

如何监管iOS设备以与思科安全连接器(CSC)配合使用？

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[配置](#)

简介

本文档介绍如何在本地监督Apple iOS设备以便清晰地使用。使用思科安全连接器(CSC)/Clarity的一个关键要求是，iOS设备应与AMP和/或Umbrella配合使用，并且这些设备需要受到监管。如果设备是通过DEP程序或Apple配置器从Apple购买的，则可以对其进行监管。Apple在iOS 5中引入了监管，作为一种特殊模式，管理员可以比通常允许的更多地控制设备。受监管模式用于机构拥有的设备。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Apple iOS设备11.3及更高版本
- Apple Configurator 2 (仅在Mac上提供)

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始(默认)配置。如果您的网络处于活动状态，请确保您了解任何配置的潜在影响。

背景信息

思科安全连接器为组织拥有的iOS设备提供前所未有的可视性和可控性。与面向终端的AMP Clarity和Umbrella相结合，此功能提供：

- 网络和设备流量的可视性。
- 每台设备的应用清点。
- 自动阻止用户和报告的网络钓鱼站点，以识别点击网络钓鱼链接的用户。
- 阻止与恶意域的连接，以保护敏感数据。

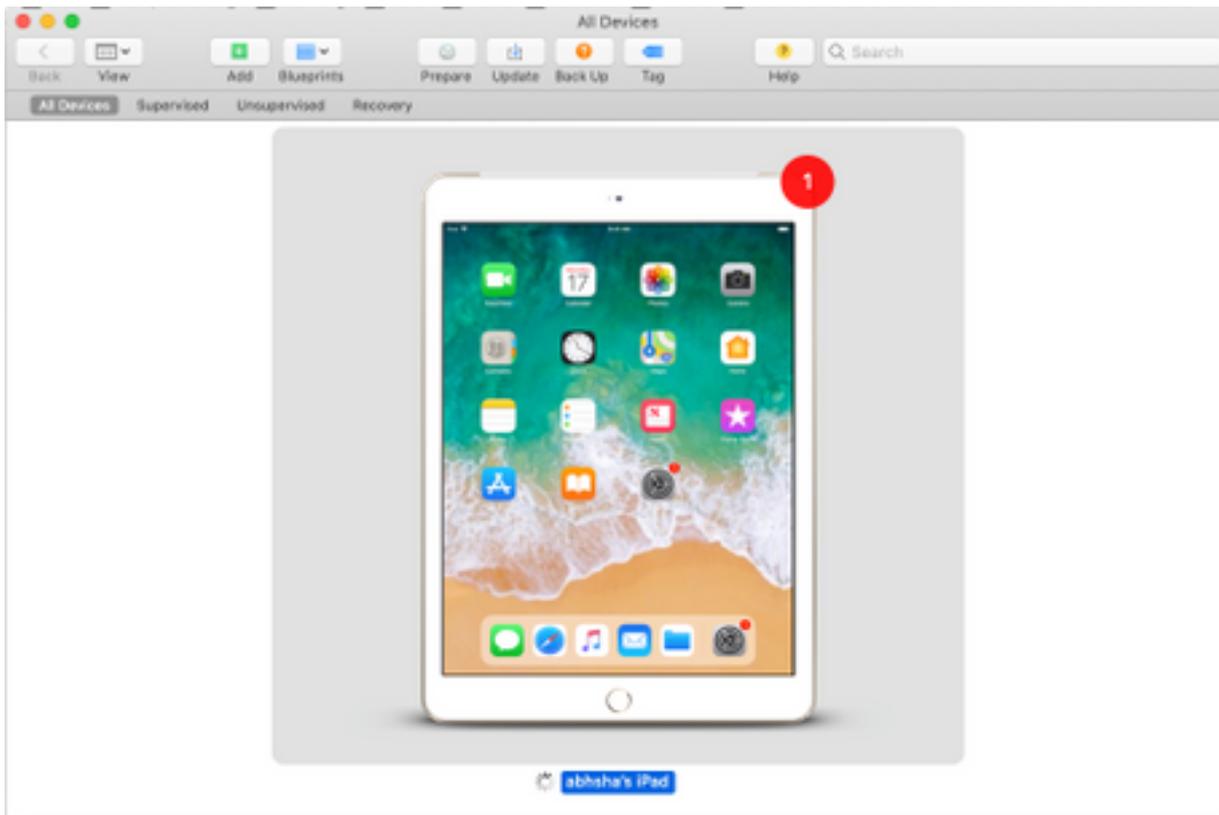
配置

警告：为了监督设备，它被完全擦除。因此，请确保已备份设备。

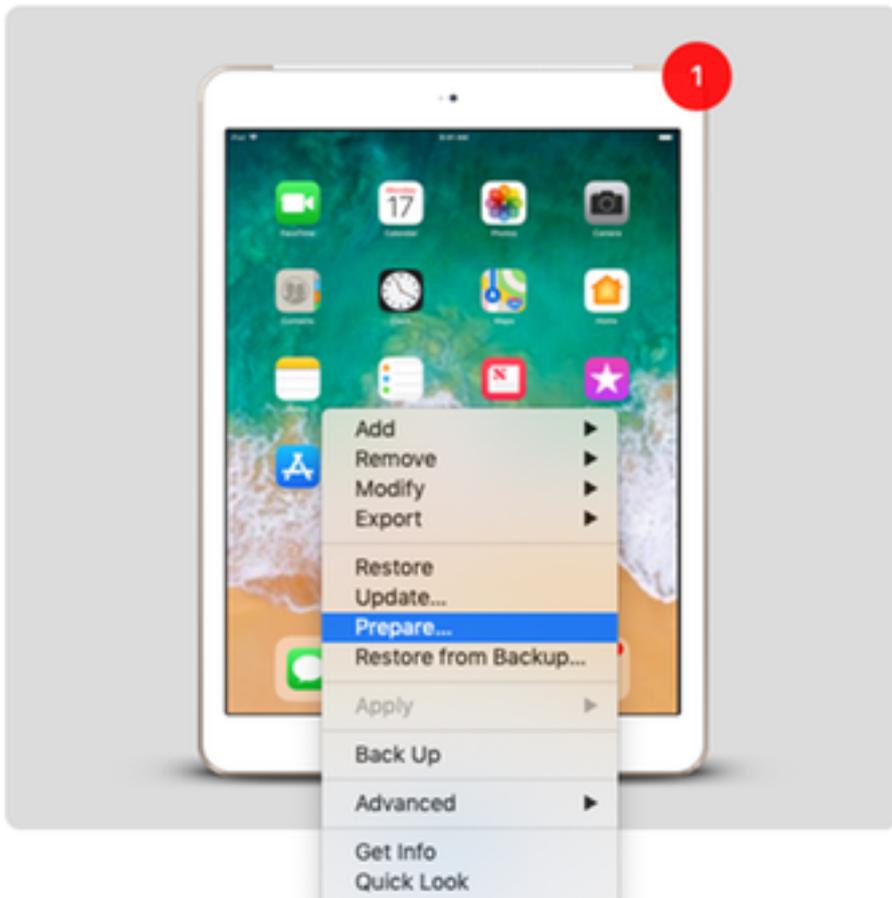
步骤1.将iOS设备连接到Mac。

步骤2.启动Apple Configurator。

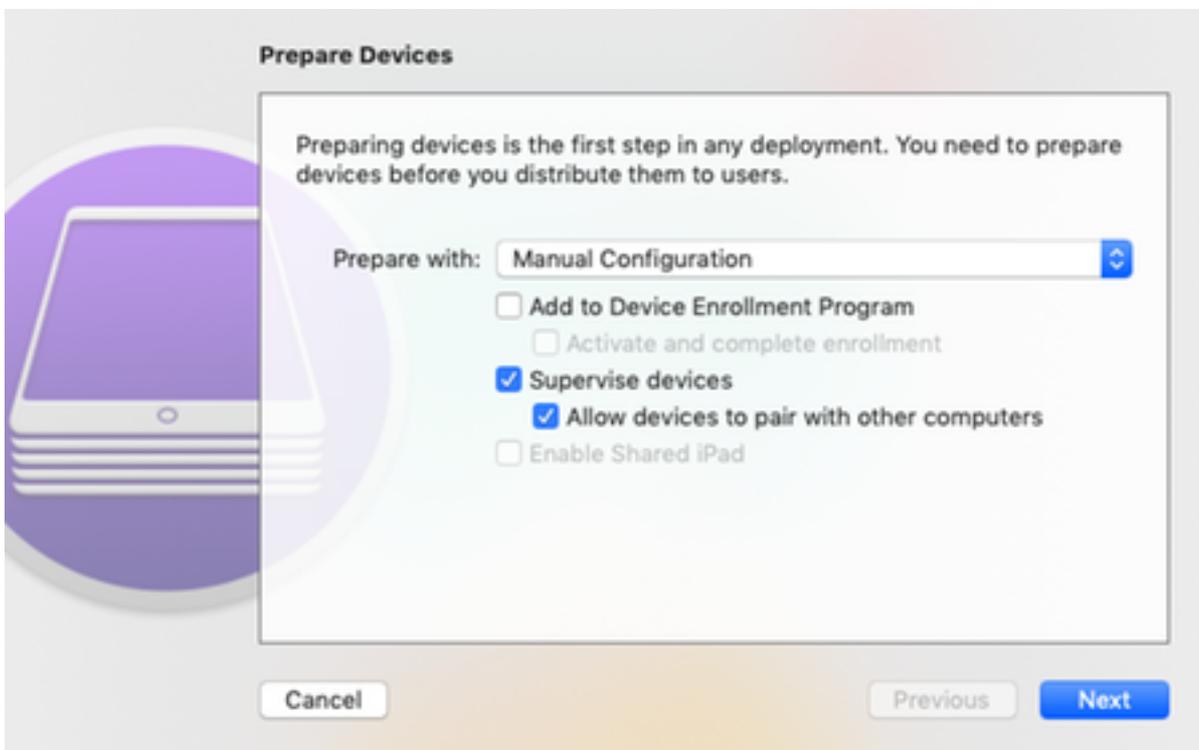
步骤3.您必须看到您的设备，如图所示。



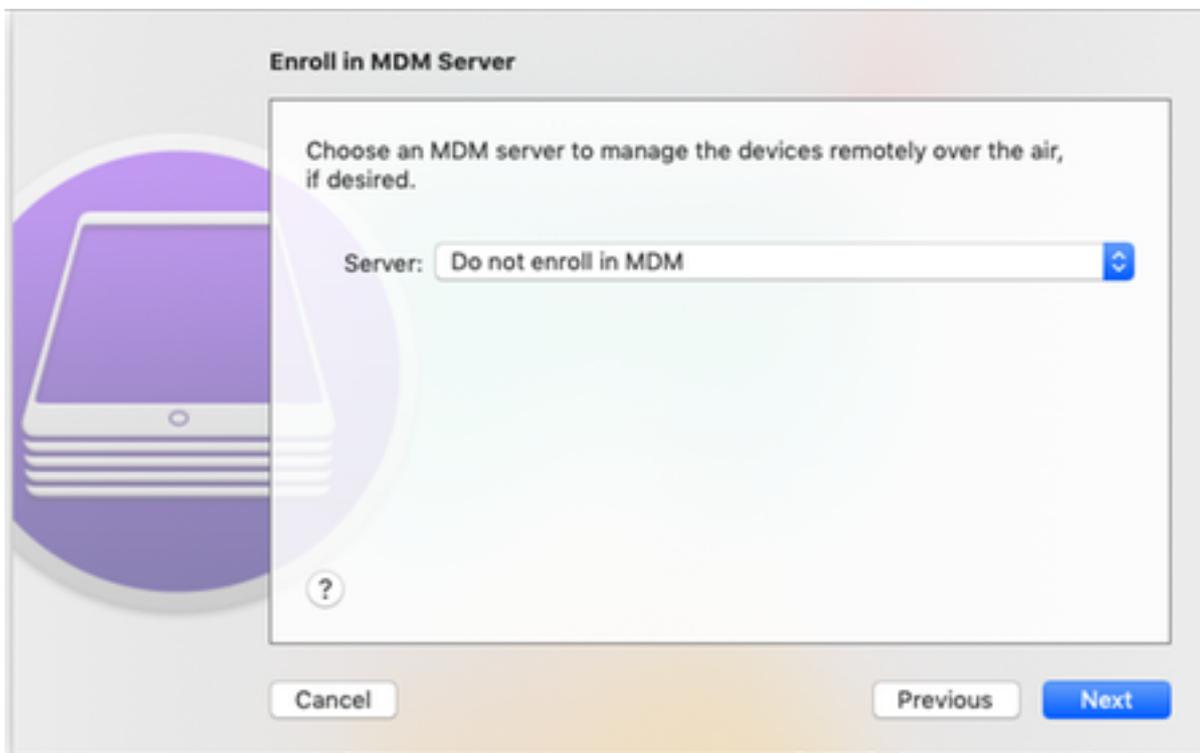
步骤4.右键单击并选择“准备”，如图所示。



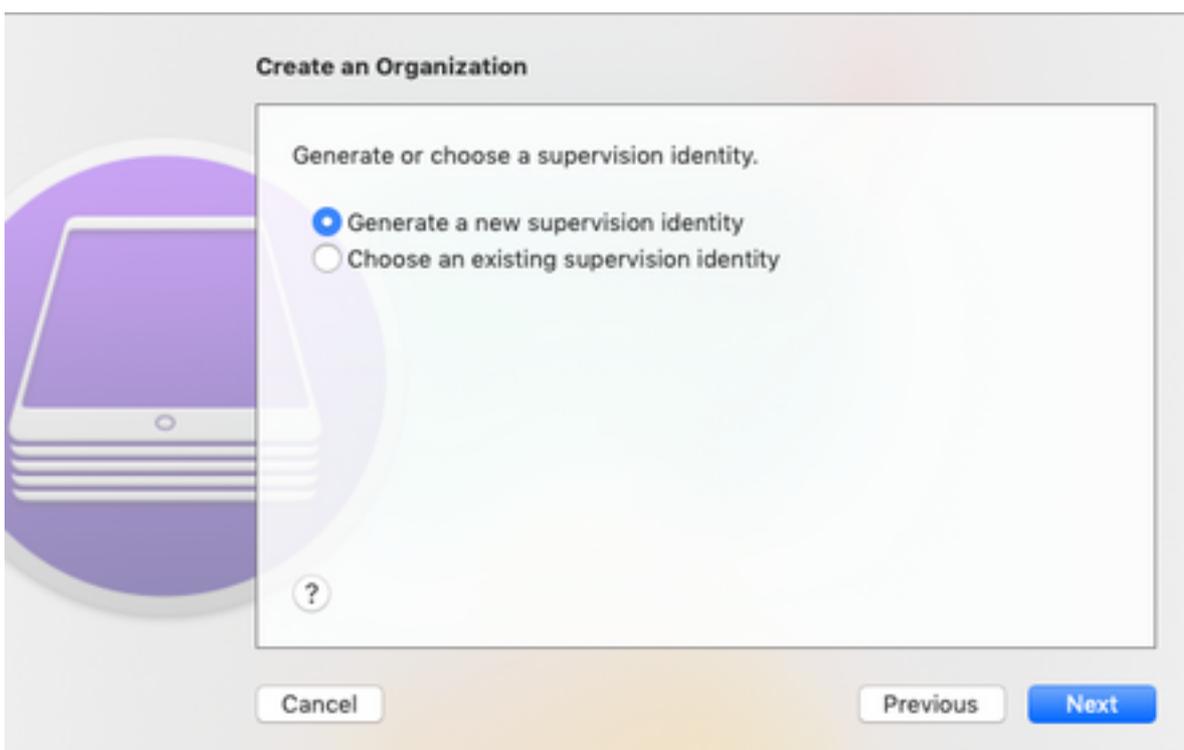
步骤5.选择Manual Configuration，并选中Supervise devices 和Allow devices to pair with other computers（如图所示）两个框，然后单击Next（下一步）。



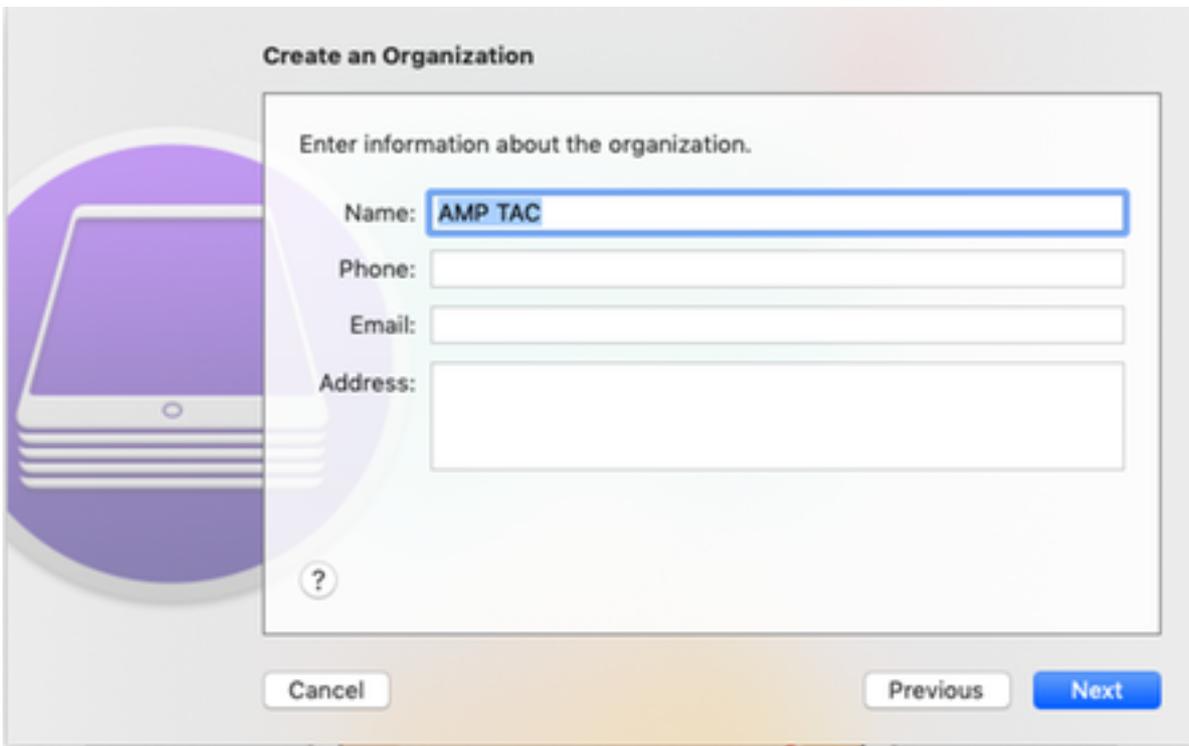
步骤6.此阶段无需通过MDM注册并点击“下一步”。



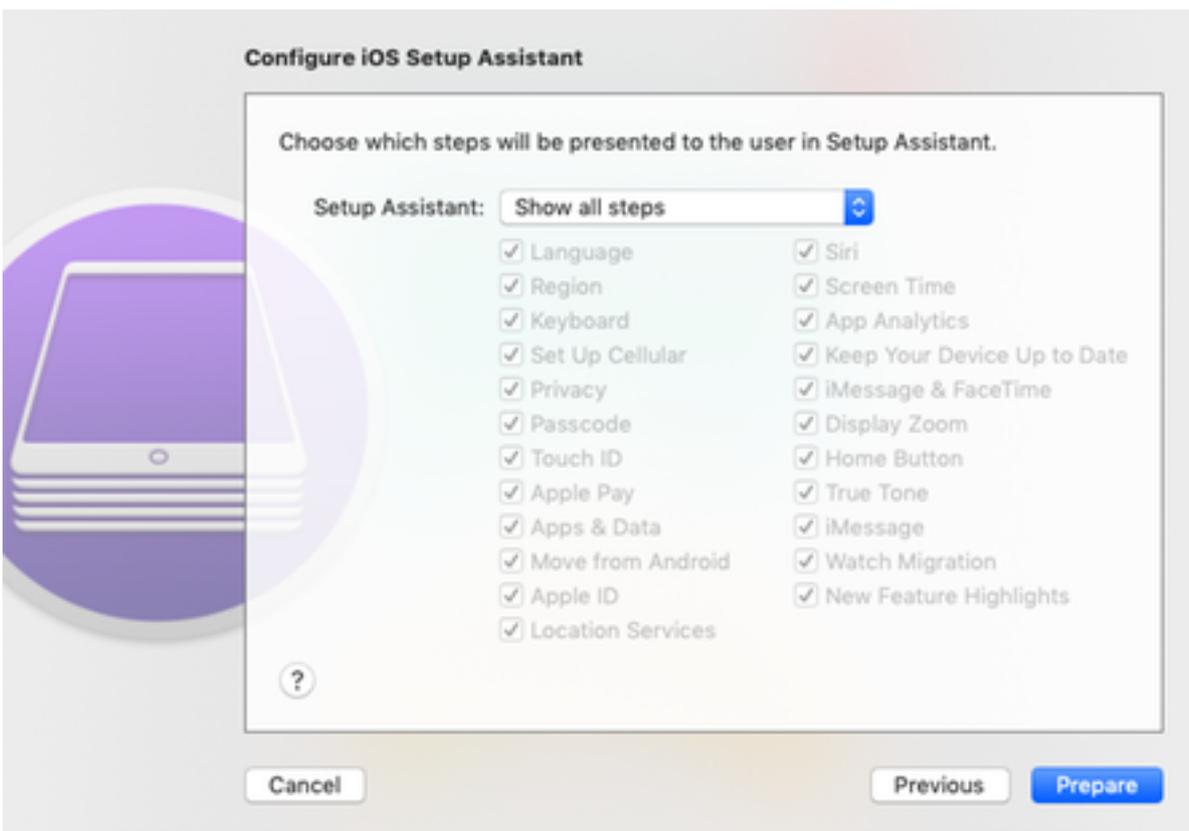
步骤7.选择**Generate a new supervisory identity**以创建新的组织，将设备分配到该组织，然后单击**Next**。



步骤8.为组织指定名称并单击**Next**。



步骤9.单击“准备”。



步骤10.然后系统提示您清除iPad以备准备。选择“Erase the iPad after you have a backup (在备份后清除iPad)”。

步骤11.在您的iPad重新启动后，应对其进行监督，并准备好与CSC配合使用。