paloalto
TECHDOCS

Strata Cloud Manager 激活和接入

docs.paloaltonetworks.com

Contact Information

Corporate Headquarters:
Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetworks.com/company/contact-support

About the Documentation

- For the most recent version of this guide or for access to related documentation, visit the Technical Documentation portal docs.paloaltonetworks.com.
- To search for a specific topic, go to our search page docs.paloaltonetworks.com/search.html.
- Have feedback or questions for us? Leave a comment on any page in the portal, or write to us at documentation@paloaltonetworks.com.

Copyright

Last Revised

April 17, 2026

Table of Contents

激活您的 Strata Cloud Manager 许可证

要开始使用 Strata Cloud Manager，您需要激活适当的许可级别 — 基础版或专业版。

- 激活 Strata Cloud Manager 基础版：免费级别提供配置管理、网络安全生命周期管理，并且如果您拥有 Strata 日志服务的付费许可证，还可以提供可见性。
- 激活 Strata Cloud Manager Pro：此级别提供高级功能以及所有 Strata Cloud Manager Essentials 功能。在激活 Strata Cloud Manager Pro 版时，还包括 Strata 日志服务的访问权限，后者提供一年的日志保留和无限存储。

如果在引入这些新的许可层级之前就已经在使用 *Strata Cloud Manager*，则现有的 *AIOps for NGFW* 高级版和 *AIOps for NGFW* 免费版许可证仍然受支持。可以继续修改、延长或续订这些许可证。此外，如果您使用的是 *NGFW* 免费版的 *AIOps*，您可以选择升级到 *NGFW* 高级版的 *AIOps*。

- 激活 NGFW 高级版的 AIOps
- 为 NGFW 高级版的 AIOps 激活 ELA
- 激活 Software NGFW Credits 许可证协议
- 激活您的 Prisma Access 许可证
- ADEM 许可

激活 Strata Cloud Manager 基础版

Strata Cloud Manager 基础版是免费的层级，提供配置和网络安全生命周期管理功能，以简化操作并提供基本安全性。有关设备型号支持的详细信息，请参阅设备型号兼容性。

您可以使用 Strata Cloud Manager 基础版许可证层激活由软件 NGFW 积分资助的 VM-Series。如果您未在部署配置文件中选择云订阅，Strata Cloud Manager 基础版将自动激活。

STEP 1 | 登录到中心。

STEP 2 | 请访问 Strata Cloud Manager 基础版激活 URL：https://apps.paloaltonetworks.com/activation/scm-essentials。

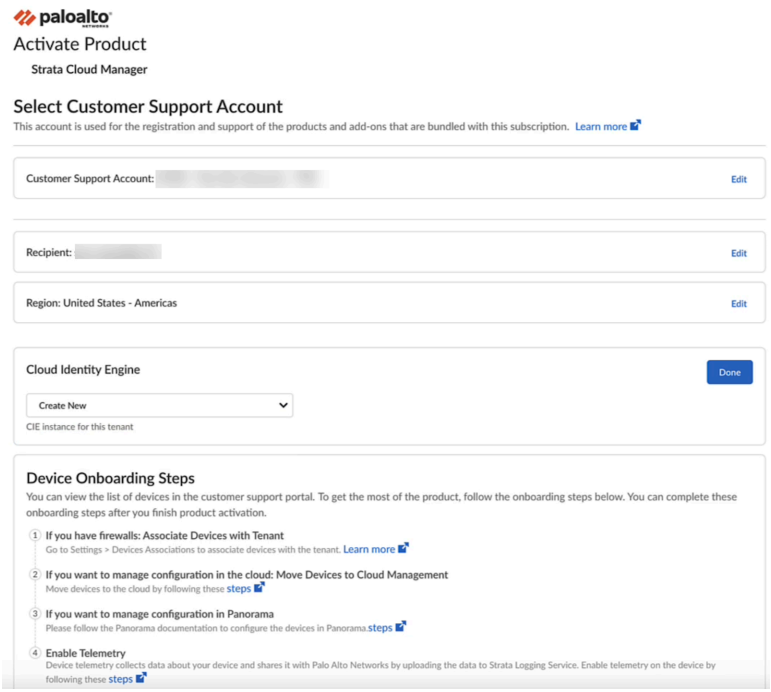
STEP 3 | 选择客户支持帐户。

STEP 4 | 创建新 租户，您将在其中激活 Strata Cloud Manager。

STEP 5 | 选择要在其中部署 Strata Cloud Manager 的区域。请参阅 Strata Cloud Manager 支持的区域。

区域支持取决于您是否希望同时管理 NGFW、Prisma Access 或两者。要同时管理两者，您必须选择一个支持 NGFW 和 Prisma Access 的区域。

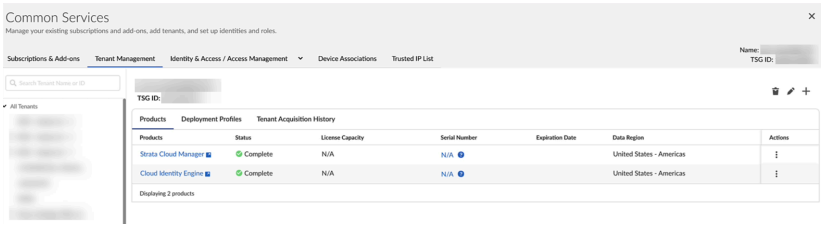
STEP 6 | 选择云身份引擎或创建新的 CIE 实例，以识别和验证整个基础架构中的所有用户。您也可以通过选择无来跳过它。



STEP 7 | 依次单击 **Agree to the Terms and Conditions**（同意条款和条件）和 **Activate**（激活）。

STEP 8 | 等待 Strata Cloud Manager 初始化，并且状态显示为完成。

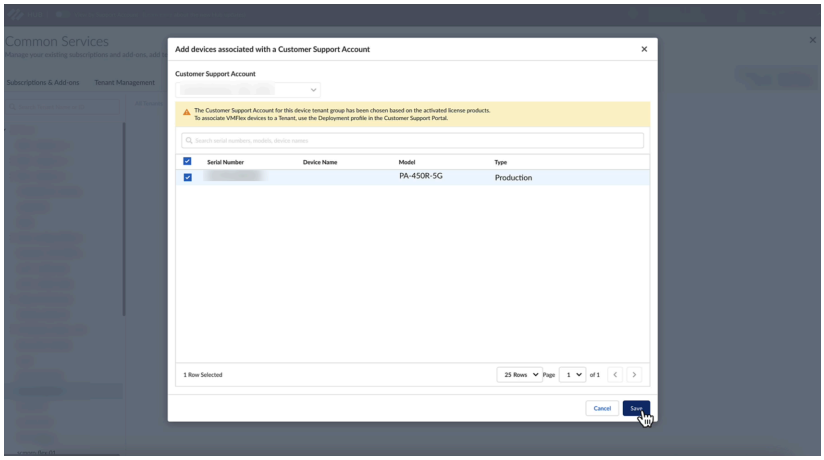
如果您创建了新的 Cloud Identity Engine 实例，请等待其状态显示为完成。



STEP 9 | 将 NGFW、Panorama 或两者关联到包含 Strata Cloud Manager 的租户。

确保将 *Panorama* 管理的所有防火墙单独关联到租户。

1. 导航到 **Common Services**（公共服务）**Device Associations**（设备关联）。
2. 添加设备。

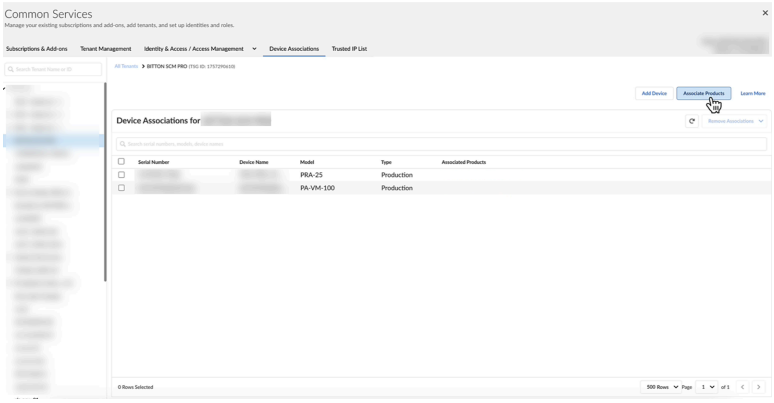


3. 选择一个或多个防火墙或 Panorama 设备，然后单击 **Save**（保存）。

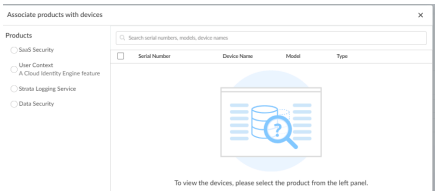
STEP 10 | 如果您有 Strata 日志服务，您可以将其与设备关联。否则可以跳过。

激活 Strata Cloud Manager 基础版后，您可以指定希望与 Strata 日志服务一起使用的防火墙或 Panorama 设备。

1. 选择 **Common Services**（公共服务）**Device Associations**（设备关联）。
2. 关联产品。



3. 在产品选择列中，选择 **Strata** 日志服务。



4. 选择设备并 **Save**（保存）。

STEP 11 | 在设备上启用遥测。Strata Cloud Manager 通过分析 PAN-OS 设备发送到 Strata 日志服务的遥测数据来评估部署中设备的运行状况。要发送此数据，您必须已经在设备上启用设备遥测。

从 *PAN-OS 12.1.2*、*11.1.11*、*11.2.8*、*10.2.17* 及更高版本开始，遥测自动启用功能将遥测配置为默认在您的设备上启用。加入新设备（*Panorama* 或防火墙）后，通过 *Strata Cloud Manager* 或中心集中控制设置，遥测将自动启用。

STEP 12 | 通过单击中心中的图标登录到 Strata Cloud Manager。

激活 Strata Cloud Manager Pro

Strata Cloud Manager Pro 版提供基础班许可证之外的高级功能。与基础版不同，其包括 Strata 日志服务，并提供一年的日志保留。有关设备型号支持的详细信息，请参阅设备型号兼容性。

当您的 Strata Cloud Manager Pro 版许可证到期时，Strata Cloud Manager 实例将恢复为 Strata Cloud Manager 基础版许可层级。许可证过期后，一些订阅仍继续以有限容量运行，而另一些则完全停止运行。看看每个订阅到期后会发生什么。

- NGFW
- Prisma Access
- 使用软件 NGFW 积分激活 VM-Series
- ELA
- ESA Pro

激活 NGFW Strata Cloud Manager Pro 版

本任务介绍如何激活 NGFW Strata Cloud Manager Pro 版。有关设备型号支持的详细信息，请参阅设备型号兼容性。

以下是 NGFW 的先决条件：

- 云管理接入先决条件 - 在将 NGFW 载 Strata Cloud Manager 之前，请验证设备就绪性的所有条件均已满足。这包括网络配置、软件兼容性和许可要求。完成这些步骤可确保使用 Strata Cloud Manager 成功管理防防火墙。
- **TCP** 端口和云管理 **FQDN** — 要在 NGFW 和 Strata Cloud Manager 之间实现无缝通信，请配置特定 TCP 端口和完全限定域名 (FQDN)。

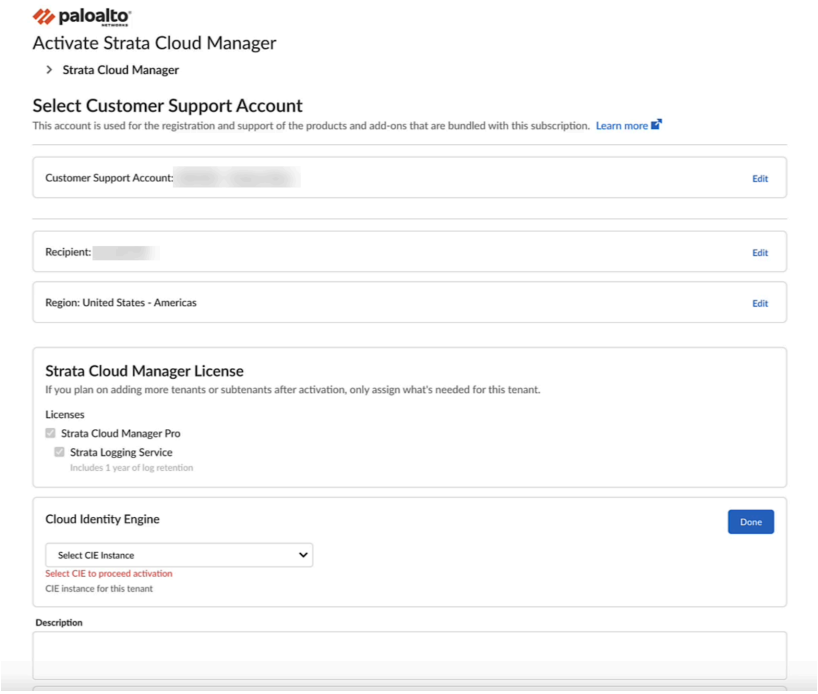
STEP 1 | 激活许可证时，您会收到 Palo Alto Networks 发送给您的一封电子邮件，确认您正在激活的许可证后，请使用激活链接开始激活。

STEP 2 | 选择要使用的客户支持帐户。

STEP 3 | 选择租户，在其中激活 Strata Cloud Manager Pro 版。如果您还没有租户，请新建。

STEP 4 | 选择要在其中部署 Strata Cloud Manager 的区域。请参阅 Strata Cloud Manager 支持的区域。

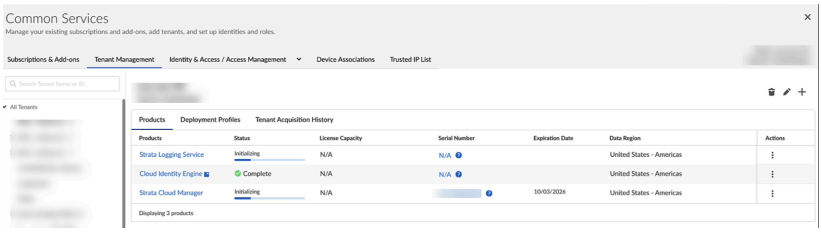
Strata Cloud Manager Pro 版包括日志保留一年的 Strata 日志服务。



STEP 5 | 选择云身份引擎或创建新的 CIE 实例，以识别和验证整个基础架构中的所有用户。

STEP 6 | 依次单击 **Agree to the Terms and Conditions**（同意条款和条件）和 **Activate**（激活）。

STEP 7 | 等待 Strata Cloud Manager、云身份引擎和 Strata 日志服务初始化，等待状态显示为完成。



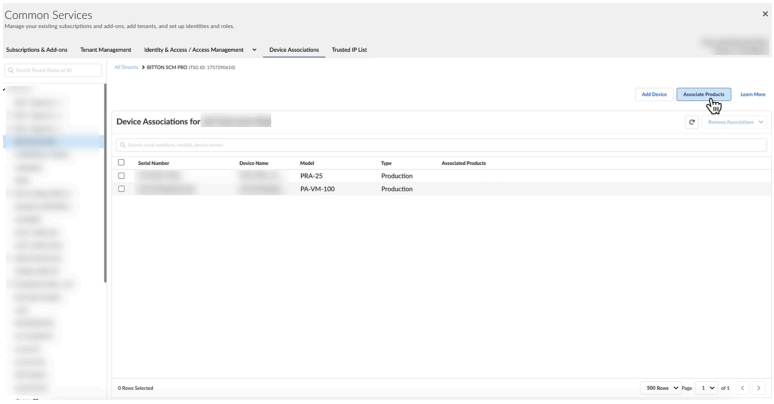
STEP 8 | 将 NGFW、Panorama 或两者关联到包含 Strata Cloud Manager 的租户。

确保将 *Panorama* 管理的所有防火墙单独关联到租户。

1. 导航到 **Common Services**（公共服务）**Device Associations**（设备关联）。
2. 添加设备。
3. 选择一个或多个防火墙或 Panorama 设备，然后单击 **Save**（保存）。

STEP 9 | 将产品关联到设备。激活 Strata Cloud Manager Pro 后，您需要指定要与其一起使用的防火墙或 Panorama 设备。

1. 导航到 **Common Services**（公共服务）**Device Associations**（设备关联）。
2. 关联产品。



3. 在产品选择列中，选择 **Strata Cloud Manager**。
4. 选择设备并 **Save**（保存）。

STEP 10 | 在设备上启用遥测。Strata Cloud Manager 通过分析 PAN-OS 设备发送到 Strata 日志服务的遥测数据来评估部署中设备的运行状况。要发送此数据，您必须已经在设备上启用设备遥测。

从 *PAN-OS 12.1.2*、*11.1.11*、*11.2.8*、*10.2.17* 及更高版本开始，遥测自动启用功能将遥测配置为默认在您的设备上启用。加入新设备（*Panorama* 或防火墙）后，通过 *Strata Cloud Manager* 或中心集中控制设置，遥测将自动启用。

STEP 11 | 通过单击中心中的图标登录到 Strata Cloud Manager。

激活 Prisma Access Strata Cloud Manager Pro 版

所有 Prisma Access 许可证类型都包括对 Strata Cloud Manager 的访问权限，所有 Prisma Access 部署都可以利用 Strata Cloud Manager 实现可见性功能（如命令中心和活动洞察）以及自主 DEM 监视。

此外，可以选择使用 Strata Cloud Manager 进行 Prisma Access 配置管理；另一个选择是使用 Panorama 进行配置管理。在这两种情况下，在 Prisma Access 许可证激活期间会引导您激活 Strata Cloud Manager Pro：

- 使用 Strata Cloud Manager 配置管理激活 Prisma Access
- 使用 Panorama 配置管理激活 Prisma Access

以软件 NGFW 积分激活 VM-Series Strata Cloud Manager Pro 版

您可以使用 Strata Cloud Manager 管理软件 NGFW 积分资助的 VM-Series 防火墙，通过 Strata Cloud Manager Pro 激活无缝访问高级管理和监视功能。

Strata Cloud Manager 支持管理独立 VM-Series 火墙和 Panorama 管理的 VM-Series 部署，为监控多个环境提供全面的解决方案：

- 激活 Strata Cloud Manager Pro
- 为 Panorama 托管 VM-Series 激活 Strata Cloud Manager Pro

使用企业许可协议激活 Strata Cloud Manager Pro 版

此任务显示如何激活 Strata Cloud Manager 的企业许可协议 (ELA)。ELA 附加组件是大型企业将订阅批量分配给从 Palo Alto Networks 购买的资产的消费模式。

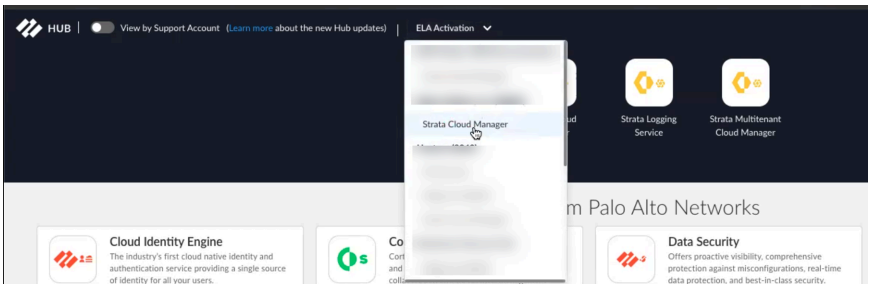
以下是 NGFW 的先决条件：

- 云管理接入先决条件 - 在将 NGFW 载 Strata Cloud Manager 之前，请验证设备就绪性的所有条件均已满足。这包括网络配置、软件兼容性和许可要求。完成这些步骤可确保使用 Strata Cloud Manager 成功管理防防火墙。
- **TCP 端口和云管理 FQDN** — 要在 NGFW 和 Strata Cloud Manager 之间实现无缝通信，请配置特定 TCP 端口和完全限定域名 (FQDN)。

对于属于同一支持帐户的设备，您可以使用相同的许可证激活多个 *Strata Cloud Manager Pro* 版租户。为此，请导航到租户管理以创建新租户。然后，转到订阅和附加组件，搜索您的订阅，单击激活云租户，这将重定向到激活页面。在激活页面上选择与最初使用的相同的 *TSG*。

STEP 1 | 使用以下激活方法之一。

- 登录到中心，然后选择 **ELA 激活 > Strata Cloud Manager**。



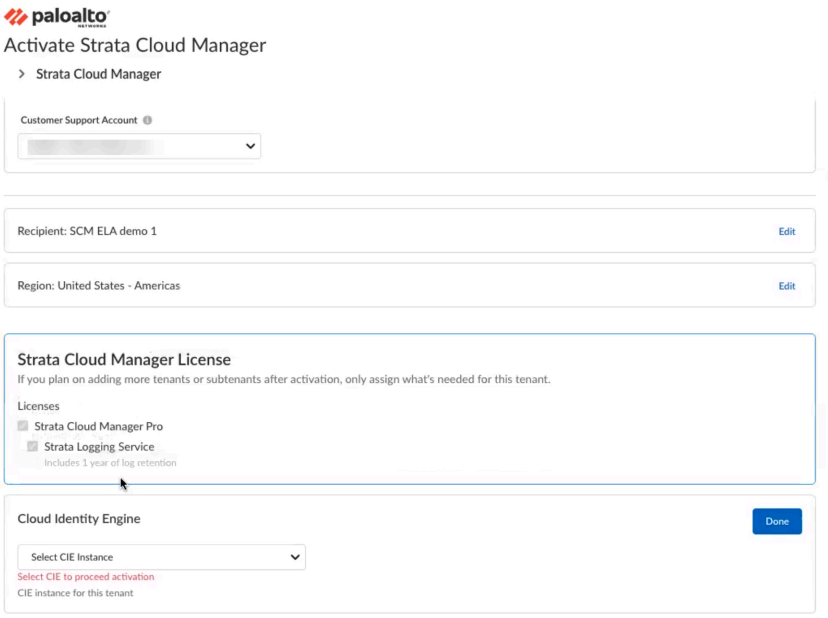
- 登录客户支持门户并从 许可证管理 > 许可证激活，然后单击 **ELA-Ngfw** 激活。

STEP 2 | 选择要使用的客户支持帐户。

STEP 3 | 选择租户，在其中激活 Strata Cloud Manager Pro 版。如果您还没有租户，请新建。

STEP 4 | 选择要在其中部署 Strata Cloud Manager 的区域。请参阅 Strata Cloud Manager 支持的区域。

Strata Cloud Manager Pro 版包括日志保留一年的 Strata 日志服务。



STEP 5 | 选择云身份引擎或创建新的 CIE 实例，以识别和验证整个基础架构中的所有用户。

STEP 6 | 依次单击 **Agree to the Terms and Conditions**（同意条款和条件）和 **Activate**（激活）。

STEP 7 | 等待 Strata Cloud Manager 和 Strata 日志服务初始化，等待两者的激活状态显示完成。

STEP 8 | 将 NGFW、Panorama 或两者关联到包含 Strata Cloud Manager 的租户。

确保将 *Panorama* 管理的所有防火墙单独关联到租户。

1. 导航到 **Common Services**（公共服务）**Device Associations**（设备关联）。
2. 添加设备。
3. 选择一个或多个防火墙或 Panorama 设备，然后单击 **Save**（保存）。

STEP 9 | 将产品关联到设备。激活 Strata Cloud Manager Pro 后，您需要指定要与其一起使用的防火墙或 Panorama 设备。

1. 登录到中心，然后选择 **Common Services**（共同事务）**> Device Associations**（设备关联）。
2. 关联产品。
3. 在许可产品选择列中，选择 **Strata Cloud Manager**。
4. 选择设备并 **Save**（保存）。

STEP 10 | 在设备上启用遥测。Strata Cloud Manager 通过分析 PAN-OS 设备发送到 Strata 日志服务的遥测数据来评估部署中设备的运行状况。要发送此数据，您必须已经在设备上启用设备遥测。

> 从 *PAN-OS 12.1.2*、*11.1.11*、*11.2.8*、*10.2.17* 及更高版本开始，遥测自动启用功能将遥测配置为默认在您的设备上启用。加入新设备（*Panorama* 或防火墙）后，通过 *Strata Cloud Manager* 或中心集中控制设置，遥测将自动启用。

STEP 11 | 通过单击中心中的图标登录到 Strata Cloud Manager。

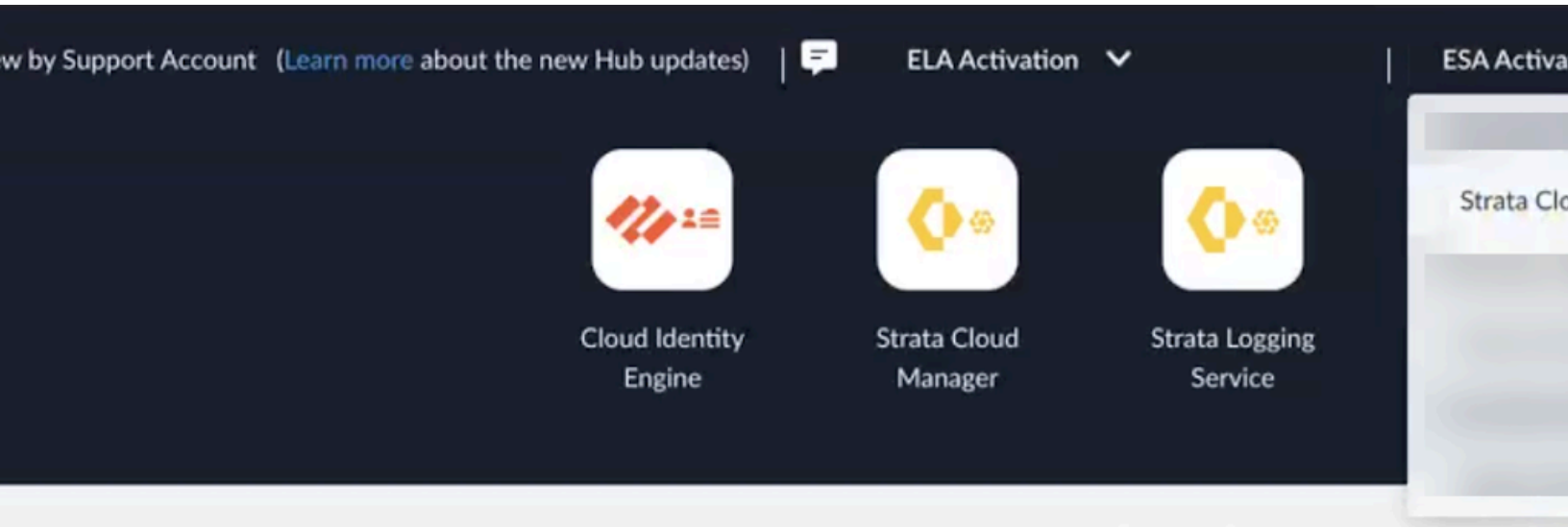
使用企业支持协议激活 Strata Cloud Manager Pro

Palo Alto Networks 企业支持协议 (ESA) 专业版包括 NGFW Strata Cloud Manager Pro 版。ESA Pro 提供简化的解决方案，让您的现有资产和预期购买获得一致的支持体验。此企业计划使组织能够随着规模的扩大而最大限度地节约成本并获取最大收益，是部署大型、不断扩展的防火墙的客户的理想选择。

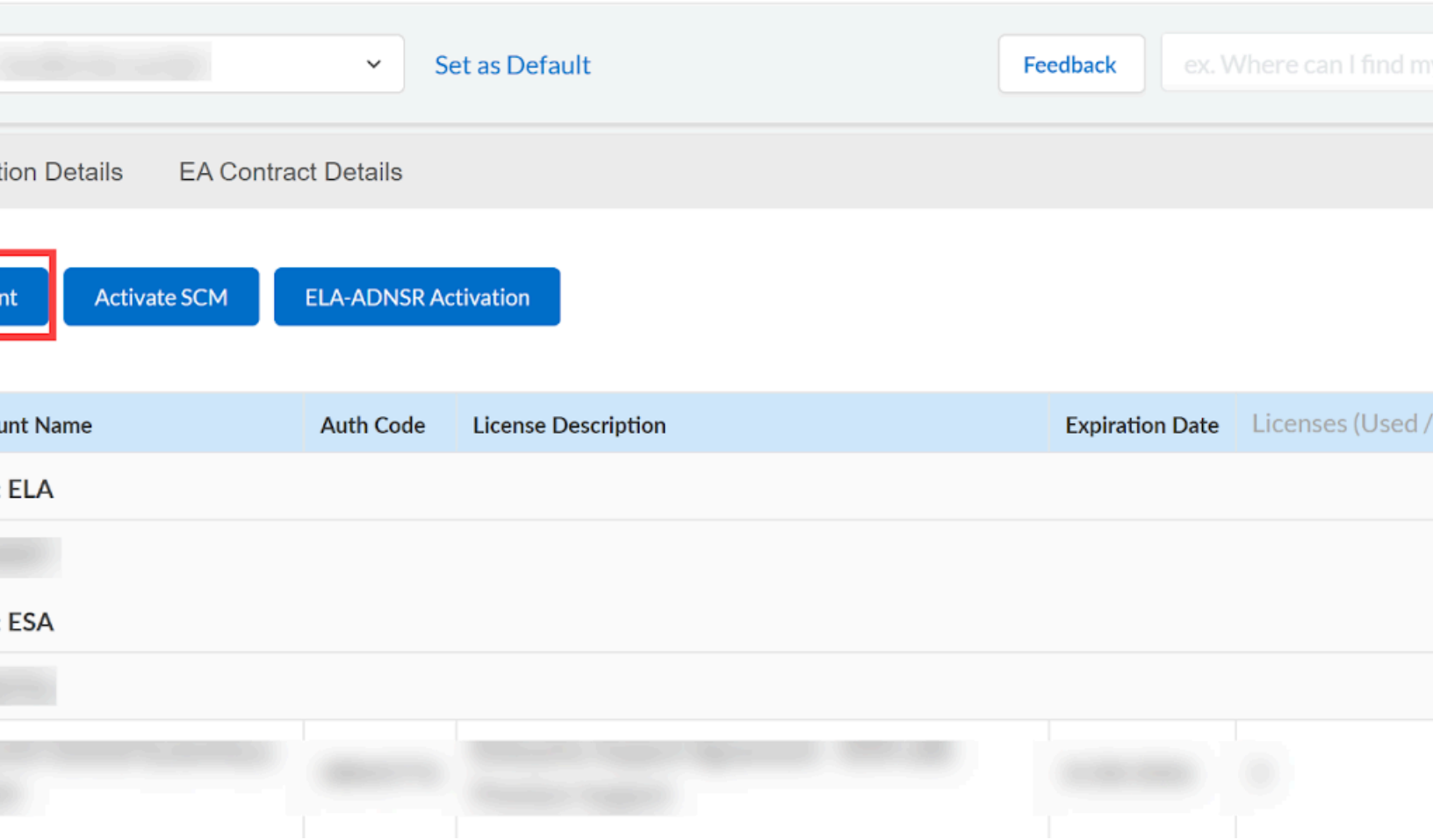
本任务显示如何激活 ESA Pro for Strata Cloud Manager。您可以从中心或客户支持门户启动 ESA Pro 激活流程，如下所述。

STEP 1 | 使用以下激活方法之一：

- 登录到中心并选择 **ESA** 激活 > **Strata Cloud Manager**。

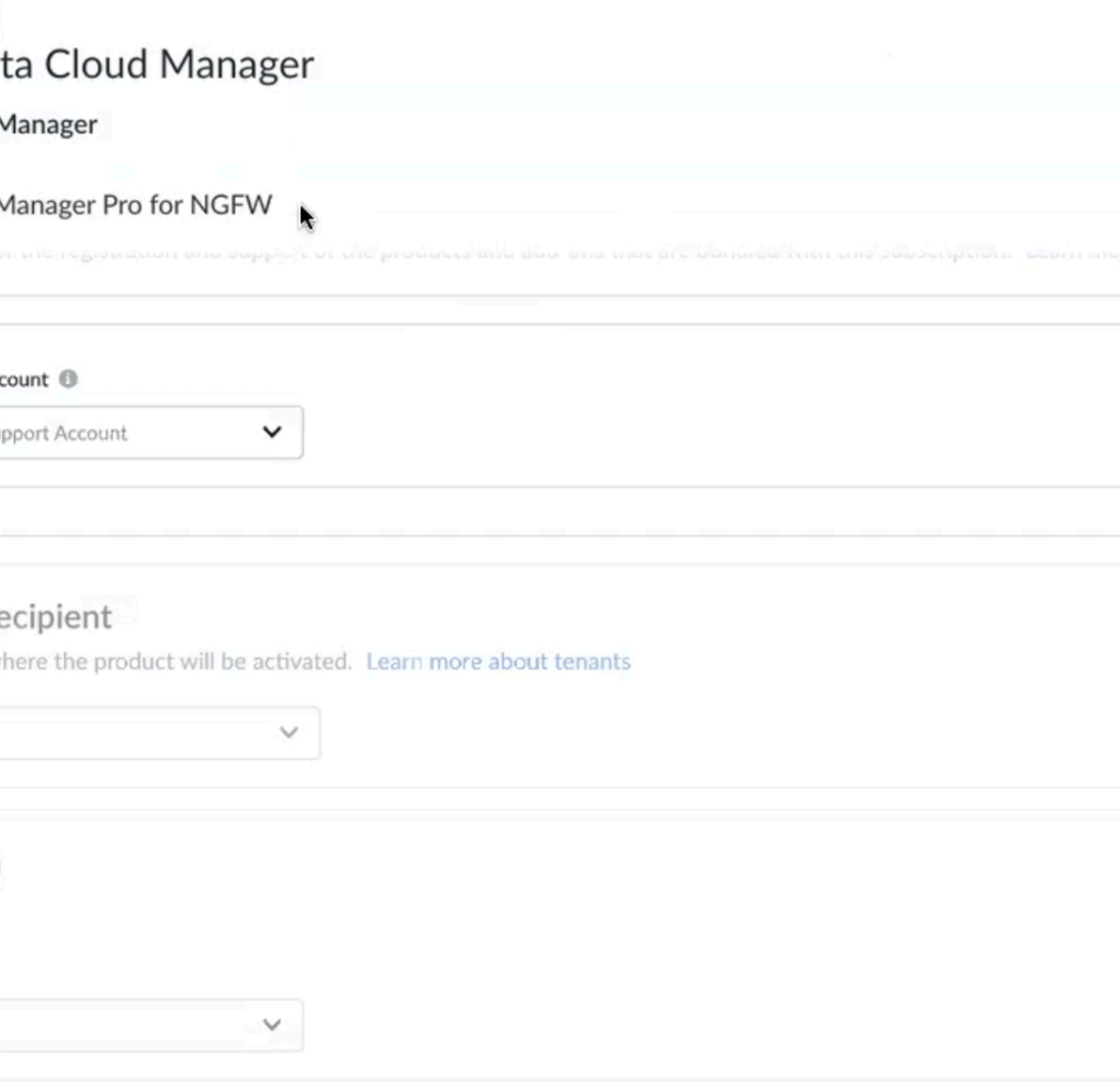


- 登录到客户支持门户。在左侧面板中，转到许可证管理，然后在许可证下选择激活企业协议。



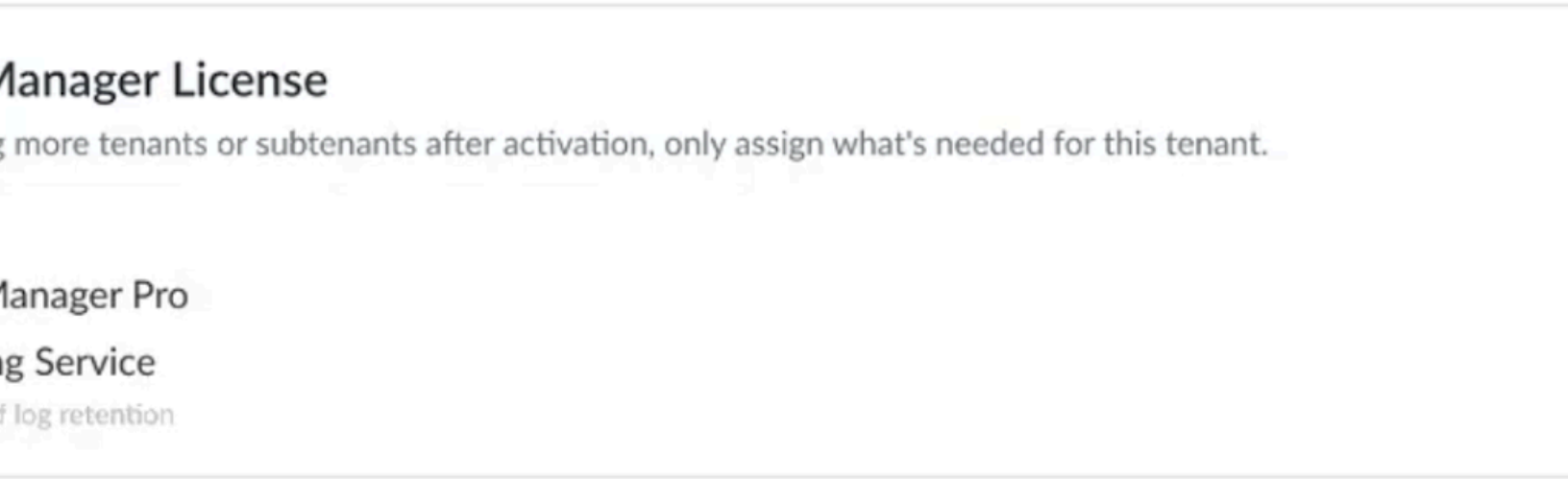
STEP 2 | 选择要使用的客户支持帐户。

STEP 3 | 创建一个新租户，您将在其中激活 Strata Cloud Manager 实例。



STEP 4 | 选择要在其中部署 Strata Cloud Manager 的区域。请参阅 Strata Cloud Manager 支持的区域。

Strata Cloud Manager Pro 许可证包括保留期为一年的 Strata 日志服务。



STEP 5 | 选择云身份引擎或创建新的 CIE 实例，以识别和验证整个基础架构中的所有用户。

STEP 6 | 依次单击 **Agree to the Terms and Conditions**（同意条款和条件）和 **Activate**（激活）。

STEP 7 | 等待 Strata Cloud Manager 和 Strata 日志服务初始化，等待两者的激活状态显示完成。

STEP 8 | 将 NGFW、Panorama 或两者关联到包含 Strata Cloud Manager 的租户。

确保将 *Panorama* 管理的所有防火墙单独关联到租户。

1. 导航到 **Common Services**（公共服务）**Device Associations**（设备关联）。
2. 添加设备。
3. 选择一个或多个防火墙或 Panorama 设备，然后单击 **Save**（保存）。

STEP 9 | 将产品关联到设备。激活 Strata Cloud Manager Pro 后，您需要指定要与其一起使用的防火墙或 Panorama 设备。

1. 登录到中心，然后选择 **Common Services**（共同事务）**> Device Associations**（设备关联）。
2. 关联产品。
3. 在许可产品选择列中，选择 **Strata Cloud Manager**。
4. 选择设备并 **Save**（保存）。

STEP 10 | 在设备上启用遥测。Strata Cloud Manager 通过分析 PAN-OS 设备发送到 Strata 日志服务的遥测数据来评估部署中设备的运行状况。要发送此数据，您必须已经在设备上启用设备遥测。

从 *PAN-OS 12.1.2*、*11.1.11*、*11.2.8*、*10.2.17* 及更高版本开始，遥测自动启用功能将遥测配置为默认在您的设备上启用。加入新设备（*Panorama* 或防火墙）后，通过 *Strata Cloud Manager* 或中心集中控制设置，遥测将自动启用。

STEP 11 | 通过单击中心中的 Strata Cloud Manager 图标登录。

从 Panorama 迁移到 Strata Cloud Manager

在何处可以使用？	需要提供什么？
• NGFW (Managed by Panorama) • Prisma Access (Managed by Panorama)	迁移 NGFW： ❑ Strata Cloud Manager 基础版或专业版许可证 ❑ 确保您的 NGFW 满足云管理的先决条件 迁移 Prisma Access： ❑ Prisma Access 许可证 ❑ 要开始从 Prisma Access（由 Panorama 管理）迁移到 Prisma Access（由 Strata Cloud Manager 管理），请联系 Palo Alto Networks 客户团队

从 Panorama 迁移到 Strata Cloud Manager 现在可用于 Prisma Access 和 NGFW 部署，让您在云环境中享受云管理和共享配置管理的好处。迁移过程解决了配置保存和策略连续性等考虑因素。

对于 NGFW 部署，您可以按照此工作流程查看配置兼容性，即使您尚未准备好迁移。您可以决定删除或接受 Strata Cloud Manager 配置管理不支持或部分支持的任何功能。在迁移期间，Strata Cloud Manager 将 Panorama 设备组层次结构转换为相应的 Strata Cloud Manager 文件夹结构，并将 Panorama 模板和模板堆栈转换为可重用的代码段。

对于 Prisma Access 部署，迁移侧重于保留远程访问基础架构、移动用户配置和站点到站点的连接，同时将管理监督过渡到 Strata Cloud Manager。

- 新一代防火墙迁移
- Prisma Access 迁移

从 Panorama 迁移到 Strata Cloud Manager (NGFW)

您可以将现有的 NGFW 配置从 Panorama 迁移到 Strata Cloud Manager 以实现基于云的配置管理。

在迁移过程中，Strata Cloud Manager：

- 复制和翻译支持的安全策略、网络配置和对象。
- 维护现有的网络拓扑和 NGFW 部署。
- 突出显示部分支持或不支持的区域。

请联系 *Palo Alto Networks* 客户团队，启用迁移工作流。

使用 Strata Cloud Manager 而不是 Panorama 管理 NGFW 可以为您提供各种优势，如对 Prisma Access 和 NGFW 进行统一管理、网络具有云原生可扩展性以及增强的可视性。

Strata Cloud Manager 通过下列关键步骤指导您完成配置迁移：

- 上传现有配置 — 导入您当前的 Panorama 配置。
- 运行兼容性评估 — 确定需要注意的不受支持的功能或配置。
- 执行验证并准备部署 — 在迁移前完成最终检查。
- 迁移控制 — 设备和设备组可以分阶段迁移，允许您迁移非关键设备或逐个站点迁移。

在完成迁移之前，请审核每一步的结果，进行必要的调整，并验证您的配置是否与 Strata Cloud Manager 完全兼容。

从 Panorama 迁移到 Strata Cloud Manager 时配置管理如何变化

Panorama 配置管理基于：

- 设备组 — 将防火墙组织成分层组，用于安全策略管理（安全规则、NAT 策略、应用程序过滤器）。
- 模板和模板栈 — 定义网络和设备设置（接口、区域、路由、系统设置）。
- 继承 — 设备组继承父组的策略；模板堆栈层具有覆盖功能的多个模板。

Strata Cloud Manager 配置管理基于：

- 文件夹 — 包含安全策略和网络配置的分层容器。
- 代码段 — 可重复使用的配置块，可附加到任意级别的文件夹。
- 容器 — 特定于设备的配置持有者，用于满足独特的防火墙墙要求。

在迁移过程中，Strata Cloud Manager 会转换基于 Panorama 的配置并将其构建到文件夹和代码段中：

Panorama	Strata Cloud Manager
设备组	文件夹
模板和模板堆栈	代码段

Panorama	Strata Cloud Manager
分享的 DG	所有防火墙文件夹
共享对象	作为附加代码段的全局文件夹
设备组中的策略	映射文件夹下的策略
对象（地址、EDL 等）	映射文件夹下的对象

Panorama 和 Strata Cloud Manager 之间需要记住的关键区别：

- Strata Cloud Manager 文件夹包含网络和安全配置，而 Panorama 在模板和设备组之间分离这些配置
- Strata Cloud Manager 文件夹提供更灵活的继承，与 Panorama 中看到的较低级别的组覆盖相比，基于代码段的覆盖
- Strata Cloud Manager 代码段与 Panorama 的模板和模板堆栈相比，提供了更多即插即用的配置方法。

迁移后，您可以通过文件夹和代码段型号管理配置。代码段附加顺序确定配置优先级，为多个配置源的组合方式提供粒度控制。您还可以为需要在文件夹继承型号之外进行唯一配置的 NGFW 创建设备特定的容器。

其他资源

了解有关设备组和模板的详细信息。

了解有关代码段和文件夹的更多信息

准备将您的 NGFW 迁移到 Strata Cloud Manager

在开始迁移之前，请确保准备好以下项目：

- 最低软件要求：PAN-OS 10.2.3 或更高版本：
- 导出 Panorama 配置文件：以 XML 格式源 Panorama 实例导出完整的运行配置
- Panorama 主密钥：获取 Panorama 配置中用于加密的主密钥（如果未使用默认密钥）
- Strata Cloud Manager 租户：验证您的 Strata Cloud Manager 租户是否已部署、获得正确许可并正在运行
- NGFW 配置：从您计划验证迁移后的 NGFW 收集最后推送的配置文件（技术支持文件）
- 网络拓扑：查看您当前的设备组层次结构、模板关系和 NGFW 分配
- 配置备份：作为安全措施，创建当前 Panorama 和 NGFW 配置的完整备份
- 管理访问权限：确保您在 Panorama 和 Strata Cloud Manager 中都有权访问超级用户角色。
- 迁移规划：确定要在初始阶段迁移的设备组、模板和 NGFW
- 兼容性矩阵：了解 Strata Cloud Manager 可能不支持哪些功能，并计划进行任何必要的配置调整

将您的 Panorama 托管 NGFW 迁移到 Strata Cloud Manager

将您的 NGFW 配置从 Panorama 迁移到 Strata Cloud Manager：

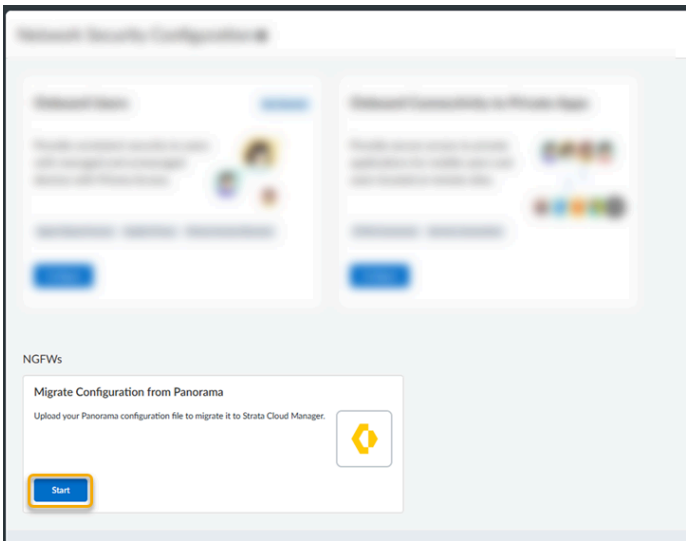
STEP 1 | 准备好 Panorama 的迁移工作

1. 使用被分配了超级用户角色的管理员帐户登录到管理您的 NGFW 的 Panorama。
2. （可选）如果您为 Panorama 配置了自定义主密钥，请记下来。

   如果您的部署使用默认主密钥，则不需要执行此步骤。
3. 请确保您当前的 Panorama 配置是最新的，并且您已通过转到提交 > 提交和推送 和 预览更改 将所有当前更改提交并推送到 Panorama。
4. （可选）检查运行配置和候选配置之间的差异，并确定是否要推送这些更改。如要提交并推送更改，请单击 **Edit Selections**（编辑选择项），然后在 **Push Scope**（推送范围）中选择您想要推送的 NGFW。
5. （可选）选择 **Commit and Push**（提交并推送）以提交并推送更改。
6. 转到 **Panorama** > **Setup**（设置） > **Operations**（操作），然后单击 **Export**（导出）名为 Panorama 的配置快照。

   在迁移过程中，需要将 .xml 文件上传到 Strata Cloud Manager。请勿上传技术支持文件或除 .xml 配置文件以外的任何其他文件。
7. 选择 **running-config.xml** 配置文件，然后单击 **OK**（确定）。

STEP 2 | 以具有超级用户角色的管理员身份登录到 Strata Cloud Manager，然后转到配置 > 接入。

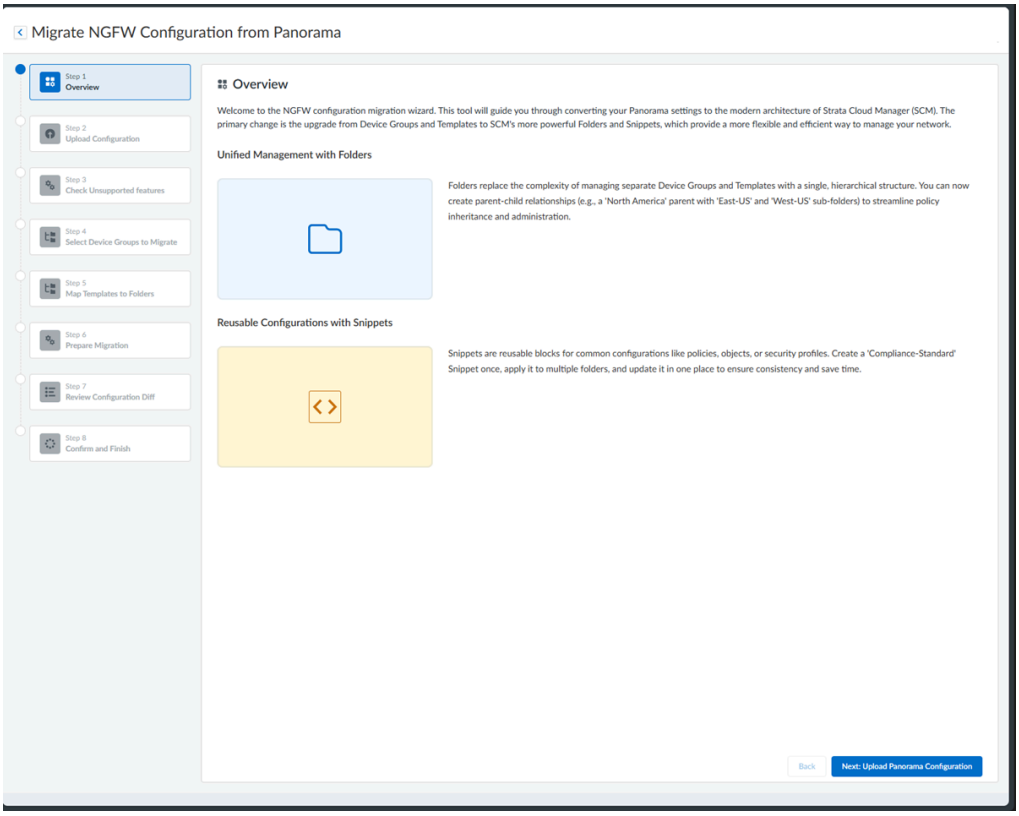


迁移程序检测到您采用了 Panorama 托管部署。

1. 确认租户是否正确。
2. （可选）在需要回滚时，为运行配置创建命名快照。

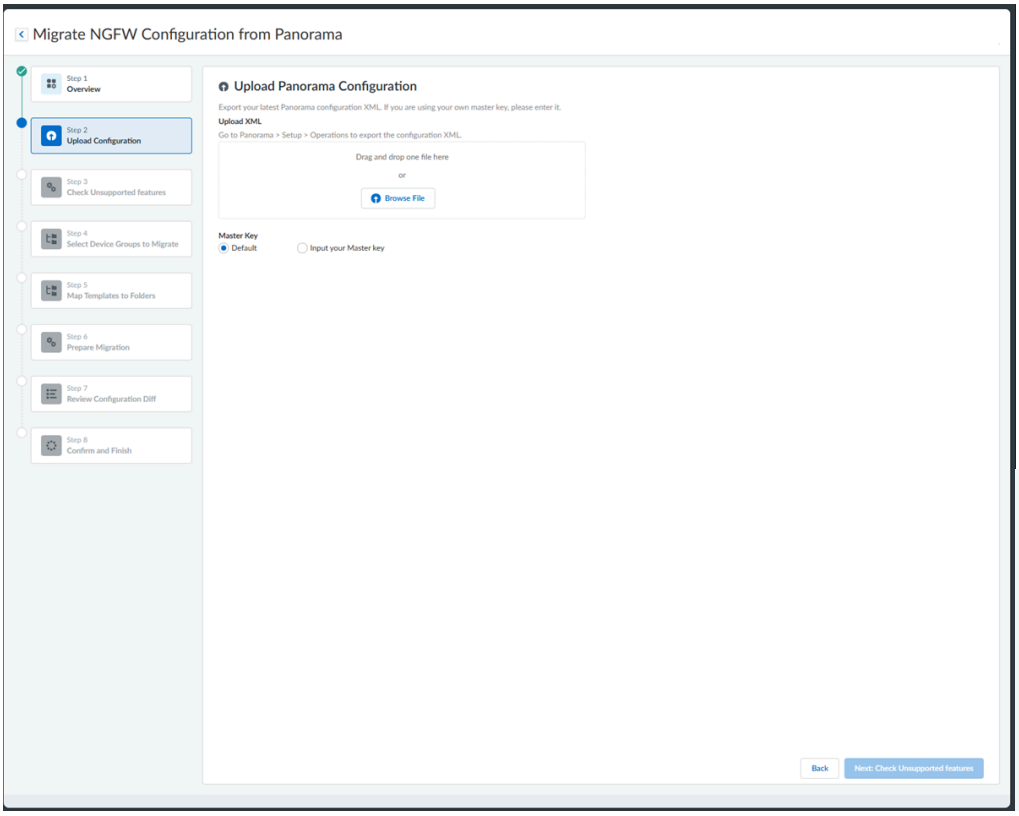
Strata Cloud Manager 升级窗口期间不应尝试迁移。检查您的升级时间表，查看您是否即将进行升级。

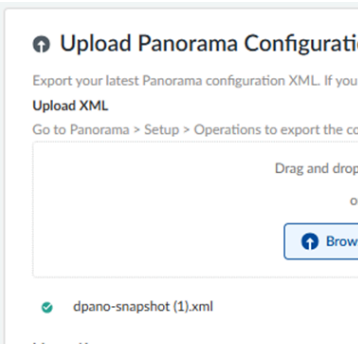
STEP 3 | 参阅迁移概述。



1. 查看 Strata Cloud Manager 的管理构建块：文件夹和代码段。
2. 单击下一步：上传 **Panorama** 配置。

STEP 4 | 提交 Panorama 配置。

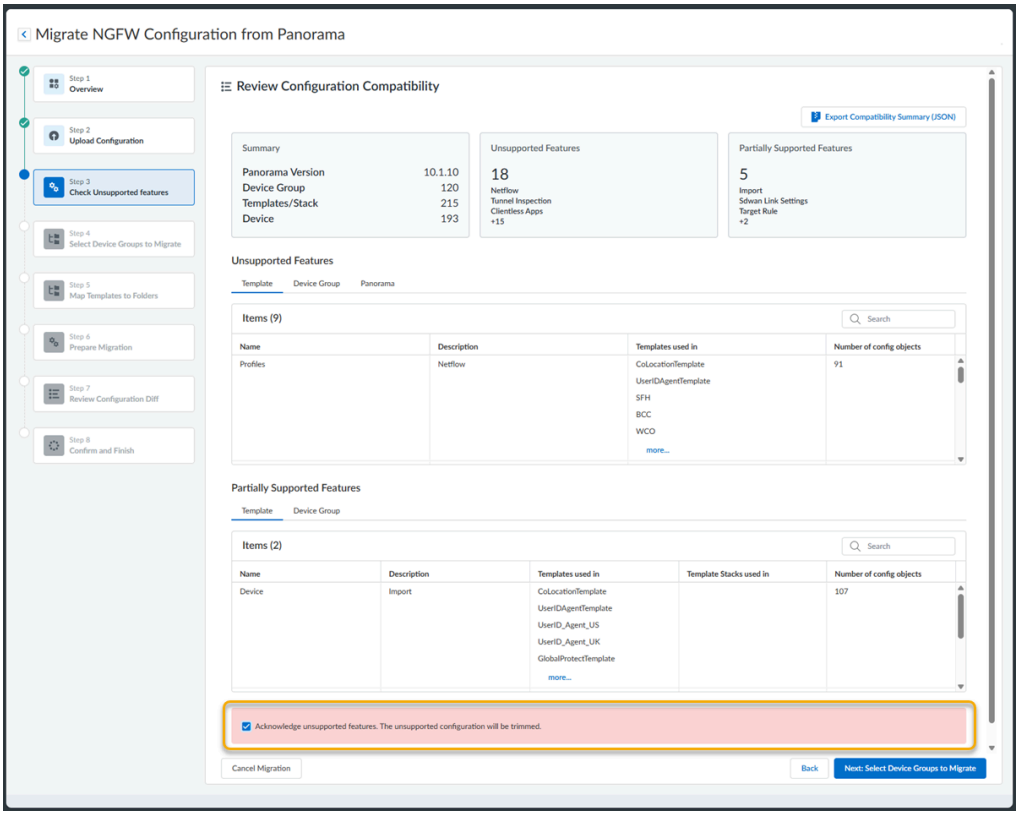




1. 从文件资源管理器中拖放或选择 选择文件，选择您在前面步骤中下载的全景配置 *.xml* 文件。
2. （可选）输入您的 主密钥，或者，如果您没有创建自定义主密钥，请使用默认。

3. 单击 **Next:**查看迁移兼容性。

STEP 5 | 检查配置兼容性。

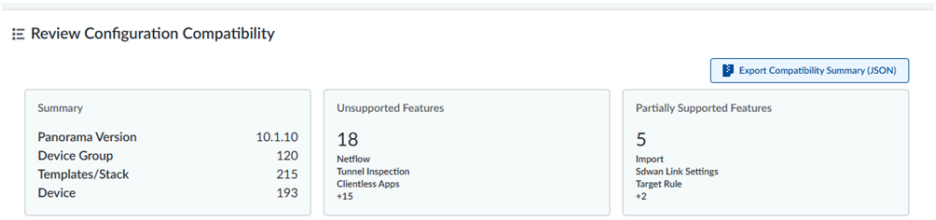


1. （可选）导出兼容性摘要并检查组织的配置兼容性，然后继续并允许 Strata Cloud Manager 删除任何不受支持或部分受支持的配置。

   对不受支持和部分支持的功能进行删除可避免迁移无法在 Strata Cloud Manager 中安全部署的功能。

   此过程只会影响 Strata Cloud Manager 的分阶段配置。Panorama 中的配置将不受影响。

   对于每个已标记的区域，您应该计划重建、替换或推迟这些配置。

2. 查看迁移期间将从配置中删除的不受支持功能。

   这些功能将从您的配置中删除，在配置迁移过程中不会在 Strata Cloud Manager 中暂存。

3. 查看部分支持功能并确定解析路径。

   确定配置中究竟会缺少什么。

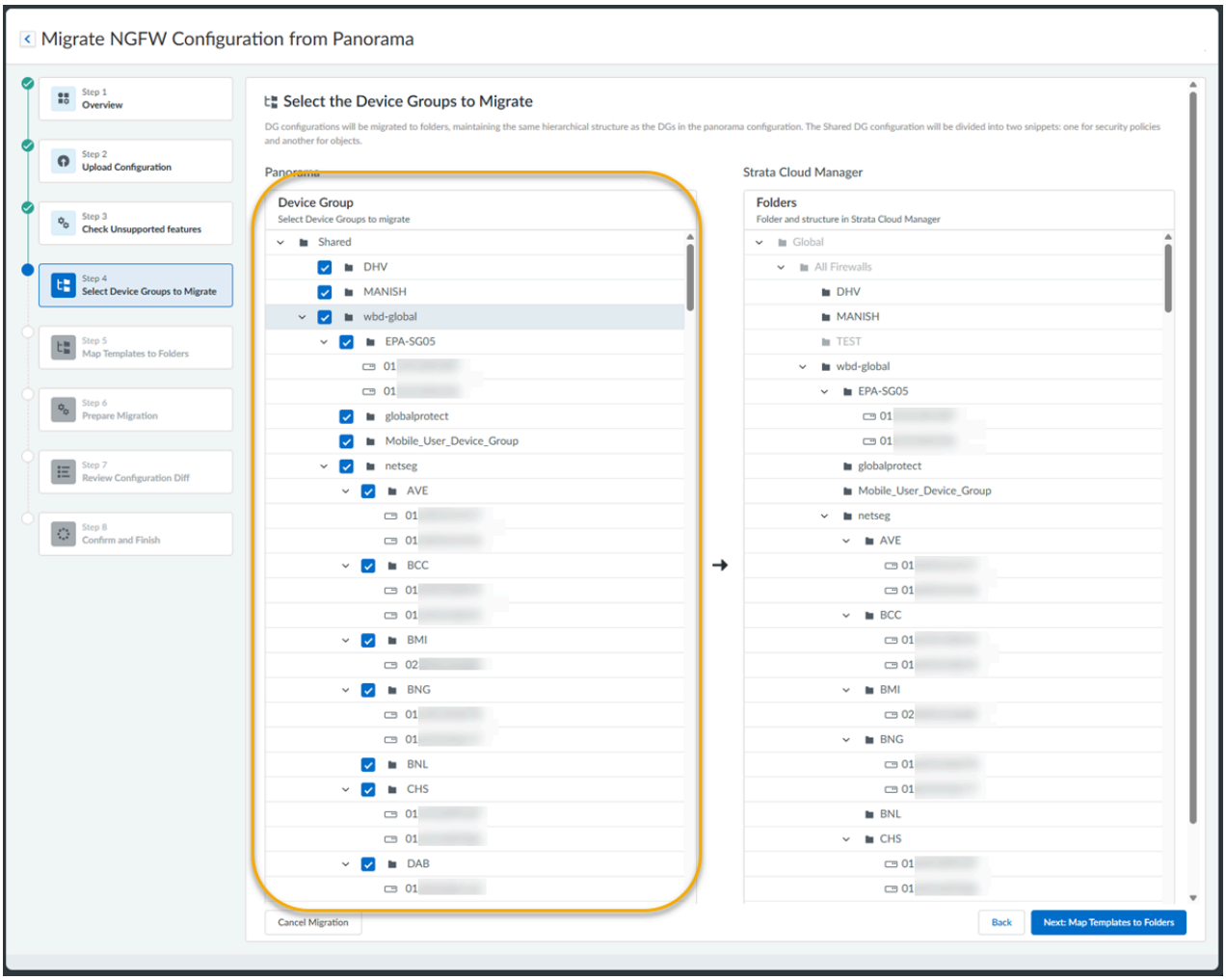
   您可以接受部分支持的功能并在迁移后构建修正计划，或者返回到 Panorama 配置并清理这些区域，然后再重新开始迁移过程。

4. 确认不支持和部分支持的功能。
5. 单击下一步：选择要迁移的设备组。

对于那些只是想比较支持的配置，或者如果决定不需要更多规划的用户，您可以在此处结束迁移过程。

STEP 6 | 选择要迁移的设备或设备组。

如果您是首次从 *Panorama* 迁移 *NGFW*，建议首先仅迁移非关键设备或设备组，以测试您的配置将如何迁移到 *Strata Cloud Manager*。

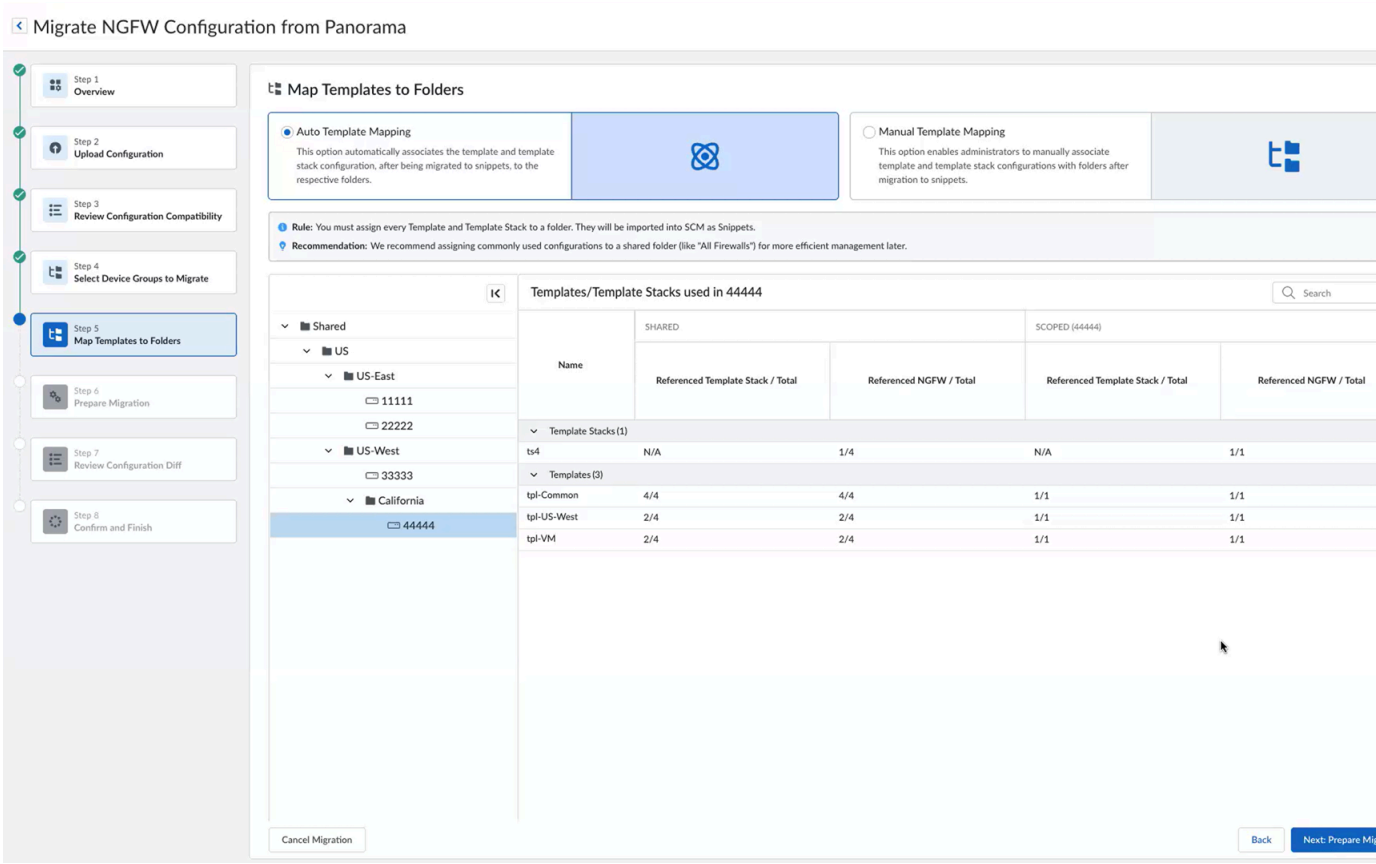


迁移期间：

- 对象导入到代码段并附加到全局文件夹。
- 策略导入工作流迁移的文件夹下。
- 共享设备组将自动映射到所有防火墙文件夹。

1. 单击下一步：将模板映射到文件夹。

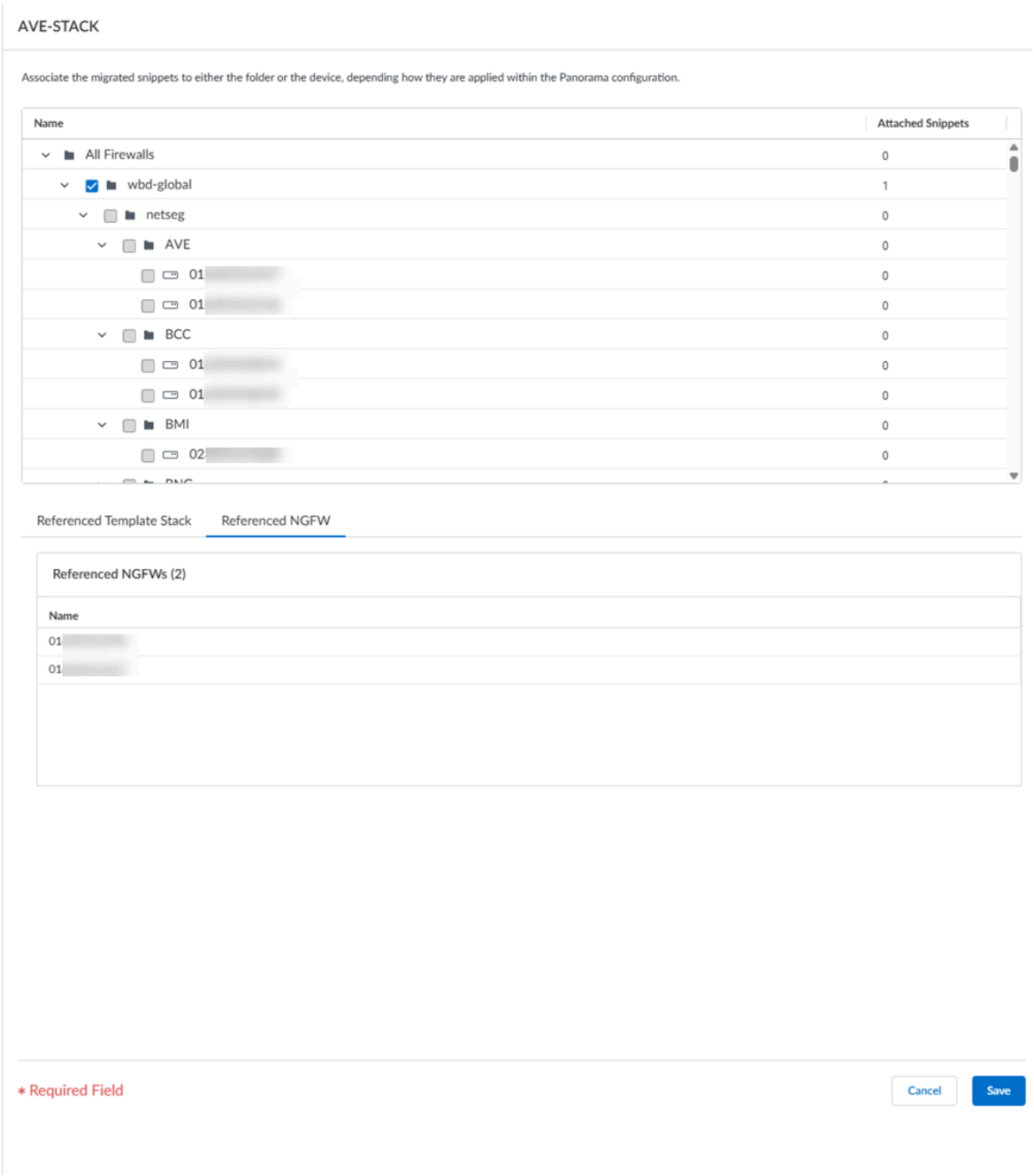
STEP 7 | 将模板映射到新配置的文件夹。



在迁移过程中，将模板配置成等效代码段。

如果两个或多个设备组重复使用同一模板，请将其提升到上一级文件夹。如果只有一个站点需要它，请将其保持在站点级别。

1. 选择设备组以显示该设备组使用的模板/模板堆栈。



2. 编辑映射以将每个模板/模板堆栈分配给一个文件夹。
3. 将多处引用的模板提升到上一级文件夹。

   例如，如果您有全局模板设置，将其映射到“所有防火墙”文件夹，即可将这些设置确立为所有 NGFW 的真实来源。
4. 将多个代码段分配给一个文件夹后，调整顺序。
5. 上移或下移以最终确定顺序。
6. 更新顺序
7. 保存新顺序。

   在继续下一步之前，请确保以下事项：

- 没有未分配的模板或模板堆栈。
- 任何被多个设备组引用的模板都被提升到了正确的文件夹。

8. 单击 **Next:**准备迁移。

   迁移过程开始。

   等待所有步骤完成。

   如果迁移有任何问题，请返回前面的步骤进行评估和更改。如果问题继续存在，请联系 *Palo Alto Networks* 支持。

STEP 8 | 准备迁移。

1. 加载配置到 **Strata Cloud Manager** 以准备迁移。

   1. 迁移工作流程：

   - 使用定义的映射和代码段顺序，将设备、设备组、模板和模板堆栈转换为文件夹和代码段。
   - 创建 Strata Cloud Manager 快照以启用分阶段更改的回滚。
   - 检查现有 Strata Cloud Manager 配置中的冲突（名称冲突、缺少引用、31 个字符限制、RBAC 范围）。
   - 构建将在 Strata Cloud Manager 加载后使用的分阶段配置。

2. 加载结果并查看创建、更新或跳过的对象、策略或代码段。
3. 查看验证结果以了解迁移后的任何错误、警告和信息性消息。
4. 单击下一步：审查配置差异。

   这将新生成的配置提交到 Strata Cloud Manager。

STEP 9 | 审查配置差异。

1. 在左侧文件夹树中，展开到文件夹，然后选择要验证的 NGFW 序列号
2. 浏览文件并选择选定序列号的 TSF。

   上传所选 NGFW 的 TSF 文件，即可正确验证所有受支持、部分受支持和不受支持的配置。

   请务必查找任何已创建、修改或删除的内容。配置被简化并不足为奇。

   由于 *Strata Cloud Manager* 中的命名约定，一些长名称在需要时会被压缩。

3. 查看配置差异窗格。
   1. 绿色窗格：已创建或添加。它们存在于 Strata Cloud Manager 中，但在原始设备上不存在。
   2. 红色窗格：已删除或简化。Strata Cloud Manager 可能不支持，但设备上有。
   3. 黄色窗格：已修改。

   差异视图可能非常广泛，一次只能显示一个 *NGFW*，并且是根据 *TSF* 上最后推送的 *XML* 计算得出的。
4. 验证每种模式或站点类型的代表性设备的差异。
5. （可选）导出差异结果。
6. （可选）如果已进行任何更正，请重新生成差异。
7. 单击 **Next:**确认并完成。

STEP 10 | 确认并完成 NGFW 到 Strata Cloud Manager 的迁移。

现在迁移已完成，请查看 Strata Cloud Manager 的可用文档。

1. 确保步骤 8 和步骤 9 的结果被接受。
2. 确认迁移。

   这正式标志着迁移完成。
3. （可选）要随时将配置恢复到迁移前的状态，请选择还原。这将启动回滚工作流程，将 Strata Cloud Manager 恢复到加载迁移之前拍摄的快照。
4. （可选）要随时取消迁移，请选择取消迁移。这将中止迁移过程并清理任何临时更改。

从 Panorama 迁移到 Strata Cloud Manager (Prisma Access)

如果您现有的 Prisma Access 部署配置由 Panorama 托管，并且希望迁移到 Strata Cloud Manager 进行配置管理，Palo Alto Networks 提供了一个产品内工作流程，可让您将现有的 Prisma Access 配置迁移到 Strata Cloud Manager。

要启用迁移工作流程，您必须联系您的 *Palo Alto Networks* 客户团队。

使用 Strata Cloud Manager 代替 Panorama 来管理您的 Prisma Access 配置有以下优势：

- 持续的最佳实践评估
- 安全的默认配置
- 基于机器学习 (ML) 的配置优化
- 简化 Web 安全工作流
- 交互式可视化摘要（命令中心），可帮助您评估网络的运行状况、安全性和效率
- 用于复杂任务的直观工作流
- 简单安全的管理 API
- 云原生架构提供可扩展性、弹性和全球覆盖
- 无需管理硬件，也无需维护软件

准备迁移到 Prisma Access (Managed by Strata Cloud Manager)

在开始迁移之前，应了解最低软件要求以及可以迁移的 Prisma Access (Managed by Panorama) 部署类型。

- 何时迁移—切勿在数据平面或基础设施升级期间执行升级。检查升级首选项，确认是否有即将进行的数据平面升级。
- 从 **Panorama** 到 **Prisma Access (Managed by Strata Cloud Manager)** 的单向迁移—您只能从 Prisma Access (Managed by Panorama) 部署迁移到 Prisma Access (Managed by Strata Cloud Manager) 部署。迁移到 Strata Cloud Manager 后，便无法再回到使用 Panorama 管理 Prisma Access 部署的场景。
- **Panorama** 最低版本—至少需要 Panorama 版本 10.0。
- 所需的管理员角色—您必须以超级用户身份登录 Strata Cloud Manager 才能开始迁移。
- 许可要求—需要有效的 Prisma Access 许可证。
- **Cloud Identity Engine**—在迁移之前，必须将 Cloud Identity Engine 的目录同步组件与当前的 Prisma Access (Managed by Panorama) 租户集成。

- 不支持的功能—迁移程序不支持 Prisma Access 的以下功能：
  - 数据过滤（或者，使用企业 DLP）
  - FedRAMP 部署
  - IoT 安全
  - 多租户部署
  - SSH 代理
  - GlobalProtect 门户和网关的独立身份验证
- **Prisma SD-WAN** 和 **Prisma Access**迁移—如果您迁移Prisma Access 和 Prisma SD-WAN 部署，则 Prisma Access 和 Prisma SD-WAN 必须共享相同的租户服务组 ID (TSG ID)。
- 配置差异问题 — 在迁移期间运行配置差异时，忽略显示以下对象名称的任何差异，因为它们不会影响您的配置：
  - Clientless-vpn crypto-settings
  - Hip-profiles rename
  - Mobile-user-redundancy
  - Exclude-video-traffic

将 Prisma Access (Managed by Panorama) 部署迁移到 Strata Cloud Manager

若要将 Prisma Access (Managed by Panorama) 迁移到 Prisma Access (Managed by Strata Cloud Manager) 部署，请完成以下步骤。

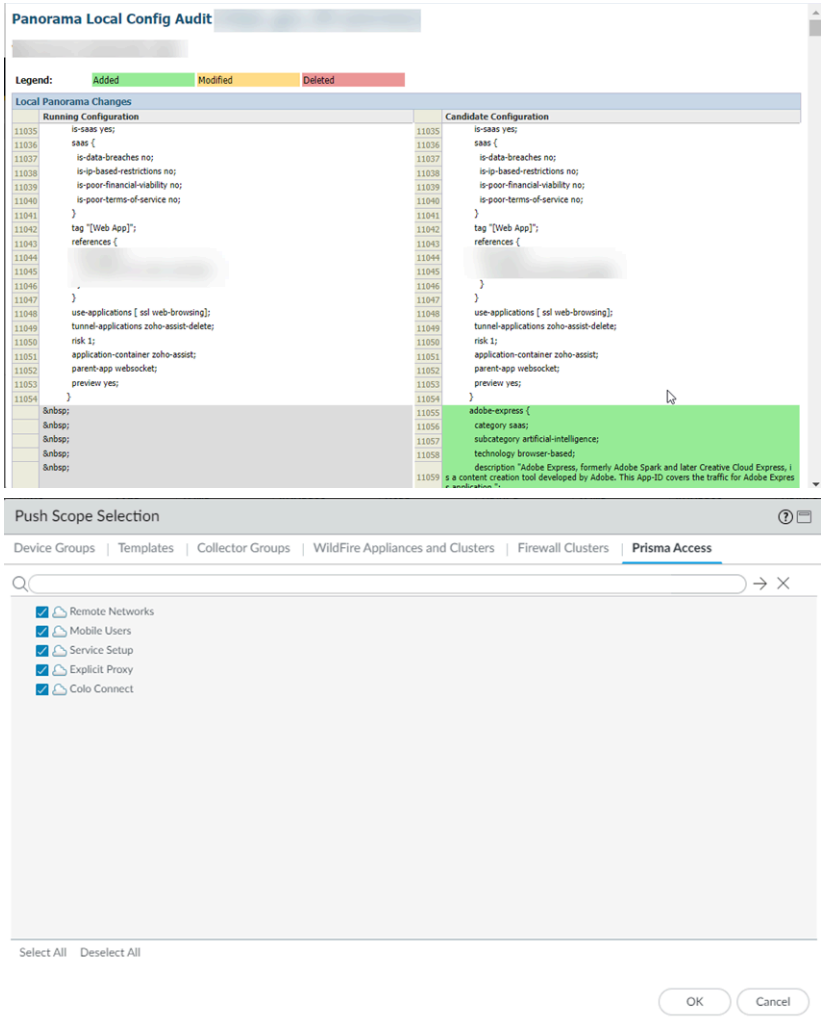
总体来说，您需要：

1. 请确保您已成功将最新配置推送到 Prisma Access，已保存最新配置，并已从管理 Prisma Access 的 Panorama 中导出了 .xml 配置文件。
2. 从 Strata Cloud Manager 启动迁移程序。
3. 检查 Panorama 配置与迁移的 Strata Cloud Manager 配置之间的配置差异（即“差异”）。
4. 解决差异并完成迁移。

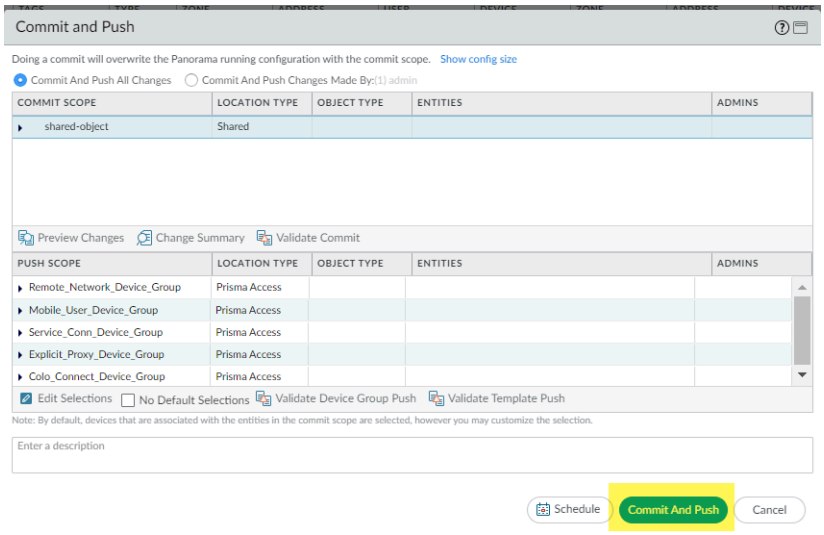
STEP 1 | 准备好 Panorama 的迁移工作

1. 登录到管理 Prisma Access 的 Panorama，并且要使用被分配了超级用户角色的管理帐户。
2. (可选) 如果您已为 Panorama 和 Prisma Access 配置了自定义主密钥，请记下来。

   如果您的部署使用默认主密钥，则不需要执行此步骤。
3. 确保您当前的 Panorama 配置是最新的，并且您已通过转到 **Commit**（提交） > **Commit & Push**（提交并推送） 以及 **Preview Changes**（预览更改），将所有更改提交并推送到 Panorama 和 Prisma Access。
4. （可选）检查运行配置和候选配置之间的差异，并确定是否要推送这些更改。如果您想要提交并推送这些更改，请单击 **Edit Selections**（编辑选择项），然后在 **Push Scope**（推送范围）中选择您想要推送的 Prisma Access 组件。



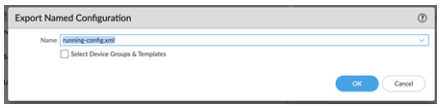
5. （可选）选择 **Commit and Push**（提交并推送）以提交并推送更改。



6. 转到 **Panorama** > **Setup**（设置） > **Operations**（操作），然后单击 **Export named Panorama configuration snapshot**（导出命名的 **Panorama** 配置快照）。

   在迁移过程中，需要将此 .xml 文件上传到 Strata Cloud Manager。请勿上传技术支持文件或除 **.xml** 配置文件以外的任何其他文件。

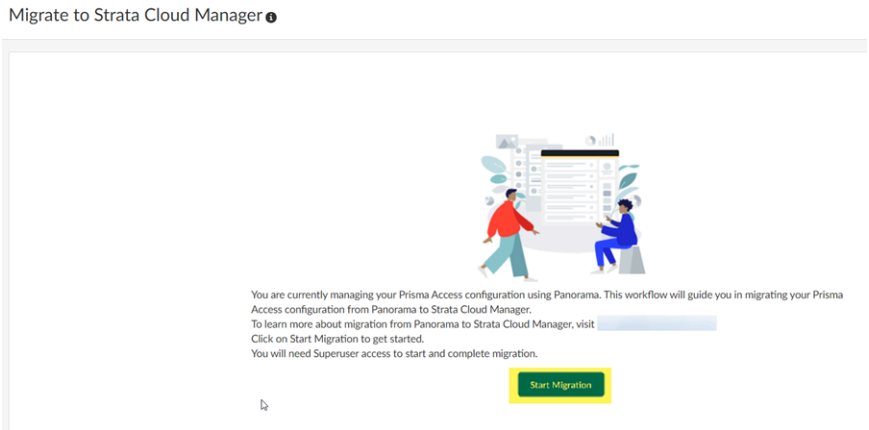
7. 选择 **running-config.xml** 配置文件，然后单击 **OK**（确定）。



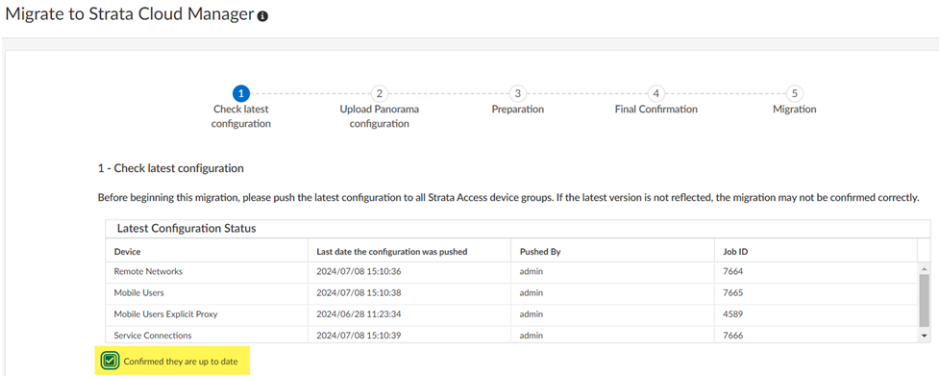
STEP 2 | 以具有超级用户角色的管理员身份登录到 Strata Cloud Manager，然后转到管理 > 配置 > **NGFW** 和 **Prisma Access**配置 > **NGFW** 和 **Prisma Access**。

迁移程序检测到您采用了 Panorama 托管部署。

STEP 3 | 开始迁移。

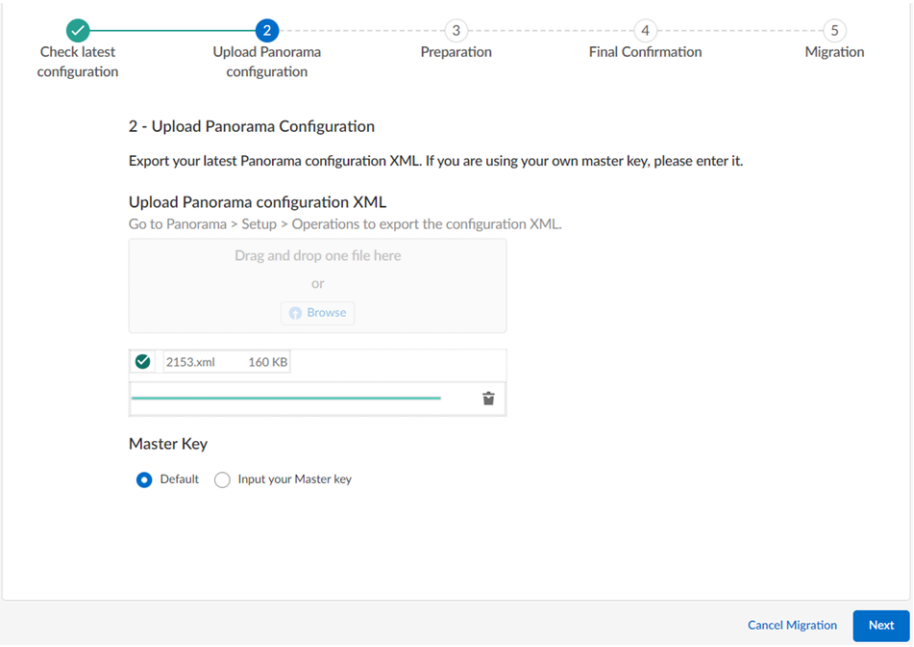


STEP 4 | 迁移程序要求您确保配置是最新的，并显示上次更新配置的用户。在您确认此配置包含了最新的更改之后，选择 **Confirmed they are up to date**（已确认它们是最新的），然后单击 **Next**（下一步）。

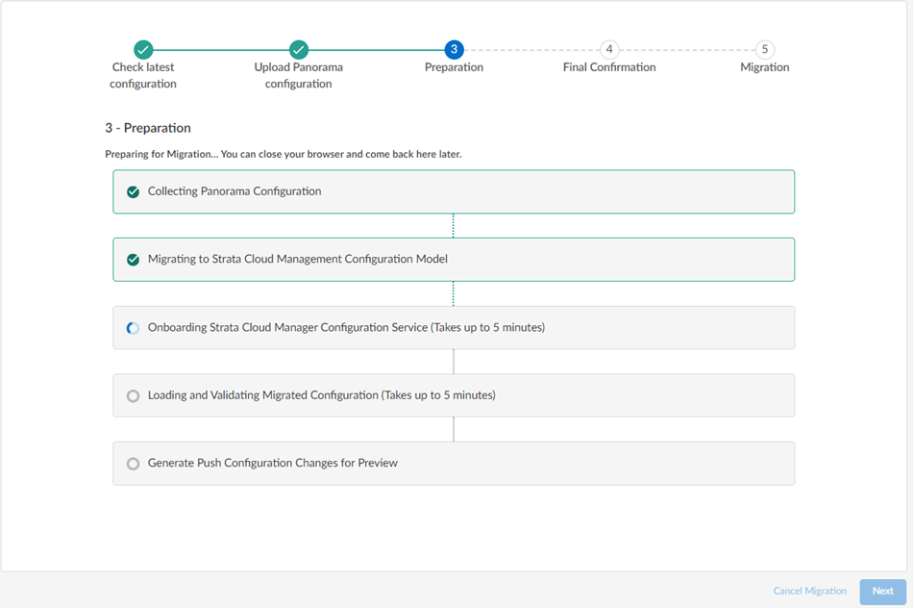


STEP 5 | 通过拖放操作，或者单击 **Choose File**（选择文件），来选择您在之前步骤中下载的 Panorama 配置 .xml 文件。

STEP 6 | 在 **Master Key**（主密钥）中输入您的主密钥，如果您没有创建自定义的主密钥，请让 Strata Cloud Manager 使用 **Default**（默认值）主密钥，然后单击 **Next**（下一步）。

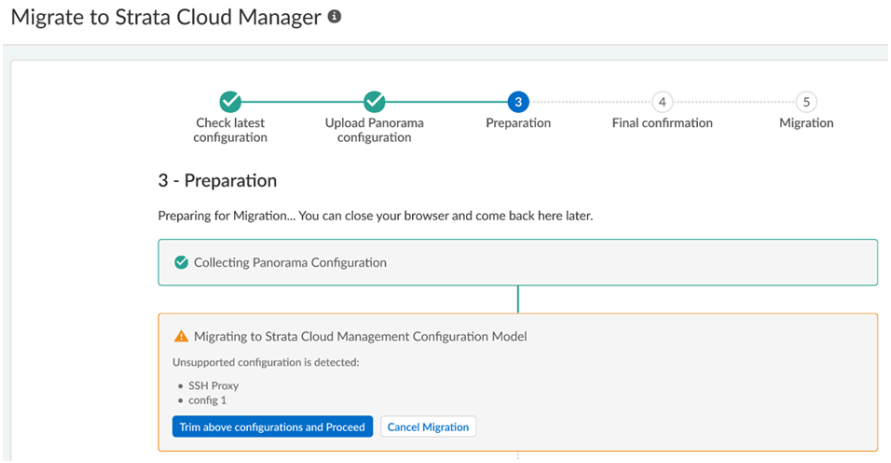


迁移程序随即开始。



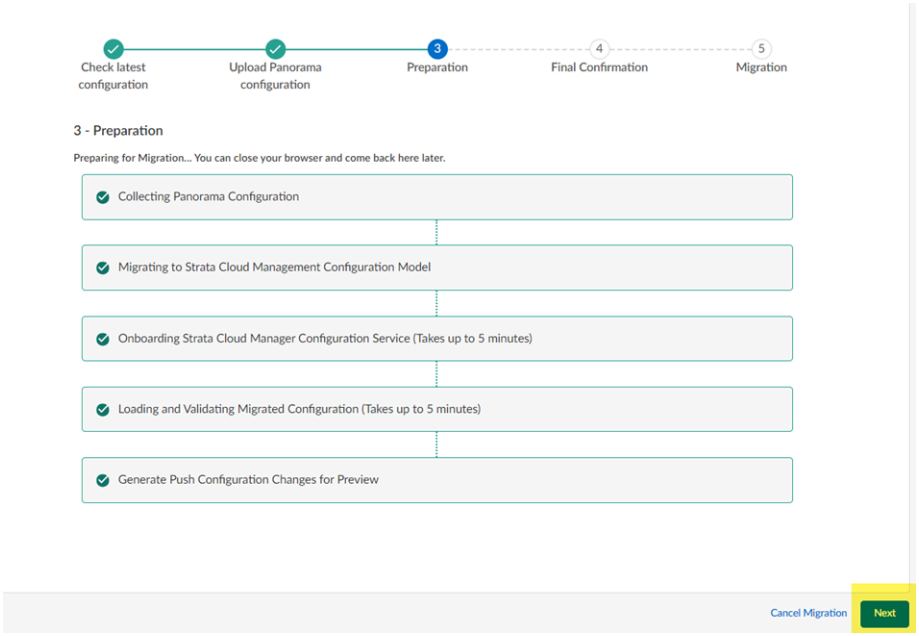
等待所有步骤完成。

STEP 7 | 如果在迁移过程中，程序显示它遇到了一个不支持的配置，可以单击简化上述配置并继续，或者单击 取消迁移。



一些不支持的配置（例如多租户配置）会导致取消迁移，并且迁移程序无法解决该问题；在这种情况下，请单击 **Cancel Migration**（取消迁移）。

STEP 8 | 迁移完成后，单击 **Next**（下一步）。

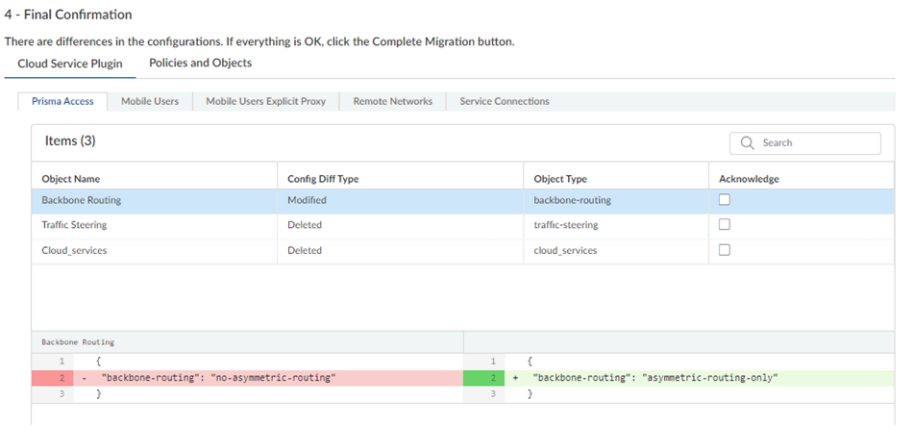


STEP 9 | 如果迁移程序进行了更改，请在最终确认屏幕中查看这些更改。

迁移程序可能会对您的配置进行更改，以处理 Panorama 和 Strata Cloud Manager 配置之间的差异，或者修复不被支持的功能。如果需要进行更改，迁移程序会在差异视图中显示这些更改内容，新增的行以绿色显示，删除的行以红色显示。

忽略显示以下对象名称的任何差异；它们不会影响您的配置：

- *Clientless-vpn crypto-settings*
- *Hip-profiles rename*
- *Mobile-user-redundancy*
- *Exclude-video-traffic*



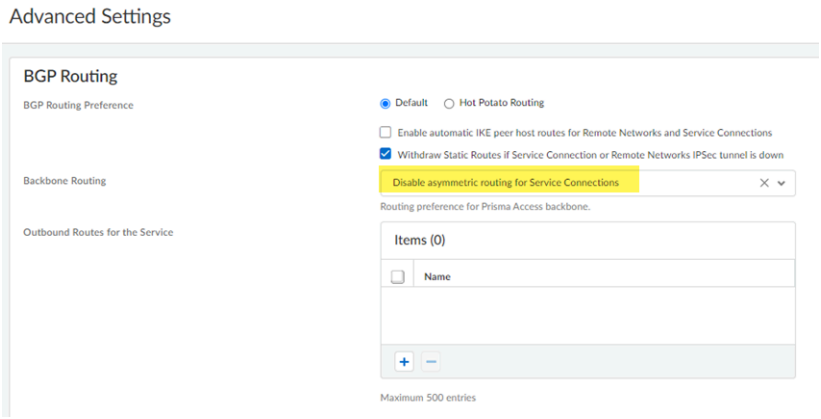
STEP 10 | （可选）对差异进行更改。

在您完成迁移并将更改推送到 Strata Cloud Manager 之前，您所做的任何更改都不会提交到配置中。

1. 导航到 Prisma Access 配置中找到差异的区域，并对配置进行更改。

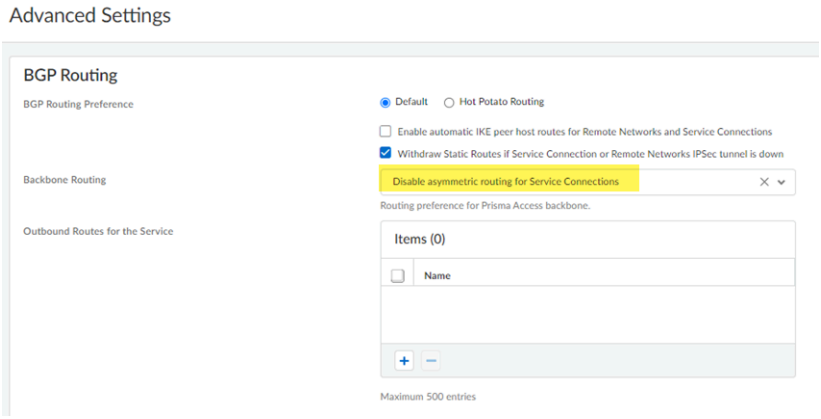
   对于上一步中的示例，迁移程序对骨干网路由进行了更改（从 **no-asymmetric-routing** 更改为 **asymmetric-routing-only**）。要将此设置改回原始配置，请转到 工作流程 > **Prisma**

Access 设置 > 服务连接 > 高级设置 配置 > **NGFW** 和 **Prisma Access** > 配置范围 > **Prisma Access** > 服务连接 > 高级设置，并将 骨干路由 配置更改为禁用服务连接的非对称路由。



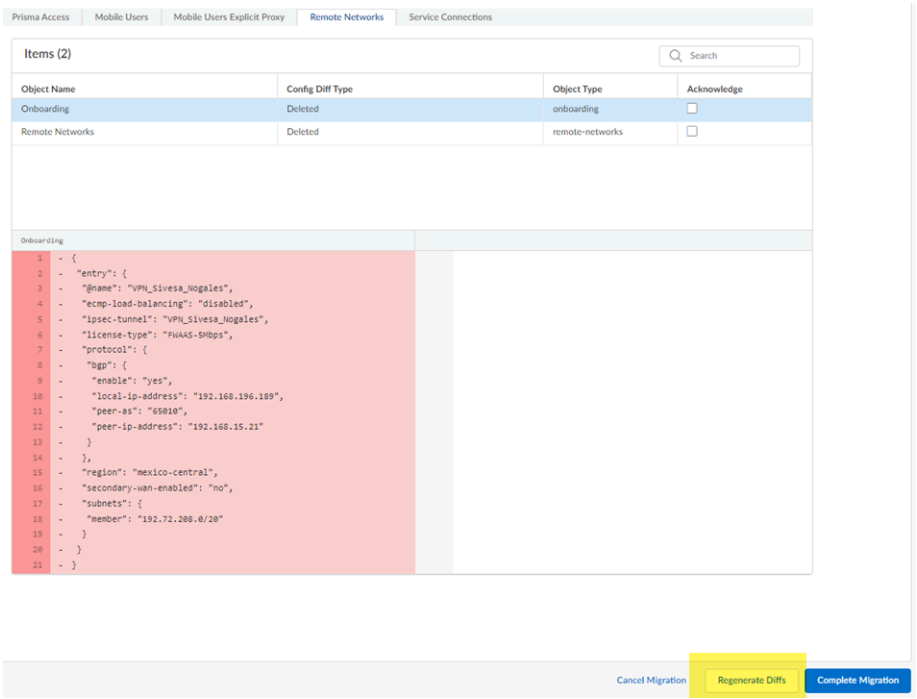
2. （可选）要跟踪您的更改，请在完成更改时单击 **Acknowledge**（确认）。

   虽然并非必需操作，但在您进行每一项更改时确认一下这些更改会很有用，这样您就可以跟踪更改。



3. 继续检查更改并进行更改和确认。

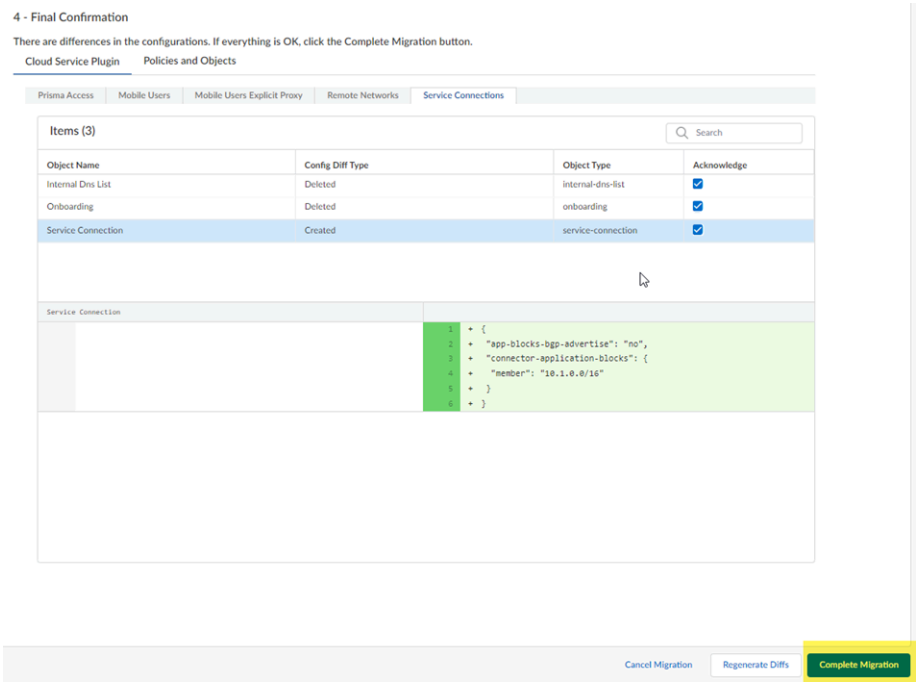
STEP 11 | （可选）如果对配置进行了任何更改，请单击 **Regenerate Diffs**（重新生成差异）以查看更新的差异。



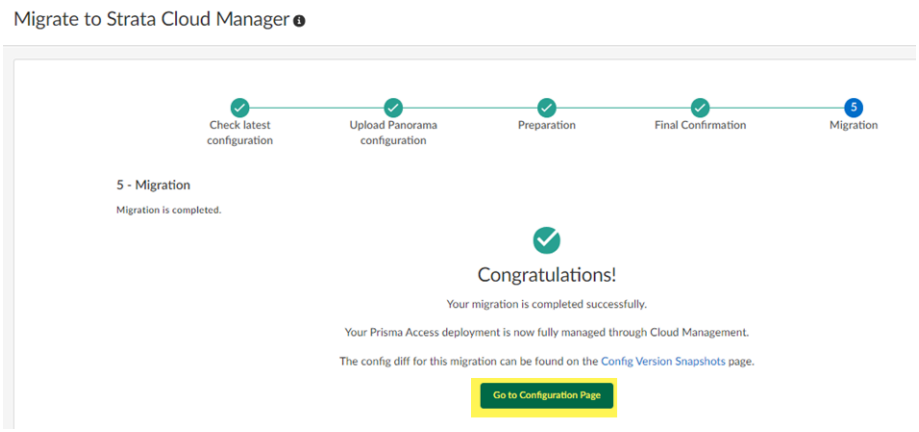
STEP 12 | 完成迁移。

您也可以单击 **Acknowledge**（确认）以确认您的更改（但不强制要求）。

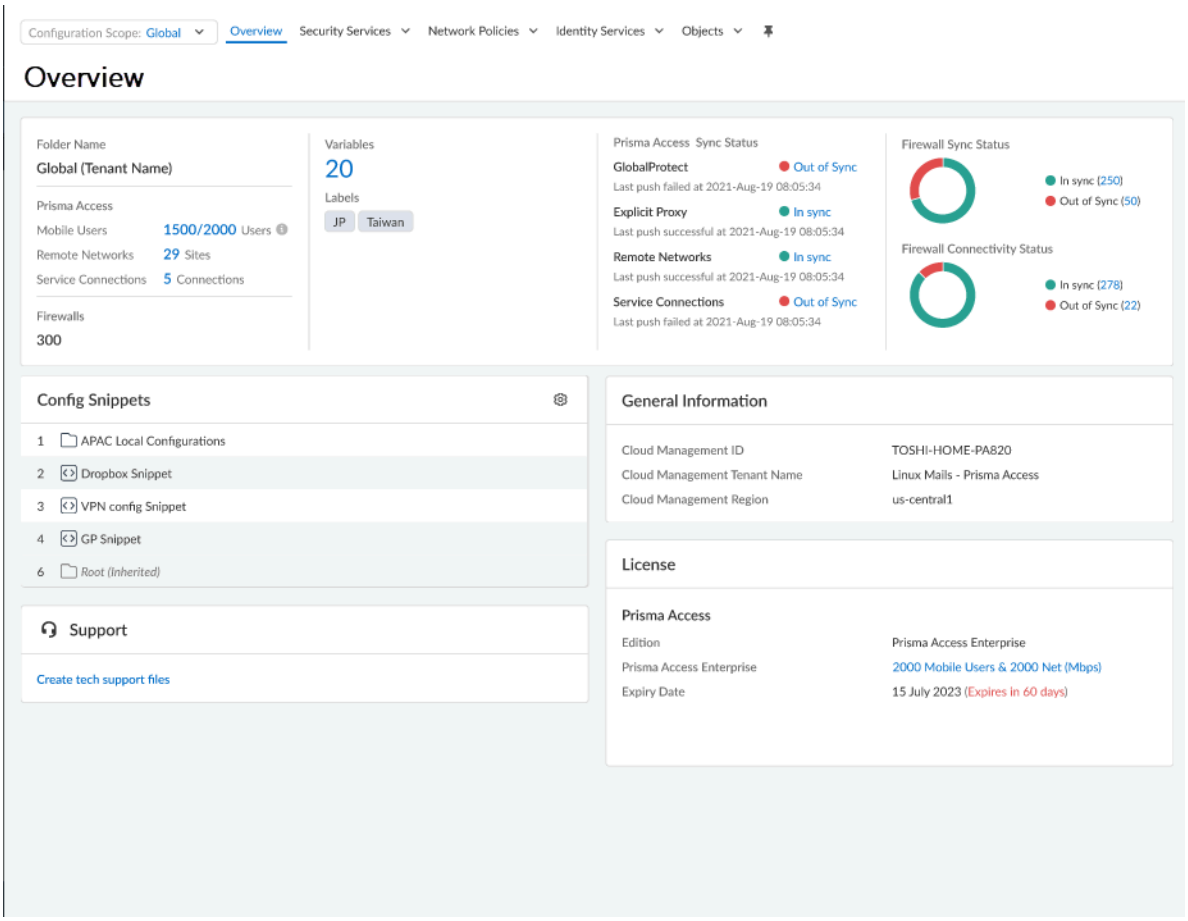
单击 **Complete Migration**（完成迁移）后，您将无法返回到 **Panorama** 托管部署，并且您的部署将永久使用 **Strata Cloud Manager** 来进行管理。



STEP 13 | （可选）单击 **Go to Configuration Page**（转到配置页）以查看迁移的配置。

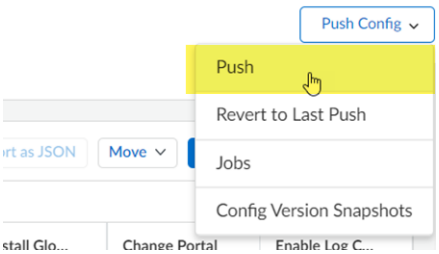


此时将显示迁移的部署。



STEP 14 | 单击 **Push Config**（推送配置） > **Push**（推送）以应用您已迁移的配置更改。

此推送操作可确保迁移已成功完成，并且 Prisma Access 已将所有更改应用于迁移的配置。



STEP 15 | 记下推送操作期间收到的任何消息，如果发现任何问题，请根据需要对配置进行更改。

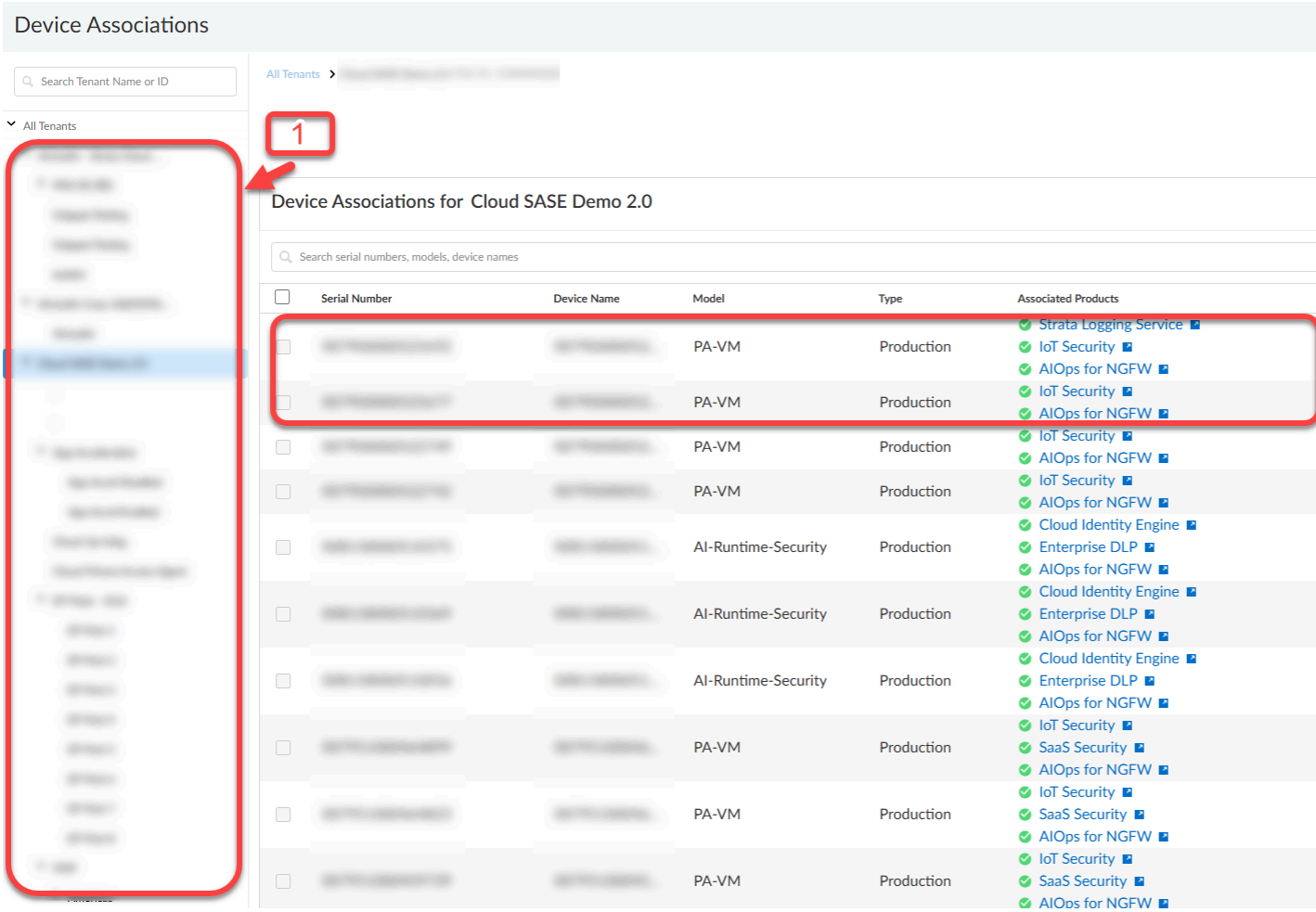
在 Strata Cloud Manager 中的设备关联

在何处可以使用？	需要提供什么？
• NGFW，包括由软件 NGFW 积分资助那些服务	以下之一： ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro 如果您在引入这些许可级别之前开始使用 Strata Cloud Manager，您的许可证仍然受支持。

作为 Strata Cloud Manager 和公共服务的一部分，**Device Associations** 提供了您部署中所有设备的集中管理视图。它使您能够将设备组织到 租户服务组 (TSG)（用于组织设备的逻辑容器）中，并便于将受支持的产品与您的设备关联。

您可以将 Device Associations 与以下产品一起使用：

- ❑ Strata Cloud Manager
- ❑ AIOps for NGFW
- ❑ IoT Security （企业许可协议）
- ❑ Next-Generation CASB for Prisma Access and NGFW (CASB-X)
- ❑ SaaS Security Inline
- ❑ Strata Logging Service



1. 在 设备关联 （设置 > 设备关联）中，您可以查看与您的客户支持帐户关联的所有租户服务组 (TSG) 的列表。
2. 选择一个 TSG 以查看与其关联的任何防火墙或 Panorama 设备。如果您没有看到任何，您可以从您的客户支持帐户 添加设备。
3. 每当您需要将新设备与您的 TSG 关联时，请添加设备。
4. 在您添加防火墙或 Panorama 设备后，您可以关联产品以开始将设备与您已激活的产品一起使用。该应用程序必须与您设备的硬件型号兼容，否则在应用程序关联期间设备将不会出现。

- 关联设备
- 关联产品
- 移除关联

设备关联（将设备与租户关联）

在您可以开始使用已激活的许可产品的防火墙或 Panorama 设备之前，您必须首先将其与您已激活的租户关联，该租户中您已激活了兼容产品。

STEP 1 | 使用中心或Strata Cloud Manager导航到**Device Associations**。

1. （可选）使用您的 Palo Alto Networks CSP 凭据登录到中心并选择常见服务 > 设备关联。
2. （可选）登录到Strata Cloud Manager并选择设置 > 设备关联。

STEP 2 | 将防火墙或 Panorama 设备添加到您的租户。

1. 选择。

   您的客户支持帐户会根据您所在租户中激活的产品自动选择。如果您没有激活任何支持的产品Device Associations，添加设备将灰显。
2. 选择一个或多个防火墙或 Panorama 设备。

   您可以使用序列号搜索特定设备。
3. 保存。

STEP 3 | 继续将产品与设备关联。

设备关联（将设备与产品关联）

激活受支持产品的许可证后，使用设备关联指定要与产品一起使用的防火墙或 Panorama 设备。

STEP 1 | 激活您的产品许可证。

如何做到这一点取决于您要激活的许可证。有关详细信息，请参阅特定产品文档。您还可以在此处查看与 Strata Cloud Manager 的许可证兼容性。

STEP 2 | 使用中心或Strata Cloud Manager导航到**Device Associations**。

1. （可选）使用您的 Palo Alto Networks CSP 凭据登录到中心并选择常见服务 > 设备关联。
2. （可选）登录到Strata Cloud Manager并选择设置 > 设备关联。

STEP 3 | 将产品与防火墙或 Panorama 设备相关联。

1. 选择关联产品。
2. 在产品选择列中，选择要关联的产品。
3. 如果适用，请选择许可证类型。

   某些产品具有特定有效期条款和设备型号的许可证。只有与您选择的许可证类型兼容的设备才会显示关联。
4. 选择设备。
5. 保存或应用许可。

STEP 4 | 验证关联是否成功。

如果关联失败，请复制错误 ID 并按照步骤打开支持案例。打开支持案例时，请务必包括错误 ID、设备序列号、TSG ID 以及关联失败的产品名称。

STEP 5 | 返回到您所关联产品的文档，以便执行进一步的接入步骤。

设备关联（删除设备关联）

例如，如果您要退出或返回防火墙或 Panorama 设备，或者要将其与其他租户服务组 (TSG) 关联，您可能要删除设备关联。

如果您要尝试将试用许可证转换为生产许可证，请转换许可证，而不是取消关联。

STEP 1 | 使用中心或Strata Cloud Manager导航到**Device Associations**。

1. （可选）使用您的 Palo Alto Networks CSP 凭据登录到中心并选择常见服务 > 设备关联。
2. （可选）登录到Strata Cloud Manager并选择设置 > 设备关联。

STEP 2 | 删除产品关联。

如果要从 TSG 中删除防防火墙或 Panorama 设备，必须先删除任何相关产品。

1. 选择要取消关联的防火墙或 Panorama 设备的产品。
2. 选择删除关联 > 删除产品关联。
3. 选择要删除的产品并删除关联。

STEP 3 | 删除租户关联。

您只能从没有应用程序关联的设备中删除租户关联。如果设备与应用程序关联，请在继续之前删除应用程序关联。

1. 选择要从租户中删除的防火墙或 Panorama 设备。
2. 选择删除关联 > 删除租户关联。
3. 确认要继续并删除。

STEP 4 | 如果要删除防火墙或 Panorama 设备以将其添加到新的 TSG，请将其与新 TSG 关联。

设备型号兼容性

这些是您可以与不同应用程序关联的设备型号。

- AIOps for NGFW 或 Strata Cloud Manager
- CASB-X
- IoT Security
- SaaS Security

AIOps for NGFW 或 Strata Cloud Manager

系列	型号
Panorama 虚拟设备	• PRA-25 • PRA-100 • PRA-1000
VM-SERIES	• VM-200 • VM-300 • VM-500 • VM-600 • VM-700
200	• 220
400	• 410 • 410R • 440 • 445 • 450 • 450R • 460
800	• 820 • 850
3000	• 3220 • 3250 • 3260 • 3410

系列	型号
	• 3420 • 3430 • 3440
5000	• 5220 • 5250 • 5260 • 5280 • 5410 • 5420 • 5430 • 5445 • 5450
7000	• 7050 • 7080

CASB-X

系列	型号
200	• 220
400	• 400 • 410 • 415 • 440 • 445 • 450 • 450R • 460
800	• 820 • 850
1000	• 1410 • 1420

系列	型号
3000	• 3200 • 3220 • 3250 • 3260 • 3410 • 3420 • 3430 • 3440
5000	• 5220 • 5250 • 5260 • 5280 • 5400 • 5420 • 5430 • 5440 • 5445 • 5450
7000	• 7050 • 7080

IoT Security

此表仅包含可与Device Associations中的IoT Security关联的设备型号。该表不包含有关不同设备型号和 PAN-OS 版本组合的IoT Security功能的信息。

系列	型号
VM-SERIES	• VM-100 • VM-300 • VM-500 • VM-700
200	• 200 • 220

系列	型号
	• 220R
400	• 410 • 410R • 440 • 450 • 450R • 460
500	• 500
800	• 820 • 850
3000	• 3020 • 3050 • 3060 • 3220 • 3250 • 3260 • 3410 • 3420 • 3430 • 3440
7000	• 7050 • 7080

SaaS Security

此表仅包含可与Device Associations中的SaaS Security关联的设备型号。该表不包含有关不同设备型号和 PAN-OS 版本组合的SaaS Security功能的信息。

系列	型号
200	• 220 • 220R
400	• 410

系列	型号
	• 410R • 440 • 440R • 450 • 450R • 460 • 460R
800	• 820 • 850
3000	• 3220 • 3250 • 3260 • 3410 • 3420 • 3430 • 3440
5000	• 5220 • 5250 • 5260 • 5280 • 5410 • 5420 • 5430 • 5450
7000	• 7050 • 7080

防火墙和许可证类型兼容性

某些产品订阅具有不同的许可证类型，这使得它们仅与特定类型的防火墙和设备兼容。当您将产品与设备关联并选择您的产品许可证时，仅与许可证类型相对应的设备将会出现。然而，一些许可证类型，如评估、试用和企业许可证协议 (ELA) 与任何防火墙型号兼容。

防火墙类型由防火墙 SKU 定义。要查看防火墙的 SKU，请登录到您的客户支持门户帐户，并选择资产 > 设备，并检查型号名称列中防火墙的序列号条目。这是 SKU，指示防火墙类型如下：

- 产品 SKU 以防火墙型号名称结尾；例如，PAN-PA-410
- 评估 SKU 以 -E60 结尾，代表*评估 + 60天*；例如，PAN-PA-410-E60
- 实验室 SKU 以 -LAB 结尾；例如，PAN-PA-410-LAB

请参见下方您的应用程序支持的防火墙和许可证类型组合。

- #unique_38
- AIOps for NGFW
- IoT Security
- SaaS Security Inline

AIOps for NGFW

AIOps for NGFW许可证类型	防火墙类型			
	NFR	LAB	PROD	EVAL
TRIAL	否	是	是	是
EVAL	否	是	是	是
NFR	是	否	否	否
LAB	否	是	否	否
PROD	否	否	是	否

IoT Security

IoT Security许可证类型	防火墙类型			
	NFR	LAB	PROD	EVAL
TRIAL	否	是	是	是
EVAL	否	是	是	是
NFR	是	否	否	否

IoT Security许可证类型	防火墙类型			
	NFR	LAB	PROD	EVAL
LAB	否	是	否	否
PROD	否	否	是	否

SaaS Security Inline

SaaS Security Inline许可证类型	防火墙类型			
	NFR	LAB	PROD	EVAL
TRIAL	否	是	是	是
EVAL	否	是	是	是
NFR	是	否	否	否
LAB	否	是	否	否
PROD	否	否	是	否