

Cisco Security Connector(CSC)で使用するiOSデバイスを監視する方法

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[設定](#)

概要

このドキュメントでは、Clarityと共に使用するために、ローカルでApple iOSデバイスを監視する方法について説明します。Cisco Security Connector(CSC)/Clarityの主な要件は、iOSデバイスをAMPまたはUmbrellaと組み合わせて使用し、これらのデバイスを監視する必要があることです。デバイスはDEPプログラムまたはApple Configuratorを通じてAppleから購入した場合に監視できます。監視は、iOS 5でAppleによって導入された特別なモードで、管理者が通常の許可よりも多くのデバイスを制御できます。監視モードは、制度的に所有されるデバイスで使用されることを意図しています。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Apple iOSデバイス11.3以降
- Apple Configurator 2 (Macでのみ利用可能)

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期 (デフォルト) 設定の状態から起動しています。ネットワークが稼働中の場合は、設定が及ぼす潜在的な影響について確実に理解しておく必要があります。

背景説明

Cisco Security Connectorは、組織が所有するiOSデバイスに対して、これまでにない可視性と制御を提供します。この機能は、エンドポイント向けAMP ClarityおよびUmbrellaと組み合わせて、次の機能を提供します。

- ネットワークとデバイスのトラフィックを可視化
- 各デバイスのアプリインベントリ。
- ユーザおよびレポートのフィッシングサイトを自動的にブロックし、フィッシングリンクをクリックしたユーザを特定します。
- 悪意のあるドメインへの接続をブロックするため、機密データは保護されたままになります。

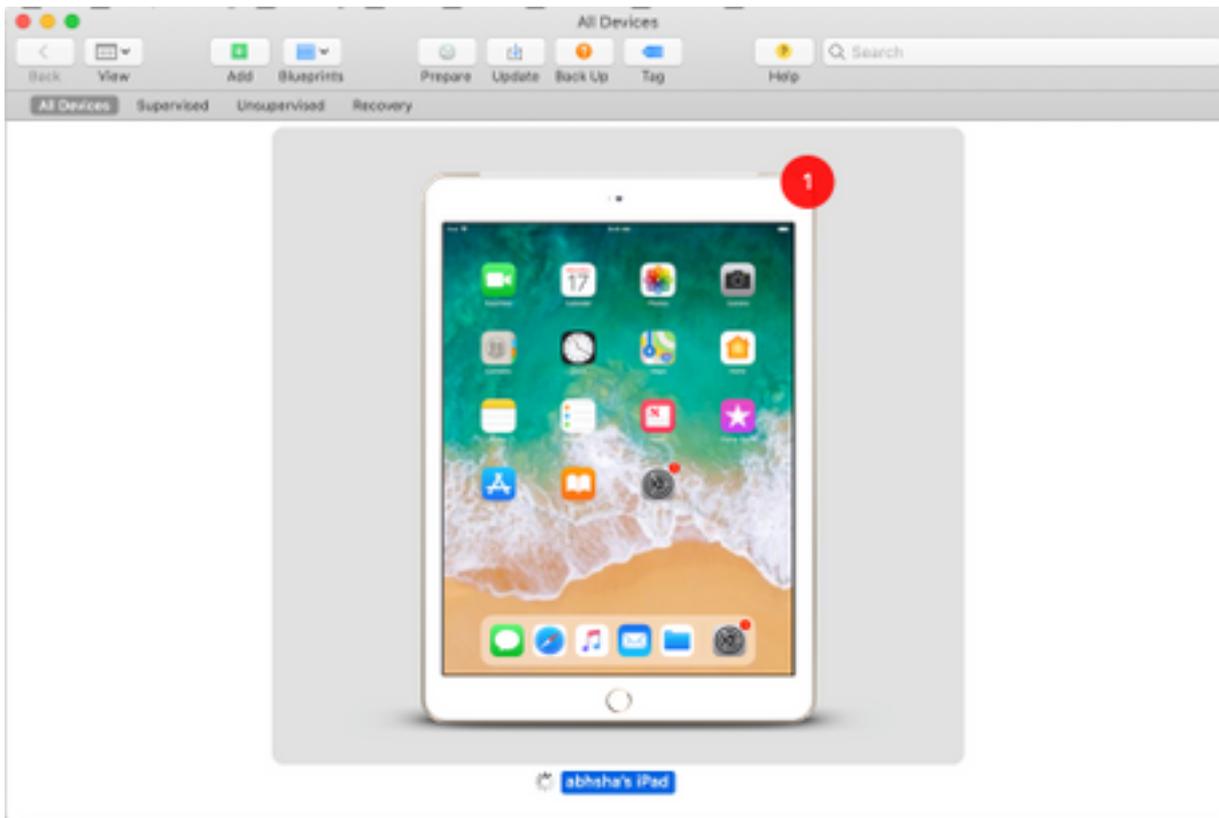
設定

警告：デバイスを監視するために、デバイスは完全にワイプされます。したがって、デバイスのバックアップを取っていることを確認してください。

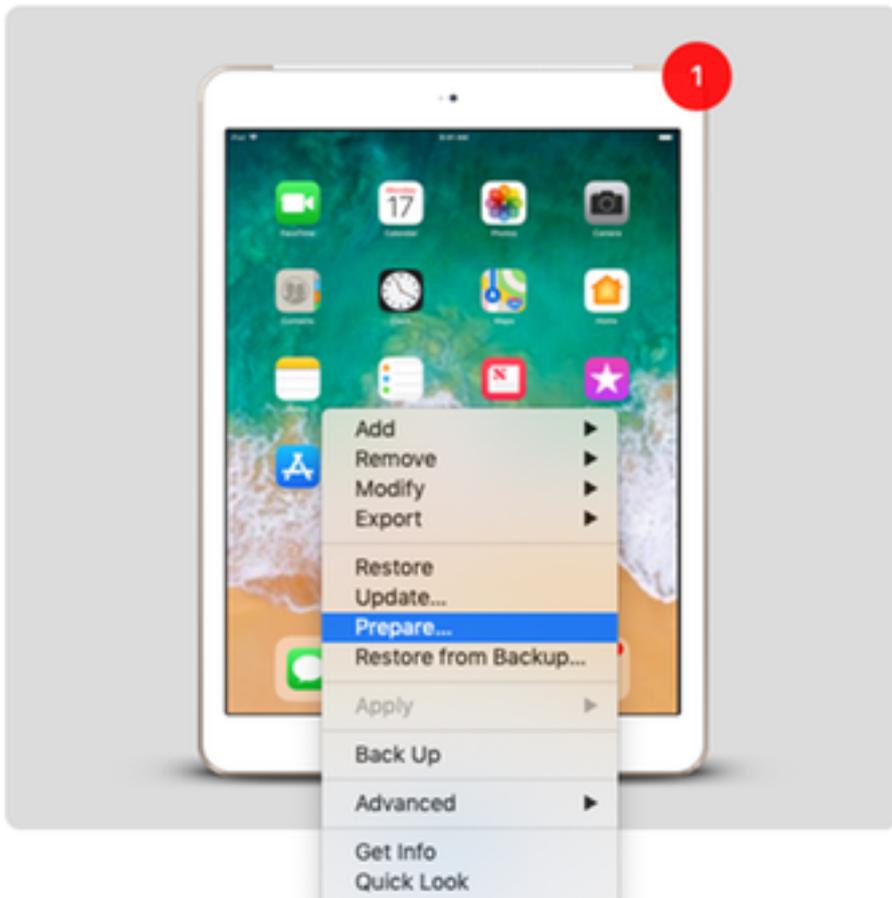
ステップ1:iOSデバイスをMacに接続します。

ステップ2:Apple Configuratorを起動します。

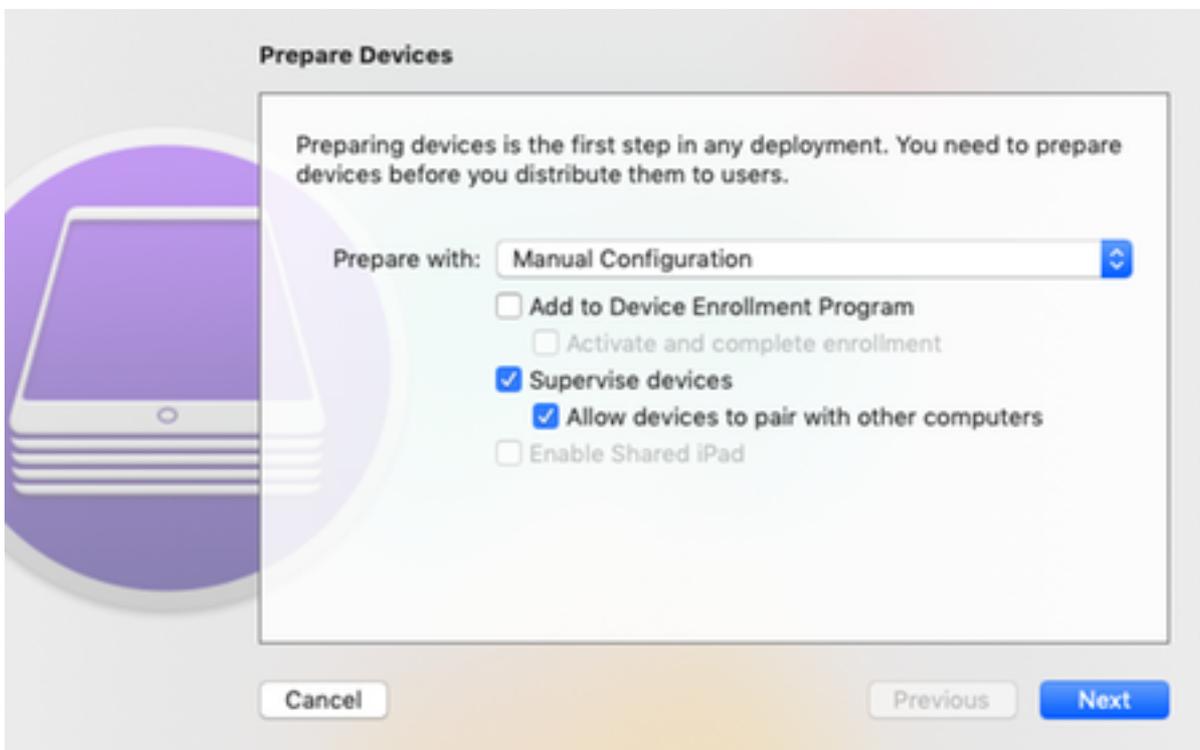
ステップ3：次の図に示すように、デバイスが表示されている必要があります。



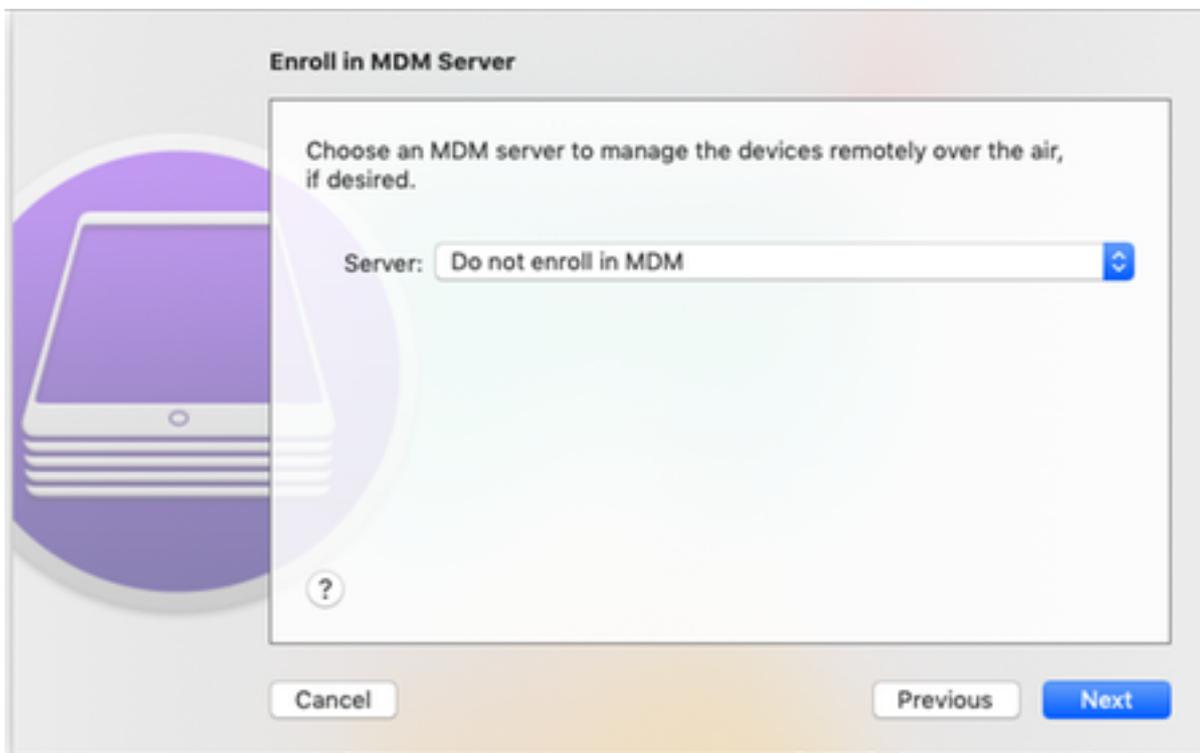
ステップ4：右クリックし、図に示すように[Prepare]を選択します。



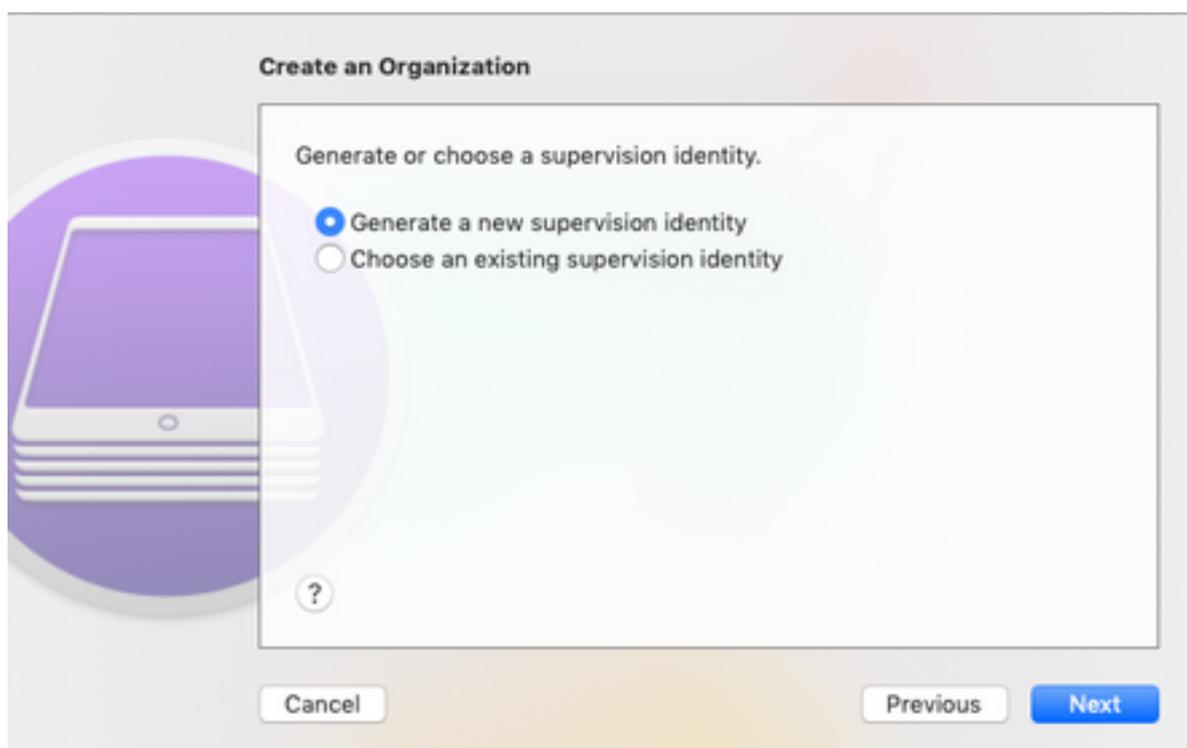
ステップ5:[Manual Configuration]を選択し、図に示すように、[Supervise devices]と[Allow devices to pair other computers]の両方のボックスをオンにし、[Next]をクリックします。



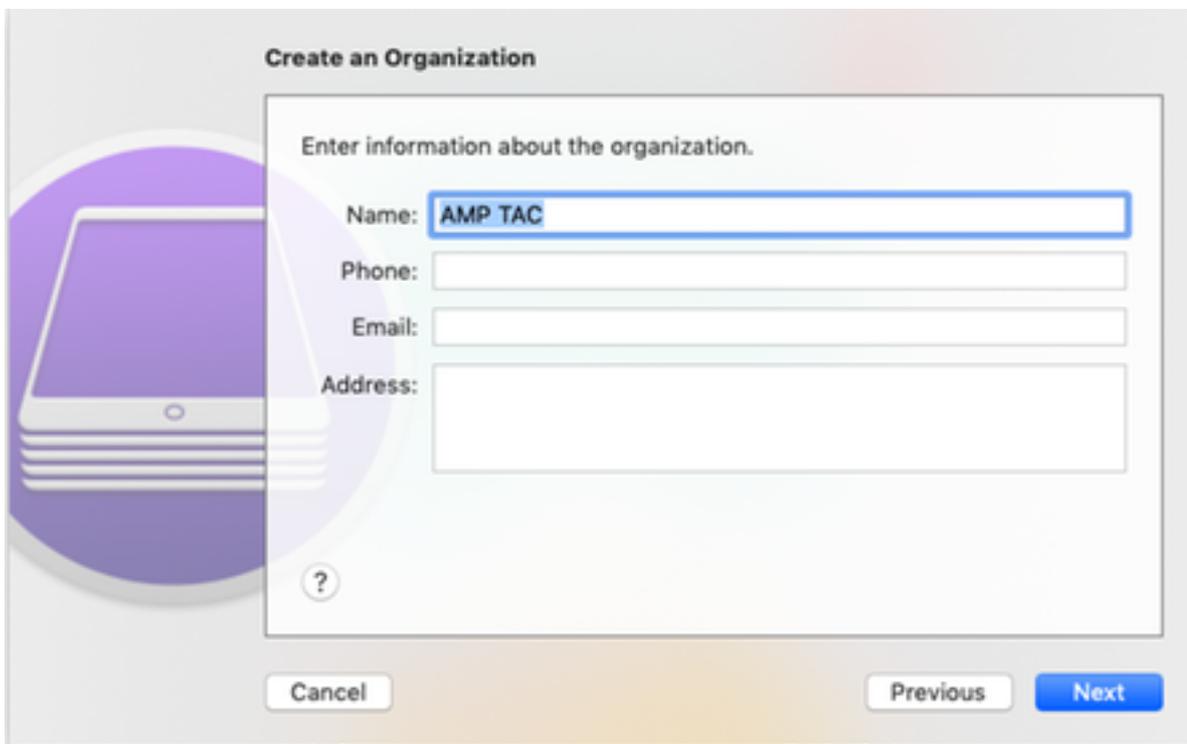
ステップ6：この段階でMDM経由で登録する必要はなく、[Next]をクリックします。



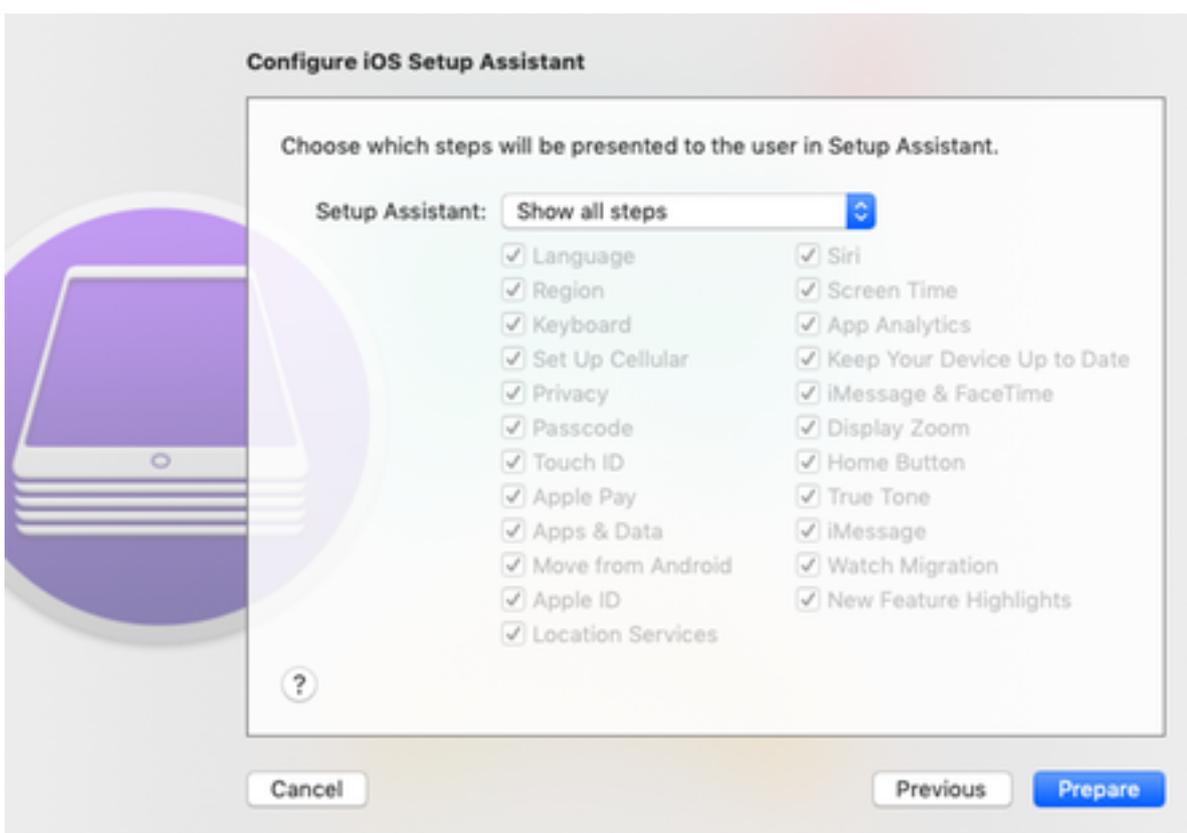
ステップ7:[Generate a new supervision identity]を選択して、デバイスを割り当てる新しい組織を作成し、[Next]をクリックします。



ステップ8：組織に名前を付け、[Next]をクリックします。



ステップ9:[Prepare]をクリックします。



ステップ10：準備のためにiPadを消去するようにプロンプトが表示されます。バックアップ後にiPadを消去する場合に選択します。

ステップ11:iPadが再び起動した後、CSCで使用できるように監視する必要があります。