Comment superviser un appareil iOS à utiliser avec Cisco Security Connector (CSC) ?

Contenu

[Introduction](#)
[Conditions préalables](#)
[Conditions requises](#)
[Components Used](#)
[Informations générales](#)
[Configuration](#)

Introduction

Ce document décrit comment superviser un appareil Apple iOS, localement, à utiliser avec Clarté. L'utilisation de Cisco Security Connector (CSC)/Clarity nécessite que les périphériques iOS soient utilisés conjointement avec AMP et/ou Umbrella et que ces périphériques soient supervisés. Les périphériques peuvent être supervisés s'ils sont achetés auprès d'Apple via le programme DEP ou via Apple Configurator. La supervision a été introduite par Apple dans iOS 5 en tant que mode spécial qui donne à un administrateur un contrôle plus important sur un périphérique que ce qui est généralement autorisé. Le mode supervisé est destiné à être utilisé sur les périphériques appartenant à des institutions.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Appareil Apple iOS 11.3 et versions ultérieures
- Apple Configurator 2 (disponible uniquement sur Mac)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est actif, assurez-vous de bien comprendre l'impact potentiel de toutes les configurations.

Informations générales

Cisco Security Connector offre une visibilité et un contrôle sans précédent pour les périphériques iOS appartenant à l'entreprise. Combinée à AMP for Endpoints Clarity et Umbrella, cette fonctionnalité offre :

- Visibilité sur le trafic réseau et périphérique.
- Inventaire des applications pour chaque périphérique.
- Blocage automatique des sites d'hameçonnage pour les utilisateurs et les rapports afin d'identifier les personnes qui ont cliqué sur les liens d'hameçonnage.
- Blocage des connexions aux domaines malveillants pour que les données sensibles restent protégées.

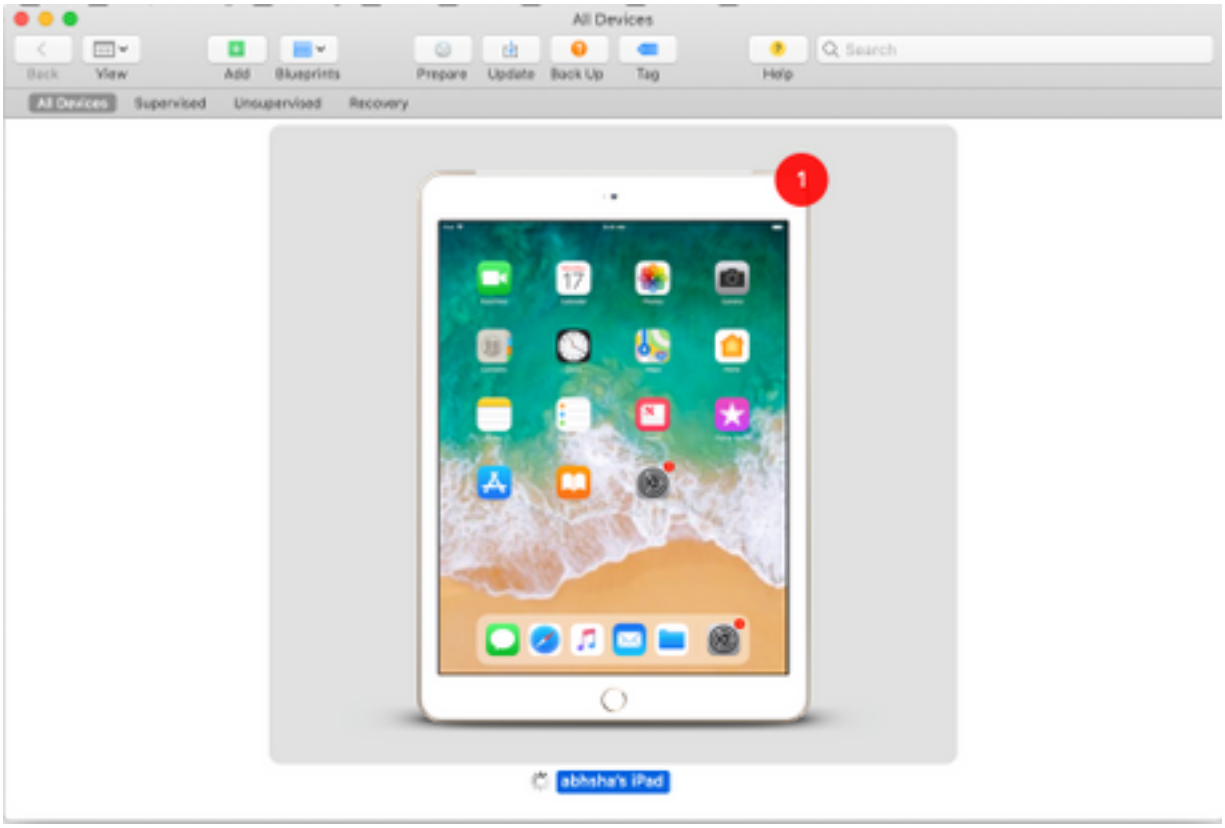
Configuration

> **Avertissement :** Afin de superviser un périphérique, il est entièrement effacé. Par conséquent, assurez-vous que vous avez effectué une sauvegarde du périphérique.

Étape 1. Connectez votre appareil iOS à votre Mac.

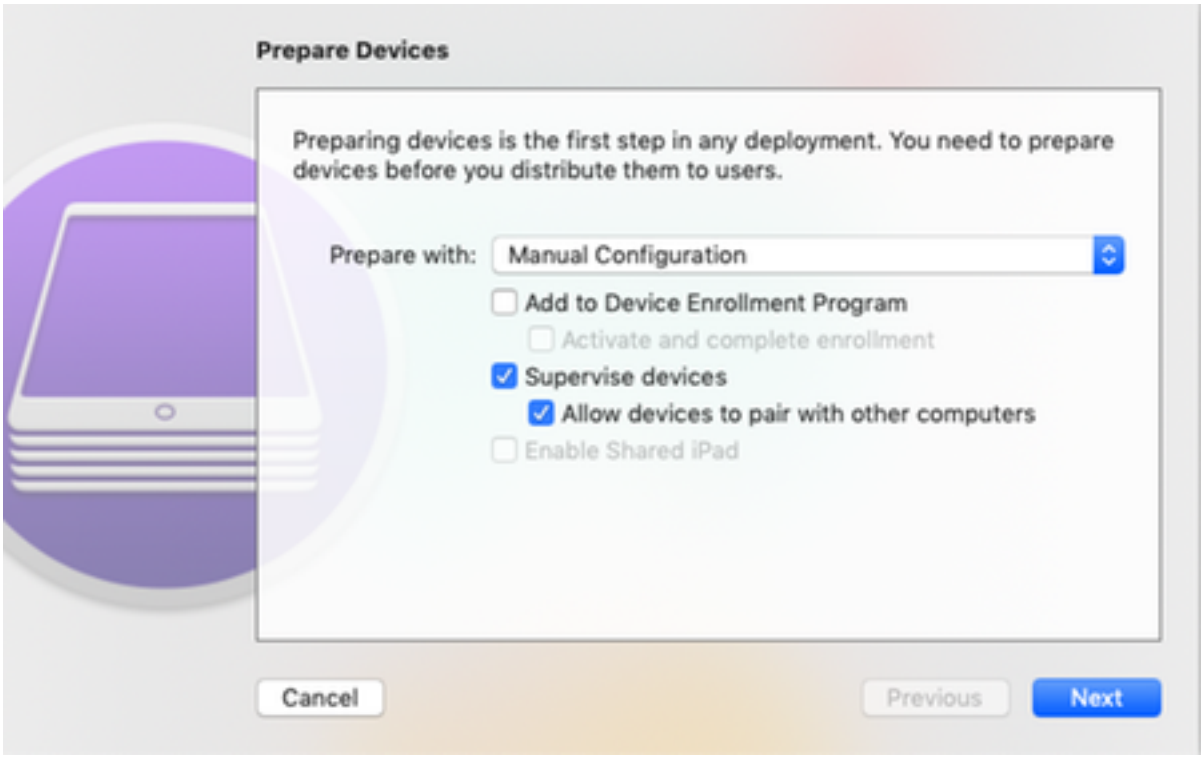
Étape 2. Lancez Apple Configurator.

Étape 3. Vous devez voir votre périphérique comme indiqué dans l'image ici.

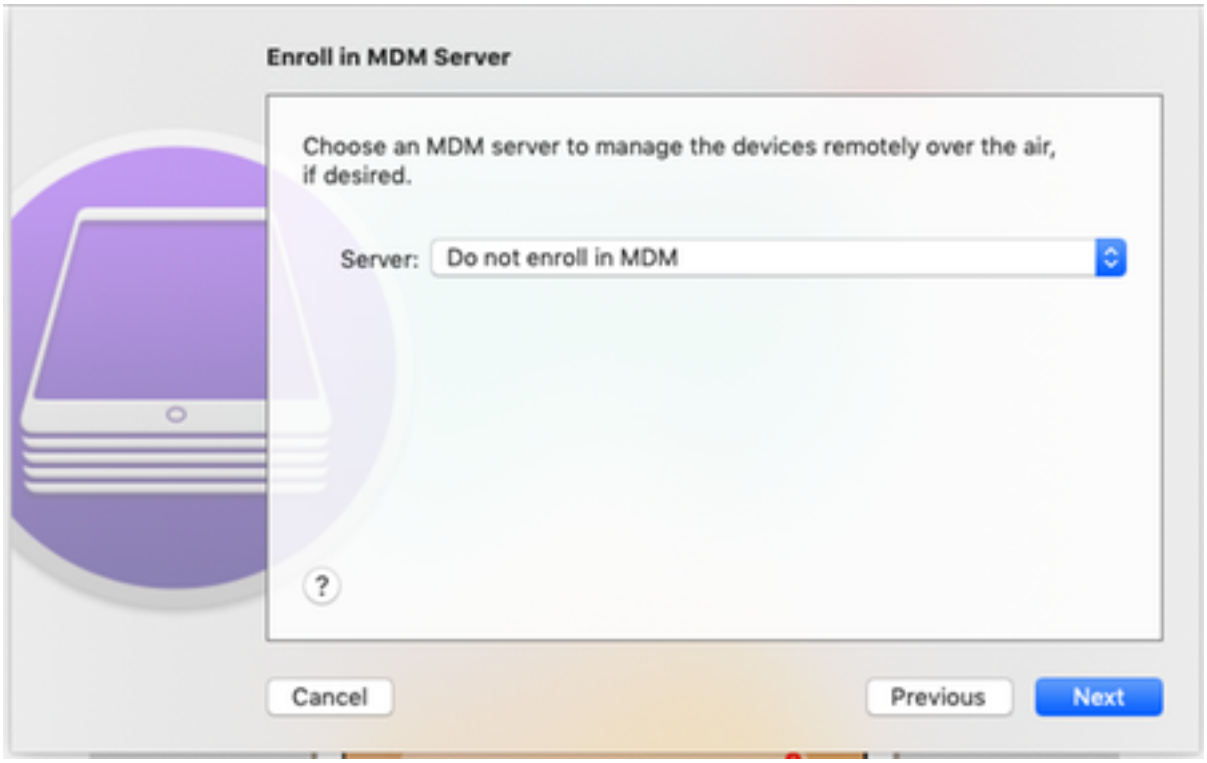


Étape 4. Cliquez avec le bouton droit de la souris et sélectionnez **Préparer** comme indiqué dans l'image.

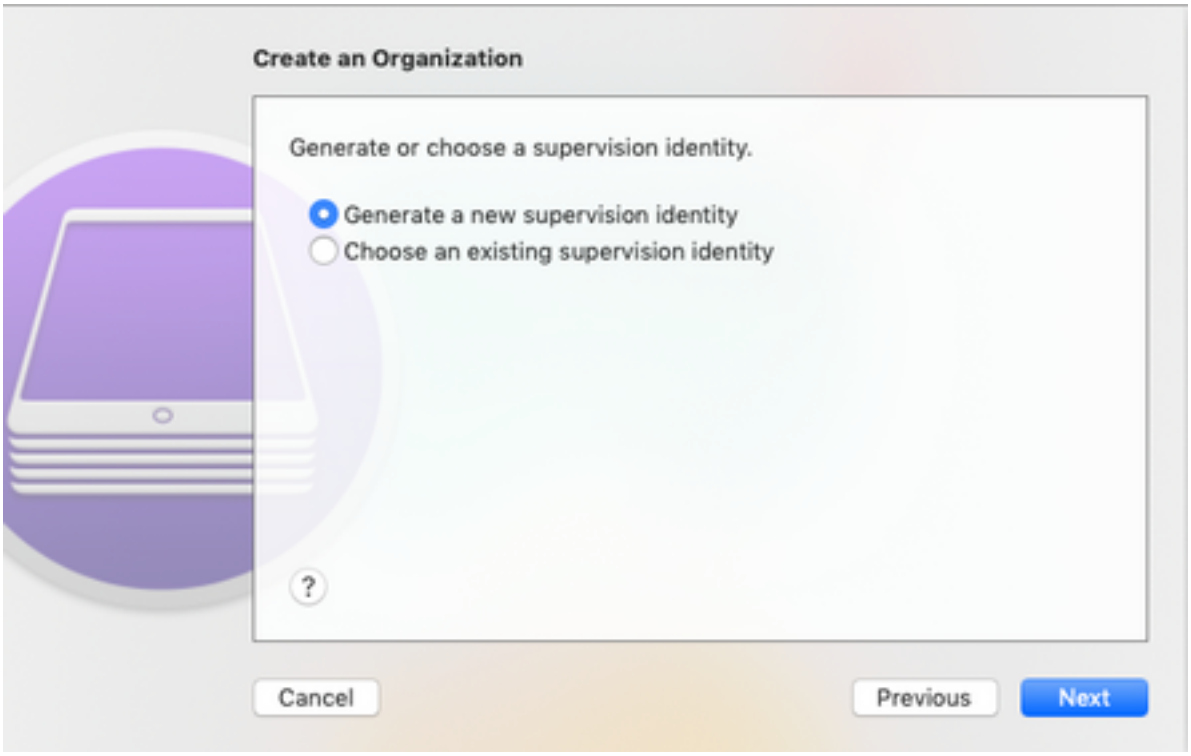
Étape 5. Sélectionnez **Configuration manuelle** et cochez les deux cases : **Superviser les périphériques** et **Autoriser les périphériques à se jumeler à d'autres ordinateurs** comme indiqué dans l'image ici et cliquez sur Suivant.



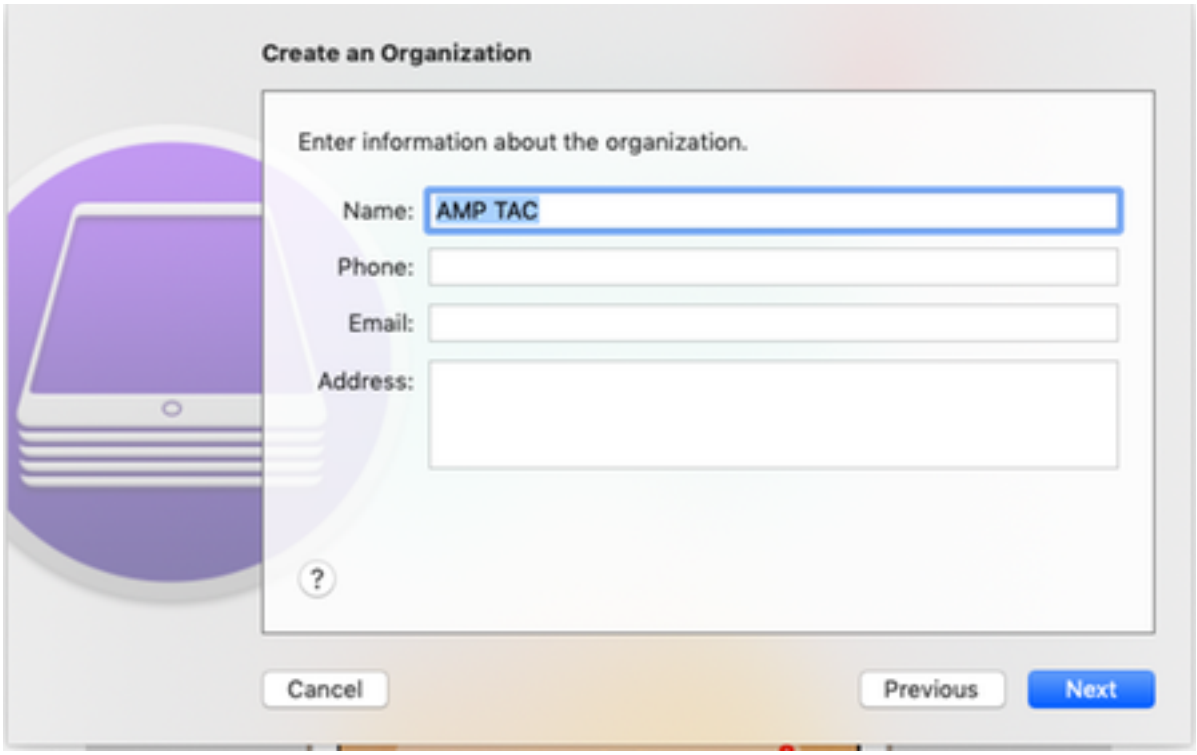
Étape 6. Il n'est pas nécessaire de l'inscrire via MDM à ce stade et cliquez sur Suivant.



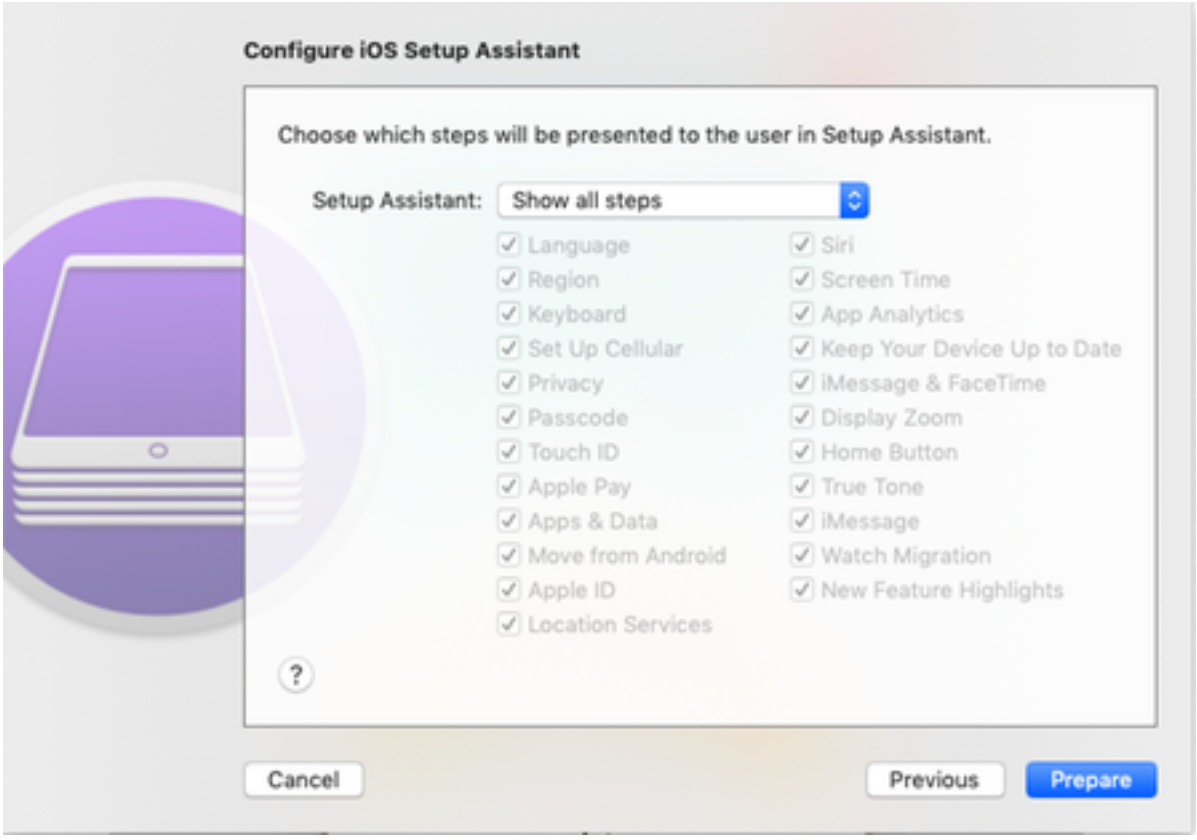
Étape 7. Sélectionnez **Générer une nouvelle identité de supervision** pour créer une organisation à laquelle les périphériques sont affectés, puis cliquez sur Suivant.



Étape 8. Donnez un nom à l'organisation et cliquez sur Suivant.



Étape 9. Cliquez sur **Préparer**.



Étape 10. Vous êtes alors invité à **effacer** l'iPad pour la préparation. Sélectionnez cette option pour effacer l'iPad après avoir effectué une sauvegarde.

Étape 11. Après le redémarrage de votre iPad, celui-ci doit être supervisé et prêt à être utilisé avec CSC.