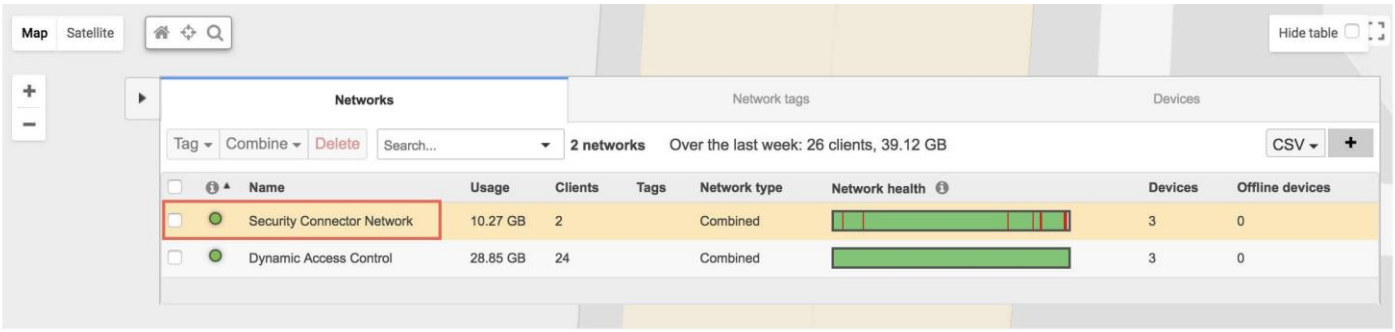


図 62. Meraki の組織化された概要

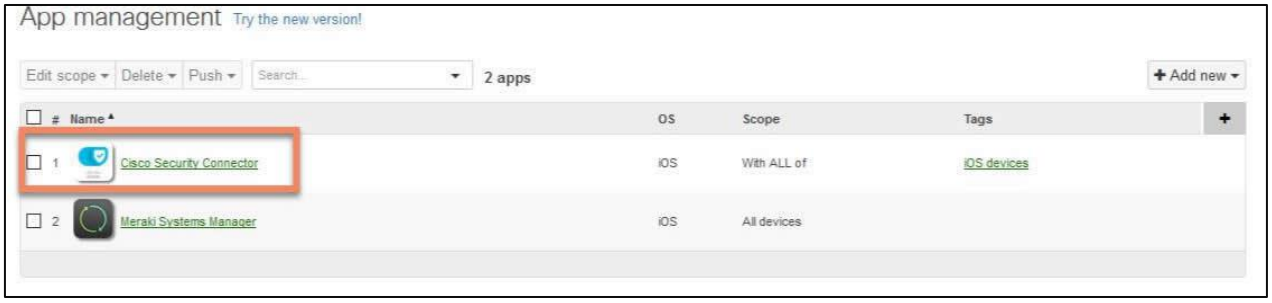


4. [システム マネージャ（System Manager）] をクリックし、[アプリ（Apps）] をクリックします。

図 63. [システム マネージャ（System Manager）] の [アプリ（Apps）] メニュー

5. **Cisco Security Connector** アプリをクリックして、どのデバイスが CSC を取得するかの指定を表示します。

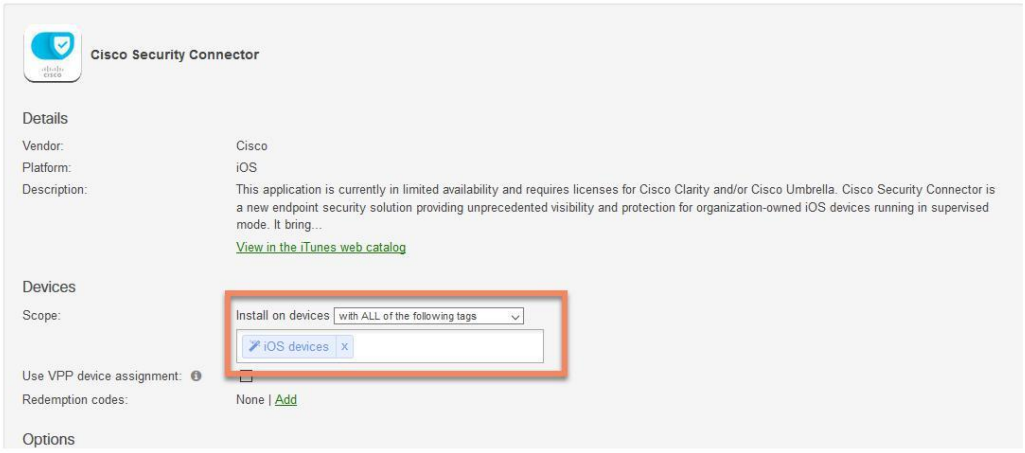
図 64. プロビジョニングされたアプリ



注：Systems Manager は、Apple App Store、Google Play ストアと統合することができ、また、ユーザがクラウドに自身のファイルをアップロードし、クラウドからアプリケーション管理を実行できるクラウド管理インフラストラクチャを持つこともできます。CSC は、Systems Manager から提供できる多数のアプリの 1 つに過ぎないことを必ず説明してください。

6. このアプリケーションがタグを利用してどのように iOS デバイスにのみ提供されるかを強調します。

図 65. CSC タグの設定



注:時刻、デバイス タイプ、AD ユーザ グループおよびセキュリティ ポリシーを含む、複数のタグ付けオプションがあります。適切なタグ付けソリューションを利用することで、Systems Manager は正しいデバイスが適切なアプリケーションを取得できるようにします。

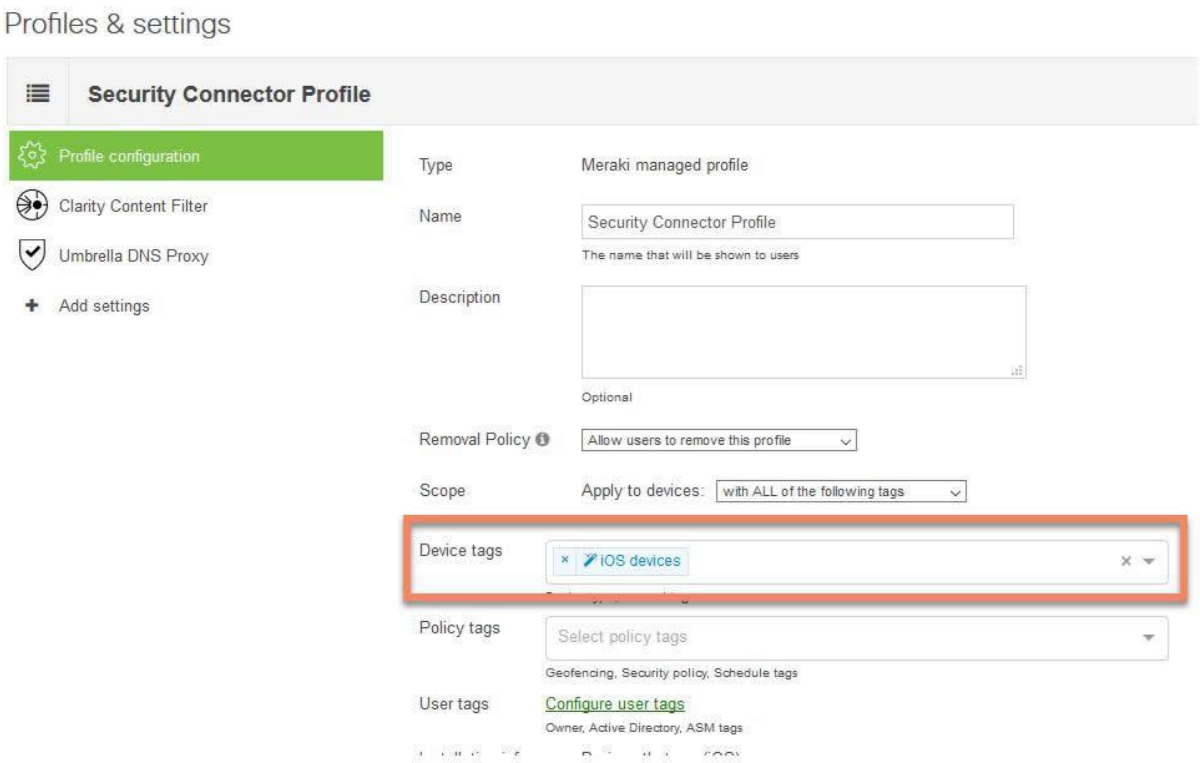
7. [System Manager] > [MDM の設定(MDM Settings)] をクリックします。

図 66. MDM 設定

注:[設定(Settings)] ページにデバイス プロファイルのセットが表示されます。デバイス プロファイルには特定のデバイスの設定と制限が含まれます。デバイス プロファイルと前に取り上げたアプリ設定とは、一緒にバインドされません。

8. プロファイルがデバイス タグを活用して iOS デバイスにだけ配信されることも説明します。

図 67. デバイス タグの選択



注:CSC 配信のアプリケーションと同様、CSC は iOS デバイス上でのみサポートされるため、この特定のデバイス プロファイルは iOS デバイスにのみ配信されます。

9. [Clarity コンテンツ フィルタ(Clarity Content Filter)] をクリックして、Clarity(AMP for Endpoints)コンソールからプッシュされた設定を強調表示します。

図 68. プロファイル設定

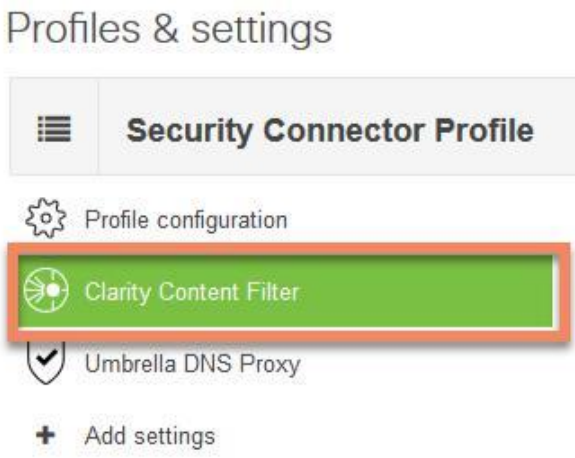
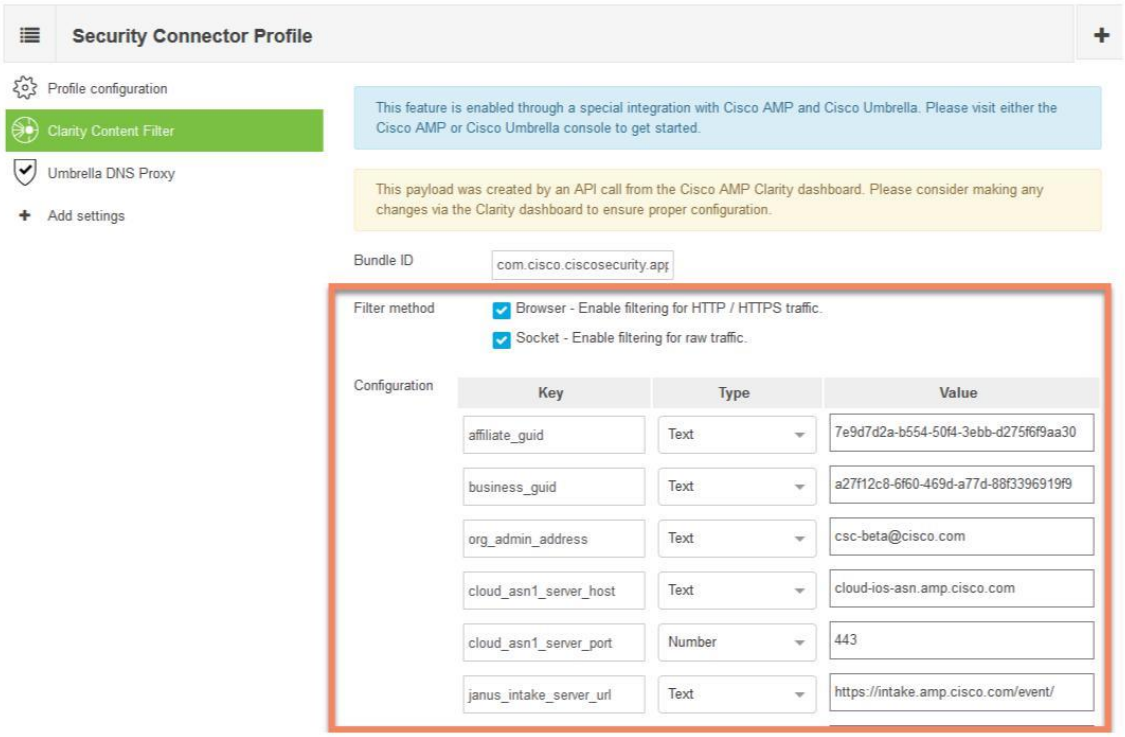


図 69. Clarity コンテンツ フィルタ設定



注:この設定は、Meraki API キーを介して接続されたときに AMP コンソールから自動的にプルされました。これは、手順 1 のビデオでも説明されました。

注:読み取り専用ユーザとしてアクセスしているため、API キーはこのデモ ダッシュボードには表示されません。

10. [Umbrella DNS プロキシ(Umbrella DNS Proxy)] をクリックして、Umbrella ダッシュボードからプッシュされるソリューションを強調表示します。

図 70. プロファイル設定

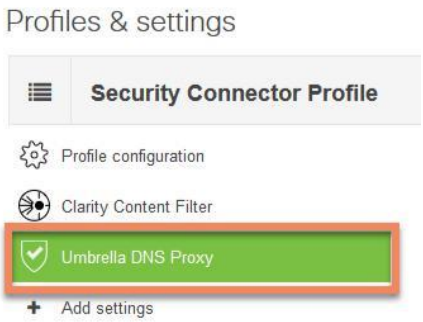
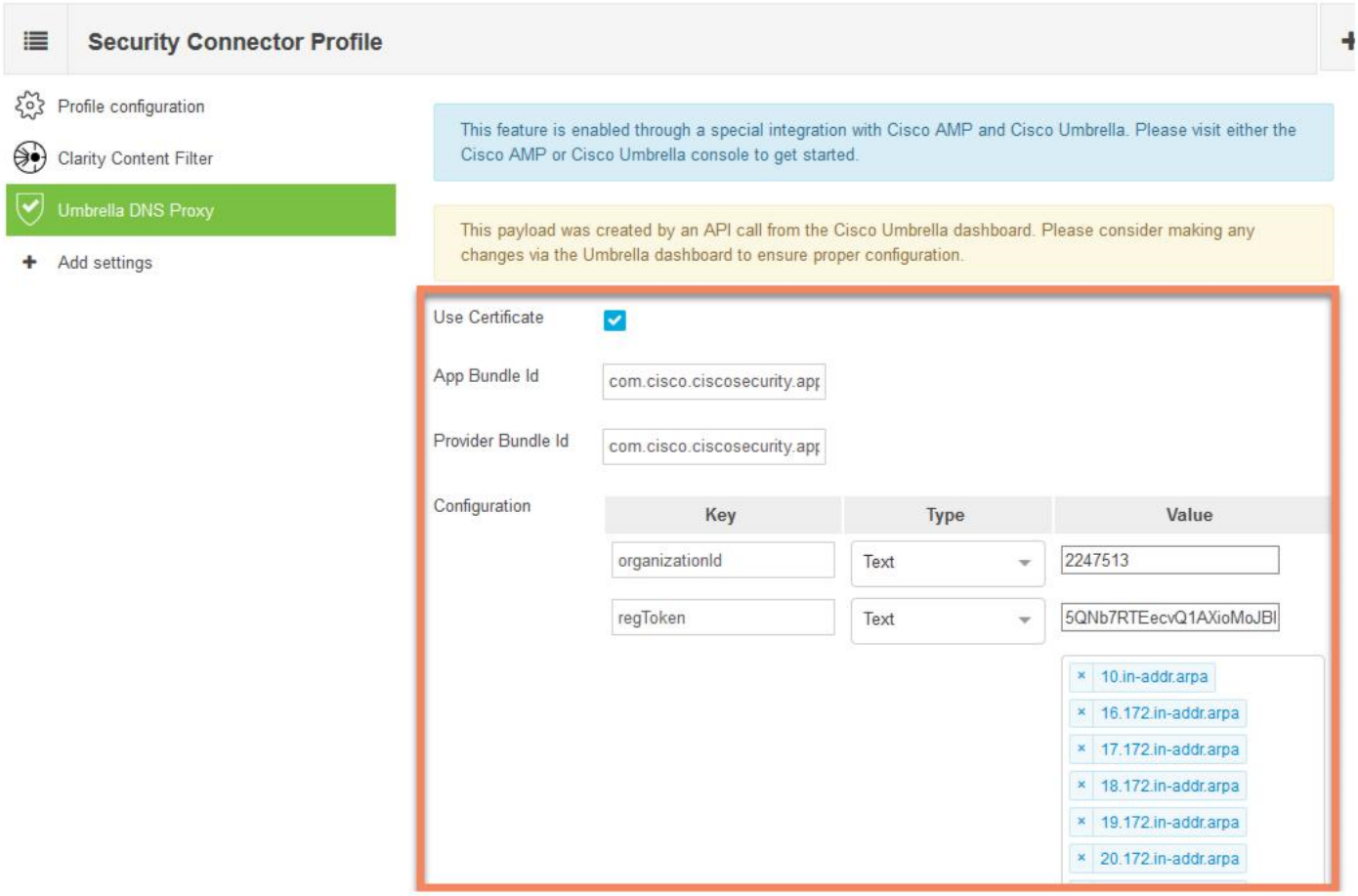


図 71. Umbrella DNS プロキシの設定



注:この設定も、Meraki API キーを介して接続されたときに Umbrella ダッシュボードから自動的にプルされました。これは、手順 1 のビデオでも説明されました。

注:読み取り専用ユーザとしてアクセスしているため、API キーはこのデモ ダッシュボードには表示されません。

11. このデモ シナリオの締めくくりとして、Meraki Systems Manager によって特定の iOS デバイスに対する CSC アプリの配信とデバイス設定が可能になったという事実を繰り返します。

ヒント:この使用例は Cisco CSC アプリと iOS デバイスに固有ですが、iOS、Android、MacOS、および Windows デバイスにモバイル アプリとエンタープライズ アプリの両方を配布するために同じ作業フローが使用されることを明確に説明します。

注:2 方向の API とプログラム可能性は、展開とインストールを簡単にする 3 つの異なるシスコ テクノロジー間の相乗効果を強調するための鍵となります。お客様が他の MDM ソリューションを所有している可能性もありますが、CSC 展開は、Meraki Systems Manager の使いやすさと現行のサポートにより、他の MDM の使用体験とは全く異なる可能性があります。

12. デモ ランディング ページに戻って、次のデモ シナリオを続行します。他のデモ シナリオのために Meraki SM ダッシュボードのブラウザ タブを開いたままにします。

シナリオ 6.　CSC アプリと iOS の設定

このシナリオでは、CSC アプリ自体を強調するために、iOS デバイス（Apple iPad）のインタラクティブ デモと、監視モードでのデバイスの管理設定を活用します。

エンドユーザは、保護されるために必ずしも CSC アプリにアクセスする必要はありませんが、このシナリオではその機能の一部を表示することができます。

手順

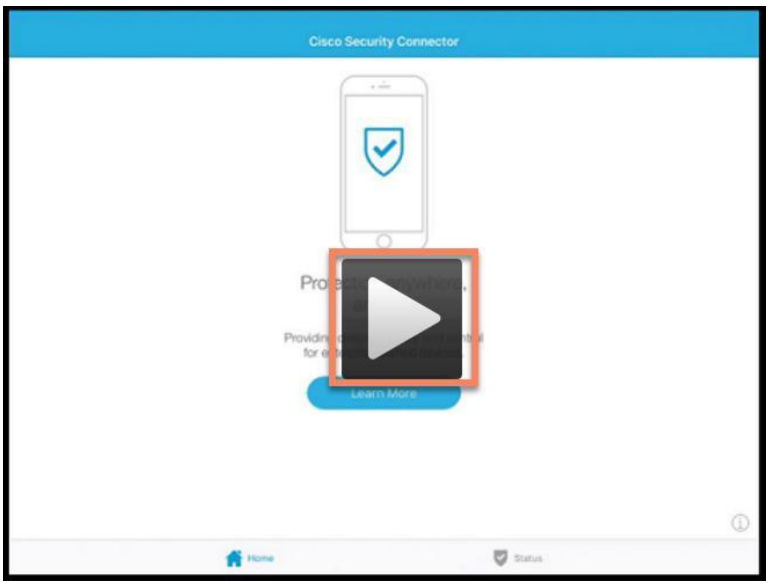
1. CSC デモ ランディング ページから、[インタラクティブ デモ（Interactive Demo）] をクリックして、インタラクティブ デモを起動します。すでに開いている場合、実行しているブラウザのタブに戻って、手順 4 に進みます。

図 72. CSC デモ ランディング ページ

Use Case	Use Case Highlights	Demo Interfaces
Demo Guide	Full step by step guide to this demo	Demo Guide
CSC Overview Video	A brief video that provides an introduction to CSC	Video
Interactive IOS Device Demo	Demonstrate how CSC helps businesses more effectively protect their users on enterprise-owned Apple iOS devices in supervised mode	Interactive Demo
Umbrella Instant Demo	Demonstrate how Cisco Umbrella provides the first line of defense against threats on the internet wherever users go.	Umbrella
AMP for Endpoints (Clarity) Instant Demo	Demonstrate how Cisco Clarity provides visibility into all network connectivity from the iOS supervised device, enabling admins to audit all traffic flows by iOS users, apps, and system processes.	Clarity
Meraki Systems Manager Instant Demo	Demonstrate how to deploy CSC through Meraki Systems Manager to iOS devices in supervised mode, and then seamlessly provision the respective Umbrella and/or Clarity configurations with CSC on the devices.	Meraki Demo Video

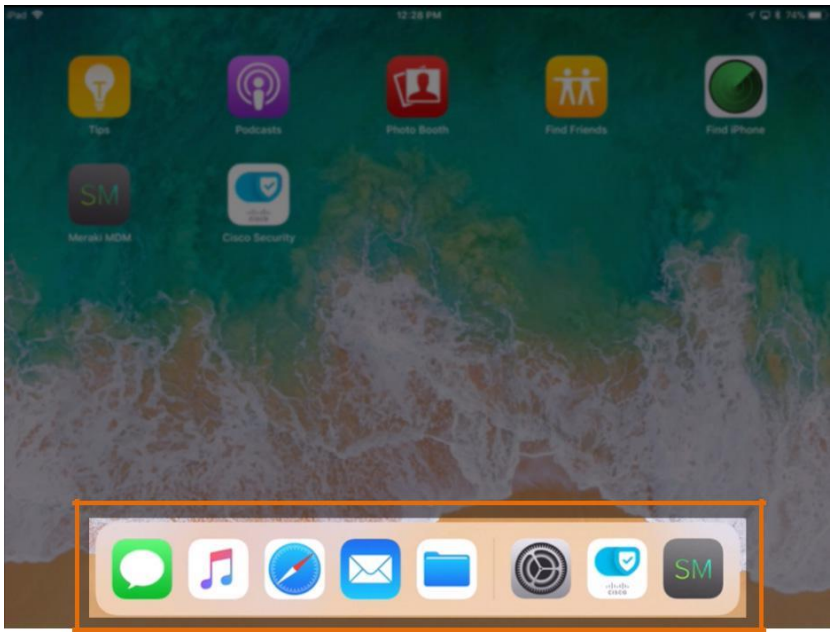
2. iOS デバイスのインタラクティブ デモは、新しいブラウザ タブで起動します。デモを開始するには、[再生（Play）] ボタンをクリックするか、またはブラウザ ウィンドウ内の任意の場所をクリックします。

図 73. インタラクティブ デモの開始ウィンドウ



3. iPad のホーム画面が表示されます。画面下部のドック領域以外はグレーアウトされます。

図 74. ドックを強調する iPad ホーム画面

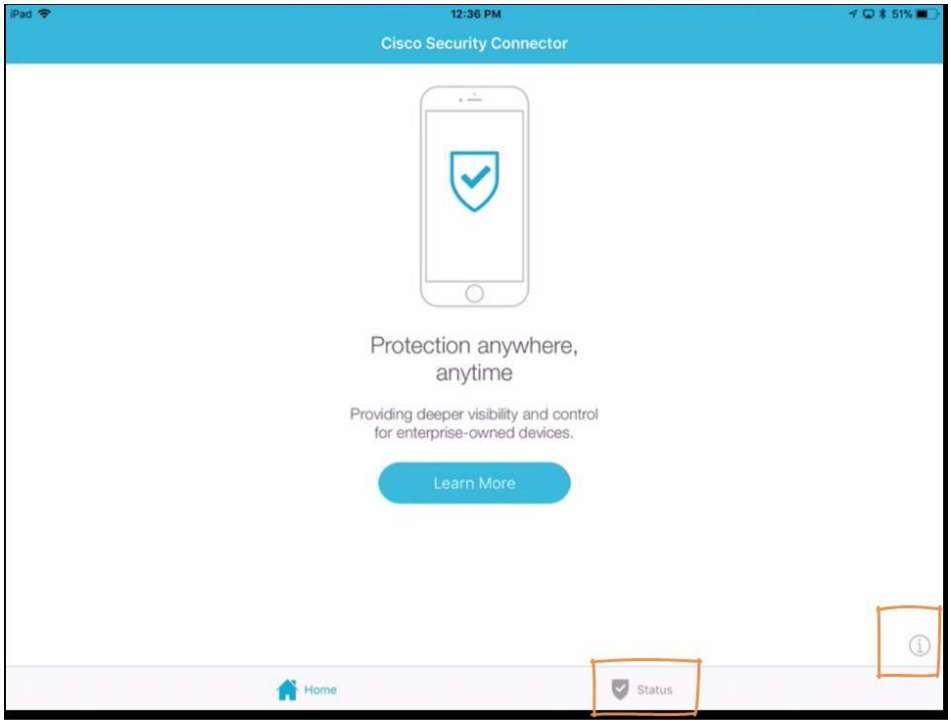


4. ドック領域から、右側の [CSC] アプリ アイコンをクリックします。

図 75. メッセージ アプリ

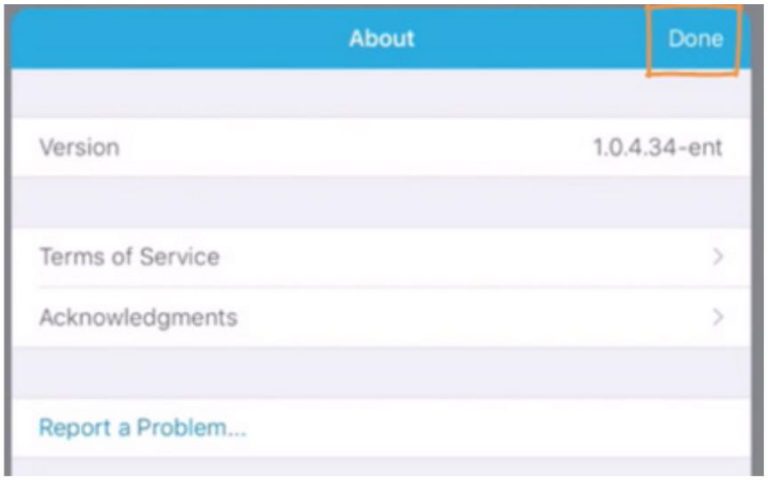
5. CSC アプリが起動し、そのホーム ページが表示されます。

図 76. CSC ホーム ページ



6. 右下の情報ボタンをクリックして、アプリケーションのバージョンなどに関する情報を示す [概要（About）] ページを表示します。

図 77. [概要（About）] ページ



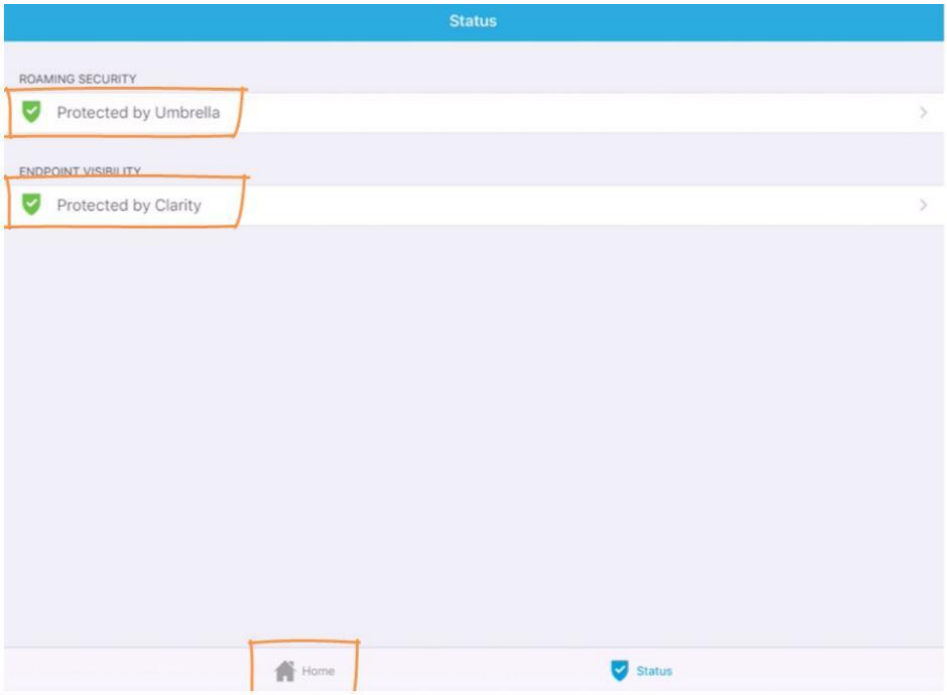
ヒント：問題が生じた場合、[問題の報告（Report a Problem）] をクリックしてログ ファイルを収集できます。ログ ファイルは、新規の電子メール メッセージに添付し、管理者またはシスコに送信できます。

7. [概要（About）] ページの上にある [完了（Done）] をクリックして、CSC ホーム ページに戻ります。

8. [ステータス（Status）] をクリックして [ステータス（Status）] ページを開きます。

9. この場合、Umbrella と Clarity の両方のエンティティがプロビジョニングされ、両方が適用されます。

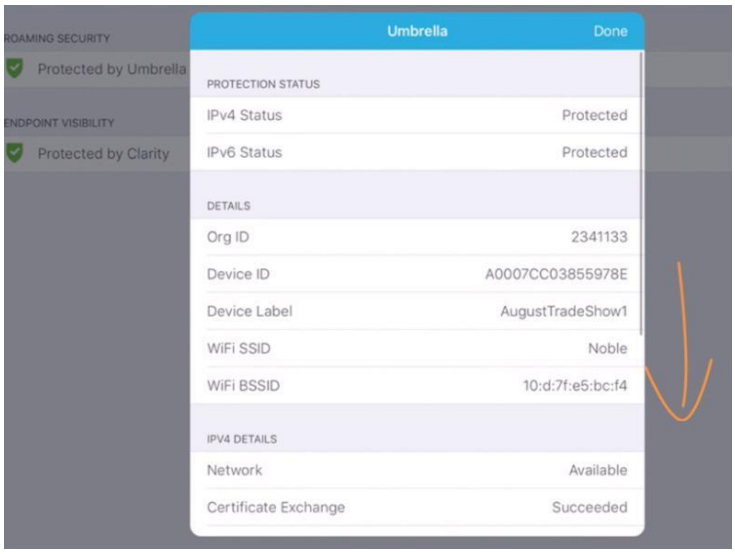
図 78. [CSC ステータス（CSC Status）] ページ



ヒント：続く手順では、最初に Umbrella エンティティ、次に Clarity エンティティをデモンストレーションします。必要に応じて順番を逆転させることができます。

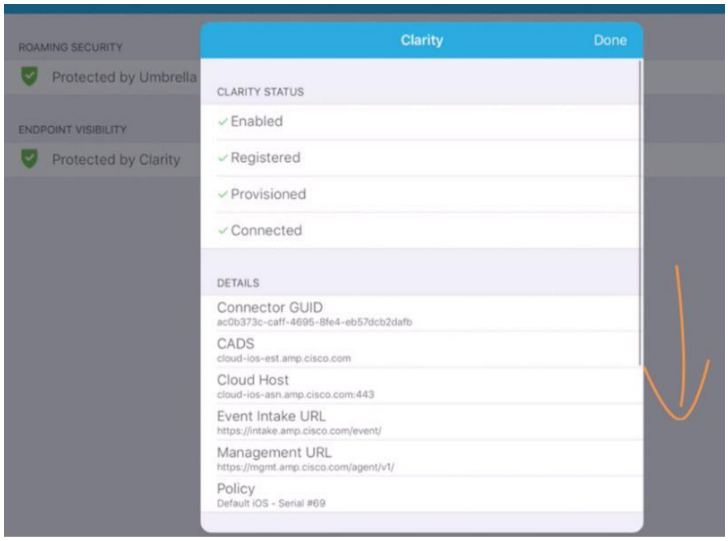
10. [Umbrella によって保護（Protected by Umbrella）] をクリックします。Umbrella スプラッシュ ページが開き、Umbrella 展開の詳細が表示されます。

図 79. Umbrella スプラッシュ ページ



11. 表示されるステータスの詳細には、IPv4 および IPv6 値、Umbrella org（企業アカウント）、デバイス ID、接続された Wi-Fi、Umbrella リゾルバ IP、および証明書詳細が含まれます。
12. オレンジの矢印をクリックしてスクロール ダウンします。
13. Umbrella スプラッシュ ページの上にある [完了（Done）] をクリックして、[CSC ステータス（CSC Status）] ページに戻ります。
14. [Clarity によって保護（Protected by Clarity）] をクリックします。Clarity スプラッシュ ページが開き、Clarity 展開の詳細が表示されます。

図 80. Clarity スプラッシュ ページ



15. 表示されるステータスの詳細には、4 つのメイン ステータスの状態と、他の接続、ホスト、およびデバッグについての情報が含まれています。
16. オレンジの矢印をクリックしてスクロール ダウンします。
17. [Clarity スプラッシュ（Clarity splash）] ページの上にある [完了（Done）] をクリックして、[CSC ステータス（CSC Status）] ページに戻ります。
18. 赤色のホーム ボタンをクリックして、デバイスのホーム画面に戻ります。
19. 次に、監視モードでデバイスの管理設定を参照します。
20. ドック領域から、右側の [設定（Settings）] アイコンをクリックします。

図 81. デバイス設定（Device Settings）

21. [設定（Settings）] メイン ページで、左上の領域（オレンジ色の境界線で強調表示される）をクリックして、監視モードの説明を表示します。

図 82. デバイスの監視

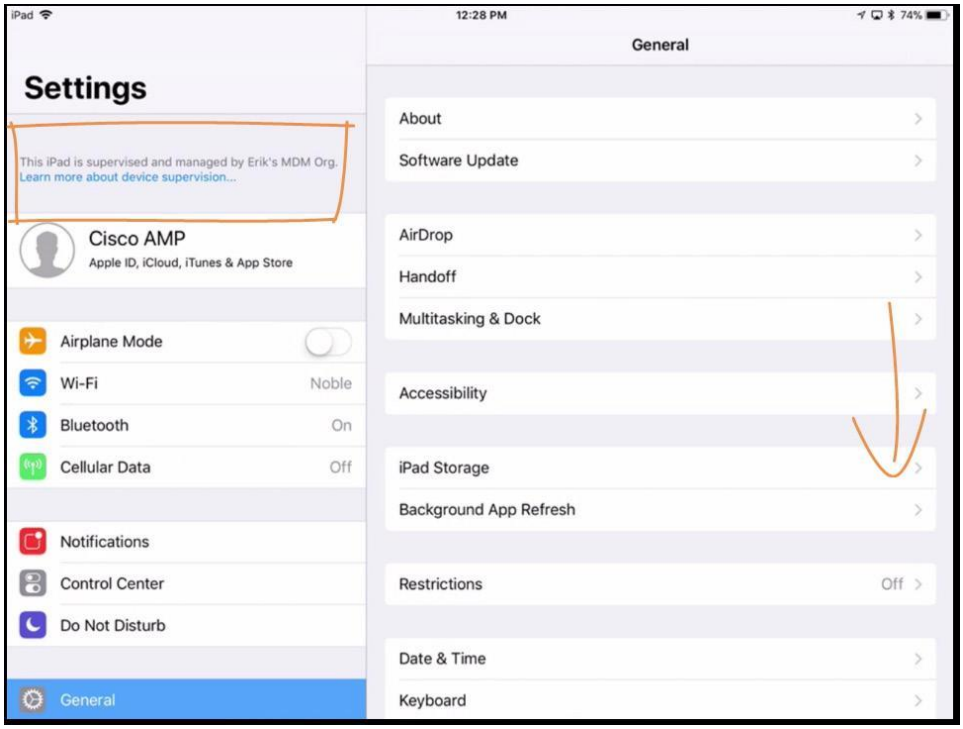
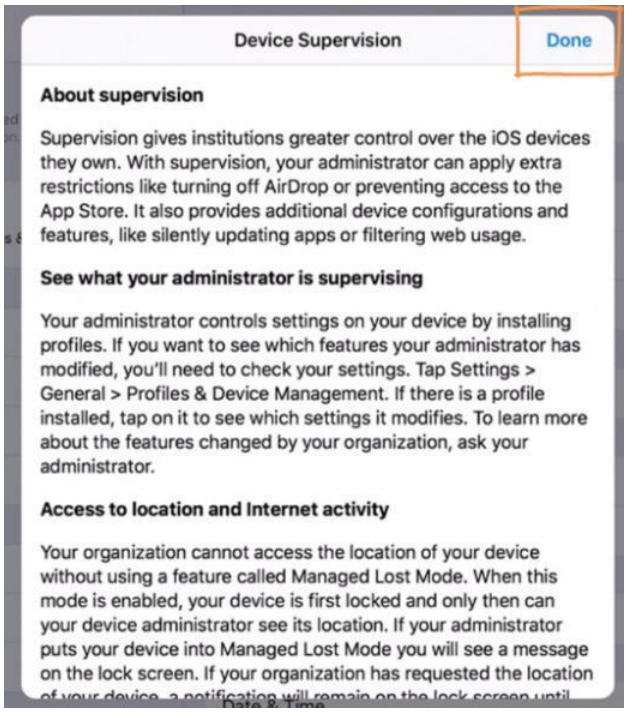


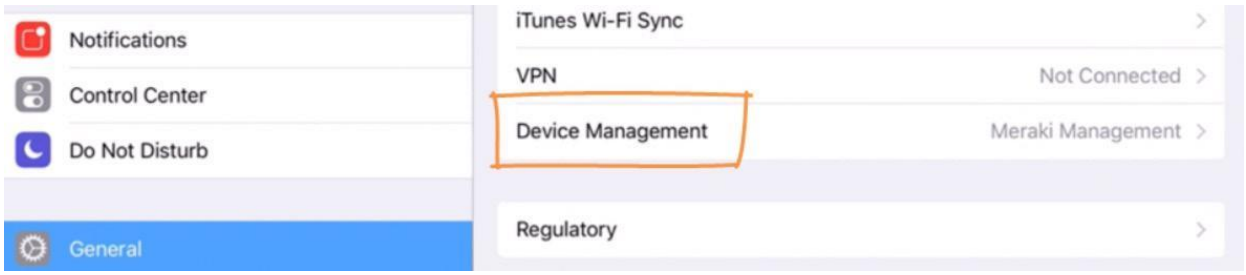
図 83. デバイスの監視



注：Cisco CSC は、監視モードでインストールされた iOS デバイス上でのみサポートされます。監視モードに関するこの説明がデバイス上にない場合、デバイスは監視モードではありません。

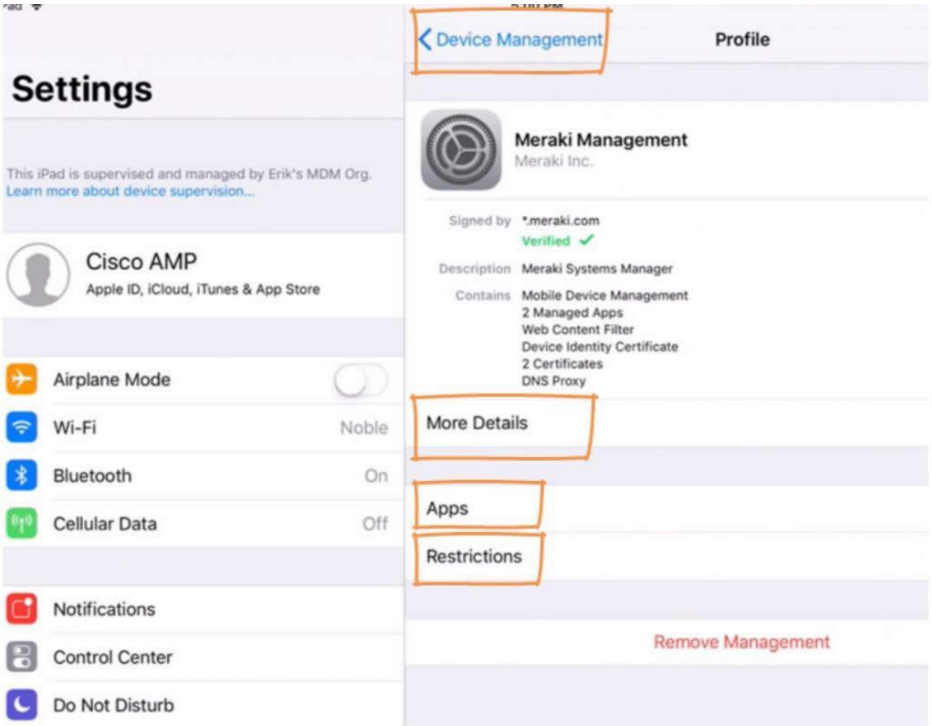
22. 上部の [完了（Done）] をクリックして、[設定（Settings）] ページに戻ります。
23. 次に、特定の監視設定のいくつかを考察します。[設定（Settings）] ページの右側にあるオレンジ色の矢印をクリックして、スクロール ダウンします。
24. [デバイスの管理（Device Management）] をクリックします。

図 84. デバイス管理設定



25. [Meraki 管理（Meraki Management）] メニューが開きます。

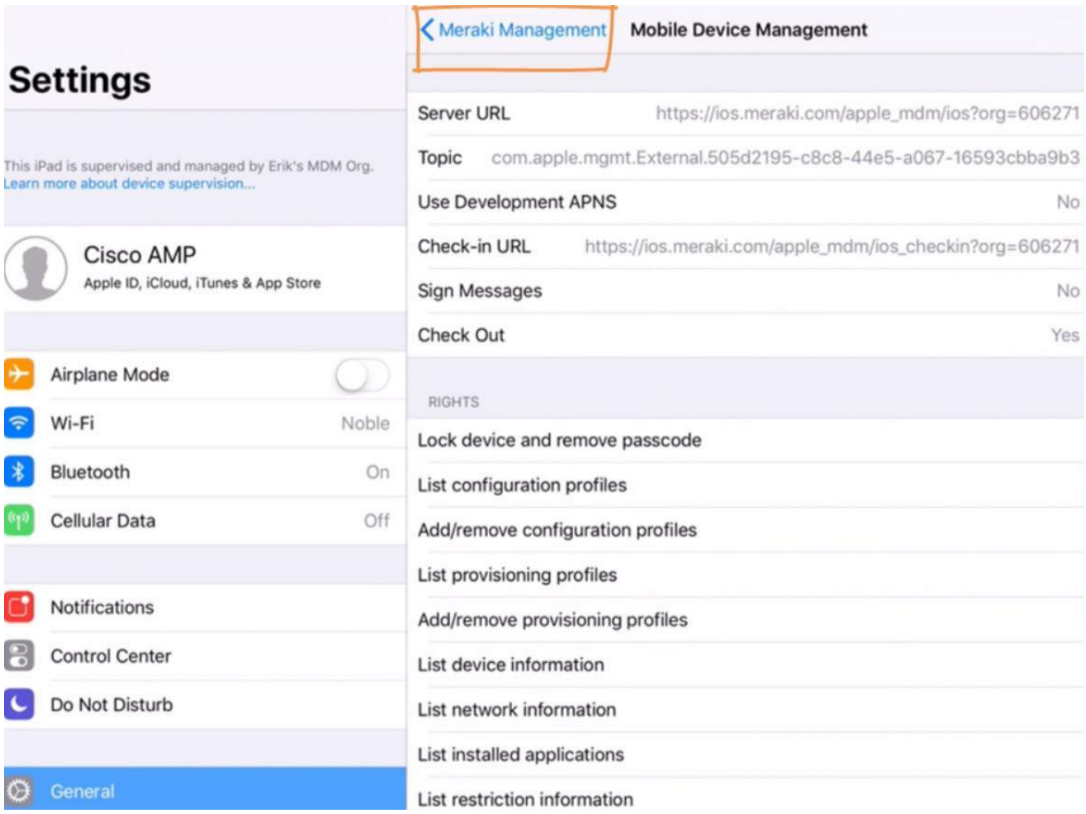
図 85. Meraki 管理



ヒント：[詳細（More Details）]、[アプリ（Apps）]、[制限（Restrictions）] という 3 つの項目をデモンストレーションする順序は、必要に応じて変更できます。

26. [詳細（More Details）] をクリックします。次のメニューから [モバイル デバイス管理（Mobile Device Management）] ページを開きます。

図 86. モバイル デバイス管理



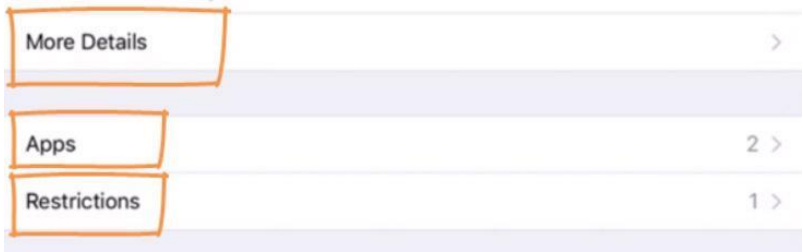
27. 上部の領域にある一般的な情報と、下にリストされている**権限**を説明します。これらの設定は MDM で構成され、デバイスに適用されます。上部の [Meraki 管理（Meraki Management）] をクリックして、[Meraki 管理（Meraki Management）] ページに戻ります。

28. [アプリケーション（Apps）] をクリックします。

注：簡潔に表示されるプロファイルのリストには、Meraki と Umbrella のプロビジョニング中のデバイスにプッシュされる署名証明書が含まれています。これにはポリシー作成時のシナリオ 4 で説明したとおり、SSL 検査に必要な Umbrella ルート証明書も含まれます。

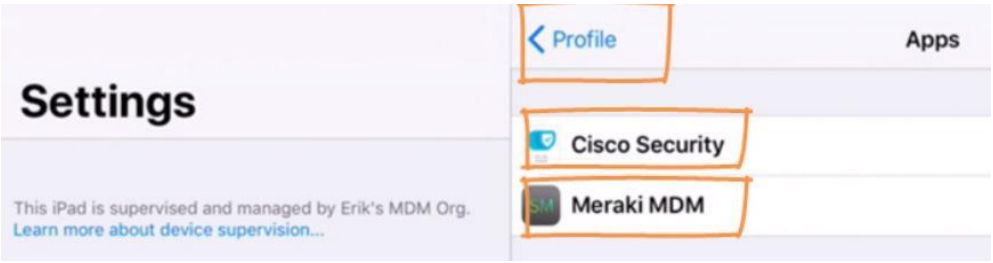
ヒント：スペース バーを押すと、デモを一時停止してプロファイルを表示できます。続行するにはページの任意の場所をクリックします。

図 87. Meraki 管理



29. [アプリ（Apps）] ページが開きます。このデバイスには MDM、Meraki SM アプリ（MDM 管理に必要）、および CSC により管理される 2 つのアプリがあります。

図 88. [アプリ（Apps）] ページ



30. インストール済みのアプリの詳細を表示するには、それぞれのアプリ アイコンをクリックします。それぞれのケースで、上部の [アプリ（Apps）] をクリックして、[アプリ（Apps）] ページに戻ります。

図 89. Cisco セキュリティ アプリ

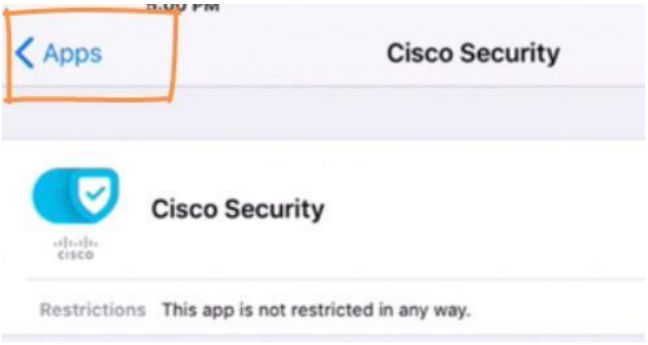


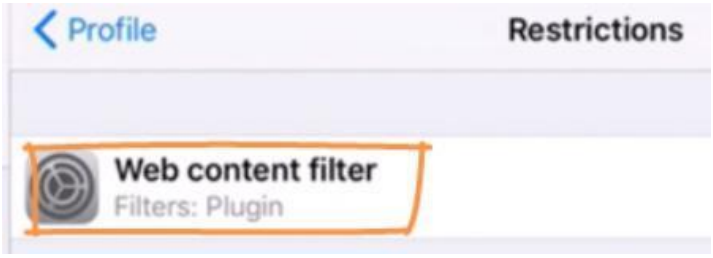
図 90. Meraki MDM アプリ

31. [プロファイル（Profile）] をクリックして、[Meraki 管理（Meraki Management）] ページに戻ります。

図 91. Meraki 管理

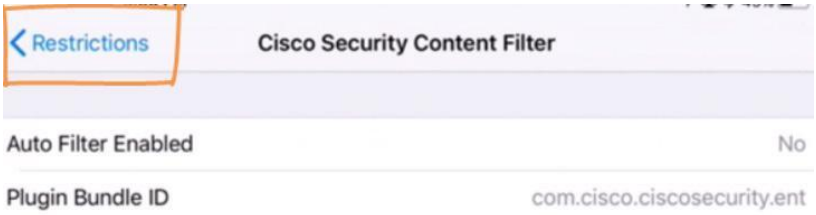
32. [制限（Restrictions）] をクリックします。
33. [制限（Restrictions）] ページで [Web コンテンツ フィルタ（Web Content Filter）] をクリックします。

図 92. Web コンテンツ フィルタ



34. [Cisco Security Content フィルタ（Cisco Security Content Filter）] ページが開きます。CSC が展開されるときに Umbrella を介して適用される制限の詳細が表示されます。

図 93. Cisco セキュリティ コンテンツ フィルタ



35. [制限（Restrictions）] をクリックして、[Meraki 管理（Meraki Management）] ページに戻ります。
36. [Meraki 管理（Meraki Management）] ページから、[デバイス管理（Device Management）] をクリックしてメインの [設定（Settings）] ページに戻るか、赤色のホーム ボタンをクリックしてデバイスのホーム画面に戻ることができます。
37. ブラウザで CSC デモ ランディング ページに戻って、他の任意のデモ シナリオを繰り返します。他のデモ シナリオのために、インタラクティブ デモが表示されたブラウザ タブは開いたままにしておきます。

まとめ

要約すると、iOS 11、Meraki System Manager、Cisco Umbrella、および Cisco Clarity を統合するシスコの統合セキュリティ アーキテクチャは、iOS ユーザを保護する最も簡単かつ効果的な方法です。これは Apple の監視対象 11 iOS デバイス向けの、唯一の完全統合型の企業対応セキュリティ ソリューションです。これは Apple とシスコとの強力なパートナーシップがなければ実現しませんでした。

Cisco Security Connector を展開することで、1 つのアプリで 2 つのセキュリティ層を取得できます。

1. iOS デバイスがネットワークの内外でインターネットに接続する際には、他の企業所有デバイスと同じレベルの制御と可視性を持つことができます。
2. インシデント調査中には、監査に関する可視性がチームに提供されます。また、SSL 復号を有効にすることなく、アプリが接続している場所を相関付けできます。

企業対応とはつまり、Apple とシスコが実現したソリューションが、エンドユーザの作業を中断させたり、管理者ユーザにギャップを残すことがないということを意味します。

Umbrella で保護されているユーザがすでに存在する場合には、その監視対象となっている iOS デバイスに保護を拡張するための追加料金は発生しません。さらに、AMP for Endpoints のライセンス発行時に iOS デバイスを含めた場合には、Clarity でその保護を拡張することもできます。

必要な可視性と制御のレベルに基づいて、一方または両方の層を使用し、Meraki Systems Manager でシームレスにソリューションを展開および設定できます。

次のステップ

お客様に POV for AMP、Umbrella、および Systems Manager を紹介する

- Umbrella
- AMP
- Meraki Systems Manager

参考リンク

- At-a-glance データ シート

お問い合せ先

シスコシステムズ合同会社

〒107 - 6227 東京都港区赤坂 9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp