Überwachen eines iOS-Geräts für die Verwendung mit dem Cisco Security Connector (CSC)

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie ein lokal zu verwendendes Apple iOS-Gerät mit Clarity überwacht wird. Eine wichtige Anforderung für die Verwendung von Cisco Security Connector (CSC)/Clarity besteht darin, dass die iOS-Geräte zusammen mit AMP und/oder Umbrella verwendet werden und diese Geräte überwacht werden müssen. Geräte können überwacht werden, wenn sie von Apple über das DEP-Programm oder über Apple Configurator erworben werden. Die Überwachung wurde von Apple in iOS 5 als spezieller Modus eingeführt, der einem Administrator mehr Kontrolle über ein Gerät bietet als dies normalerweise zulässig ist. Der Überwachungsmodus ist für die Verwendung auf Geräten vorgesehen, die institutionell gehören.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Apple iOS-Gerät 11.3 und höher
- Apple Configurator 2 (nur auf Mac verfügbar)

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen von Konfigurationen verstehen.

Hintergrundinformationen

Cisco Security Connector bietet beispiellose Transparenz und Kontrolle für unternehmenseigene iOS-Geräte. Kombiniert mit AMP für Endgeräte-Transparenz und Umbrella bietet diese Funktion:

- Transparenz für Netzwerk- und Gerätedatenverkehr
- App-Bestand für jedes Gerät.
- Automatische Blockierung von Phishing-Sites für Benutzer und Berichte, um zu ermitteln, wer auf Phishing-Links geklickt hat.
- Sperren von Verbindungen zu schädlichen Domänen, damit vertrauliche Daten geschützt bleiben.

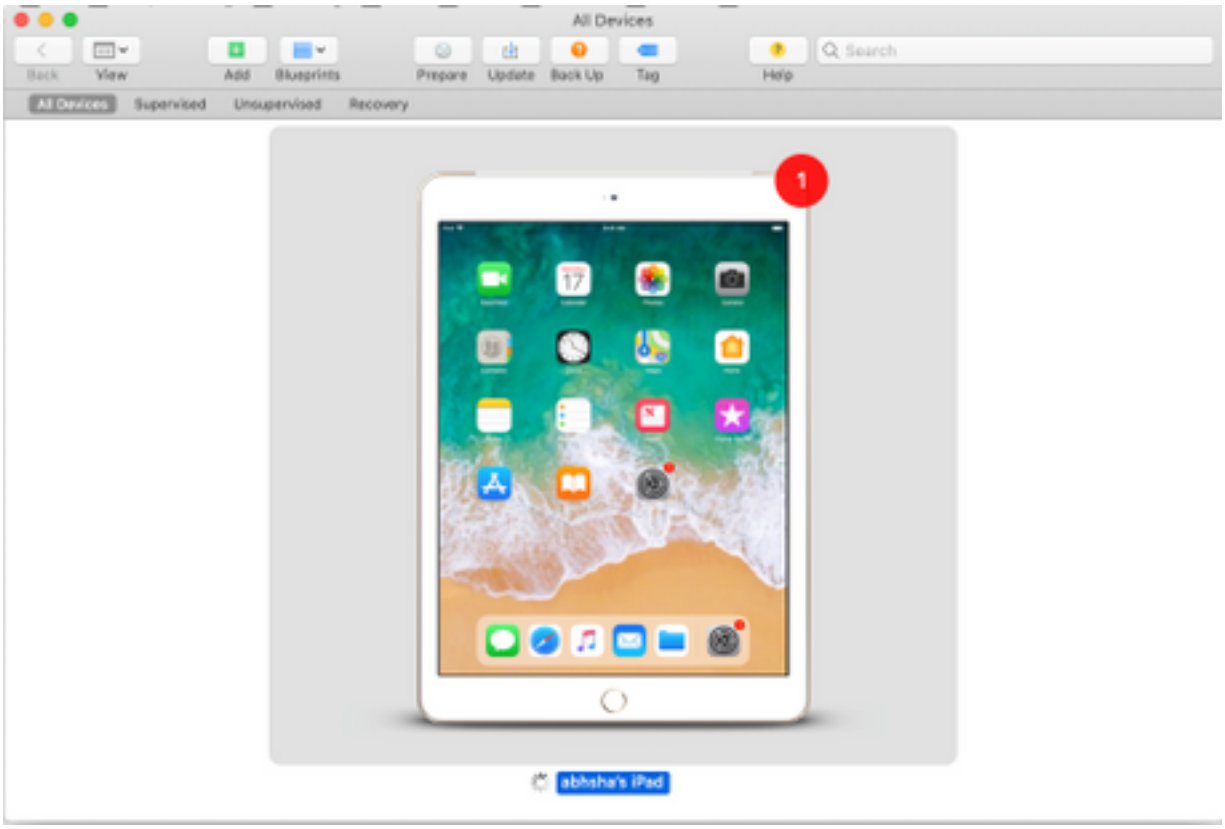
Konfigurieren

> **Warnung**: Um ein Gerät zu überwachen, wird es vollständig gelöscht. Stellen Sie daher sicher, dass Sie eine Sicherung des Geräts durchgeführt haben.

Schritt 1: Verbinden Sie Ihr iOS-Gerät mit Ihrem Mac.

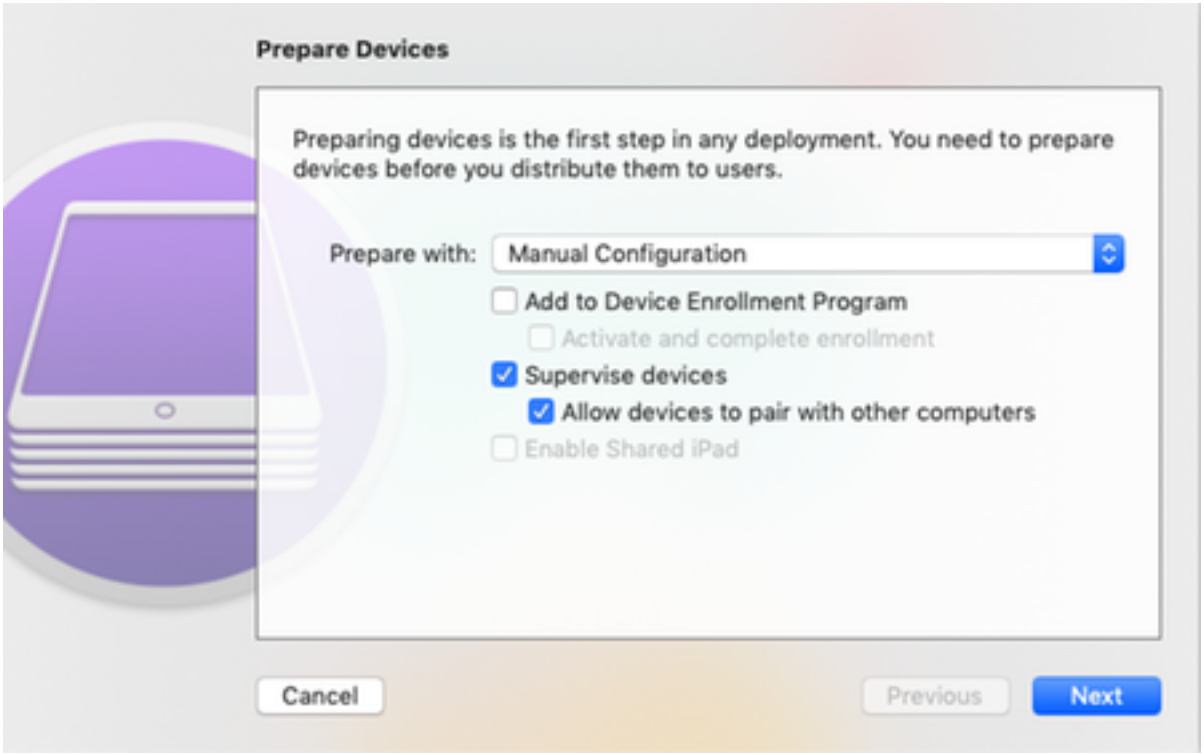
Schritt 2: Apple Configurator starten.

Schritt 3: Sie müssen Ihr Gerät wie im Bild hier gezeigt sehen.

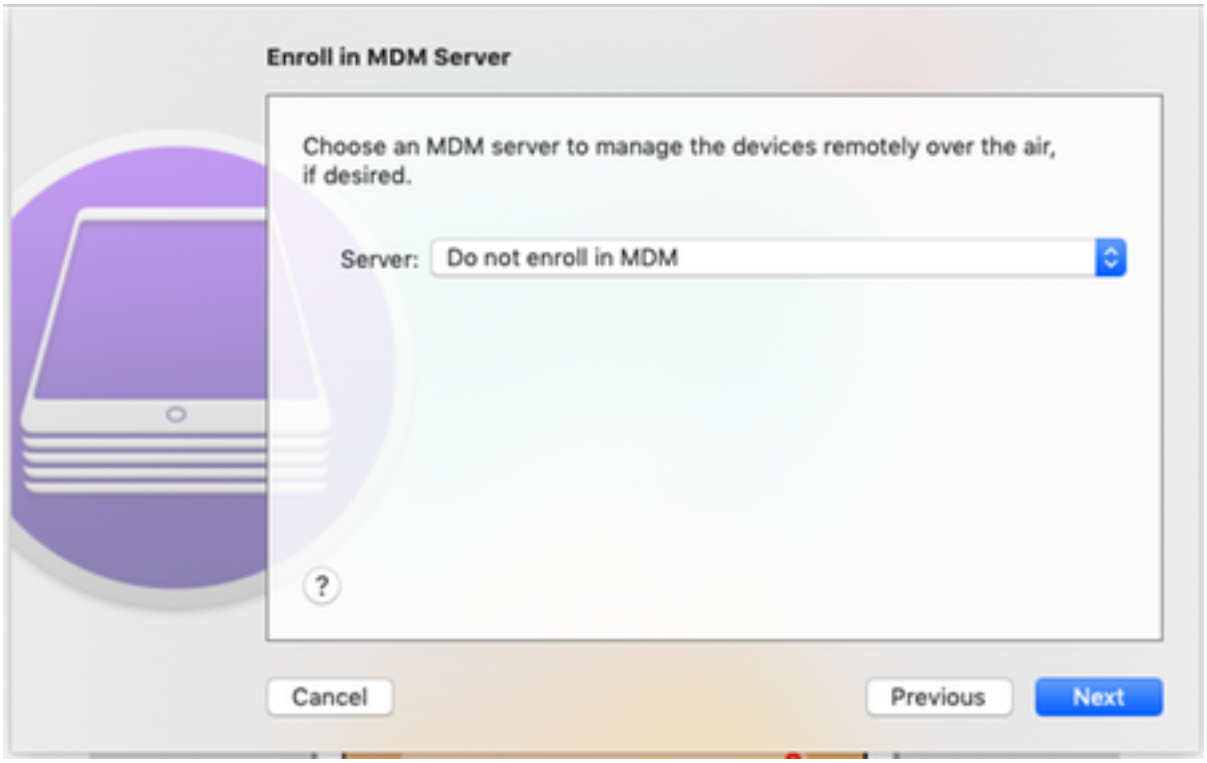


Schritt 4: Klicken Sie mit der rechten Maustaste, und wählen Sie **Bereiten** aus, wie im Bild gezeigt.

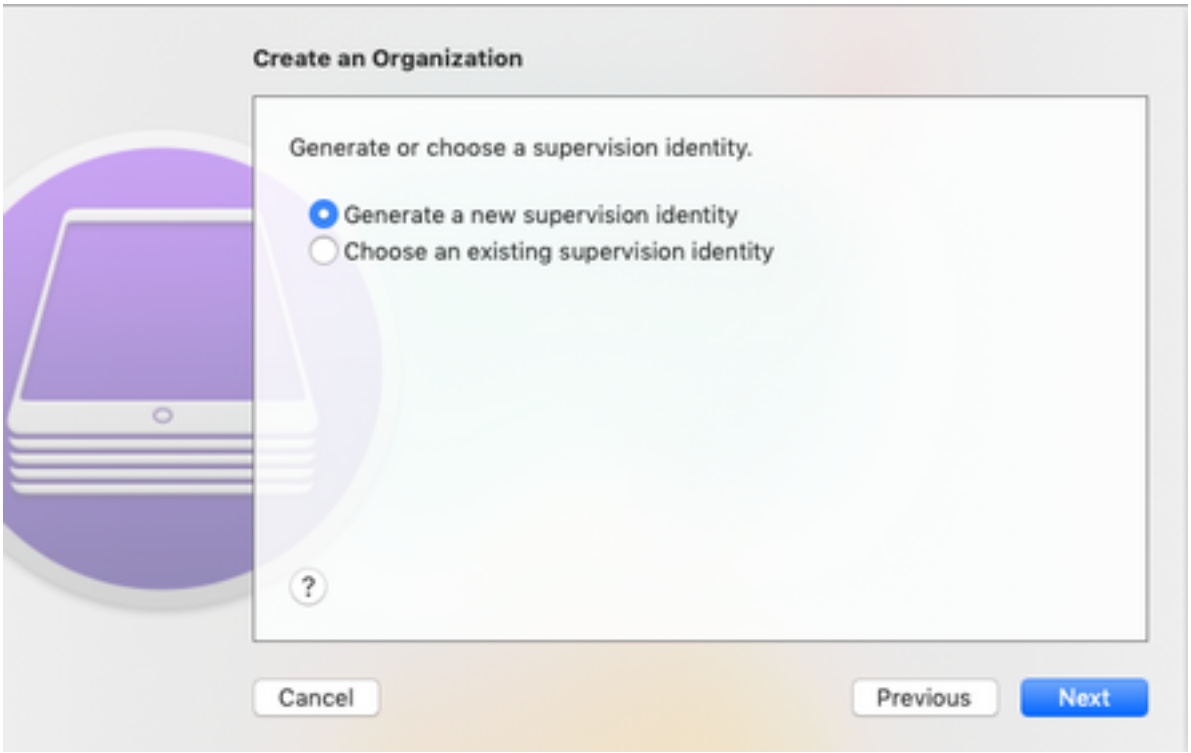
Schritt 5: Wählen Sie **Manual Configuration (Manuelle Konfiguration) aus**, und aktivieren Sie die Kontrollkästchen **Supervisor devices (Geräte überwachen)** und **Allow devices to pair with other computers (Geräte können mit anderen Computern verbunden werden**, wie im Bild hier gezeigt, und klicken Sie auf Next (Weiter).



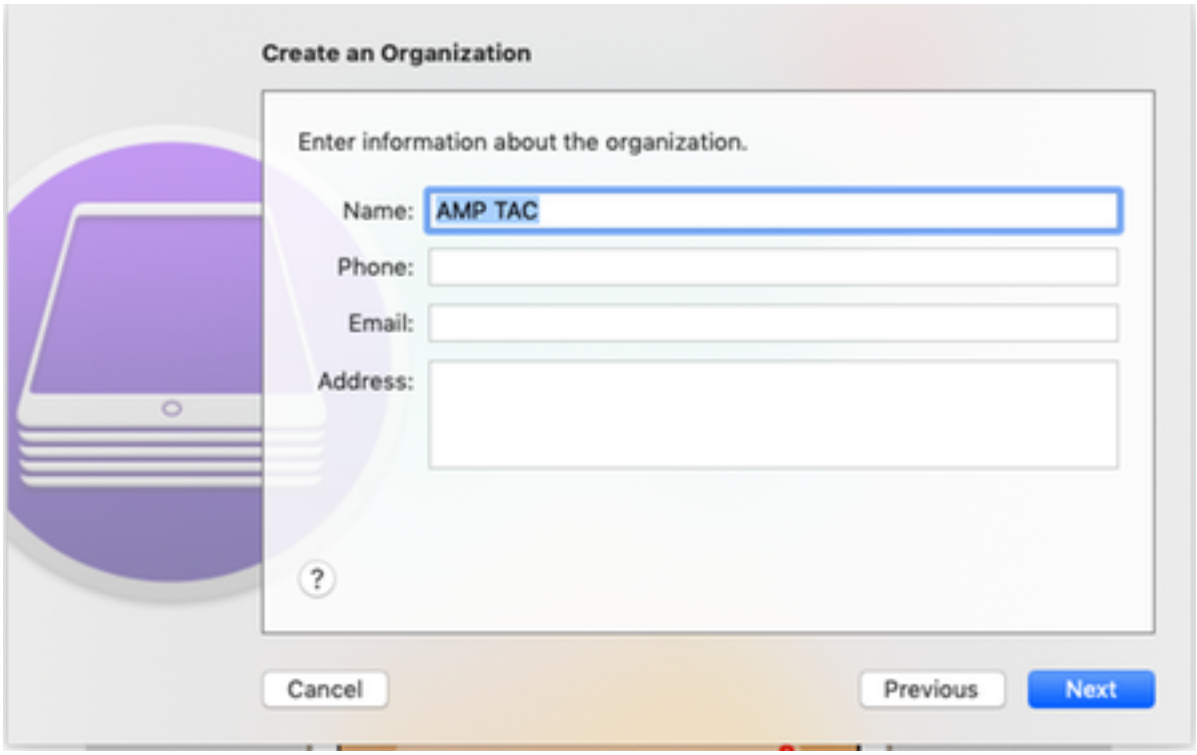
Schritt 6: Es ist nicht erforderlich, sich über MDM zu registrieren und auf "Weiter" zu klicken.



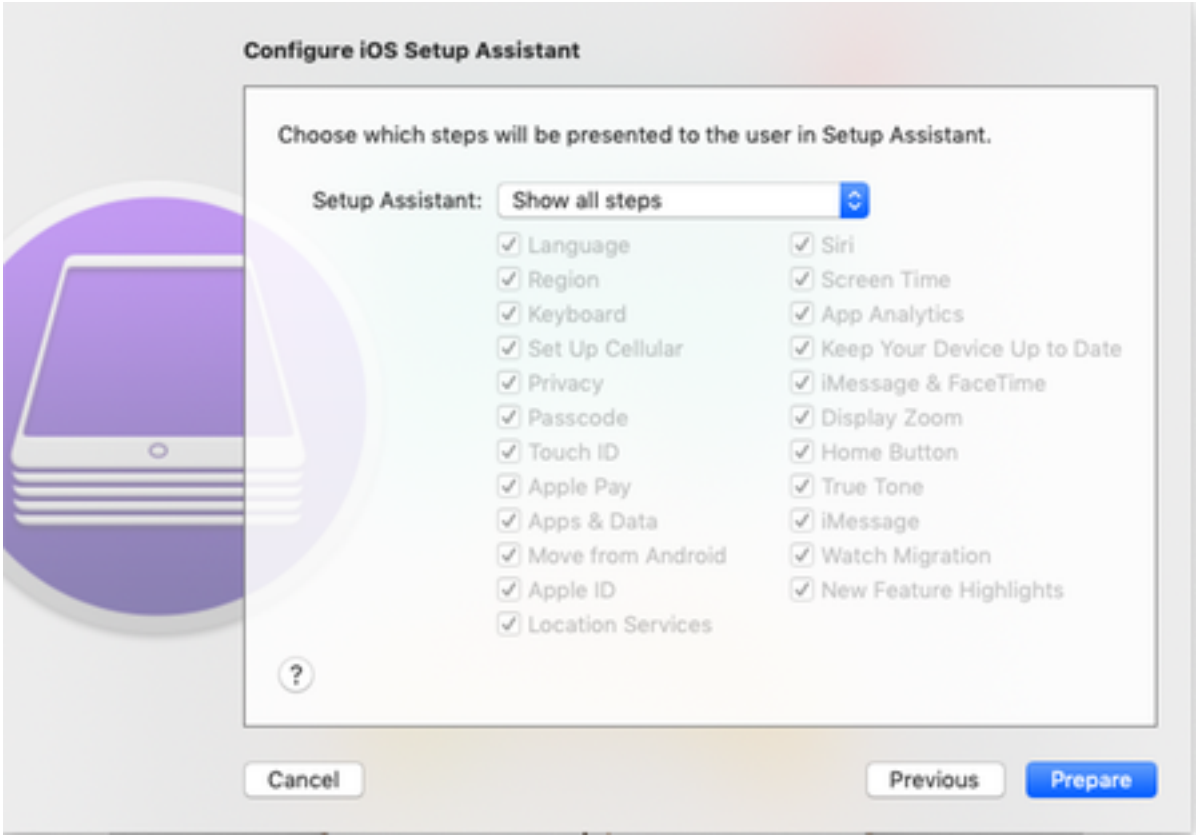
Schritt 7: Wählen Sie **Eine neue Überwachungsidentität erstellen**, um eine neue Organisation zu erstellen, der Geräte zugewiesen sind, und klicken Sie auf Weiter.



Schritt 8: Geben Sie dem Unternehmen einen Namen, und klicken Sie auf "Weiter".



Schritt 9: Klicken Sie auf **Vorbereiten**.



Schritt 10: Sie werden dann aufgefordert, das iPad zur Vorbereitung **zu löschen**. Wählen Sie diese Option aus, um das iPad zu löschen, nachdem Sie eine Sicherung durchgeführt haben.

Schritt 11: Nachdem Ihr iPad wieder hochgefahren ist, sollte dies überwacht und mit CSC einsatzbereit sein.