将FDM板载到Defense Orchestrator

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

配置

- 网络图
- 配置

验证

故障排除

相关信息

简介

本文档介绍如何使用注册密钥将由Firepower设备管理器(FDM)管理的设备注册到Cisco Defense Orchestrator (CDO)。

先决条件

要求

Cisco 建议您了解以下主题：

- Firepower设备管理器(FDM)
- 思科防御协调器(CDO)

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行版本7.4.1的Firepower设备管理器(FDM) Azure

有关兼容版本和产品的完整列表，请参阅《安全防火墙威胁防御兼容性指南》以了解其他详细信息。

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，请确保您了解所有命令的潜在影响。

背景信息

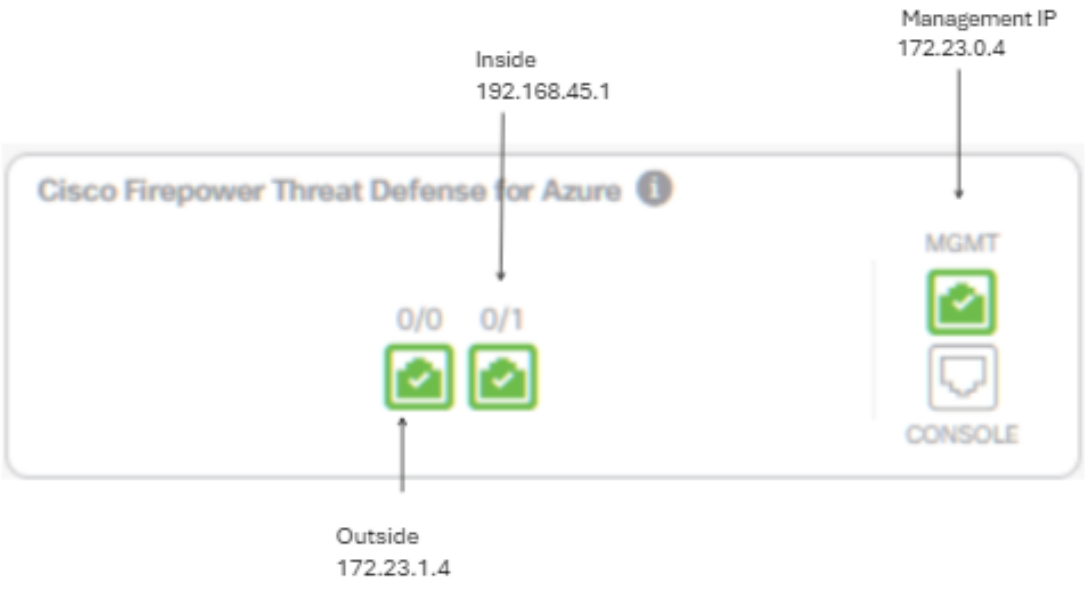
在使用注册密钥开始将FDM管理的设备注册到Cisco Defense Orchestrator (CDO)之前，请确保满足以下必备条件：

1. 兼容版本：您的设备必须运行版本6.6或更高版本。
2. 网络要求：将Cisco Defense Orchestrator连接到受管设备
3. 管理软件：设备必须通过安全防火墙设备管理器(FDM)进行管理。
4. 许可：您的设备可以使用90天评估许可证或智能许可证。
5. 现有注册：确保设备尚未向思科云服务注册，以避免在注册过程中发生冲突。
6. Pending Changes：验证设备上是否没有挂起的更改。
7. DNS配置：必须在FDM管理的设备上正确配置DNS设置。
8. 时间服务：可以准确配置设备上的时间服务，以确保与网络时间协议同步。
9. FDM支持激活的要求。防火墙设备管理器(FDM)支持及其功能仅在请求时授予。未在其租户上启用FDM支持的用户无法管理配置或部署到FDM管理的设备。要激活此平台，用户必须向支持团队发送请求以启用FDM支持。

配置

网络图

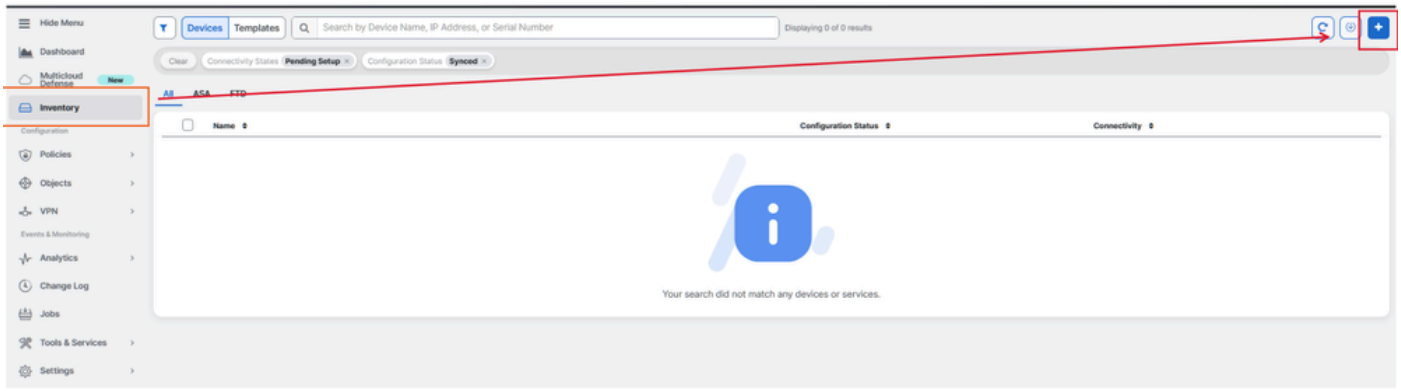
本文重点介绍FDM（Firepower设备管理器）设备，该设备通过其管理接口进行控制。此接口具有向Cisco Defense Orchestrator (CDO)注册设备所必需的互联网访问权限。



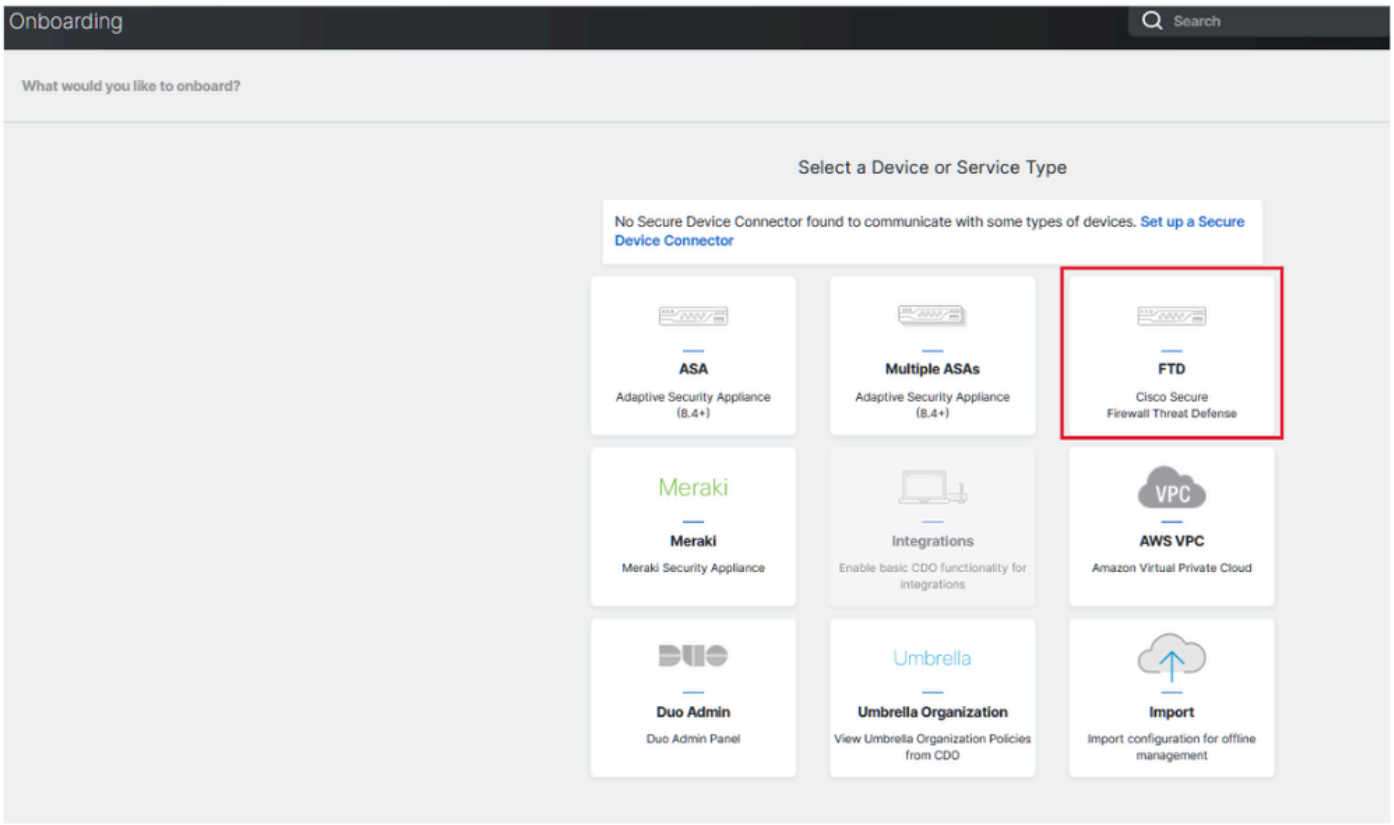
配置

步骤1: 登录到思科防御组合(CDO)。

第二步： 导航到资产窗格，并选择蓝色加号按钮注册设备。



第三步：选择FTD选项。

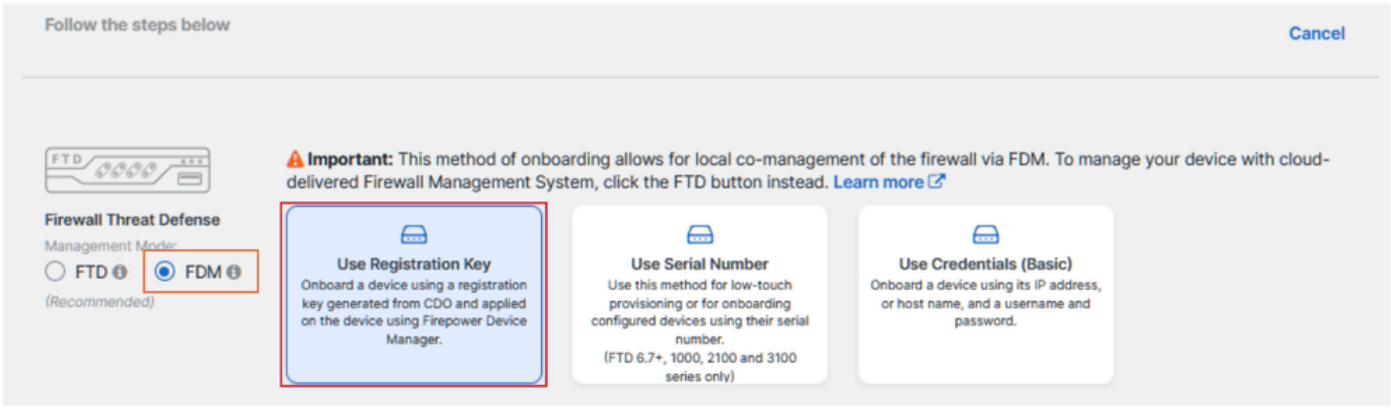


第4步继续执行“板载FTD设备”部分以开始注册过程。请务必注意可供您自行激活威胁防御设备的方法：

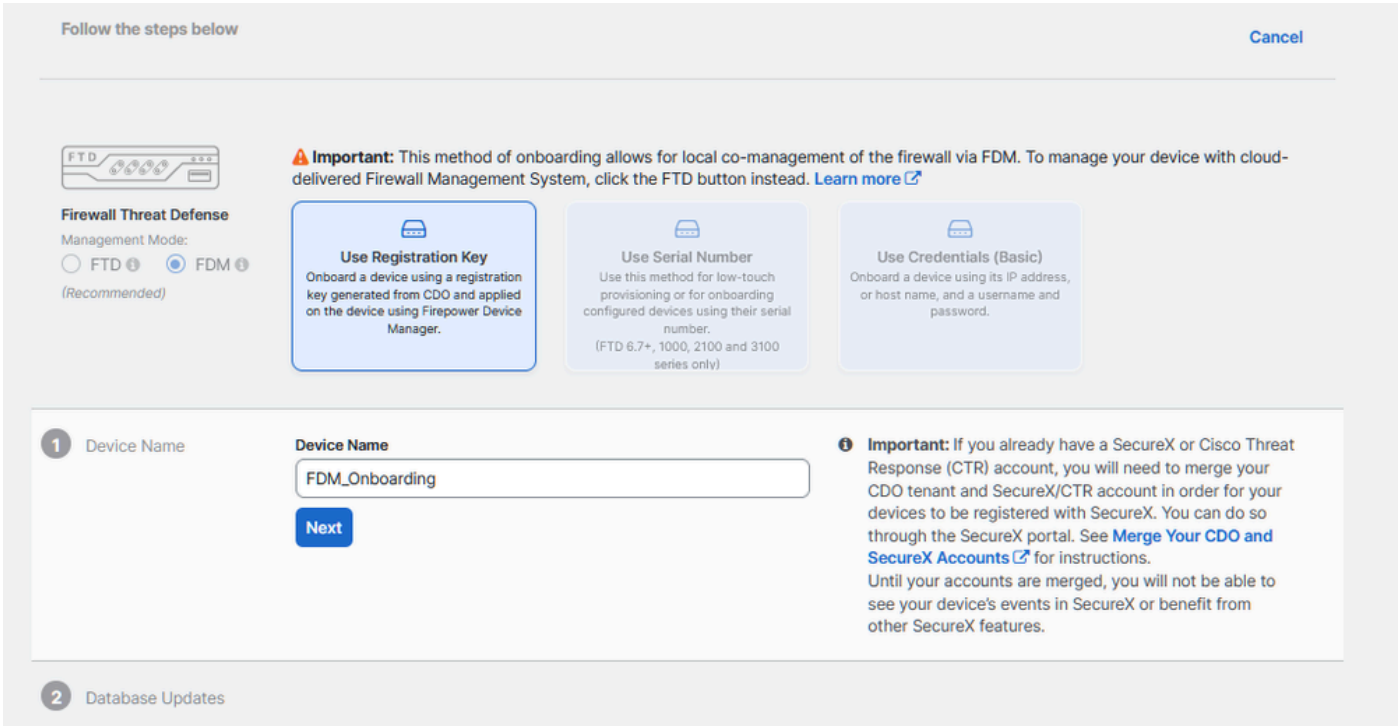
- 按序列号(By Serial Number)：此方法适用于物理设备，例如具有受支持软件版本的Firepower 1000、Firepower 2100或安全防火墙3100系列。它需要机箱或PCA序列号以及到互联网的网络连接。
- 通过注册密钥：这是首选的自注册方法，对于通过DHCP接收IP地址的设备尤其有利，因为即使设备IP地址发生更改，此方法也有助于保持与CDO的连接。

- 使用凭证(Using Credentials)：此替代方法涉及输入设备凭证及其外部、内部或管理接口的IP地址，该地址是根据网络中的设备配置定制的。

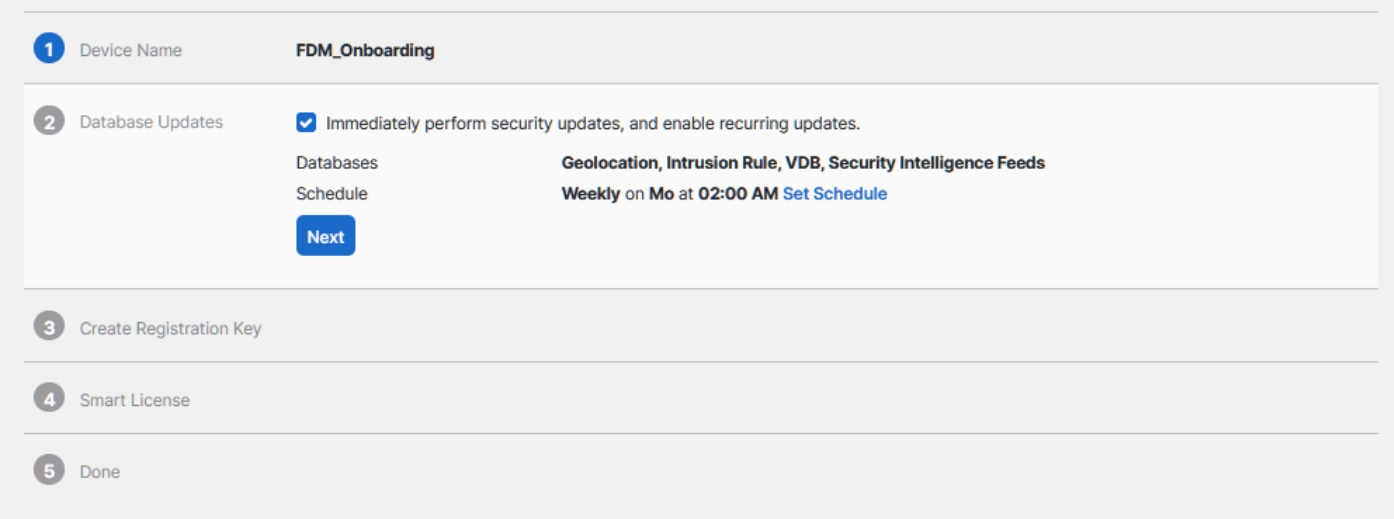
对于此过程，请选择FDM选项，然后选择Use Registration Key选项以确保与CDO的连接的一致性，而不考虑设备IP地址的可能更改。



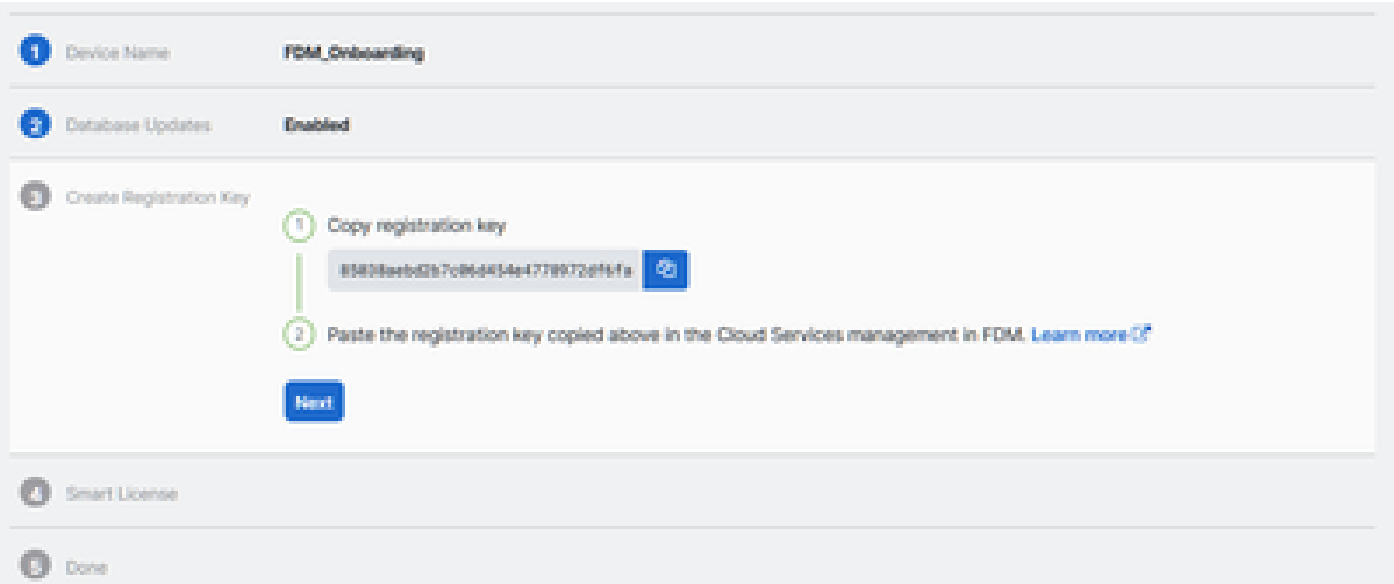
第五步：在Device Name字段中输入所需的设备名称，并指定Policy Assignment。此外，选择必须与设备关联的订用许可证。



第六步： 默认情况下，Database Updates部分配置为立即执行安全更新并设置定期更新。更改此设置不会更改通过安全防火墙设备管理器建立的任何现有更新计划。



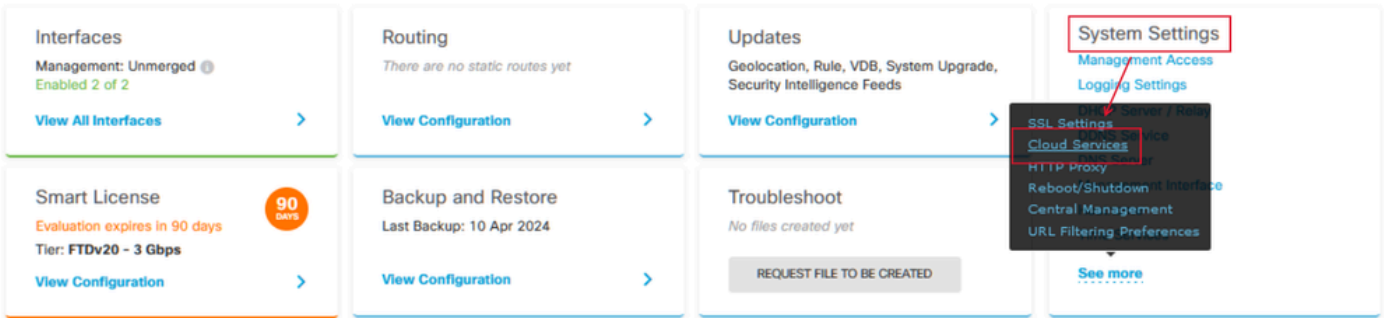
步骤 7. 在CLI Registration Key部分，CDO自动生成注册密钥。在完成之前退出登录界面会在资产中为设备创建占位符。如有必要，可稍后从此位置检索注册密钥。



步骤 8 使用“复制”图标复制生成的注册密钥。

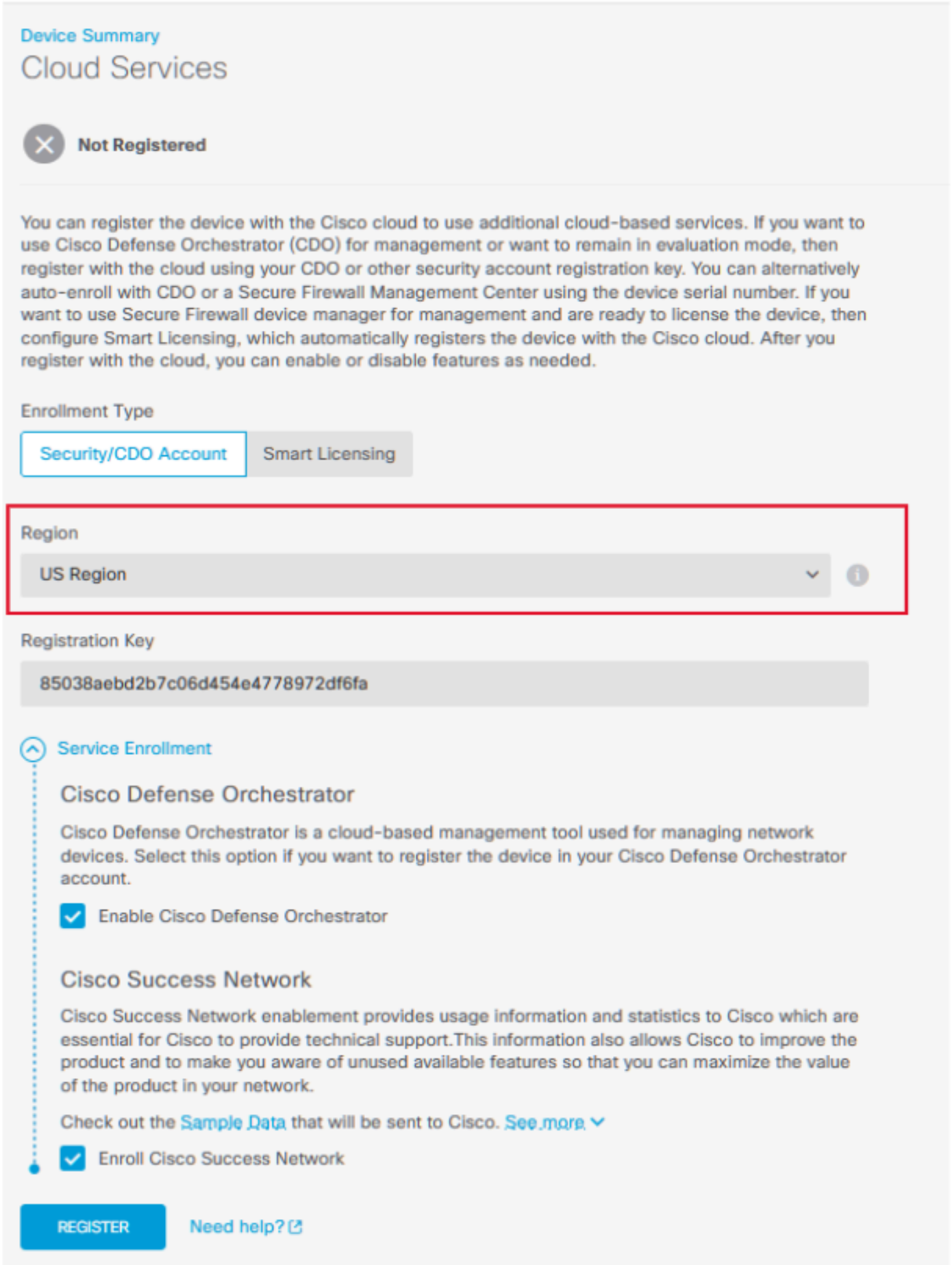
步骤 9 访问用于登录CDO的Secure Firewall设备管理器设备。

步骤 10 从System Settings（系统设置）菜单中选择Cloud Services（云服务）。

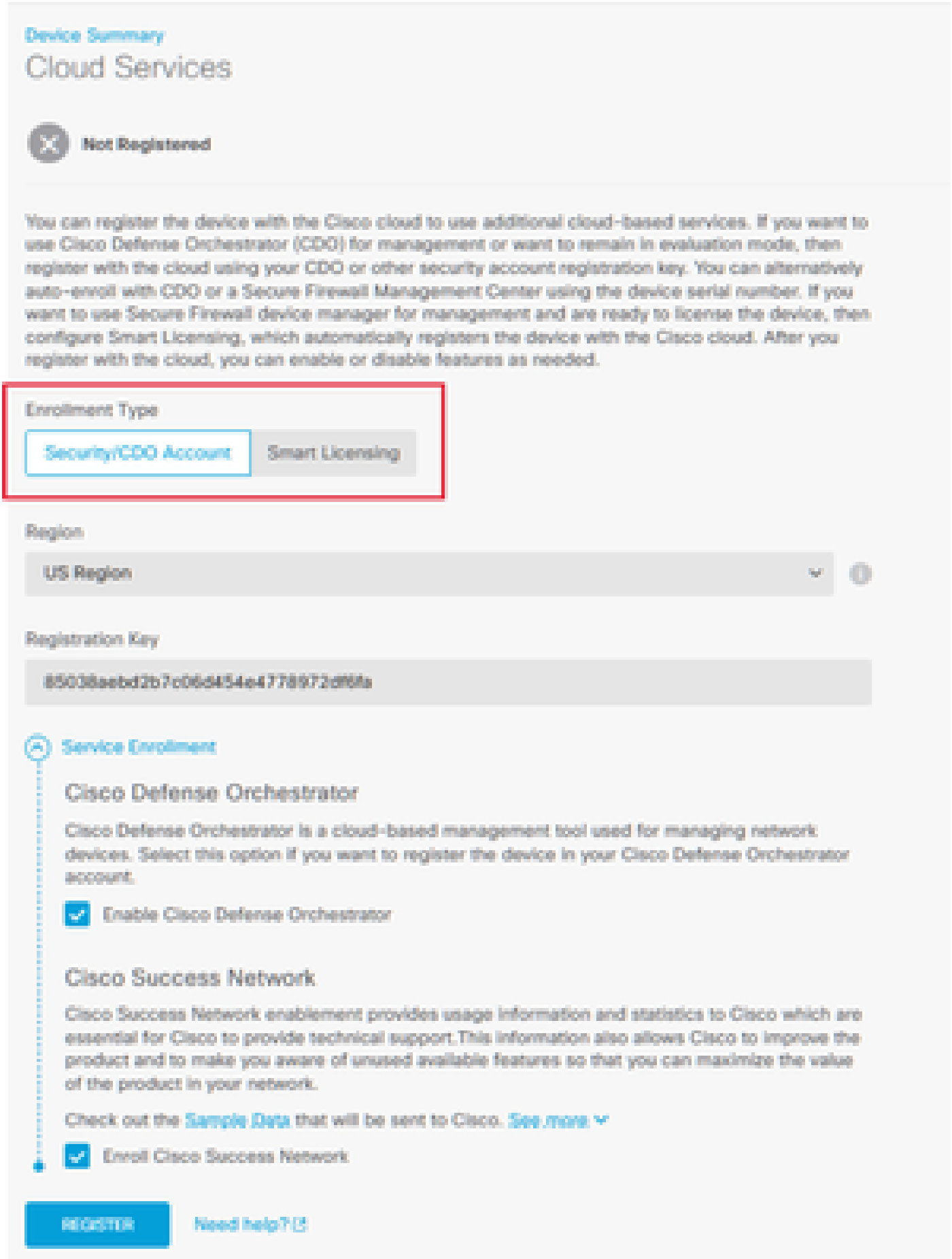


步骤 11 在Region下拉列表中指定正确的思科云区域，与租户地理位置保持一致：

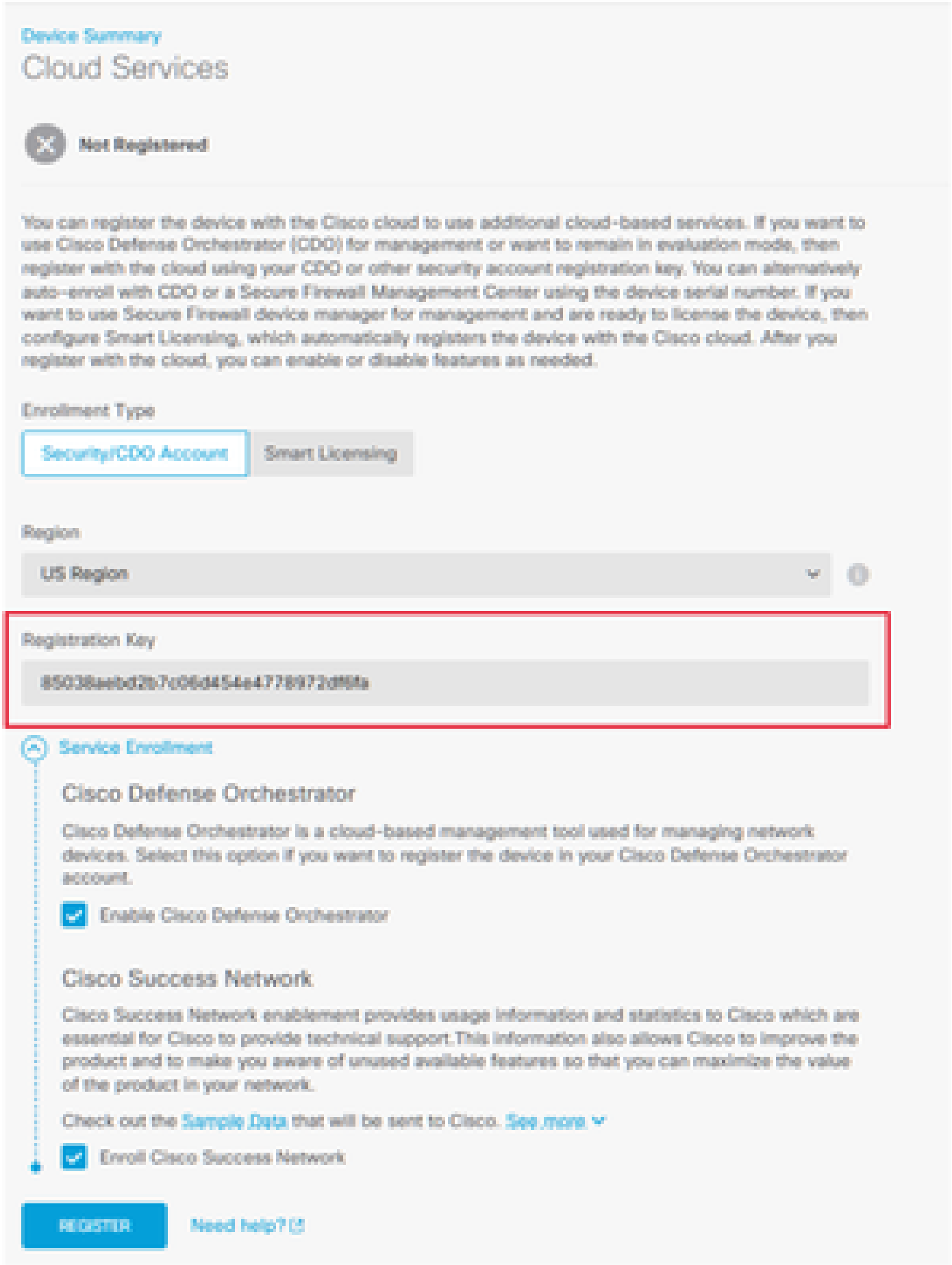
- 对于defenseorchestrator.com，请选择US。
- 对于defenseorchestrator.eu，请选择EU。
- 对于apj.cdo.cisco.com，请选择APJ。



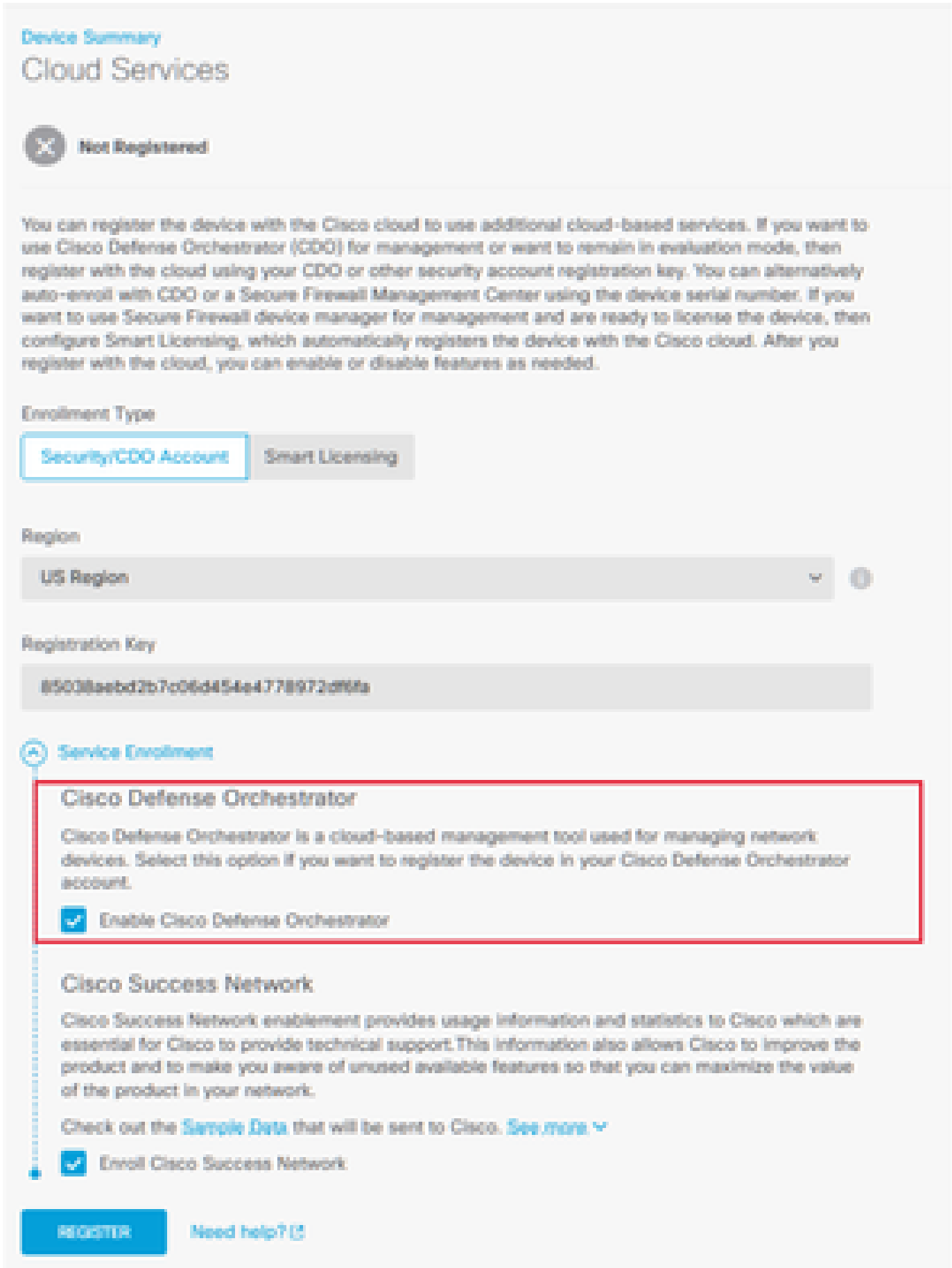
步骤 12 在Enrollment Type（注册类型）部分，选择Security Account（安全帐户）。



步骤 13 将注册密钥粘贴到Registration Key字段中。

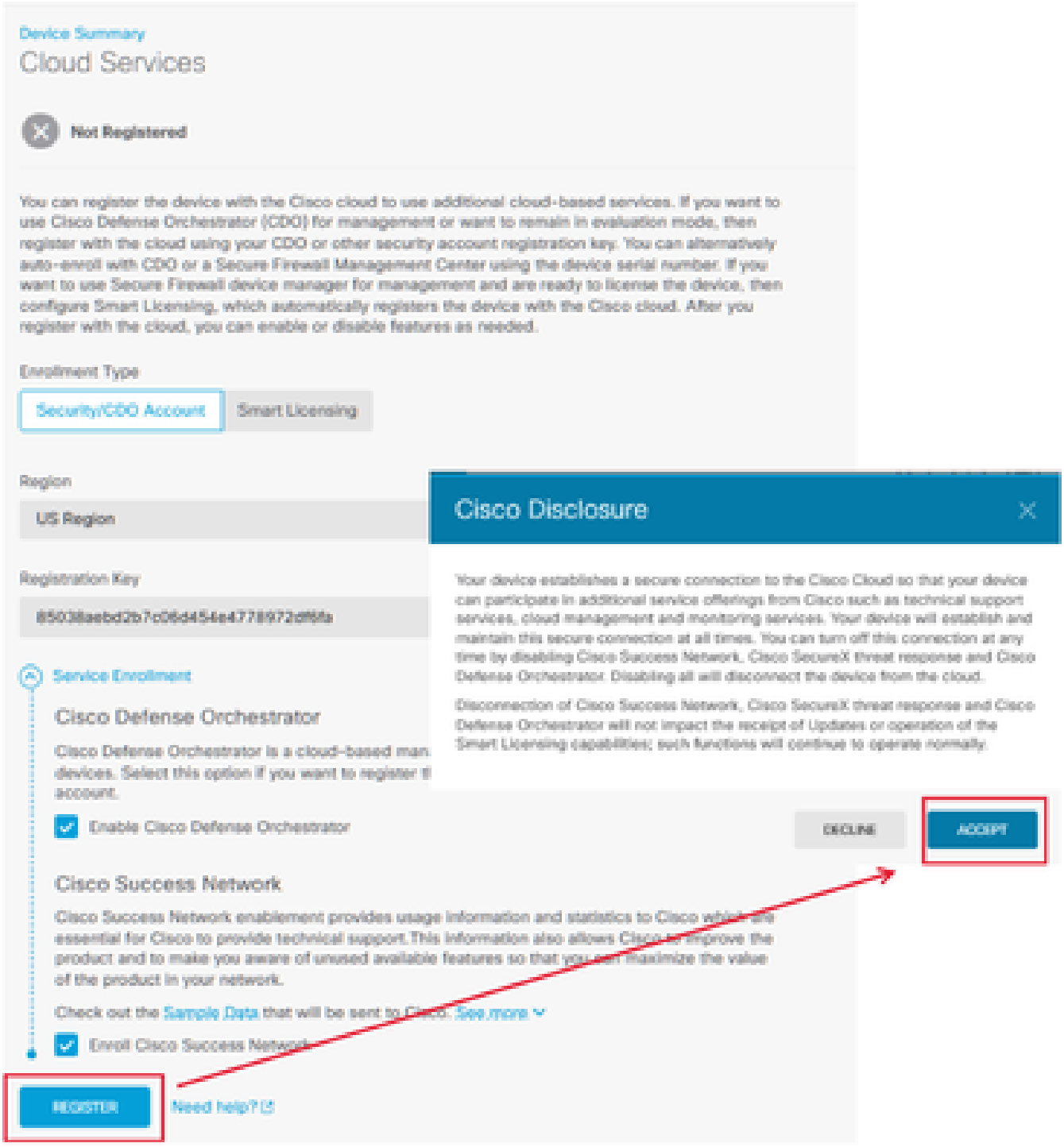


步骤 14 对于版本6.7或更高版本的设备，请确认在Service Enrollment（服务注册）部分启用了Cisco Defense Orchestrator。



第15步：（可选）查看Cisco Success Network Enrollment详细信息。如果不希望参与，请取消选中Enroll Cisco Success Network复选框。

步骤 16 选择注册并接受Cisco Disclosure（思科披露）。安全防火墙设备管理器向CDO提交注册。



步骤 17 返回CDO，在“注册密钥创建”区域中，选择“下一步”。

第18步（可选）确定并选择设备专用的许可证，然后选择下一步(Next)。

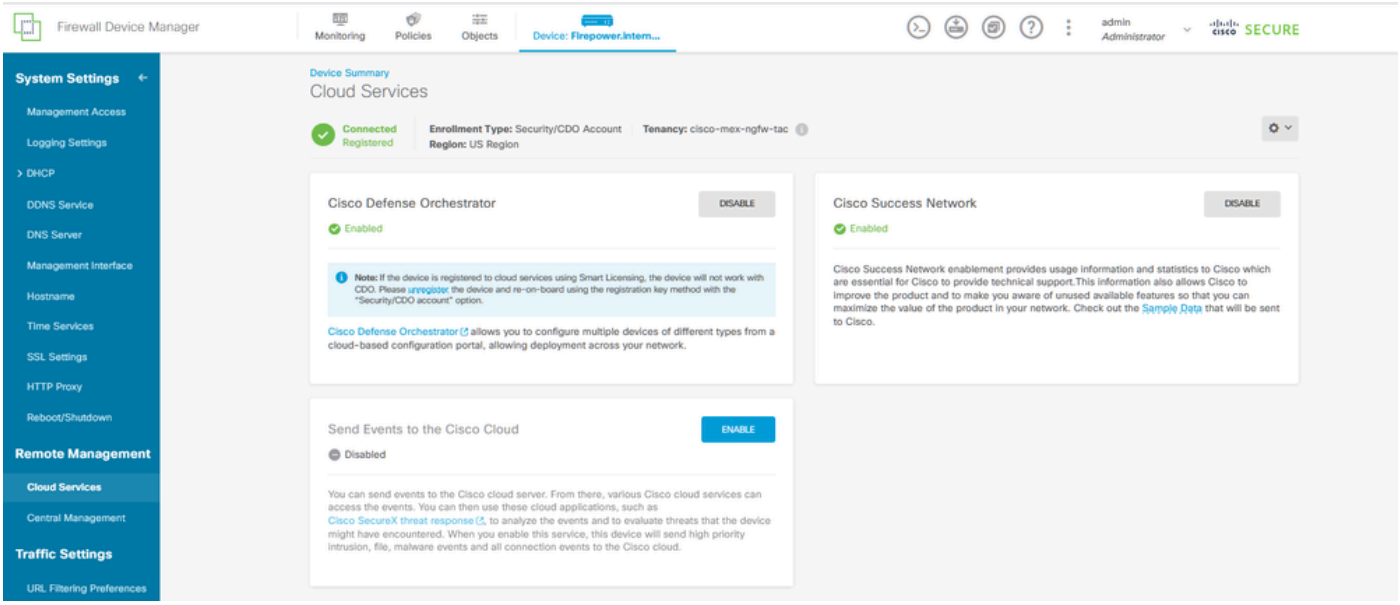
步骤 19. 观察CDO资产过渡中的设备状态，从未调配过渡到定位，然后过渡到同步，最后过渡到同步。



验证

使用本部分可确认配置能否正常运行。

导航到CDO门户并检查设备状态，状态将显示Online和Synced。 此外，还可以通过FDM GUI执行状态验证。导航到系统>云服务观察思科防御协调器和思科成功网络的连接状态。接口显示已连接状态，确认已成功与服务集成。



故障排除

本部分提供了可用于对配置进行故障排除的信息。

- 云服务FQDN故障的解决

如果由于无法解析云服务FQDN而导致设备注册失败，请检查网络连接或DNS配置，并再次尝试设备登录。

- 注册密钥无效错误

如果由于防火墙设备管理器中输入的注册密钥无效而导致设备注册未完成，请继续从Cisco Defense Orchestrator复制正确的注册密钥，并重试注册过程。如果设备已经获得智能许可，请在防火墙设备管理器中输入注册密钥之前删除智能许可证。

- 许可证发放不足

在设备连接状态指示“Insufficient License”（许可证不足）的情况下，请继续执行：

1. 留出一些时间让设备获取许可证，因为思科智能软件管理器可能需要一段时间才能将新许可证应用到设备。
2. 如果设备状态保持不变，请通过注销然后重新登录刷新CDO门户，以解决许可证服务器和设备之间的潜在网络通信问题。

3. 如果门户刷新未更新设备状态，请执行以下操作：

   - 从思科智能软件管理器生成新的注册密钥并进行复制。有关指南，请参阅生成智能许可视频。
   - 在CDO导航栏中，选择Inventory页面。
   - 选择列出的Insufficient License状态的设备。
   - 在Device Details窗格中，点击Insufficient Licenses警报下的Manage Licenses。系统将提示“管理许可证”窗口。
   - 在Activate字段中，粘贴新注册密钥并选择Register Device。

成功应用新的注册密钥后，设备连接状态必须更改为“在线”。

有关使用注册密钥的替代方法注册Firepower设备管理器(FDM)的全面指南，请参阅以下链接中提供的详细文档：对FDM管理的设备进行故障排除。

此资源为可用于将FDM成功加载到Cisco Defense Orchestrator (CDO)的不同注册技术提供分步说明和故障排除提示。

相关信息

- 排除FDM管理的设备故障
- 使用Cisco Defense Orchestrator管理FDM设备
- 思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。