paloalto
TECHDOCS

Strata Cloud Manager 入门

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

February 5, 2025

Table of Contents

Strata Cloud Manager 简介

在何处可以使用？	需要提供什么？
• NGFW，包括由 软件 NGFW 积分提供资助的项目 • Prisma Access (Managed by Panorama or Strata Cloud Manager) • Prisma SD-WAN	这些许可证均包含对 Strata Cloud Manager 的访问权限： ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Prisma SD-WAN ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → 您可用的特性和功能Strata Cloud Manager取决于您使用的许可证。

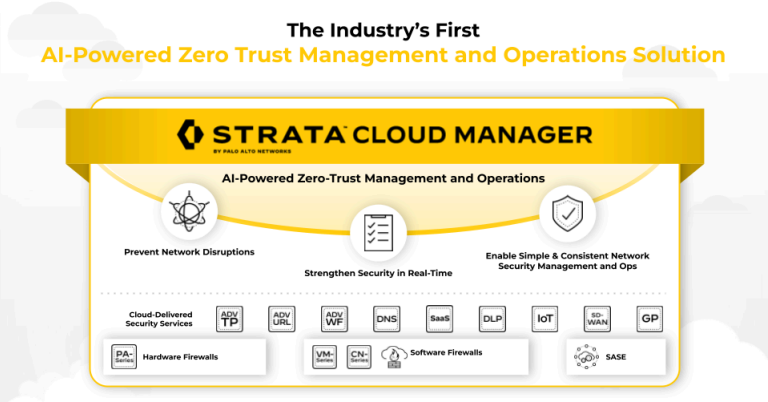
Palo Alto Networks Strata Cloud Manager 为您提供由 AI 驱动的整个网络安全部署的统一管理和运营。使用 Strata Cloud Manager，您可以通过单一、简化的用户界面轻松管理整个 Palo Alto Networks 网络安全基础设施 - 您的 NGFW 和 SASE 环境。全面了解所有网络安全实施点的用户、分支站点、应用程序和威胁；这为您提供可操作的见解、更好的安全性以及轻松的故障排除和问题解决。

- ❑ 预测并预防网络中断

  Strata Cloud Manager 预测和防止网络中断并快速补救问题，以便您和您的用户能够继续日常业务并保持高效。
- ❑ 利用实时最佳实践增强安全性

  Strata Cloud Manager 识别重要且未充分利用的安全功能，并指导您根据符合您需求的最佳实践启用它们。利 内置的最佳实践和由 AIOps 提供支持的内联补救功能来加强您的安全态势。
- ❑ 简单一致的网络安全管理和操作

  Strata Cloud Manager 整合了您的安全工具，以改善操作和洞察力，从而您可以为整个网络安全堆栈采用简单而一致的管理体验。



Strata Cloud Manager 如何增强安全性

最大限度地利用安全功能

- 查看您正在使用的安全功能，并确定您可以利用的安全功能采用方面的差距。→ 功能采用
- 查看您的安全服务订阅的采用率。→ CDSS 采用率
- 了解您的安全功能如何遵循最佳实践，或者您可以在哪些方面进行改进以加强您的安全态势。→ 内置最佳实践

加强和优化现有配置

根据使用数据和自动生成的建议清理并简化您的安全策略。

- 清理策略中未引用的对象以及没有任何流量命中的规则；这些对象和规则可能会阻碍性能并使策略管理复杂化。→ 配置清理
- 过于宽泛的规则会带来安全漏洞，因为它们允许网络中未使用的应用程序。策略优化器可让您将这些过于宽松的规则转换为更具体、更集中的规则，仅允许您实际使用的应用程序。→ 策略优化器

安全配置实时指导

- 最佳实践护栏为您提供实时验证，确保您的安全策略规则符合最佳实践。→ 实时、内联最佳实践配置检查

Strata Cloud Manager 如何预测和预防网络中断

全面的可观察性

- 了解安全基础设施如何保障您的网络安全。→ 命令中心
- 了解用户、分支站点、应用程序和 IT 基础设施的运行状况和性能，从单一指示板。→SASE 运行状况指示板
- 通过单个指示板了解设备的运行状况和性能。→ 设备运行状况指示板

预测运行状况并修复中断

自动预测可防止潜在的中断；当检测到问题时，可操作的见解可加快解决问题。

- 机器辅助预测即将发生的停电事件，并提供补救措施建议。→ 预测和异常检测
- 通过可能原因分析减少解决时间。→ 查看可能原因

规划不断变化的安全需求

- 通过主动识别潜在容量来提高稳定性。→ 容量分析器

Strata Cloud Manager 如何随时随地持续工作

一致的配置

通过简化的流程在所有实施点应用一致的策略，并且无需对 NGFW 和 SASE 部署进行单独更改。

- 设置并加入 NGFW 和 Prisma Access 移动用户和远程网络，并规划 NGFW 的软件升级。→ Strata Cloud Manager 中的工作流程
- 配置在您的 NGFW 和 Prisma Access 之间共享的安全策略。→ NGFW 和 Prisma Access 的共享管理

灵活的配置组织

通过简单的文件夹和设备管理工作流程简化大规模配置管理。

- 在整个环境中全局应用配置设置并实施策略，或将设置和策略定位到组织的某些部分。→ 配置范围
- 逻辑地对防火墙或部署类型（Prisma Access 移动用户、远程网络或服务连接）进行分组，以简化配置管理。→ 文件夹管理
- 群组配置，您可以快速推送到防火墙或部署。→ 代码段
- 您可以灵活地适应特定于设备或部署的唯一配置值。→ 变量

实现对威胁的统一可见性

- 全面了解您的网络流量、订阅、用户、应用程序、网络、威胁等。→ 监控
- 获取网络中运行的应用程序、ION 设备、威胁、用户和安全订阅的交互式视图。指示板可让您了解部署中的运行状况、安全状况和活动，帮助您预防或解决网络中的性能和安全漏洞。→ 指示板
- 获取有关网络流量模式、带宽利用率、安全订阅数据等的报告。报告提供有关您的网络的可行见解，您可以将其用于规划和监控目的。→ 报告

Strata Cloud Manager 支持的产品

在何处可以使用？	需要提供什么？
• NGFW，包括由 软件 NGFW 积分提供资助的项目 • Prisma Access (Managed by Panorama or Strata Cloud Manager) • Prisma SD-WAN	这些许可证均包含对 Strata Cloud Manager 的访问权限： ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Prisma SD-WAN ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → 您可用的特性和功能Strata Cloud Manager取决于您使用的许可证。

Strata Cloud Manager 为您的 NGFW 和 SASE 网络提供 AI 驱动的统一管理和运营，以及 Strata Cloud Manager 根据您的许可证为您提供的功能。以下是允许 Strata Cloud Manager 管理 NGFW 和 SASE，以及解锁 Strata Cloud Manager 网络安全功能的许可证。→ 下面介绍如何验证您的许可证

表 **1:**

Strata Cloud Manager 基础版	Strata Cloud Manager Essentials 提供管理和安全功能，这些功能可免费使用： • 新一代防火墙 (NGFW) • Prisma Access Strata Logging Service 是 Strata Cloud Manager Essentials 的可选附加组件。 *Strata Cloud Manager Essentials* 和 *Strata Cloud Manager Pro* 可以在没有以下功能的客户支持门户 *(CSP)* 帐户中激活：具有指定存储的 *Strata Logging Service* 服务、*AIOps for NGFW* 免费版/高级版或 *Prisma Access*。
Strata Cloud Manager Pro	Strata Cloud Manager Pro 是付费套餐，包含 Strata Cloud Manager Essentials 的所有功能，以及用于增强运营运行状况、防止网络中断、加强实时安全态势和用于监控用户体验性能的自主数字体验管理 (ADEM) 的高级功能。Strata Cloud Manager Pro 包括 Strata Logging Service，具有一年的日志保留和无限的

	存储空间，可在整个部署中实现集中日志记录和无缝数据检索。您可以购买以下产品的 Strata Cloud Manager Pro： • 新一代防火墙 (NGFW) • VM Series 由 Software NGFW Credits 资助 • Prisma Access
适用于 **NGFW Premium** 的 **AIOps**	对于拥有 AIOps for NGFW Premium 许可证的 NGFW，Strata Cloud Manager 可让您全面了解 NGFW 的运行状况和安全性，并可以实施主动检查以弥补安全漏洞。 • **NGFW (Managed by PAN-OS or Panorama)** → 对于具有 AIOps for NGFW Premium 许可证的 PAN-OS 和 Panorama 托管 NGFW，请使用 Strata Cloud Manager 监督您的部署运行状况和安全态势。 • **NGFW (Managed by Strata Cloud Manager)** → 凭借 AIOps for NGFW 许可证，您还可以使用 Strata Cloud Manager 来进行 **NGFW** 的云管理。 • 联系您的客户团队，使用 *Strata Cloud Manager* 来启用 Cloud Management for NGFW。 • *Strata Cloud Manager* 仅为使用 *AIOps for NGFW Premium* 许可证的 *NGFW* 提供统一的管理和操作。继续使用 AIOps for NGFW 免费版应用程序为已加入 *AIOps for NGFW Free* 的 *NGFW* 提供服务。
软件 **NGFW** 积分	对于使用软件 NGFW 积分赞助的 VM-Series，Strata Cloud Manager 支持 NGFW Premium 功能的 AIOps，包括 NGFW 的云管理。
Prisma Access	您可以通过两种方式管理 Prisma Access：使用 Strata Cloud Manager 或 Panorama。Strata Cloud Manager 为 Prisma Access 提供可见性功能，无论您使用哪种管理界面，这些功能都受支持。这意味着，如果您使用 Panorama 管理 Prisma Access，仍然可以使用 Strata Cloud Manager 来全面监控 Prisma Access 环境。 **Prisma Access (Managed by Strata Cloud Manager)** 使用 Strata Cloud Manager 来全面载入、管理和监控您的 Prisma Access 环境。 这包括使用 Strata Cloud Manager 管理和监控 Prisma Access 附带的云交付安全服务。

	Strata Cloud Manager 为您提供对 Prisma Access 环境的全面监控、警报和可见性： • 人工智能驱动的自主 DEM • 在 Strata Cloud Manager 中监控 Prisma Access • Strata Cloud Manager 指示板 • Strata Cloud Manager 监控 • Strata Cloud Manager 报告 **Prisma Access (Managed by Panorama)** 如果您使用 Panorama 管理 Prisma Access，则必须继续使用 Panorama 管理您的环境。不过，您可以使用 Strata Cloud Manager 为您的 Prisma Access 环境提供全面监控、警报和可视性： • 人工智能驱动的自主 DEM • 在 Strata Cloud Manager 中监控 Prisma Access • Strata Cloud Manager 指示板 • Strata Cloud Manager 监控 • Strata Cloud Manager 报告
人工智能驱动的 **ADEM**	驱动的 ADEM 是 Prisma Access 附加许可证，可自动执行复杂的 IT 操作，从而提高生产力并缩短解决问题的时间。Strata Cloud Manager 为所有 Prisma Access 用户（Panorama - Managed Prisma Access 和 Prisma Access Cloud Management）提供人工智能驱动的 ADEM 支持。 如果您使用 *Panorama* 管理 *Prisma Access*，则必须继续使用 *Panorama* 管理您的环境，并且可以使用 *Strata Cloud Manager* 进行 *ADEM* 监控。
Prisma SD-WAN	使用 Strata Cloud Manager 来管理 Prisma SD-WAN。Prisma SD-WAN 是一种云交付服务，可实现应用程序定义的自主 SD-WAN，帮助您保护和连接您的分支机构、数据中心和大型校园站点，而不会增加成本和复杂性。AppFabric 通过应用程序感知安全地连接您的站点，并让您可以自由地使用任何 WAN、任何云来实现薄分支（来自云端的安全性）解决方案。
云交付安全服务 **(CDSS)**： • 高级威胁防护 • 高级 **URL** 筛选 • **Advanced WildFire** • **DNS** 安全 • 企业 **DLP**	如果您拥有 Prisma Access 或 AIOps for NGFW Premium 许可证，则可以使用 Strata Cloud Manager 管理和监控您的安全订阅。Strata Cloud Manager 为您的企业流量提供一致的安全订阅保护。 Strata Cloud Manager 功能为安全订阅提供的功能取决于您的许可证，可能包括： • Strata Cloud Manager 为安全订阅提供指示板和报告

• **IoT Security** • **SaaS Security**	• Strata Cloud Manager 为安全订阅提供统一管理。如果您使用 Strata Cloud Manager 来在 NGFW 和/或 Prisma Access 之间实施共享安全策略，您可以对安全订阅使用单一的集中式配置。

Strata Cloud Manager 的基本界面

在何处可以使用？	需要提供什么？
• NGFW，包括由 软件 NGFW 积分提供资助的项目 • Prisma Access (Managed by Panorama or Strata Cloud Manager) • Prisma SD-WAN	这些许可证均包含对 Strata Cloud Manager 的访问权限： ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Prisma SD-WAN ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → 您可用的特性和功能Strata Cloud Manager取决于您使用的许可证。

以下是 Strata Cloud Manager 的基本界面。Strata Cloud Manager 用户界面提供了网络的全面视图，并为您提供了管理 NGFW 和 SASE 的统一工作流程。通过新的简化和一致的导航来与您的所有网络数据进行交互，获得自动为您呈现的可操作见解，并共同管理和监控 Prisma Access、您的 NGFW 和云交付的安全服务。

浏览左侧导航栏上的每个菜单 – 这些路径现在是您通过 Strata Cloud Manager 使用任何 Palo Alto Networks 产品或订阅的标准路径。这样很方便：

- 采用新功能和订阅
- 加入新用户、设备、站点或位置

因为它们将直接插入您现有的管理设置中。

重要信息

Strata Cloud Manager 中提供的功能取决于您的订阅。您可以查看 *Strata Cloud Manager* 文档，了解 *Strata Cloud Manager* 功能的许可证要求。

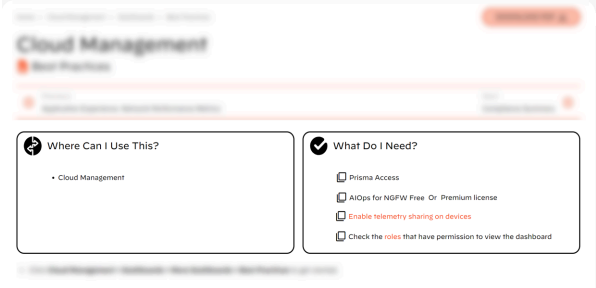
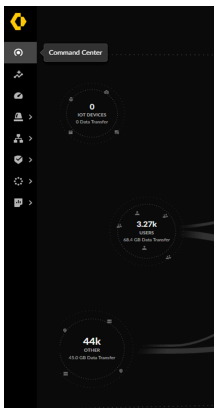
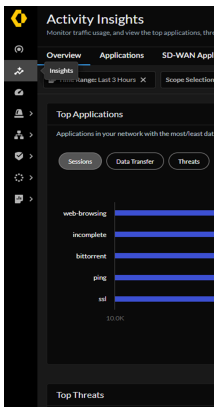
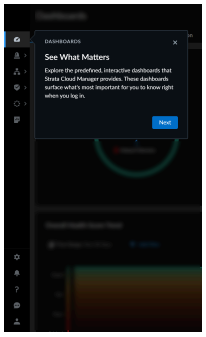
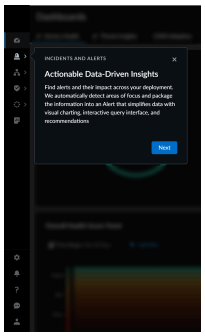
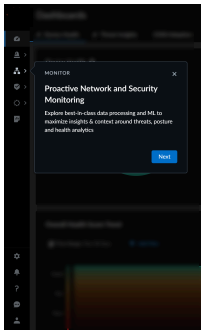
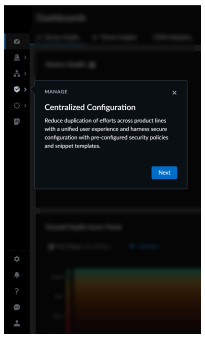
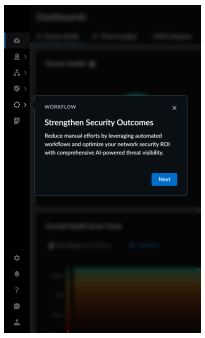
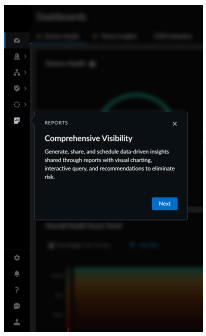
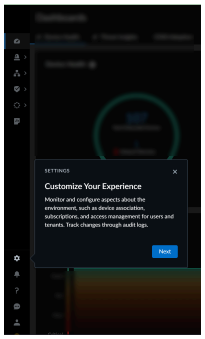


表 **2:**

命令中心	评估网络运行状况、安全性和效率的第一个位置 命令中心是您的网络和安全基础设施的可视化概览。它为您提供了四种不同的视图，每种视图都有自己的跟踪数据、指标和可操作的见解，供您检查和交互。 • 命令中心：Strata Cloud Manager	
Activity Insights	统一的网络数据，全部集中在一个位置 Activity Insights 可让您深入了解 Prisma Access 和 NGFW 部署中的网络活动。Activity Insights 将您的网络数据（如网络流量、应用程序使用情况、威胁和用户活动）统一在一个位置。 • 见解：Activity Insights	
指示板	立即了解重要内容 指示板显示您登录时需要了解的最重要的内容。每个指示板都旨在突出显示您可以采取措施以改善安全状况或网络运行状况的领域。 探索提供的所有预定义的交互式指示板，您可以固定您的收藏夹。 • 指示板：Strata Cloud Manager	
事件和警报	可操作的数据驱动型洞察 Strata Cloud Manager 提供统一的事件和警报框架。在一个位置，查看、调查和解决网络上的警报和事件，并跳转到日志以检查关联的活动。 • 事件和警报：Strata Cloud Manager	

监视	主动网络和安全监控 监控网络上所有内容的运行状况和安全性，并使用 IoC 搜索调查网络上构件文件的历史记录并查看 Global Analysis 结果。根据您使用的订阅和产品，您可以监视： • NGFW 设备 • Prisma Access • 应用程序 • 用户 • 分支站点 • 数据中心 • 网络服务（如 GlobalProtect 和 DNS） • Palo Alto Networks 订阅 • Prisma Access 位置 • Prisma SD-WAN • 资产	
管理	集中配置 管理跨网络安全产品和订阅的共享策略；第一天，您可以从基于预定义的最佳实践策略和设置以及内联最佳实践检查的安全配置开始。 • 管理：NGFW 和 Prisma Access • 管理：IoT 策略建议 • 管理：企业 DLP • 管理：SaaS Security	
工作流	加强安全成果 当您首次进入工作流程时，探索指示板会立即显示您可以采取的关键和建议的操作，以改善安全状况或优化配置管理。继续在此处设置和注册 NGFW 和 Prisma Access 移动用户和远程网络，并规划 NGFW 的软件升级。 • 设置 Prisma Access • 设置 NGFW	

	• 软件升级规划工具 (AIOps for NGFW)	
报告	全面可见性 生成、共享和安排数据驱动型洞察，通过具有可视化图表、交互式查询和建议的报告共享，以消除风险。 • 报告：Strata Cloud Manager	
设置	加入和激活设置 这些是您在添加新用户、许可证或管理员时，以及在开始使用 Strata Cloud Manager 时会回来查看的设置： • 订阅 • 租户 • 设备关联 • 身份和访问权限 • 审核日志	

启动 Strata Cloud Manager

在何处可以使用？	需要提供什么？
• NGFW，包括由 软件 NGFW 积分提供资助的项目 • Prisma Access (Managed by Panorama or Strata Cloud Manager) • Prisma SD-WAN	这些许可证均包含对 Strata Cloud Manager 的访问权限： ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Prisma SD-WAN ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → 您可用的特性和功能Strata Cloud Manager取决于您使用的许可证。

Strata Cloud Manager 应用程序可在 Palo Alto Networks 中心使用，您可以直接通过 stratacloudmanager.paloaltonetworks.com 访问它。

Prisma Access 许可证、AIOps for NGFW Premium 许可证或 Prisma SD-WAN 许可证是以下产品的基本要求：Strata Cloud Manager 统一管理和运营。如果您至少拥有其中一个许可证，可以访问 Strata Cloud Manager 来查看或管理您的产品。

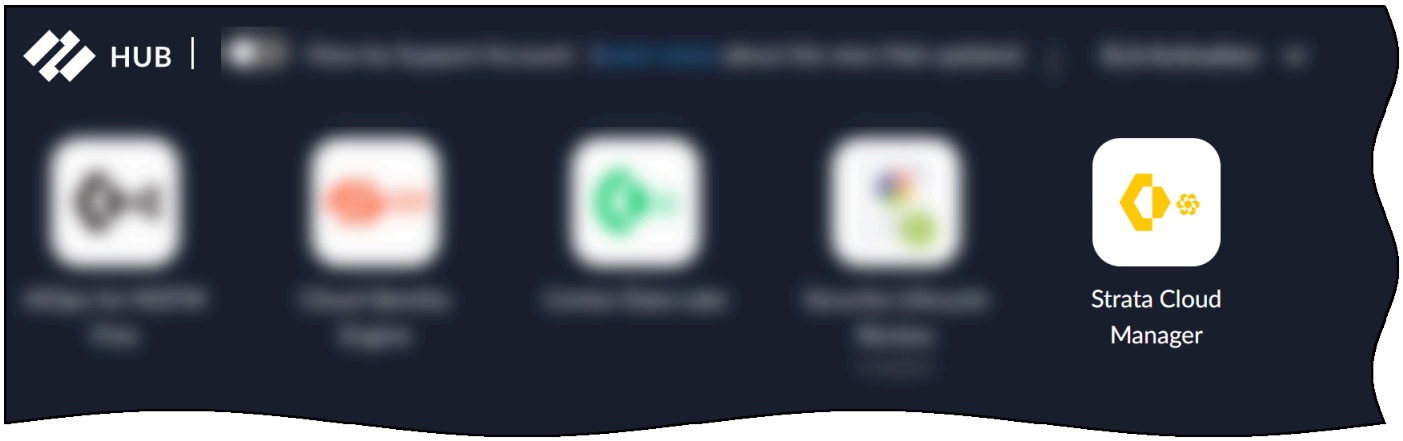
如果您拥有多个此类许可证，Strata Cloud Manager 为您提供与这些产品交互的单一界面，以及额外的许可证或附加订阅（如 Palo Alto Networks 安全订阅）。→ 查看支持的产品和许可证*Strata Cloud Manager* 统一管理和运营

启动或访问 **Strata Cloud Manager**：

- 如果您在 2023 年 10 月或之后首次使用 Prisma Access、AIOps for NGFW Premium 或 Prisma SD-WAN，请参阅如何首次启动 Strata Cloud Manager
- 如果您之前使用中心上的独立应用来管理产品，请参阅从专用产品应用程序迁移至 Strata Cloud Manager

首次启动 Strata Cloud Manager

激活 Prisma Access、AIOps for NGFW Premium 或 Prisma SD-WAN 许可证后，Strata Cloud Manager 应用程序将在 Palo Alto Networks 中心提供给您，或者您可以直接通过 stratacloudmanager.paloaltonetworks.com 访问它。



启动应用程序并Strata Cloud Manager 的基本界面。继续加入您的产品：

- 开始使用 AIOps for NGFW Premium，包括 Cloud Management for NGFW
- 开始使用 Prisma Access
- 开始使用 Prisma SD-WAN

从专用产品应用程序迁移至 Strata Cloud Manager

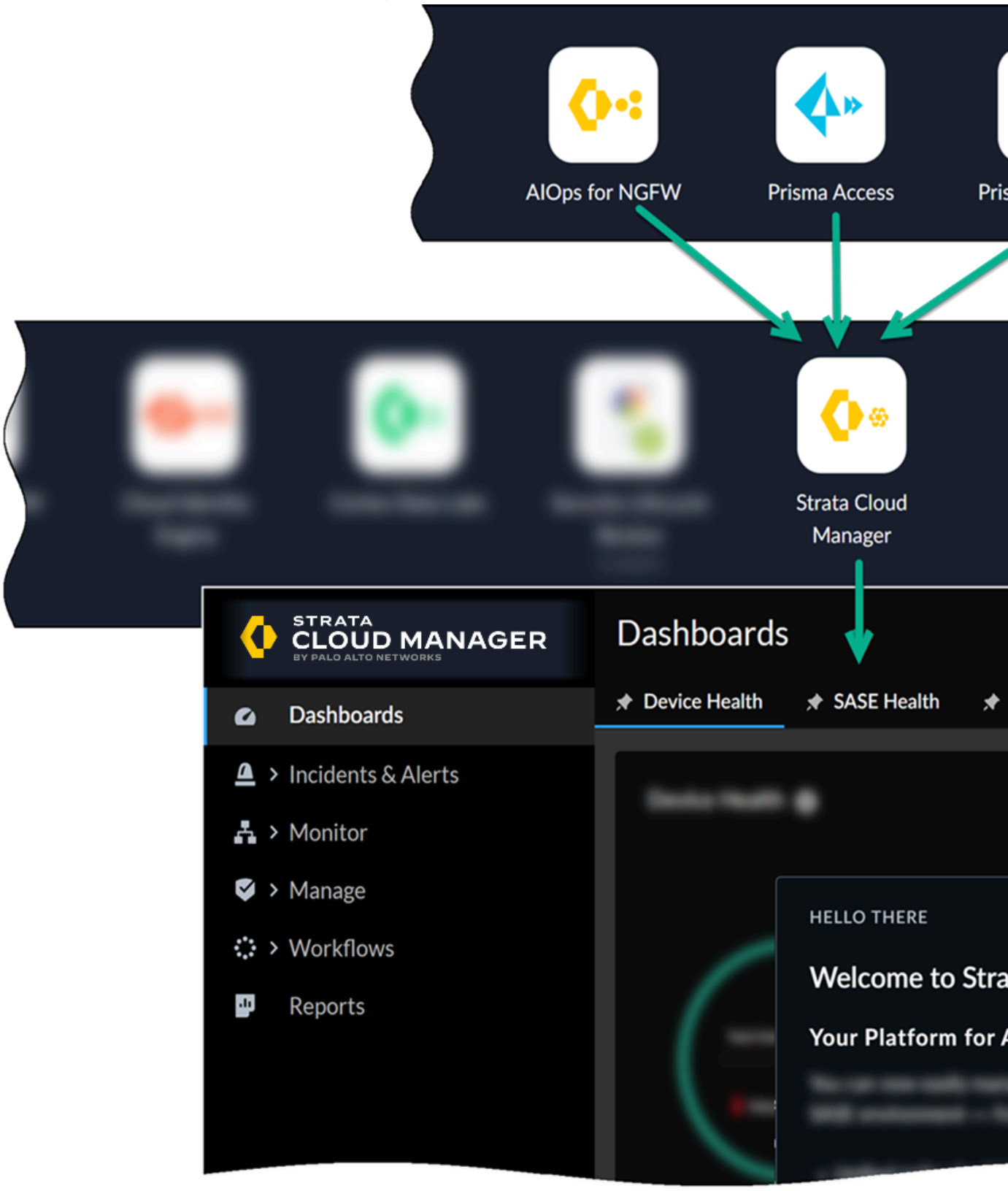
重要信息

这仅适用于您之前使用独立应用程序来管理或与您的产品交互的情况：*Prisma Access* 应用程序、*AIOps for NGFW Premium* 应用程序或 *Prisma SD-WAN* 应用程序。这些应用程序已更新（或即将更新），以便为您提供 *Strata Cloud Manager* 的统一管理和运营。

从专用产品应用程序迁移至 **Strata Cloud Manager**：

- Strata Cloud Manager 根据许可证支持提供统一的管理和操作 — 以下是您可以使用 Strata Cloud Manager 监控或管理的产品。
- 产品内通知会提前告知您即将推出的更新，以便为您提供 Strata Cloud Manager。
- 更新是无缝的，不会影响您的数据、警报或资产。

- 更新完成后，您将登录中心上的 Strata Cloud Manager 应用程序；您将不再在中心上使用 Prisma Access、NGFW Premium 的 AIOps 或 Prisma SD-WAN 的单独应用程序。



- 您的产品应用程序会自动将您重定向到 stratacloudmanager.paloaltonetworks.com。这是 Strata Cloud Manager URL。

  如果您之前使用多个正在为 *Strata Cloud Manager* 更新的产品应用程序，则更新后的产品应用程序将全部重定向到同一个 *Strata Cloud Manager* 实例。
- Strata Cloud Manager 为您提供跨网络安全产品通用的全新导航。首先了解一下 Strata Cloud Manager 并探索新的导航体验和功能。
- 在新的统一管理界面中查找您的产品功能：
  - AIOps for NGFW：我的功能在 Strata Cloud Manager 中的哪里？
  - Prisma SD-WAN：我的功能在 Strata Cloud Manager 中的哪里？
  - Prisma Access 见解：我的功能在 Strata Cloud Manager 中的哪里？
  - Prisma Access：我的功能在 Strata Cloud 管理器中的哪里？

Strata Cloud Manager 入门

在何处可以使用？	需要提供什么？
• NGFW，包括由 软件 NGFW 积分提供资助的项目 • Prisma Access (Managed by Panorama or Strata Cloud Manager) • Prisma SD-WAN	这些许可证均包含对 Strata Cloud Manager 的访问权限： ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Prisma SD-WAN ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → 您可用的特性和功能Strata Cloud Manager取决于您使用的许可证。

Strata Cloud Manager 为您的 NGFW 和 SASE 网络提供人工智能支持的统一管理和运营。下面是首次使用 Strata Cloud Manager 时的速查表。

如果您计划使用 Strata Cloud Manager 加入和管理 Prisma Access、NGFW（需要 AIOps for NGFW Premium），或同时加入和管理这两者，其中将包括开始使用 Prisma Access 和 NGFW 的共享管理 所需要了解的信息

❑ （在中心内）激活您的许可证购买许可证

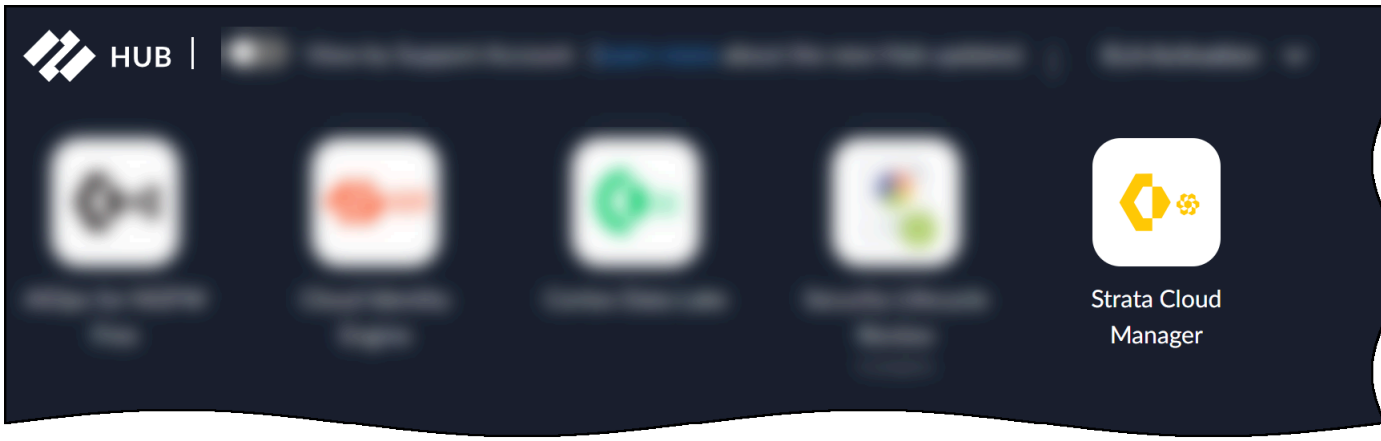
后，您将收到一封包含激活链接的电子邮件。该链接可在中心内启动引导工作流；请按照您要激活的每个许可证的激活工作流操作：

- AIOps for NGFW Premium 许可证
- 激活 Prisma Access 许可证
- Prisma SD-WAN

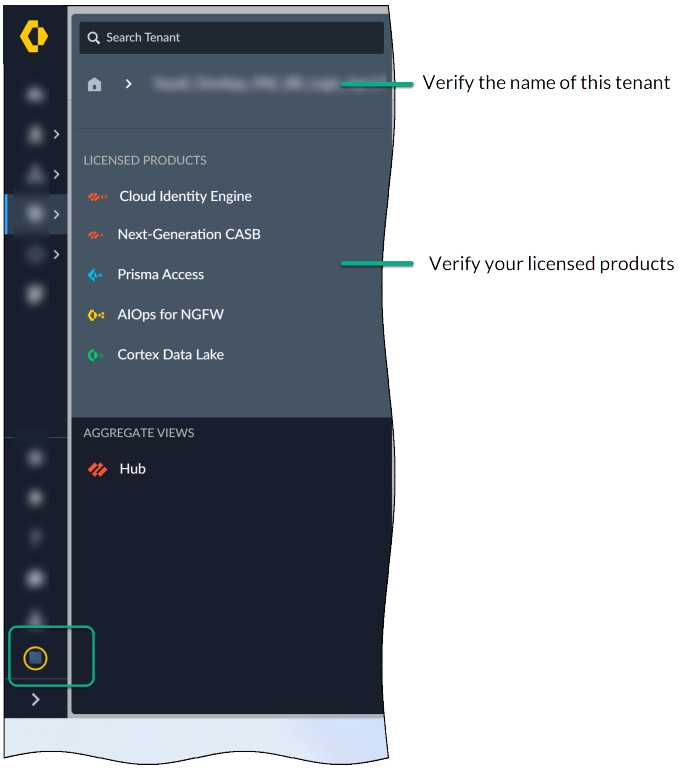
激活这些许可证中的任何一个即可启用 Strata Cloud Manager。激活这些许可证中的至少一个后，继续激活任何其他许可证或附加组件订阅。

- 启动 **Strata Cloud Manager**

  在激活 Prisma Access、AIOps for NGFW Premium 或 Prisma SD-WAN 许可证后，Strata Cloud Manager 应用程序将可在 Palo Alto Networks 中心上供您使用，您也可以直接访问 stratacloudmanager.paloaltonetworks.com。

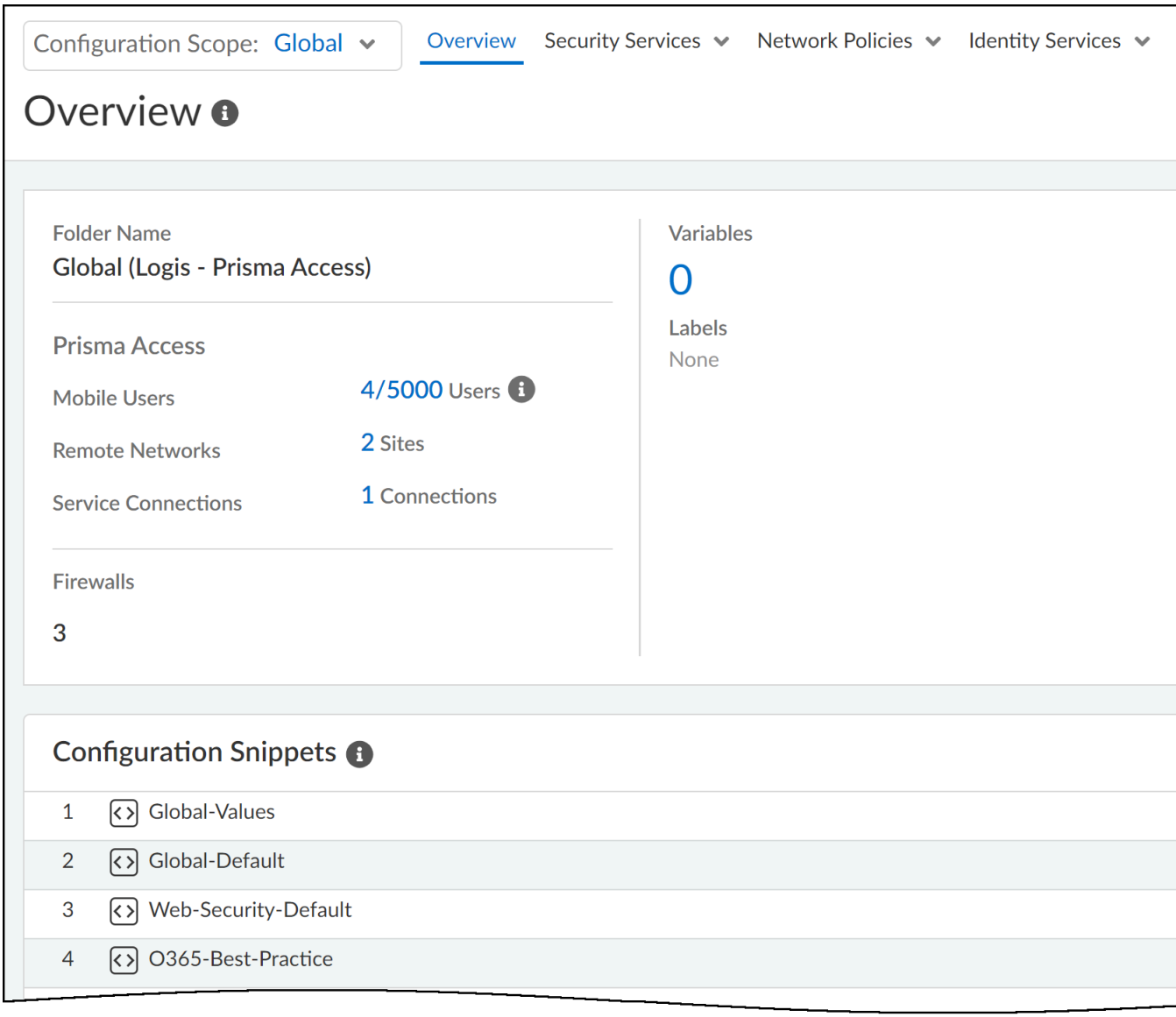


- 验证许可证
  - 在导航菜单底部，选择您的租户详细信息，并验证您使用的租户名称以及您的许可产品。此处详细介绍租户和订阅管理。



  - 转到 **Manage**（管理） > **Configuration**（配置） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**），检查 Prisma Access 许可证状态和详细信息，并查看可能提供的其他详细信息。

    您可能尚未加入 *NGFW*，或者仍在预配 *Prisma Access* 环境，因而此处显式的数据不多。如果是这样，请在完成此处的其余步骤之后尽快回来查看。



- 使用 **Strata Cloud Manager** 进行监控和查看
  - 使用命令中心探索网络和安全基础架构的可视化界面。
  - 查看 Activity Insights 中的重要网络数据。
  - 浏览可用的Strata Cloud Manager指示板。许多指示板还支持报告，您可以安排或与利益相关者共享。
  - 监控您的 Prisma Access 环境、Prisma SD-WAN 和 NGFW。
  - 跨 Prisma Access、NGFW 和 Prisma SD-WAN 查看您的事件和警报。
- 内联最佳实践建议和工作流

  详细了解直接内置于 Strata Cloud Manager 中的最佳实践指导和自动化。

- **Strata Cloud Manager** 加入设置

  Strata Cloud Manager 将通用服务集中在 **Settings**（设置）菜单中。转到 **Settings**（设置）来管理：

  - 角色和权限 — 了解有关 Strata Cloud Manager 上可用的角色和相关权限的详细信息。
  - 设备关联 — 将支持的云应用程序与您的设备相关联。
  - 租户管理 — 创建和管理由租户代表的业务组织和单位的层次结构。

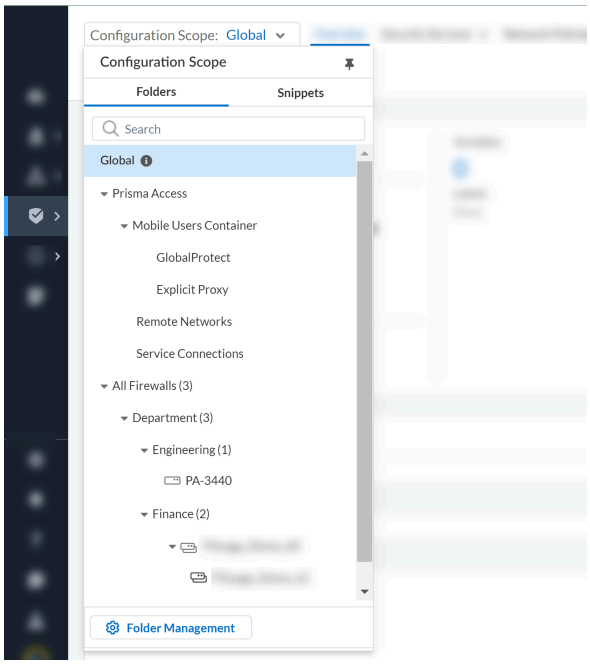
Prisma Access 和 NGFW 的共享管理

对于 Prisma Access 和 NGFW，Strata Cloud Manager 提供共享管理；加入 NGFW 和 Prisma Access 用户、远程网络以及到 Strata Cloud Manager 的服务连接，并实施共同的安全策略。

- 将 **NGFW** 和 **Prisma Access** 加入 **Strata Cloud Manager**
  - 设置 Prisma Access 并加入移动用户、远程网络和服务连接：
    - 设置 Prisma Access 服务基础设施
    - 设置 Prisma Access 移动用户，包括 GlobalProtect 和显式代理连接
    - 设置 Prisma Access 远程网络
    - 设置 Prisma Access 服务连接
  - 加入和设置 NGFW：
    - 加入和设置 NGFW Cloud Management

组织您的配置

处理 Strata Cloud Manager 配置设置时，当前 管理：配置范围 始终对您可见，您可以切换视图以管理更广泛或更精细的配置。配置范围使您能够全局应用策略，或者为某些 NGFW 或 Prisma Access 部署提供有针对性的实施。



下面是有关如何开始组织 Strata Cloud Manager 配置的详细信息：

- 工作流程：文件夹管理

  使用文件夹对 NGFW 进行逻辑分组，以简化配置管理。Prisma Access 文件夹是根据部署类型预定义的。您还可以在文件夹级别启用 Web Security（为管理 Internet 和 SaaS 应用程序访问的管理员提供简化的管理体验）。

- 管理：代码段

  使用代码段对配置进行分组，您可以将其快速推送到 NGFW 或 Prisma Access 部署中。

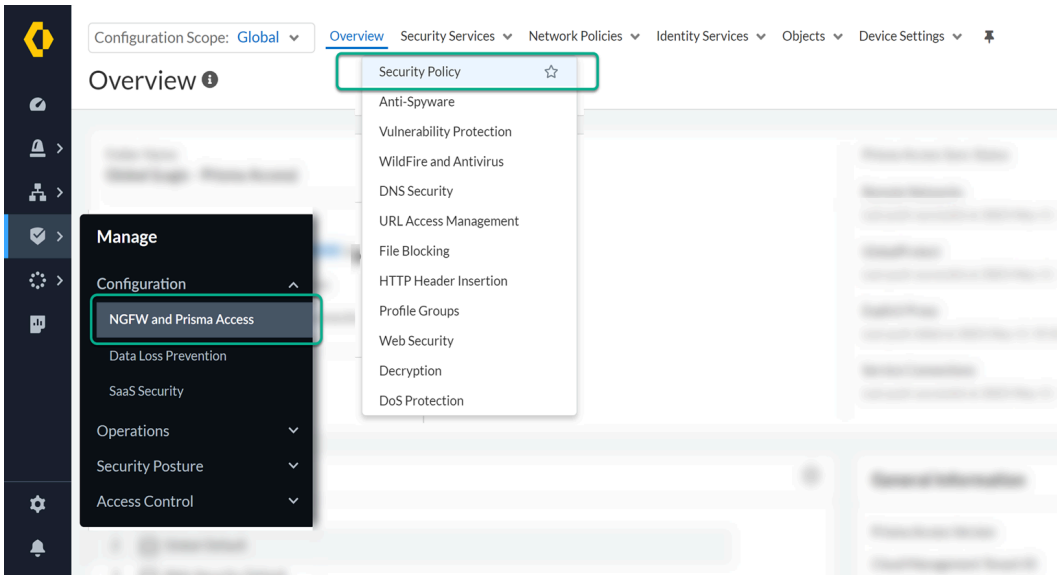
- 管理：变量

  使用配置变量来适应设备或部署特定的配置对象。

- **NGFW** 和 **Prisma Access** 的共享安全策略

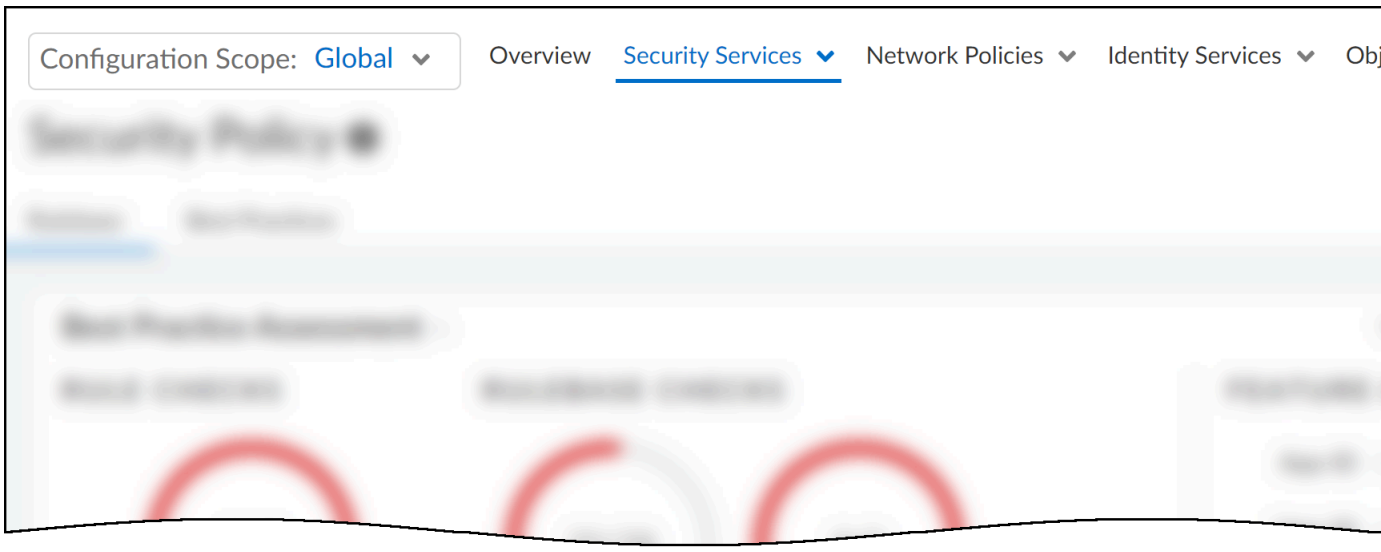
  Strata Cloud Manager 为您提供了 Prisma Access 和 NGFW 的统一管理。您的 Strata Cloud Manager vsecurity 策略是共享的，您可以跨 Prisma Access 和 NGFW 全局应用该策略，或者将特定设置定向到 Prisma Access 部署或特定防火墙组。

  转到 **Manage**（管理） > **Configuration**（配置） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**）以开始。



- 将配置更改推送到 **NGFW** 和 **Prisma Access**

  管理 Strata Cloud Manager 配置时，选择 **Push Config**（推送配置），将配置更改推送到您的 NGFW 和 Prisma Access：



  系统会提示您根据文件夹设置配置推送的范围。下面是更多关于如何执行以下操作的内容：

  - 推送配置更改
  - 查看配置推送的状态
  - 了解如何清理配置

Strata Cloud Manager 内置最佳实践

在何处可以使用？	需要提供什么？
• NGFW，包括由 软件 NGFW 积分提供资助的项目 • Prisma Access (Managed by Panorama or Strata Cloud Manager) • Prisma SD-WAN	这些许可证均包含对 Strata Cloud Manager 的访问权限： ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Prisma SD-WAN ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → 您可用的特性和功能Strata Cloud Manager取决于您使用的许可证。

Palo Alto Networks 最佳实践旨在通过简化检查网络基础设施合规性的流程来帮助您获得最安全的网络。我们已将最佳实践检查直接构建在 Strata Cloud Manager 中，以便您可以获得对配置的实时评估。通过遵循最佳实践来加强您的安全态势。您可以利用 Strata Cloud Manager，根据最佳实践评估您的 Panorama、NGFW 和 Panorama Managed Prisma Access 安全配置并修正未通过的最佳实践检查。

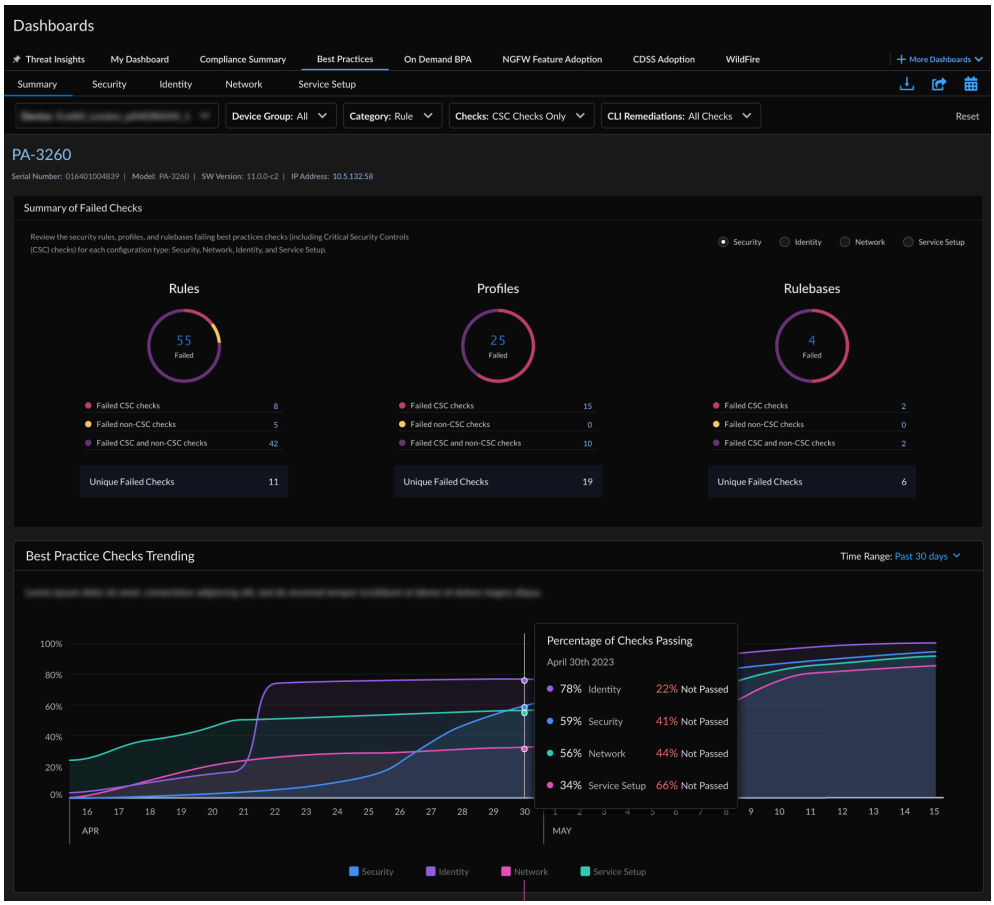
最佳实践指导旨在帮助您增强安全态势，同时帮助您有效地管理环境并最大限度地提高用户的工作效率。不断根据这些内联检查评估您的配置 - 当您看到改善安全性的机会时，请立即采取行动。

了解最佳实践的采用和合规性

首先，您可以通过检查以下态势 **Dashboards**（指示板）来快速评估您的整体安全态势。

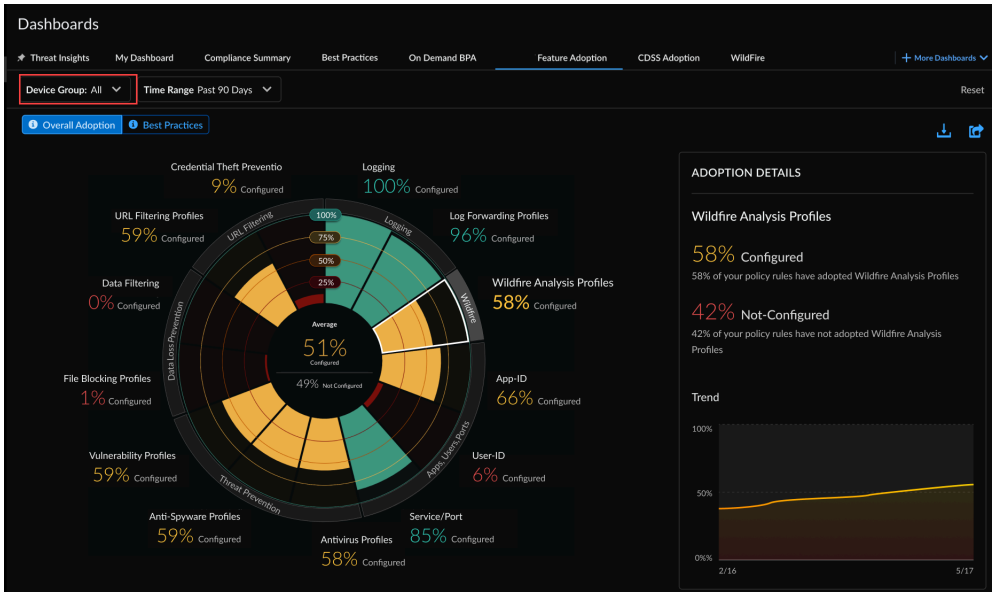
了解您在高层次上的表现，并找出您可能想要开始采取行动的方面。

- 对于每日最佳实践报告及其与互联网安全中心关键安全控制 (CSC) 检查的映射，请检查 指示板 最佳实践 指示板，以帮助您确定可以进行更改来提高最佳实践合规性的方面。以 PDF 格式共享最佳实践报告，并安排定期将其发送到您的收件箱。

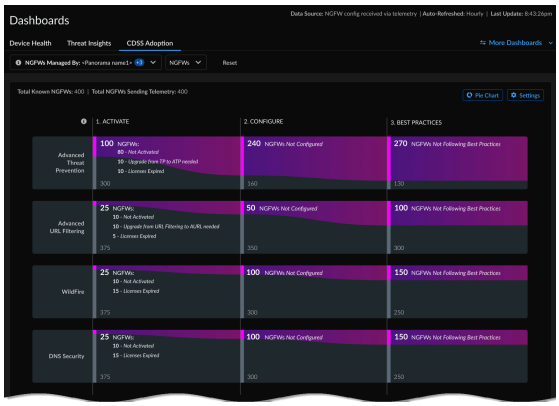


- 要查看过去 12 个月内安全检查更改的历史记录，请检查合规性摘要 指示板，这些更改由互联网安全中心 (CIS) 和国家标准与技术研究所 (NIST) 框架进行分组。

- 监视 指示板功能采用 并随时了解您在部署中使用的安全功能以及潜在的覆盖差距。

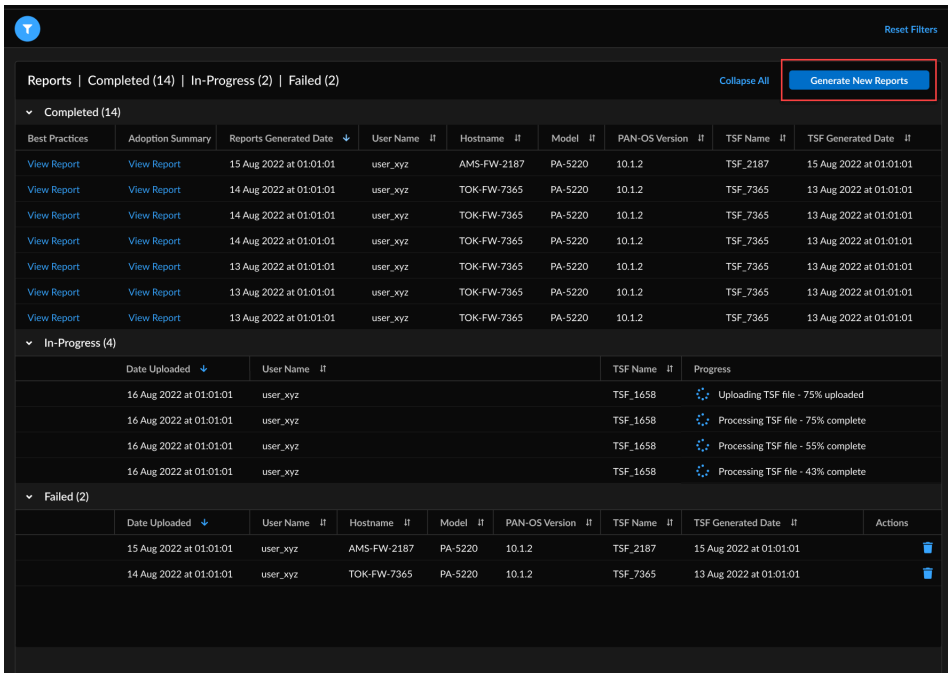


- 监视 指示板CDSS 采用 - 查看设备中的安全服务或功能订阅及其许可证使用情况，以识别安全漏洞并加强企业的安全态势。



- 通过 指示板安全态势洞察，根据已载入 NGFW 设备的安全态势，了解部署的安全状态和趋势，并在发生事件或需要仔细检查安全设置时发出警报。

- 为运行 9.1 及更高版本（非遥测）的 PAN-OS 设备生成 BPA 报告，现在其中包括功能采用指标。



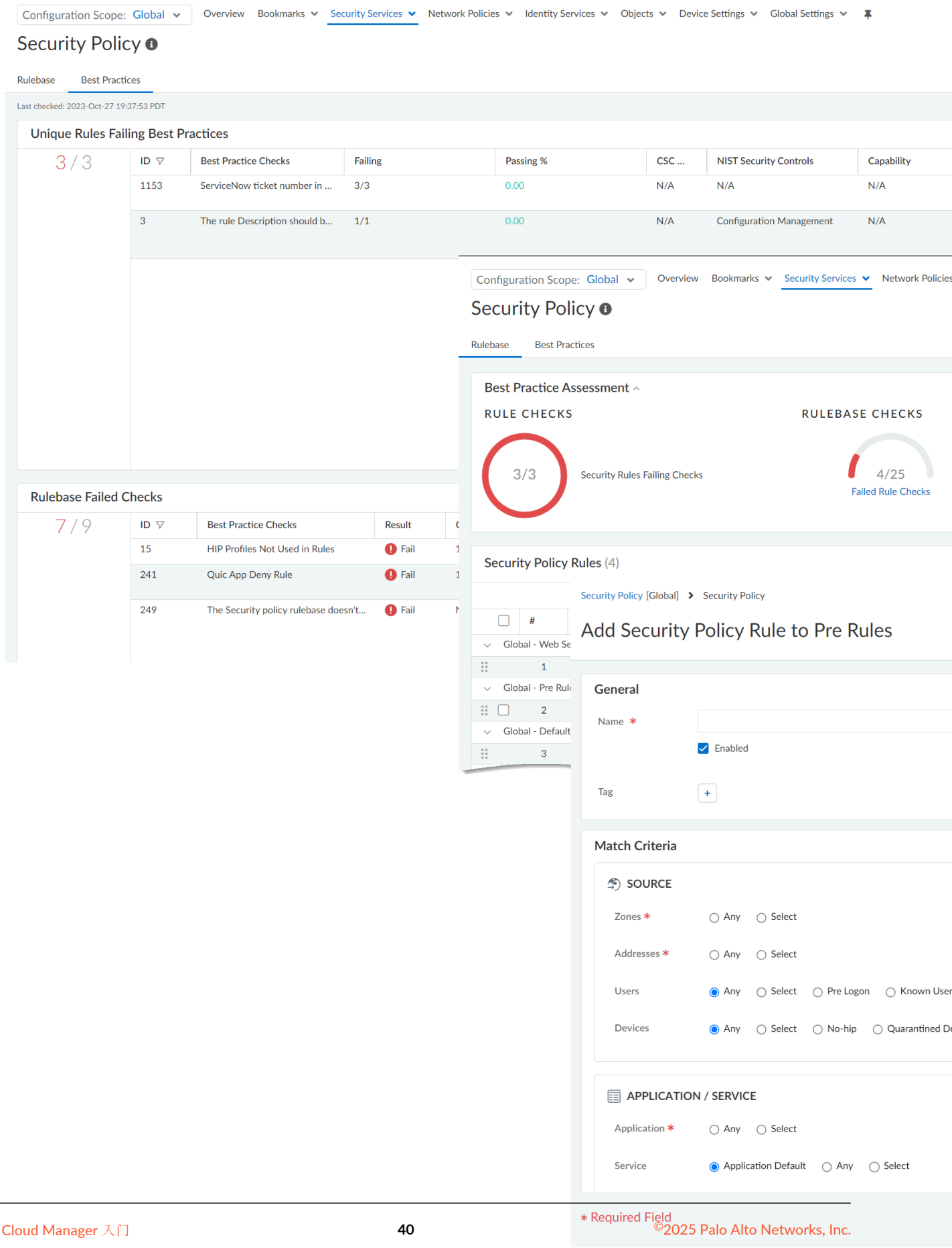
加强安全态势的最佳实践工具

找到一组工具来帮助您改善安全态势。

- 为您的部署定制安全态势检查，以最大限度地提高管理：安全态势设置中的相关建议
- 使用配置清理来识别并删除未使用的配置对象和策略规则。
- 配置策略优化器设置来精炼和优化过于宽松的安全规则，以便它们只允许网络中实际使用的应用程序。
- 创建您自己的合规性检查 — 定制现有的最佳实践检查并创建和管理特殊例外，以更好地满足您组织的业务需求。
- 使用Policy Analyzer 快速确保您对安全策略规则所做的更新符合您的要求，并且不会引入错误或错误配置（例如导致重复或冲突规则的更改）。

实时、内联的最佳实践配置检查

最佳实践指导旨在帮助您增强安全态势，同时帮助您有效地管理环境并最大限度地提高用户的工作效率。不断根据这些内联检查评估您的配置 - 当您看到改善安全性的机会时，请立即采取行动。



- 最佳实践分数

  最佳实践分数显示在功能指示板上（例如安全策略、解密或 URL 访问控制）。这些分数可以让您快速了解您的最佳实践进度。您只需一眼便能确定需要进一步调查的区域或想要采取行动来改善安全态势的区域。

- 最佳实践字段检查

  字段级检查可以准确地显示您的配置与最佳实践不一致的设置。最佳实践指导以在线方式提供，以便您可以立即采取行动。

- 最佳实践评估

  这里可以全面了解功能的实现如何与最佳实践保持一致。检查失败的检查，看看可以在哪些地方进行改进（您也可以查看通过的检查）。规则库检查突出显示您可以在单个规则之外进行的配置更改，例如，对跨多个规则使用的策略对象进行的配置更改。

最佳实践检查适用于：

- 您的安全策略规则库

  规则库检查查看安全策略的组织和管理方式，包括适用于许多规则的配置设置。

- 安全规则
- 安全配置文件
  - 防间谍软件
  - 漏洞保护
  - WildFire 和 防病毒软件
  - URL 访问管理
  - DNS 安全
- 身份验证
- 解密
- **GlobalProtect**

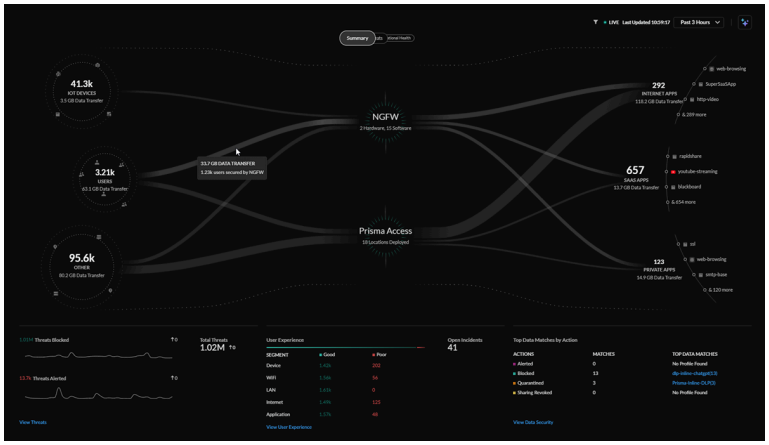
想要了解更多有关 ***Palo Alto Networks*** 最佳实践的信息？

这是最佳实践主页，您可以在此处找到帮助您过渡到并实施最佳实践的资源。

命令中心：Strata Cloud Manager

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW，包括由 软件 NGFW 积分提供资助的项目 • Prisma SD-WAN	这些许可证中的每一个都包括 Strata Cloud Manager 访问权限： ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Pro ❑ Strata Cloud Manager Essentials ❑ Prisma SD-WAN 访问命令中心所需的其他许可证和先决条件： ❑ Strata Logging Service ❑ 用于在命令中心查看某些指标的特定许可证，如下所述 ❑ 具有查看命令中心权限的角色 → 您可用的特性和功能Strata Cloud Manager取决于您使用的许可证。

Strata Cloud Manager 命令中心是新的 NetSec 主页；它是一个交互式可视化摘要，可帮助您评估网络的运行状况、安全性和效率。命令中心提供了 NetSec 平台的综合视图，并让您在单一位置全面了解您的源、应用程序、Prisma Access 部署、NGFW 和安全服务。



命令中心允许您与数据交互并可视化网络上事件之间的关系，以便您可以立即采取行动来加强您的安全性。

命令中心与新的 Activity Insights dashboards（Activity Insights 指示板） **Insights [见解] > Activity Insights**）集成，并将通过可操作的洞察突出显示您已加入的许可证和订阅检测到的异常，同时提供修正这些异常的途径。

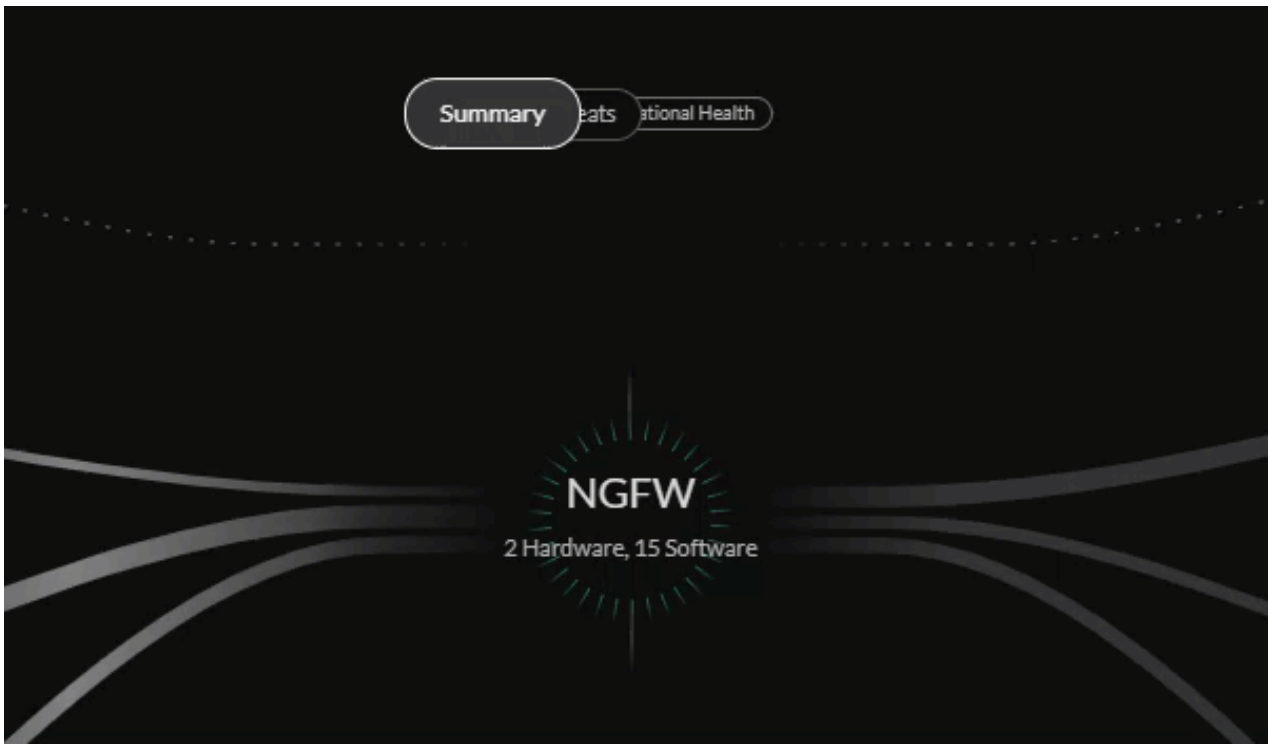
从新首页您可以看到：

- 全面查看网络上在源（用户、IoT、外部主机）和应用程序（互联网、SaaS、私有）之间流动的所有流量。
- 如何访问和保护用户、设备和应用程序等资产。
- 导航到具有上下文的特定指示板，以便更深入地了解影响您网络的问题。
- 用户工作时遇到的威胁类型。

要开始，请启动 Strata Cloud Manager 并单击 **Command Center**（命令中心）（ ）。

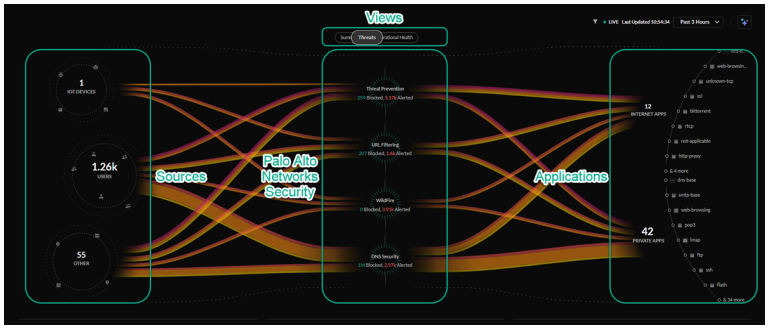
如何与 Strata Cloud Manager 命令中心交互

命令中心的每个视图都整齐地分解了评估网络运行状况和安全所需的所有信息。



命令中心的数据每 5 分钟刷新一次，默认显示过去 24 小时的数据。您还可以按过去 1 小时、3 小时、7 天或 30 天筛选这些数据。

每个命令中心视图显示从源流出的不同类型的视觉数据，通过 Prisma Access 和 NGFW 或部署在网络上的安全订阅，到达网络上的各种应用程序。



来源气泡（混合工作者、办公室用户、IoT 设备和其他）位于左侧，应用程序气泡（通过互联网、SaaS 访问以及在本地或云中托管）位于右侧。应用程序气泡显示每个类别中最常用的三个应用程序。

来源包括：

- **IoT Devices**（**IoT** 设备）– 由有效 IoT Security 许可证发现并启用的设备。
- **Users**（用户）– 远程用户和分支用户。

- **Other**（其他）– 访问互联网上的资源的内部和外部主机。

应用程序包括：

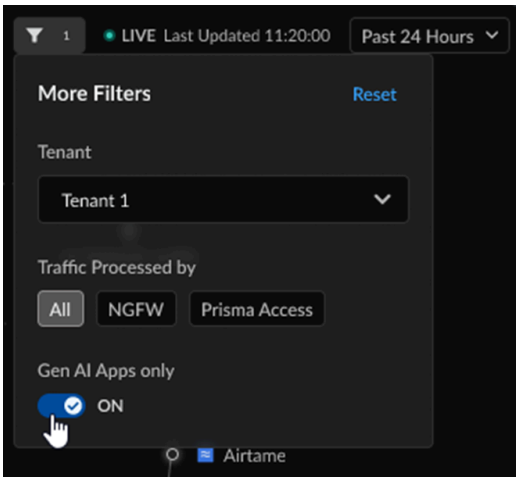
- **Internet Apps**（互联网应用程序）— 使用网络浏览器访问的应用程序。
- **SaaS Apps**（**SaaS** 应用程序）— 由应用服务提供商拥有和管理的云应用程序。
- **Private Apps**（私有应用程序）— 托管在数据中心的应用程序。

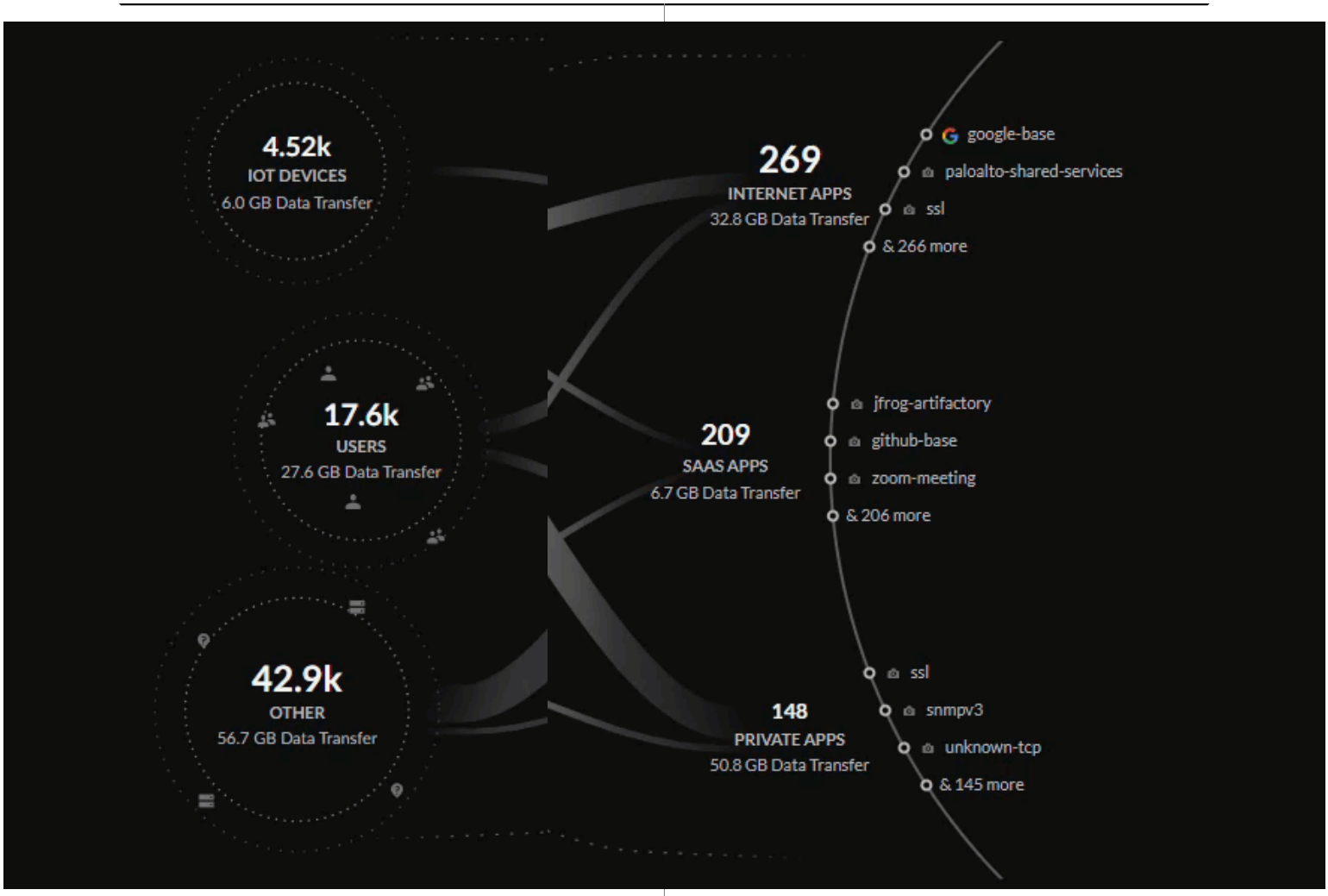
您可以通过单击源、部署或应用程序的气泡来筛选中心视图中的数据。这将为您提供与所选气泡相关的该视图的跟踪数据的更详细视图。

通过选择筛选器 (▼)，您可以按特定于 **Tenant**（租户）、**NGFW** 或 **Prisma Access** 的数据筛选命令中心视图中的数据。

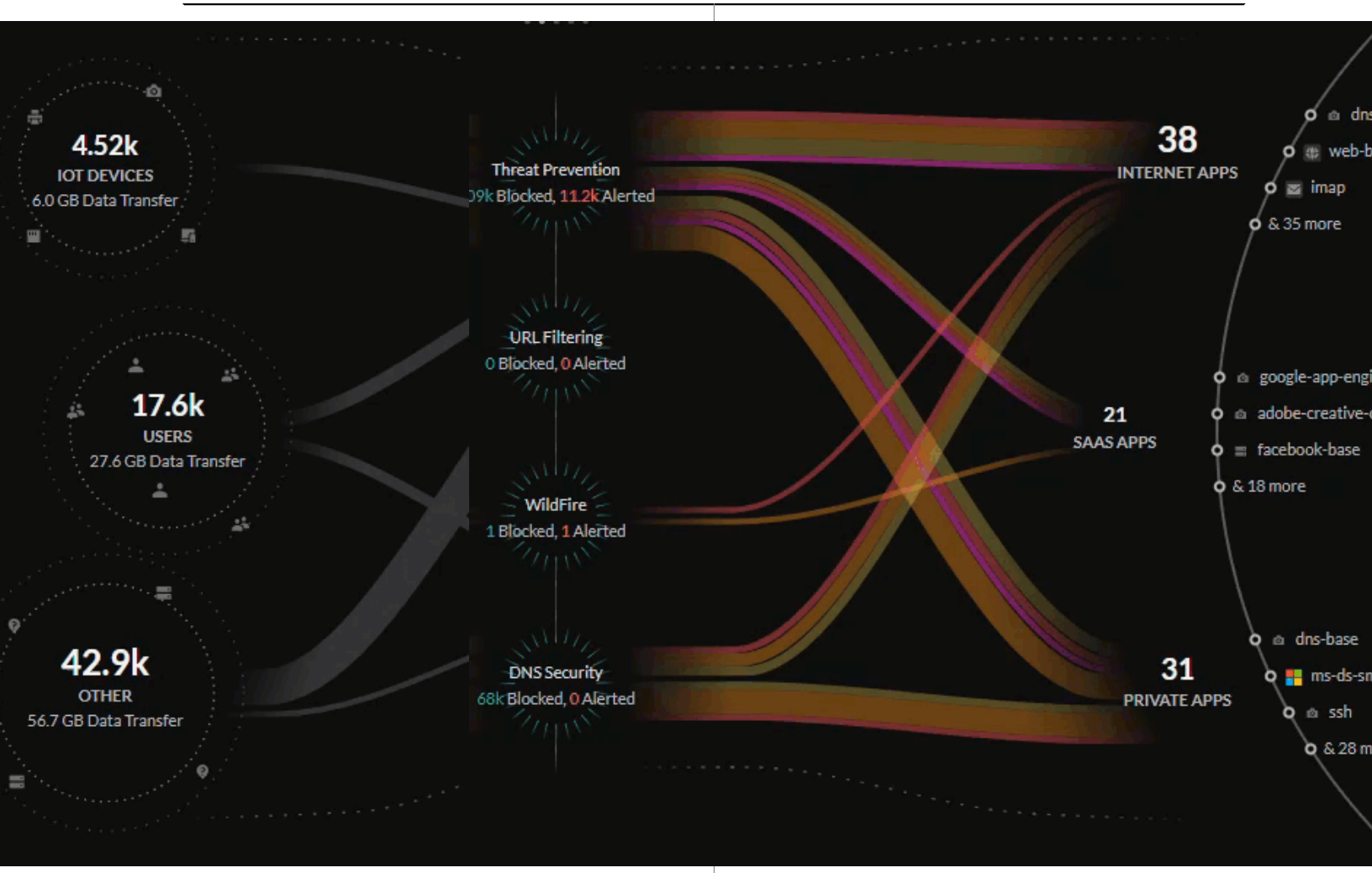
通过 AI Access 许可证，您可以 **GenAI Apps only**（仅通过 **GenAI** 应用程序）筛选所有命令中心视图中的流量，以便更好地评估网络上的用户正在使用的 GenAI 应用程序如何影响您的 Data Security。

有关 *AI Access Security* 和 *AI Access Security* 许可证的更多信息，请单击此处。

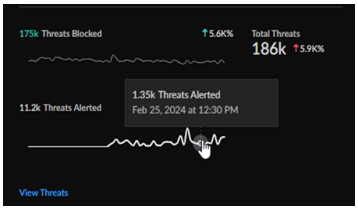




查看其中一个视图时，您可以将鼠标悬停在线条上以获取有关网络的更多信息，例如流量或网络上阻止或允许的威胁。



集中视图摘要下方是通过您激活的订阅跟踪的几个关键指标，可为您的网络提供可操作的见解。这些关键指标提供了导航到几个详细上下文页面之一的功能，您可以在其中找到有关已出现的指标的更多信息并深入了解可能的解决方案。



Strata Cloud Manager 命令中心视图

命令中心为您提供四种不同的视图，每种视图都有自己的跟踪数据和指标以供检查和交互。

- 摘要
- 威胁
- Operational Health
- Data Security

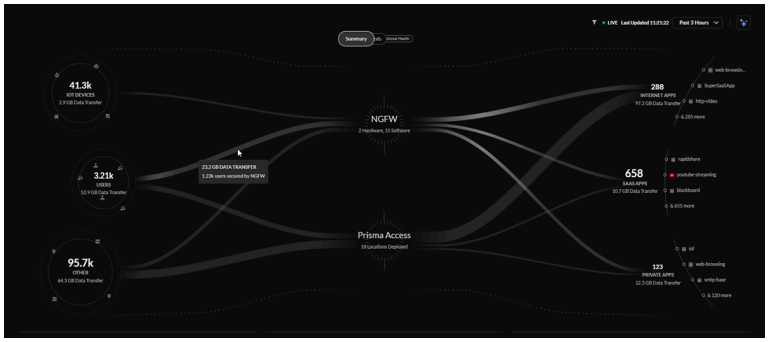
命令中心（摘要）

Summary（摘要）视图向您展示了来自用户、外部主机、IoT 设备和应用程序的所有流量的高级视图，以及其他视图突出显示的网络上的一些问题和异常的预览。每天查看网络运行状况时，您首先可以使用此视图。

摘要许可证	• 要使用 Strata Command Center，您必须至少拥有随 Strata Logging Service 提供的以下许可证之一：
	  ❑ Prisma Access 许可证
	  ❑ AIOps for NGFW Premium 许可证
	• 或者随 Strata Logging Service 许可证提供的 AIOPs for NGFW 免费版许可证
	• 摘要视图中的其他指标所需的许可证：
	  ❑ Cloud-Delivered Security Services (CDSS) 订阅
	  ❑ Data Security 订阅
	  ❑ ADEM 许可证
	  ❑ AI Access 许可证

摘要中心视图

摘要中心视图提供了 IoT 设备、用户、从互联网访问资源的外部主机、互联网应用、SaaS 应用和网络上的私有应用之间传输的数据。



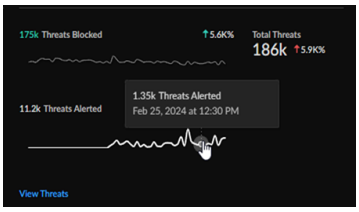
摘要中心视图中的线条表示网络上的数据传输和流量，线条的粗细表示从源和应用程序传输的数据量。

您可以看到网络基础设施如何保护这些源：

- Prisma Access 部署
- 从您的 Strata Logging Service 清单部署的新一代防火墙

威胁总计数

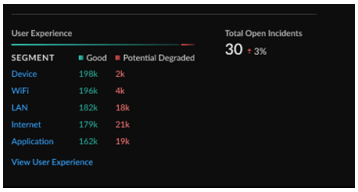
Total Threats Count（威胁总计数）小部件可让您快速查看网络中检测到的威胁总数、已阻止的威胁数量、已发出警报的威胁数量以及选定时间范围内的威胁变化。



单击转到 Activities Insights**Insights [见解] > Activity Insights > Threats [威胁]**）屏幕，查看网络上威胁的详细数据。

未解决事件和用户体验

Open Incidents and User Experience（未解决的事件和用户体验）小部件可让您查看未解决的事件总数，从用户设备到应用程序的服务交付链中各个细分市场的良好和可能降级的用户体验的细分情况，以及选定时间范围内打开的事件的变化。



单击转到应用程序体验指示板**Dashboards [指示板] > Application Experience [应用程序体验]**），了解有关网络运行状况和用户体验以及性能指标的详细数据。

按操作列出的主要数据配置文件

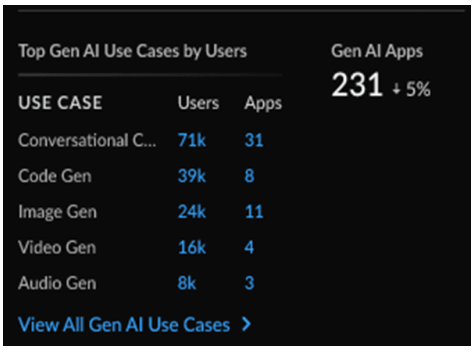
通过 **Top Data Profiles**（主要数据配置文件）小部件，您可以查看顶级预定义数据筛选配置文件、网络流量中找到的匹配数量，以及根据这些数据配置文件对敏感数据采取的操作。

单击转到Data Security视图**Command Center [命令中心] > Data Security**），查看网络上敏感数据的详细分类。

按用户和 GenAI 应用程序列出的最佳 GenAI 用例

Top GenAI Use Cases by User（按用户划分的主要 **GenAI** 用例）小部件可让您查看网络上用户使用的 GenAI 应用的最常见用例、每个用例的用户数量以及每个用例下的 GenAI 应用数量。

您还可以查看网络上 GenAI 应用程序的总数，以及基于时间筛选器的应用程序的百分比变化。



单击 Activity Insights 中的 AI Access Security**Insights [见解] > AI Access]**）指示板，了解您网络上 GenAI 应用采用情况的更详细分析，以及如何更好地保护数据的建议。

有关 *AI Access Security* 以及您的组织如何安全地采用 *GenAI* 应用程序，同时降低 *Data Security* 风险的更多信息，请从此处开始。

威胁

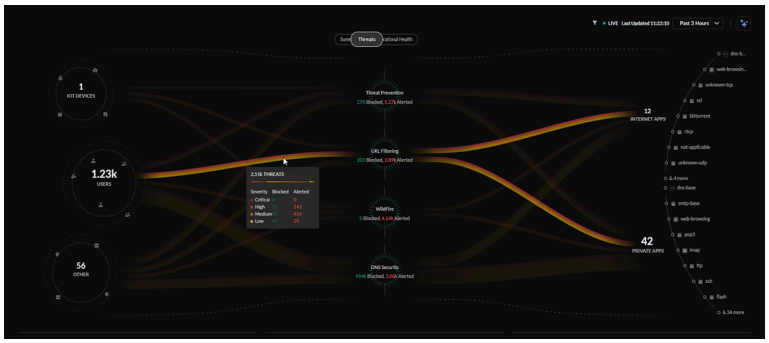
Threats（威胁）视图显示网络上检测到的流量以及 CDSS 订阅检测到的威胁。您可以使用此视图监视网络上已阻止和已发出警报的威胁，或调查网络中需要更新策略以更好地阻止任何已发出警报的威胁的区域。

威胁许可证	• 威胁许可证，包括： ❑ Threat Prevention 许可证 ❑ URL 筛选许可证 ❑ WildFire 许可证 ❑ DNS Security 许可证

威胁中心视图

通过威胁中心视图可以查看网络上已由活动的云交付安全服务订阅识别的所有威胁。

威胁视图将显示您的 Palo Alto Networks CDSS 订阅如何通过监控网络上的潜在威胁来保护您的流量。命令中心让您可以深入了解 IoT 设备、用户和应用程序的流量百分比，以及允许或警告的威胁总数。



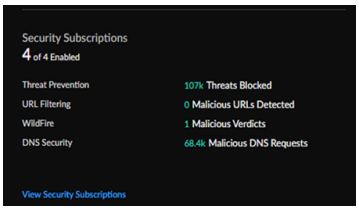
威胁中心视图中的线条表示安全订阅正在监视的通信量，粗细表示检测到的威胁量，颜色表示威胁的严重性是严重、高、中还是低。

安全订阅

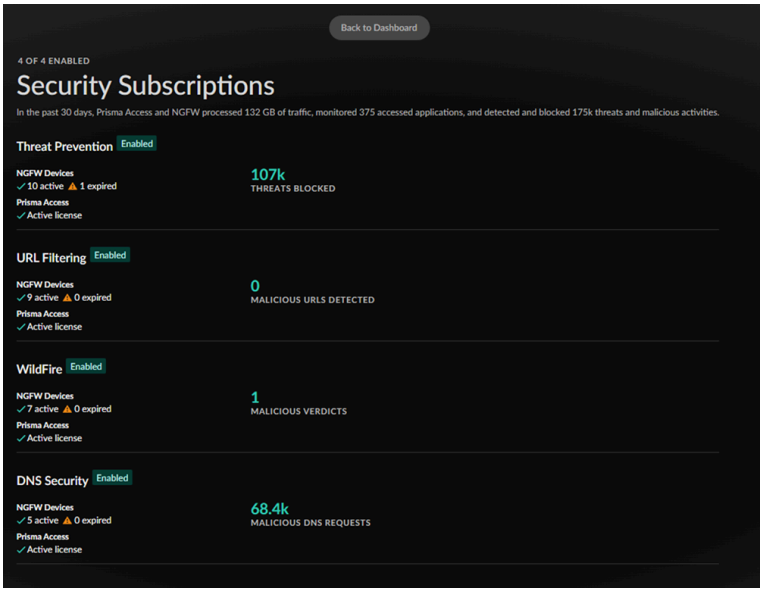
Security Subscriptions（安全订阅）小部件可让您查看云交付的安全订阅，哪些订阅是活动的，以及它们如何保护您的网络的快照。

订阅	说明
Threat Prevention	Threat Prevention 可保护您的网络免受商品威胁（普遍存在但无法消除）和有组织的网络对手造成的有针对性的高级威胁的侵害。

订阅	说明
URL Filtering	URL 筛选是我们全面的 URL 筛选解决方案，可保护您的网络和用户免受基于 Web 的威胁。
WildFire	云交付的 WildFire 恶意软件分析服务使用来自业界最大的全球社区的数据和威胁情报，并应用高级分析来自动识别未知威胁并阻止攻击者。
DNS Security	使用 Palo Alto Networks DNS 安全服务自动保护您的 DNS 流量。

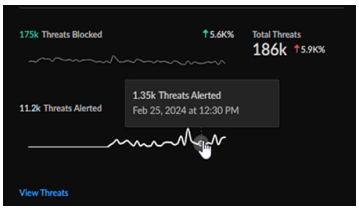


Security Subscriptions（安全订阅）小部件**Command Center [**命令中心**] > View Security Subscriptions [**查看安全订阅**]**），您可以查看与 NGFW 和 Prisma Access 部署相关的订阅状态的详细报告。单击 **Back to the Dashboard**（返回指示板）以返回 **Threats**（威胁）视图。



威胁总计数

Total Threats Count（威胁总计数）小部件可让您快速查看网络中检测到的威胁总数、已阻止的威胁数量、已发出警报的威胁数量以及选定时间范围内的威胁变化。



有关网络上威胁的详细数据，请单击转到 Activities Insights**Insights [见解] > Activity Insights > Threats [威胁]**）。

阻止和警告威胁

Blocked and Alerted Threats（阻止和报警的威胁）小部件为您提供了网络中检测到的威胁的自上而下视图，按类别、威胁级别（严重、高、中和低）以及威胁是否已被阻止或发出警报对其进行组织。

单击查看影响您网络的所有威胁的详细表格**Insights [见解] > Activity Insights > Threats [威胁]**）。

Operational Health

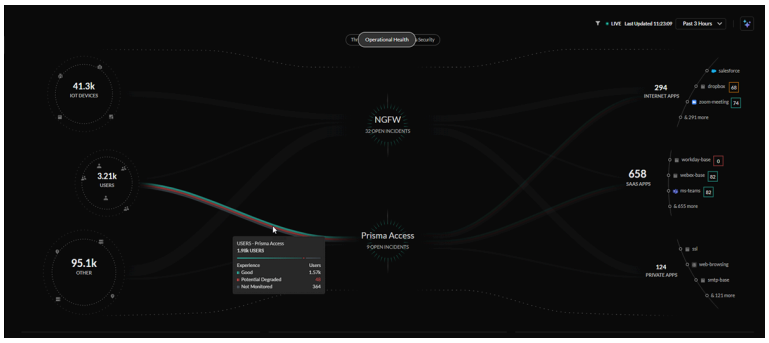
Operational Health 视图显示网络上基础设施和用户体验的运行状况。您可以使用此视图监视 NGFW 和 Prisma Access 部署的运行状况以及网络上的用户体验，并查看每个区域中未解决事件的严重性。

Operational Health 许可证	• 监控订阅，包括： ❑ ADEM Observability ❑ AI-Powered ADEM ❑ AIOps for NGFW Premium

Operational Health 中心视图

Operational Health 中心视图提供了对网络基础设施和用户体验运行状况的了解。如果用户拥有自主数字体验管理 (ADEM)　许可证，他们将在此视图中接收增强的数据。

Operational Health 视图将显示 Palo Alto Networks ADEM 订阅如何监控 SASE 环境中所有用户和应用程序的数字体验。



Operational Health 中心视图中的线代表网络上的所有用户。用户按用户体验得分进行组织，线条的颜色表示“良好”、“较差”或未受监控的评级。

未解决事件总数和事件（按严重性）

Open Health Incidents by Severity（按严重性列出的未解决运行状况事件）小部件可让您查看网络上所有未解决的事件，并按事件的范围（NGFW、Prisma Access 和 Prisma SD-WAN）、严重性和数量查看详细信息。

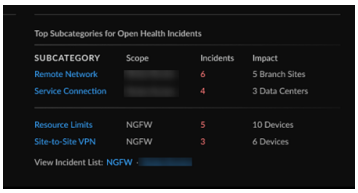
该小部件根据选定的时间段跟踪打开的事件的百分比变化。

对于每个可用范围，单击转到 **Incidents and Alerts**（事件和警报）指示板**Incidents and Alerts [**事件和警报**] > Prisma Access / NGFW > All Incidents [**所有事件**]**）。

未解决运行状况事件的顶级子类别

通过 **Top Subcategories for Open Health Incidents**（未解决运行状况事件的顶级子类别）小部件，您可以查看网络上未解决运行状况事件的顶级子类别，这些子类别按范围、子类别、事件数量以及受影响的内容（数据中心、站点、设备等）进行组织。

小部件将显示单个范围的前五个子类别，或多个范围的前两个子类别（如果可用）。



有关事件的更多详细信息，请单击转到 **Incidents and Alerts**（事件和警报）指示板**Incidents and Alerts [**事件和警报**] > Prisma Access/NGFW / Prisma SD-WAN**）。

监控的用户和用户体验

Open Incidents and User Experience（未解决的事件和用户体验）小部件可让您查看未解决的事件总数，从用户设备到应用程序的服务交付链中各个细分市场的良好和可能降级的用户体验的细分情况，以及选定时间范围内打开的事件的变化。

单击转到 **Application Experience**（应用程序体验）指示板**Dashboards [**指示板**] > Application Experience [**应用程序体验**]**），了解您的网络体验和性能指标的详细数据。

最佳实践

Data Security

Data Security 视图显示在整个网络和各种连接的 SaaS 应用程序中检测到的所有敏感数据。您可以使用它监控和识别组织中高风险敏感数据流。

Data Security 许可证	• Data Security 许可证，包括： ❑ SaaS Security 许可证 ❑ Data Security 许可证 ❑ Enterprise DLP 许可证

Data Security 中心视图

Data Security 中心视图提供整个网络和连接的SaaS应用程序的敏感和高风险数据映射。命令中心可让您深入了解组织中敏感数据用户、检测到敏感数据活动（资产上传、下载或资产暴露）的特定受制裁、未制裁、容忍或未标记的应用程序，以及允许、阻止、隔离、吊销共享或暴露的资产数量。

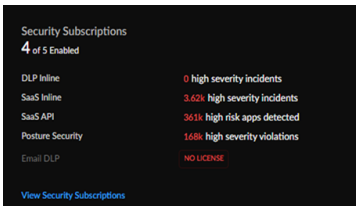
Data Security 中心视图中的线条表示通过静态数据和动态 Data Security 解决方案检测到的敏感数据，线条的粗细表示数据量，颜色表示该数据是否已标记为关键、高、中或低风险。

安全订阅

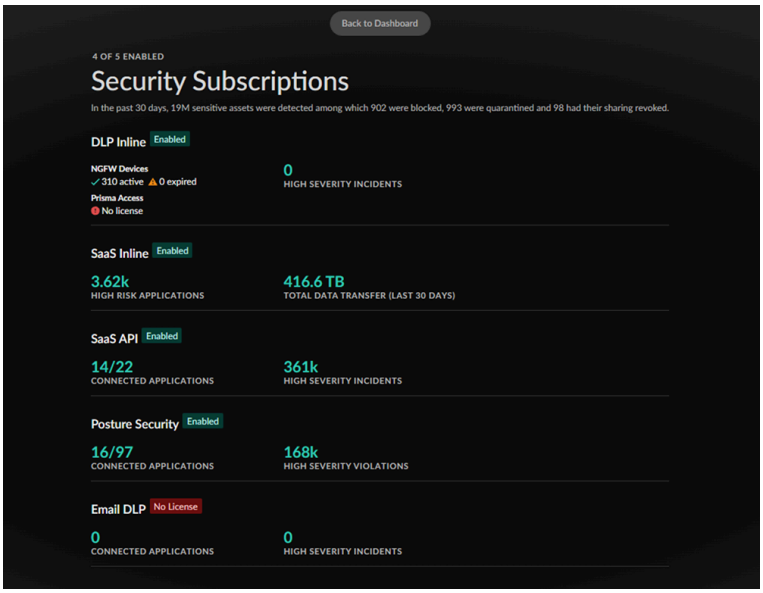
Security Subscriptions（安全订阅）小部件可让您查看您的 Data Security 订阅，哪些处于活动状态，以及这些订阅如何保护您的网络安全的快照。

订阅	说明
DLP Inline	Enterprise DLP 是一种基于云的服务，它使用监督的机器学习算法将敏感文档分类，以防止泄露、数据丢失和数据泄露。
SaaS Inline	SaaS Inline 解决方案与 Strata Logging Service 配合使用，可发现网络上正在使用的所有 SaaS 应用程序。

订阅	说明
SaaS API	SaaS API 是基于云的服务，您可以使用云应用的API直接连接到您认可的 SaaS 应用，并在应用内提供数据分类、共享或权限可见性以及威胁检测。
Posture Security	SaaS Security Posture Management (SSPM) 通过持续监控帮助检测和补救受制裁的 SaaS 应用程序中的错误配置设置。
Email DLP	Email DLP 是 Enterprise DLP 的一个附加组件，它通过 AI/ML 支持的数据检测防止包含敏感信息的电子邮件泄露。

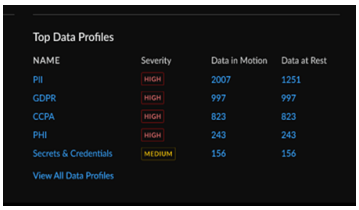


单击 **Security Subscriptions**（安全订阅）小部件**Command Center [**命令中心**] > View Security Subscriptions**（查看安全订阅））可为您提供与 NGFW 和 Prisma Access 部署相关的订阅状态的详细报告。单击 **Back to the Dashboard**（返回指示板）可返回 **Data Security** 视图。



主要数据配置文件

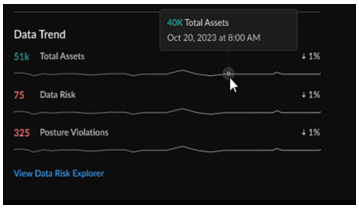
Top Data Profiles（主要数据配置文件）小部件显示在所有检查的敏感数据中检测到的顶级数据配置文件、数据配置文件的严重性以及在线检测到的与运动数据与静止数据匹配的资产数量。



单击以转到 **Data Loss Prevention** 指示板**Manage [管理] > Configuration [配置] > Data Loss Prevention [数据丢失预防]**），以查看所有预定义的数据配置文件并添加自定义数据配置文件。

Data Trend

Data Trend 小部件显示由 Data Security 订阅监控的敏感数据的趋势，按总资产、数据风险和状态违规的百分比变化进行组织。



单击转到 **Data Risk**（数据风险）指示板**Manage [管理] > Configuration [配置] > Data Loss Prevention > Data Risk [数据风险]**），以了解您的整体数据风险得分，并查看可操作的建议，以改善您组织的 Data Security 态势。

见解：Activity Insights

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW，包括由 软件 NGFW 积分提供资助的项目 • Prisma SD-WAN	这些许可证中的每一个都包括 Strata Cloud Manager 访问权限： ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Prisma SD-WAN ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro 访问某些“Activity Insights”视图所需的其他许可证和先决条件是： ❑ Strata Logging Service ❑ 云交付安全服务 (CDSS) ❑ ADEM 可观测性 ❑ WAN Clarity 报告 ❑ 有权查看指示板的角色 → 您可用的特性和功能Strata Cloud Manager取决于您使用的许可证。

Activity Insights 可让您深入了解 Prisma Access 和 NGFW 部署的网络活动。此视图将您的网络数据（例如网络流量、应用程序使用情况、威胁和用户活动）统一到一个界面中。Activity Insights 提供可视化、监控和报告功能，帮助您轻松完成任务。一旦您通过 Strata Cloud Manager 命令中心确定需要关注的领域，请使用上下文链接导航到 Activity Insights 或 其他指示板，以便进行进一步分析。

Activity Insights 具有高级筛选器，可帮助您专注于与您的部署相关的安全方面。利用 Activity Insights 中的高级报告功能，您可以从概览选项卡中的数据下载、共享和安排报告。该报告分别显示指示板中应用的每个筛选器的数据。或者，您可以从 **Strata Cloud Manager** > **Reports**（报告）菜单安排 Activity Insights 和指示板的报告。

启动 Strata Cloud Manager 并单击 **Insights**（见解）（  以开始。

Activity Insights 向您显示什么？

Activity Insights 显示部署在 Prisma Access 和 NGFW 环境下的每个 Strata Logging Service 租户的聚合数据。您可以筛选特定部署的数据。Activity Insights 有不同的标签。每个选项卡都提供了与应用程序、用户、威胁、URL 和网络使用情况相关的网络数据的统一视图。

- **Overview（概览）**- 显示选定时间范围内涉及的活动数最多的应用程序、威胁、用户、URL 和会话的数据。通过此视图可以快速识别网络中的任何异常，然后深入研究需要调查的活动。
- **Applications（应用程序）**- 概述网络中所有应用程序的使用情况，包括数据传输、应用程序风险和用于监控应用程序体验的 ADEM 功能。
- **SD-WAN Applications（SD-WAN 应用程序）**- 查看 Prisma SD-WAN 应用程序的性能，包括一段时间内的运行状况评分、事务统计数据和带宽利用率指标的详细信息。
- **Threats（威胁）**- 提供 Palo Alto Networks 安全服务在您的网络中检测和阻止的所有威胁的整体视图。
- **Users（用户）**- 深入了解用户的流量和活动，包括 ADEM 监控用户体验的功能。
- **URL**- 显示您网络中访问的 URL，其中有多少是恶意的，访问 URL 的用户和应用程序，允许网络中的 URL 的规则以及安全服务的强制执行情况。
- **Rules（规则）**- 提供有关允许用户和应用程序生成的流量，在流量会话中检测到的威胁以及影响规则的 URL 的安全策略规则的见解。
- **Regions（区域）**- 显示与应用程序、用户、威胁和 URL 相关的网络流量详细信息。

如何使用指示板上的数据？

找到这里可以帮助您 -

- 确定您想要监控的应用程序，改善低分数应用程序的用户体验，并控制未经批准和有风险的应用程序。
- 查看与您的部署最相关的威胁，并获取有关威胁的背景信息以供调查。
- 根据日志中的发现结果优化安全策略规则和流量规则，以弥补安全漏洞。
- 监控用户活动以检测和阻止潜在威胁并防止敏感信息的滥用。

Activity Insights：概述

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW，包括由 软件 NGFW 积分提供资助的项目 • Prisma SD-WAN	这些许可证中的每一个都包括 Strata Cloud Manager 访问权限： ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Prisma SD-WAN ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro 访问某些“Activity Insights”视图所需的其他许可证和先决条件是： ❑ Strata Logging Service ❑ 云交付安全服务 (CDSS) ❑ ADEM 可观测性 ❑ WAN Clarity 报告 ❑ 有权查看指示板的角色 → 您可用的特性和功能Strata Cloud Manager取决于您使用的许可证。

查看所选时间段内网络中最常见的应用程序、威胁、用户、URL 和规则的摘要。浏览此视图可快速识别网络中的任何异常情况，然后深入研究需要调查的活动。概览视图包括：

- 对于会话数、数据传输、检测到的威胁、访问的 URL 和访问应用程序的用户，网络中活动量最大的前 5 个应用程序和应用程序类别。单击查看所有应用程序以查看应用程序的详细信息。

- 对会话、用户和应用程序影响最大的前 5 个威胁和威胁类别。分别在日志查看器、用户和应用程序选项卡中查看会话、用户和应用程序的详细信息。

- 阻止、允许和已提醒的会话的网络流量趋势、传输的数据量以及产生最多流量的用户。

- 流量会话、传输的数据、流量中发现的威胁、访问的 URL 以及受监控应用程序的用户体验得分最高的前 5 名用户。
- 访问量最大的 URL 以及有关访问这些 URL 的会话、用户和应用程序的详细信息。

- 部署中配置的受影响最大的前 5 个安全策略规则，使用筛选器来了解与规则匹配的会话、用户、URL、威胁、传输的数据、流量中涉及的应用程序。

您可以使用筛选器来查看要重点关注且与部署相关的数据点。这些筛选器可在指示板的所有选项卡中找到。

筛选器

Activity Insights 具有高级筛选器，可帮助您专注于与您的部署相关的安全方面。可用的筛选器包括：

- **Time Range**（时间范围）- 查看指定时间段的数据
- **Scope Selection**（范围选择）- 特定于部署的数据：Prisma Access、NGFW
- **Subtenant**（子租户）- 显示数据的 Prisma Access 实例
- **User Name**（用户名）- 查看涉及单个用户的活动
- **Application**（应用程序）- 与特定应用程序相关的网络事件
- **Application Type**（应用程序类型）- 应用程序类型；SaaS、互联网、私有
- **Threat Category**（威胁类别）- 特定威胁类别的数据
- **Threat Action**（威胁操作）- 查看特定于允许或已阻止的威胁的视图
- **URL Risk Level**（**URL** 风险等级）- 与具有特定风险等级的 URL 相关的数据；高、中或低
- **URL Category**（**URL** 类别）- 根据 URL 类别筛选数据
- **Source Location**（来源位置）- 查看源自特定位置的活动
- **Destination Location**（目的地位置）- 查看特定目标区域的活动
- **URL** - 与访问的特定 URL 相关的活动。
- **SaaS Application**（**SaaS** 应用程序）- 有关特定 SaaS 应用程序的数据
- **Sanctioned Application**（批准的应用程序）- 仅查看已批准或未批准的应用程序的数据
- **Port Type**（端口类型）- 对来自通过标准或非标准端口的应用程序的流量进行排序。
- **Protocol**（协议）- 查看使用特定 TCP、UDP 或 HTTP 端口的流量
- **Source Type**（来源类型）- 查看由特定设备、用户或其他人生成的活动。

报告

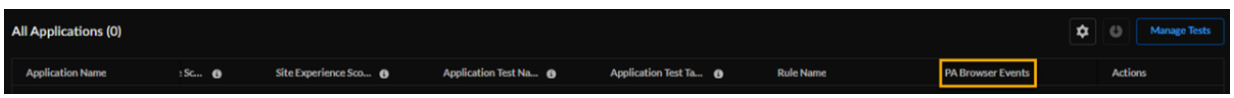
单击概述选项卡中的一个图标  ，从概述选项卡中的数据下载、共享和计划报告。您也可以从**Strata Cloud Manager** > **Reports**（报告）菜单中计划报告，单击 图标，然后从 **Type**（类型）下拉列表中选择“Activity Insights- 摘要”。

Activity Insights：应用程序

在何处可以使用？	需要提供什么？
• Prisma Access （利用 *Strata Cloud Manager* 或 *Panorama* 配置管理） • NGFW （利用 *Strata Cloud Manager* 或 *Panorama* 配置管理）	您必须拥有至少一个许可证才能使用Activity Insights： ❑ Prisma Access ❑ AIOps for NGFW Free (use the AIOps for NGFW Free app) 或 AIOps for NGFW Premium license (use the Strata Cloud Manager app) 查看“Activity Insights:应用程序”选项卡所需的其他许可证是： ❑ Strata Logging Service ❑ ADEM Observability 将解锁其他 Prisma Access 功能

监控您的 Prisma Access 和 NGFW 设置中的应用程序，使用该应用程序的用户、风险分数、每个应用程序的用户体验，并了解风险应用程序带来的安全影响。应用程序使用情况调查结果可以帮助您完善安全策略，以控制未经批准和存在风险的应用程序。单击 **Activity Insights > Applications**（应用程序）以查看以下信息：

- **Applications by Risk Score**（按风险评分划分的应用程序）- 组织中运行的应用程序总数以及表现良好、一般、不佳的应用程序的数量。根据应用程序体验分数，这些应用程序被分为“良好”、“一般”和“较差”。
- **Application Data Transfer**（应用程序数据传输）- 在所选时间范围内通过 NGFW 和 Prisma Access 防火墙下载和上传的总数据量。您可以进行筛选以查看源自应用程序类别并从设备（数据中心或防火墙）流经目的地的数据传输。
- **All Applications**（所有应用程序）- 使用此小部件查看哪些 Prisma Access 应用程序通过在其上运行综合测试来进行监控，以及在 NGFW 环境中运行的应用程序。该表还显示了它们的体验分数，这些分数可以让您了解每个应用程序的运行状况。如果您订阅了 Prisma Access Browser，则看到 **PA Browser Events**（PA 浏览器事件）列。选择事件数量，它会将您重定向到 Prisma Access Browser 管理页面。

  您可以使用 csv 格式下载表格中的数据（仅限 Prisma Access 应用程序）。单击 **Manage Tests**（管理测试）按钮，在“应用程序测试”表中查看为所有 Prisma Access 应用程序设置的所有综合测试。如果要创建测试来监控应用程序，请单击用户体验列下的 **Monitor App to view Health**（监控应用程序以查看运行状况）。

- **Application Details**（应用程序详细信息）- 查看应用程序的一般详细信息以及有关应用程序活动和应用程序体验的详细信息。
  - **Activity**（活动）选项卡显示应用程序中看到的威胁总数、访问该应用程序的用户总数，通过应用程序传输的数据，PA 浏览器数据事件和 PA 浏览器访问事件。

    下图显示了有关 **PA Browser Data Events**（PA 浏览器数据事件）和 **PA Browser Access Events**（PA 浏览器访问事件）的应用程序详细信息。默认视图显示所有事件和已阻止事件的 **Aggregate**（汇总），或者您可以选择查看按 **Event Type**（事件类型）和 **Count**（计数）划分的**Breakdown**（细分数据）。

  - **Experience**（体验）选项卡显示应用程序体验分数，所选时间范围内的分数趋势和网络性能指标。

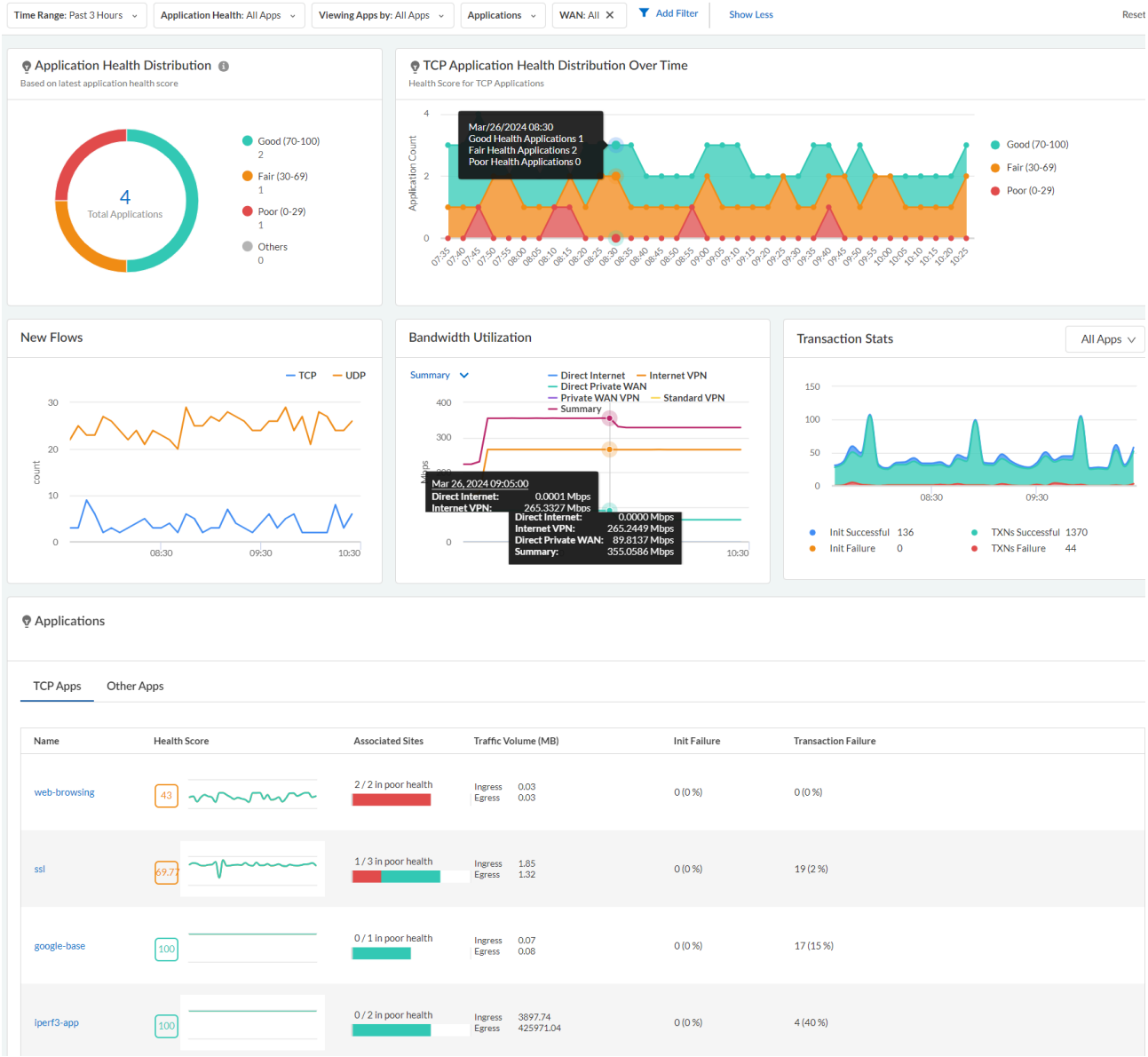
如果应用程序是容器应用程序，则显示的统计数据是容器中所有应用程序的汇总。例如，*Gmail* 是一个容器应用程序（*Gmail* 没有 *App-ID*）。它将诸如 *Gmail* 发帖、*Gmail* 下载、*Gmail* 上传等应用程序分组。为该容器应用程序设置的风险分数是为所包含应用程序找到的最高风险分数。所有其他指标都是通过汇总所包含应用程序的值来计算的。

报告 - 您无法生成涵盖此视图中数据的报告。但是，您可以使用 **Application Usage**（应用程序使用情况）报告来查看网络中的应用程序使用情况数据。要计划报告，请从 **Strata Cloud Manager** > **Reports**（报告）菜单中单击 图标，然后从 **Type**（类型）下拉列表中选择“应用程序使用情况”。

Activity Insights：SD-WAN 应用程序

在何处可以使用？	需要提供什么？
• Prisma SD-WAN	❑ Prisma SD-WAN 许可证 ❑ 用于查看某些小部件的 WAN Clarity Reporting 许可证

查看在 Prisma SD-WAN 中表现不佳的主要应用程序。查看确定的所有较差应用程序的运行状况评分，基于运行状况评分的租户的较差应用程序列表，以及过去 3 小时内以 5 分钟为间隔的较差应用程序的平均运行状况评分。



- 应用程序运行状况分布（需要 WAN Clarity 许可证）：针对给定租户的良好、一般和较差应用程序的分布。
- **TCP** 应用程序运行状况的时间分布（需要 WAN Clarity 许可证）：TCP 应用程序运行状况在一段时间内的良好、一般和较差分布。时间序列图应根据选定的持续时间进行计算和刷新。例如，支持的持续时间分别为 1 小时、3 小时、1 天、7 天、30 天和 90 天，间隔分别为 1 分钟、5 分钟、1 小时和 1 天。
- 新流量：显示给定时间段内某个应用程序、一组特定应用程序或所有应用程序的新 TCP 和 UDP 流。当 TCP 流看到第一个 SYN 数据包时，则将其视为一个新的流。当 UDP 流在任一方向上看到第一个 UDP 数据包时，会将其视为一个新流。流是由源和目的地 IP、源和目的地端口以及协议标识的双向数据包序列。
- 带宽利用率：“带宽利用率”图表显示网络中某条路径上利用的带宽量。使用该图表确定网络中可能影响应用程序性能的 WAN 拥塞。它是带宽峰值、特定站点消耗的总带宽和应用程序的可视化表示（如果上传是在传入或传出方向）。在“带宽利用率”图表中移动光标，以获得具有应用程序或时间戳的带宽利用率的更详细视图。通常，应用程序按其带宽利用率的顺序列出。
- 事务统计数据：提供有关 TCP 流的事务统计信息，包括特定应用程序或所有应用程序的启动/事务成功和失败、特定路径或所有路径以及所有运行状况事件。
- 应用程序：列出所有应用程序详细信息，例如名称、应用程序配置文件、运行状况评分、受影响的站点、通信量、初始化/失败和事务/失败。单击应用程序名称时，您可以在新页面上看到各个应用程序详细信息。

Activity Insights：威胁

在何处可以使用？	需要提供什么？
• Prisma Access （利用 *Strata Cloud Manager* 或 *Panorama* 配置管理） • NGFW （利用 *Strata Cloud Manager* 或 *Panorama* 配置管理）	您必须拥有至少以下一个许可证才能使用 Activity Insights： ❑ Prisma Access ❑ AIOps for NGFW Free (use the AIOps for NGFW Free app) 或 AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro 查看“Activity Insights：威胁”选项卡所需的其他许可证包括： ❑ Strata Logging Service ❑ CDSS 许可证 ❑ ADEM Observability 将解锁额外的 Prisma Access 功能

全面了解网络中的威胁活动和各种类型的威胁。该选项卡显示 Prisma Access 和 NGFW 部署中看到的威胁会话总数，并根据所选时间段内的威胁类别和威胁严重程度细分这些数量。您可以搜索与威胁相关的安全工件（文件哈希、URL、域或 IP 地址（IPv4 或 IPv6）），以了解 Palo Alto Networks 威胁情报分析和第三方分析结果。

查看网络中独特威胁的以下详细信息：

- **Threat Name**（威胁名称）- 威胁特征名称。使用此功能可以查找有关威胁的最新威胁库信息，包括一定时间范围内的所有威胁会话。
- **Threat ID**（威胁 **ID**）— 唯一威胁签名 ID。使用威胁 ID 查找 Palo Alto Networks 威胁数据库中有关此签名的最新信息。
- **Threat Category and Subcategory**（威胁类别和子类别）- 基于威胁特征（防病毒、间谍软件 (C2) 和漏洞）的威胁类型。
- **Licenses**（许可证）- 检测到威胁的 Palo Alto Networks 安全服务。

- **Severity**（严重性）- 威胁的严重性取决于利用漏洞的难易程度、漏洞的影响、易受攻击产品的普遍性、漏洞的影响等。严重程度分类如下：
  - 严重 — 当漏洞影响广泛部署的软件的默认安装时，漏洞利用可能会导致 Root 权限被盗用。漏洞代码（有关如何利用系统代码、方法、概念验证（POC）的信息）广泛可用且易于利用。攻击者不需要任何特殊的身份验证凭证，也不需要有关个别受害者的知识。
  - 高 — 能够演变为关键威胁但有抑制因素的威胁；例如，可能难以利用，不会导致攻击者的权限得到提升，或者受害者群体不会很大。
  - 中 — 影响力最低的小威胁，例如不会危害目标的 DoS 攻击或如下攻击：需要攻击者与受害者驻留在同一 LAN 中，仅会影响非标准配置或不知名应用程序，或者提供的访问权限有限。
  - 低 — 警告级别的威胁，对组织的基础结构产生的影响非常小。它们通常需要本地或物理系统访问权限，并且可能经常会导致受害者隐私或 DoS 问题及信息遭到泄露。
  - 信息性 — 可疑事件不会构成直接威胁，但据报告，这些事件引起了人们对可能存在的更深层次问题的关注。
- **Total Sessions**（总会话数）— 检测到威胁的会话数。单击威胁名称可以查看指定时间范围内的所有相关威胁会话。威胁会话表提供有关威胁的背景信息，例如 Palo Alto Network 安全服务检测到威胁的时间、用户、规则、应用程序、受威胁影响的设备以及对威胁采取的措施（允许或阻止）。
- **Total Users**（总用户数）— 遭受威胁的用户数量。
- **Allowed Threats and Blocked Threats**（允许的威胁和阻止的威胁）- 审查对威胁实施的操作，以确保这些操作不会在您的网络上触发误报。
- **Actions**（操作）- 调查日志查看器中威胁的日志历史记录。

报告 - 您无法生成涵盖此视图中数据的报表。

Activity Insights：用户

在何处可以使用？	需要提供什么？
• Prisma Access （利用 *Strata Cloud Manager* 或 *Panorama* 配置管理） • NGFW （利用 *Strata Cloud Manager* 或 *Panorama* 配置管理）	您必须至少拥有以下许可证中的一个才能使用 Activity Insights： ❑ Prisma Access ❑ AIOps for NGFW Free (use the AIOps for NGFW Free app) 或 AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro 查看 Activity Insights 所需的其他许可证：用户选项卡包括： ❑ Strata Logging Service ❑ Advanced URL Filtering 许可证 ❑ Cloud Identity Engine 许可证 ❑ Advanced Threat Prevention 许可证 ❑ ADEM Observability 将解锁其他 Prisma Access 功能

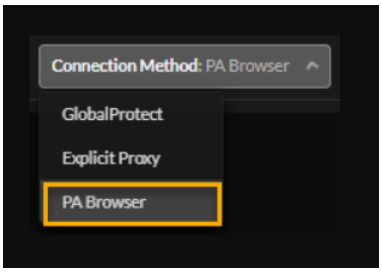
监控 Prisma Access 和 NGFW 环境中的用户活动。您可以从设备上的 GlobalProtect 应用程序，或者从设备上的 Web 浏览器，查看通过显式代理连接到 Prisma Access 和 NGFW 安全服务的用户的数据。监控用户活动有助于检测和阻止潜在威胁，防止敏感信息滥用，以及调整安全策略规则以弥补安全漏洞。

您可以根据以下内容筛选用户数据：

- 部署；Prisma Access、NGFW
- 连接方法和版本；GlobalProtect、Explicit Proxy、Prisma Access Browser
- 用户名
- 设备名称
- 流量来源位置和 Prisma Access 位置
- 用户访问的应用程序和用户体验分数筛选器

在此处查看以下详细信息：

- 已连接/活跃用户 - 监控有关当前连接的 GlobalProtect、代理移动用户和 Prisma Access Browser 的汇总数据。



查看在获取数据时或时间戳中指示的连接到您的网络的用户数量。您可以按用户或用户设备查看趋势。选择数字以查看 **Connected Users | Connected User Devices**（已连接的用户 **|** 已连接的用户设备）表，了解有关所有已连接用户及其所有设备的详细信息。

在趋势依据中按用户或按用户设备、**Connected Users | Connected User Devices**（已连接的用户 **|** 已连接的用户设备）以及 **Project Distribution by Theater**（按威胁划分的项目分布）动态权限访问数据。

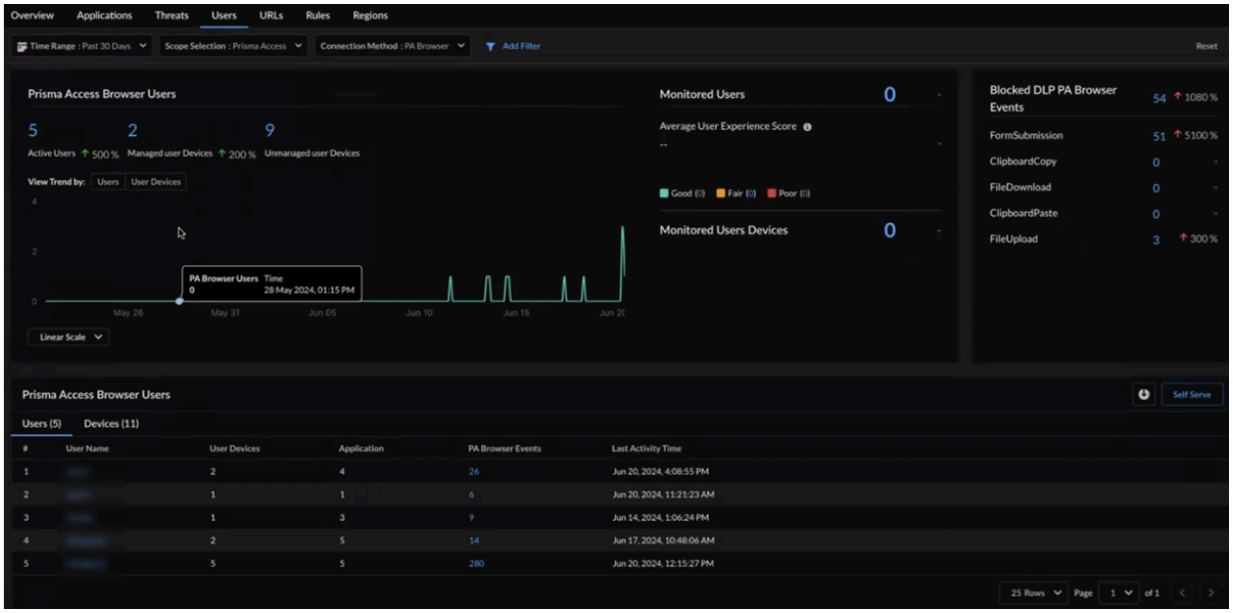
- 监控用户 - 查看 ADEM 监控的用户或用户设备的总数及其平均用户体验，即 ADEM 上监控的所有用户的体验分数总和。单击数字可查看与用户体验相关的用户活动详细信息。
- 风险用户 - 查看受威胁影响的用户数量。向上或向下箭头将此时间范围与之前的时间范围进行比较，以确定连接设备数量的百分比差异。选择查看 GlobalProtect 版本或 IP 池利用率的更多详细信息，以查看有关您环境中有风险的用户的详细信息。
- **GlobalProtect** 版本详细信息显示您的设备上安装的 GlobalProtect 版本。您可以看到每个版本有多少用户正在连接。使用数据来强制遵守最新的 GlobalProtect 应用程序版本。将鼠标悬停在分布趋势线上可以查看当时连接的用户的 IP 地址。
- 根据当时连接的用户数按不同 IP 池分配威胁查看 **IP** 池利用率。图表上的 IP 池利用率百分比是所有子网中可用的 IP 池块中使用的 IP 池块数。当您看到 IP 池条接近任何区域的最大容量时，您可以通过添加子网采取主动措施。

- 用户表显示在时间范围内登录的用户的信息，单击用户名可以了解个人用户的浏览模式：他们最常访问的网站、他们正在传输数据的网站以及尝试访问高风险网站。
  - 威胁
    - 浏览摘要 - 查看用户传输数据最多的网站类型以及用户访问的网站次数。
    - 访问量最大的 **10** 个 **URL** 类别 - 根据数据传输查看用户的主要 URL 类别。您还可以查看属于每个 URL 类别的已访问的唯一 URL 的数量。
    - **URL** 浏览摘要 - 在用户访问的唯一 URL 中，警惕对恶意和高风险 URL 的访问 - 这些网站可能会使您的网络面临威胁、数据丢失和合规性违规。如果您发现这些网站的访问量超出预期，请调整您的安全策略规则来弥补差距。
    - 前 **10** 个 **URL** - 查看用户最常访问的网站的风险级别。需要监控高风险 URL，因为它们可能会使您的网络面临威胁。
    - 按风险阻止的 **URL** - 这些是用户最常尝试访问的被阻止的 URL。查看 URL 筛选日志，并查看是否需要调整安全策略规则来更改操作。
    - 严重威胁 - 查看为用户检测到的威胁总数以及基于威胁严重程度的数字。将该数字与其他用户的数字进行比较。如果数字异常高，请调整安全策略规则。
    - 主要严重威胁 - 这些是用户最常检测到的威胁。
  - 连接 - 显示特定时间段内用户登录的设备趋势以及每个用户登录和注销事件的设备连接详细信息。
  - 体验 - 提供设备的用户体验数据、每个受监控应用程序的体验分数和趋势以及受监控用户和各个设备的应用程序的性能指标。

- Prisma Access Browser - 选择 **Prisma Access Browser** 连接方法来查看有关 Prisma Access Browser 用户的信息。

  Prisma Access Browser 用户活动趋势图显示在所选时间范围筛选器中某个时间点处于活跃状态的用户数量。该图表显示这些活跃用户的设备安装了 Prisma Access 连接代理（托管设备）和没有任何代理（非托管）用户的细目分类。

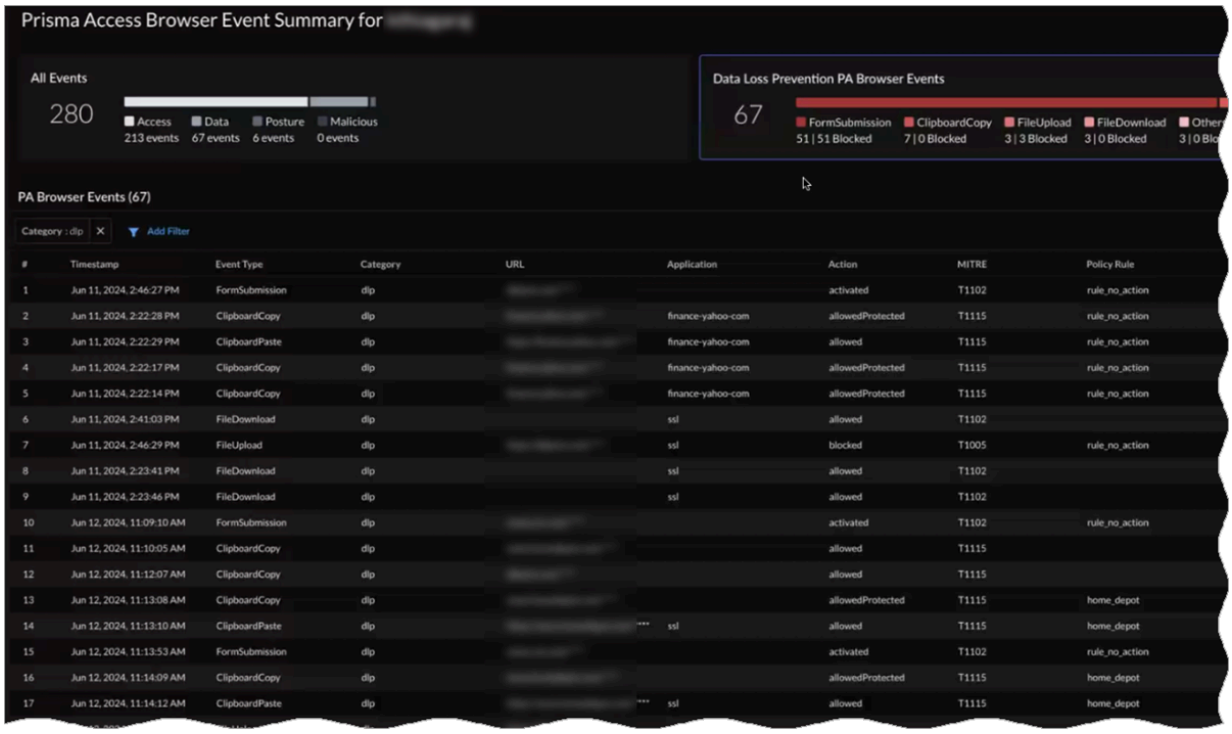
  Prisma Access Browser 提供对浏览器用户操作的无与伦比的可视性，可以指示用户在其设备上针对企业数据资产的操作是否受到 Enterprise DLP 策略的允许或阻止。被阻止的 **DLP PA** 浏览器事件小部件显示的事件表明用户在浏览器上执行的被策略阻止的操作。



  Prisma Access Browser 用户 表显示通过 Prisma Access Browser 访问应用程序的活跃用户列表。单击任何 **User Name**（用户名）即可在 **User Details**（用户详细信息） > **Activity**（活动）页面中查看该用户的 **Activity**（活动）。

  Prisma Access Browser Event Summary（**Prisma Access Browser** 事件摘要）页面列出用户在选定的时间间隔内通过浏览器执行的所有浏览器操作。**PA Browser Events**（**PA** 浏览器事件）表的默认视图显示所有 DLP **Browser Events**（浏览器事件）的列表，无论策略是允许还是阻止。您可以通过选择适当的事件类别将视图切换到其他事件类别，例如 **Access Events**（访问事件）、**Posture Events**（安装状况事件）或 **Malicious Events**（恶意事件）。在

每个 **Event**（事件）类别中，您可以查看事件类型的细分，以及显示浏览器事件执行时间的时间戳，有关访问的应用程序 URL 的信息、应用程序名称，以及任何相关的 MITRE 攻击说明。

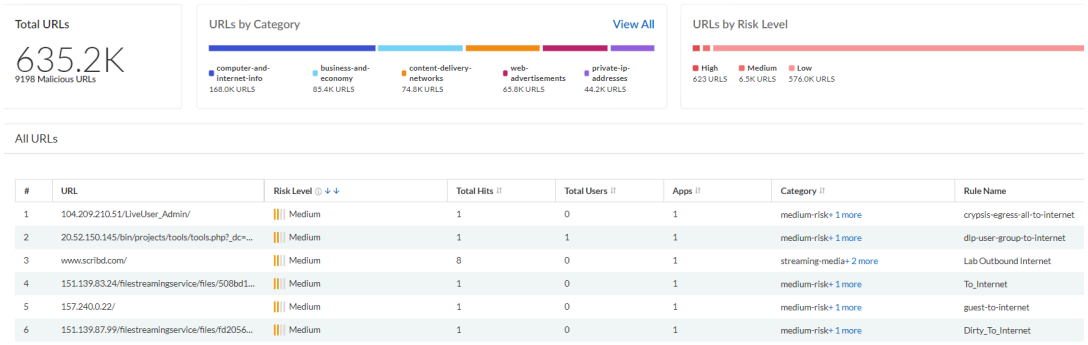


报告 - 您无法生成涵盖此视图中数据的报告。但是，您可以使用“用户活动”报告来查看网络中特定用户的活动。要从 **Strata Cloud Manager** > **Reports**（报告）菜单安排报告，请单击 图标，并从类型下拉菜单中选择用户。

Activity Insights：URL

在何处可以使用？	需要提供什么？
• Prisma Access （利用 *Strata Cloud Manager* 或 *Panorama* 配置管理） • NGFW （利用 *Strata Cloud Manager* 或 *Panorama* 配置管理）	您必须至少拥有以下许可证中的一个才能使用 Activity Insights： ❑ Prisma Access ❑ AIOps for NGFW Free (use the AIOps for NGFW Free app) 或 AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro 查看 Activity Insights 所需的其他许可证：“URL”选项卡包括： ❑ Strata Logging Service ❑ Advanced URL Filtering 许可证

此视图总结了高级 URL 筛选服务检测到的 Prisma Access 和 NGFW 部署中的 URL 活动。您可以查看在指定时间段内在您的网络中检测到的 URL 总数，以及按 URL 类别和风险级别细分这些 URL。使用筛选选项筛选指示板中的视图。



使用此处的数据可以 -

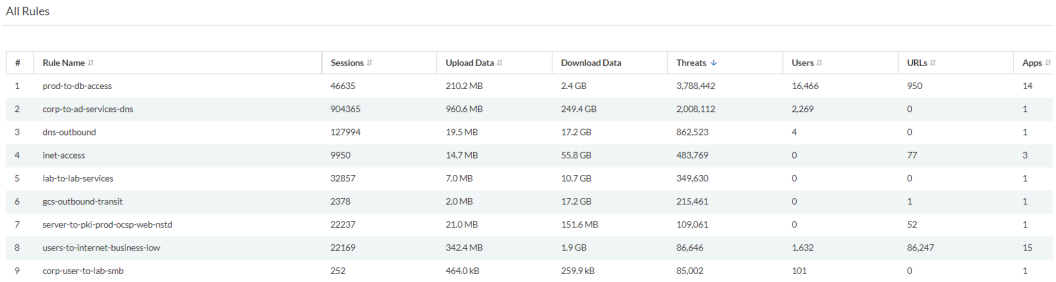
- 确定访问次数最多的 URL 类别、具有 URL 类别的唯一 URL、您网络中的 URL 历史记录以及全局分析结果。根据 URL 筛选服务筛选的恶意 URL，这些 URL 类别可能会使您的网络暴露给恶意和漏洞利用内容。最佳做法是阻止这些 URL 类别。
- 查看高风险 URL 及其对用户、应用程序和规则的影响。高风险 URL 网站未确认是恶意网站；但是，它们仍然可能使您的网络面临威胁（非恶意网站，但由防御性 ISP 托管的网站就是高风险网站的例子）。考虑对这些网站使用严格的解密和安全策略规则。

报告 - 您无法生成涵盖此视图中数据的报表。

Activity Insights：规则

在何处可以使用？	需要提供什么？
• Prisma Access （利用 *Strata Cloud Manager* 或 *Panorama* 配置管理） • NGFW （利用 *Strata Cloud Manager* 或 *Panorama* 配置管理）	您必须至少拥有以下许可证中的一个才能使用 Activity Insights： ❑ Prisma Access ❑ AIOps for NGFW Free (use the AIOps for NGFW Free app) 或 AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro 查看 Activity Insights 所需的其他许可证：规则选项卡包括： ❑ Strata Logging Service

查看与网络中的所有流量匹配的安全策略规则。安全策略规则根据流量属性（例如源和目标 IP 地址、应用程序、用户和服务）确定是阻止还是允许会话。通过网络的所有流量与会话匹配，每个会话与安全策略规则匹配。当发生会话匹配时，将应用安全策略规则。


All Rules

#	Rule Name	Sessions	Upload Data	Download Data	Threats	Users	URLs	Apps
1	prod-to-db-access	46635	210.2 MB	2.4 GB	3,788,442	16,466	950	14
2	corp-to-ad-services-dns	904365	960.6 MB	249.4 GB	2,008,112	2,269	0	1
3	dns-outbound	127994	19.5 MB	17.2 GB	862,523	4	0	1
4	inet-access	9950	14.7 MB	55.8 GB	483,769	0	77	3
5	lab-to-lab-services	32857	7.0 MB	10.7 GB	349,630	0	0	1
6	gcs-outbound-transit	2378	2.0 MB	17.2 GB	215,461	0	1	1
7	server-to-pki-prod-ocsp-web-nstd	22237	21.0 MB	151.6 MB	109,061	0	52	1
8	users-to-internet-business-low	22169	342.4 MB	1.9 GB	86,646	1,632	86,247	15
9	corp-user-to-lab-smb	252	464.0 kB	259.9 kB	85,002	101	0	1

指示板显示与安全策略规则匹配的网络事件的以下详细信息：

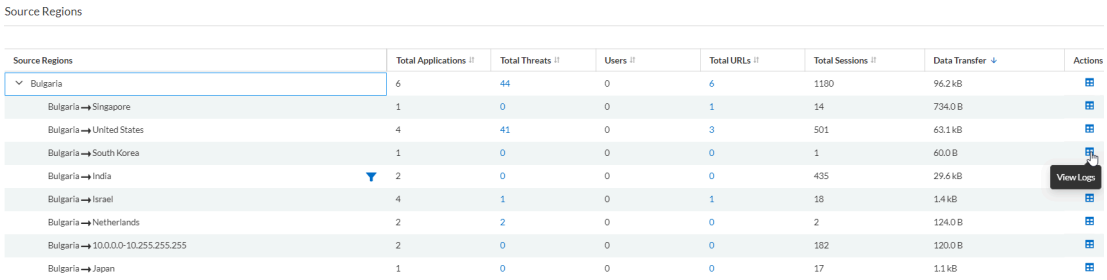
流量会话、传输的数据、会话中检测到的威胁、受影响的用户、浏览的 URL 和访问的应用程序。查看与流量会话最匹配的规则，分析这些会话以了解规则是否过于宽松，如果需要，请优化规则。

报告 - 您无法生成涵盖此视图中数据的报表。

Activity Insights：区域

在何处可以使用？	需要提供什么？
• Prisma Access （利用 *Strata Cloud Manager* 或 *Panorama* 配置管理） • NGFW （利用 *Strata Cloud Manager* 或 *Panorama* 配置管理）	您必须至少拥有以下许可证中的一个才能使用 Activity Insights： ❑ Prisma Access ❑ AIOps for NGFW Free (use the AIOps for NGFW Free app) 或 AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro 查看 Activity Insights 所需的其他许可证：区域选项卡包括： ❑ Strata Logging Service

这些是流量源自您网络中的区域。该视图提供有关威胁、用户、URL、网络会话和源自这些位置的数据传输的信息。您还可以深入查看以了解流量的目标位置。单击“操作”查看会话的流量日志。您可以使用这些数据来识别并缩小区域范围，这些区域的目标是试图渗透您网络的威胁的目标。优化规则，这些规则适用于目标区域。



一些筛选选项可以缩小进出特定源区域和目标区域的流量范围。其他筛选选项包括：

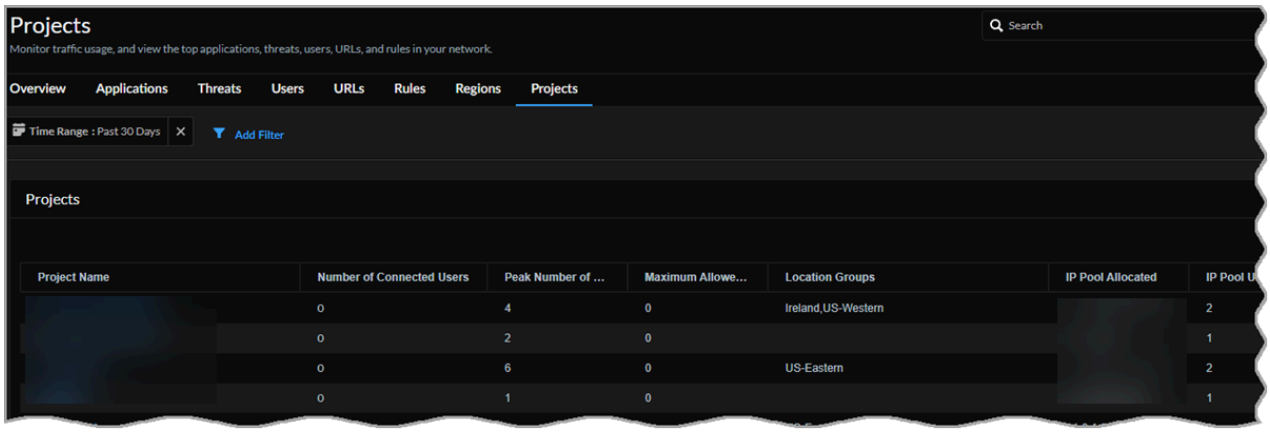
- 在特定部署中看到的流量；Prisma Access、NGFW
- 传入和传出已批准或未批准的应用程序的流量
- 使用特定端口和协议的流量
- 涉及特定威胁类型、威胁类别、URL 和 URL 类别的流量

报告 - 您无法生成涵盖此视图中数据的报表。但是，您可以利用网络使用情况报告来了解有关网络流量的详细信息。要计划报告，请从 **Strata Cloud Manager** > **Reports**（报告）菜单中，单击 图标，然后从类型下拉列表中选择网络使用情况。

Activity Insights：项目

在何处可以使用？	需要提供什么？
• Prisma Access （利用 *Strata Cloud Manager* 或 *Panorama* 配置管理） • NGFW （利用 *Strata Cloud Manager* 或 *Panorama* 配置管理）	您必须至少拥有以下许可证之一才能使用 Activity Insights： ❑ Prisma Access ❑ AIOps for NGFW Free (use the AIOps for NGFW Free app) 或 AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro

通过使用 Strata Cloud Manager 监控您的动态特权访问项目活动，获得 Prisma Access Agent 部署的可见性。



- **Projects**（项目）表提供了动态特权访问用户使用 Prisma Access 访问的项目概览。选择任何项目的名称可查看其详细信息页面。
- 该项目的详细信息页面显示：
  - **Overview**（概览）— 查看此项目所选时间范围内允许的最大用户数和峰值用户数。
  - **IP Pools Utilization**（IP 池利用率）— 查看此项目中池正在使用的 IP 数量和仍然可用的 IP 数量。
  - **Connected Users**（已连接用户）— 查看所选时间范围内已连接用户的图形。
  - **Connected Users by Location Group**（按位置组已连接用户）— 按所在的 Prisma Access 位置组查看用户数。

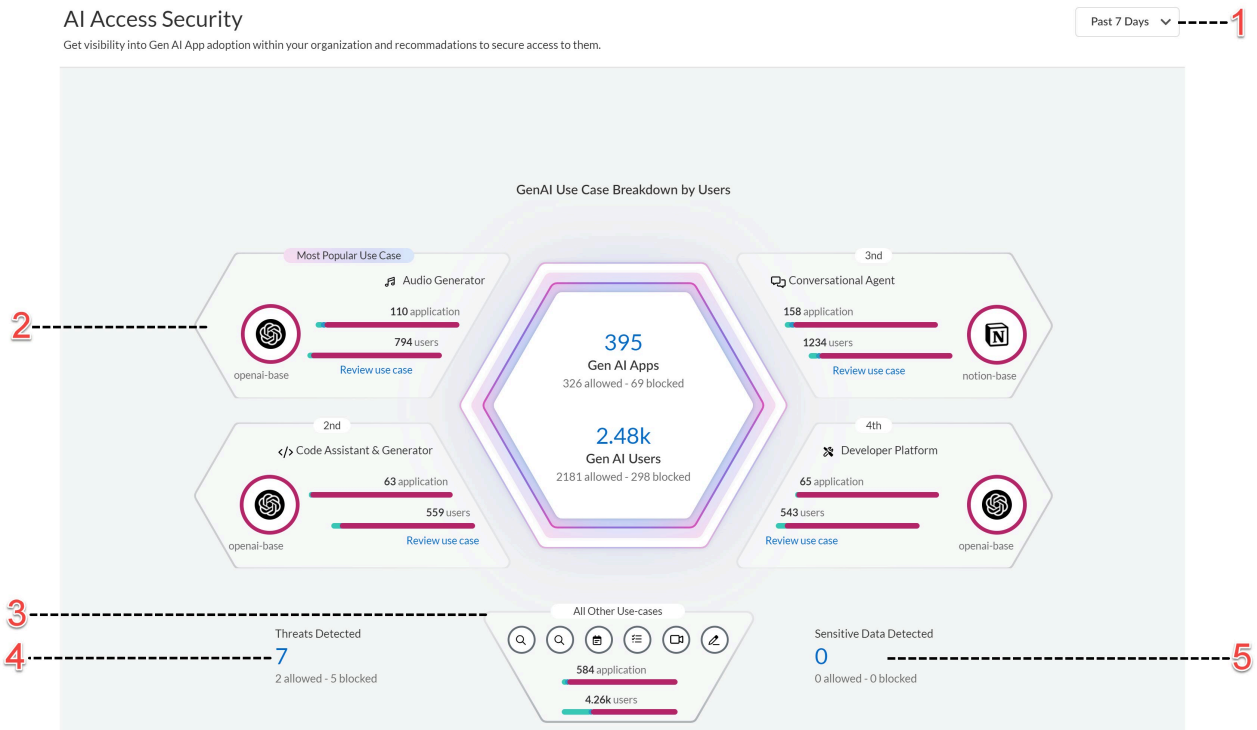
见解：AI Access

在何处可以使用？	需要提供什么？
• Prisma Access （利用 *Strata Cloud Manager* 或 *Panorama* 配置管理） • NGFW （利用 *Strata Cloud Manager* 或 *Panorama* 配置管理）	以下许可证之一： ❑ AI Access Security 许可证 ❑ CASB-PA 许可证 ❑ CASB-X 许可证 有关支持 AI Access Security 的许可证的更多信息，请单击此处。

生成人工智能 (GenAI) 应用程序是能够响应用户提示生成文本、图像、视频和其他形式数据并根据用户数据输入不断学习的人工智能应用程序。它们的使用正以惊人的速度增长，并为企业提供了无限的机会。然而，GenAI 应用程序不断改进的性质给企业和安全管理员带来了新的危险 — 您如何确保您的员工不会将敏感或专有数据暴露给 GenAI 应用程序？

Palo Alto Networks 推出了 AI Access Security，以确保在整个组织内安全采用 GenAI 应用程序。

使用 AI Access Security Insights 指示板筛选网络上的 GenAI 应用程序使用情况。AI Access Security Insights 指示板提供深入的详细信息，帮助您了解哪些 GenAI 应用程序正在被使用以及由谁使用。



要了解有关如何保护您的敏感数据免受 *GenAI* 应用程序攻击的更多信息，请单击此处。

见解：AI 运行时安全性

在何处可以使用？	需要提供什么？
• Prisma Access （利用 *Strata Cloud Manager* 或 *Panorama* 配置管理） • NGFW （利用 *Strata Cloud Manager* 或 *Panorama* 配置管理）	❑ 激活您的 AI 运行时安全许可证 ❑ AI 运行时安全设置先决条件 ❑ 在 SCM 中注册并激活云帐户

Palo Alto Networks AI Runtime Security 是一种专门构建的集中式安全解决方案，通过利用实时、AI 驱动的安全性来保护您组织的云网络架构免受特定于 AI 和常规的网络攻击。它可以保护您的新一代 AI 模型、AI 应用程序和 AI 数据集免受网络威胁，例如即时注入、敏感数据泄露、不安全输出（例如恶意软件和 URL）以及模型 DoS 攻击。

使用 AI Runtime Security Insights 指示板了解您的云网络攻击面并保护您的云资产免受恶意威胁。

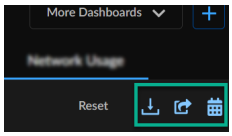
要了解有关如何保护您的 *AI* 和非 *AI* 网络流量免受潜在攻击的更多信息，请单击此处。

指示板：Strata Cloud Manager

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW，包括由 软件 NGFW 积分提供资助的项目 • Prisma SD-WAN	这些许可证中的每一个都包括 Strata Cloud Manager 访问权限： ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro ❑ Prisma SD-WAN 访问某些指示板所需的其他许可证和先决条件是： ❑ 云交付安全服务 (CDSS) ❑ ADEM 可观测性 ❑ 有权查看指示板的角色 → 您可用的特性和功能Strata Cloud Manager取决于您使用的许可证。

Strata Cloud Manager 提供了一组交互式指示板，让您全面了解网络中运行的应用程序、ION 设备、威胁、用户和安全订阅。指示板可让您了解部署中的运行状况、安全态势和活动，帮助您预防或解决网络中的性能和安全漏洞。指示板支持扩展到支持云管理的 Palo Alto Networks 产品和订阅，以及其他来源，包括 Traps、Cortex XDR、Prisma SaaS 和 Proofpoint。您经常看到的数据取决于您的订阅。您可以查看每个指示板主题，了解该指示板的许可证要求、角色权限是否会影响可见的数据，以及了解每个订阅解锁的不同类型的数据。

您可以从左侧导航窗格上的 **Dashboards**（指示板）菜单访问指示板。SASE Health 指示板默认固定在登录页面上。单击 **More Dashboards**（更多指示板），然后选择或清除指示板名称旁边的复选框，以将指示板固定或取消固定到指示板登录页面。您还可以使用构建我的指示板选项构建您自己的指示板。一些指示板还可以选择下载和共享报告，您可以离线共享并安排定期更新。要查看指示板是否支持报告，请检查以下图标：



与 Cloud Identity Engine 集成

我们建议设置 Cloud Identity Engine（目录同步）以充分利用指示板。Cloud Identity Engine 是一款免费的 Palo Alto Networks 应用程序，它允许其他应用程序以只读方式访问您的 Active Directory 信息，并使您能够：

- 获取用户活动数据 - Cloud Identity Engine 使您能够指定要为其运行报告的用户。
- 通过设置 Cloud Identity Engine，您可以轻松安全地与组织的其他成员共享报告，并可以轻松地将收件人添加到计划报告中。系统会根据 Cloud Identity Engine 检查您的报告收件人，如果未找到匹配项，则会执行额外的验证步骤，即根据与您的支持帐户关联的电子邮件地址域检查电子邮件地址域。这些检查可确保报告不会被发送到您的组织之外。

集成的应用程序必须部署在同一区域。您可以随时转到中心，将 Cloud Identity Engine 与 Prisma Access 或 Directory Sync 集成。# 集成 Palo Alto Networks 应用程序

支持指示板

产品中的某些指示板支持正在等待迁移到 *Strata Cloud Manager*。

功能	支持平台				许可证和其他要求	汇总数据的范围
	Prisma Access（云托管）	**Prisma Access**（Par 托管）*	**AIOps for N(**	**Prisma SASE** 多租户平台		
	• Prisma Access (Managed by Strata Cloud Manager) 和 Prisma Access (Managed by Panorama) 的文档		• AIOps for NGFW 的文档	• Prisma SASE 多租户平台文档		
SASE 运行状况	是	是	是		• ADEM 可观测性 • 人工智能驱动的 ADEM	
最佳实践	是	否	PAN OS 版本：10.0 或更高版本	是	[仅适用于 AIOps for NGFW] 在设备中启用遥测共享	• Prisma Access (Manage 每个租户 • AIOps for NGFW：与 AIOps for NGFW 实例关联的每个 NGFW/ Panorama
合规性摘要	否	否	是	否	[仅适用于 AIOps for NGFW] 在设备中启用遥测共享	AIOps for NGFW：与 AIOps for NGFW 实例关联的每个 NGFW / Panorama
按需 BPA	否	否	是	否	TSF	AIOps for NGFW：与 AIOps for NGFW 实例关联的每

功能	支持平台				许可证和其他要求	汇总数据的范围
	Prisma Access（云托管）	Prisma Access（Par 托管）*	AIOps for N(	Prisma SASE 多租户平台		
						个 NGFW / Panorama
执行摘要	是	是	是	是	• Strata Logging Service 许可证 • 威胁防御许可证 • URL 筛选许可证 • WildFire 许可证 • Enterprise DLP 许可证	每个 Strata Logging Service 租户
WildFire	是	否	是	是**	WildFire 许可证	每个租户服务组 (TSG)
DNS 安全	是	是	是	是**	DNS Security 许可证	每个租户服务组 (TSG)
日志查看器	是	是	是	是	Strata Logging Service 许可证	每个 Strata Logging Service 租户
IOC 搜索	是	否	是	是**	在搜索中查看趋势图的要求： • DNS 许可证 • WildFire 许可证 • Strata Logging Service 许可证	

功能	支持平台				许可证和其他要求	汇总数据的范围
	Prisma Access（云托管）	Prisma Access（Par 托管）*	AIOps for N(	Prisma SASE 多租户平台		
					• URL 筛选	
下载/共享/计划	是	是	是	是		请参阅本表格中相应的功能列
Saas Security	是	否	否	否	• SaaS Security 许可证 • Strata Logging Service	每个 Prisma Access 租户
DLP 事件	是	否	否	否	Enterprise DLP 许可证	每个 Prisma Access 租户
设备运行状况	否	否	是	否	• [仅适用于 AIOps for NGFW] 在设备中启用遥测共享	AIOps for NGFW：关联 AIOps for NGFW 实例的每个 NGFW/ Panorama
安全态势洞察	否	否	是	否		AIOps for NGFW：关联 AIOps for NGFW 实例的每个 NGFW/ Panorama
高级威胁防护	否	否	是	否	• Threat Prevention 或 Advanced Threat Prevention 许可证 • Strata Logging Service	每个 Strata Logging Service 租户

功能	支持平台				许可证和其他要求	汇总数据的范围
	Prisma Access（云托管）	Prisma Access（Par 托管）*	AIOps for N(	Prisma SASE 多租户平台		
IoT Security	是	是	是	否	IoT Security 许可证	每个 IoT Security 租户
Prisma SD-WAN	否	否	否	是	Prisma SD-WAN 许可证	每个 Prisma SD-WAN 租户
PAN-OS CVE	否	是	是		[仅适用于 AIOps for NGFW] 在设备中启用遥测共享	• AIOps for NGFW：与 AIOps for NGFW 实例关联的每个 NGFW / Panorama • 使用 API 访问的 PSIRT CVE 数据库
CDSS 采用	是	是	是		[仅适用于 AIOps for NGFW] 在设备中启用遥测共享	AIOps for NGFW：与 AIOps for NGFW 实例关联的每个 NGFW / Panorama
功能采用	否	是	是		[仅适用于 AIOps for NGFW] 在设备中启用遥测共享	AIOps for NGFW：与 AIOps for NGFW 实例关联的每个 NGFW / Panorama

Prisma Access（Panorama 托管）* -

- 对于托管在非美洲地区的 Strata Logging Service 的 Prisma Access（Panorama 托管）用户，您需要同意允许 Prisma Access 读取和处理来自美洲以外地区的 Strata Logging Service 的数据。

查看并接受指示板主页上的隐私声明，以表示您的同意并查看更多指示板和日志。只有应用程序、实例和帐户管理员可以看到并接受隐私声明。

- Prisma Access（Panorama 托管）多租户环境不支持指示板。

是* -“是”表示支持所有版本的 Prisma Access 和 PAN-OS。

是**- 在多租户平台上，租户被标识为租户服务组 (TSG)，并分配有 TSG ID。每个客户支持门户 (CSP) 可以关联一个或多个租户。指示板中显示的数据取决于以下场景：

- 您从应用中访问指示板的应用程序需要得到 TSG 支持，并通过 SASE 平台或中心上的租户视图进行访问。
- 您已使用中心内的通用服务将设备与您的租户关联。
- 验证您的租户是否与 CSP 具有一对一或多对一映射。
  - 如果您的租户与 CSP 有一对一映射，您可以查看所有来源的指示板数据（例如，在 WildFire 指示板中，显示来自 Palo Alto Networks 防火墙、Prisma Access、Traps、Cortex XDR、Prisma SaaS、Proofpoint 和手动上传的样本数据）。
  - 如果每个 CSP 关联多个租户，则指示板仅显示与特定租户关联的 Prisma Access、Palo Alto Networks 防火墙和 Panorama 设备的数据，而不显示来自其他来源的数据。

AIOps for NGFW* - AIOps for NGFW 中可用的指示板取决于您是否拥有免费或高级许可层级。

指示板构建自定义指示板

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW，包括由 软件 NGFW 积分提供资助的项目 • Prisma SD-WAN	这些许可证中的每一个都包括 Strata Cloud Manager 访问权限： ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro ❑ Prisma SD-WAN 提高可见性所需的其他许可证和先决条件是： ❑ 用于解锁指示板中某些小部件的许可证 ❑ 具有查看指示板权限的角色 → 您可用的特性和功能Strata Cloud Manager取决于您使用的许可证。

除了默认指示板之外，您还可以创建自定义指示板，以使用小部件了解网络中您感兴趣的区域。小部件是用于创建指示板的组件。小部件被分类并存储在小部件库中。单击 **Dashboards**（指示板）**> +**，并从下拉列表中选择一个类别来查看小部件。小部件库中可用的小部件取决于您的安全服务订阅。例如，如果您有 AIOps for NGFW Premium 和 Advanced WildFire 许可证，则可以查看并使用 WildFire 类别下的所有小部件来创建指示板。

这些是可用于创建指示板的小部件类别。请参阅下面的链接来了解访问这些类别下的小部件的许可要求，然后了解它们。

- 指示板高级威胁防护
- 指示板DNS 安全
- 指示板WildFire

创建指示板

您可以在自定义指示板中添加最多 10 个小部件，并为每个用户创建 10 个自定义指示板。指示板和小部件可以随时定制。您可以自定义小部件磁贴、描述、显示或隐藏筛选器、指示板设置（如布局、指示板名称和描述），还可以在指示板中包含筛选器。

STEP 1 | 单击 **Dashboards**（指示板） **> +**。

STEP 2 | 输入指示板的名称。

STEP 3 | 从小部件库下拉菜单中选择一个小部件类别。

STEP 4 | 将小部件添加到指示板 - 将鼠标悬停在小部件上即可了解有关该小部件的信息。将小部件拖放到指示板画布上。

您可以将更多相同或不同类型的小部件从另一个小部件类别添加到指示板画布。

STEP 5 | 切换 **Sample Data**（示例数据）和 **Real Data**（真实数据）视图以了解指示板小部件的界面。示例数据可帮助您直观地了解指示板的外观以及您可以看到的信息类型。使用真实数据选项来查看部署的实际数据。

STEP 6 | （可选）您可以在编辑器视图中自定义指示板：

- 重新排列指示板中的小部件 - 选择小部件并将其拖放到画布中的所需位置。
- 编辑小部件 - 使用每个小部件右上角的编辑图标来编辑小部件设置。可用的设置取决于小部件，并且在所有小部件中都不相同。例如，您可以编辑小部件名称、描述和选项来筛选和排序小部件中的数据（例如判定、操作）。

您可以在编辑器视图中或保存指示板后编辑小部件设置。

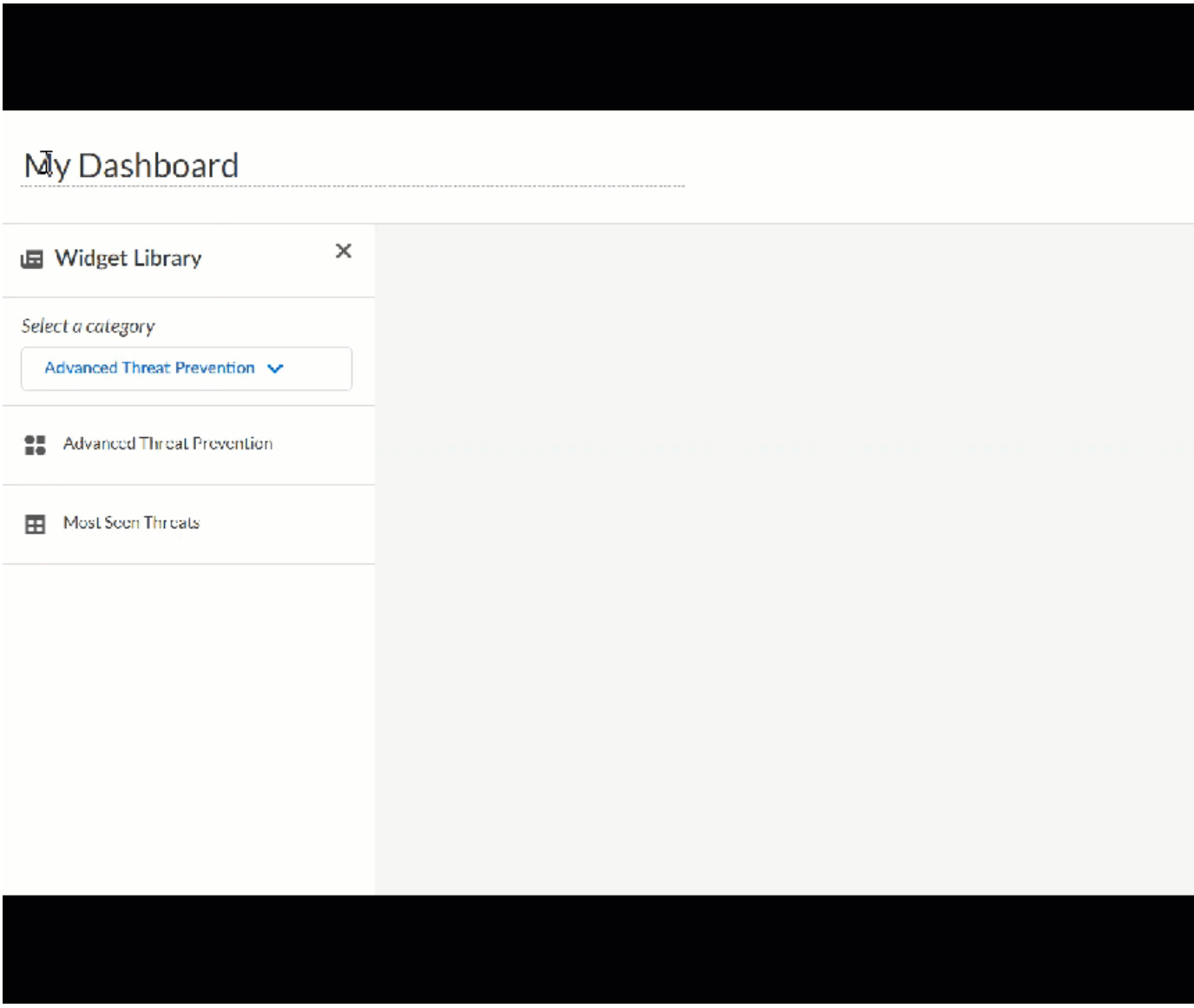
STEP 7 | 保存指示板，然后单击页面顶部的 **Go to see dashboard**（前往查看指示板）以打开指示板。

STEP 8 | （可选）保存指示板后，您可以：

- 更改您想要查看指示板数据的时间范围。

  您保存指示板后才能更改时间。在编辑器视图中，时间范围默认为 24 小时。

- 使用编辑或删除图标来修改或删除自定义指示板。



指示板设备运行状况

在何处可以使用？	需要提供什么？
• NGFW，包括由 软件 NGFW 积分提供资助的项目	❑ Strata Cloud Manager Essentials ❑ AIOps for NGFW Premium 或 Strata Cloud Manager Pro → 您可用的特性和功能Strata Cloud Manager取决于您使用的许可证。

- 要开始，请单击 **Dashboards**（仪表板） > **Device Health**（设备运行状况）。

该指示板显示什么？

指示板显示已载入租户的所有防火墙的聚合数据，并且还发送遥测数据。

设备运行状况指示板根据已安装的 NGFW 的运行状况评分显示您的部署的累积运行状况和性能。设备运行状况由运行状况评分的严重程度 (0-100) 及其对应的运行状况等级（良好、一般、较差、严重）决定。运行状况分数是根据打开的警报的优先级、数量、类型和状态计算的。

如何使用指示板上的数据？

此指示板可帮助您：

- 通过查看历史运行状况评分数据，了解您在一段时间内所做的部署改进。
- 缩小部署中需要关注的设备范围，并确定问题的优先顺序以解决这些问题。

此指示板不支持报告功能（下载、共享和计划报告）。

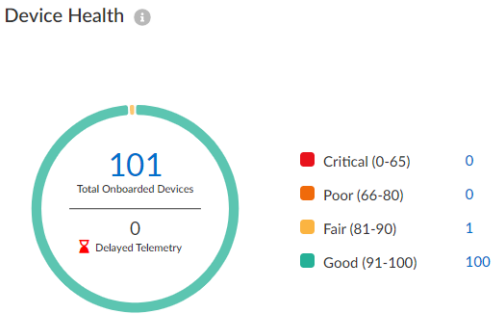
设备运行状况指示板：设备运行状况评分

在何处可以使用？	需要提供什么？
• NGFW，包括由 软件 NGFW 积分提供资助的项目	☐ Strata Cloud Manager Essentials ☐ AIOps for NGFW Premium 或 Strata Cloud Manager Pro → 您可用的特性和功能Strata Cloud Manager取决于您使用的许可证。

- 单击 **Dashboards**（指示板） > **Device Health**（设备运行状况）以查看指示板。

指示板小部件显示：

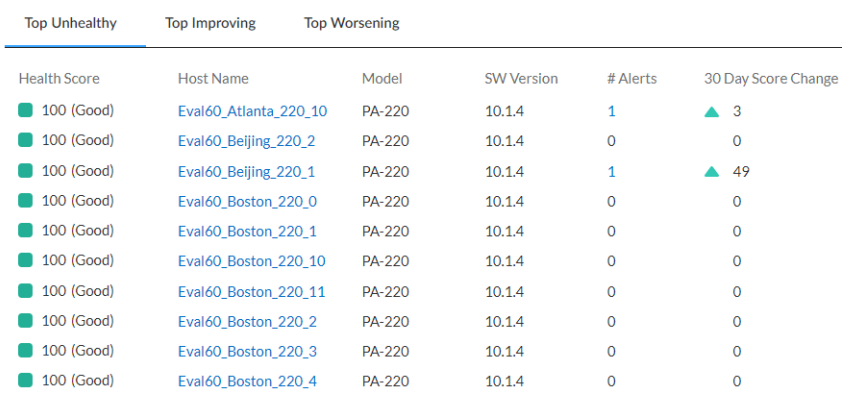
- 已加入的 NGFW 总数。
- 超过 12 小时未发送遥测数据的设备数量。
- 部署中的已载入设备的运行状况评分的严重性。单击数字链接可了解设备详细信息、设备运行状况统计信息以及设备上需要注意的警报。



设备运行状况指示板：设备统计信息

在何处可以使用？	需要提供什么？
• NGFW，包括由 软件 NGFW 积分提供资助的项目	☐ Strata Cloud Manager Essentials ☐ AIOps for NGFW Premium 或 Strata Cloud Manager Pro → 您可用的特性和功能Strata Cloud Manager取决于您使用的许可证。

- 单击 **Dashboards**（指示板） > **Device Health**（设备运行状况）以查看指示板。



Health Score	Host Name	Model	SW Version	# Alerts	30 Day Score Change
100 (Good)	Eval60_Atlanta_220_10	PA-220	10.1.4	1	▲ 3
100 (Good)	Eval60_Beijing_220_2	PA-220	10.1.4	0	0
100 (Good)	Eval60_Beijing_220_1	PA-220	10.1.4	1	▲ 49
100 (Good)	Eval60_Boston_220_0	PA-220	10.1.4	0	0
100 (Good)	Eval60_Boston_220_1	PA-220	10.1.4	0	0
100 (Good)	Eval60_Boston_220_10	PA-220	10.1.4	0	0
100 (Good)	Eval60_Boston_220_11	PA-220	10.1.4	0	0
100 (Good)	Eval60_Boston_220_2	PA-220	10.1.4	0	0
100 (Good)	Eval60_Boston_220_3	PA-220	10.1.4	0	0
100 (Good)	Eval60_Boston_220_4	PA-220	10.1.4	0	0

运行状况不佳的主要设备

这些是您的部署中运行状况和性能问题最多的设备。您还可以深入了解设备详细信息和设备上的警报。修复关键警报以改善运行状况评分和部署运行状况。

主要改进

查看 30 天内运行状况分数有所提高的前 10 台设备（与设备当前运行状况分数相比）。

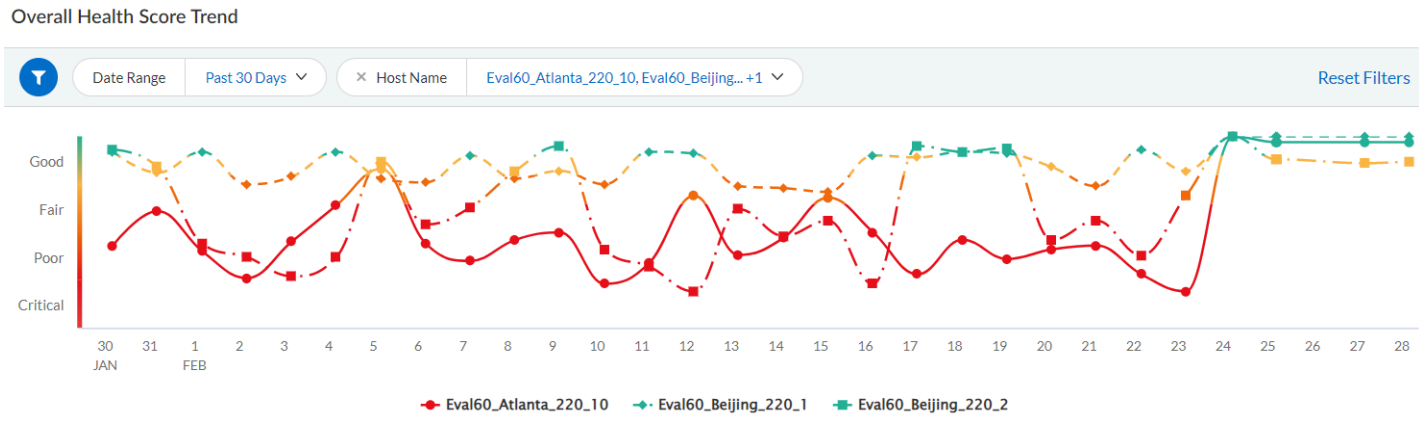
主要恶化

检查 30 天时间范围内的设备运行状况。这些是与设备当前运行状况评分相比运行状况评分下降最多的 10 台设备。

设备运行状况指示板：分数趋势

在何处可以使用？	需要提供什么？
• NGFW，包括由 软件 NGFW 积分提供资助的项目	☐ Strata Cloud Manager Essentials ☐ AIOps for NGFW Premium 或 Strata Cloud Manager Pro → 您可用的特性和功能Strata Cloud Manager取决于您使用的许可证。

- 单击 **Dashboards**（指示板） > **Device Health**（设备运行状况）以查看指示板。



该图表显示所选时间段内的部署运行状况趋势。将鼠标悬停在触发点上即可了解导致运行状况评分严重程度的设备。您可以查看按主机名、型号或软件版本筛选的一个或多个设备的趋势。

指示板执行摘要

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW，包括由 软件 NGFW 积分提供资助的项目 • Prisma SD-WAN	这些许可证中的每一个都包括 Strata Cloud Manager 访问权限： ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro ❑ Prisma SD-WAN 提高可见性所需的其他许可证和先决条件是： ❑ 用于解锁指示板中某些小部件的许可证 ❑ 具有查看指示板权限的角色 → 您可用的特性和功能Strata Cloud Manager取决于您使用的许可证。

- 要开始，请单击 **Strata Cloud Manager** > **Dashboards**（指示板） > **More Dashboards**（更多指示板） > **Executive Summary**（执行摘要）。

该指示板显示什么？

该指示板显示每个 *Strata Logging Service* 租户的聚合数据。

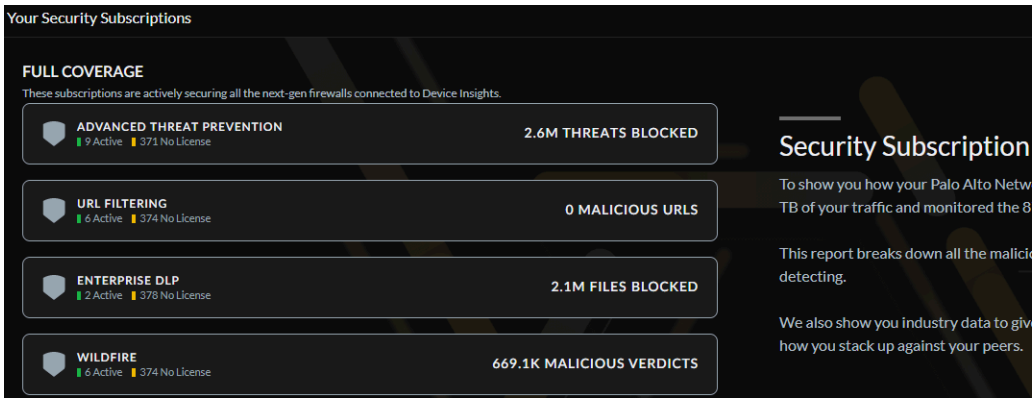
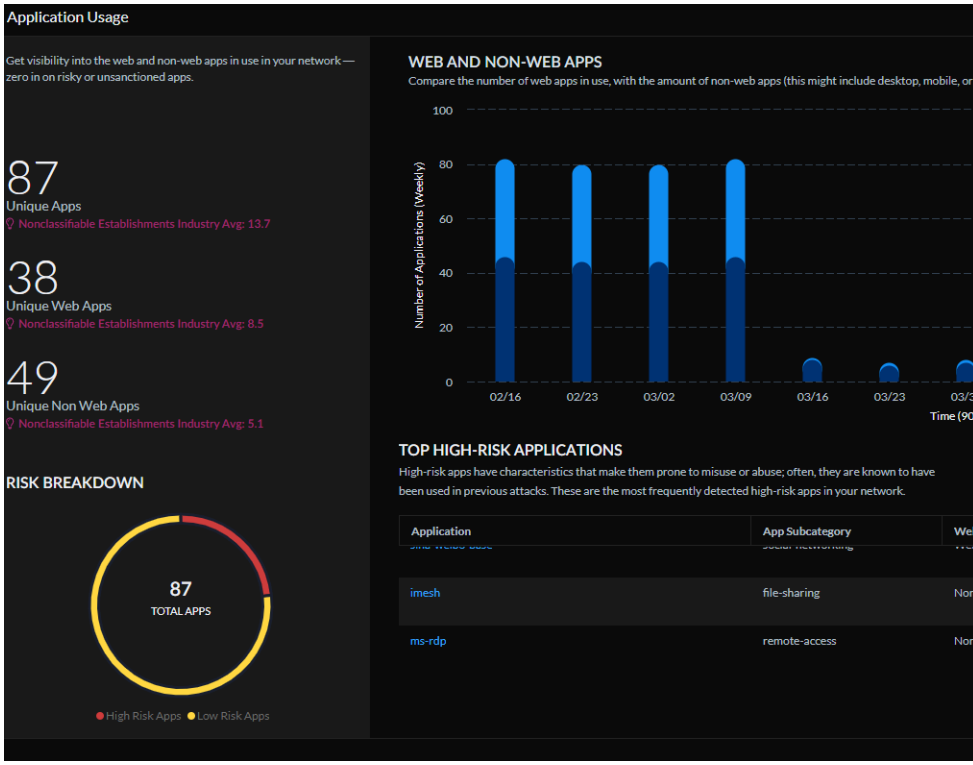
执行摘要指示板显示您的 Palo Alto Networks 安全订阅如何保护您。此报告详细分析这些订阅检测到的网络中的恶意活动：**WildFire**、**Advanced Threat Prevention**、 **URL** 筛选和 **Enterprise DLP**。指示板显示了这些服务中每一项服务的数据，并提供了安全服务指示板的链接，以便更深入地进行进一步调查。

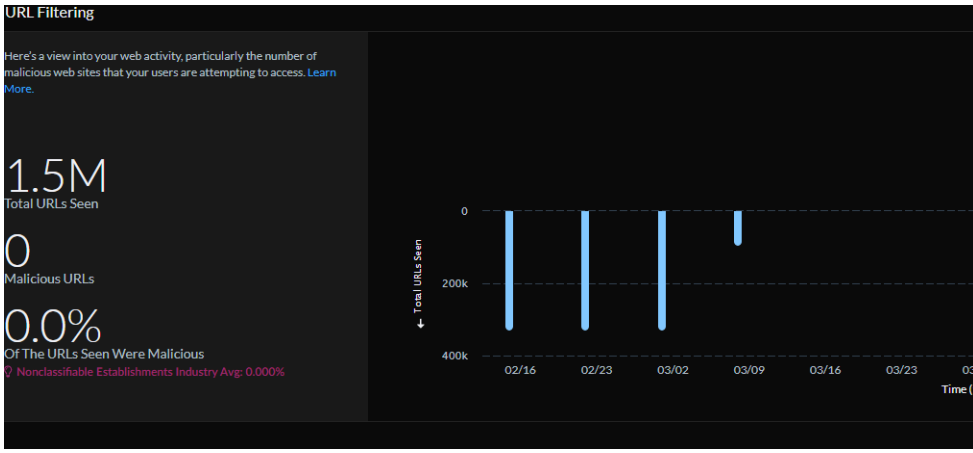
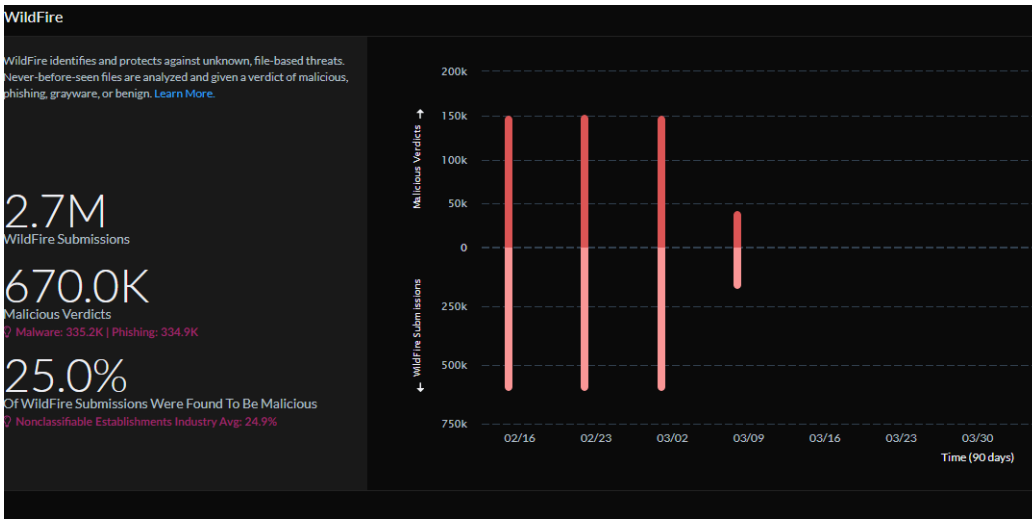
此指示板支持报告。指示板右上方的这些图标 表示此指示板支持报告。您可以共享、下载和安排包含此指示板显示的数据的报告。

如何使用指示板中的数据？

- 查看活动 Palo Alto Networks 订阅检测到的所有恶意活动。查看是否需要优化订阅设置或安全规则设置以消除任何安全漏洞。
- 向您展示行业数据，让您了解您所面临的威胁形势以及您与同行的竞争情况。

指示板提供以下数据。

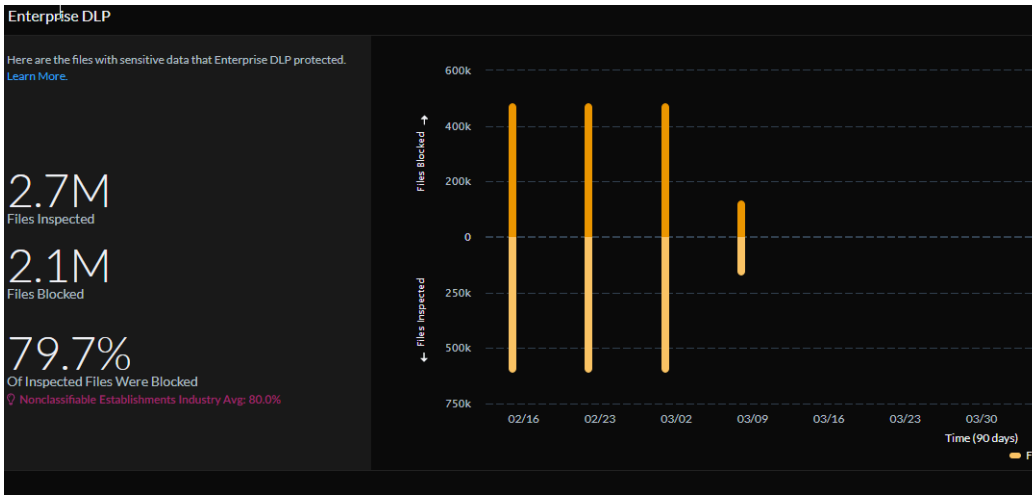
执行摘要指示板：您的安全订阅	此报告提供您的订阅正在检测和阻止的恶意活动的数字： • 高风险应用 • 严重威胁（漏洞利用、恶意软件和 C2） • 恶意 Web 活动 • 基于文件的威胁（包括从未见过的威胁） • 数据丢失 
执行摘要指示板：**Application Usage**（应用程序使用）	查看高风险应用程序的流量日志，了解如何加强安全态势。 
执行摘要指示板：高级威胁防护	检查允许大多数威胁的安全策略规则。查看这些规则，了解可以在哪些地方启用更严格的威胁强制执行。了解更多信息。

需要 *Advanced Threat Prevention* 许可证。	
执行摘要指示板：**URL** 筛选 需要高级 *URL* 筛选许可证。	查看网络中的恶意 Web 活动，特别是您的用户试图访问的恶意网站的数量。 
执行摘要指示板：**WildFire** 需要 *Advanced WildFire* 许可证。	此指示板中的同行数据可让您了解您所在行业的威胁形势，以及您的安全覆盖范围与类似组织的比较情况。此行业数据也会显示您未使用的订阅;这有助于您查看是否存在可以增加覆盖范围以缩小安全漏洞的地方。 这里是此指示板提供的数据类型的特写-这里可以看到 WildFire 为保护您的网络和行业所做的工作。了解详细信息。# 
执行摘要指示板：**Enterprise DLP**	了解您的 Palo Alto Networks Enterprise DLP 服务如何通过实施 Data Security 标准来保护您的数据。指示板可让您深入了解 DLP 阻止大多数上传的应用程序以及网络中 DLP 阻止的文件总数。您

需要 *Enterprise DLP* 许可证。

还可以使用这些数据与行业同行进行比较，并对您的安全态势标准进行基准测试。

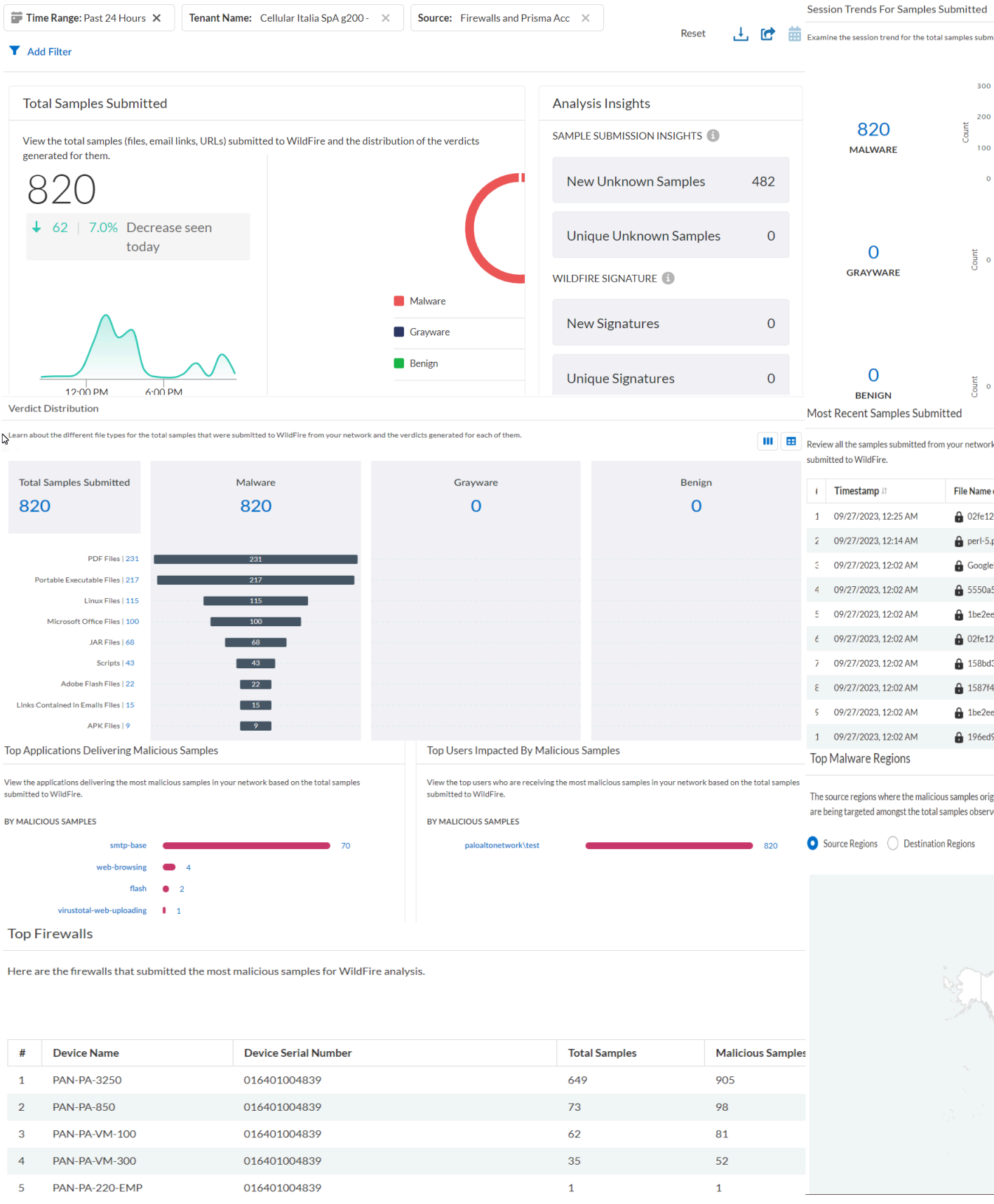
查看应用程序和源用户名，以更好地了解 DLP 事件的起源并对其进行管理。



指示板WildFire

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW，包括由 软件 NGFW 积分提供资助的项目	这些许可证中的每一个都包括 Strata Cloud Manager 访问权限： ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro 提高可见性所需的其他许可证和先决条件是： ❑ 有权查看指示板的角色 ❑ Advanced WildFire → 您可用的特性和功能Strata Cloud Manager取决于您使用的许可证。

- 要开始，请单击 **Strata Cloud Manager** > **Dashboards**（指示板） > **More Dashboards**（更多指示板） > **WildFire**。



#	Device Name	Device Serial Number	Total Samples	Malicious Samples
1	PAN-PA-3250	016401004839	649	905
2	PAN-PA-850	016401004839	73	98
3	PAN-PA-VM-100	016401004839	62	81
4	PAN-PA-VM-300	016401004839	35	52
5	PAN-PA-220-EMP	016401004839	1	1

该指示板显示什么？

指示板显示每个租户服务组 *(TSG)* 的聚合数据。指示板显示与租户关联的 *Prisma Access*、*Palo Alto Networks* 防火墙和 *Panorama* 设备上的数据，前提是您的租户与您的客户支持门户帐户进行一对一映射。如果每个客户支持门户关联了多个租户，则指示板不会显示来自其他来源的数据。

WildFire 指示板可向您展示 WildFire 如何防御隐藏在文件和可执行文件中的全新恶意软件。此指示板支持报告。指示板右上方的这些图标 表示此指示板支持报告。您可以共享、下载和安排包含此指示板显示的数据的报告。

如何使用指示板上的数据？

使用此指示板可以

- （需要 AIOps for NGFW Premium 许可证）监控 WildFire 提交的内容，并获取提交给 WildFire 云进行分析的 WildFire 样本的详细信息
- 查看目标用户的详细信息、交付文件的应用程序、提交样本进行分析的防火墙以及与文件命令和控制活动相关的所有 URL。
- （需要 AIOps for NGFW Premium 许可证）查看 WildFire 日志和分析报告，并根据该报告优化部署的 WildFire 设置。

Wildfire 指示板：筛选器

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW，包括由 软件 NGFW 积分提供资助的项目	这些许可证中的每一个都包括 Strata Cloud Manager 访问权限： ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro 提高可见性所需的其他许可证和先决条件是： ❑ 有权查看指示板的角色 ❑ Advanced WildFire → 您可用的特性和功能Strata Cloud Manager取决于您使用的许可证。

WildFire 指示板提供了这些筛选选项，以缩小指示板中的特定数据的范围。

- 时间范围 — 从过去 **24** 小时、过去 **7** 天、过去 **30** 天或自定义时间范围中选择，以显示特定时间范围内的数据。

- 租户名称 — 显示指示板数据的租户。
- 来源 — 指示板数据的范围来自 Prisma Access 和 Palo Alto Networks 防火墙。
- 示例 — 从公共或私有选项中选择，查看从 Wildfire 公共云或私有云环境提交的数据。
- 判定 — 查看在 WildFire 分析中被确定为良性、恶意软件或灰色软件的样本。
- 操作 — 从允许或阻止选项中进行选择，以显示您的策略规则允许或阻止的 WildFire 样本。
- 文件类型 — 根据 WildFire 分析的样本的文件类型查看数据。了解 WildFire 分析支持的文件类型。
- 文件哈希 — 查看 WildFire 分析的文件哈希数据。下面列出了 WildFire 为分析的每个文件生成的哈希版本：
  - **SHA-1** — 显示文件的 SHA-1 值。
  - **SHA-256** — 显示文件的 SHA-256 值。
  - **MD5** — 显示文件的 MD5 信息。
- 应用程序名称 — 根据应用程序交付的示例筛选数据。
- 来源区域 — 筛选以查看从特定位置发送的样本。
- 目标区域 — 筛选以查看在特定位置收到的样本。
- 用户名 — 输入用户名以筛选目标在您的网络中提供样本的用户的数据。
- 设备序列号 — 筛选提交样本以进行 WildFire 分析的设备的数据。

Wildfire 指示板：提交的样本总数

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW，包括由 软件 NGFW 积分提供资助的项目	这些许可证中的每一个都包括 Strata Cloud Manager 访问权限： ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro 提高可见性所需的其他许可证和先决条件是： ❑ 有权查看指示板的角色 ❑ Advanced WildFire → 您可用的特性和功能Strata Cloud Manager取决于您使用的许可证。

- 单击 **Dashboards**（指示板） > **More Dashboards**（更多指示板） > **WildFire**以查看指示板。

所选时间段内提交用于 WildFire 分析的样本总数。小部件显示每个来源提交的样本数和为样本生成的判定。小部件还显示提交用于 WildFire 分析的样本中的峰值。调查恶意软件样本中的峰值，并采取措施减轻威胁对网络的影响。

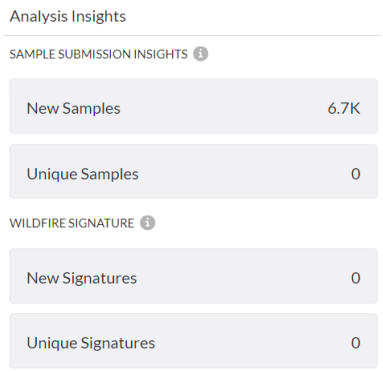
Wildfire 指示板：Analysis Insights

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW，包括由 软件 NGFW 积分提供资助的项目	这些许可证中的每一个都包括 Strata Cloud Manager 访问权限： ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro 提高可见性所需的其他许可证和先决条件是： ❑ 有权查看指示板的角色 ❑ Advanced WildFire → 您可用的特性和功能Strata Cloud Manager取决于您使用的许可证。

- 单击 **Dashboards**（指示板） > **More Dashboards**（更多指示板） > **WildFire**以查看指示板。

深入了解从您的网络提交的独特 WildFire 样本和生成的签名。使用这些数据来了解在所选时间范围内仅在您的网络中观察到的新威胁，以及您的网络受生成的签名保护的次数。

- 唯一未知样本 — 从您的网络提交给 WildFire 的样本数量，这些样本仅在您的网络中可见，WildFire 之前未知，并且在其他公共或私有订阅源中不可用。
- 新的未知样本 — 从您的网络向 WildFire 提交的、之前未知的 WildFire 的新样本数量（使用不同的 SHA256）。
- 唯一签名 — 根据您的环境特有的样本生成的签名数量。
- 新签名 — WildFire 从您上传的所有样本中创建的新签名数量。



Wildfire 指示板：提交样本的会话趋势

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW，包括由 软件 NGFW 积分提供资助的项目	这些许可证中的每一个都包括 Strata Cloud Manager 访问权限： ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro 提高可见性所需的其他许可证和先决条件是： ❑ 有权查看指示板的角色 ❑ Advanced WildFire → 您可用的特性和功能Strata Cloud Manager取决于您使用的许可证。

- 单击 **Dashboards**（指示板） > **More Dashboards**（更多指示板） > **WildFire**以查看指示板。

检查从您的网络提交到 WildFire 的所有样本的趋势，以及对这些样本的判定。您可以执行对这些样本执行 IOC 搜索，了解样本在网络中的历史以及全局分析结果。

Wildfire 指示板：判定分布

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW，包括由 软件 NGFW 积分提供资助的项目	这些许可证中的每一个都包括 Strata Cloud Manager 访问权限： ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro 提高可见性所需的其他许可证和先决条件是： ❑ 有权查看指示板的角色 ❑ Advanced WildFire → 您可用的特性和功能Strata Cloud Manager取决于您使用的许可证。

- 单击 **Dashboards**（指示板） > **More Dashboards**（更多指示板） > **WildFire**以查看指示板。

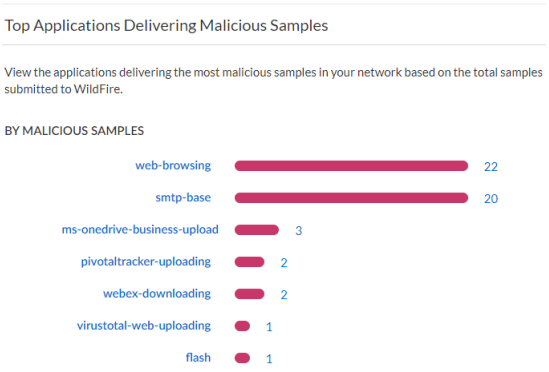
详细了解 WildFire 在您的网络中首次检测到的净新样本的判定 。重点关注最常隐藏恶意软件的样本类型。单击链接可以了解有关示例的更多信息。

Wildfire 指示板：传播恶意样本的主要应用程序

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW，包括由 软件 NGFW 积分提供资助的项目	这些许可证中的每一个都包括 Strata Cloud Manager 访问权限： ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro 提高可见性所需的其他许可证和先决条件是： ❑ 有权查看指示板的角色 ❑ Advanced WildFire → 您可用的特性和功能Strata Cloud Manager取决于您使用的许可证。

- 单击 **Dashboards**（指示板） > **More Dashboards**（更多指示板） > **WildFire**以查看指示板。

查看在您的网络中提供最多恶意样本的应用程序的详细信息。单击恶意样本数量可查看样本详细信息。

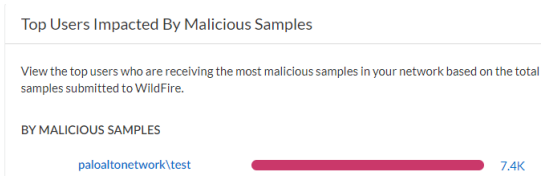


Wildfire 指示板：受恶意样本影响的主要用户

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW，包括由 软件 NGFW 积分提供资助的项目	这些许可证中的每一个都包括 Strata Cloud Manager 访问权限： ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro 提高可见性所需的其他许可证和先决条件是： ❑ 有权查看指示板的角色 ❑ Advanced WildFire → 您可用的特性和功能Strata Cloud Manager取决于您使用的许可证。

- 单击 **Dashboards**（指示板） > **More Dashboards**（更多指示板） > **WildFire**以查看指示板。

这显示了在您的网络中最常用于传递恶意样本的用户帐户。单击用户名即可调查用户活动模式。



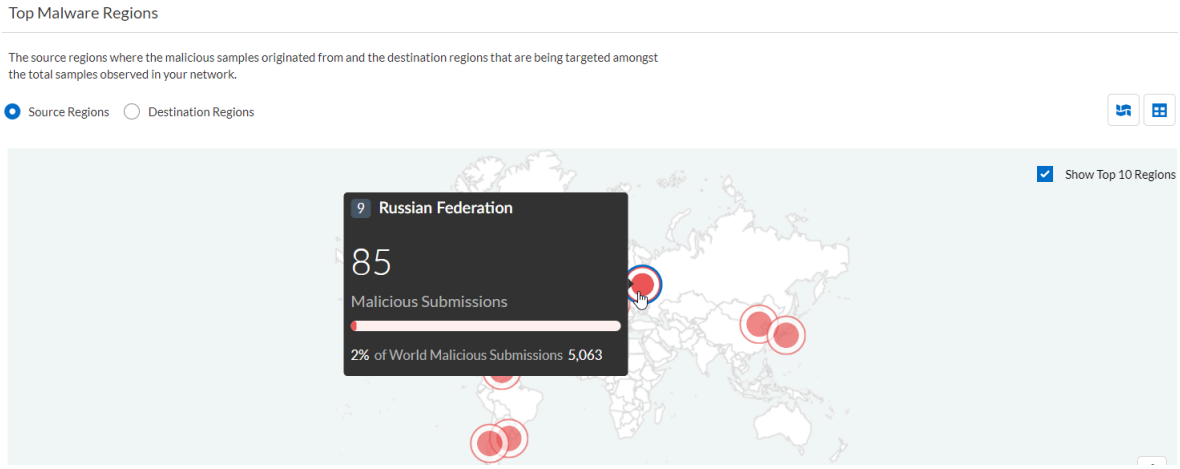
Wildfire 指示板：主要恶意软件区域

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama or Strata Cloud Manager)	这些许可证中的每一个都包括 Strata Cloud Manager 访问权限：

在何处可以使用？	需要提供什么？
• NGFW，包括由 软件 NGFW 积分提供资助的项目	❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro 提高可见性所需的其他许可证和先决条件是： ❑ 有权查看指示板的角色 ❑ Advanced WildFire → 您可用的特性和功能Strata Cloud Manager取决于您使用的许可证。

- 单击 **Dashboards**（指示板） > **More Dashboards**（更多指示板） > **WildFire**以查看指示板。

查看恶意样本的来源或在您的网络中传递到的位置。您可以以地图或表格格式查看源区域和目标区域的样本计数。使用此选项可以缩小恶意软件攻击的区域和恶意软件攻击的类型。



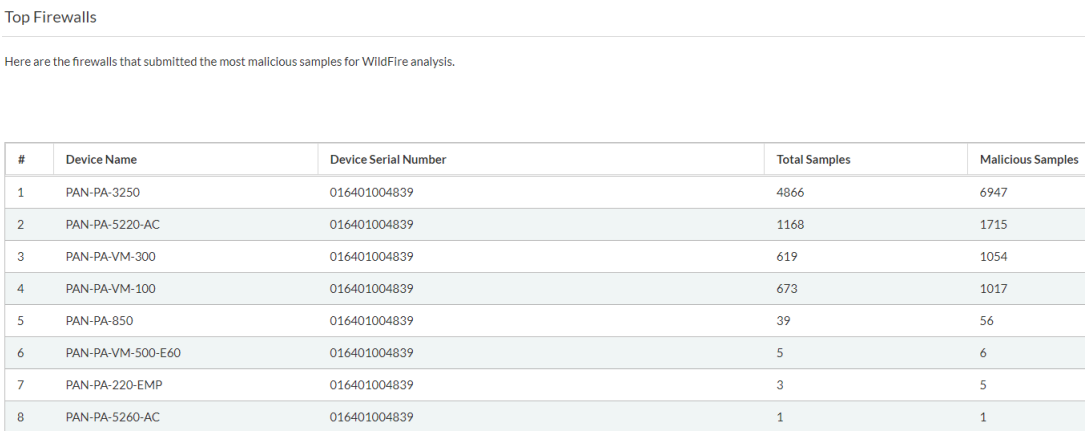
Wildfire 指示板：顶级防火墙

在何处可以使用？	需要提供什么？
• NGFW，包括由 软件 NGFW 积分提供资助的项目	这些许可证中的每一个都包括 Strata Cloud Manager 访问权限： ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro 提高可见性所需的其他许可证和先决条件是： ❑ 有权查看指示板的角色

在何处可以使用？	需要提供什么？
	❑ Advanced WildFire → 您可用的特性和功能Strata Cloud Manager取决于您使用的许可证。

- 单击 **Dashboards**（指示板） > **More Dashboards**（更多指示板） > **WildFire**以查看指示板。

查看向 WildFire 分析提交最多恶意样本的防火墙。检查这些防火墙以追踪受影响的端点并重新配置策略规则以减轻威胁并在源头遏制恶意文件。



Top Firewalls

Here are the firewalls that submitted the most malicious samples for WildFire analysis.

#	Device Name	Device Serial Number	Total Samples	Malicious Samples
1	PAN-PA-3250	016401004839	4866	6947
2	PAN-PA-5220-AC	016401004839	1168	1715
3	PAN-PA-VM-300	016401004839	619	1054
4	PAN-PA-VM-100	016401004839	673	1017
5	PAN-PA-850	016401004839	39	56
6	PAN-PA-VM-500-E60	016401004839	5	6
7	PAN-PA-220-EMP	016401004839	3	5
8	PAN-PA-5260-AC	016401004839	1	1

指示板DNS 安全

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW，包括由 软件 NGFW 积分提供资助的项目	这些许可证中的每一个都包括 Strata Cloud Manager 访问权限： ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro 提高可见性所需的其他许可证和先决条件是： ❑ 有权查看指示板的角色 ❑ DNS Security 或 Advanced DNS Security → 您可用的特性和功能Strata Cloud Manager取决于您使用的许可证。

- 要开始，请单击 **Strata Cloud Manager** > **Dashboards**（指示板） > **More Dashboards**（更多指示板） > **DNS Security**。

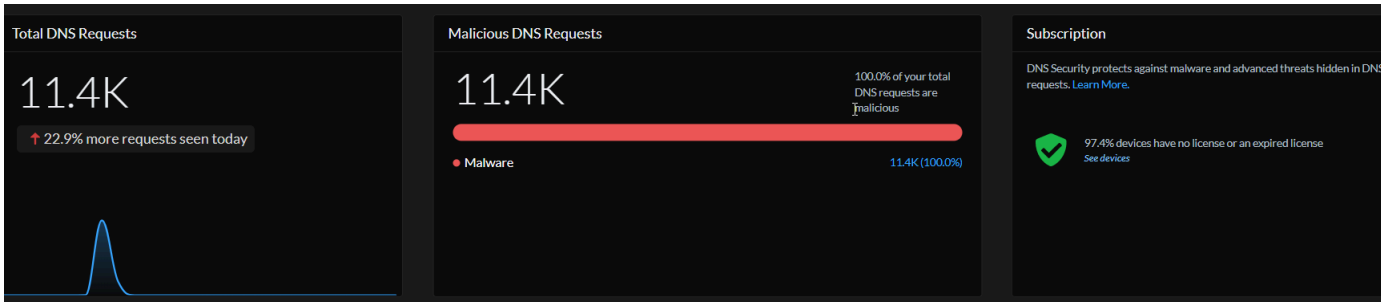
该指示板显示什么？

指示板显示每个租户服务组 *(TSG)* 的聚合数据。指示板显示与您的租户关联的 *Prisma Access*、*Palo Alto Networks* 防火墙和 *Panorama* 设备中的数据。

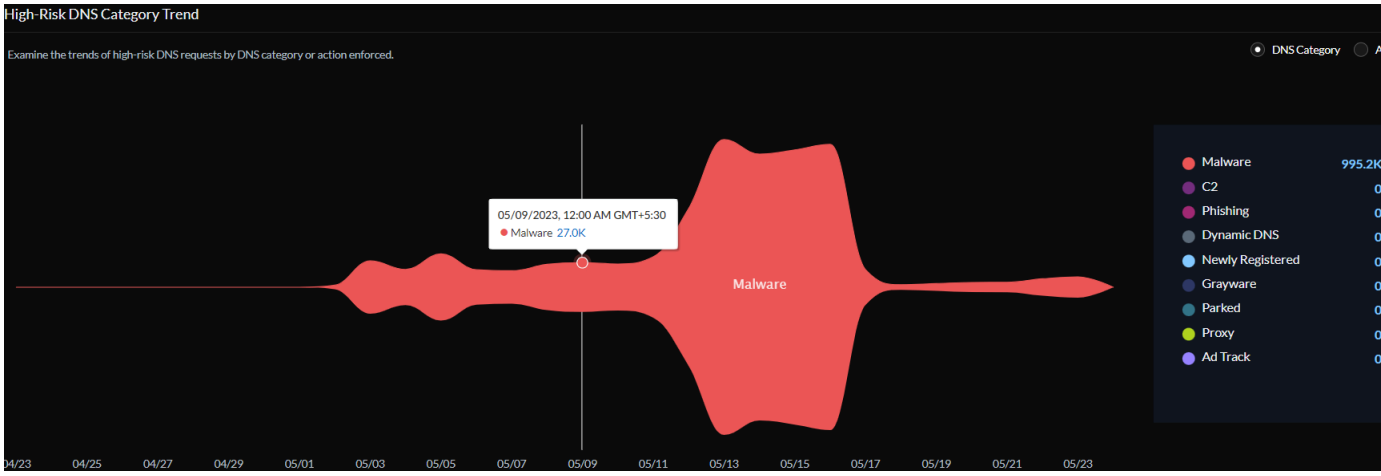
新的 DNS Security 指示板显示您的 DNS Security 订阅如何保护您免受使用 DNS 的高级威胁和恶意软件的攻击。您还可以按时间范围、采取的操作、域、解析器 IP 和 DNS 类别筛选指示板上显示的信息。数据显示在指示板上的源和租户名称显示在租户名称和源筛选器中。您可以查看：DNS 请求统计信息和趋势

- **DNS** 请求总数 — 显示 DNS Security 处理的 DNS 请求总数。折线图根据用户定义的时间范围绘制 DNS 请求的数量。自定义时间范围将相应地更新折线图。
- 恶意 **DNS** 请求 — 显示一个堆叠条形图，显示被归类为恶意的 DNS 请求。单击数字链接可查看 DNS 请求的详细信息。

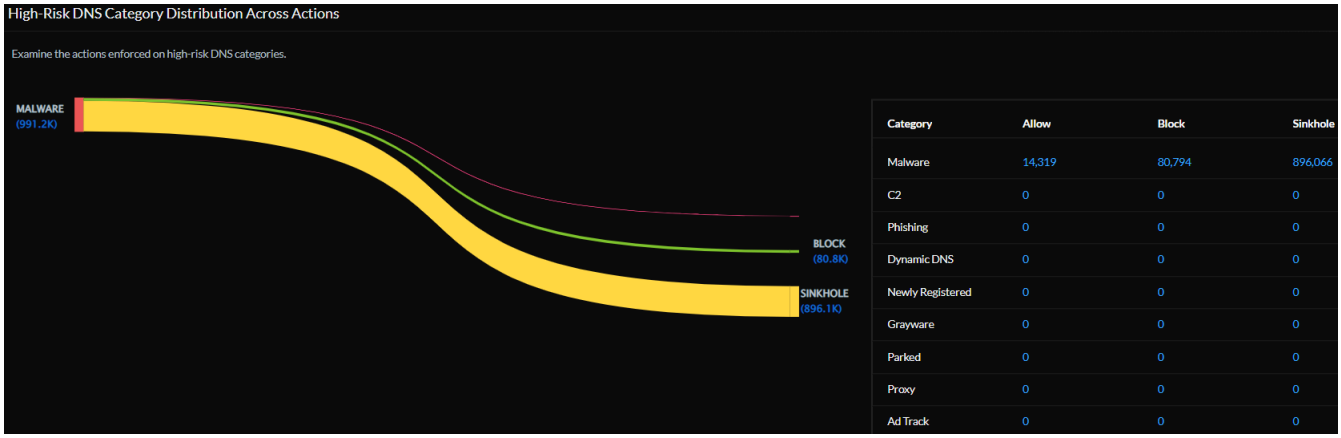
- 订阅 — 显示网络中具有活动 DNS Security 订阅的设备数量。未配备 DNS Security 或订阅已过期的设备的百分比也会显示在完整列表的链接中。



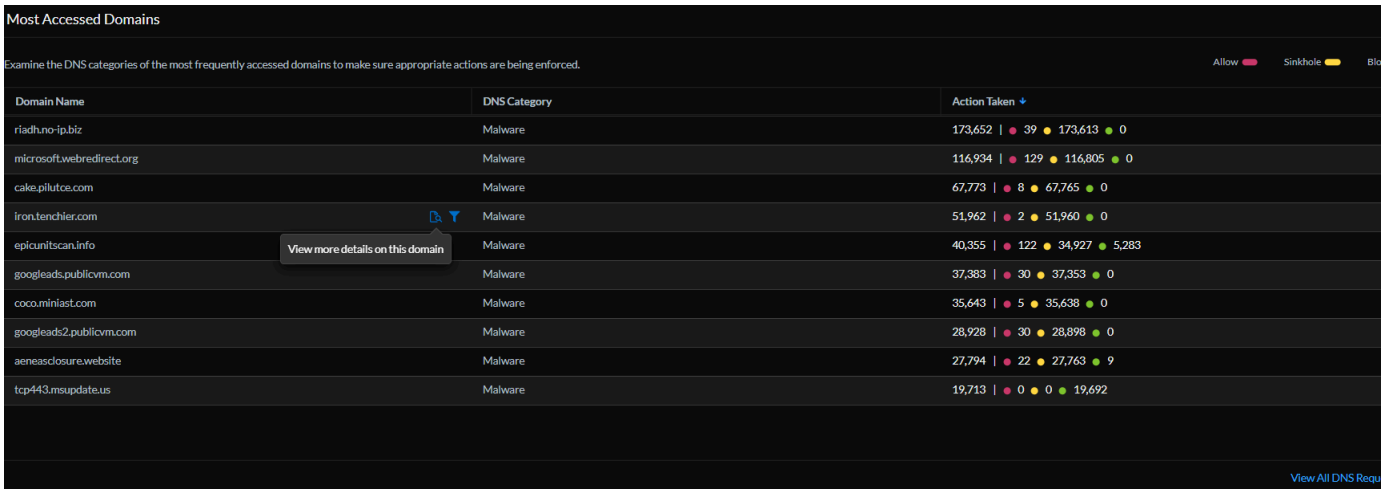
- 高风险 **DNS** 类别趋势 - 根据 DNS 类别或针对它们采取的操作检查高风险 DNS 请求的趋势。将鼠标悬停在特定的流上可以打开一个弹出窗口，显示请求的数量或强制执行的操作类型。



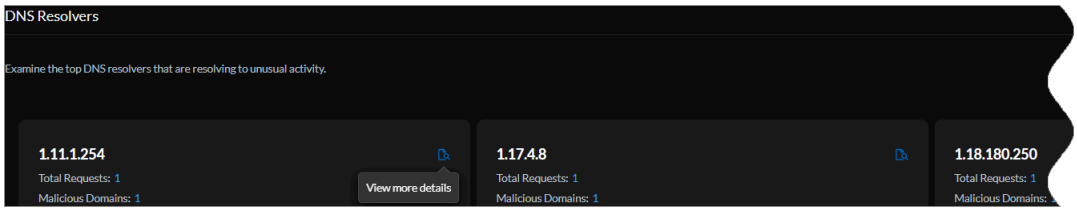
- 高风险 **DNS** 类别在操作中的分布 — 检查防火墙针对特定高风险 DNS 类别所采取的操作。



- 最常访问的域 - 提供网络中最常请求的 10 个域的列表，以及 DNS 类别和所采取的操作。您可以查看更多详细信息和域的相关日志。选择 **View All DNS Requests**（查看所有 **DNS** 请求），查看已访问的域的完整列表。



- **DNS** 解析器 - 监控网络中的恶意和可疑 DNS 解析活动。查看解析到恶意域名的顶级 DNS 解析器以及正在解析少得可疑的 DNS 请求的解析器。单击搜索图标以查看有关工件（IP 地址）的更多详细信息。您可以查看网络中工件的历史记录和全局分析结果。

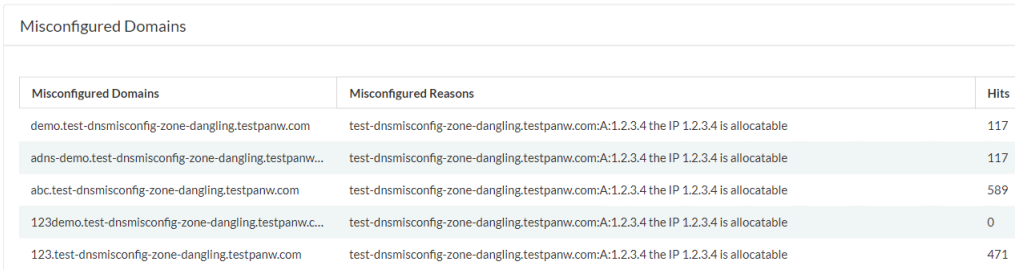


- 访问恶意域的用户 - 检查网络上试图解析恶意URL的主机名或域的主机。
- （需要 **Advanced DNS Security** 许可证）劫持域 - 提供由 Advanced DNS Security 确定的劫持域列表。每个条目都有一个分类原因和基于源 IP 的流量命中计数。

Hijacked Domains

Hijacked	Hits
xyz.test-ipv4-wildcard.hijacking.testpanw.com	117
www.test-ipv4-wildcard.hijacking.testpanw.com	118
www.test-cname-rrname-sub-wc.hijacking.testpanw.com	353
test.test-ipv4-wildcard.hijacking.testpanw.com	118
test-ipv6.hijacking.testpanw.com	469
test-ipv4.hijacking.testpanw.com	472
test-cname-rrname.hijacking.testpanw.com	234
test-cname-rrname-wc.hijacking.testpanw.com	117
qpwc.test-ipv4-wildcard.hijacking.testpanw.com	118

- （需要高级 DNS 安全许可证）错误配置的域 - -提供与用户指定的面向公众的父域关联的不可解析域的列表。对于每个条目，都有一个错误配置原因和基于源IP的流量命中计数。


Misconfigured Domains

Misconfigured Domains	Misconfigured Reasons	Hits
demo.test-dnsmisconfig-zone-dangling.testpanw.com	test-dnsmisconfig-zone-dangling.testpanw.com:A:1.2.3.4 the IP 1.2.3.4 is allocatable	117
adns-demo.test-dnsmisconfig-zone-dangling.testpanw...	test-dnsmisconfig-zone-dangling.testpanw.com:A:1.2.3.4 the IP 1.2.3.4 is allocatable	117
abc.test-dnsmisconfig-zone-dangling.testpanw.com	test-dnsmisconfig-zone-dangling.testpanw.com:A:1.2.3.4 the IP 1.2.3.4 is allocatable	589
123demo.test-dnsmisconfig-zone-dangling.testpanw.c...	test-dnsmisconfig-zone-dangling.testpanw.com:A:1.2.3.4 the IP 1.2.3.4 is allocatable	0
123.test-dnsmisconfig-zone-dangling.testpanw.com	test-dnsmisconfig-zone-dangling.testpanw.com:A:1.2.3.4 the IP 1.2.3.4 is allocatable	471

此指示板支持报告。指示板右上方的这些图标 表示此指示板支持报告。您可以共享、下载和安排包含此指示板显示的数据的报告。

如何使用指示板中的数据？

此指示板可帮助您：

- 检查 DNS 请求是如何处理和分类的
- 深入了解基于 DNS 的威胁
- 使用高级 DNS 安全检测来自被劫持和错误配置域的 DNS 请求

指示板AI 运行时安全性

Strata Cloud Manager (SCM) Command Center 指示板提供了集群和 VM 中部署的云工作负载的整合视图，例如 Pod、模型、应用程序、VM 和命名空间。

在何处可以使用？	需要提供什么？
• AI Runtime Security	❑ AI Runtime Security 许可证 ❑ AI Runtime Security 设置先决条件 ❑ 初始配置和载入 SCM 中的云帐户

发现云资源

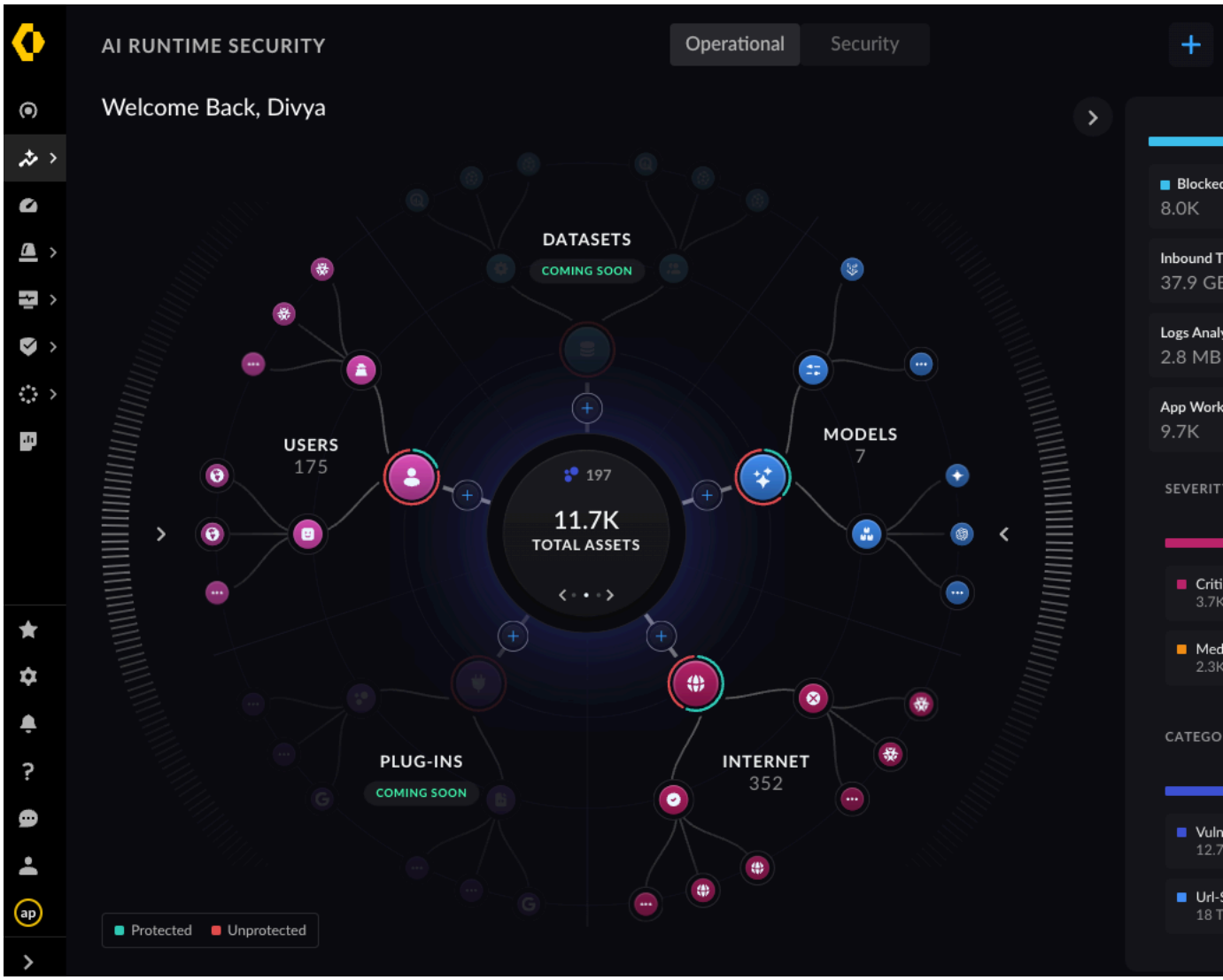
在 SCM 中成功载入云帐户并激活服务帐户后，SCM 指示板会提供云工作负载的统一实时资产发现。

云应用命令中心在 SCM 中的 **Insights**（见解）→ **AI Runtime Security** 下提供可操作的见解，以发现载入的云帐户中的所有云资产。

SCM 指示板上的资产发现分为操作视图和安全视图。

该发现根据威胁紧急性和风险类别（如漏洞检测、URL 安全和提示注入）显示威胁细分。

1. 操作视图是以下各项的聚合视图：
    1. 在载入的云环境中发现的资产的总数和明细
    2. 流量 - AI Runtime Security 实例保护的流量和未保护的流量
    3. 应用程序工作负载（容器、无服务器函数和 VM）
    4. 正在查询的 AI 模型
    5. 访问 Internet 目标的用户应用程序
    6. 应用程序用户 从外部应用程序访问的应用程序
    7. 入站和出站流量统计



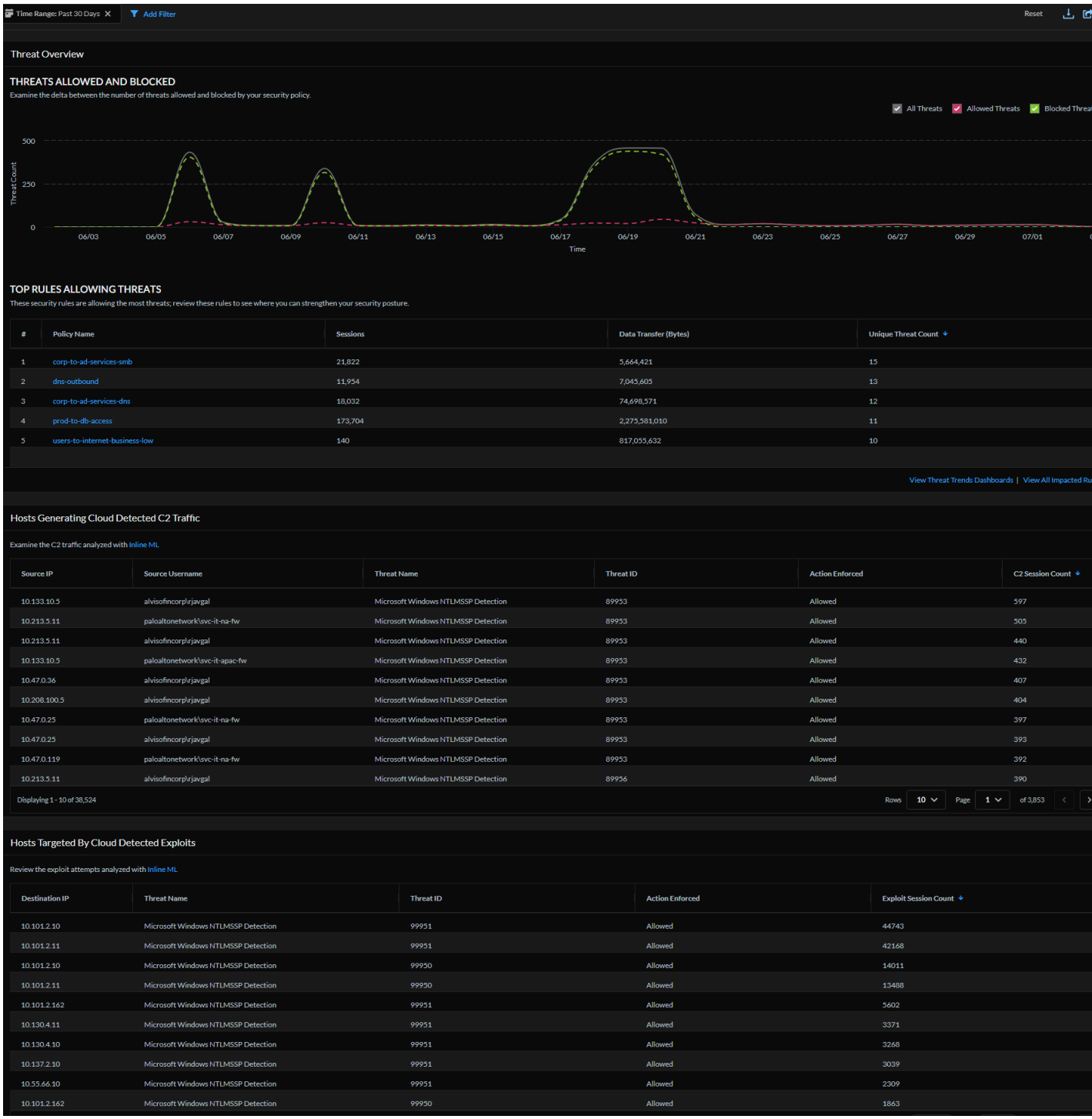
2. 在安全视图中：
   1. 您可以添加一个（“+”图标）AI Runtime Security 实例，以保护操作视图中标识的未受保护的网络流量。
   2. 如果 AI Runtime Security 实例保护已存在，则通过可用的 AI Runtime Security 实例重定向未受保护的流量。

接下来，检测用户应用程序、AI 模型和 Internet 之间有风险的网络流路径。要监控和保护您的云网络架构，请参阅 AI 流量网络风险分析和部署 AI 运行时安全实例。

指示板高级威胁防护

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW，包括由 软件 NGFW 积分提供资助的项目	这些许可证中的每一个都包括 Strata Cloud Manager 访问权限： ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro 提高可见性所需的其他许可证和先决条件是： ❑ 有权查看指示板的角色 ❑ Threat Prevention 或 Advanced Threat Prevention → 您可用的特性和功能Strata Cloud Manager取决于您使用的许可证。

- 单击 **Strata Cloud Manager** > **Dashboards**（指示板） > **More Dashboards**（更多指示板） > **Advanced Threat Prevention**以开始。



该指示板显示什么？

该指示板显示每个 *Strata Logging Service* 租户的聚合数据。

通过 Advanced Threat Prevention 指示板可深入了解网络中检测到的威胁，并识别增强安全态势的机会。使用内联云分析模型和从各种 Palo Alto Networks 服务收集的恶意流量数据生成的威胁

签名来检测威胁。此指示板提供允许和阻止的威胁的时间线视图，以及生成云检测到的 C2 流量的主机和云检测到的漏洞攻击目标主机的列表。

此指示板支持报告。指示板右上方的这些图标 表示此指示板支持报告。您可以共享、下载和安排包含此指示板显示的数据的报告。

如何使用指示板中的数据？

使用此指示板可以：

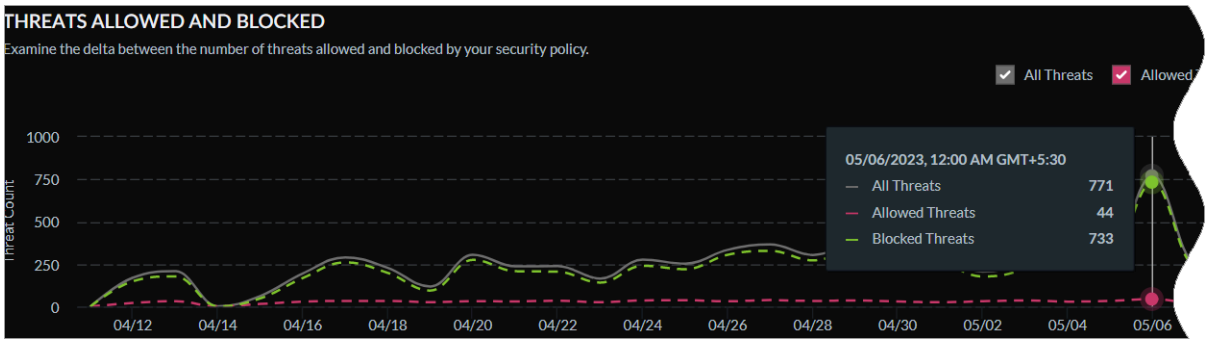
- 获取网络流量中的威胁可见性
- 分析威胁会话以提高策略规则的准确性
- 深入了解内联云分析检测到的实时威胁
- 从日志和云报告中获取威胁环境，并利用这些数据改进事件响应流程。

Advanced Threat Prevention 指示板：威胁概述

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW，包括由 软件 NGFW 积分提供资助的项目	这些许可证中的每一个都包括 Strata Cloud Manager 访问权限： ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro 提高可见性所需的其他许可证和先决条件是： ❑ 有权查看指示板的角色 ❑ Threat Prevention 或 Advanced Threat Prevention → 您可用的特性和功能Strata Cloud Manager取决于您使用的许可证。

- 单击 **Strata Cloud Manager** > **Dashboards**（指示板） > **More Dashboards**（更多指示板） > **Advanced Threat Prevention**，以查看该指示板。

比较安全规则允许和阻止的威胁之间的差异。

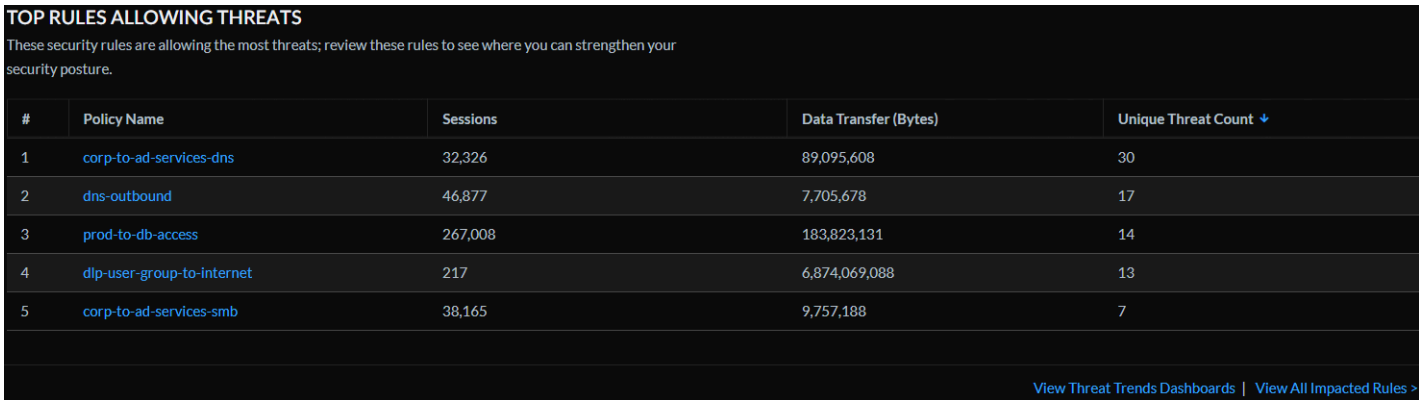


Advanced Threat Prevention 指示板：允许威胁的主要规则

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW，包括由 软件 NGFW 积分提供资助的项目	这些许可证中的每一个都包括 Strata Cloud Manager 访问权限： ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro 提高可见性所需的其他许可证和先决条件是： ❑ 有权查看指示板的角色 ❑ Threat Prevention 或 Advanced Threat Prevention → 您可用的特性和功能Strata Cloud Manager取决于您使用的许可证。

- 单击 **Strata Cloud Manager** > **Dashboards**（指示板） > **More Dashboards**（更多指示板） > **Advanced Threat Prevention**，以查看该指示板。

检查与安全策略规则匹配的威胁会话，查看是否需要修改策略规则以加强您的安全态势。您可以在 Activity Insights 中进一步分析威胁和匹配规则。



列	说明
策略名称	允许相应威胁的安全策略规则。
会话	与安全策略规则匹配的威胁会话数。
数据传输（字节）	与安全策略规则匹配的会话中流过的数据量。
唯一威胁计数	与安全策略规则匹配的威胁数量。

Advanced Threat Prevention 指示板：主机生成云检测到的 C2 流量

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW，包括由 软件 NGFW 积分提供资助的项目	这些许可证中的每一个都包括 Strata Cloud Manager 访问权限： ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro 提高可见性所需的其他许可证和先决条件是： ❑ 有权查看指示板的角色 ❑ Threat Prevention 或 Advanced Threat Prevention → 您可用的特性和功能Strata Cloud Manager取决于您使用的许可证。

- 单击 **Strata Cloud Manager** > **Dashboards**（指示板） > **More Dashboards**（更多指示板） > **Advanced Threat Prevention**，以查看该指示板。

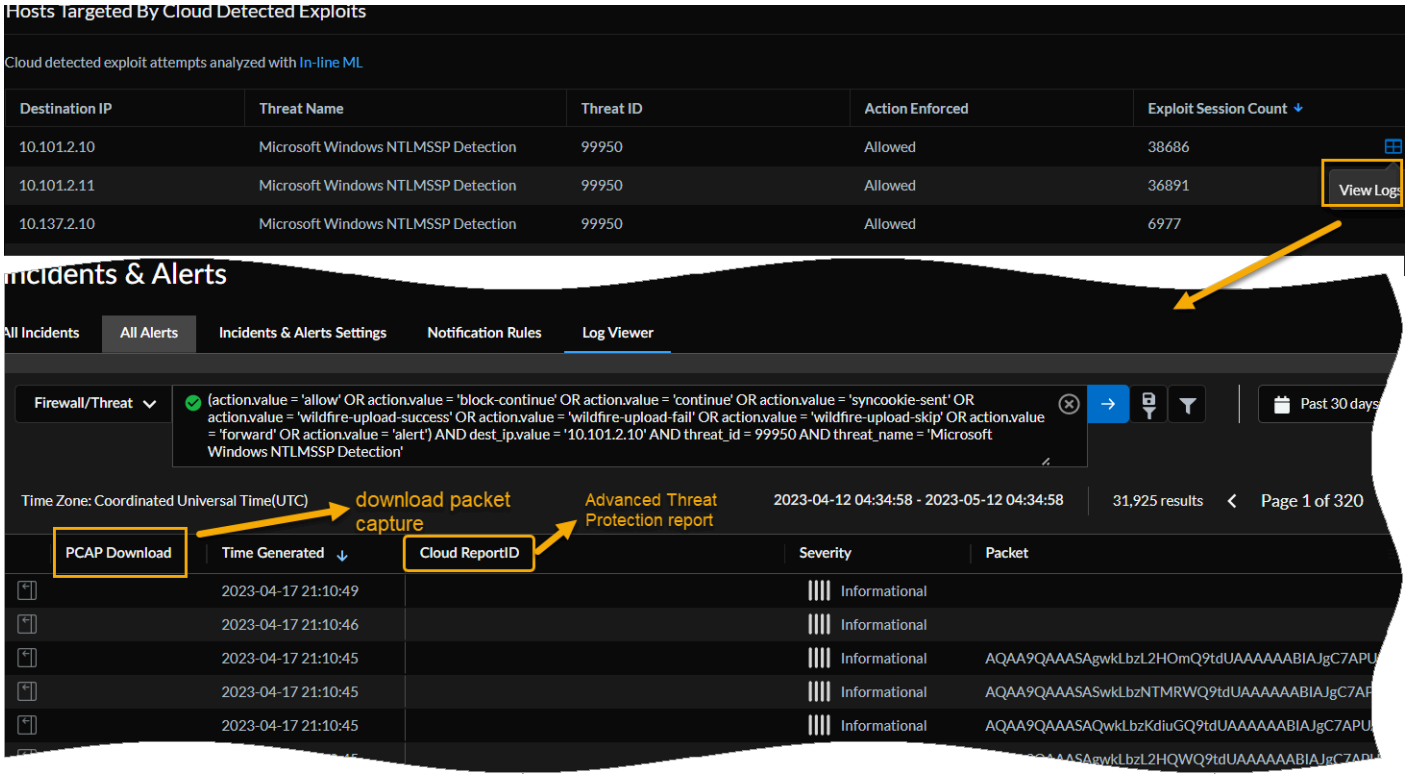
检查负责生成命令和控制 (C2) 流量的源 IP 和用户。Advanced Threat Prevention 使用基于云的引擎和云分析来检测和分析未知 C2 的流量和漏洞。单击源 IP 旁的搜索图标以查看与源 IP 相关的使用模式。日志查看器的上下文链接有助于分析威胁会话、下载数据包捕获和云报告以获取更多上下文，并利用 Palo Alto Networks 威胁分析数据和改进事件响应流程。

Advanced Threat Prevention 指示板：被云检测到的漏洞攻击的目标

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW，包括由 软件 NGFW 积分提供资助的项目	这些许可证中的每一个都包括 Strata Cloud Manager 访问权限： ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro 提高可见性所需的其他许可证和先决条件是： ❑ 有权查看指示板的角色 ❑ Threat Prevention 或 Advanced Threat Prevention → 您可用的特性和功能Strata Cloud Manager取决于您使用的许可证。

- 单击 **Strata Cloud Manager** > **Dashboards**（指示板） > **More Dashboards**（更多指示板） > **Advanced Threat Prevention**，以查看该指示板。

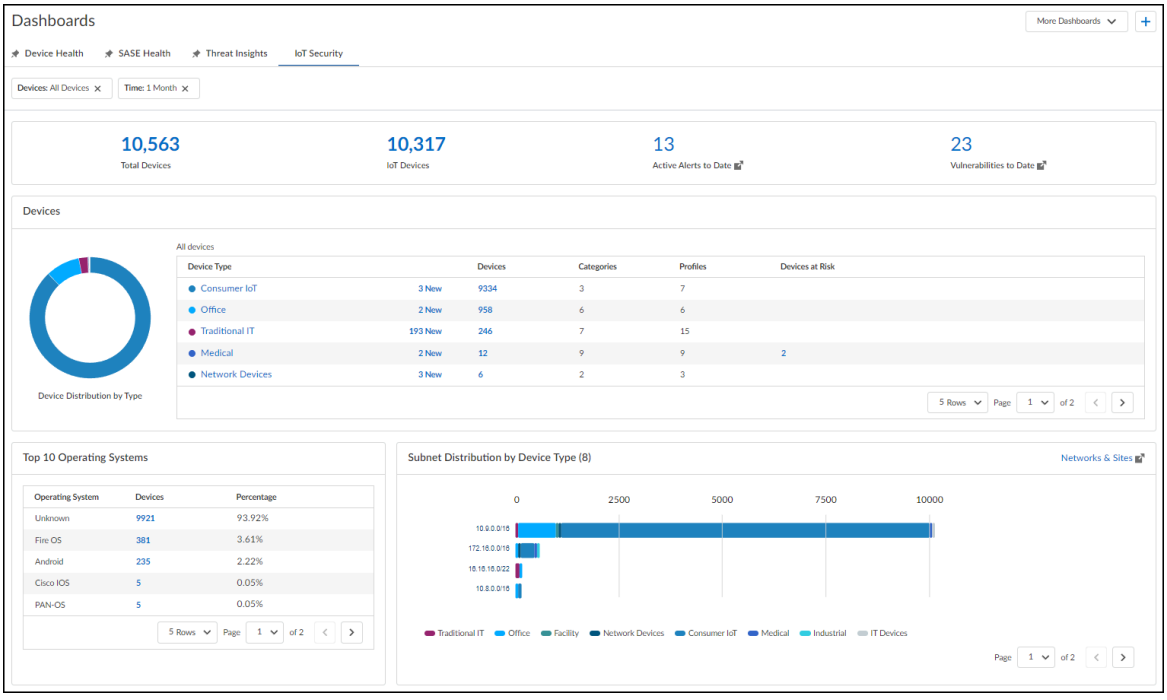
这些是漏洞攻击的目标 IP。Advanced Threat Prevention 使用基于云的引擎和内联云分析来检测和分析此流量。将鼠标悬停在目标IP地址上，然后单击搜索图标以查看与目标 IP 相关的使用模式。查看日志以了解威胁的背景。从日志中下载云报告和数据包捕获以获取更多上下文，并使用 Palo Alto Networks 威胁分析数据和威胁情报来改进您的事件响应流程。



指示板IoT Security

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW，包括由 软件 NGFW 积分提供资助的项目	这些许可证中的每一个都包括 Strata Cloud Manager 访问权限： ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro 提高可见性所需的其他许可证和先决条件是： ❑ 有权查看指示板的角色 ❑ IoT Security → 您可用的特性和功能Strata Cloud Manager取决于您使用的许可证。

要开始，请选择 **Dashboards**（指示板） > **More Dashboards**（更多指示板） > **IoT Security**。



该指示板显示什么？

IoT Security 指示板提供了有关网络上的设备、其设备配置文件和操作系统的信息，以及它们如何按设备类型在子网中分布。对于高级 IoT Security 产品（Enterprise IoT Security Plus、Industrial

IoT Security 或 Medical IoT Security），IoT Security 指示板还显示到目前为止的活动警报总数和漏洞总数。

蓝色格式的文本是交互式的。下面是当您单击时会发生的情况：

- 摘要（顶部）– **Total Devices**（设备总数）和 **IoT Devices**（IoT 设备）链接到 **Monitor**（监控） > **Assets**（资产）页面，应用筛选器显示所有设备或所有 IoT 设备的清单。到目前为止的活动警报和到目前为止的活动漏洞的蓝色文本将打开 IoT Security 门户中的相应页面。（当没有警报或漏洞时，数字为 0 且没有链接。）
- 设备 – 单击图表中的某个部分或设备类型列中的条目，放大查看所选类型中的设备类别，并从中查看所选类别中的设备配置文件。单击图表内的 **Back**（发挥），或单击表上方的痕迹导航可缩小到更广泛的设备分类级别。

  设备和风险设备列中的数字链接到 **Monitor**（监视） > **Assets**（资产）页面。Strata Cloud Manager 会自动应用筛选器来显示与所选列和行匹配的设备，根据显示的当前级别，筛选器可以是设备类型、类别名称或配置文件名称。

  您有时会看到 *IoT Security* 在网络上检测到的新设备数量。这些数字显示在“设备”列中数字的左边。如果 *IoT Security* 在指示板顶部设置的时间筛选器内首次在网络上检测到设备，则认为设备为“新建”。
- 前 10 个操作系统 – 设备列中的数字链接到 **Monitor**（监控） > **Assets**（资产）页面，并应用筛选器仅显示具有所选操作系统的设备。
- 按设备类型划分的子网分布 – 将光标悬停在子网的条形图上，查看子网中按设备类型分组的设备数量。此信息可帮助您确定是否在同一子网中混入了太多不相关的设备类型。例如，如果在一个子网中看到设施、工业和消费类 IoT 设备，您可能希望将每种类型的设备细分为各自独立的子网。单击 **Networks & Sites**（网络和站点）将启动一个新的浏览器窗口，并在 IoT Security 门户中打开 **Networks**（网络） > **Networks and Sites**（网络和站点） > **Networks**（网络）。

您如何使用此指示板中的数据？

使用此指示板中的数据了解网络上的设备：

Filters（筛选器）（页面顶部）

- 按设备类型和时间段（过去的年、月、周、日或小时）筛选指示板中显示的数据，以查看有关感兴趣设备的数据。

Summary（摘要）（指示板顶部）

- 查看由设备类型和时间筛选器确定的网络中处于活动状态的设备的总数。
- 在活动设备总数中，查看有多少是特定的 IoT 设备。
- 通过查看到目前为止检测到的活动警报和漏洞的数量，了解设备运行的安全环境。

设备

- 了解各种设备类型中有多少台设备，并深入查看以了解各种设备类别中有多少台设备，然后了解各种设备配置文件中有多少台设备。了解在设备分类的每个越来越细的级别上有多少关键风险设备，以及它们是哪种设备。

前 **10** 个操作系统

- 检测到操作系统为 IoT Security 的所有设备中，查看前 10 个最常见的操作系统，每个操作系统使用了多少设备，百分比是多少。

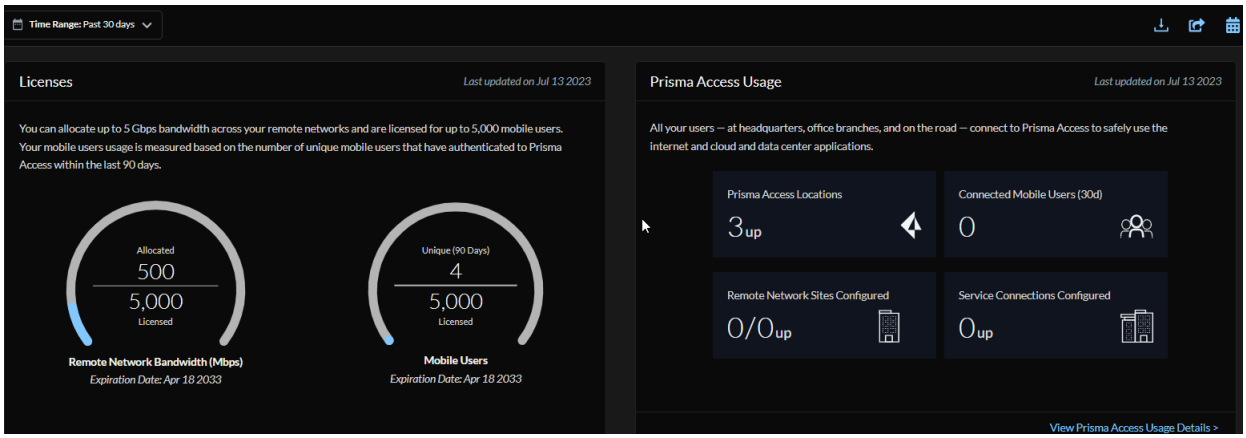
按设备类型划分的子网分布

- 了解不同设备类型在整个网络中的子网中如何分布。如果在同一子网中看到大量设备类型的混合，请考虑将它们细分为各自独立的子网。

指示板Prisma Access

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama or Strata Cloud Manager)	以下之一： ❑ Prisma Access 许可证 ❑ Strata Cloud Manager Pro → 您可用的特性和功能Strata Cloud Manager取决于您使用的许可证。

- 要开始，请单击 **Strata Cloud Manager** > **Dashboards**（指示板） > **More Dashboards**（更多指示板） > **Prisma Access**。



该指示板显示什么？

了解如何利用许可证提供的功能，并大致了解 Prisma Access 环境的运行状况和性能。

Prisma Access 使用情况数据包括：

- 您的 Prisma Access 使用情况概述 - 您的许可证、Prisma Access 位置以及移动用户容量和/或带宽利用率
- 适用于移动用户和远程网络的 Prisma Access 主要位置
- 远程网络和服务连接站点以及消耗最高的远程网络和服务连接站点的总体带宽消耗
- 隧道断开趋势，包括受影响最严重的隧道

指示板显示每个 *Prisma Access* 租户的聚合数据。

此指示板支持报告。指示板右上方的这些图标 表示此指示板支持报告。您可以共享、下载和安排包含此指示板显示的数据的报告。

如何使用指示板中的数据？

此指示板有助于了解网络中的 Prisma Access 使用情况，并根据指示板数据调整配置设置。

指示板应用程序体验

在何处可以使用？	需要提供什么？
• Prisma Access （利用 *Strata Cloud Manager* 或 *Panorama* 配置管理）	❑ Prisma Access 许可证 ❑ 查看受监控应用程序数据的 ADEM Observability 许可证 ❑ 远程网络许可证 （需要查看远程站点体验数据）

- 单击 **Strata Cloud Manager** > **Dashboards**（指示板） > **More Dashboards**（更多指示板） > **Application Experience**（应用程序体验）以开始。

该指示板显示什么？

此指示板中显示的数据将发生变化，并与您选择的卡片（移动用户体验或远程站点体验）对应。如果您是 AI-Powered ADEM，您可能希望首先调查整个组织中使用的应用程序，并使用此信息来确定要为其创建应用程序测试的应用程序。此外，如果您有用户或远程站点报告应用程序问题，则可以使用此指示板来开始隔离问题。应用程序使用数据是从通过 Prisma Access 的真实用户流量中提取的。它包括来自移动用户和远程站点的流量。

您可以添加筛选器来缩小结果范围，以仅显示特定应用程序、部署类型、体验分数、移动用户、组或 Prisma Access 位置的数据。查看应用程序的个人体验分数，以及受任何现有性能问题影响的用户和远程站点的数量。

如何使用指示板中的数据？

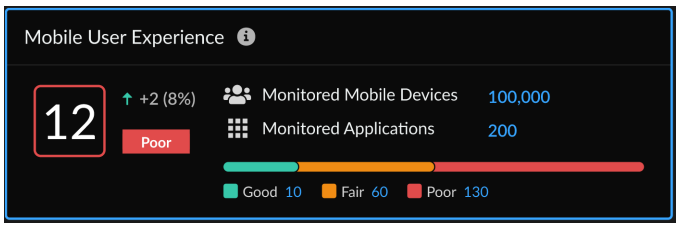
在调查了网络上运行的应用程序并确定要监控的应用程序后，您可以创建应用程序测试。在创建应用程序测试时，请记住，尽管您可以创建针对多个用户或站点的应用程序测试，但测试的数量基于每个用户或 ION 设备运行的应用程序测试数量（例如，如果您有一个针对 Slack 的应用程序测试并将其定位到 1000 个用户，这将作为 1000 次测试计入您的许可证）。

应用程序体验指示板：移动用户体验卡片

在何处可以使用？	需要提供什么？
• Prisma Access （利用 *Strata Cloud Manager* 或 *Panorama* 配置管理）	❑ Prisma Access 许可证 ❑ 查看 **Monitored Applications**（监控的应用程序）的 ADEM Observability 许可证

此小部件向您显示所有受监控应用程序的所有移动用户的应用程序区段分数的平均值。它还会显示按用户设备数量划分的“良好”、“一般”和“较差”体验的细分。您可以深入了解“一般”或“较差”体验的用户，以便开始调查。此卡片中的体验分数将显示用户的整体数字体验。对于按每个移

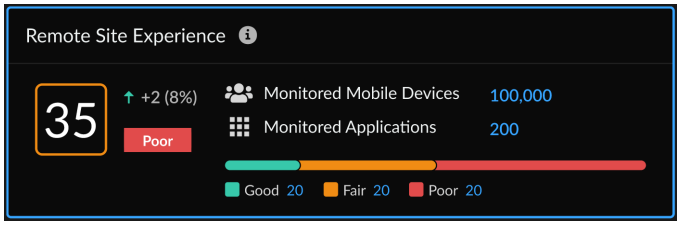
动用户监控的每个应用程序，ADEM 根据 5 个关键指标（应用程序可用性、DNS 解析时间、TCP 连接时间、SSL 连接时间和 HTTP 延迟）计算分数。如果应用程序未通过可用性测试（应用程序不可用），则体验分数为 0。如果可以访问应用程序，则只有这样才能计算剩余的四个指标。上述每个指标（应用程序可访问性除外）都有不同的权重以及基准的下限和上限阈值，它们的综合权重等于 100。这些单个指标分数的总和决定用户的应用程序体验分数。每个应用程序的所有测试样本结果的平均值决定用户的体验分数。



应用程序体验指示板：远程站点体验卡片

在何处可以使用？	需要提供什么？
• Prisma Access （利用 *Strata Cloud Manager* 或 *Panorama* 配置管理）	❑ Prisma Access 许可证 ❑ 查看 **Monitored Applications**（监控的应用程序）的 ADEM Observability 许可证 ❑ 远程网络许可证

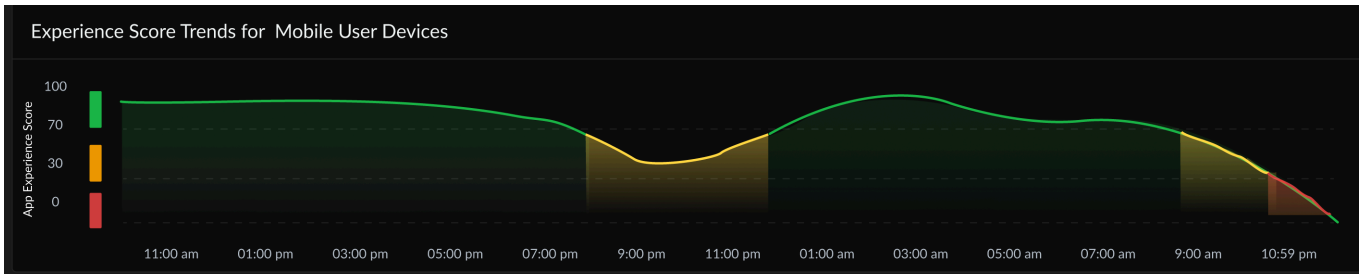
远程站点体验分数是所有活动 WAN 路径上所有受监控应用程序的平均分数。它是从该远程站点监控的各个应用程序收集的所有测试样本结果的平均值。它是远程站点或分支的总体体验分数（位于彩色编码方框中），即在该站点监控的所有应用程序的活动路径上收集的所有测试样本的体验分数的平均值。虽然每个备份路径的体验分数将单独计算，并且可用于每个远程站点和应用程序，但是在计算远程站点的体验分数时不会考虑备份路径的体验分数。您可以通过单击“一般”或“较差”旁边的数字来深入了解性能一般或较差的站点。



应用程序体验指示板：体验分数趋势

在何处可以使用？	需要提供什么？
• Prisma Access （利用 *Strata Cloud Manager* 或 *Panorama* 配置管理）	❑ Prisma Access 许可证 ❑ 查看 **Monitored Applications**（监控的应用程序）的 ADEM Observability 许可证

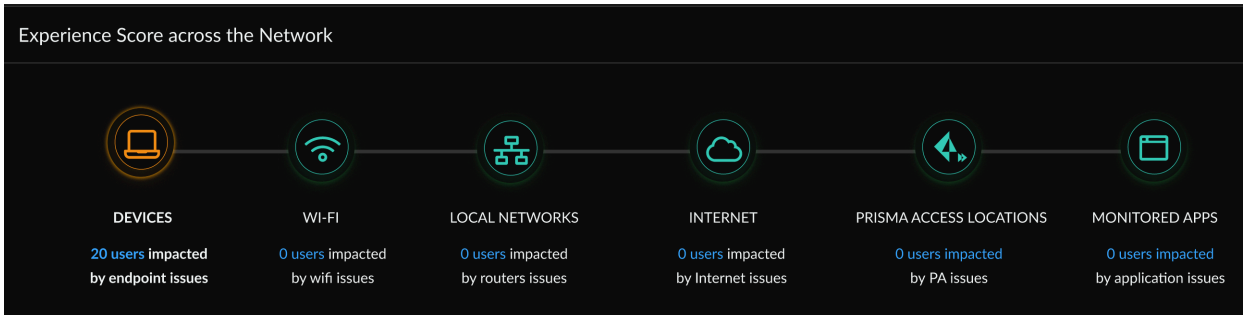
此小部件显示所有移动用户的平均移动用户体验的时间序列图。体验分数在选定时间范围内按设定的时间间隔进行计算和显示。Y 轴根据分数范围进行颜色编码，以显示体验分数的质量（红色 = 较差，黄色 = 一般，绿色 = 良好）。将鼠标光标悬停在趋势线上，可查看光标所在位置的体验得分。



应用程序体验指示板：整个网络的体验得分

在何处可以使用？	需要提供什么？
• Prisma Access （利用 *Strata Cloud Manager* 或 *Panorama* 配置管理）	❑ Prisma Access 许可证 ❑ 查看 **Monitored Applications**（监控的应用程序）的 ADEM Observability 许可证

识别可能导致组织内部出现问题的网段，从端点（针对移动用户）或分支（远程站点）一直到应用程序。您可以看到从端点和 Prisma SD-WAN 远程站点一直到应用程序，哪个网段可能导致组织内部出现问题。您可以查看哪个细分市场（如 ISP 或计算位置中断/SaaS 应用中断）正在影响组织内的数字化体验，以及受其影响的用户或站点的确切数量。图标采用颜色编码，并基于所有移动用户的段运行状况得分平均值。绿色图标代表良好（得分 >=70），黄色代表一般（得分30-70），红色代表较差（得分 < 30）。



设备 - 设备运行状况指标（CPU/内存/磁盘空间/磁盘队列/电池）

Wi-Fi - WIFI 指标（信号质量，Tx、Rx、SSID、BSSID、信道）

本地网络 - 网络性能指标（延迟/丢失/抖动）

Internet - 网络性能指标（延迟/丢失/抖动）如果设备未连接到 GlobalProtect、Internet 网段，则网络性能指标将与为应用程序网段执行的 TCP Ping 测试相同。

Prisma Access 位置 - 网络性能指标（延迟/丢失/抖动）如果设备未连接到 GlobalProtect，则不执行此网段的测试。

监控的应用程序 - 网络性能指标（延迟/丢失/抖动）应用性能指标（可用性、DNS 查找、TCP 连接、SSL 连接、HTTP 延迟、第一个字节的时间、最后一个字节的时间、数据传输）

应用程序体验指示板：应用程序体验分数的全球分布

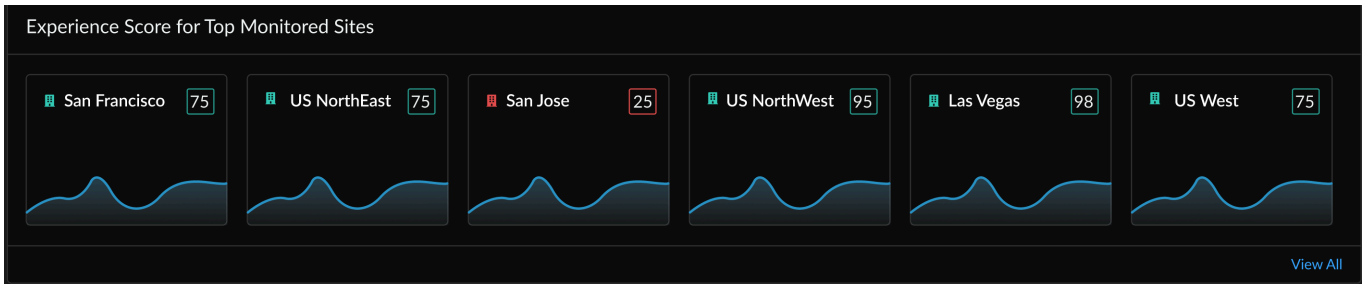
在何处可以使用？	需要提供什么？
• Prisma Access （利用 *Strata Cloud Manager* 或 *Panorama* 配置管理）	❑ Prisma Access 许可证 ❑ 查看 **Monitored Applications**（监控的应用程序）的 ADEM Observability 许可证

根据您选择的卡片，此小部件中的地图视图根据在特定 Prisma Access 位置监视的移动用户和应用程序的总数，或根据远程站点和应用程序的总数，向您显示 Prisma Access 位置的体验。Prisma Access 位置使用圆圈进行标记，圆圈使用颜色编码来表示所有受监视的移动用户和连接到该圆圈出现的特定 Prisma Access 位置的远程站点的应用程序分段分数的状态。将鼠标光标悬停在圆圈上可查看该位置的体验得分，以及所监视的移动用户设备或远程站点总数和该位置所监视的应用总数。地理上非常接近的多个位置用一个带数字的圆圈表示。数字表示该区域中有多少个位置分组在一起。要查看哪些位置分组在一起，请放大地图。

应用程序体验指示板：受监控最频繁的网站的体验评分

在何处可以使用？	需要提供什么？
• Prisma Access （利用 *Strata Cloud Manager* 或 *Panorama* 配置管理）	❑ Prisma Access 许可证 ❑ 查看 **Monitored Applications**（监控的应用程序）的 ADEM Observability 许可证

这个小部件为每个应用程序显示一张卡片，并显示得分最高的网站。此小部件显示选定时间范围内远程站点的体验分数趋势。将鼠标光标悬停在趋势线上即可查看该特定时间点的体验分数。

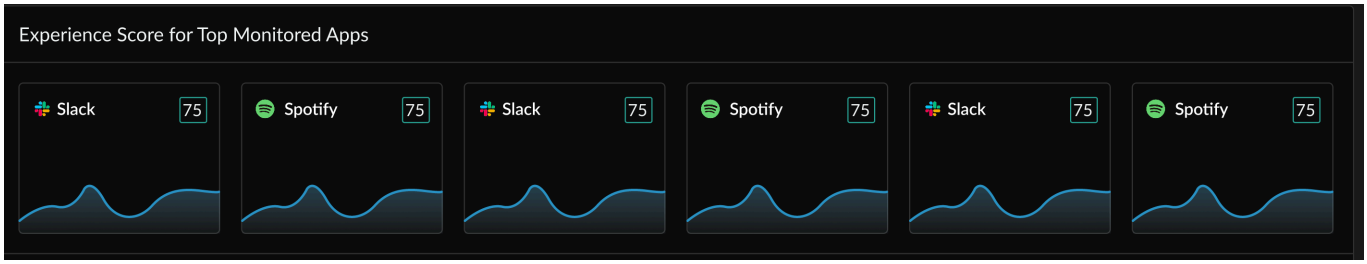


应用程序体验指示板：受监控次数最多的应用程序的体验分数

在何处可以使用？	需要提供什么？
• Prisma Access （利用 *Strata Cloud Manager* 或 *Panorama* 配置管理）	❑ Prisma Access 许可证 ❑ 查看 **Monitored Applications**（监控的应用程序）的 ADEM Observability 许可证

每个应用程序卡片都会显示远程站点上该特定应用程序的所有受监控移动用户的平均应用程序分段分数（方框中的数字）。体验分数是所有受监控应用程序的应用体验分数的平均值。体验分数描述的是应用程序活动路径的端到端体验。它是仅针对该特定应用程序在活动路径上收集的所有测试样本的平均值。趋势线显示所选时间范围内所有 5 分钟 APM 数据样本的平均值。

您可以看到正在监控多少个应用程序以及监控了多少个活动路径和备份路径。每个应用程序卡片都会显示受影响的路径数量。单击应用程序卡即可查看该特定应用程序的指标。



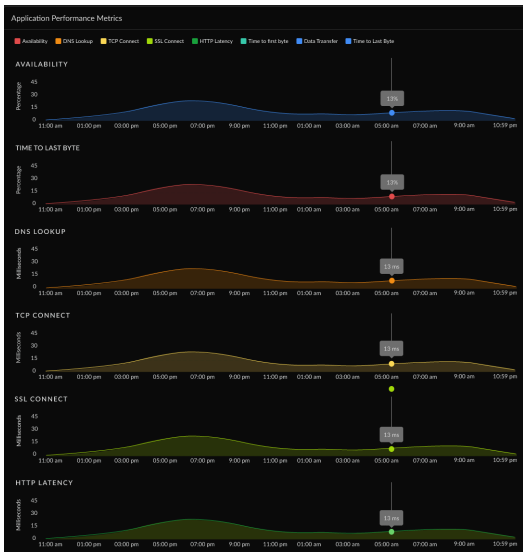
应用程序体验指示板：应用程序性能度量

在何处可以使用？	需要提供什么？
• Prisma Access （利用 *Strata Cloud Manager* 或 *Panorama* 配置管理）	❑ Prisma Access 许可证 ❑ 查看 **Monitored Applications**（监控的应用程序）的 ADEM Observability 许可证

自主 DEM 使用 TCP Ping 和 Curl 来确定端到端应用程序性能。

指标	说明
可用性	**Time Range**（时间范围）内的应用程序可用性（百分比）。
DNS 查找	DNS 解析时间。
TCP 连接	建立 TCP 连接所需的时间。
SSL 连接	建立 SSL 连接所需的时间。

指标	说明
HTTP 延迟	建立 HTTP 连接所需的时间。
第一个字节的时间	第一个字节的时间中的 DNS 连接、TCP 连接、SSL 连接和 HTTP 延迟时间的总和结果。
数据传输	传输整个数据所用的总时间。
最后一个字节的时间	第一个字节的时间 + 数据传输时间。



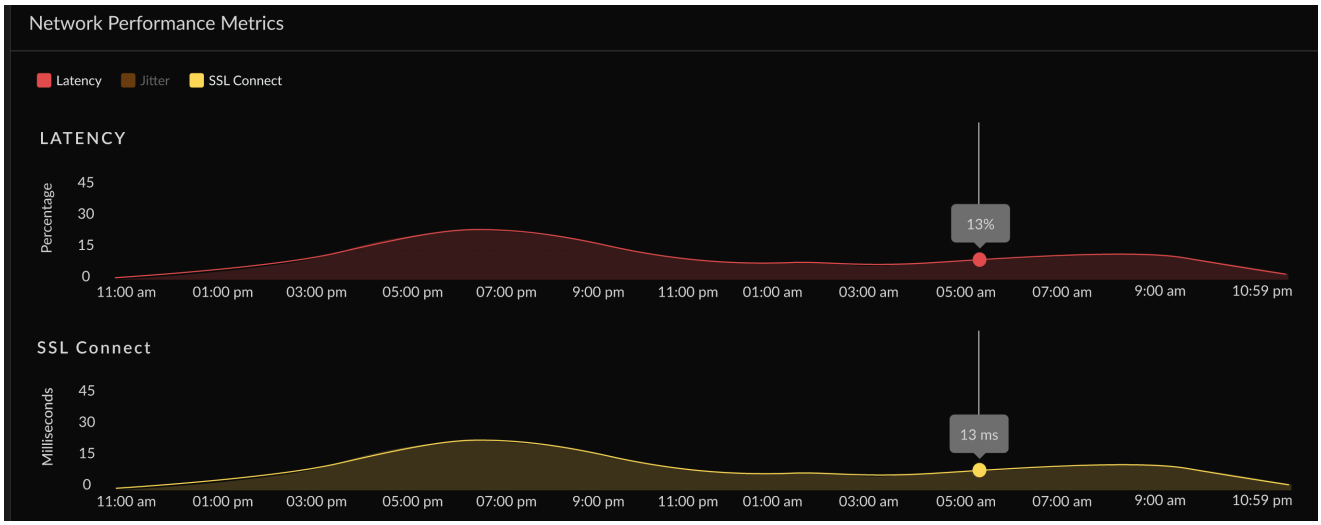
应用程序体验指示板：网络性能指标

在何处可以使用？	需要提供什么？
• Prisma Access （利用 *Strata Cloud Manager* 或 *Panorama* 配置管理）	❑ Prisma Access 许可证 ❑ 查看 **Monitored Applications**（监控的应用程序）的 ADEM Observability 许可证

ADEM 使用 ICMP Ping 来确定每个分段的网络性能。

指标	说明
可用性	**Time Range**（时间范围）内的网络可用性指标。
网络延迟	通过网络传输数据所花费的时间。
数据包丢失	数据传输过程中数据包丢失。

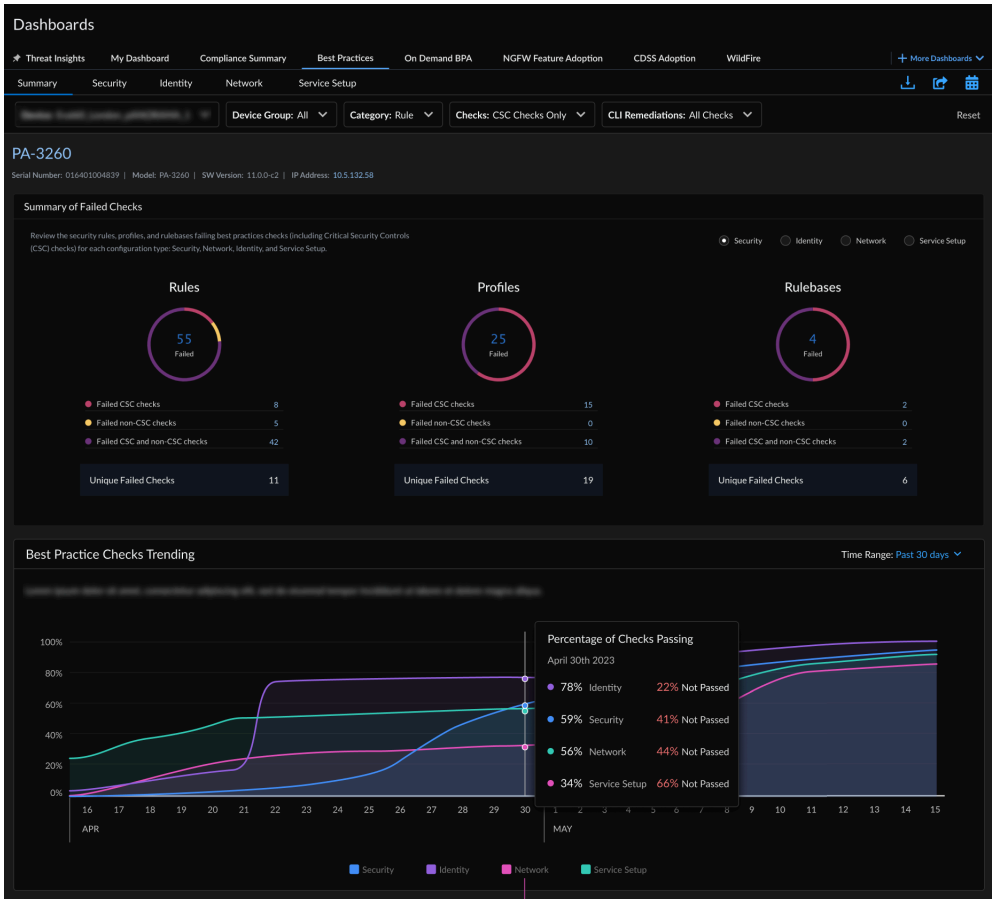
指标	说明
抖动	**Time Range**（时间范围）内的延迟变化。



指示板最佳实践

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW，包括由 软件 NGFW 积分提供资助的项目	这些许可证中的每一个都包括 Strata Cloud Manager 访问权限： ❑ Prisma Access ❑ AIOps for NGFW Premium ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → 您可用的特性和功能Strata Cloud Manager取决于您使用的许可证。

- 要开始，请单击 **Strata Cloud Manager** > **Dashboards**（指示板） > **More Dashboards**（更多指示板） > **Best Practices**（最佳实践）。



该指示板显示什么？

指示板显示与您的租户关联的每个 *Prisma Access* 和 *NGFW/Panorama* 的聚合数据。

最佳实践指示板根据 Palo Alto Networks 的最佳实践指导衡量您的安全态势。重要的是，最佳实践评估包括对互联网安全中心关键安全控制 (CSC) 的检查。CSC 检查与其他最佳实践检查是分开进行，因此您可以轻松挑选并优先安排能让您实现 CSC 合规性的更新。

最佳实践指示板分为五个部分：

- 摘要

  提供跨配置类型（安全、网络、身份和服务设置）的设备所有失败检查的综合视图，查看 BPA 检查的历史趋势图，并评估关键功能领域的最佳实践采用率。

- 安全

  显示选定设备和位置中未能通过最佳实践和 CSC 检查的规则、规则库或配置文件。如果可用，CLI 修正允许您解决策略规则的问题。CLI 修正使用您在生成按需 BPA 报告时上传的 TSF 数据生成。

  - 规则库

    查看策略的组织方式，以及跨多个规则应用的配置设置是否符合最佳实践（包括 CSC 检查）。

  - 规则

    显示未通过最佳实践和 CSC 检查的规则。查看您可以在哪里采取快速操作来修复失败的检查。规则是根据会话计数排序的，因此您可以线查看和更新影响最大流量的规则。

  - 配置文件

    向您展示您的配置文件与最佳实践（包括 CSC 检查）之间的差距。配置文件可对与安全或解密规则匹配的通信执行高级检查。

- 标识

  显示设备的身份验证强制设置（身份验证规则、身份验证配置文件和身份验证门户）是否满足最佳做法并符合 CSC 检查。

- 网络

  检查应用程序覆盖规则和网络设置是否符合最佳实践和 CSC 检查。

- 服务设置

  查看设备上启用的订阅与最佳实践和 CSC 检查结果之间的匹配程度。可以在此处查看 WildFire 设置、GlobalProtect 门户和 GlobalProtect 网关配置，还可修复失败的检查。

此指示板支持报告。指示板右上方的这些图标 表示此指示板支持报告。您可以共享、下载和安排包含此指示板显示的数据的报告。

如何使用指示板上的数据？

虽然最佳实践指导旨在帮助您加强安全态势，但本报告中的调查结果还可以帮助您确定有哪些领域需要改进，以更有效地管理环境。

指示板合规性摘要

在何处可以使用？	需要提供什么？
• NGFW，包括由 软件 NGFW 积分提供资助的项目	❑ AIOps for NGFW Premium 或 Strata Cloud Manager Pro → 您可用的特性和功能Strata Cloud Manager取决于您使用的许可证。

您可以查看过去 12 个月内对安全检查所做的更改的历史记录，这些更改由互联网安全中心 (CIS) 和美国国家标准与技术研究院 (NIST) 框架分组在一起。对于每个框架，您将看到一个控制列表，以及当前和平均符合率的百分比、最佳实践检查的总数以及每个控制的失败检查的数量。

与图表和列表交互以查看控件及其历史统计数据之间的关系。查看各个控制及其相关检查的详细信息，并选择最佳实践检查以查看未通过检查的防火墙配置。

CIS 关键安全控制框架是一组优先的推荐行动和最佳实践，有助于保护组织及其数据免受已知的网络攻击媒介的侵害。您可以查看 16 个基本和基础 CIS 控件中的 11 个控件的检查摘要：

- CSC 3：持续漏洞管理
- CSC 4：管理权限的受控使用
- CSC 6：审计日志的维护、监控和分析
- CSC 7：电子邮件和网络浏览器保护
- CSC 8：恶意软件防御
- CSC 9：网络端口、协议和服务的限制和控制
- CSC 11：保护网络设备的配置，如防火墙、路由器和交换机
- CSC 12：边界防御
- CSC 13：数据保护
- CSC 14：基于“按需知悉”的原则进行受控访问
- CSC 16：帐户监视和控制

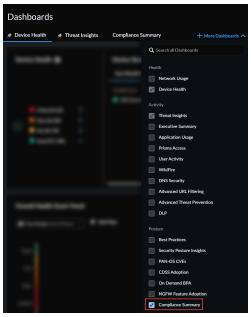
NIST 网络安全框架 **SP 800-53** 控制框架为联邦机构和其他组织提供指导，帮助其实施和维护其信息系统的安全和隐私控制。您可以查看 NIST 控件的八个系列的检查摘要：

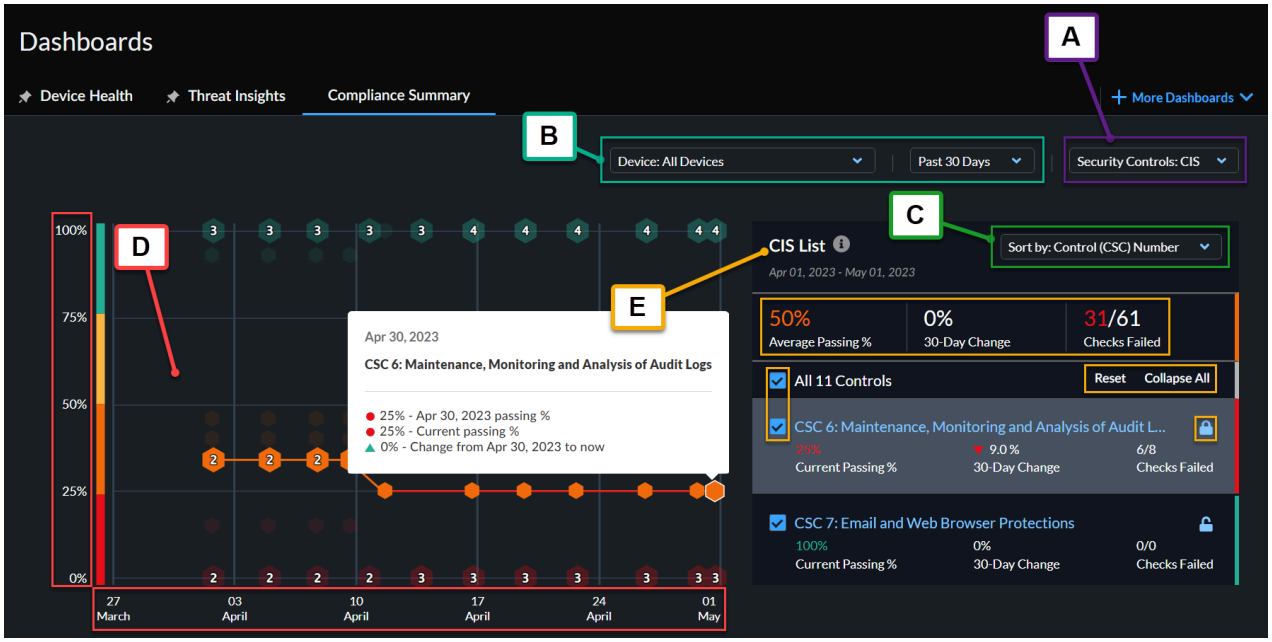
- SC：访问控制
- AU：审计和问责制
- CM：配置管理
- CP：应急计划
- IA：身份识别和身份认证
- RA：风险评估
- SC：系统和通信保护

- SI：系统和信息完整性

要进入合规性摘要指示板，请转到 **Dashboards**（指示板），然后选择 **Compliance Summary**（合规性摘要）选项卡。

如果在选项卡选项中没有看到合规性摘要，请选择更多指示板，然后从态势下列出的选项中选中合规性摘要复选框。





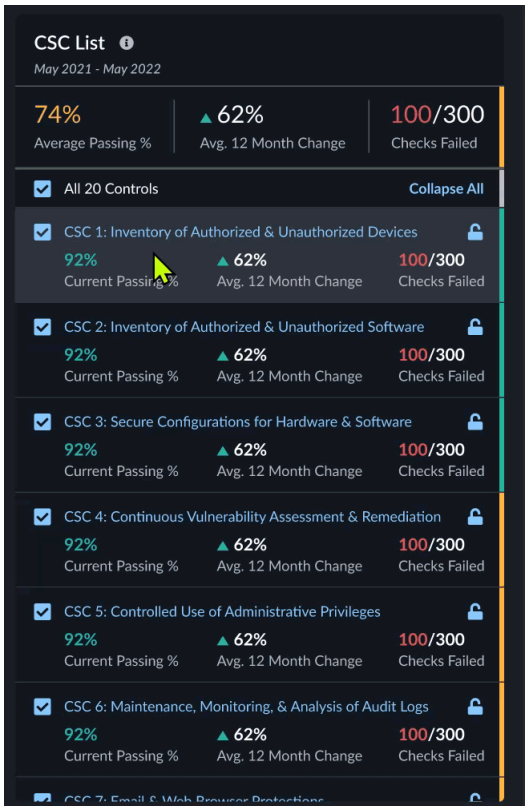
A) 安全控制选择器	选择 CIS 或 NIST 控件
B) 按以下条件筛选	• 设备

	• 时间范围
	  • 过去 7 天
	  • 过去 30 天
	  • 过去 90 天
	  • 过去 6 个月
	  • 过去 12 个月

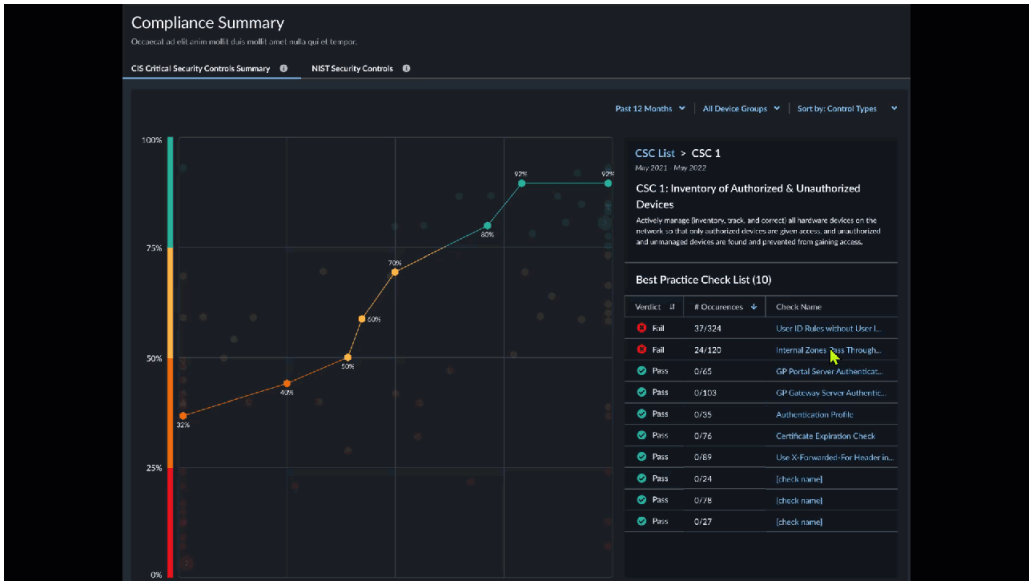
C) 排序依据	• 控件 CSC 编号 • 当前通过率 • 更改百分比 • 失败的检查数
D) 折线图	• 通过率 - 显示给定检查类型的通过率。 • 时间轴 - 显示何时测量给定检查类型的百分比。

E) 检查清单	• 统计数据
	  • 平均通过率 - 显示通过检查的平均百分比。
	  • 12 个月变化 - 显示 12 个月内的变化。
	  • 检查失败 - 显示检查失败的次数。
	• 所选控件 - 选中后，控件将出现在折线图上。
	• 重置 - 移除所有锁。
	• 全部折叠/全部展开 - 显示/隐藏列表中的统计数据。
	• 锁定折线图 - 将锁定的检查保留在折线图上以供查看。

- 选择列表中的控件以查看其包含的最佳实践检查。



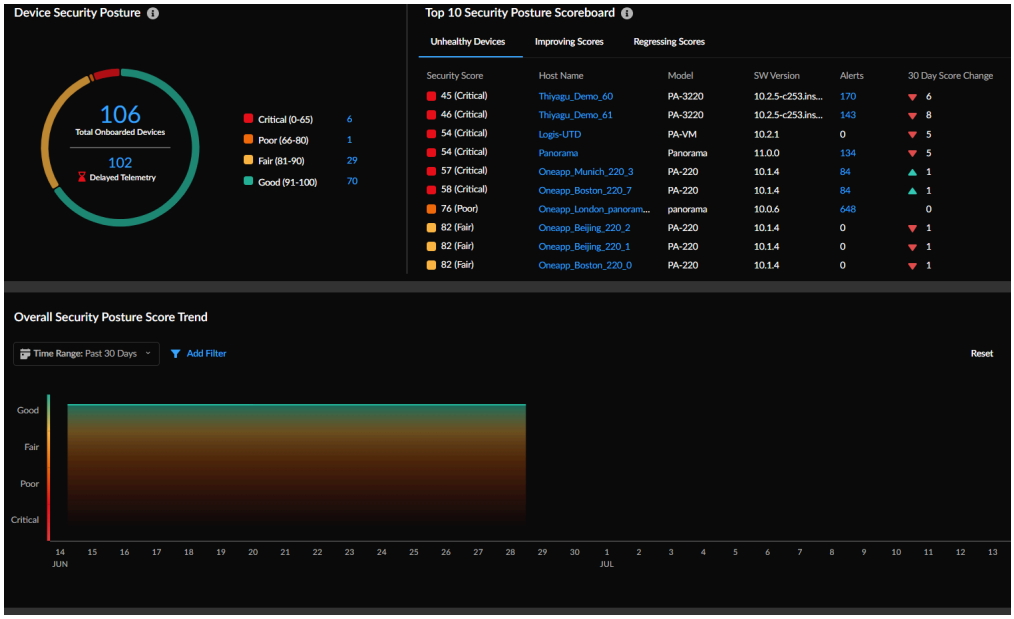
- 选择最佳实践检查以查看未通过检查的防火墙配置。



指示板安全态势洞察

在何处可以使用？	需要提供什么？
• NGFW，包括由 软件 NGFW 积分提供资助的项目	❑ Strata Cloud Manager Essentials ❑ AIOps for NGFW Premium 或 Strata Cloud Manager Pro → 您可用的特性和功能Strata Cloud Manager取决于您使用的许可证。

- 要开始，请单击 **Strata Cloud Manager** > **Dashboards**（指示板） > **More Dashboards**（更多指示板） > **Security Posture Insights**（安全态势见解）。



该指示板显示什么？

指示板显示与租户相关的所有防火墙的汇总数据，还会发送遥测数据。

根据载入 NGFW 设备的安全态势，了解部署的安全状态和趋势。安全分数 (0-100) 的严重程度及其相应的安全等级（良好、一般、较差、严重）决定了设备的安全状况。安全分数是根据打开警报的优先级、数量、类型和状态计算得出的。

如何使用指示板上的数据？

使用此指示板可以：

- 了解影响部署安全态势的问题趋势。

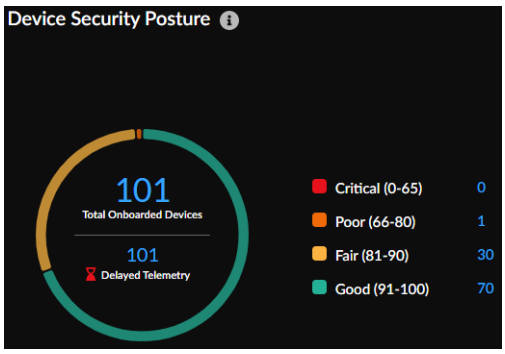
- 通过查看历史安全评分数据，了解您在部署中做出的安全改进。
- 缩小有机会改善安全状况的设备的范围，并对问题进行优先排序以解决这些问题。

此指示板不支持报告功能（下载、共享和计划报告）。

安全态势洞察指示板：设备安全态势

在何处可以使用？	需要提供什么？
• NGFW，包括由 软件 NGFW 积分提供资助的项目	❑ Strata Cloud Manager Essentials ❑ AIOps for NGFW Premium 或 Strata Cloud Manager Pro → 您可用的特性和功能Strata Cloud Manager取决于您使用的许可证。

- 要查看指示板，请单击 **Strata Cloud Manager** > **Dashboards**（指示板） > **More Dashboards**（更多指示板） > **Security Posture Insights**（安全态势见解）。



指示板小部件显示：

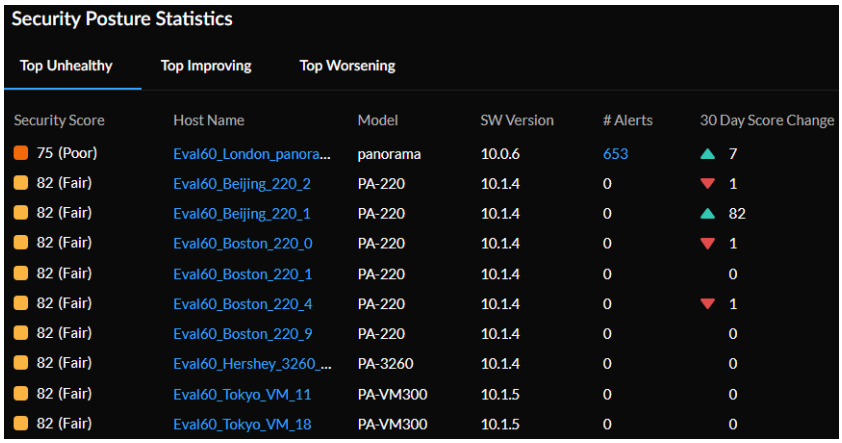
- 已加入的 NGFW 总数。
- 超过 12 小时未发送遥测数据的设备数量。
- 您部署中的载入设备的安全分数优先级。单击数字链接即可了解设备详细信息和安全统计数据。

安全态势洞察指示板：安全态势统计信息

在何处可以使用？	需要提供什么？
• NGFW，包括由 软件 NGFW 积分提供资助的项目	❑ Strata Cloud Manager Essentials ❑ AIOps for NGFW Premium 或 Strata Cloud Manager Pro

在何处可以使用？	需要提供什么？
	→ 您可用的特性和功能Strata Cloud Manager取决于您使用的许可证。

- 要查看指示板，请单击 **Strata Cloud Manager** > **Dashboards**（指示板） > **More Dashboards**（更多指示板） > **Security Posture Insights**（安全态势见解）。



运行状况不佳的主要设备

这些是对部署安全态势影响最大的 10 个设备。向下钻取以查看设备详细信息和设备上的警报。对设备上的关键警报执行补救步骤，以改善安全状况。

主要改进

查看在 30 天时间段内安全态势得分提高的前 10 台设备与设备当前安全分数的对比。

主要恶化

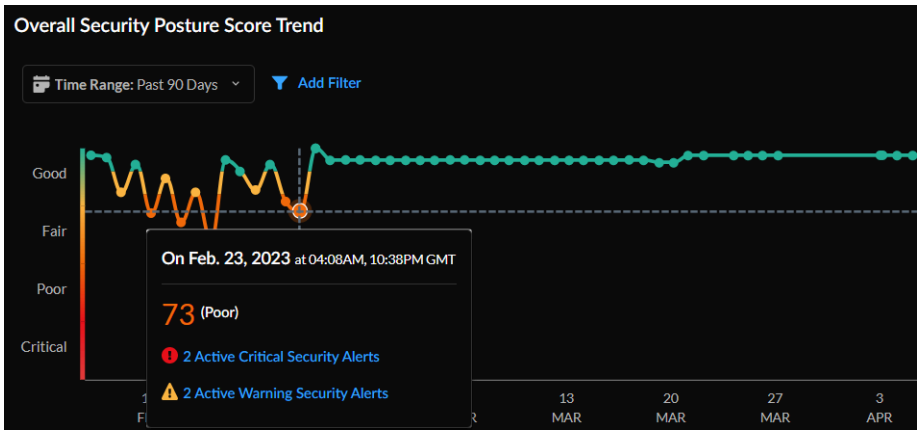
这些是与设备当前安全分数相比安全态势分数下降的设备。查看这些设备上的警报并优先修复它们。

安全态势洞察指示板：分数趋势

在何处可以使用？	需要提供什么？
• NGFW，包括由 软件 NGFW 积分提供资助的项目	☐ Strata Cloud Manager Essentials ☐ AIOps for NGFW Premium 或 Strata Cloud Manager Pro → 您可用的特性和功能Strata Cloud Manager取决于您使用的许可证。

- 要查看指示板，请单击 **Strata Cloud Manager** > **Dashboards**（指示板） > **More Dashboards**（更多指示板） > **Security Posture Insights**（安全态势见解）。

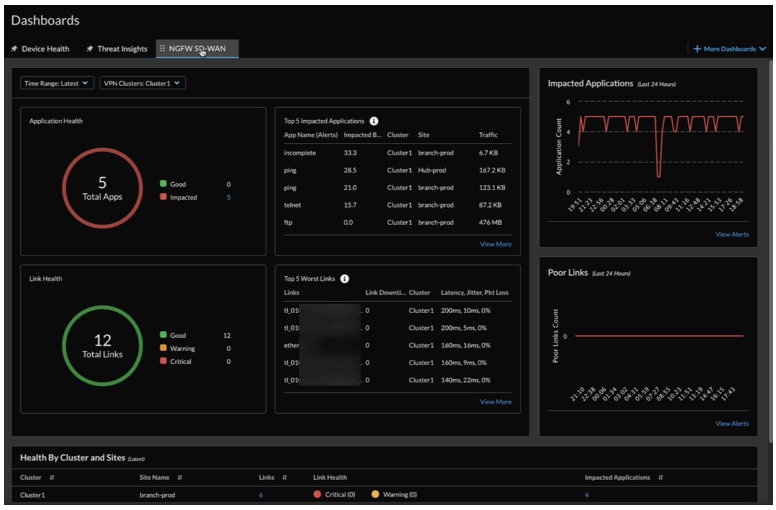
该图表显示了您的部署在选定时间段内的安全态势趋势。将鼠标悬停在触发点上，可了解影响安全态势趋势的设备和活动警报。您可以查看按主机名、型号或软件版本筛选的一个或多个设备的趋势。



指示板NGFW SD-WAN

在何处可以使用？	需要提供什么？
• NGFW，包括由 软件 NGFW 积分提供资助的项目	❑ AIOps for NGFW Premium 或 Strata Cloud Manager Pro → 您可用的特性和功能Strata Cloud Manager取决于您使用的许可证。

- 要开始，请单击 **Dashboards**（指示板）**> More Dashboards**（更多指示板）**> NGFW SD-WAN**。



要利用此指示板，您可以在 Strata Cloud Manager 上为 Palo Alto Networks 新一代防火墙设置软件定义广域网 (SD-WAN)。

该指示板显示什么？

NGFW SD-WAN 指示板向您显示具有 SD-WAN 的云管理防火墙的链接和应用流量的性能指标。

如何使用指示板上的数据？

此指示板可帮助您：

- 通过查看所有 VPN 群集的摘要信息，了解应用程序和链接 VPN 群集中的性能指标，以排除故障。
- 向下钻取，将问题隔离到受影响的站点、应用程序和链接。
- 发出可操作的警报，以调查和补救较差链接和应用程序。通过 ML 支持的异常检测、正常带和预测，可操作的警报基于数据驱动的阈值，您将获得趋势方面的洞察。

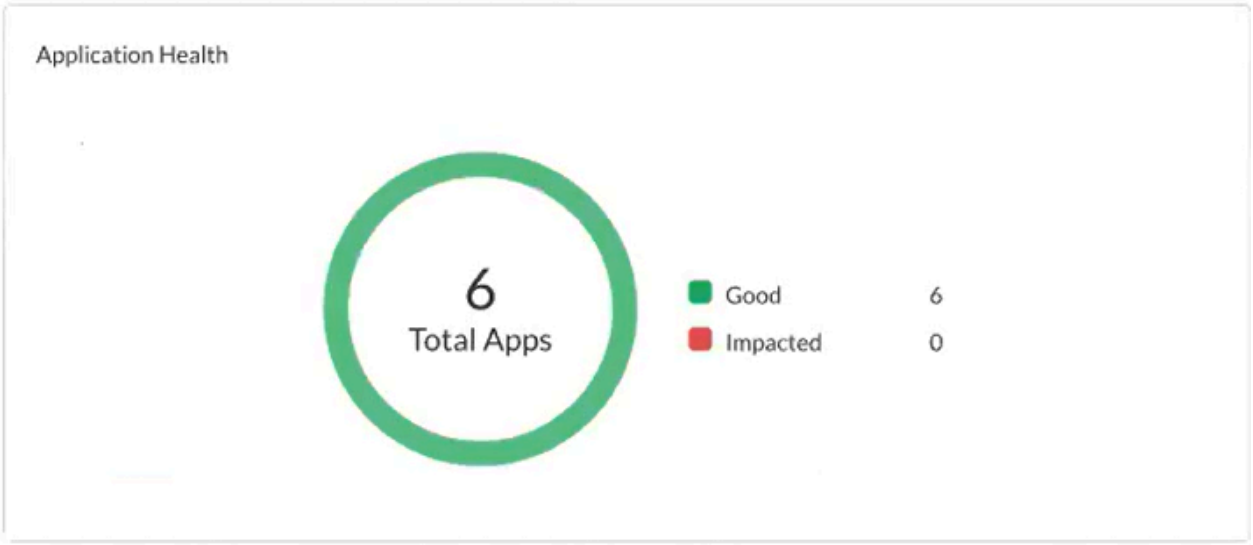
下面是一个视频，展示了如何监控 NGFW SD-WAN 指示板。

NGFW SD-WAN 指示板：应用程序运行状况

在何处可以使用？	需要提供什么？
• NGFW，包括由 软件 NGFW 积分提供资助的项目	❑ AIOps for NGFW Premium 或 Strata Cloud Manager Pro → 您可用的特性和功能Strata Cloud Manager取决于您使用的许可证。

指示板显示：

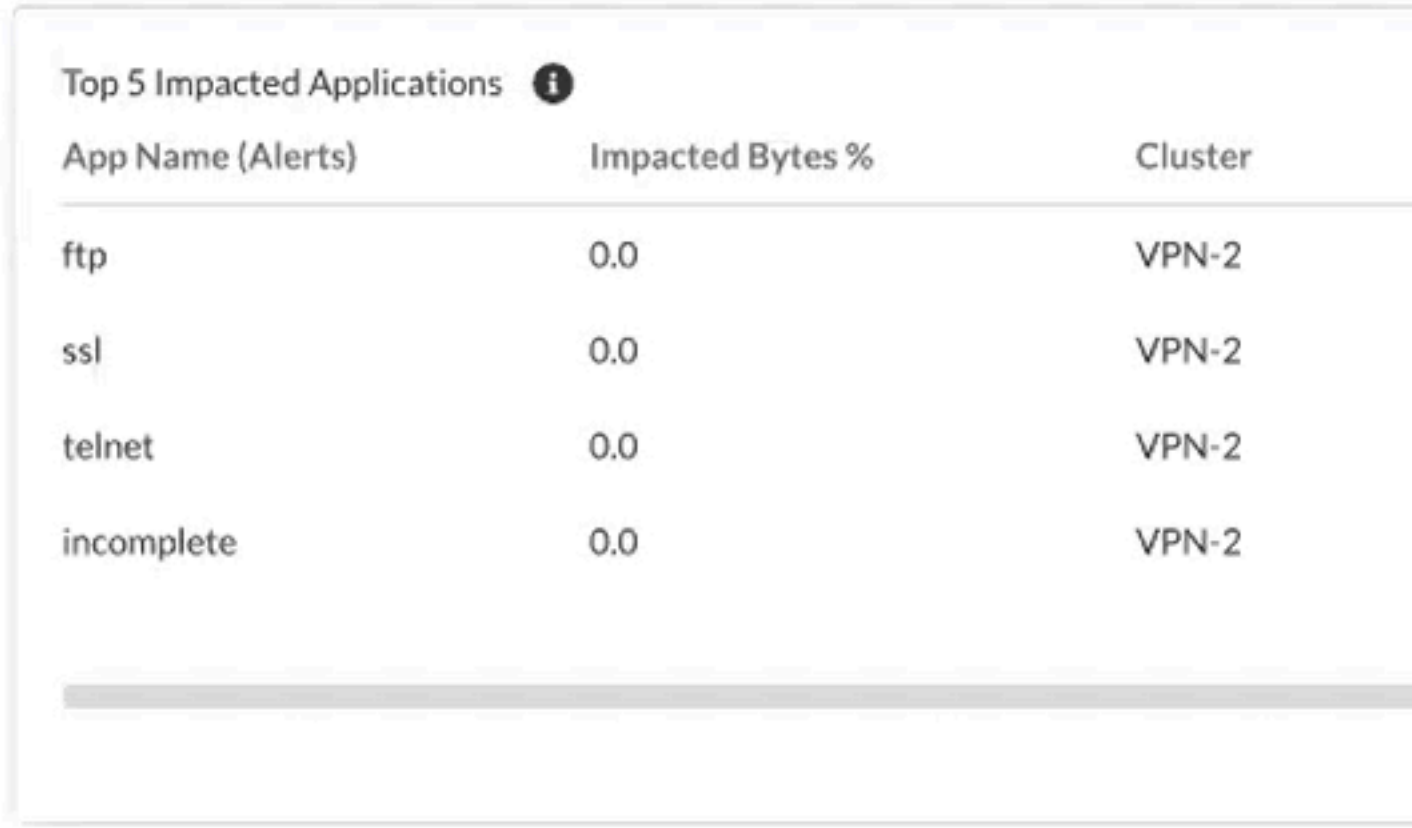
- 选定持续时间和 VPN 群集的应用程序总数。
- 受影响的应用程序的数量，即 VPN 集群中的一个或多个应用程序，其路径中的抖动、延迟或数据包丢失性能都没有达到防火墙可选择路径质量配置文件中的指定阈值。
- 运行状况良好的应用程序数量，即 VPN 群集中未遇到抖动、延迟或数据包丢失性能问题的应用程序数量。



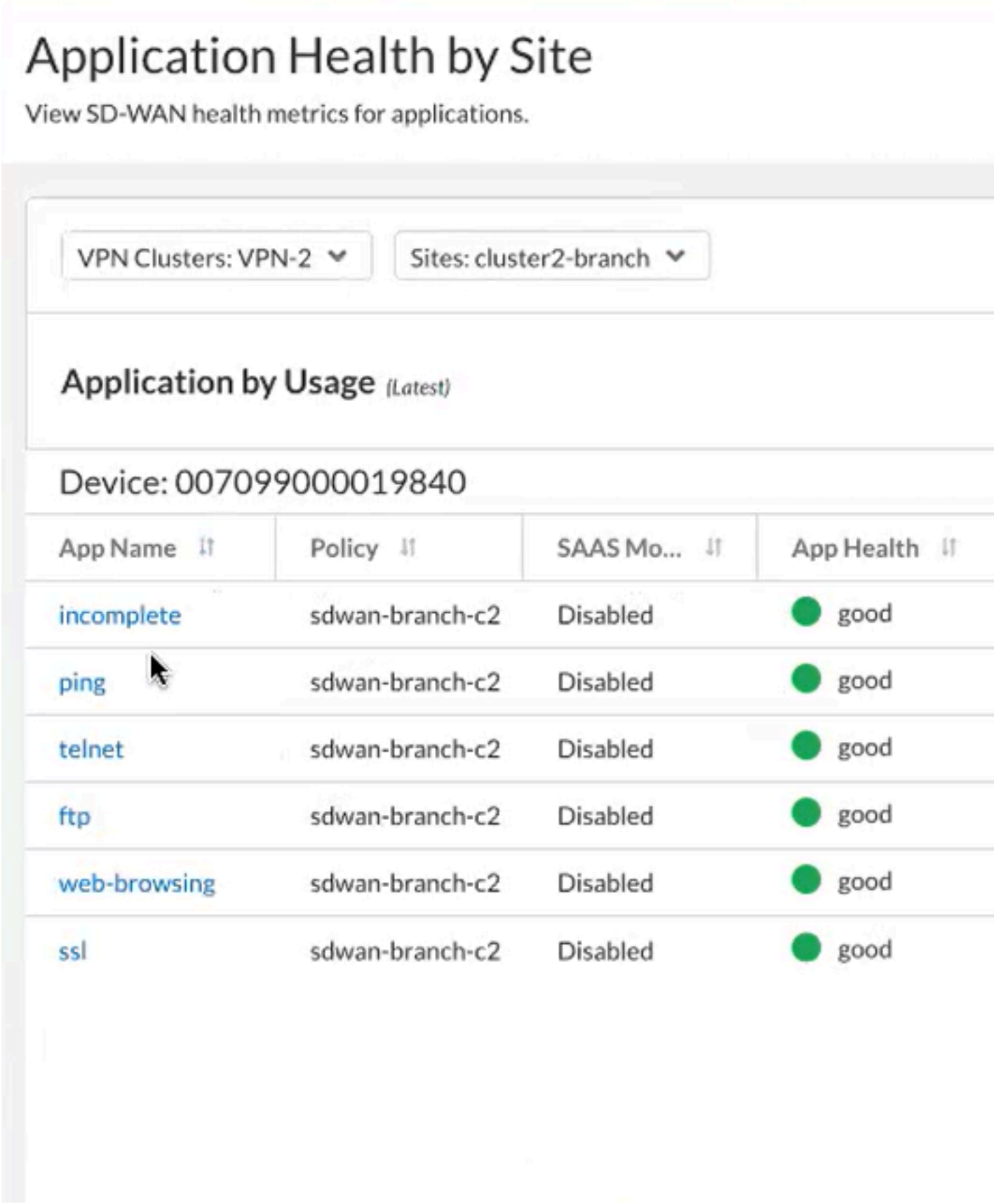
NGFW SD-WAN 指示板：受影响最大的应用程序

在何处可以使用？	需要提供什么？
• NGFW，包括由 软件 NGFW 积分提供资助的项目	❑ AIOps for NGFW Premium 或 Strata Cloud Manager Pro → 您可用的特性和功能Strata Cloud Manager取决于您使用的许可证。

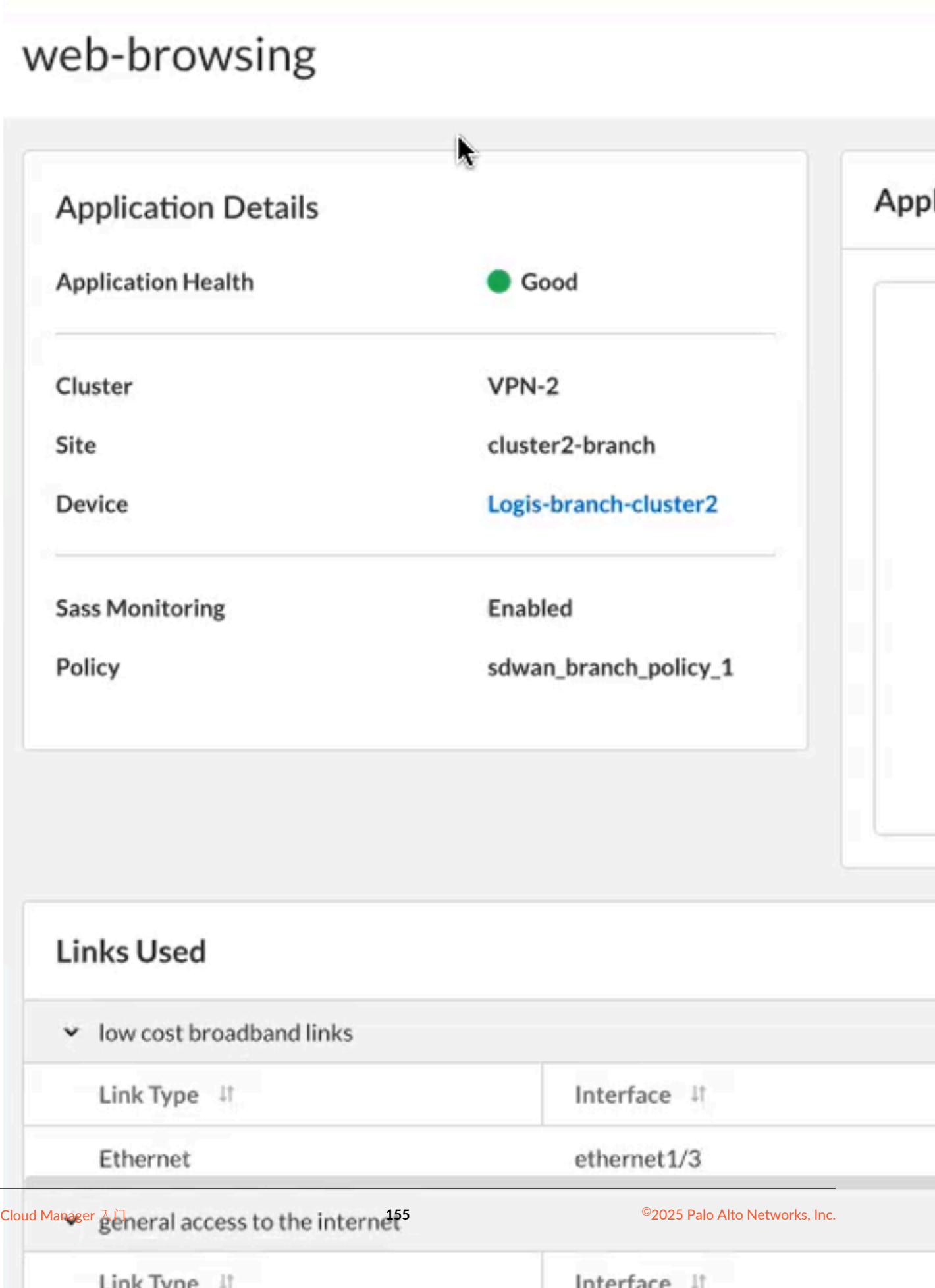
对于所选时间期限和 VPN 集群，Strata Cloud Manager 根据受影响的流量与总字节数的计算百分比显示前 5 个受影响的应用程序。计算出的百分比越高表示对应用程序的影响越大。



单击查看更多可检查所有受影响的应用程序。



此外，单击应用程序可查看其详细信息，包括流量和使用的链接。您也可以单击已使用的链接来查看其详细信息。



NGFW SD-WAN 指示板：受影响的应用程序

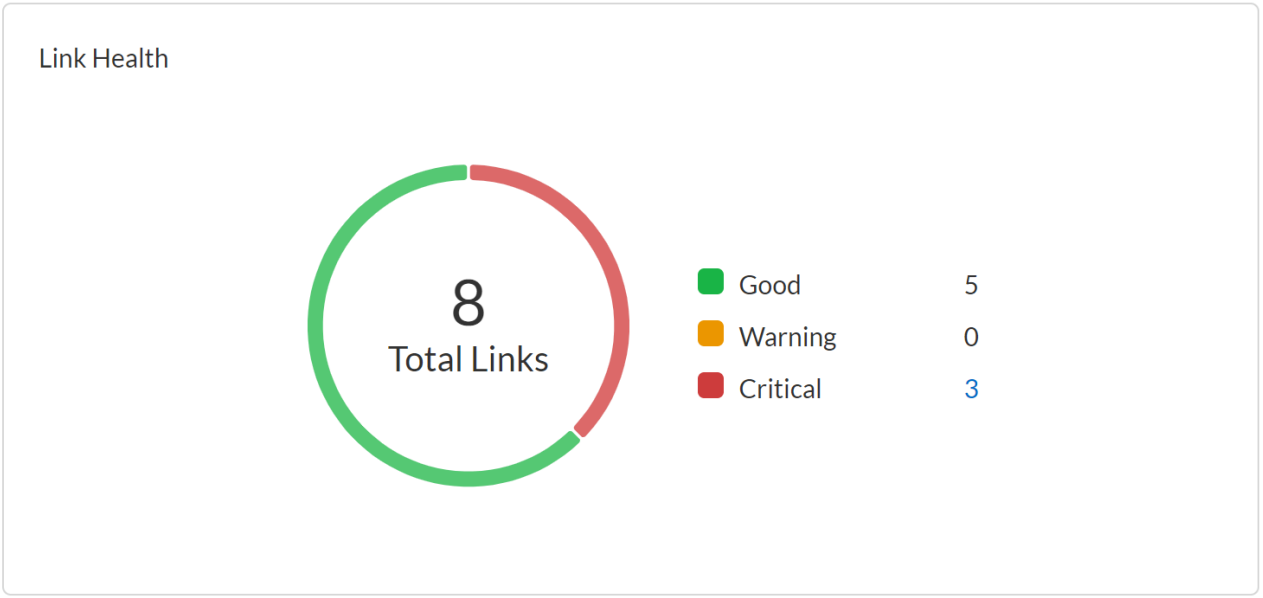
在何处可以使用？	需要提供什么？
• NGFW，包括由 软件 NGFW 积分提供资助的项目	❑ AIOps for NGFW Premium 或 Strata Cloud Manager Pro → 您可用的特性和功能Strata Cloud Manager取决于您使用的许可证。

- 图表显示了过去 24 小时内受影响应用程序的趋势。将光标悬停在趋势线上可以查看特定时间点受影响的应用程序。
- 单击查看警报可查看由于受影响的应用程序而引发的相关警报。

NGFW SD-WAN 指示板：链接运行状况

在何处可以使用？	需要提供什么？
• NGFW，包括由 软件 NGFW 积分提供资助的项目	❑ AIOps for NGFW Premium 或 Strata Cloud Manager Pro → 您可用的特性和功能Strata Cloud Manager取决于您使用的许可证。

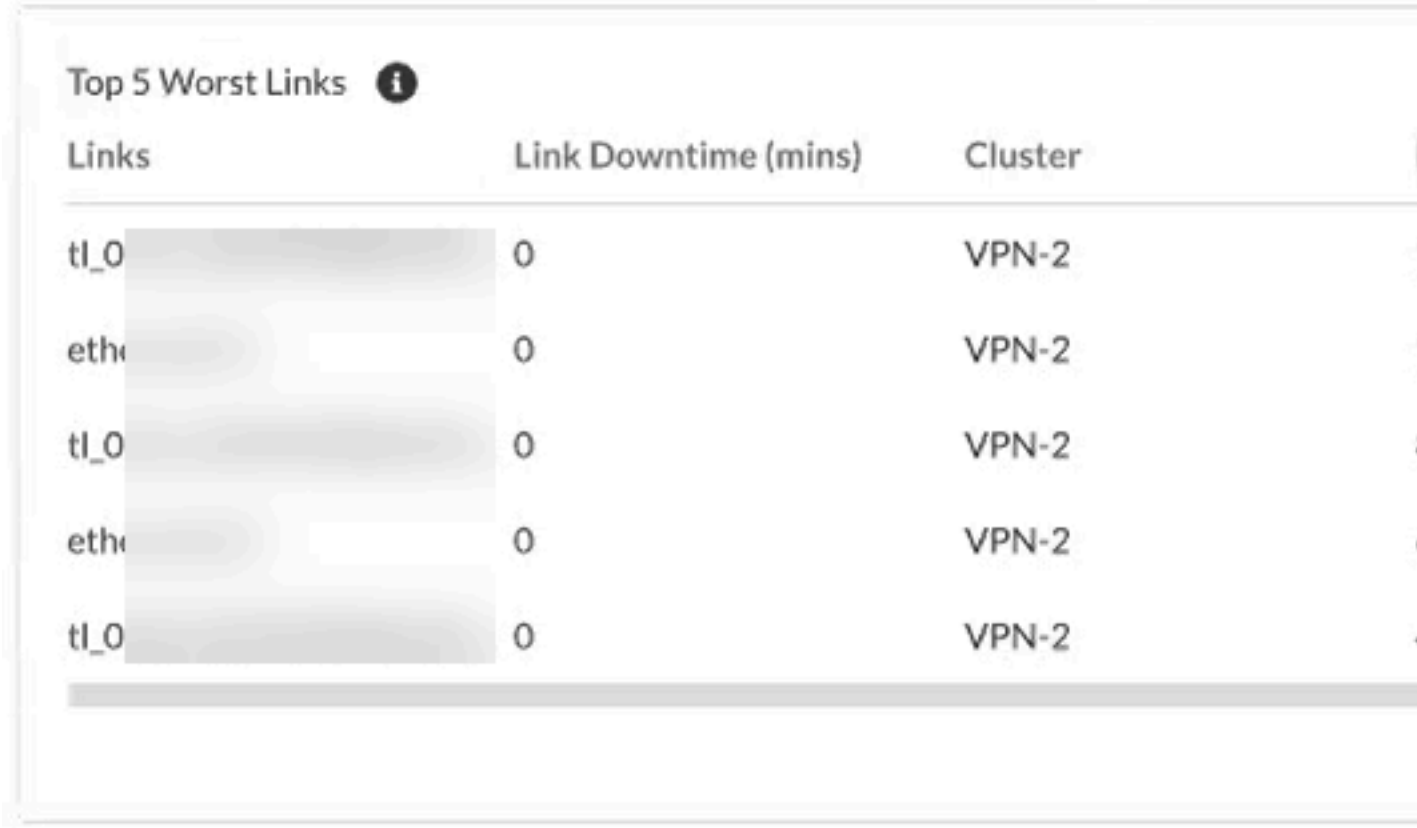
- 选定时间长度和 VPN 集群的链接总数。
- 被归类为“严重”、“警告”和“良好”的链接数。
- 单击严重的数字链接可查看由于 SD-WAN 链接性能而引发的警报。



NGFW SD-WAN 指示板：最差的链接

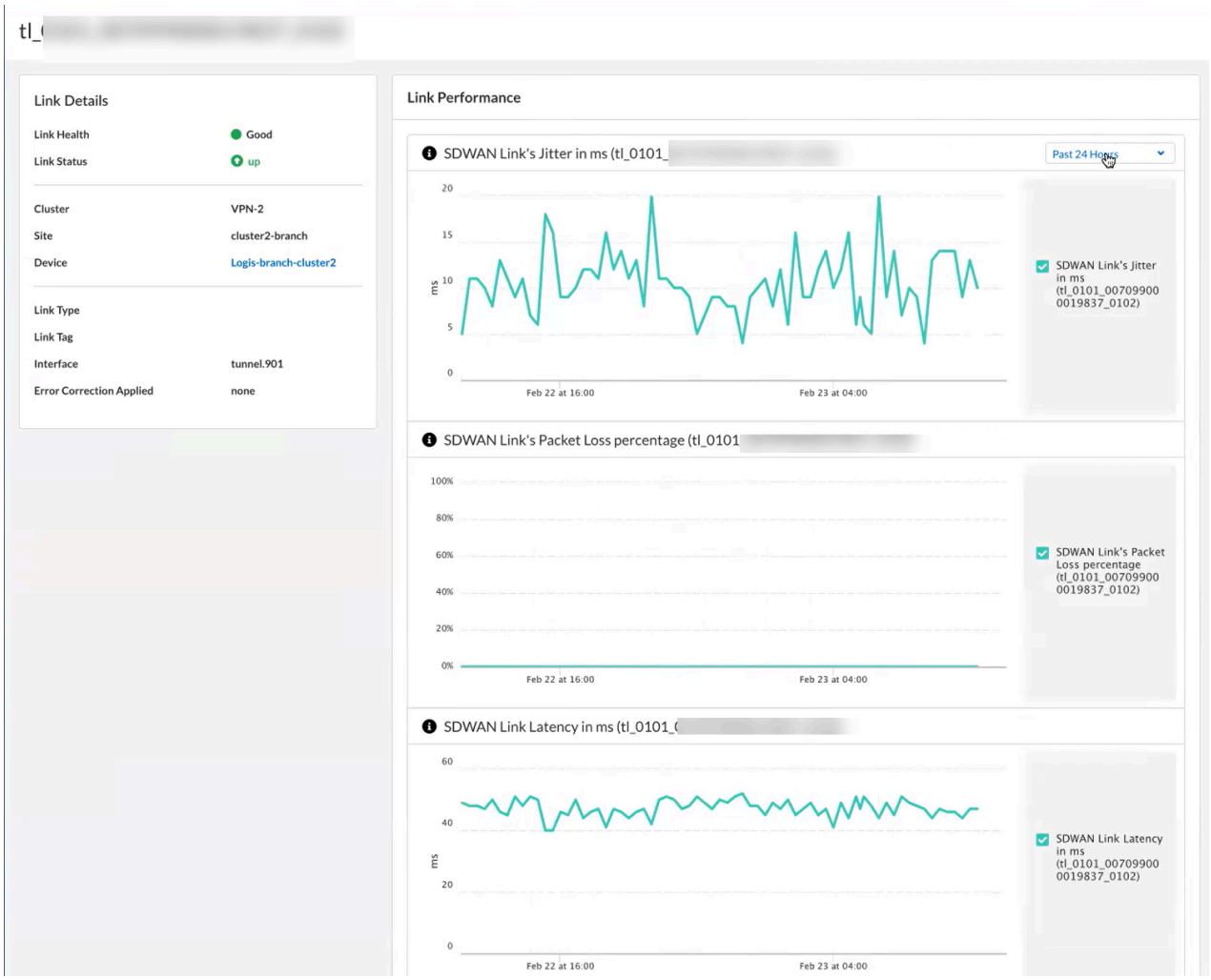
在何处可以使用？	需要提供什么？
• NGFW，包括由 软件 NGFW 积分提供资助的项目	❑ AIOps for NGFW Premium 或 Strata Cloud Manager Pro → 您可用的特性和功能Strata Cloud Manager取决于您使用的许可证。

对于所选时间期限和 VPN 集群，Strata Cloud Manager 根据接口指标（隧道停机、延迟、抖动和数据包丢失）的计算平均值显示前 5 个最差的链接。根据隧道停机、延迟、丢包和抖动的优先级对链路进行排名。较高的计算平均值表明链路质量较差。



单击查看更多可检查所有受影响的链接。

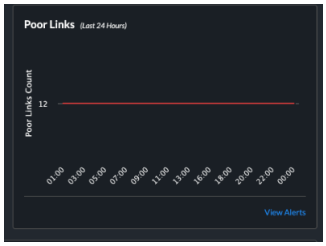
此外，单击链接可以查看其详细信息，包括基于链接性能的图表。



NGFW SD-WAN 指示板：较差链接

在何处可以使用？	需要提供什么？
• NGFW，包括由 软件 NGFW 积分提供资助的项目	❑ AIOps for NGFW Premium 或 Strata Cloud Manager Pro → 您可用的特性和功能Strata Cloud Manager取决于您使用的许可证。

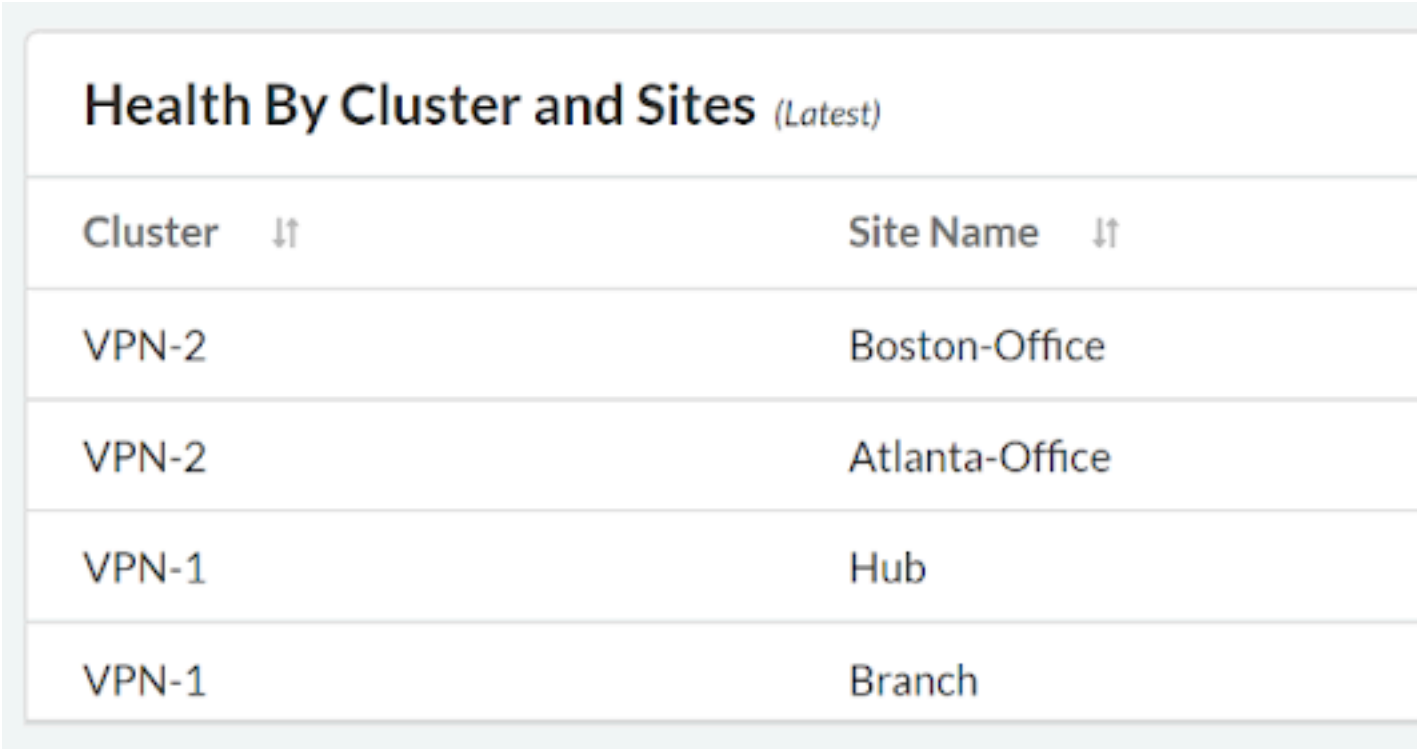
- 图表显示了过去 24 小时内检测到的较差链接的趋势。将光标悬停在趋势线上可以查看特定时间点的较差链接。
- 单击查看警报可查看由于链接较差而引发的相关警报。



NGFW SD-WAN 指示板：按群集和站点划分的运行状况

在何处可以使用？	需要提供什么？
• NGFW，包括由 软件 NGFW 积分提供资助的项目	❑ AIOps for NGFW Premium 或 Strata Cloud Manager Pro → 您可用的特性和功能Strata Cloud Manager取决于您使用的许可证。

查看每个站点的链接数量、其运行状况以及受影响的应用程序。



单击这些列下的编号链接以查看有关它们的详细信息。

指示板Prisma SD-WAN

在何处可以使用？	需要提供什么？
• Prisma SD-WAN	❑ Prisma SD-WAN 许可证 提高可见性所需的其他许可证和先决条件是： ❑ 解锁指示板中某些小部件的许可证 ❑ 用于预测分析的 WAN Clarity ❑ 具有查看指示板权限的角色 → 您可用的特性和功能Strata Cloud Manager取决于您使用的许可证。

该指示板显示什么？

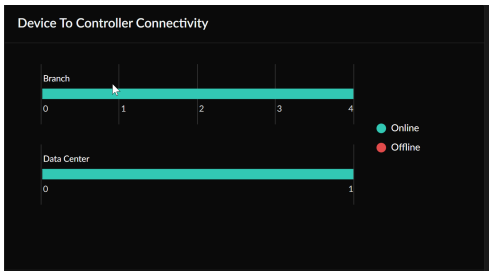
指示板向您展示了 Prisma SD-WAN 的网络、设备和应用程序指标的高级别图形视图。此外，它还向您展示了：

- 分支机构和数据中心设备与控制器的连接状态。
- 传入和传出流量的应用程序利用率数据。
- 过去一周租户所有分支站点的基本网络见解和报告。
- 按生成事件的数量显示有关顶级分支机构和数据中心站点的信息。
- 跨站点的链路质量指标，如MOS分数、丢包、抖动和延迟。
- 根据前三到六个月的信息预测站点级别的容量利用率。

Prisma SD-WAN 指示板：设备到控制器的连接

在何处可以使用？	需要提供什么？
• Prisma SD-WAN	❑ Prisma SD-WAN 许可证 提高可见性所需的其他许可证和先决条件是： ❑ 解锁指示板中某些小部件的许可证 ❑ 用于预测分析的 WAN Clarity ❑ 具有查看指示板权限的角色 → 您可用的特性和功能Strata Cloud Manager取决于您使用的许可证。

设备到连接小部件描述了分支机构和数据中心连接到 Prisma SD-WAN 控制器的在线和离线 ION 设备的数量。使用此交互式图表，您可以查看相应分支机构和数据中心的已声明设备的联机或脱机状态。

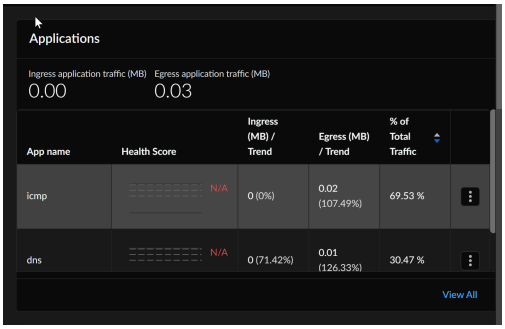


单击交互式图形上的 **Branch**（分支）或 **Data Center**（数据中心），您可以查看已声明和未声明的设备名称、状态、安装的软件版本、上次活动以及设备的冗余状态。

Prisma SD-WAN 指示板：应用程序

在何处可以使用？	需要提供什么？
• Prisma SD-WAN	❑ Prisma SD-WAN 许可证 提高可见性所需的其他许可证和先决条件是： ❑ 解锁指示板中某些小部件的许可证 ❑ 用于预测分析的 WAN Clarity ❑ 具有查看指示板权限的角色 → 您可用的特性和功能Strata Cloud Manager取决于您使用的许可证。

应用程序小部件显示在所选时间范围内，关于站点的应用程序利用的信息。将显示该时间范围的应用程序总进出流量。按流量显示的前 10 个应用程序与其他流量一起显示。单击 **View All**（查看全部），查看应用程序运行状况分布、TCP 应用程序随时间的运行状况分布、新流量、带宽利用率、所选时间范围的事务统计以及顶级应用程序。您可以深入查看指示板中所选时间范围内每个站点的应用程序性能和指标。

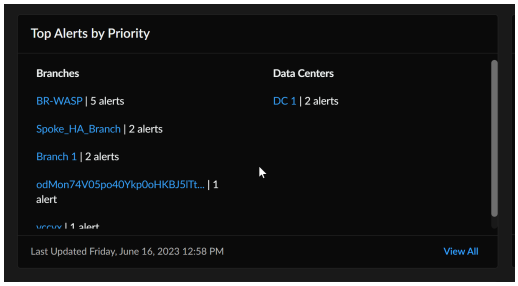


最初会显示所有 TCP 应用程序的指标，但可以选择前 10 个 TCP 应用程序中的任何一个，以更狭窄地关注特定的顶级应用程序。

Prisma SD-WAN 指示板：按优先级排序的主要警报

在何处可以使用？	需要提供什么？
• Prisma SD-WAN	❑ Prisma SD-WAN 许可证 提高可见性所需的其他许可证和先决条件是： ❑ 解锁指示板中某些小部件的许可证 ❑ 用于预测分析的 WAN Clarity ❑ 具有查看指示板权限的角色 → 您可用的特性和功能Strata Cloud Manager取决于您使用的许可证。

按优先级排列的前几个警报小部件按优先级显示前 5 个警报。您可以根据所选时间范围内生成的警报数量查看排名靠前的分支机构和数据中心站点的信息。您可以深入了解查看选定时间范围内每个站点的警报信息。



单击 **View All**（查看全部）可查看有关警报的以下信息：

- 警报的创建时间。
- 事件的名称。
- 主要受影响的对象。
- 警报的严重性。
- 警报的优先级。

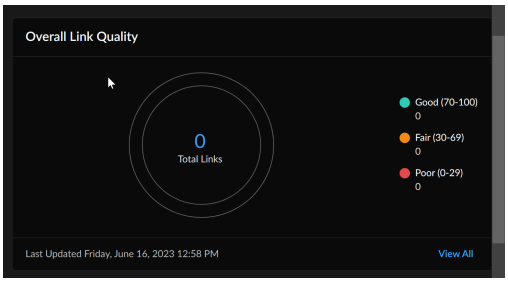
单击省略号可以对警报进行故障排除。

Prisma SD-WAN 指示板：整体链路质量

在何处可以使用？	需要提供什么？
• Prisma SD-WAN	❑ Prisma SD-WAN 许可证 提高可见性所需的其他许可证和先决条件是： ❑ 解锁指示板中某些小部件的许可证 ❑ 用于预测分析的 WAN Clarity

在何处可以使用？	需要提供什么？
	❑ 具有查看指示板权限的角色 → 您可用的特性和功能Strata Cloud Manager取决于您使用的许可证。

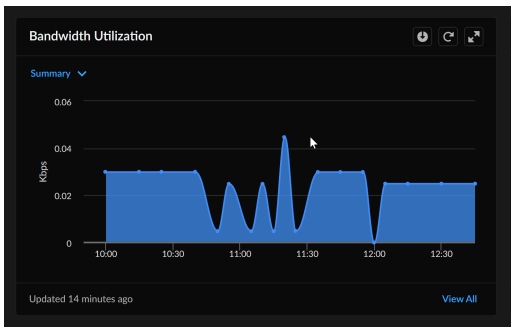
链接质量小部件提供在所选时间范围内，您的所有站点的当前状态的整体快照。您可以深入查看链路性能、链路数据包丢失、链路抖动和链路延迟，并允许您在链路质量指标指示板中更详细地分析要查看的信息。



Prisma SD-WAN 指示板：带宽利用率

在何处可以使用？	需要提供什么？
• Prisma SD-WAN	❑ Prisma SD-WAN 许可证 提高可见性所需的其他许可证和先决条件是： ❑ 解锁指示板中某些小部件的许可证 ❑ 用于预测分析的 WAN Clarity ❑ 具有查看指示板权限的角色 → 您可用的特性和功能Strata Cloud Manager取决于您使用的许可证。

带宽利用率小部件显示网络中跟踪上使用的带宽量。它是带宽峰值、特定站点消耗的总带宽和应用程序的可视化表示;如果上传是在传入、传出方向或两者中。



在 **Bandwidth Utilization**（带宽利用率）图表，通过应用程序或时间戳获得带宽利用率的更精细视图。通常，应用程序按其带宽利用率的顺序列出。该图表显示一段时间内消耗的带宽。1H 视图提

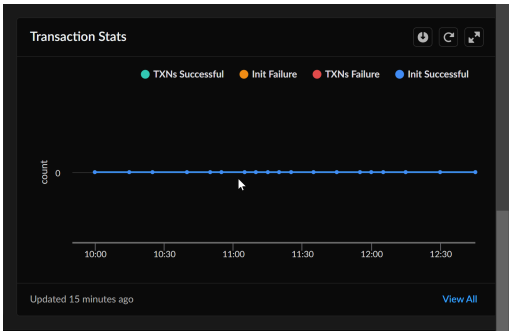
供每分钟的精细数据，而 1D 图片每 5 分钟显示一次数据。每个样本的 1D 图表数据平均超过 5 分钟。如果利用率持续超过 5 分钟，您可以在两个图表中看到相应的峰值利用率。

您可以使用小部件中的下载选项下载 PDF、CSV、XLS 或 PNG 格式的带宽利用率图表。

Prisma SD-WAN 指示板：事务统计信息

在何处可以使用？	需要提供什么？
• Prisma SD-WAN	❑ Prisma SD-WAN 许可证 提高可见性所需的其他许可证和先决条件是： ❑ 解锁指示板中某些小部件的许可证 ❑ 用于预测分析的 WAN Clarity ❑ 具有查看指示板权限的角色 → 您可用的特性和功能Strata Cloud Manager取决于您使用的许可证。

事务统计小部件提供 TCP 流的事务统计数据，包括特定应用程序或所有应用程序、特定路径或所有路径以及所有运行状况事件的启动/事务成功和失败。它测量网络以及在网络路径上运行的应用程序的性能和可用性。对于给定路径上的每个请求，Prisma SD-WAN 实时监控启动和数据传输事务的事务错误率。



从事务统计图表中，可以按带宽利用率或路径查看应用程序列表。您可以筛选成功的事务以获得事务失败统计的详细视图。该图表显示以下类别的成功或失败事务数量：

- **Init Sucessful**（初始化成功）：三次握手成功完成。
- **TXNs Sucessful**（**TXN** 成功）：三次握手完成后，数据传送成功。
- **Init Failure**（初始化失败）：未能完成三次握手。失败的原因可能包括防火墙配置错误、应用程序服务器问题、网络访问控制列表配置错误或 WAN 网络提供商问题。
- **TXNs Failure**（**TXN** 故障）：三次握手完成后，数据传输不成功。失败的原因可能包括防火墙配置错误、应用程序服务器问题、网络访问控制列表配置错误或 WAN 网络提供商问题。

您可以使用小部件中的下载选项下载 PDF、CSV、XLS 或 PNG 格式的带宽利用率图表。

Prisma SD-WAN 指示板：预测分析

在何处可以使用？	需要提供什么？
• Prisma SD-WAN	❑ Prisma SD-WAN 许可证 提高可见性所需的其他许可证和先决条件是： ❑ 解锁指示板中某些小部件的许可证 ❑ 用于预测分析的 WAN Clarity ❑ 具有查看指示板权限的角色 → 您可用的特性和功能Strata Cloud Manager取决于您使用的许可证。

预测分析插件可深入了解站点和应用程序的运行状况，并进行主动监控，以识别关键问题并更快地进行故障排除，从而提高服务水平。它识别关键站点、链接和应用程序，并根据 AI/ML 运行状况分数在租户级别将其归类为 **Good**（良好）、**Fair**（一般）和 **Poor**（较差）。该小部件包括根据前三到六个月的信息预测分支站点级别的容量利用率。

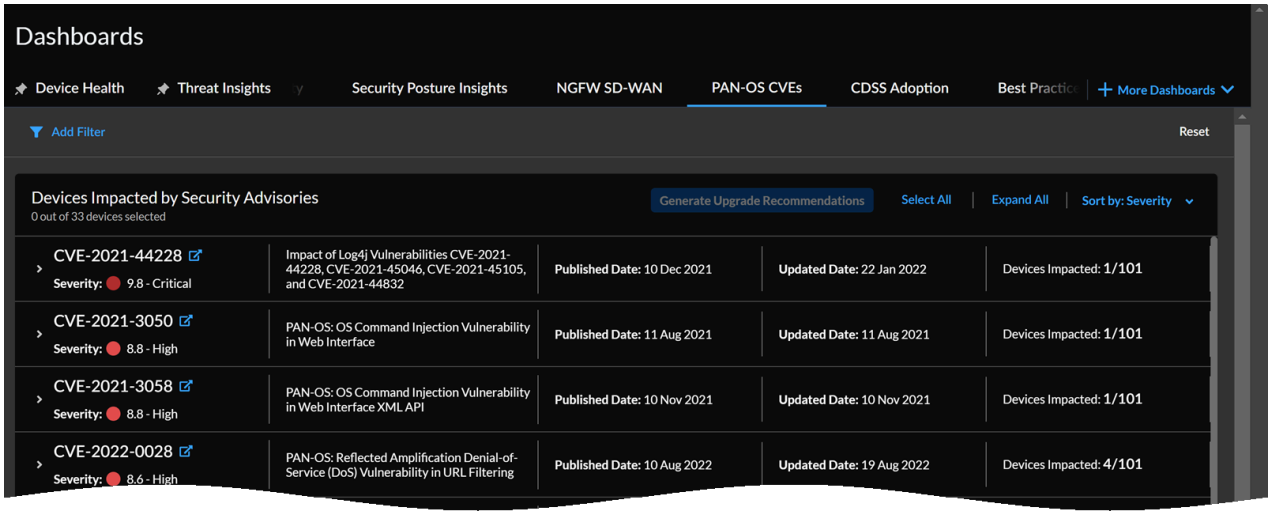
查看指标的默认时间范围为三小时；但是，您可以根据所需的信息范围将其调整为更短或更长的时间段。深入了解在过去 28 天内带宽利用率提高的前 10 个站点；每当 28 天预测不可用时，您可以查看七天的预测，并预测未来的分支机构容量利用率。

单击 **View All**（查看全部），深入了解分支机构站点、应用程序、链接、网络见解、过去 30 天流量增长的热门站点以及站点容量预测和异常。

指示板PAN-OS CVE

在何处可以使用？	需要提供什么？
• NGFW，包括由 软件 NGFW 积分提供资助的项目	❑ Strata Cloud Manager Essentials ❑ AIOps for NGFW Premium 或 Strata Cloud Manager Pro → 您可用的特性和功能Strata Cloud Manager取决于您使用的许可证。

- 要开始，请单击 **Dashboards**（指示板）**> More Dashboards**（更多指示板）**> PAN-OS CVE**。



该指示板显示什么？

指示板显示所有防火墙的汇总数据，以及载入到您的租户的 *Panorama*，并且还发送遥测数据。此外，它还显示了来自 *NGFW PSIRT* 数据库的 *CVE* 遥测数据。

PAN-OS CVE 指示板根据设备上已启用的功能显示受特定漏洞影响的设备数量。Strata Cloud Manager 分析已启用的功能以确定受 CVE 影响的设备。

了解受影响设备的漏洞后，可以使用升级建议功能规划修补程序。展开 CVE 并选择要升级以修复漏洞的防火墙，然后单击 **Generate Upgrade Recommendations**（生成升级建议）。您将被重定向到 NGFW - 升级建议，以查看生成的报告。

下面介绍如何评估影响设备的漏洞并生成升级建议，以便修复漏洞。

如何使用指示板上的数据？

此指示板可帮助您：

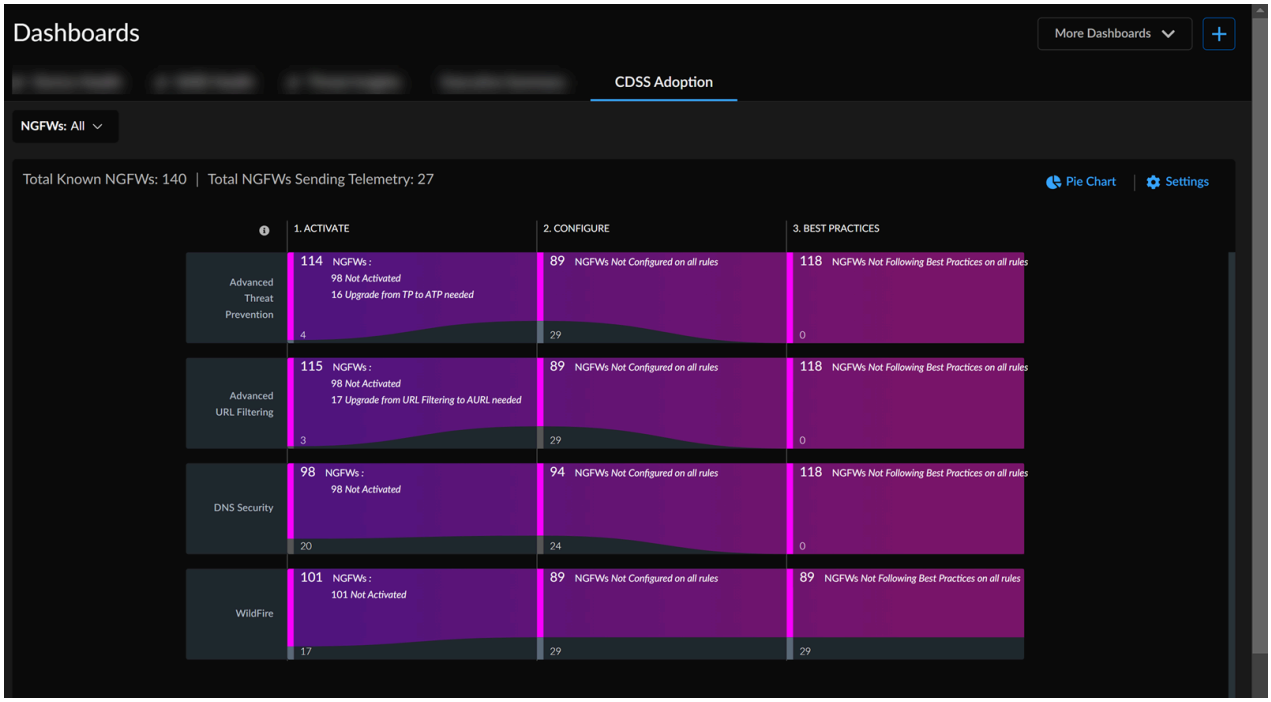
- 决定升级哪些设备以缓解漏洞。

- 通过展开 CVE 查看受影响的设备的详细信息，如主机名、型号、序列号、软件版本和上次遥测更新。
- 筛选 CVE，并按 **Severity**（严重性）或 **Devices Impacted**（受影响的设备）进一步排序。
- 单击 CVE，查看相关公告。

指示板CDSS 采用

在何处可以使用？	需要提供什么？
• NGFW，包括由 软件 NGFW 积分提供资助的项目	❑ Strata Cloud Manager Essentials ❑ AIOps for NGFW Premium 或 Strata Cloud Manager Pro → 您可用的特性和功能Strata Cloud Manager取决于您使用的许可证。

- 要开始，请单击 **Dashboards**（指示板） > **Posture**（态势） > **CDSS Adoption**（**CDSS** 采用）。



该指示板显示什么？

- 指示板显示已载入租户的所有防火墙的聚合数据，并且还发送遥测数据。
- 目前，此指示板仅支持四种安全订阅：*Advanced Threat Prevention*、高级 *URL* 筛选、*DNS* 安全和 *Wildfire*。

CDSS Adoption（**CDSS** 采用）指示板显示推荐的云交付安全服务 (CDSS) 订阅及其在设备中的使用情况。这可以帮助您识别安全漏洞并强化企业的安全状况。导航到此页面后，您将看到一个弹出窗口，要求您确认或更新 NGFW 中的区域角色，以获取准确的安全服务建议。您可以按照此弹出窗口中的链接将服务区映射到角色。

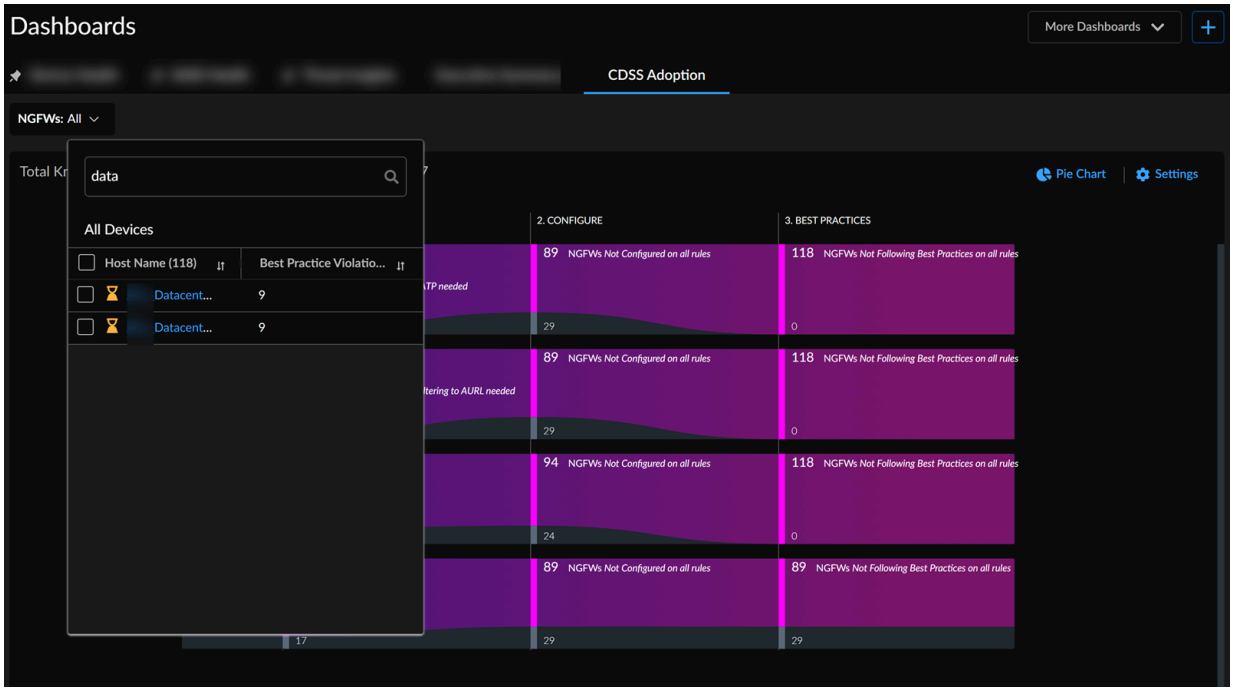
以下视频演示了如何使用 **CDSS Adoption**（**CDSS** 采用）指示板：

如何使用指示板上的数据？

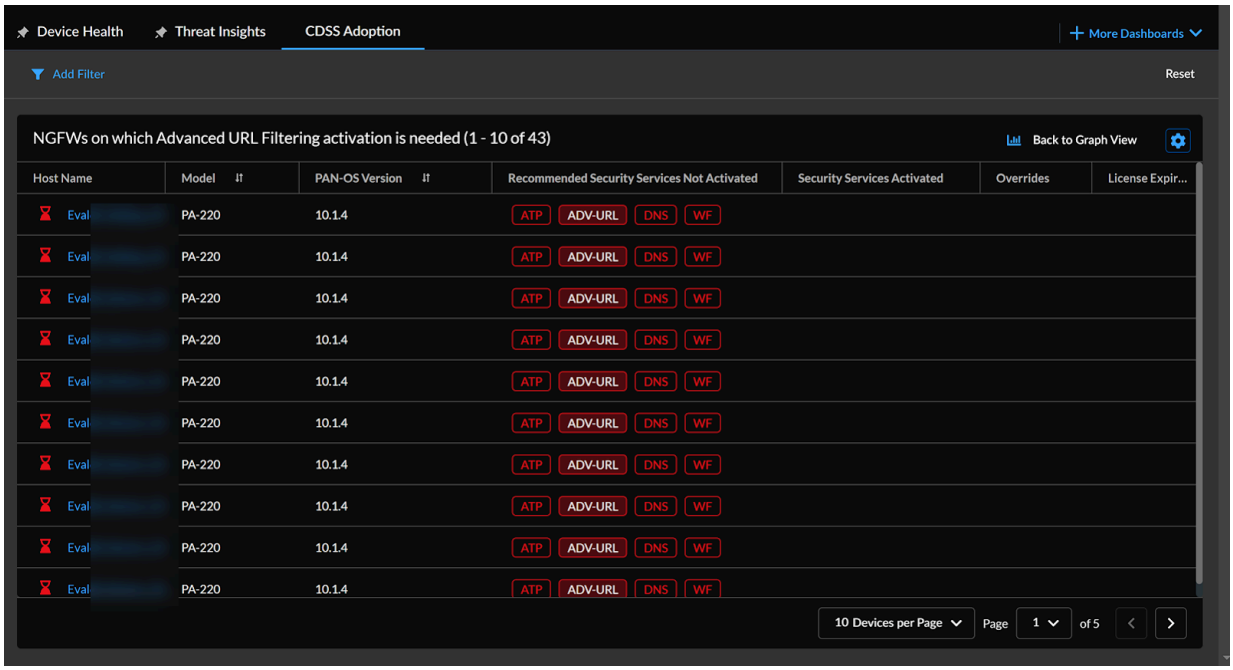
此指示板可帮助您完成以下工作：

- 在 Overview（概览）页面的顶部，您可以查看已知 NGFW 总数和在 NGFW 实例的 AIOps 中发送遥测数据的 NGFW 数量。CDSS 采用包括从激活、配置到遵守最佳实践。要跟踪每个订阅的进度，只需单击图表中的数字即可查看此旅程中需要更新的设备列表。要在设备中使用安全订阅许可证，您需要激活它，然后相应地设置服务或功能。

  要关注特定 NGFW 的安全服务数据，请根据它筛选图表。您还可以在此下拉列表中查看设备的最佳实践违规。

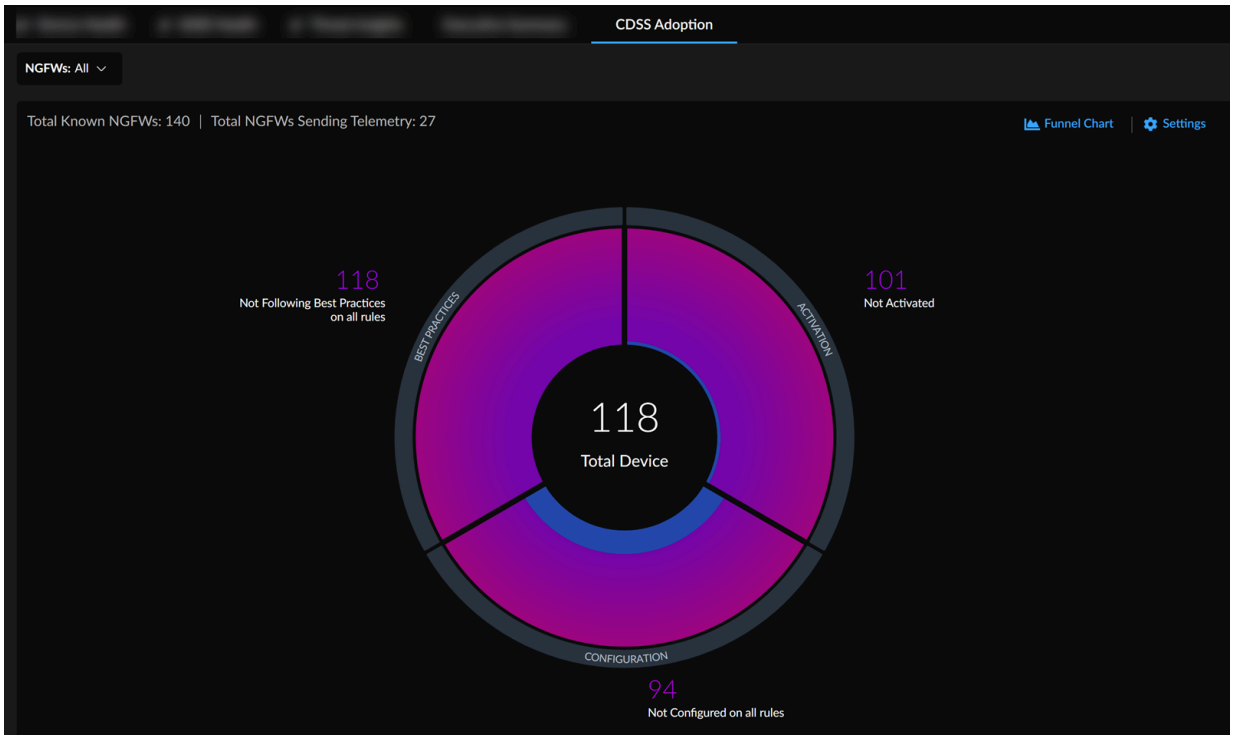


- 您可以单击 **ACTIVATE**（激活）、**CONFIGURE**（配置）或 **BEST PRACTICES**（最佳实践），以表格格式查看详细信息。

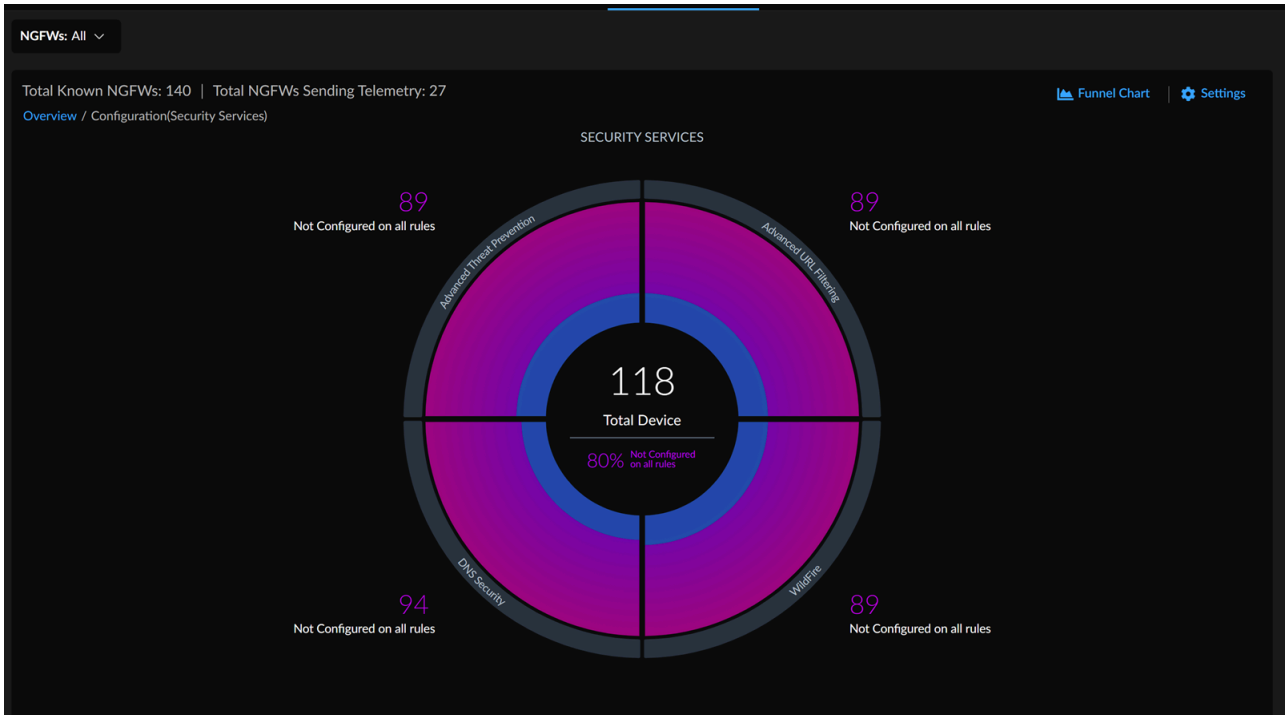


在此示例中，适用于 NGFW 的 AIOps 建议为 NGFW 激活高级 URL 筛选 (ADV-URL) 以及 Advanced Threat Prevention (ATP)、域名系统 (DNS) 和 WildFire (WF) 安全服务。您可以单击 **Back to Graph View**（返回图表视图），导航到“概览”页面。

- 您还可以以饼图格式查看相同的安全状况数据。单击饼图图标，以饼图形式查看推荐的安全服务信息。



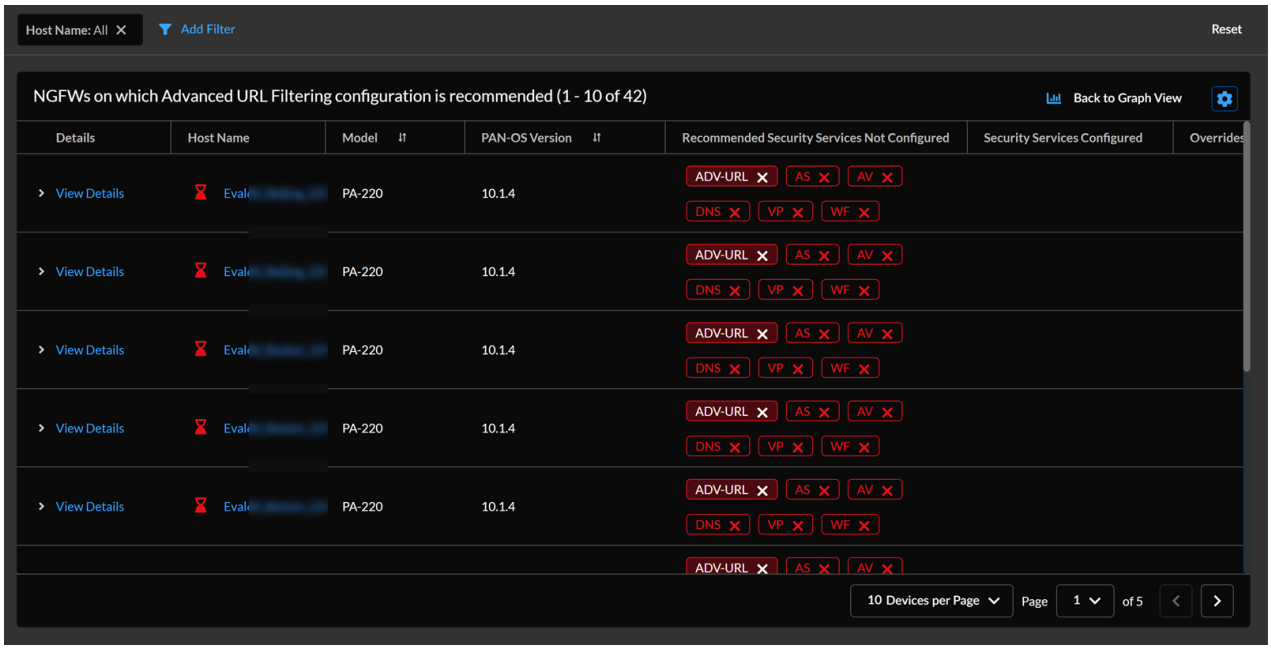
- 您可以单击饼图的各个部分以查看有关各个安全服务的信息。



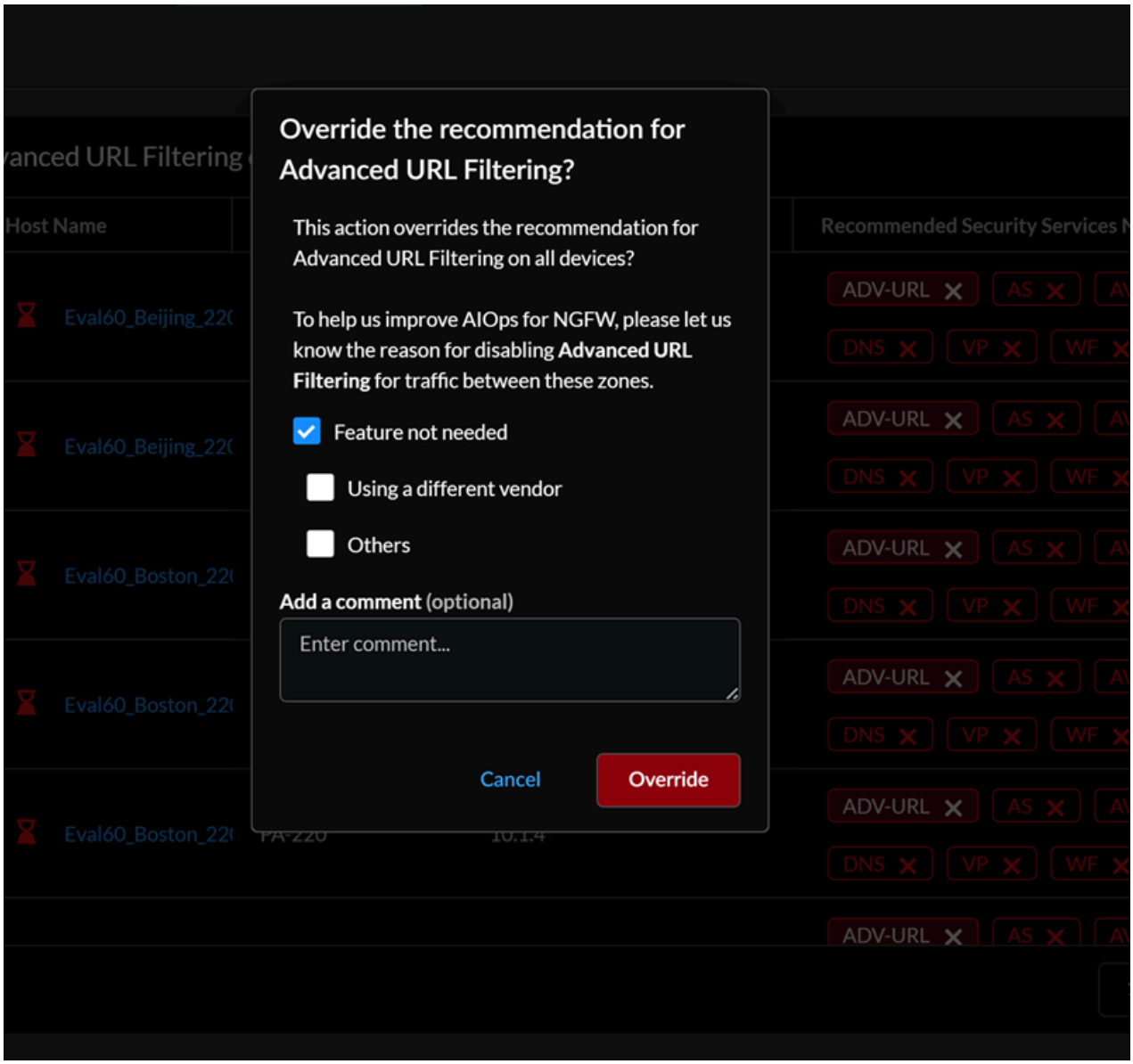
在此示例中，要查看未配置 DNS 安全性的 NGFW，您可以单击饼图的 **DNS Security** 部分的值，也可以单击饼图的 **DNS Security** 部分。

覆盖建议的安全服务

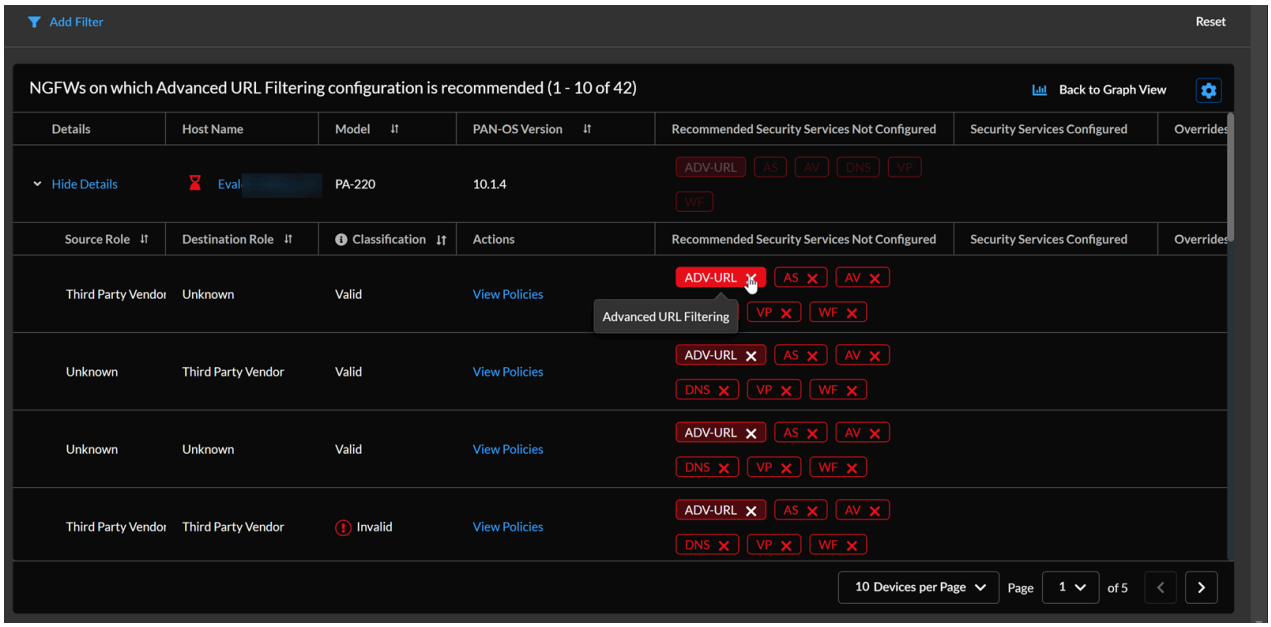
如果出于任何原因而不需要推荐的安全服务时，可以覆盖。要以表格形式查看详细信息，请单击 **CONFIGURE**（配置）下的值，您还可以覆盖“建议的安全服务”。



在此示例中，适用于 NGFW 的 AIOps 建议为设备配置高级 URL 筛选 (ADV-URL) 以及其他安全服务。您可以取消 NGFW 设备及其下所有服务区的 ADV-URL 安全服务。

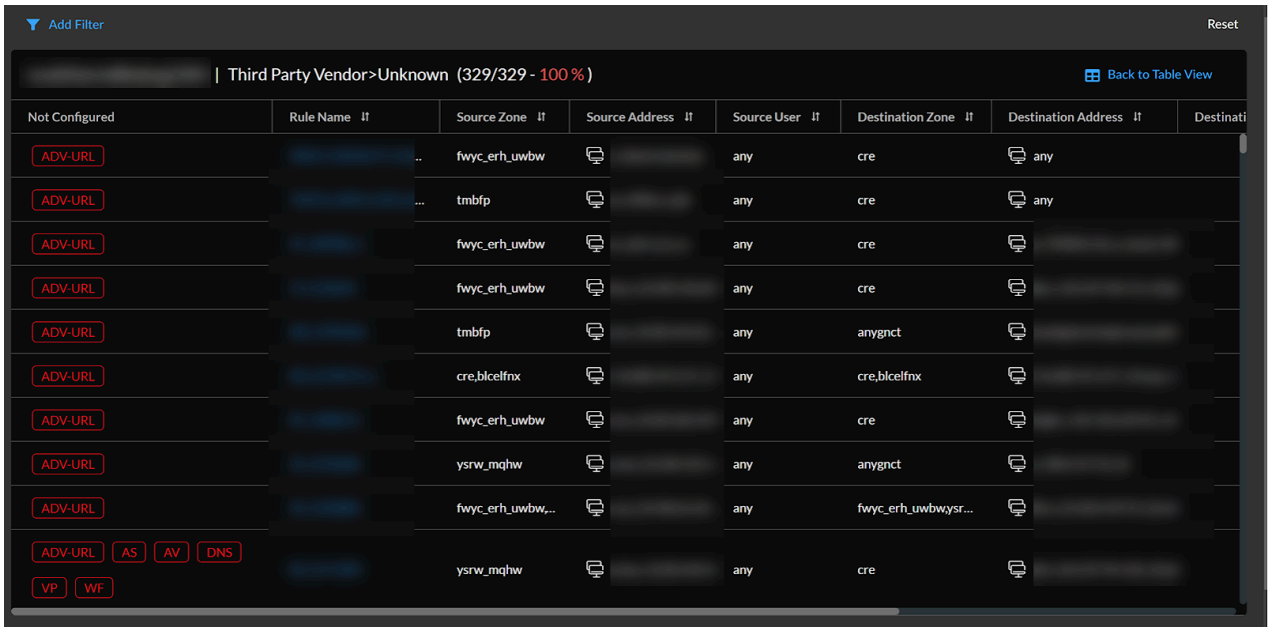


您还可以在服务区级别覆盖建议的安全服务。对于 NGFW，单击 **View Details**（查看详情），以便查看源和目标角色、策略及其建议的安全服务。



在此示例中，对于作为源角色，您可以将 **ADV-URL** 安全服务覆盖为 **Third Party Vendor**（第三方供应商），将目标角色覆盖为 **Unknown**（未知）。您还可以通过单击 **Overrides**（覆盖）列下的安全服务来恢复覆盖的建议。

对于与角色关联的策略，您可以 **View Policies**（查看策略）。选择一条规则可查看其详细信息，而无需离开应用程序。



单击 **Back to Table View**（返回表格视图）。以表格形式查看安全服务。

指示板功能采用

在何处可以使用？	需要提供什么？
• NGFW，包括由 软件 NGFW 积分提供资助的项目	❑ Strata Cloud Manager Essentials ❑ AIOps for NGFW Premium 或 Strata Cloud Manager Pro → 您可用的特性和功能Strata Cloud Manager取决于您使用的许可证。

- 要开始，请单击 **Dashboards**（指示板） > **Feature Adoption**（功能采用）。

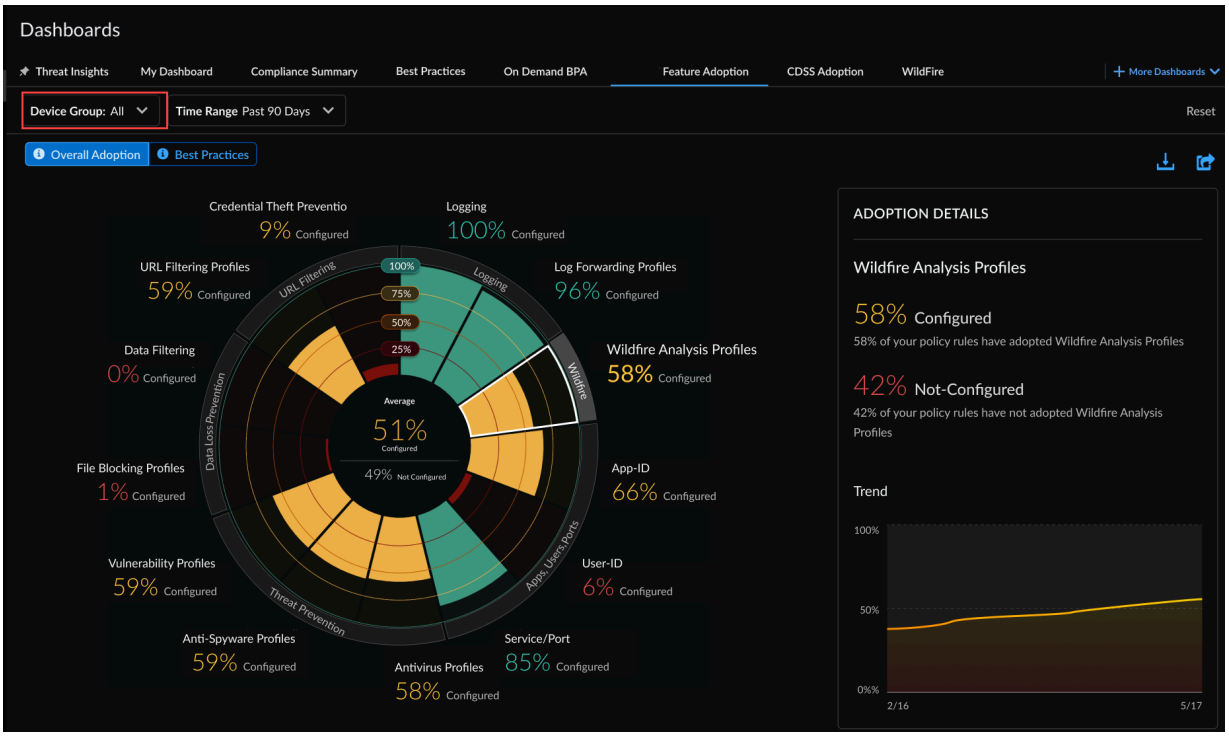
该指示板显示什么？

指示板显示已载入租户的所有防火墙的聚合数据，并且还发送遥测数据。

Feature Adoption（功能采用）指示板向您显示您在部署中使用的安全功能，您可以使用它来识别采用中的差距。这可以帮助您确保充分利用您的 Palo Alto Networks 安全订阅和防火墙功能。

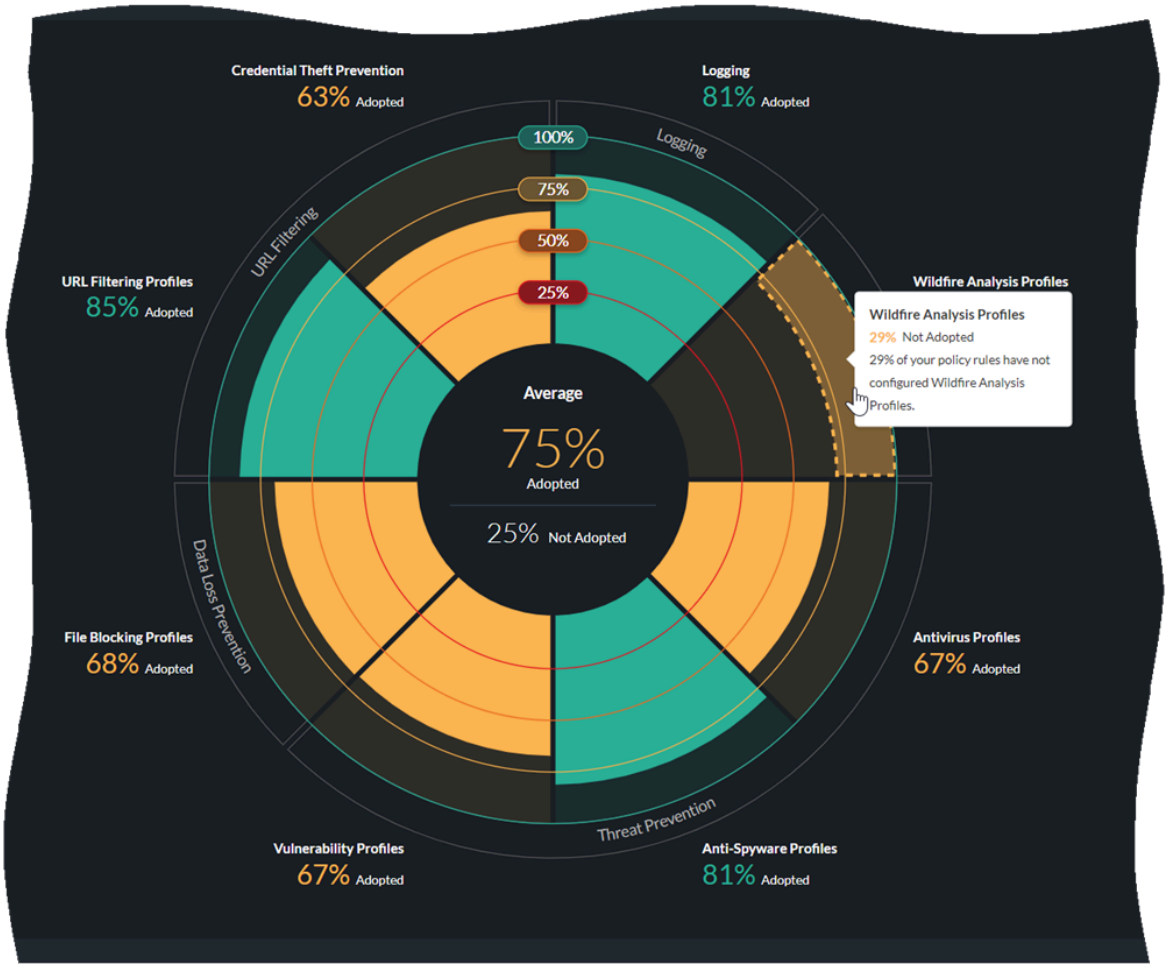
如何使用此指示板

为了关注特定防火墙集的功能采用情况，您可以根据设备组（包括 Panorama 管理的设备）筛选图表。您还可以查看历史采用趋势图表。

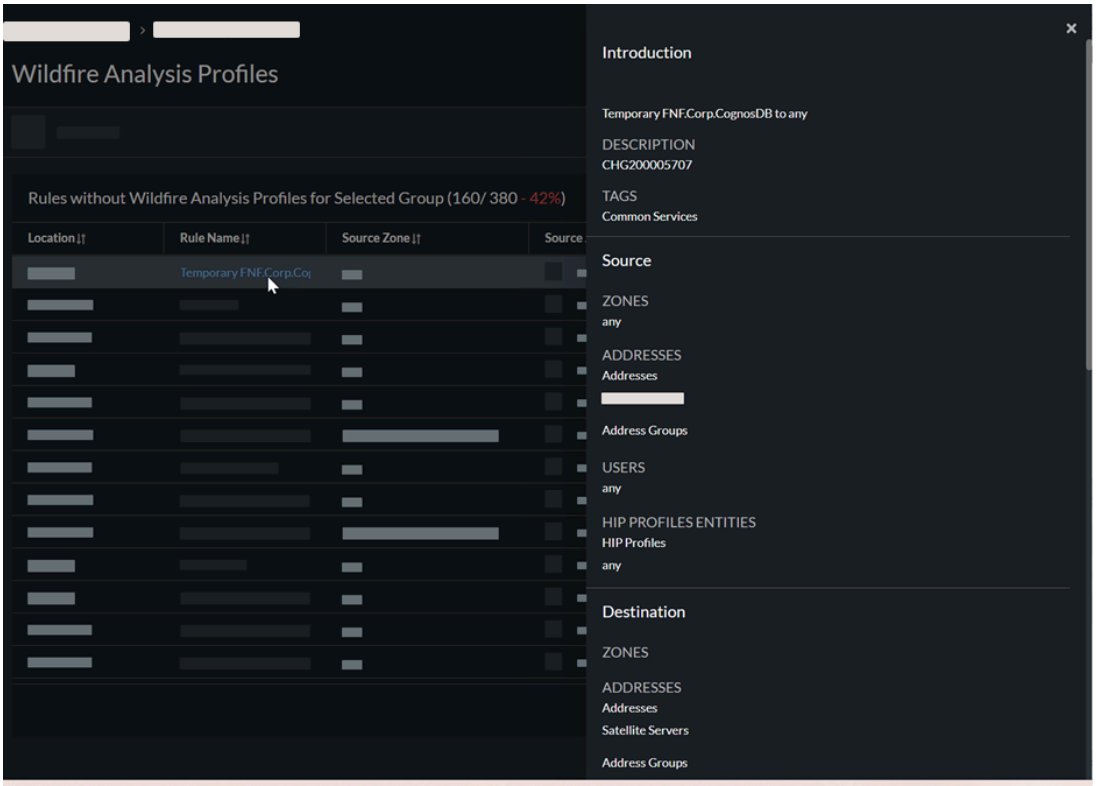


- 当您使用 *TSF* 生成按需 *BPA* 报告时，*TSF* 的采用信息将反映在功能采用指示板上。（*PAN-OS 9.1* 及更高版本的 *TSF*）
- 您可以以 *.csv* 格式导出采用数据，以便在 *Microsoft Excel* 等第三方应用程序中使用

选择图表上某个功能的部分可以查看哪些策略规则缺少该功能。



选择一条规则可查看其详细信息，而无需离开应用程序。

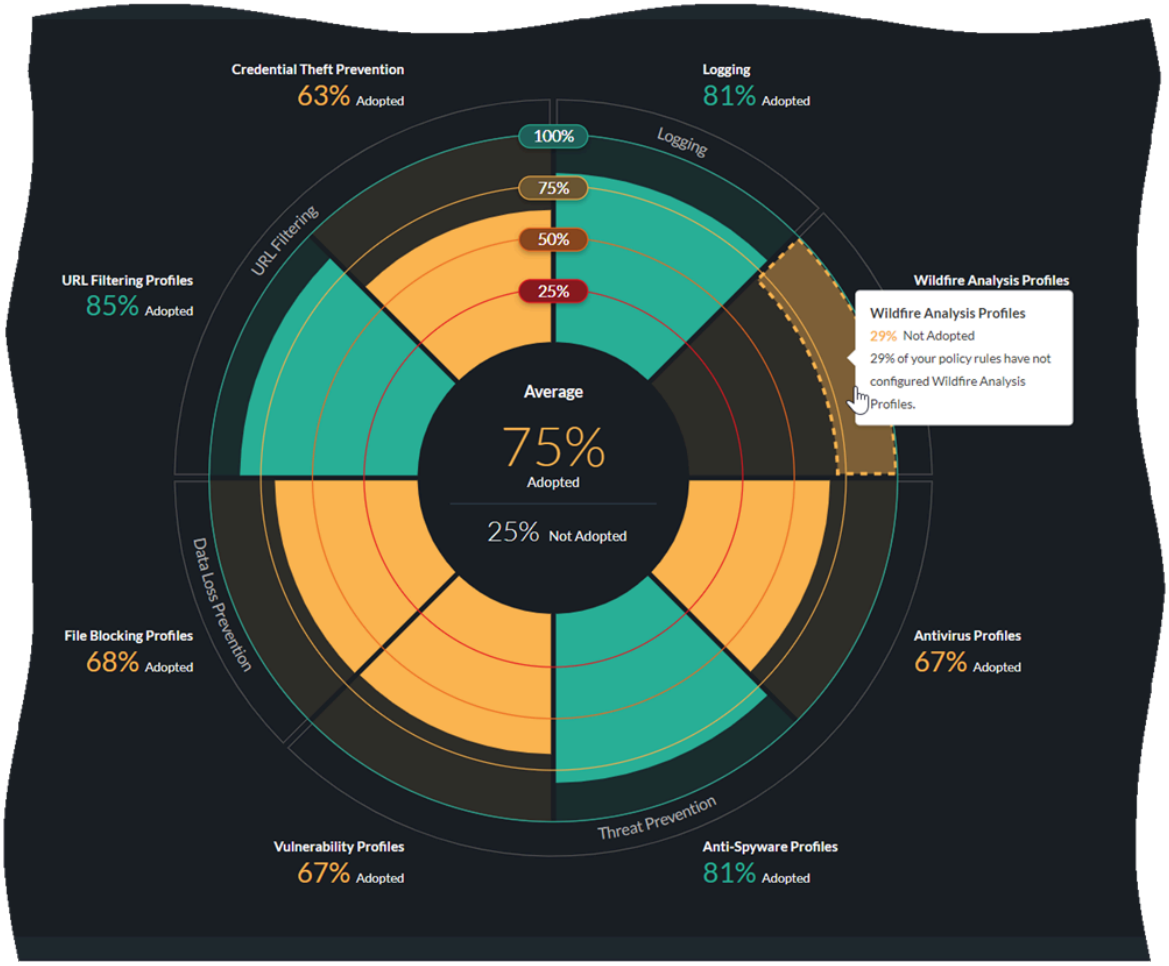


识别采用差距

该指示板显示了您的安全策略在哪些方面表现强劲，以及在能力采用方面存在哪些差距，您可以集中精力进行改进。要获得对流量的最大可见性和最大程度的防御攻击，请设立安全功能采用目标，并将以下建议用作最佳实践基准。根据基准评估当前态势，以确定安全策略功能采用中的差距。

采用摘要有助于识别可提高安全策略功能采用率的设备、服务区和领域。您可以按设备组、序列号以及 Vsys、服务区、基础架构区域、标记、规则详细信息和服务区映射查看采用信息。按设备组进行筛选以缩小范围并识别差距。

在 **Dashboard**（指示板） > **Feature Adoption**（功能采用）中，选择 **Overall Adoption**（整体采用）以检查以下功能的采用率。选择 **Best Practices**（最佳实践），以便查看符合 Palo Alto Networks 最佳实践的这些功能的采用率。使用此信息作为差距识别标准 — 如果实际采用率与建议不符，则计划缩小差距：



- 将 WildFire Analysis、防病毒软件、防间谍软件、漏洞和文件阻止安全配置文件应用于允许流量的所有规则，目标是达到或接近 100# 的采用率。如果您未将配置文件应用于允许规则，请确保有充分的不应用配置文件的业务原因。

  在所有允许规则上配置安全配置文件可让防火墙检查已解密的流量是否存在威胁，无论应用程序或服务/端口如何。更新配置后，您可以运行非遥测设备的 BPA 来测量进度并捕获未附加安全配置文件的新规则。

  您可以将 *WildFire* 配置文件应用于没有 *WildFire* 许可证的规则。覆盖范围仅限于 *PE* 文件，但这仍然可以提供对未知恶意文件的有用可见性。

- 在防间谍软件配置文件中，将 DNS Sinkhole 应用于所有规则，以防止遭到入侵的内部主机发送恶意和自定义域的 DNS 查询，从而识别和跟踪可能受到攻击的主机，并避免 DNS 检查中的漏洞。启用 DNS Sinkhole 可在不影响可用性的情况下保护您的网络，因此您可以且应该立即启用它。
- 对所有出站 Internet 流量应用 URL 筛选和凭证防窃（网络钓鱼）保护。

在采用摘要的应用程序、用户和端口摘要中，检查以下功能的采用率。使用建议作为差距识别条件 — 如果实际采用率与建议不符，则计划缩小差距：

- 将 App-ID 应用到尽可能接近 100# 的规则。将 User-ID 应用到具有用户的源服务区或地址范围的所有规则（某些服务区可能没有用户源；例如，数据中心服务区的源应该是服务器，而不是

用户）。利用 App-ID 和 User-ID 创建策略，允许适当的用户使用受限制（和容忍）的应用程序。明确阻止恶意和不需要的应用程序。

- 目标为 100# 或接近 100# 的服务/端口采用率 — 不允许非标准端口上的应用程序，除非有充分的业务原因。

在“采用摘要”的日志摘要中，检查以下功能的采用率。使用建议作为差距识别条件 — 如果实际采用率与建议不符，则计划缩小差距：

- 目标是采用或接近 100# 的日志和日志转发采用率。
- 在所有服务区配置服务区保护配置文件

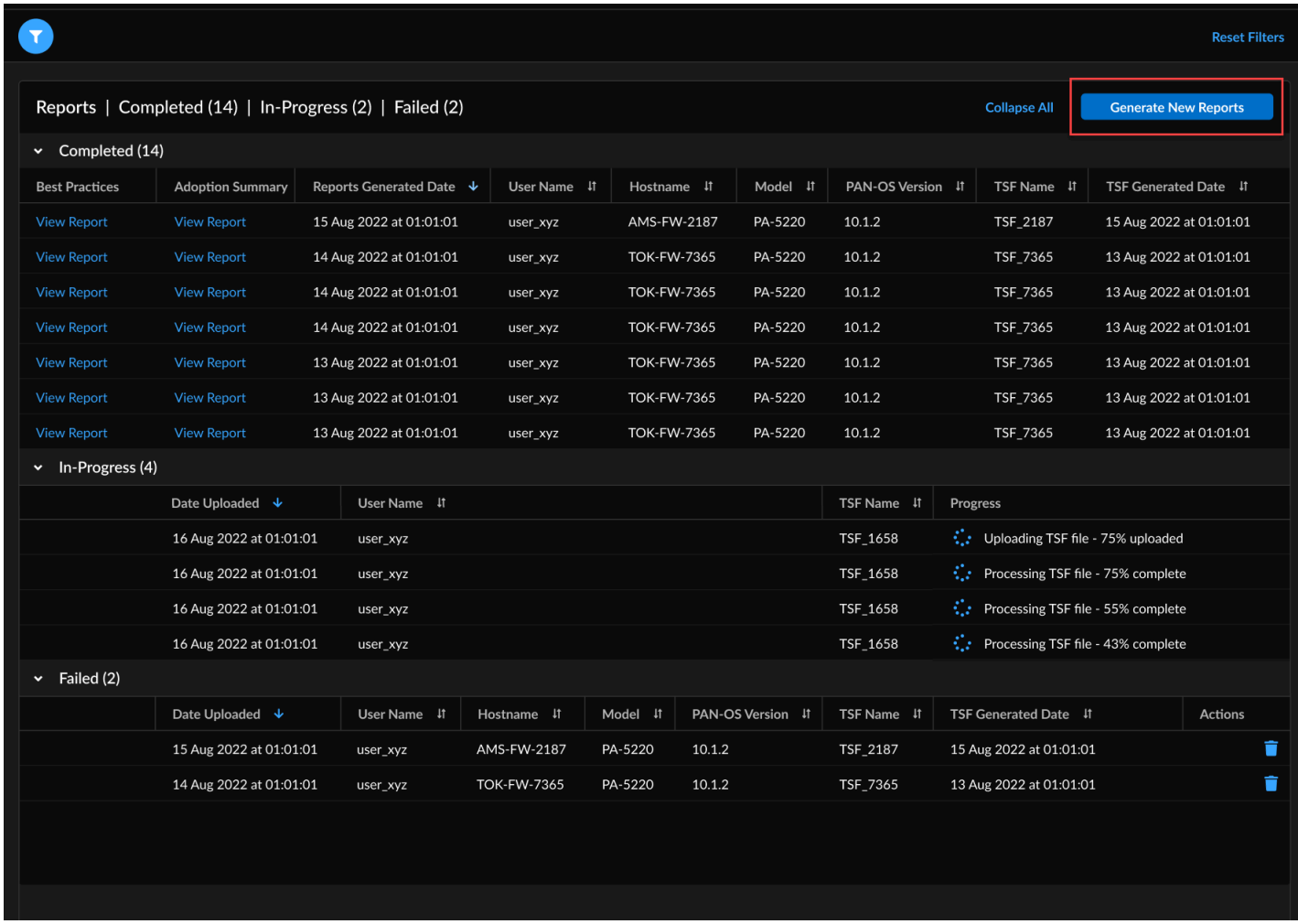
在摘要中：

功能	采用率目标
WildFire	尽可能接近 100# 的安全策略规则
反病毒	尽可能接近 100# 的安全策略规则
防间谍软件	尽可能接近 100# 的安全策略规则
漏洞	尽可能接近 100# 的安全策略规则
文件传送阻止	尽可能接近 100# 的安全策略规则
URL 筛选和凭据防窃	所有出站 Internet 流量
App-ID	尽可能接近 100# 的安全策略规则
User-ID	具有用户的源服务区或地址范围的所有规则
服务/端口	尽可能接近 100# 的安全策略规则
记录	尽可能接近 100# 的安全策略规则
日志转发	尽可能接近 100# 的安全策略规则
服务区保护	所有服务区

指示板按需 BPA

在何处可以使用？	需要提供什么？
• NGFW，包括由 软件 NGFW 积分提供资助的项目	❑ Strata Cloud Manager Essentials ❑ AIOps for NGFW Premium 或 Strata Cloud Manager Pro → 您可用的特性和功能Strata Cloud Manager取决于您使用的许可证。

- 要开始，请转到 **Dashboards**（指示板） > **On Demand BPA**（按需 **BPA**）。



该指示板显示什么？

指示板根据上传的设备 *TSF* 文件显示最佳实践评估 *(BPA)* 报告。

现在，您可以直接从 Strata Cloud Manager 中运行最佳实践评估 (BPA) 和功能采用摘要。只需上传技术支持文件 (TSF)。您可以为未发送遥测数据或未加入 AIOps for NGFW 的设备生成按需 BPA 报告。

如何使用指示板上的数据？

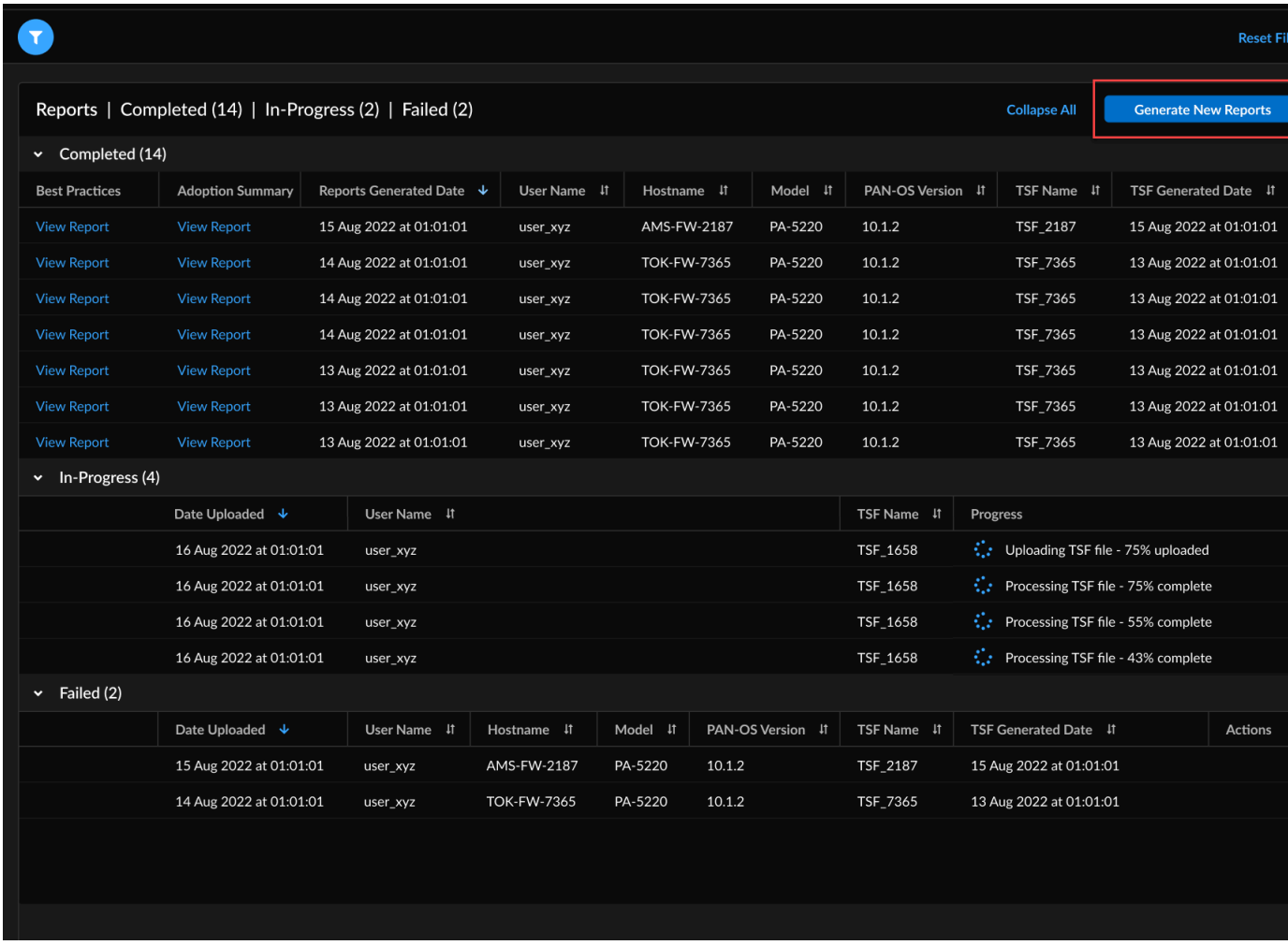
BPA 根据 Palo Alto Networks 的最佳实践评估您的安全状况，并优先考虑设备的改进。安全最佳实践可防止已知和未知威胁，缩小攻击范围并提供流量可见性，从而可以了解和控制网络上的应用程序、用户以及内容。此外，最佳实践还包括检查互联网安全中心的关键安全控制 (CSC)。请参阅最佳实践指南以强化安全态势并实施改进。

按需生成 BPA 报告

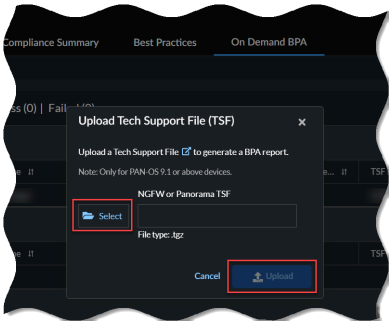
按照以下步骤按需生成 BPA 报告。

STEP 1 | 转到 **Dashboards**（指示板） > **On Demand BPA**（按需 **BPA**）。

STEP 2 | **Generate New BPA Report**（生成新的 **BPA** 报告）。



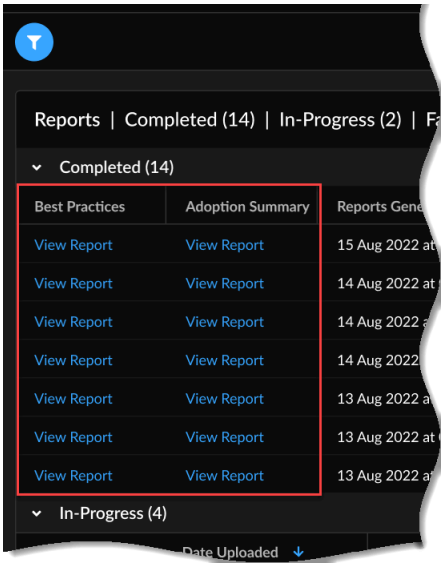
STEP 3 | **Select TSF**（选择 **TSF**）和 **Upload TSF**（上传 **TSF**）文件。



上传时间取决于 .tgz 文件大小和互联网速度。如果文件较大，上传文件可能需要几分钟时间。展开 **In-Progress**（进行中）可查看 TSF 文件的状态。

- 按需 *BPA* 仅支持 *.tgz* 文件格式的技术支持文件 *(TSF)*。
- 按需 *BPA* 支持使用 *PAN-OS* 版本为 *9.1* 或更高版本的设备提供的 *TSF* 来生成报告。
- 有关 *Palo Alto Networks* 数据采集、处理和遥测存储的信息，请参阅信任中心的 AIOps for NGFW 隐私。

STEP 4 | 在下面 **View Report**（查看报告）**Completed**（已完成），以便查看结果。



指示板SASE 运行状况

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama or Strata Cloud Manager)	• 以下之一： ❑ Prisma Access 和 ADEM 可观测性 ❑ Strata Cloud Manager Pro • 有权查看指示板的角色 → 您可用的特性和功能Strata Cloud Manager取决于您使用的许可证。

该指示板显示什么？

此指示板向您显示当前连接到 Prisma Access 的移动用户、远程站点和应用程序（如果您购买了 AI-Powered ADEM 许可证）的总体运行状况。圆圈中的数字表示当前从显示的 Prisma Access 位置连接的用户或站点数。点代表单个用户或站点。地图上蓝色背景的区域表示该区域中显示的数字是预测或预报。

使用以下一个或多个筛选器筛选此指示板中显示的数据

- 时间范围
- Prisma Access 位置
- 源位置

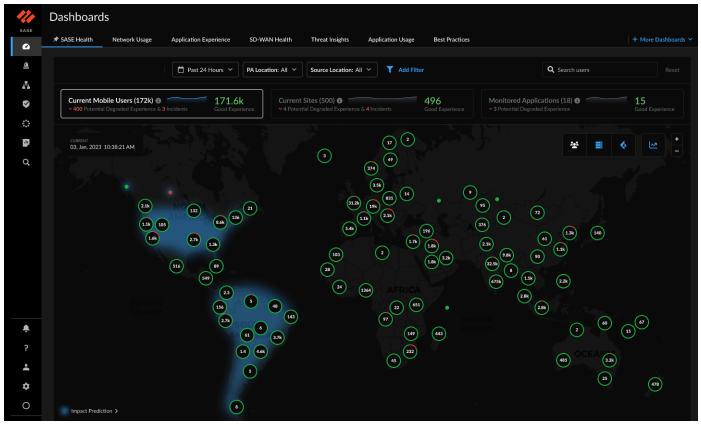
如何使用指示板中的数据？

使用指示板，获得连接到 Prisma Access 的移动用户和远程站点的概况和总体运行状况，这些站点按其在地图上的位置进行分类。您也可以在此指示板中查看他们的总体运行状况。

SASE 运行状况指示板：当前移动用户 - 地图视图

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama or Strata Cloud Manager)	• 以下之一： ❑ Prisma Access 和 ADEM 可观测性 ❑ Strata Cloud Manager Pro • 有权查看指示板的角色 → 您可用的特性和功能Strata Cloud Manager取决于您使用的许可证。

SASE Health（**SASE** 运行状况）指示板中的 **Current Mobile Users**（当前移动用户）选项卡显示所有位置的移动用户体验细分概览。圆圈中的数字对应于当前使用 GlobalProtect 连接到 Prisma Access 的移动用户数。点代表单个移动用户。绿色圆圈或圆点表示良好的用户体验得分。同样，红色表示体验值降低。降级体验得分由“一般”和“较差”得分组合而成。**Current Mobile Users**（当前移动用户）右侧的线形图向您显示所选 **Time Range**（时间范围）内所有移动用户的平均体验得分趋势。

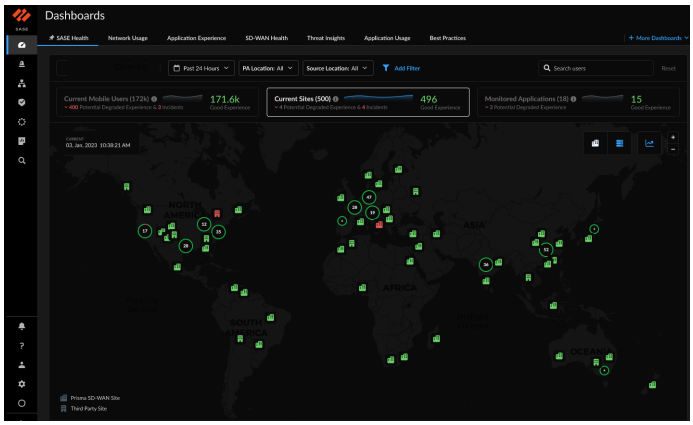


单击 **Potential Degraded Experience**（潜在降级体验）或 **Incidents**（事件）旁的数字（代表潜在降级体验用户计数），在左侧打开的窗格中查看降级用户体验的详细信息。

SASE 运行状况指示板：当前站点 - 地图视图

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama or Strata Cloud Manager)	• 以下之一： ❑ Prisma Access 和 ADEM 可观测性 ❑ Strata Cloud Manager Pro • 有权查看指示板的角色 → 您可用的特性和功能Strata Cloud Manager取决于您使用的许可证。

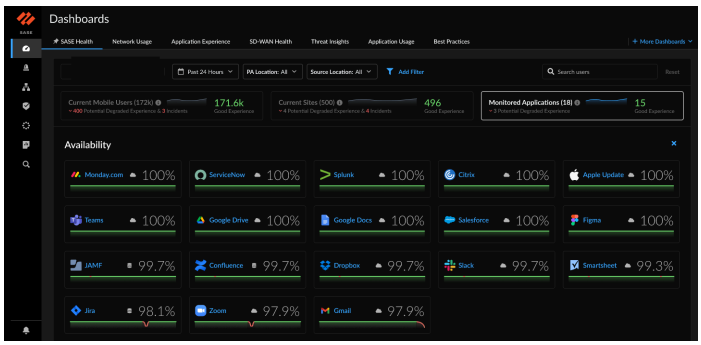
此指示板显示连接到全球 Prisma Access Locations 的已配置站点的数量。括号中的数字是已连接网站的总数，卡片右侧的数字是获得良好体验分数的网站数。在计算已连接网站的数量时，不会排除因任何原因无法获得体验分数的网站。蓝色折线图表示一段时间内所有网站的平均体验得分趋势。在当前站点下方，您会看到体验评分下降（较差）的网站数量以及所有网站的事件数量。事件可以分为以下一个或多个类别：基础设施、网络服务、数据中心和第三方站点（数据中心已关闭）。



SASE 运行状况指示板：受监控的应用程序

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama or Strata Cloud Manager)	• 以下之一： ❑ Prisma Access 和 ADEM 可观测性 ❑ Strata Cloud Manager Pro • 有权查看指示板的角色 → 您可用的特性和功能Strata Cloud Manager取决于您使用的许可证。

请参阅 **SASE Health**（**SASE** 运行状况）指示板的 **Monitored Applications**（受监控的应用程序）选项卡中的应用程序可用性指标。此指示板显示通过 ADEM 监控的应用程序数量，以及其中有多少应用程序分数下降。此数字考虑了 Mobile Users 和 Remote Sites 的应用程序体验。应用程序体验分数为 “较差”和“一般”的应用程序被视为体验降级。您还可以查看应用程序在使用筛选条件选择的时间范围内的可用性。



应用程序名称右侧的数字表示该应用程序可用的 **Time Range**（时间范围）。

监视：Strata Cloud Manager

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW，包括由 软件 NGFW 积分提供资助的项目 • Prisma SD-WAN	这些许可证中的每一个都包括 Strata Cloud Manager 访问权限： ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro ❑ Prisma SD-WAN 提高可见性所需的其他许可证和先决条件是： ❑ ADEM 可观测性 ❑ 远程网络自主 DEM ❑ 人工智能驱动的 ADEM ❑ WAN Clarity 报告 ❑ 有权查看指示板的角色 → 您可用的特性和功能Strata Cloud Manager取决于您使用的许可证。

全面了解您的网络流量，以及您使用 Strata Cloud Manager 管理的产品和订阅。您可以在 Prisma Access 中保护性地监视远程网络、应用程序、NGFW 设备和移动用户的运行状况和连接状态。Strata Cloud Manager 还提供了监视常用网络服务的性能、订阅许可证的消费详细信息以及管理用于分析连接问题的工具的功能。Prisma SD-WAN 用户还可以在此集中监控 Prisma SD-WAN 应用、ION 设备、数据中心的运行状况和连接状态。

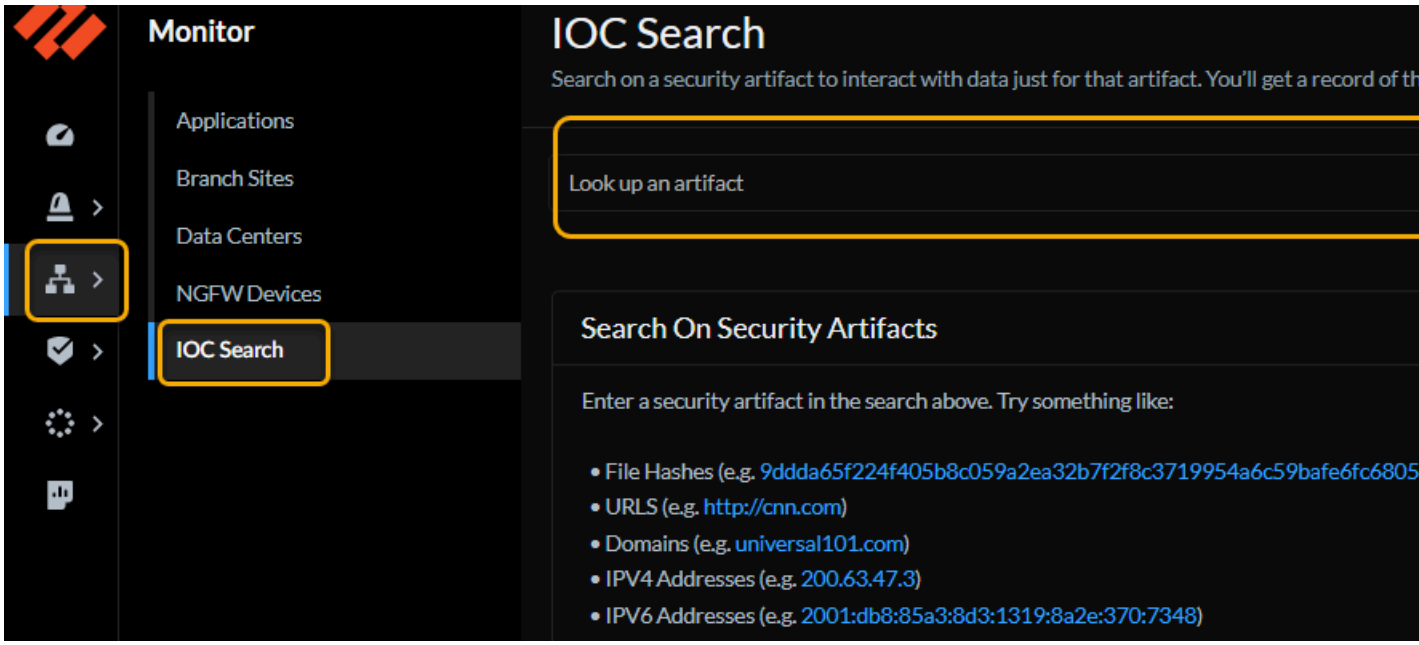
监视：IOC 搜索

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW，包括由 软件 NGFW 积分提供资助的项目 • Prisma SD-WAN	这些许可证中的每一个都包括 Strata Cloud Manager 访问权限： ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro ❑ Prisma SD-WAN 提高可见性所需的其他许可证和先决条件是： ❑ ADEM 可观测性 ❑ 远程网络自主 DEM ❑ 人工智能驱动的 ADEM ❑ WAN Clarity 报告 ❑ 有权查看指示板的角色 → 您可用的特性和功能Strata Cloud Manager取决于您使用的许可证。

您可以搜索安全工件以与该工件的数据进行交互。搜索结果包括：

- 该工件在您的网络中的历史和活动。评估该工件在您的网络中的流行程度，并与业内同行进行比较。
- Palo Alto Networks 对该工件的威胁情报基于对 Palo Alto Networks 处理和分析的所有流量的分析。
- 综合第三方对该工件的分析结果。

要开始，请单击 **Monitor**（监控） > **IOC Search**（**IOC** 搜索）。

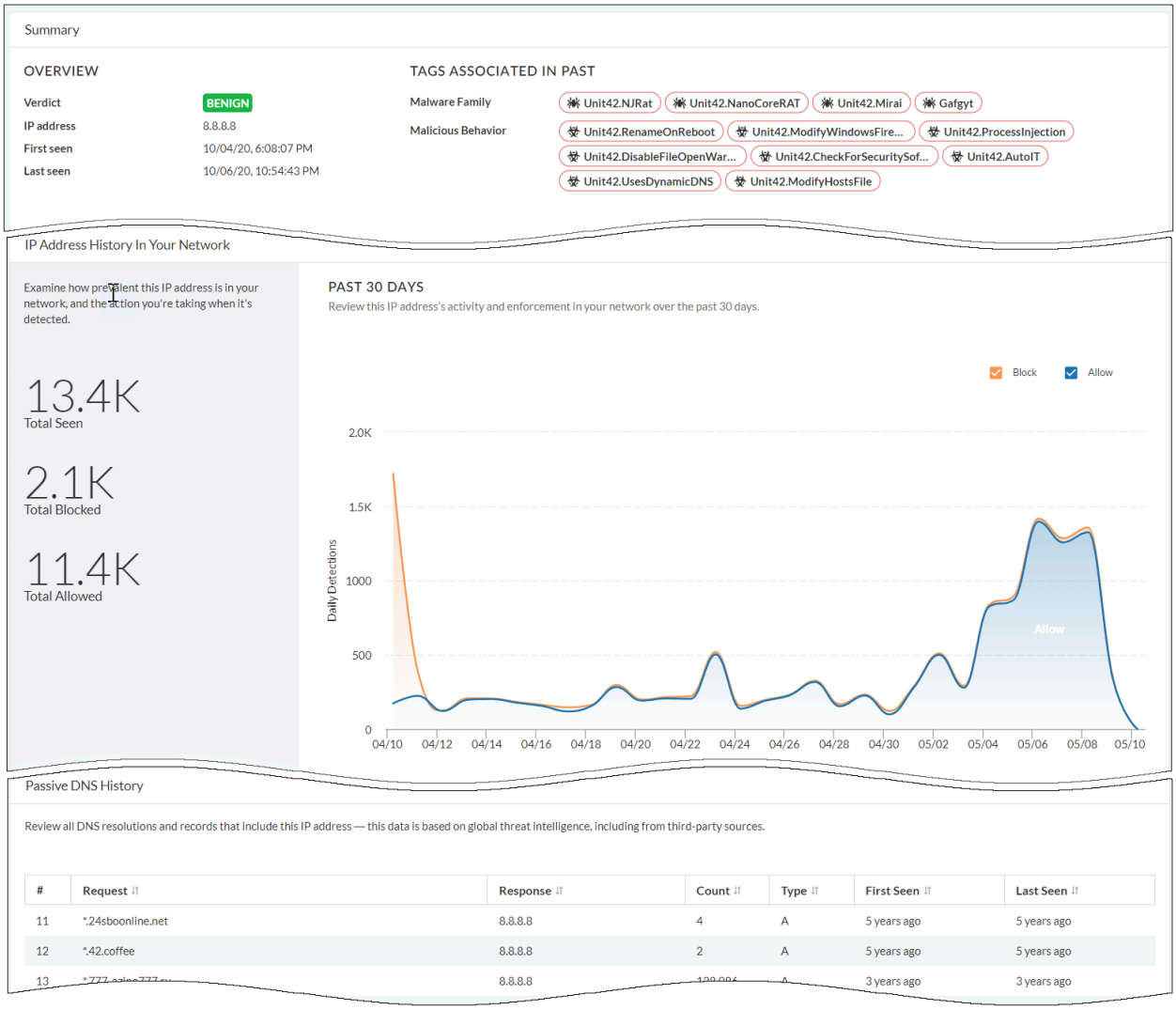


首先，搜索以下类型的工件之一：文件哈希、**URL**、域或 **IP** 地址（IPv4 或 IPv6）。

IP 地址

您可以查找某个 IP 地址来分析您网络中与 IP 地址活动相关的威胁信息。搜索结果显示以下数据：

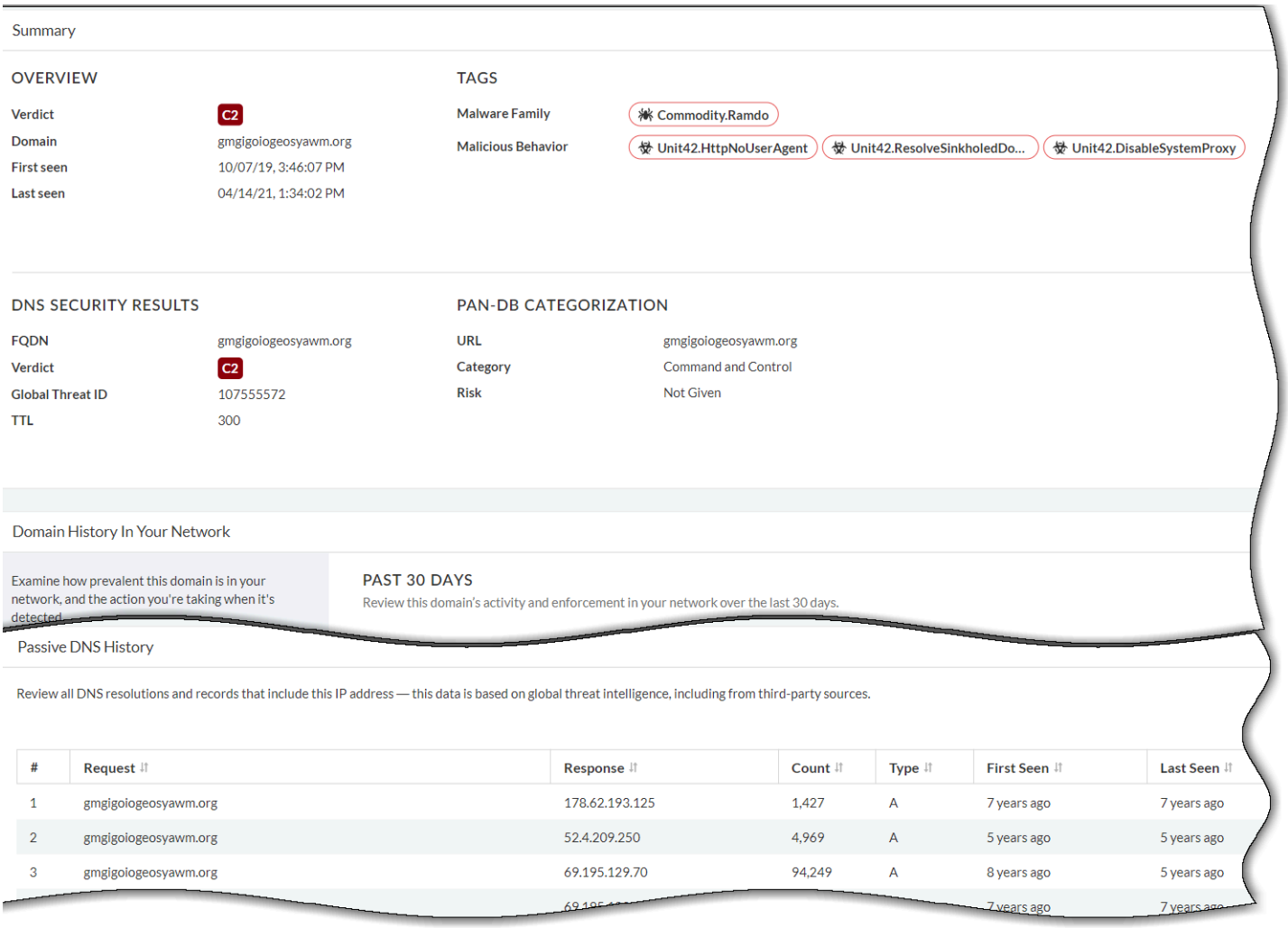
- 过去 30 天内在您的网络中检测到 IP 地址的总次数。
- 对 IP 地址采取的操作（允许或阻止）的图形表示。
- 根据 Palo Alto Networks 威胁情报和第三方来源的包含 IP 地址的 DNS 请求列表。



域

查看与您的网络中的域相关的活动的摘要。搜索结果包括：

- 根据 WildFire 样本分析对网络中的域进行分类。
- 过去 30 天内与该域相关的活动总数。
- 以图形格式对每项活动实施强制措施。
- 来自 WildFire 分析的信息，支持用于为域分配判定的数据。
- 从包含此域实例的所有 WildFire 提交中收集的 DNS 活动。



Summary

OVERVIEW

Verdict	C2
Domain	gmgigoiogeosyawm.org
First seen	10/07/19, 3:46:07 PM
Last seen	04/14/21, 1:34:02 PM

TAGS

Malware Family	Commodity.Ramdo
Malicious Behavior	Unit42.HttpNoUserAgent, Unit42.ResolveSinkholedDo..., Unit42.DisableSystemProxy

DNS SECURITY RESULTS

FQDN	gmgigoiogeosyawm.org
Verdict	C2
Global Threat ID	107555572
TTL	300

PAN-DB CATEGORIZATION

URL	gmgigoiogeosyawm.org
Category	Command and Control
Risk	Not Given

Domain History In Your Network

Examine how prevalent this domain is in your network, and the action you're taking when it's detected.

PAST 30 DAYS

Review this domain's activity and enforcement in your network over the last 30 days.

Passive DNS History

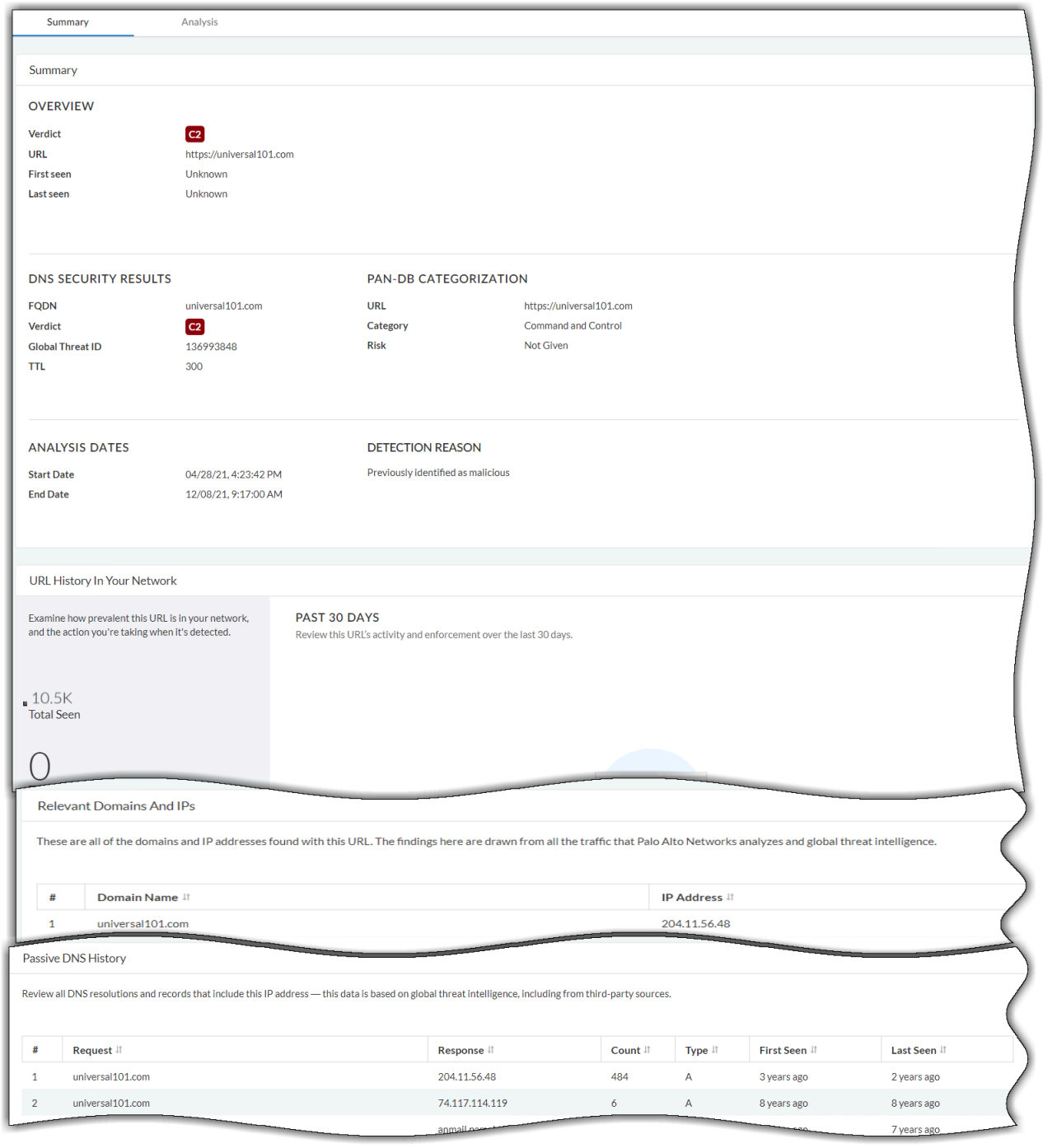
Review all DNS resolutions and records that include this IP address — this data is based on global threat intelligence, including from third-party sources.

#	Request	Response	Count	Type	First Seen	Last Seen
1	gmgigoiogeosyawm.org	178.62.193.125	1,427	A	7 years ago	7 years ago
2	gmgigoiogeosyawm.org	52.4.209.250	4,969	A	5 years ago	5 years ago
3	gmgigoiogeosyawm.org	69.195.129.70	94,249	A	8 years ago	5 years ago
					7 years ago	7 years ago

URL

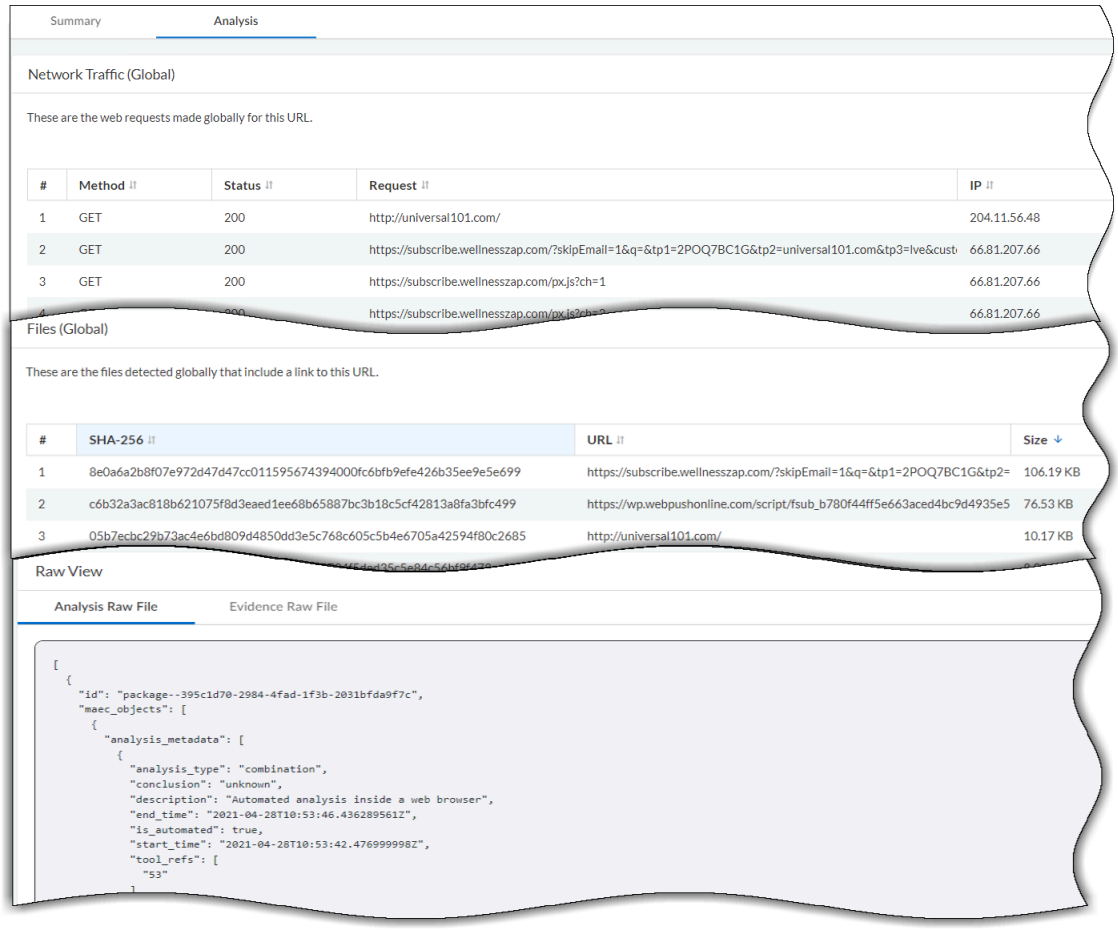
了解 Palo Alto Networks 分析的所有流量中的 URL 活动。搜索结果包括：

摘要 - 查看网络中 URL 活动的摘要。数据包括：URL 和 PAN-DB 分类的 DNS 安全性发现。



屏幕截图 - 当您在 URL 工件上搜索时显示网站的快照。

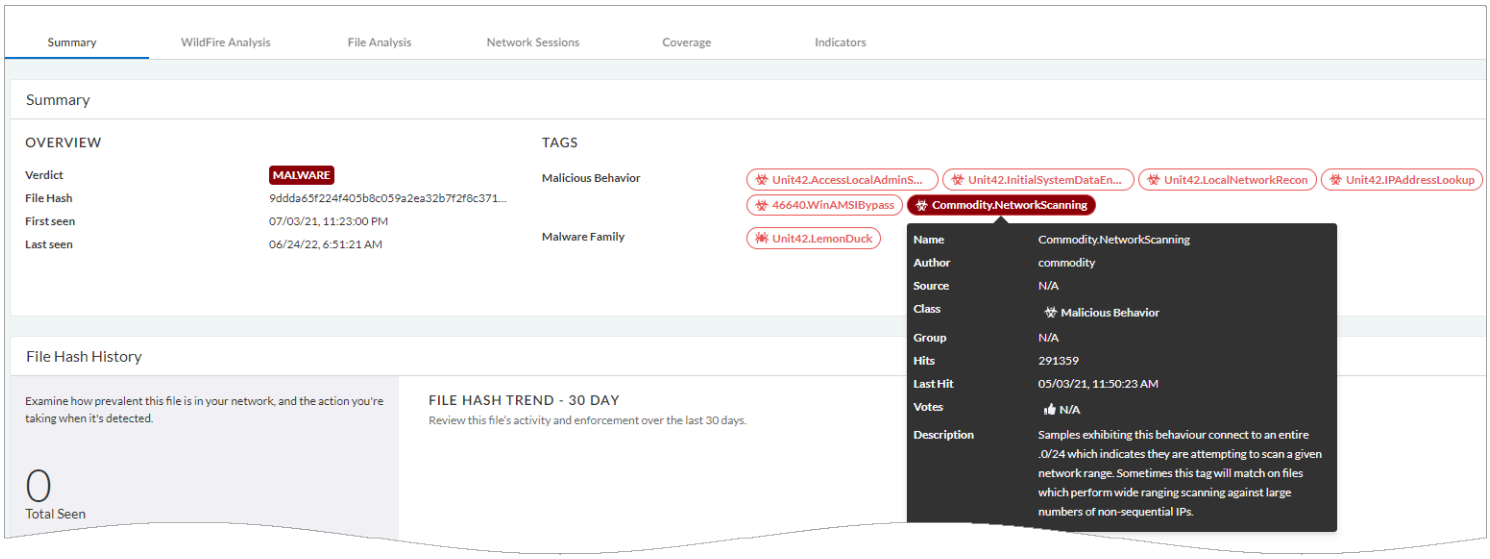
分析 - 查看文件分析数据，其中包括对此 URL 发出的全局请求以及使用此 URL 检测到的文件。您可以使用文件哈希值或文件视图来了解更多信息。



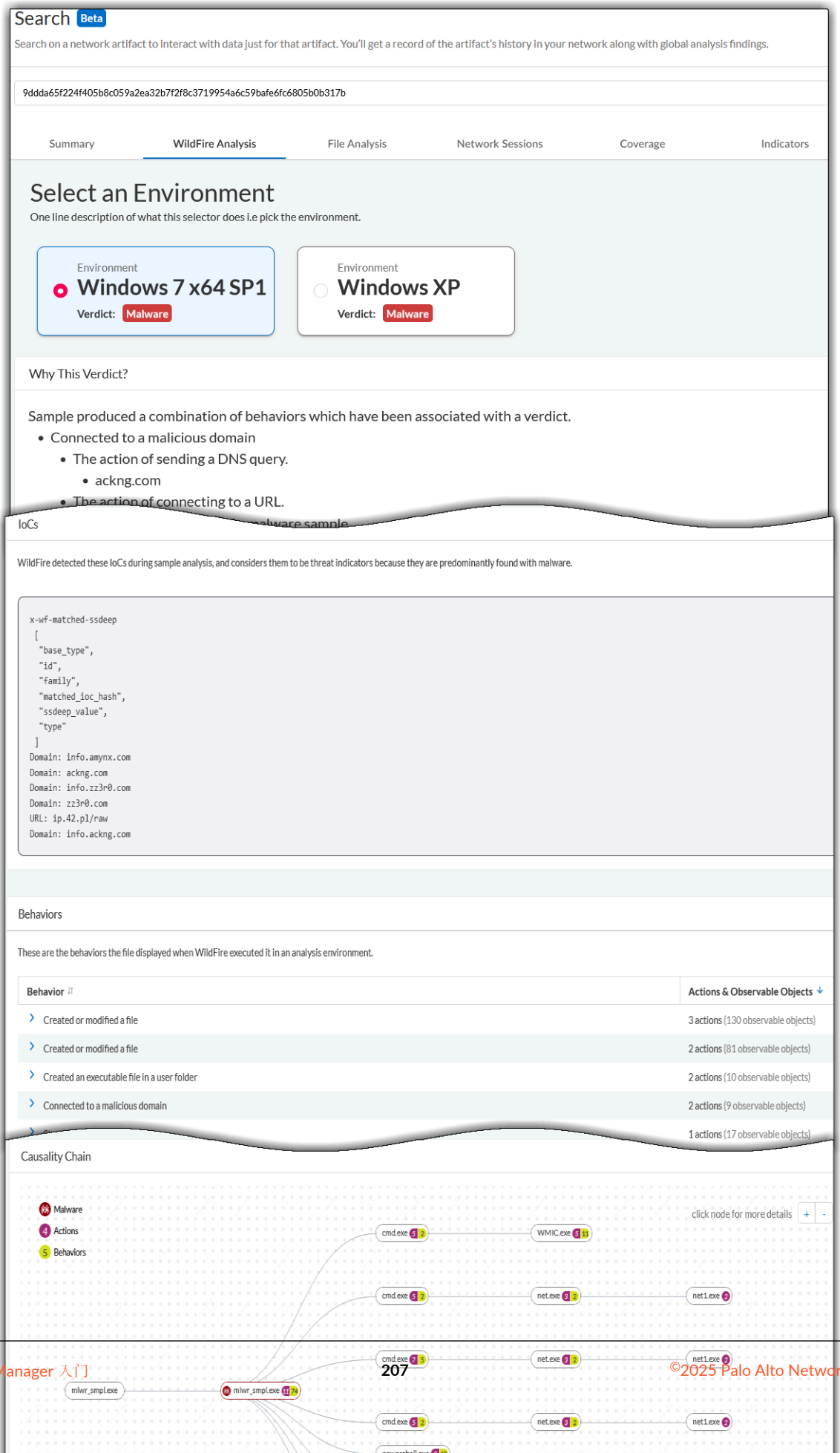
文件哈希

文件哈希搜索总结了文件的活动、文件属性的分析以及 WildFire 样本分析的详细信息。您可以深入研究搜索结果以查看以下数据：

摘要 - 查看文件哈希判定结果以及文件在网络中的活动历史记录。单击标签名称可以查看该标签的详细信息。标签可以帮助您了解文件是否属于任何威胁家族、活动或行为者的一部分。



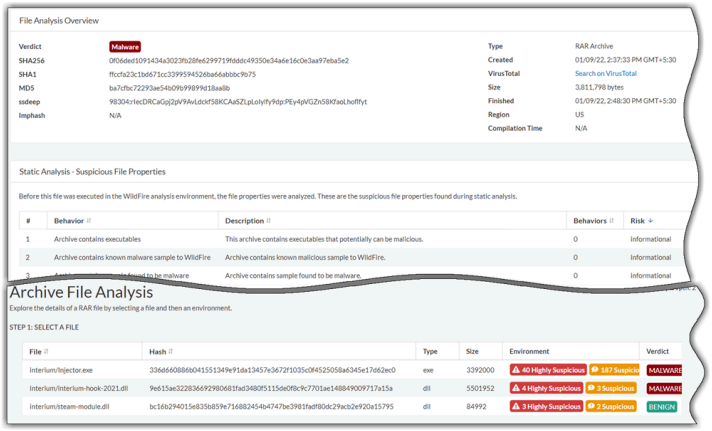
WildFire 分析 - 评估样本（文件）在 WildFire 分析期间的表现。您可以查看样本判定信息、样本分析过程中检测到的威胁指标以及在分析环境中处理样本时的行为。您还可以查看 WildFire 样本分析期间捕获的各个过程里程碑的屏幕截图。



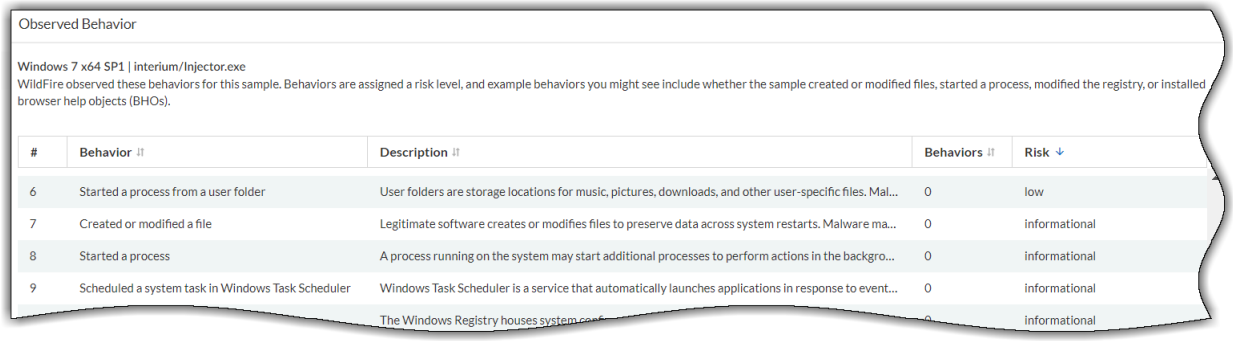
文件分析 - 比较在 WildFire 分析环境中执行样本（文件）前后的分析。

概述 - 在此处查看样本的判定。如果判定结果有误，可以请求变更判定。Palo Alto Networks 威胁团队将对样本进行进一步调查，如果发现不正确，则会更新结论。

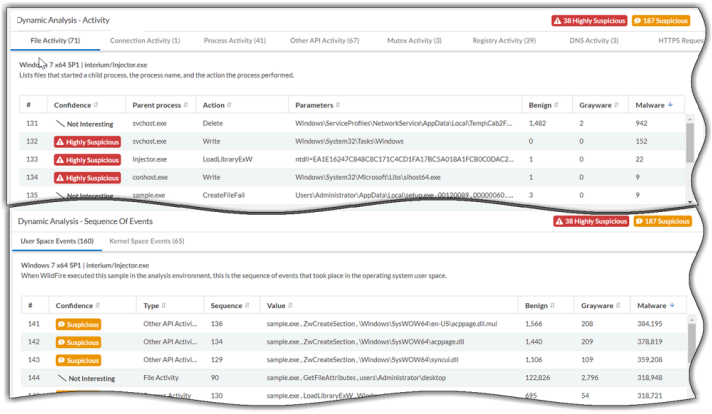
静态分析 - 静态分析在 WildFire 分析环境中执行文件之前查看特定文件的内容。搜索还显示静态分析期间发现的可疑文件属性。搜索结果根据文件类型而不同。此处的屏幕截图显示了档案文件的静态分析。



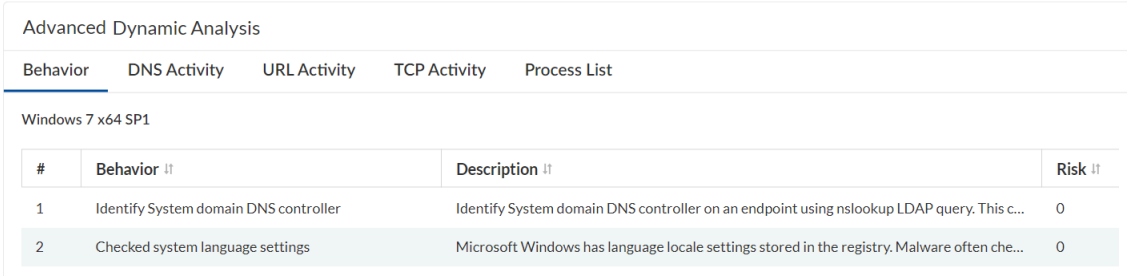
观察到的行为 - 查看特定环境中样本的 WildFire 行为分析。



动态分析 - 详细检查文件，提取受损网络的附加信息和指标。您可以检查所涉及的过程活动以及执行文件时系统中发生的事件序列。

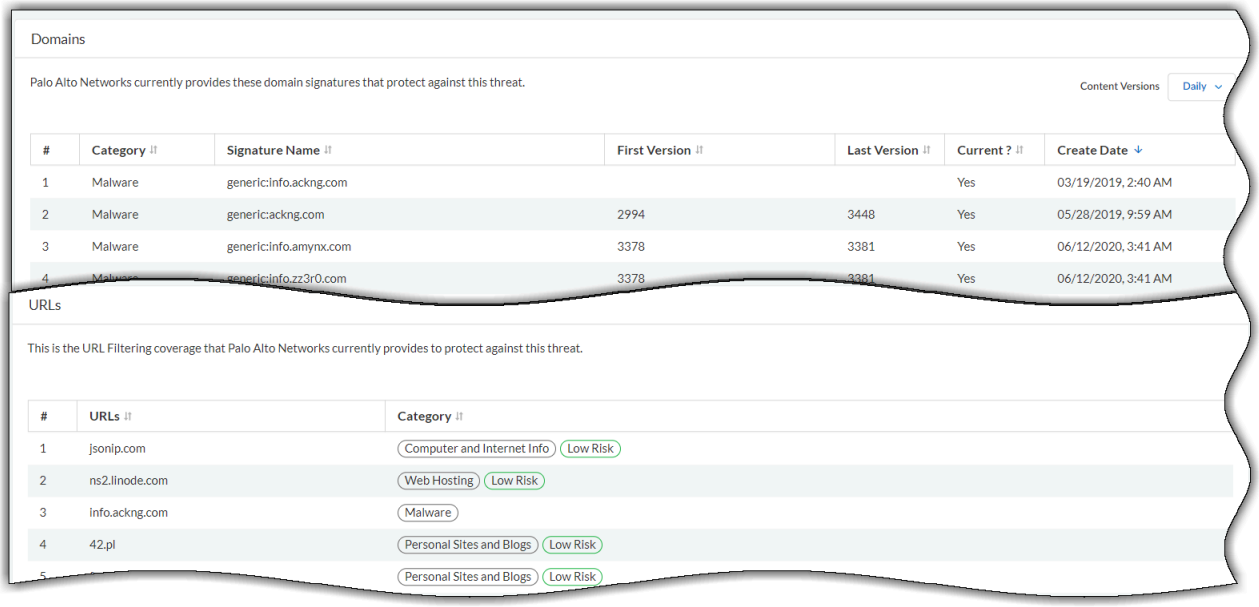


高级动态分析 - 查看通过 Advanced WildFire 技术（智能运行时内存分析、虚拟机管理程序动态分析、依赖关系模拟等）分析的样本的分析结果，这是一种基于云的引擎，可检测和防止高度规避的恶意软件威胁。您可以查看观察到的行为并使用此信息进行执行后分析。

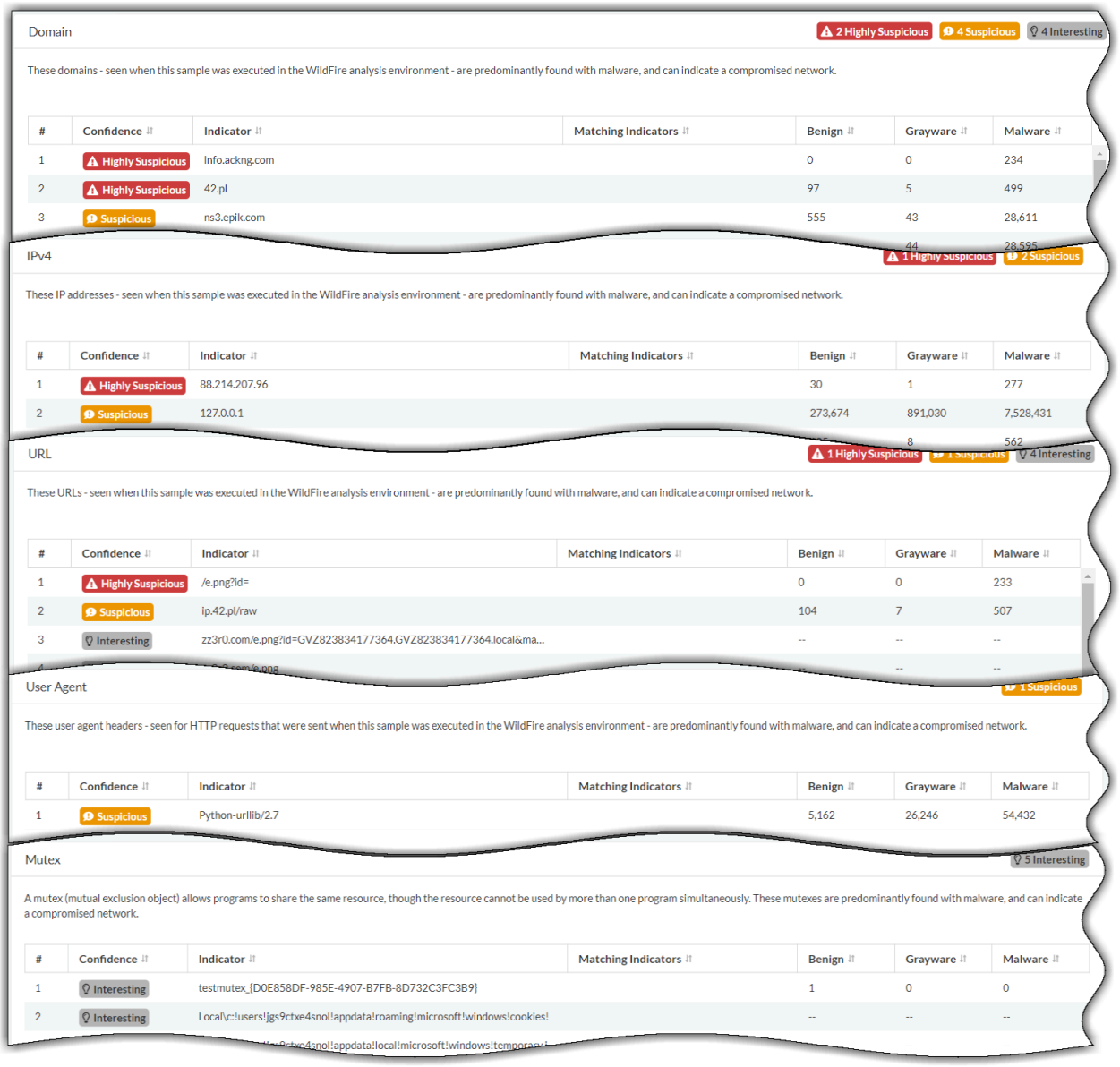


网络会话 - 了解示例的网络会话。使用这些数据来了解有关威胁的背景的更多信息，了解受影响的主机和客户端，以及用于传播恶意软件的应用程序。

覆盖范围 - 检查样本的签名覆盖范围以评估针对威胁的保护级别。您可以查看标记到下载样本的域的签名以及样本访问的 URL。



指标 - 查看组成网络的指标工件。指标根据工件类型进行分类：域、IP 地址、URL、用户代理标头和互斥对象。高风险文物被标记为可疑或高度可疑。



Domain

2 Highly Suspicious | 4 Suspicious | 4 Interesting

These domains - seen when this sample was executed in the WildFire analysis environment - are predominantly found with malware, and can indicate a compromised network.

#	Confidence	Indicator	Matching Indicators	Benign	Grayware	Malware
1	Highly Suspicious	info.ackng.com		0	0	234
2	Highly Suspicious	42.pl		97	5	499
3	Suspicious	ns3.epik.com		555	43	28,611
					44	28,595

IPv4

1 Highly Suspicious | 2 Suspicious

These IP addresses - seen when this sample was executed in the WildFire analysis environment - are predominantly found with malware, and can indicate a compromised network.

#	Confidence	Indicator	Matching Indicators	Benign	Grayware	Malware
1	Highly Suspicious	88.214.207.96		30	1	277
2	Suspicious	127.0.0.1		273,674	891,030	7,528,431
					8	562

URL

1 Highly Suspicious | 4 Interesting

These URLs - seen when this sample was executed in the WildFire analysis environment - are predominantly found with malware, and can indicate a compromised network.

#	Confidence	Indicator	Matching Indicators	Benign	Grayware	Malware
1	Highly Suspicious	/e.png?id=		0	0	233
2	Suspicious	ip.42.pl/raw		104	7	507
3	Interesting	zz3r0.com/e.png?id=GVZ823834177364.GVZ823834177364.local&ma...		--	--	--
					--	--

User Agent

1 Suspicious

These user agent headers - seen for HTTP requests that were sent when this sample was executed in the WildFire analysis environment - are predominantly found with malware, and can indicate a compromised network.

#	Confidence	Indicator	Matching Indicators	Benign	Grayware	Malware
1	Suspicious	Python-urllib/2.7		5,162	26,246	54,432

Mutex

5 Interesting

A mutex (mutual exclusion object) allows programs to share the same resource, though the resource cannot be used by more than one program simultaneously. These mutexes are predominantly found with malware, and can indicate a compromised network.

#	Confidence	Indicator	Matching Indicators	Benign	Grayware	Malware
1	Interesting	testmutex_{D0E858DF-985E-4907-B7FB-8D732C3FC3B9}		1	0	0
2	Interesting	Local\c:!users!jgs9ctxe4snol!appdata!roaming!microsoft!windows!cookies!		--	--	--
					--	--

监视：分支站点

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW，包括由 软件 NGFW 积分提供资助的项目 • Prisma SD-WAN	这些许可证中的每一个都包括 Strata Cloud Manager 访问权限： ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro ❑ Prisma SD-WAN 提高可见性所需的其他许可证和先决条件是： ❑ ADEM 可观测性 ❑ 远程网络自主 DEM ❑ 人工智能驱动的 ADEM ❑ WAN Clarity 报告 ❑ 有权查看指示板的角色 → 您可用的特性和功能Strata Cloud Manager取决于您使用的许可证。

分支站点：**Prisma Access**

选择 **Monitor**（监控） > **Branch Sites**（分支站点） > **Prisma Access**，以便查看远程网络的运行状况和连接情况，以及部署在不同 Prisma Access 位置的所有远程网络的使用情况。它向您显示实时连接状态和带宽消耗详情以及其他部署详细信息。移动用户、分支机构和零售店连接到远程网络。.您还可以查看远程网络和移动用户中配置的隧道的运行状况。

除了使用 Prisma Access 许可证显示的小部件外，如果您拥有 ADEM Observability 或 AI-Powered ADEM 许可证，此指示板还会显示站点体验分数和 Prisma SD-WAN 分支站点详细信息页面。

分支站点：**Prisma SD-WAN**

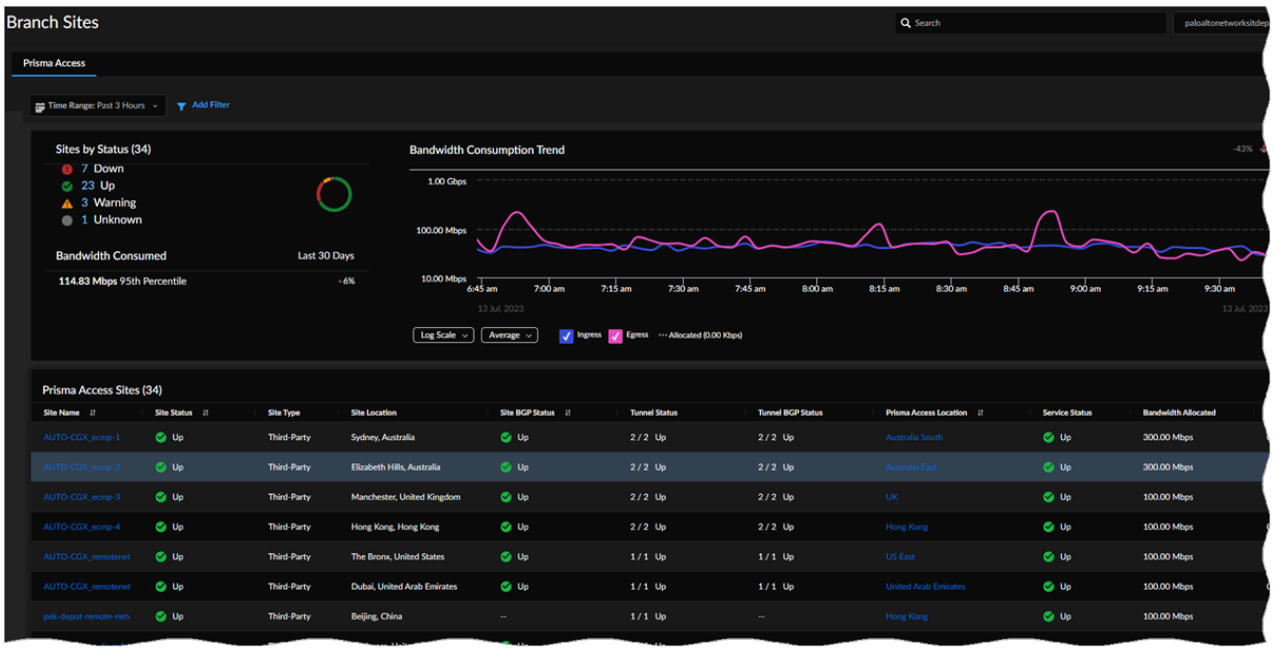
选择 **Monitor**（监控） > **Branch Sites**（分支站点） > **Prisma SD-WAN**，以便在 Prisma SD-WAN 中设置分支站点。分支站点包括您在 Prisma SD-WAN 中拥有的分支机构。您可以在 ION 设备到达指定站点之前或之后分支站点。Prisma SD-WAN 中的分支站点提供以下视图：

- 分支站点的地图视图提供了分支站点设备与控制器的连接状态以及站点的警报状态。
- 列表视图显示在选定 **Time Range**（时间范围）内有多少个站点处于活动状态，以及分支站点的整体运行状况指标。
- 活动视图显示关键应用程序分析、最新的站点运行状况评分以及站点运行状况随时间的变化分布。

- Prisma Access
- Prisma SD-WAN

分支站点 (Prisma Access)

选择 **Branch Sites**（分支站点） > **Prisma Access**，以便查看远程网络的运行状况和连接性，以及您部署在不同 Prisma Access 位置的所有远程网络的使用情况。



它向您显示实时连接状态和带宽消耗详情以及其他部署详细信息。移动用户、分支机构和零售店连接到远程网络。.您还可以查看远程网络和移动用户中配置的隧道的运行状况。有关这些小部件的详细说明，请参阅查看和监控分支站点。

您可以：

- 按状态查看远程网络站点。
- 查看远程网络带宽消耗的趋势。
- 查看您的 Prisma Access 站点，然后选择任何站点以查看更多详细信息。
- 打开 **IPSec** 终止节点利用率详细信息，查看站点中每个 SPN 的带宽消耗详细信息。
- 查看站点的隧道数据和隧道趋势。
- 查看站点状态、运行状况、连接和消耗信息。

分支站点 (Prisma SD-WAN)

您可以在 ION 设备到达指定站点之前或之后分支站点。Prisma SD-WAN 中的分支站点提供以下视图：

- 分支站点的地图视图提供了分支站点设备与控制器的连接状态以及站点的警报状态。选择分支站点时将显示以下信息：
  - 站点摘要：用于分析和故障排除。
  - 配置：用于站点和设备配置。
  - 覆盖连接：用于查看所有 VPN 覆盖连接的状态。
- 列表视图显示在所选 **Time Range**（时间范围）内有多少个站点处于活动状态以及分支站点的整体运行状况指标。较差站点的平均得分是所有被认定为较差站点的较差样本的平均值。时间序列图根据所选的持续时间计算和刷新。例如，支持的持续时间分别为一小时、三小时、24 小时、七天、30 天和 90 天，间隔分别为一分钟、五分钟、一小时和一天。
  - **Site Connectivity Health Distribution**（站点连接运行状况分布）：根据最新的站点连接运行状况分布，针对给定租户的良好、一般和较差站点的分布图。
  - **Site Connectivity Health Distribution Over Time**（站点连接运行状况时间分布）：运行设备软件 5.6.1 或更高版本的运行状况分数的时间序列图。
  - **Site Application Experience Score**（站点应用体验评分）：现场应用体验评分。
  - **Prisma SD-WAN Branch Sites**（**Prisma SD-WAN** 分支站点）：查看分支站点的站点运行状况、站点连接运行状况、电路运行状况、安全结构运行状况以及接近的容量阈值。您可以根据站点预测、警报状态和 ADEM 状态进一步深入了解和筛选分支站点。
- 活动视图显示关键应用程序分析、最新的站点运行状况评分以及站点运行状况随时间的变化分布。这些包括：
  - 站点运行状况分布：根据最新的站点运行状况评分，显示给定租户的良好、一般和较差站点图表的分布。
  - 站点运行状况分布随时间的变化：根据分支站点的运行状况评分，显示给定租户的站点运行状况分布随时间的变化时间序列图。
  - 带宽利用率：显示站点和 WAN 路径上每个应用程序的带宽利用率，以及网络中消耗带宽最多的前十大应用程序的数据。
  - 事务统计信息：显示 TCP 流的事务统计信息，包括特定应用程序或所有应用程序、特定路径或所有路径以及所有运行状况事件的启动/事务成功和失败。
  - 新流量：显示某个应用程序、一组特定的应用程序或给定时间段内所有应用程序的新 TCP 和 UDP 流量。
  - 并发流：帮助您了解网络上应用程序的活动连接数。

监视：数据中心

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW，包括由 软件 NGFW 积分提供资助的项目 • Prisma SD-WAN	这些许可证中的每一个都包括 Strata Cloud Manager 访问权限： ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro ❑ Prisma SD-WAN 提高可见性所需的其他许可证和先决条件是： ❑ ADEM 可观测性 ❑ 远程网络自主 DEM ❑ 人工智能驱动的 ADEM ❑ WAN Clarity 报告 ❑ 有权查看指示板的角色 → 您可用的特性和功能Strata Cloud Manager取决于您使用的许可证。

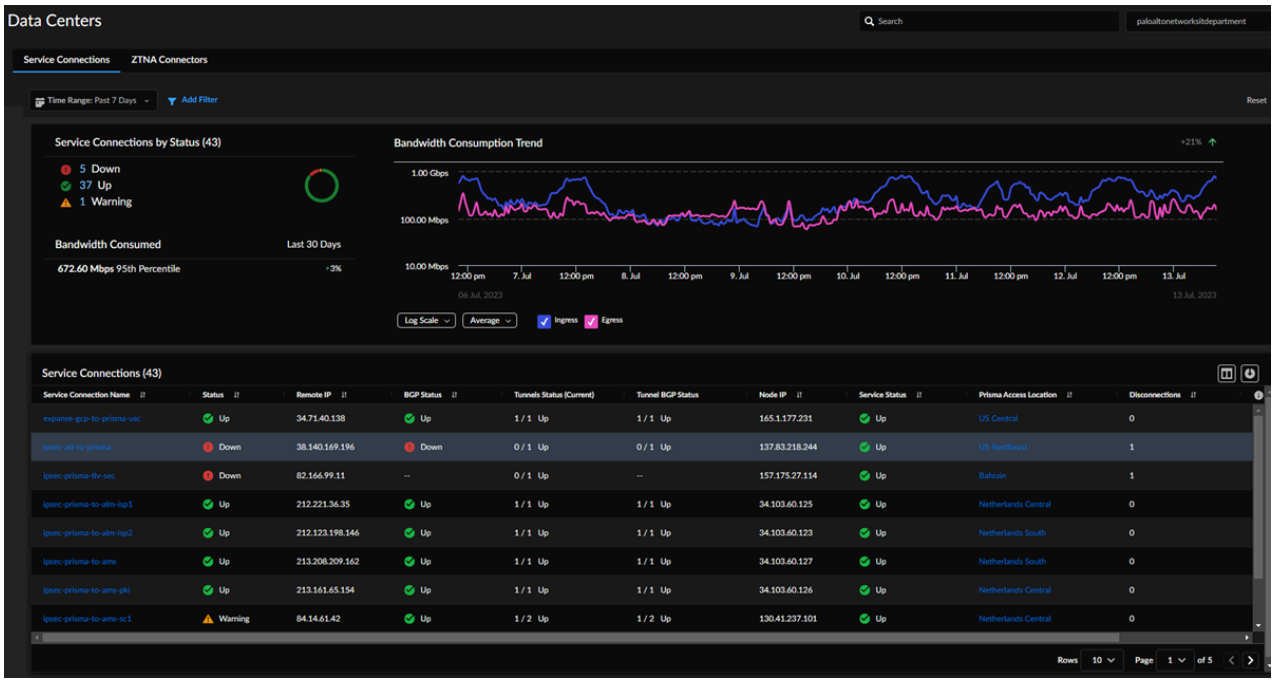
监控服务连接、ZTNA 连接器和站点连接在 Prisma SD-WAN 数据中心的运行情况。选择 **Monitor**（监控） > **Prisma Access** > **Data Centers**（数据中心） > **Service Connections**（服务连接）或 **ZTNA Connectors**（**ZTNA** 连接器）选项卡，以便在 Prisma Access 中查看服务连接和 ZTNA 连接器的运行状况和状态。

对于每个 Prisma SD-WAN 数据中心，选择 **Monitor**（监控） > **Data Centers**（数据中心） > **Prisma SD-WAN**，以查看站点连接信息和 VPN 重叠连接的状态。

- 服务连接
- ZTNA 连接器
- Prisma SD-WAN

服务连接

要开始，请选择 **Monitor**（监控） > **Data Centers**（数据中心） > **Service Connections**（服务连接）。



查看聚合的服务连接数据以及有关单个服务连接的信息。服务连接可实现移动用户和远程网络。除了提供对公司资源的访问，服务连接还允许您的移动用户到达分支机构。有关这些小部件的详细说明，请参阅《*Prisma Access* 管理指南》中的查看和监控数据中心。

- 选择一个时间范围，按状态及其带宽消耗趋势查看服务连接。
- 查看所有服务连接的运行状况。
- 查看您所有服务连接的带宽消耗趋势。
- 查看有关服务连接的数据，例如状态、远程 IP 地址、BGP 状态、当前通道状态和其他数据。选择任何服务连接以查看其详细信息。

ZTNA 连接器

要开始，请选择 **Monitor**（监控） > **Data Centers**（数据中心） > **ZTNA Connectors**（**ZTNA** 连接器）。

零信任网络接入 (ZTNA) 连接器简化了所有应用程序的私有应用程序访问。您环境中的 ZTNA 连接器虚拟机会自动在您的私有应用程序和 Prisma Access 之间构建隧道。查看所有已配置的 ZTNA 连接器的摘要，包括与连接器关联的**Application Targets**（应用程序目标）、其平均带宽和中位带宽以及 **Status**（状态）（启动、部分启动或关闭）。有关这些小部件的详细说明，请参阅《*Prisma Access* 管理指南》中的查看和监控数据中心。

您可以：

- 查看 ZTNA 连接器组的运行状况和状态。
- 查看各个 ZTNA 连接器的运行状况和状态。

数据中心 (Prisma SD-WAN)

Prisma SD-WAN 站点包括您希望在广域网中拥有的数据中心 。您可以在数据中心托管企业应用程序和服务。作为创建数据中心的一部分，您可以选择默认域和策略集，设置 WAN 网络、电路类别、电路标签和电路规格。Prisma SD-WAN 数据中心屏幕显示数据中心列表，其中包括数据中心名称、ION 设备以及站点的任何打开的警报。

对于数据中心，您会看到：

- **Configuration**（配置）选项卡显示站点连接信息、部署模式、WAN 多播对等组配置文件、Internet 和专用 WAN 电路以及 IP 前缀。您还可以配置用户代理并查看数据中心的集群配置的详细信息。
- **Overlay Connections**（覆盖连接）选项卡显示所有 VPN 覆盖连接的状态。每个站点的连接性是根据其 VPN 覆盖连接的状态计算的。

监视：网络服务

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW，包括由 软件 NGFW 积分提供资助的项目 • Prisma SD-WAN	这些许可证中的每一个都包括 Strata Cloud Manager 访问权限： ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro ❑ Prisma SD-WAN 提高可见性所需的其他许可证和先决条件是： ❑ ADEM 可观测性 ❑ 远程网络自主 DEM ❑ 人工智能驱动的 ADEM ❑ WAN Clarity 报告 ❑ 有权查看指示板的角色 → 您可用的特性和功能Strata Cloud Manager取决于您使用的许可证。

从 **Monitor**（监控） > **Network Services**（网络服务）页面中，可以查看影响用户访问应用程序的体验的常见网络服务的性能。选择 **GlobalProtect Authentication**（**GlobalProtect** 身份验证）选项卡以查看 GlobalProtect 在不同位置的身份验证成功或失败计数。选择 **Network Services:DNS**（网络服务：**DNS**），以查看跨租户收到的有关 Prisma Access DNS 代理的 DNS 代理请求和响应。

- GlobalProtect 身份验证
- DNS

GlobalProtect 身份验证

要开始，请选择 **Monitor**（监控） > **Network Services**（网络服务） > **GlobalProtect Authentication**（**GlobalProtect** 身份验证）。

您可以在 Insights 中查看影响访问应用程序的用户体验的常见网络服务的性能。网络服务包括报告 GlobalProtect 身份验证成功和失败的次数，作为衡量移动用户能够连接到 Prisma Access 的指标。您可以查看：

- 有关身份验证成功的详细信息对不同位置的 GlobalProtect 至关重要。
- GlobalProtect 在不同位置的身份验证失败计数。
- GlobalProtect 在不同位置的身份验证超时失败。

有关这些小部件的详细说明，请参阅查看和监视网络服务。

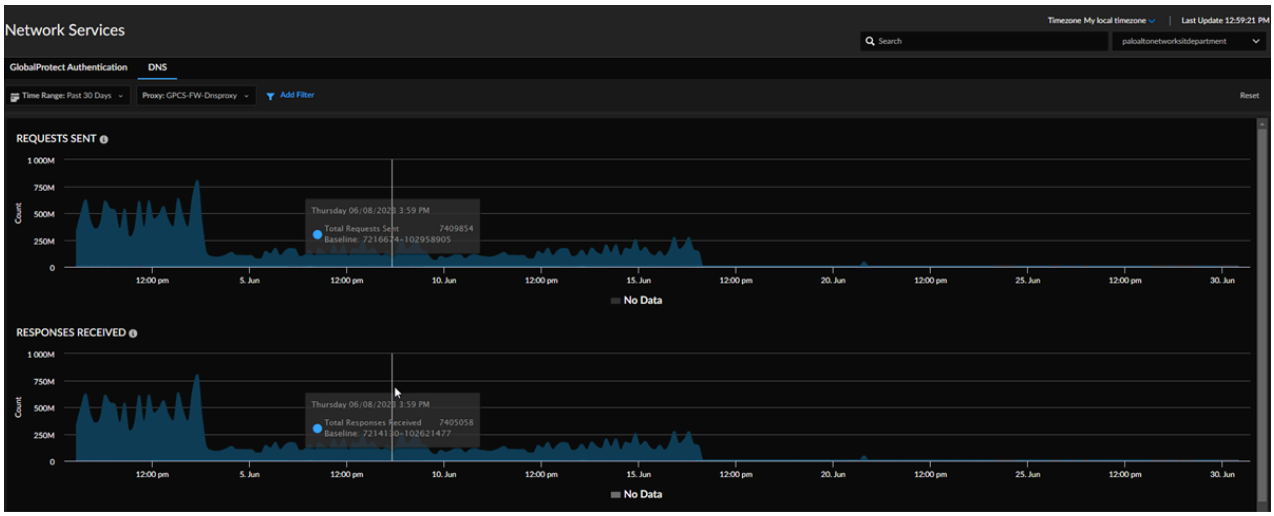
DNS

要开始，请选择 **Monitor**（监控） > **Network Services**（网络服务） > **DNS**。

网络服务：**DNS**（网络服务：**DNS**）显示 DNS 代理请求和响应。您可以使用以下筛选器：

- 时间范围
- **DNS** 代理名称

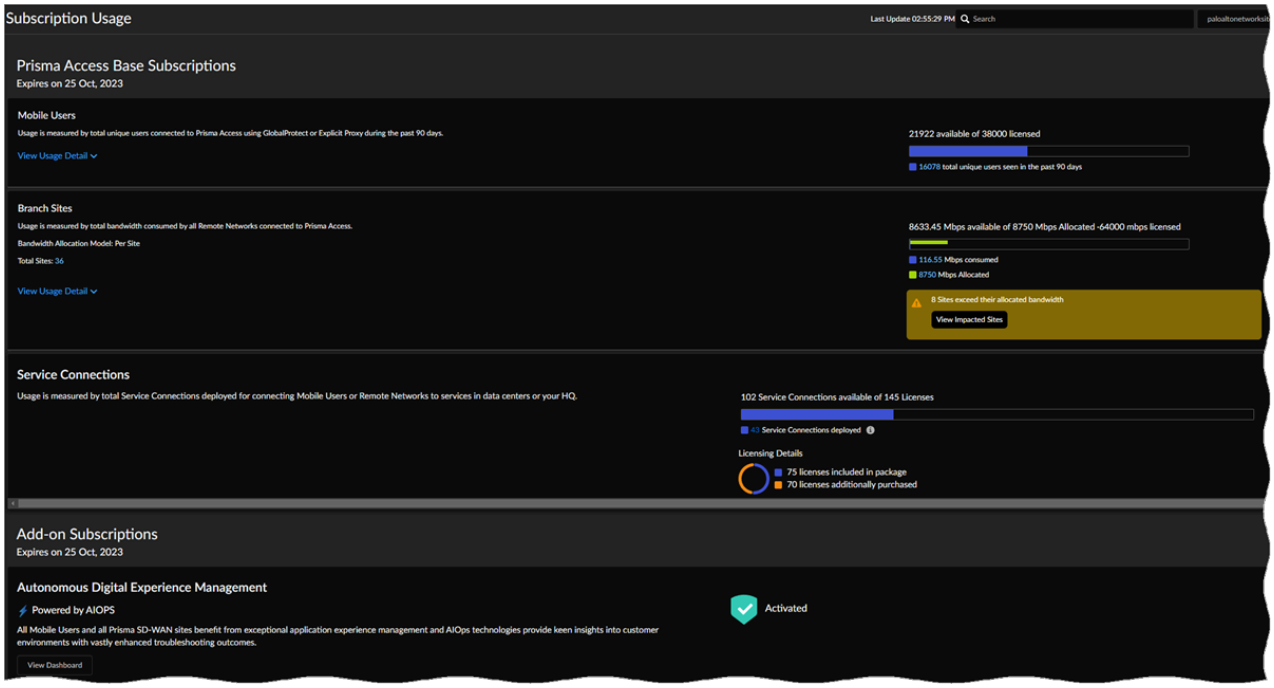
DNS 代理筛选器值与过去 30 天相关，并在加载时自动选择（也就是说，如果没有显式代理数据，则没有显式代理筛选器）。有关更多详细信息，请参阅查看和监控网络服务。



监视：订阅使用情况

在何处可以使用？	需要提供什么？
• Prisma Access （利用 *Strata Cloud Manager* 或 *Panorama* 配置管理）	❑ Prisma Access 许可证 ❑ AI-Powered ADEM 以解锁某些功能。

选择 **Monitor**（监控） > **Subscription Usage**（订阅使用情况），以查看有关 **Prisma Access Base Subscriptions**（**Prisma Access** 基本订阅）使用情况的详细信息，包括连接的唯一用户总数、远程网络用户消耗的带宽、部署的服务连接总数以及有关任何附加订阅的详细信息。



- **Mobile Users**（移动用户）：查看到目前为止您已使用了多少唯一 **Mobile Users**（移动用户）许可证。该小部件显示过去 90 天内连接到 Prisma Access 的唯一移动用户使用的许可证总数，因为许可证基于过去 90 天的 Prisma Access 登录数据。在过去 90 天内至少登录过 Prisma Access 一次的用户将贡献一个移动用户许可证的使用。
- **Branch Sites**（分支站点）：查看连接到 Prisma Access 的所有远程网络消耗的总带宽使用量。查看您分配了多少带宽以及您使用了多少带宽（以 Mbps 为单位）。您可以通过连接到 Prisma Access 的所有远程网络所消耗的总带宽来查看使用情况。
- **Subscriptions Usage**（订阅使用情况）：查看到目前为止您已使用了多少 **Service Connections**（服务连接）许可证。

请参阅此页面上的 **Add-on Subscriptions**（附加订阅）部分，以查看您已购买的其他许可证，例如移动用户和远程网络的 **Autonomous Digital Experience Management**（自主数字体验管理）许可证。您可以看到购买的许可证总数以及迄今为止未使用的许可证数量。查看 **Application Tests for**

Mobile User Monitoring（移动用户监控的应用程序测试）— 您可以为移动用户创建的剩余应用程序测试数。应用程序测试由移动用户的数量决定，每个移动用户最多允许 10 个应用程序测试。

有关详细信息，请参阅查看和监视订阅使用情况。

监视：ION 设备

在何处可以使用？	需要提供什么？
• Prisma SD-WAN	❑ Prisma SD-WAN 许可证

凭借 Prisma SD-WAN 中的 ION 设备，您能够将不同的 WAN 网络（如 MPLS、LTE 和互联网链路）组合成单个高性能混合广域网 (WAN)。

Device List（设备列表）屏幕提供 Prisma SD-WAN 设备列表的信息，包括 ION 设备的软件版本和状态，您可以在其中升级设备的软件版本或配置设备。

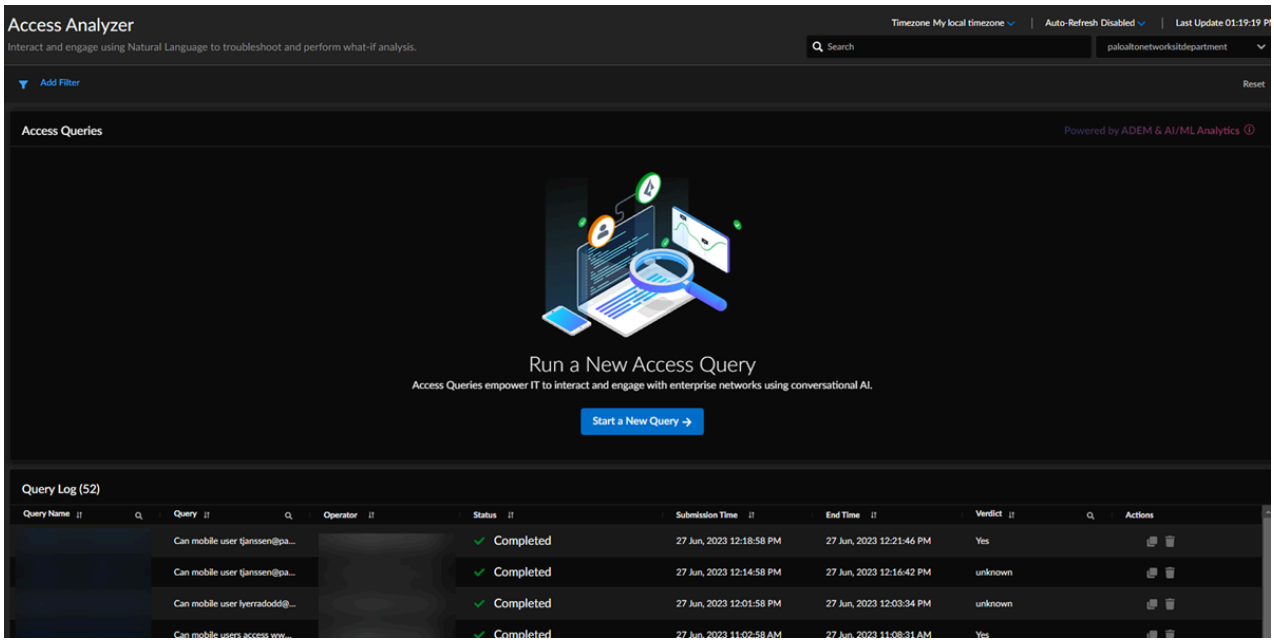
实体	说明
设备名称	显示为 ION 设备配置的名称。
设备信息	显示 ION 设备的类型和序列号。
软件	显示设备的当前软件版本。单击 **Upgrade**（升级）以更改设备软件版本。
上次活动	显示上次配置和升级 ION 设备的时间信息。
State（状态）	显示 ION 设备的当前状态。
冗余	显示 ION 设备是否为高可用性 (HA) 配置的一部分。
操作	您可以从省略号菜单中选择配置 ION 设备。

Device Activity（设备活动）屏幕显示过去 24 小时内站点的各种设备活动报告。

监视：访问分析器

在何处可以使用？	需要提供什么？
• Prisma Access （利用 *Strata Cloud Manager* 或 *Panorama* 配置管理）	❑ Prisma Access 许可证 ❑ AI-Powered ADEM 许可证

选择 **Monitor**（监控） > **Access Analyzer** 以启动新的访问分析器查询并查看现有查询的表。



Access Analyzer 可自动监控您的 SASE 环境。它提供了一个对话式 AI 工具，用于上下文故障排除和假设分析，以分析 SASE 环境中的访问和连接问题。

您可以：

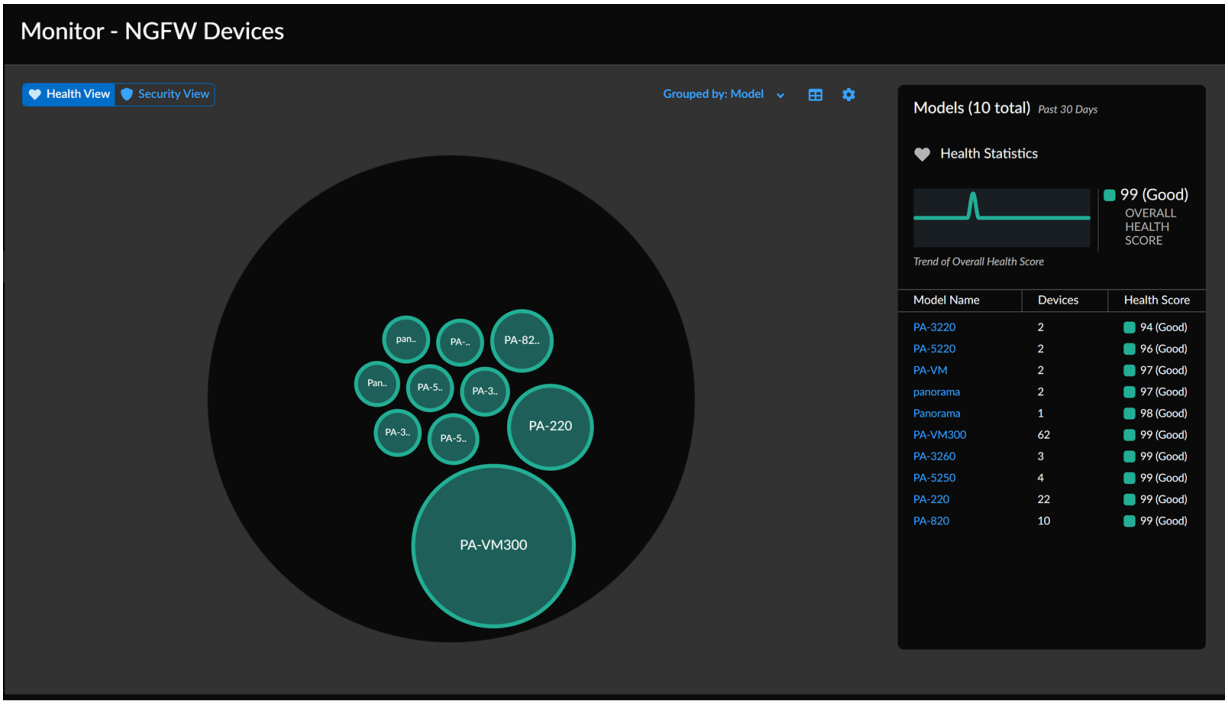
- 了解如何在 Access Analyzer 中创建自然语言查询。
- 开始新的 Access Analyzer 查询。
- 查看现有查询的列表，并从表中选择任何查询以查看更多详细信息。

监视：NGFW 设备

在何处可以使用？	需要提供什么？
• NGFW （利用 *Strata Cloud Manager* 或 *Panorama* 配置管理）	❑ AIOps for NGFW Free (use the AIOps for NGFW Free ap 或 AIOps for NGFW Premium license (use the Strata Cloud ❑ 软件 NGFW 积分 （适用于 *VM-Series* 软件 *NGFW*）

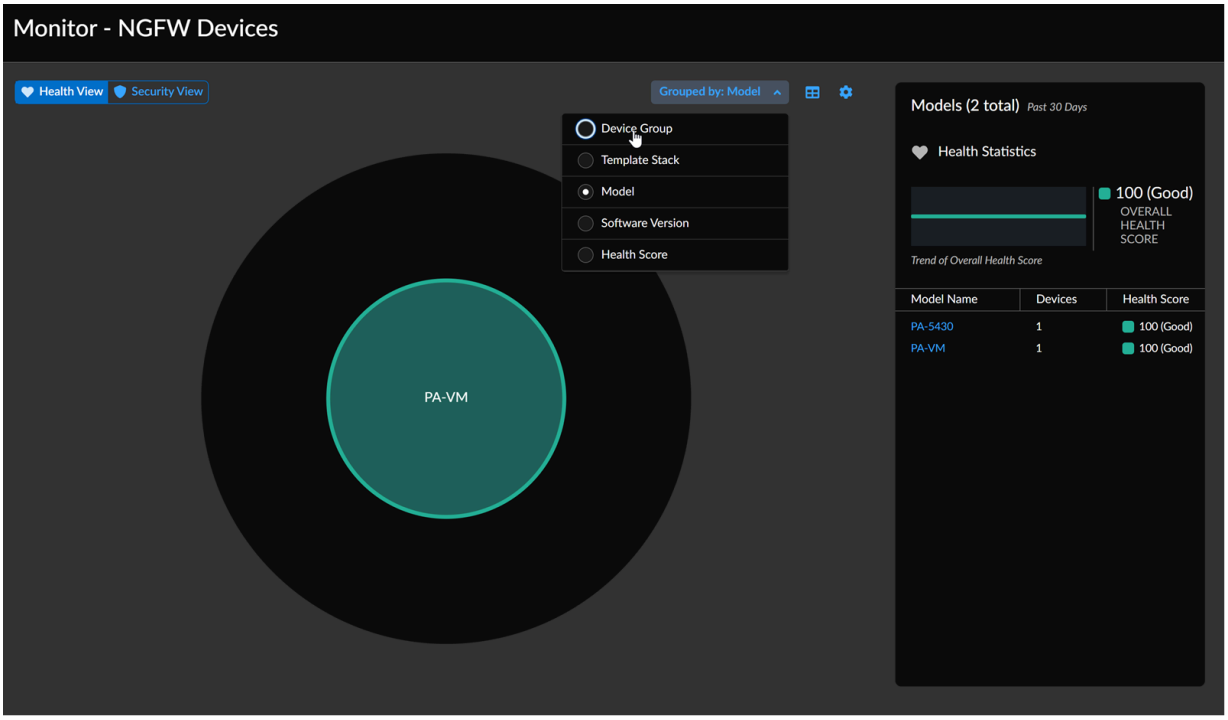
在 **Monitor**（监控） > **NGFW Devices**（**NGFW** 设备） 中，您可以获得部署中设备的彩色编码、交互式表示，以便轻松直观的管理和调查。

STEP 1 | 选择 **Monitor**（监控） > **NGFW Devices**（**NGFW** 设备）。



STEP 2 | 选择 **Health**（运行状况）或 **Security**（安全）。

STEP 3 | 选择要作为可视化 **Grouped by**（分组依据）的属性。



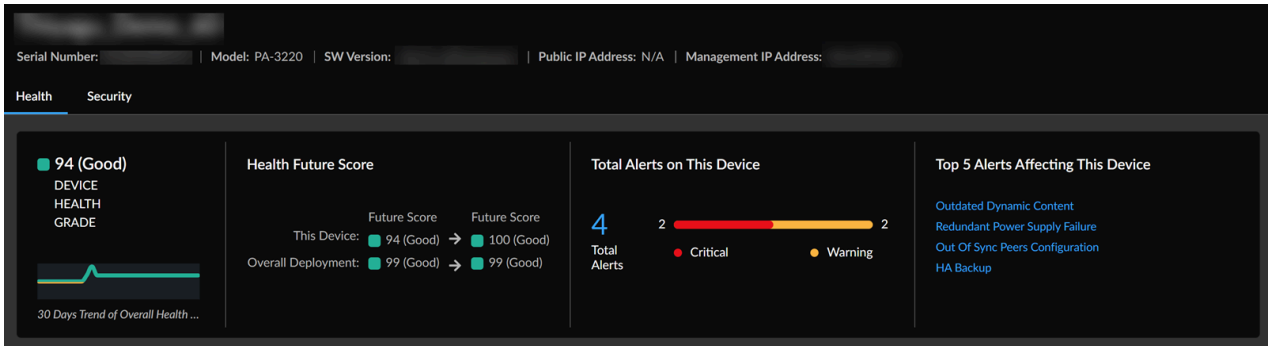
Device Group（设备组）和 ***Template Stack***（模板堆栈）分组选项仅在 *Panorama* 管理部署中可用，其中 *Panorama* 正在发送设备遥测。

STEP 4 | 选择一个组以查看其中的设备，然后选择一个设备以查看有关该设备的一般信息。

如果您想了解有关设备的更多信息，请选择该设备。

查看设备详细信息

通过从 **NGFW Devices**（**NGFW** 设备）可视化中选择设备，或者通过跟随应用中其他地方的链接，您可以查看有关防火墙或 Panorama 设备的特定详细信息，如运行状况等级、指标、连接等。



设备运行状况等级

设备的当前运行状况等级和显示其过去 30 <x>天历史的图表。可能的运行状况等级为“良好”、“一般”、“较差”和“严重”。

修复后的运行状况等级

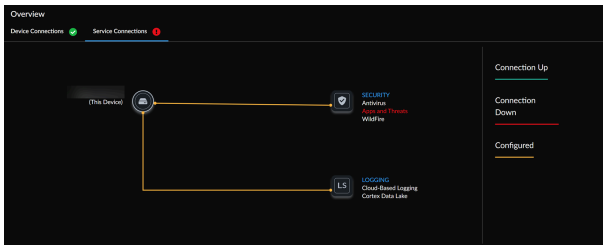
处理打开警报后设备的运行状况等级。此磁贴还显示关闭警报后整体部署的运行状况。

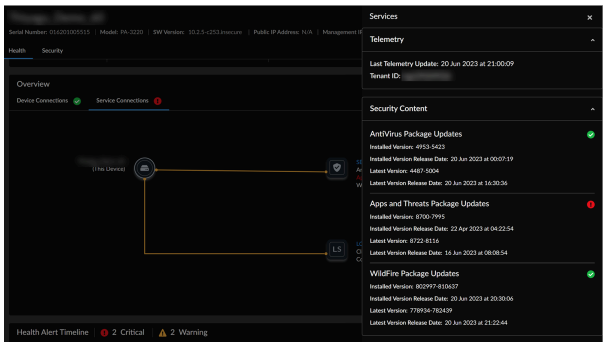
警报总数

设备上未解决的警报总数。

前 **5** 个警报

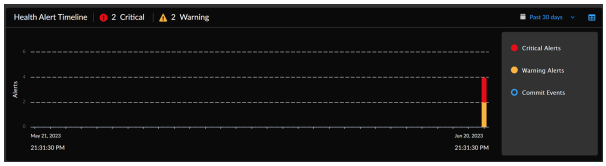
过去 30 天内此设备上最常见的五个警报。

概述 > 设备连接 连接到您当前正在查看的设备的其他设备。选择一个设备以查看其详细信息。	
概述 > 服务连接 与设备集成的所有安全和日志记录服务的概述。选择一个服务以查看其详细信息。	



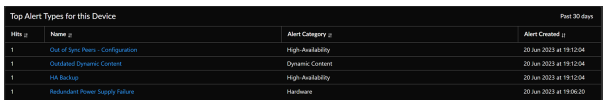
警报时间表

设备警报和提交事件的时间表。警报分为严重事件、警告事件或提交事件。切换以表格式查看警报数据。



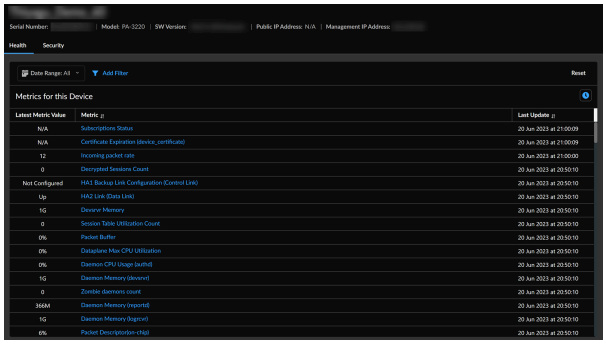
此设备的主要警报类型

过去 30 天内最常见的警报。选择要查看其警报详情的警报。



前 **10** 大应用程序使用率

防火墙上使用数据最多的十个应用程序。

此设备的指标 针对设备运行为安全检查收集的所有运行状况指标的列表，包括 HA 链路数据。 选择一个指标以查看其详细信息。	

监视：容量分析器

在何处可以使用？	需要提供什么？
• NGFW	❑ AIOps for NGFW Premium 或 Strata Cloud Manager Pro → 您可用的特性和功能Strata Cloud Manager取决于您使用的许可证。

容量分析器允许您分析和监控设备的资源容量，方法是根据设备的型号类型跟踪其指标使用情况。容量分析器具有以下优点：

- 全面了解现有指标利用率和最大限度的未利用指标容量。
- 一个热图可视化，在单个视图中展示硬件平台的指标使用情况，并帮助深入了解详细信息。
- 能够根据您的特定需求计划升级到更高容量的防火墙。

VM Series 防火墙不支持 ***Capacity Analyzer*** 功能。

以下视频展示了如何使用容量分析器功能：

容量分析器已得到增强，可支持警报，帮助您预测接近其最大容量的资源消耗并及时触发通知。容量分析器警报会提前3个月生成，以确定潜在的容量瓶颈。这有助于您在 NGFW 容量达到最大使用率之前规划配置清理或升迁，并保持系统稳定性。有关受支持的容量警报列表，请参阅高级运行状况警报。

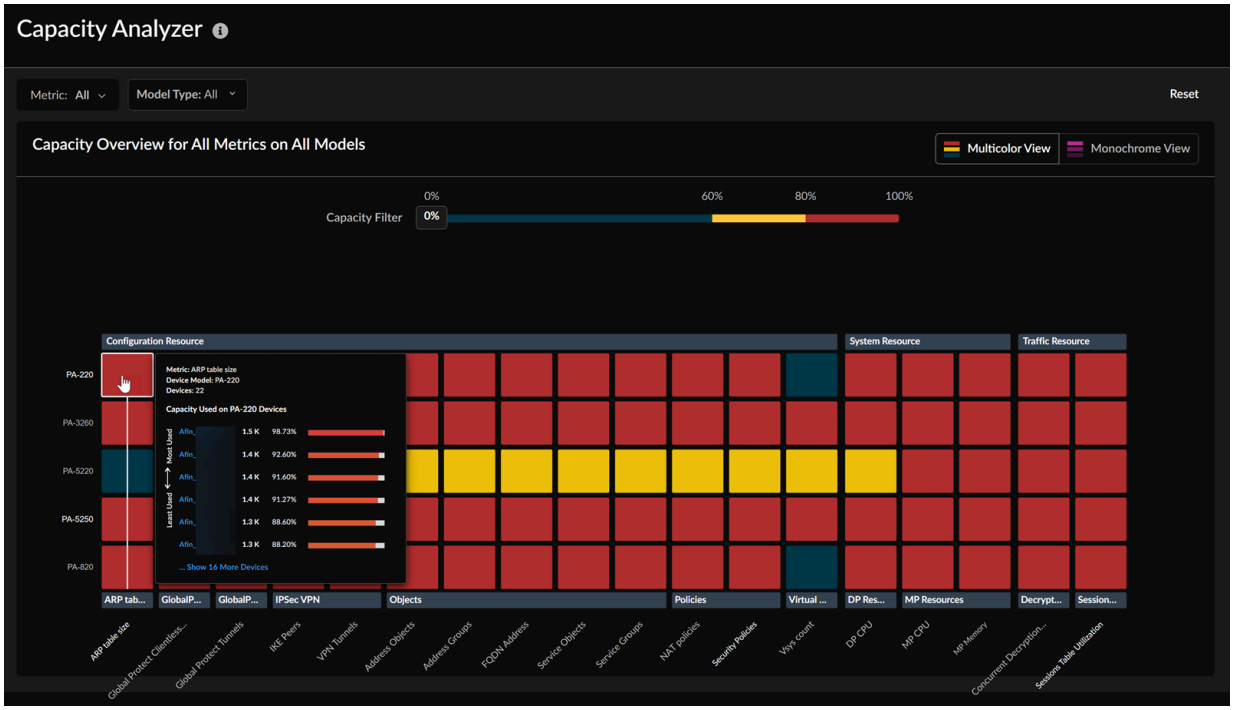
容量分析器根据以下类型对指标进行分组：

- 配置资源指标，如NAT策略和地址对象。
- 系统操作资源指标，如 CPU、内存、磁盘和日志。
- 流量资源指标，如解密使用率和会话表利用率。

热图显示每个设备的指标使用情况。较深的颜色表示较高的利用率，较浅的颜色表示较低的利用率。默认情况下，选择 **Multicolor View**（多色视图）。您也可以切换到 **Monochrome View**（单色视图）。

以下是您可以使用容量分析器热图来获取有关指标使用情况的信息的不同方法：

- 将光标悬停在设备的公制块上可查看提供以下详细信息的工具提示：
  - 指标的名称
  - 设备型号和设备列表
  - 设备容量范围



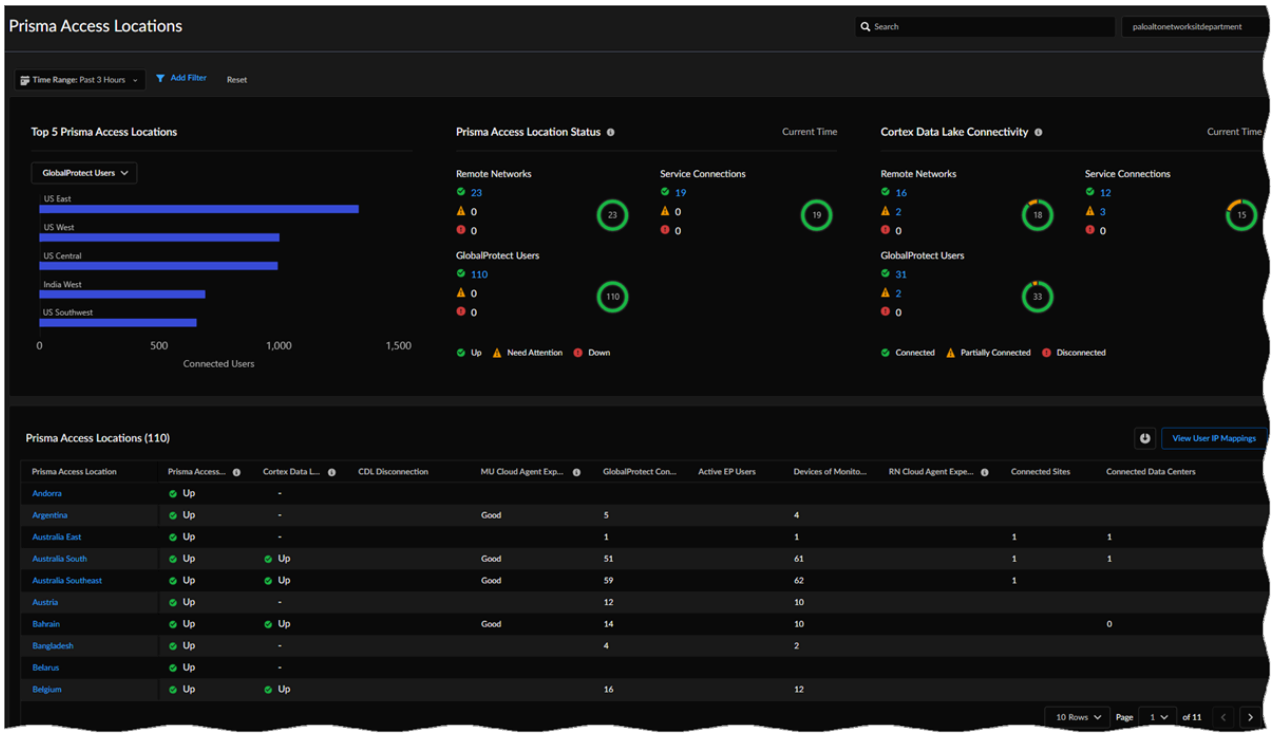
- 使用以下属性筛选数据：
  - **Metric**（指标）- 选择一个或多个要使用度量名称查看或搜索的指标。
  - **Model**（型号）- 选择一个或多个设备型号或使用型号名称进行搜索。
  - **Capacity**（容量）- 选择 **Capacity Filter**（容量筛选器）标尺上的容量。

要了解有关如何使用容量分析器热图的详细信息，请参阅分析指标容量。

监视：Prisma Access 位置

在何处可以使用？	需要提供什么？
• Prisma Access （利用 *Strata Cloud Manager* 或 *Panorama* 配置管理）	❑ Prisma Access 许可证 这是一个 Prisma Access Insights 功能。

要开始，请选择 **Monitor**（监控） > **Prisma Access Locations**（**Prisma Access** 位置）。这里可以查看远程网络和移动用户的所有 Prisma Access 位置的运行状况。有关这些小部件的详细说明，请参阅《*Prisma Access* 管理指南》中的查看和监视 Prisma Access 位置。

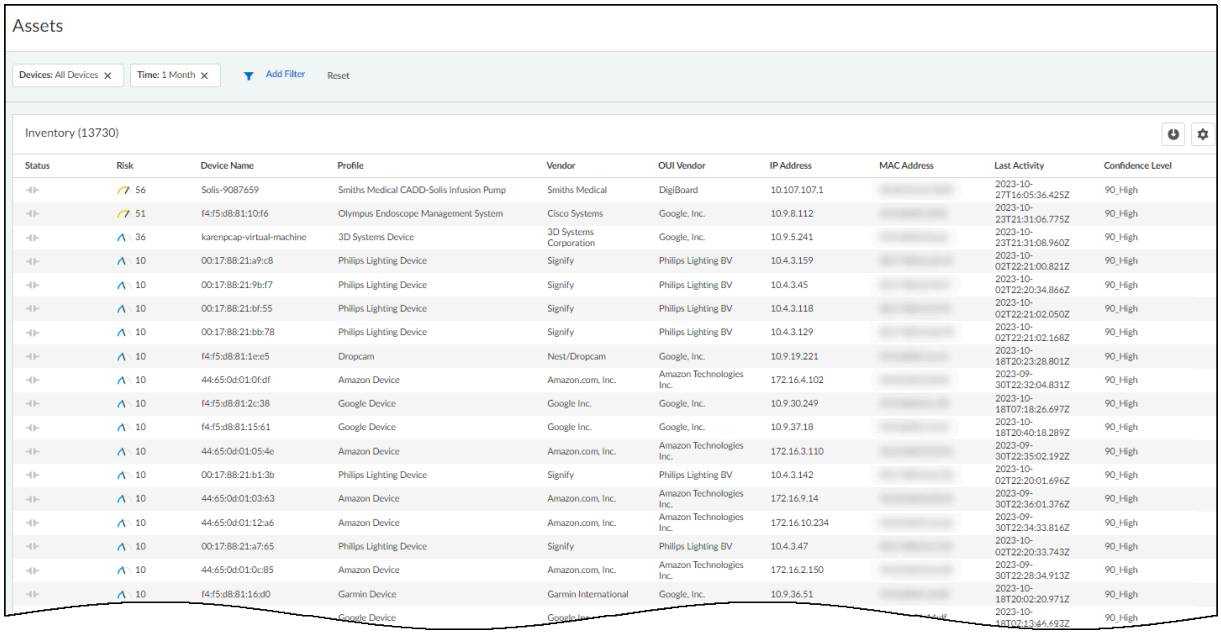


- 根据消耗的总带宽，请参阅远程网络、服务连接、GlobalProtect 移动用户或显式代理移动用户的前 5 个 Prisma Access 位置。
- 查看 Prisma Access 位置的状态。
- 查看 Strata Logging Service 连接。
- 查看 Prisma Access 位置表，其中列出了所有 Prisma Access 位置，并按名称选择单个 Prisma Access 位置以查看其详细信息。

监视：资产

在何处可以使用？	需要提供什么？
• NGFW （利用 *Strata Cloud Manager* 或 *Panorama* 配置管理）	❑ IoT Security 订阅 ❑ 软件 NGFW 积分 （适用于 *VM-Series* 软件 *NGFW*）

首先，选择监控 > 资产。这里可以查看网络上 IoT、OT 和 IT 设备的动态维护清单，其中包含每个设备的众多属性，例如其 IP 和 MAC 地址；配置文件、供应商、型号和操作系统；以及（对于高级 IoT Security 产品）其设备级风险评分。



使用此清单中的数据来了解您网络上的资产：

- 查看网络上检测到的设备（包括 IoT、OT 和 IT 设备）的动态生成和最新库存。
- 虽然 IoT 指示板可以高层次地显示您拥有的设备类型，但资产清单可让您探索单个设备以查看更多详细信息并评估其安全态势。
- 按站点、设备类型、时间段以及一个或多个设备属性筛选指示板中显示的数据，以查看有关感兴趣的设备的数据。
- 显示和隐藏列以查看对您重要的设备属性。有超过 100 个属性列可供选择。
- 将当前活动页面上显示的数据下载为 CSV 格式的文件，以便包含在报告中或供将来参考。该文件包含下载时显示的设备和设备属性。

事件和警报：Strata Cloud Manager

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW，包括由 软件 NGFW 积分提供资助的项目 • Prisma SD-WAN	这些许可证中的每一个都包括 Strata Cloud Manager 访问权限： ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Prisma SD-WAN ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro 提高可见性所需的其他许可证和先决条件是： ❑ 有权查看指示板的角色 → 您可用的特性和功能Strata Cloud Manager取决于您使用的许可证。

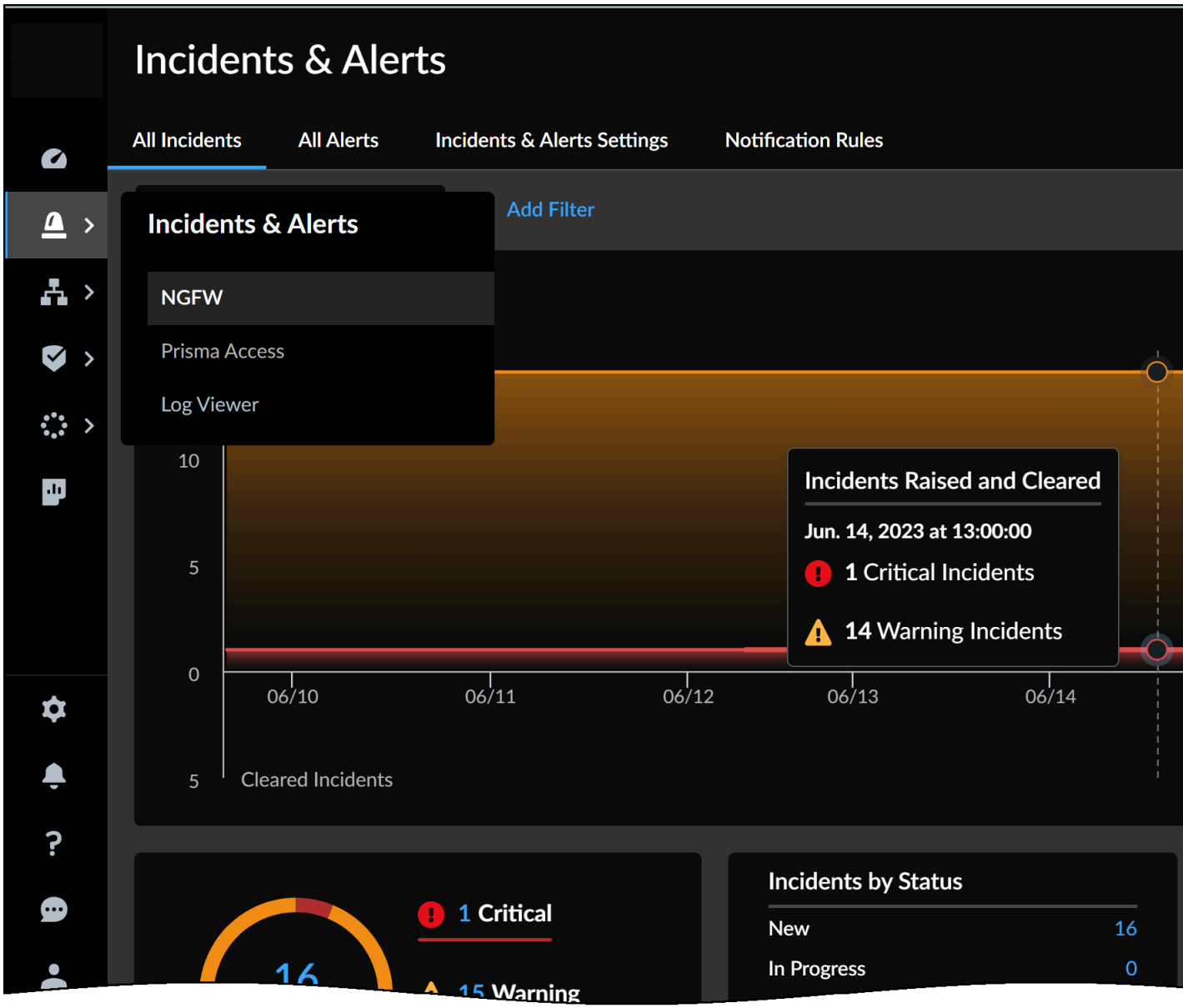
Strata Cloud Manager 为您提供一个通用框架，用于交互和调查 Palo Alto Networks 产品和订阅在您的企业中检测的事件和警报：

- 事件和警报：NGFW
- 事件和警报：Prisma Access
- 事件和警报：Prisma SD-WAN

为了帮助您保持设备和部署的持续运行状况，并避免对您的业务造成中断，请浏览每个事件和警报页面，以便：

- 查看整个网络中的事件和警报，并深入调查。
- 创建并查看触发事件和警报通知的规则。

您可以在事件和警报之间移动，事件和警报：日志查看器 会调查网络上触发事件和警报或与事件和警报关联的活动。



事件和警报：NGFW

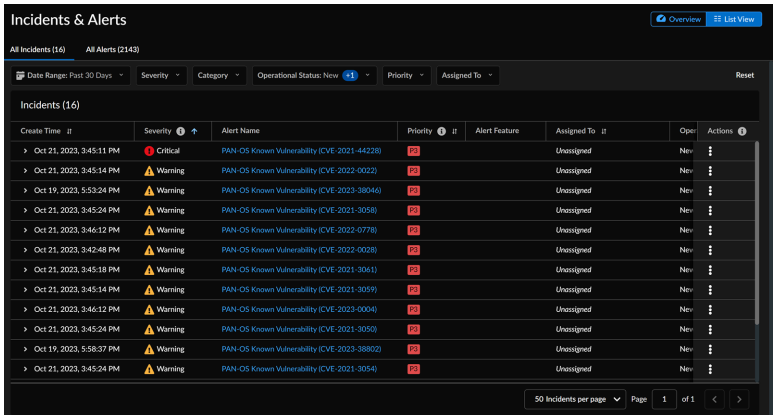
在何处可以使用？	需要提供什么？
• NGFW，包括由 软件 NGFW 积分提供资助的项目	❑ 以下许可证之一： ❑ AIOps for NGFW Free (use the AIOps for NGFW Free app) 或 AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro

为了帮助您维护设备的持续运行状况并避免中断业务的事件，您的应用程序会根据它在防火墙部署中检测到的一个或多个问题生成事件和警报。利用 **Incidents & Alerts**（事件和警报） > **NGFW**，您可以获得跨 NGFW 的事件和警报的单一视图。

下面介绍如何启动和运行 **NGFW Incidents & Alerts**（**NGFW** 事件和警报）：

- 事件可让您随时了解漏洞。您可以调查它们并在必要时采取预防措施。

  导航到 **Incidents & Alerts**（事件和警报） > **NGFW** > **All Incidents**（所有警报），以便 view incidents across your network, and interact with them（查看您的网络中的警报并与其交互）。



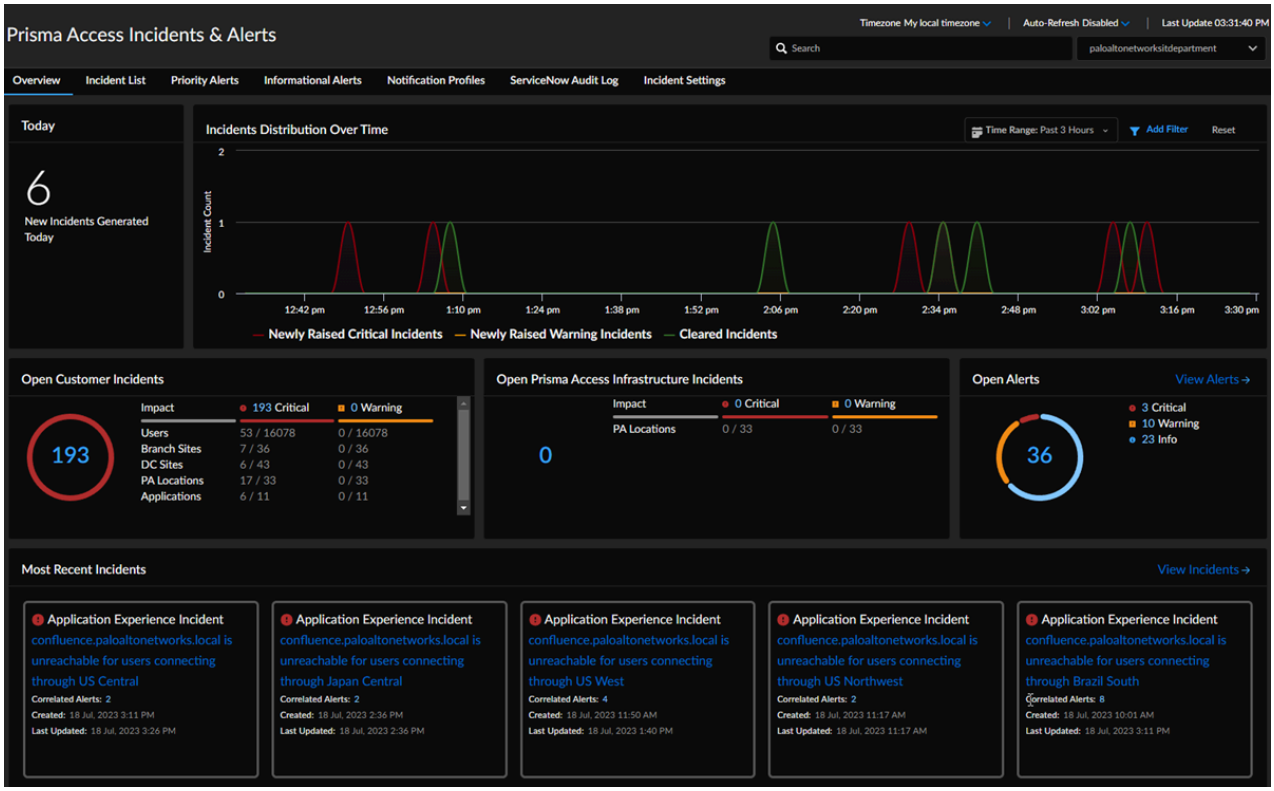
- 警报表示需要解决的特定问题（防火墙功能降级或丧失）。也可以根据多个事件的关联或聚合来生成警报。通过将事件聚合到单个警报中，有助于分类警报、简化团队之间的警报移交流程、集中关键信息并减轻通知疲劳。

  导航到 **Incidents & Alerts**（事件和警报） > **NGFW** > **All Alerts**（所有警报），以便查看您的网络中的警报并与其交互。

事件和警报：Prisma Access

在何处可以使用？	需要提供什么？
• Prisma Access （利用 *Strata Cloud Manager* 或 *Panorama* 配置管理）	❑ AI-Powered ADEM 许可证 ❑ ADEM Observability 许可证 ❑ Prisma Access 许可证

要开始，请选择 **Incidents & Alerts**（事件和警报） > **Prisma Access Incidents & Alerts**（**Prisma Access** 事件和警报）。您的环境中可用的事件和警报取决于您的许可证。



获取概览

查看与您的 Prisma Access 环境相关的事件和警报信息的概览。您的环境中可用的事件和警报取决于您的许可证。

查看所有事件

查看事件列表，其中显示您环境中的所有事件。使用 **Add Filter**（添加筛选器）下拉菜单，在表格中按列选择事件（您可以筛选多个）。在表格中，选择任何 **Incident**（事件），以查看详细信息。

查看优先警报

查看优先警报，其中介绍您的 Prisma Access 环境的状态。

查看信息警报

查看信息警报，它会通知您即将进行的软件升级以及正在进行或已完成的升级的状态。

通知配置文件

从通知配置文件中，您可以查看有关 **Notification Subscriptions**（通知订阅）的信息，并创建新的或修改现有的 **Notification Profile**（通知配置文件）。

ServiceNow 审核日志

如果您正在使用 ServiceNow，则可以查看 ServiceNow 审核日志，其中会显示每个 ServiceNow **Incident ID**（事件 **ID**）。它还向您展示了对每个事件执行的 ServiceNow 操作，例如创建、更新和删除。

事件设置

从事件设置中，您可以根据事件类别和事件代码自定义接收的事件。

按代码分类的事件和警报

通过代码 ID 查看事件和警报，了解它们所描述的问题，并找出如何修补这些问题。事件和警报按许可证分类：

- AI 驱动的 ADEM 事件
- ADEM 事件
- Prisma Access 事件
- 优先警报
- 信息警报

有关事件和警报的信息，请参阅事件和警报参考指南。

有关 ServiceNow 集成的信息，请参阅 集成指南中的将 ServiceNow 与 Prisma Access 集成。

事件和警报：Prisma SD-WAN

在何处可以使用？	需要提供什么？
• Prisma SD-WAN	❑ Prisma SD-WAN 许可证

Prisma SD-WAN 在系统达到系统定义或客户定义的阈值或系统出现故障时生成事件和警报。使用这些事件和警报对系统进行故障排除。

选择 **Incidents and Alerts**（事件和警报） > **Prisma SD-WAN**，以便在 Strata Cloud Manager 中查看事件和警报。

使用以下选项卡浏览 Prisma SD-WAN 中的事件和警报。

- 概述
- 事件
- 警报
- 设置

概述

在 Prisma SD-WAN 中查看事件和警报及其类别。**Overview**（概览）选项卡默认视图。

查看显示以下信息的顶级事件和警报。

事件类型	显示事件的类别。
说明	显示事件的描述。
严重性级别	显示事件的严重性。
优先级	显示事件的优先级。
相关警报	显示此事件中聚合的事件数。
状态	显示事件的状态。
创建于	显示系统引发事件的时间。
上次更新	显示系统上次更新事件的时间。

事件

事件是系统发生故障的指示。提出和清除各种严重程度的事件：

- 严重 — 整个或部分网络出现故障，需要立即采取行动。
- 警告 — 影响网络，需要立即关注。

- — 网络降级，需要尽快关注

。

警报

警报可能是也可能不是网络故障的指示。当系统达到系统定义或客户定义的阈值时，会发出警报。

设置

使用 **Settings**（设置）选项卡创建事件策略，以根据配置的指定分类和操作属性管理事件代码抑制。您可以使用事件策略规则抑制或上报在计划时间段内发生的事件。此外，您还可以将系统生成的事件的默认优先级更改为更符合业务需求的优先级。

事件和警报：日志查看器

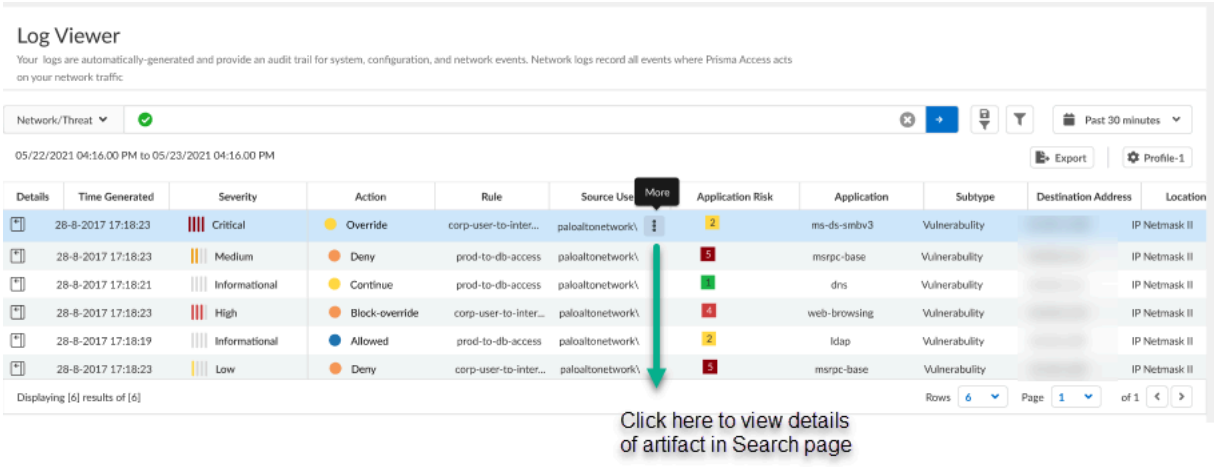
在何处可以使用？	需要提供什么？
• Prisma Access （利用 *Strata Cloud Manager* 或 *Panorama* 配置管理） • NGFW，包括由 软件 NGFW 积分提供资助的项目	❑ 这些许可证中的每一个都包括 Strata Cloud Manager 访问权限： ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) 或 AIOps for NGFW Free (use the AIOps for NGFW Free app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro ❑ 有权查看指示板的角色

Log Viewer（日志查看器）提供了浏览功能 — 您可以在其中查看存储在 Strata Logging Service 中的日志并与之交互。

Log Viewer（日志查看器）为系统、配置和网络事件提供审计跟踪。从指示板跳转到日志，以获取详细信息并调查结果。查询字段和时间范围首选项可帮助您缩小感兴趣的特定日志的范围。

- 了解有关如何构建查询的详细信息
- 在 Strata Logging Service发行说明中发现新的日志查看器功能。

Log Viewer（日志查看器）突出显示日志的操作和严重性，以帮助您了解会话是如何实施的。您还可以在搜索页面中查看日志的安全对象的详细信息。



* 您可以在搜索以下日志类型和日志字段中查看详细信息：

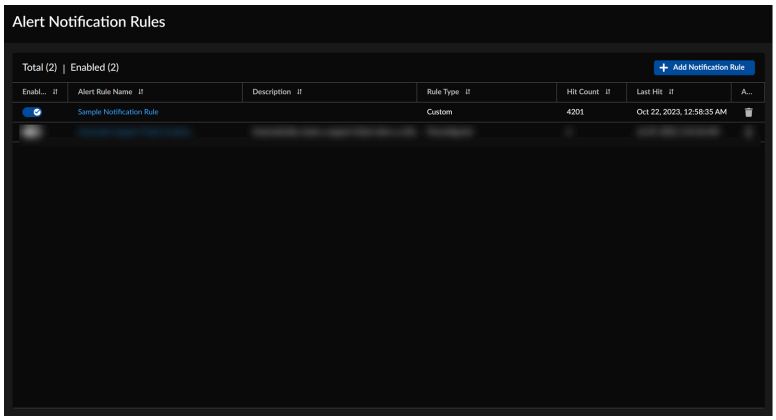
日志类型	列名
流量、威胁、URL、文件	• Source Address（源地址） • 目标地址 • NAT 源 • NAT 目标
威胁、文件	文件哈希
URL	• URL • URL 域名
DNS 安全	• Source Address（源地址） • 目标地址 • 域 • FQDN

事件和警报设置

在何处可以使用？	需要提供什么？
• NGFW，包括由 软件 NGFW 积分提供资助的项目	❑ AIOps for NGFW Free (use the AIOps for NGFW Free app) 或 AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro

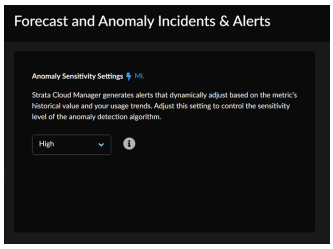
- 要定义通知首选项，如触发通知的警报、接收通知的方式以及接收通知的频率，请创建通知规则。

  导航至 **Incidents & Alerts**（事件和警报） > **Incident & Alert Settings**（事件和警报设置） > **Notification Rules**（通知规则），以查看并将规则添加到触发器通知。



- Strata Cloud Manager 生成警报和事件，根据指标的历史价值和您的使用趋势动态调整。您可以调整此设置来控制异常检测算法的敏感度级别。

  导航至 **Incidents & Alerts**（事件和警报） > **Incident & Alert Settings**（事件和警报设置） > **Anomaly Sensitivity**（异常敏感度），以便配置异常检测算法的敏感度级别。

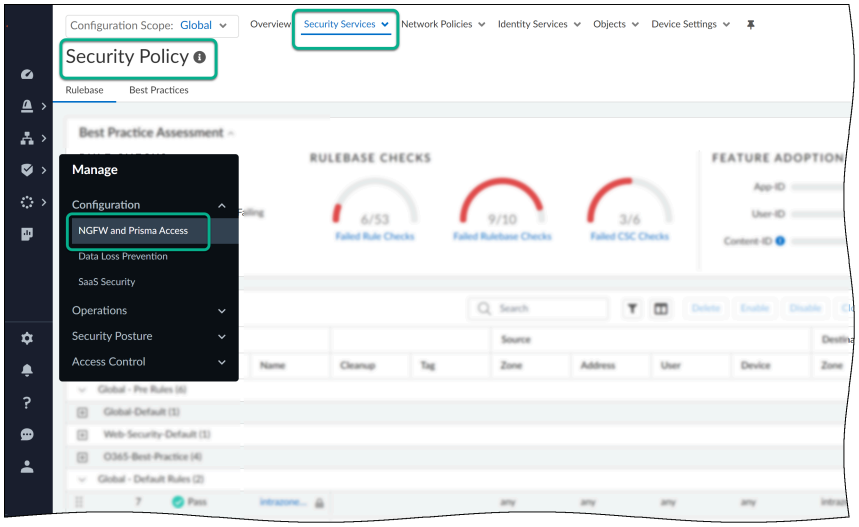


管理：NGFW 和 Prisma Access

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW，包括由 软件 NGFW 积分提供资助的项目	这些许可证中的每一个都包括 Strata Cloud Manager 访问权限： ❑ Prisma Access ❑ AIOps for NGFW Premium ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → 您可用的特性和功能Strata Cloud Manager取决于您使用的许可证。

Strata Cloud Manager 使您能够配置在 NGFW 和 Prisma Access 之间共享的安全策略。要开始使用：

- ❑ 使用以下工具设置 Prisma Access、NGFW 或两者 Strata Cloud Manager
- ❑ 设置文件夹来对需要类似设置的 NGFW 进行分组。Prisma Access 文件夹是预定义的，使您能够根据部署类型进行目标配置：移动用户、远程网络、服务连接。
- ❑ 设置您要在其中工作的 管理：配置范围。您可以配置在 NGFW 和 Prisma Access 环境中全局应用的设置，还可以根据 文件夹将配置定位到特定的 NGFW 或 Prisma Access 部署。
- ❑ 使用 管理：代码段 为一系列 NGFW 或部署制定标准化的通用基础配置。代码段使您能够快速加入具有已知良好配置的新设备、用户或位置，并减少加入新设备所需的时间。
- ❑ 转到 **Manage**（管理） > **Configuration**（配置） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**），开始创建安全策略，并使用上述管理功能在 NGFW 和 Prisma Access 之间共享它。



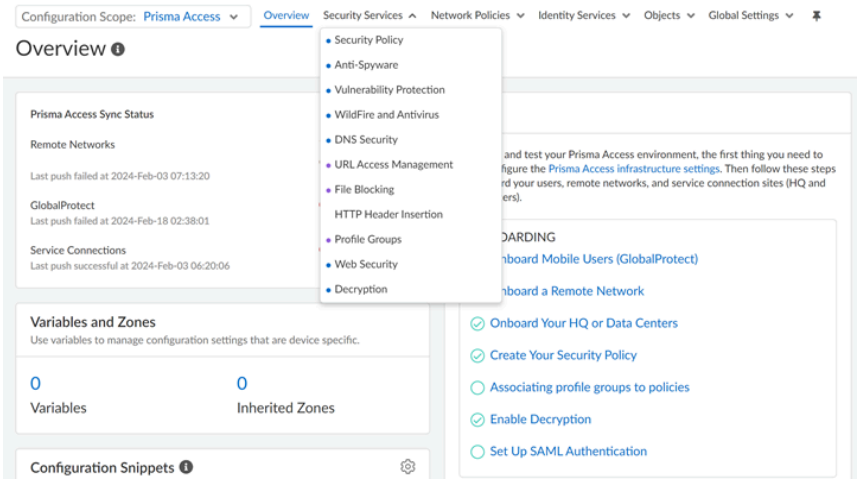
管理：配置范围

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW，包括由 软件 NGFW 积分提供资助的项目	这些许可证中的每一个都包括 Strata Cloud Manager 访问权限： ❑ Prisma Access ❑ AIOps for NGFW Premium ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → 您可用的特性和功能Strata Cloud Manager取决于您使用的许可证。

使用 Strata Cloud Manager，您可以应用配置设置并在整个环境中全局实施策略，或者将设置和策略定位到组织的某些部分。在进行 Strata Cloud Manager 配置管理时，您始终可以看到当前的 **Configuration Scope**（配置范围），您可以切换视图以管理更广泛或更精细的配置。

您可以清楚地了解适用于特定配置范围的配置元素，以及它们是继承自通用配置范围还是由系统生成。颜色编码的配置指示器可帮助您了解配置的继承来源，还可以直观地区分对象类型，以便进行扫描。

- 灰点表示继承的配置
- 紫点表示预定义的配置
- 蓝点表示该对象存在于当前配置范围中



全局配置设置可帮助您轻松管理和执行适用于所有网络流量的策略要求。或者，您可以根据合理的部署类型来确定策略和配置设置。

- **Prisma Access**
  - 移动用户容器 — 设置适用于所有移动用户连接类型：全局保护和显式代理，或分别针对每种连接类型。
  - 远程网络 — 设置适用于远程网络站点（分支机构、零售点等）。
  - 服务连接— 设置适用于服务连接站点（总部和数据中心）。
- 所有防火墙 — 设置适用于您的所有 NGFW，或适用于将需要共享或特定配置设置或策略实施的 NGFW 组合在一起的特定文件夹。

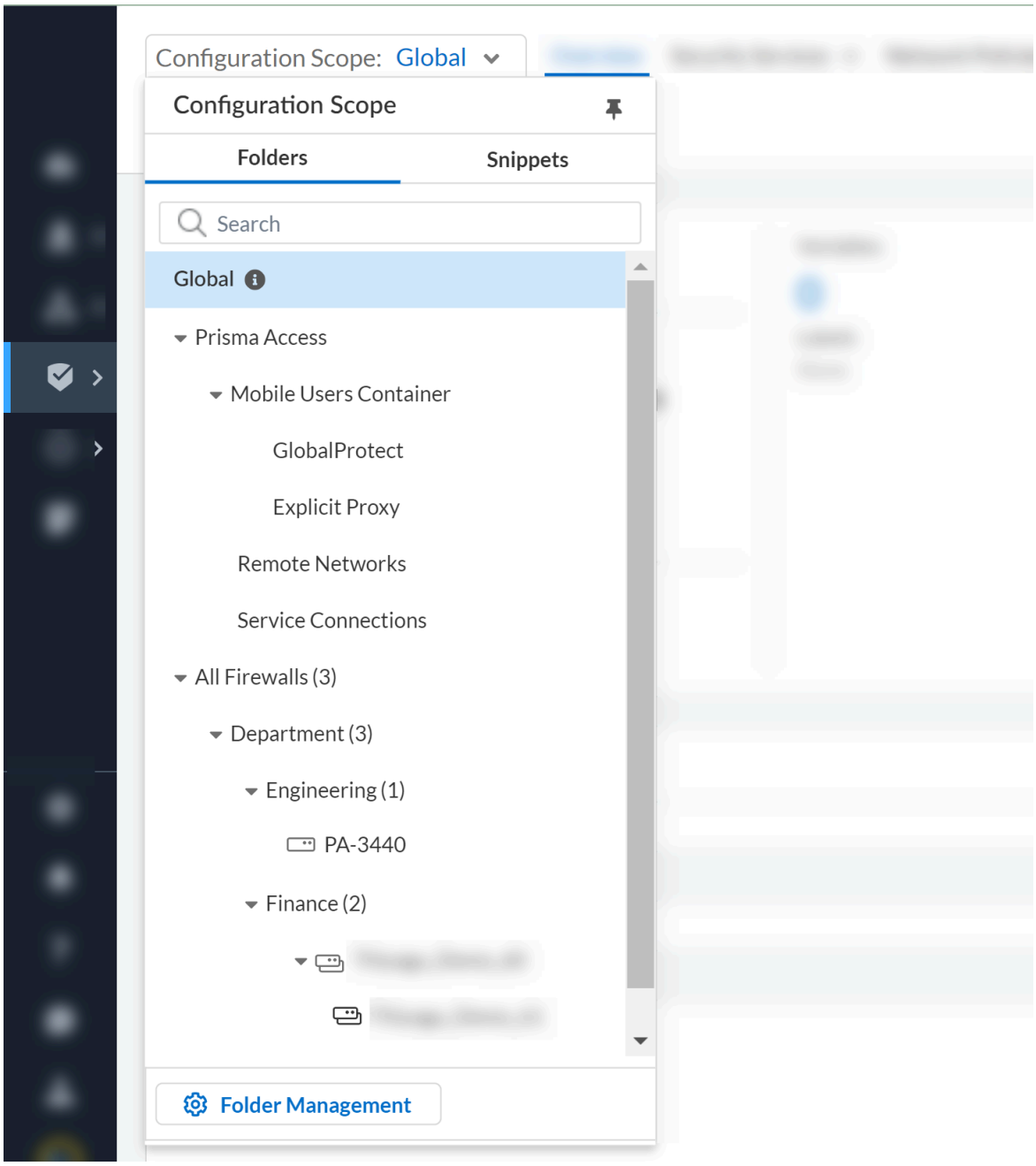
了解有关以下内容的更多信息：

- 工作流程：文件夹管理

  使用文件夹对设备和部署类型进行逻辑分组，以简化配置管理。
- 管理：代码段

  使用代码段对配置进行分组，您可以快速将其推送到防火墙或部署。
- 管理：变量

  使用配置变量来容纳设备或部署特定的配置对象。



管理：代码段

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW，包括由 软件 NGFW 积分提供资助的项目	这些许可证中的每一个都包括 Strata Cloud Manager 访问权限： ❑ Prisma Access ❑ AIOps for NGFW Premium ❑ Strata Cloud Manager Essentials

在何处可以使用？	需要提供什么？
	❑ Strata Cloud Manager Pro → 您可用的特性和功能Strata Cloud Manager取决于您使用的许可证。

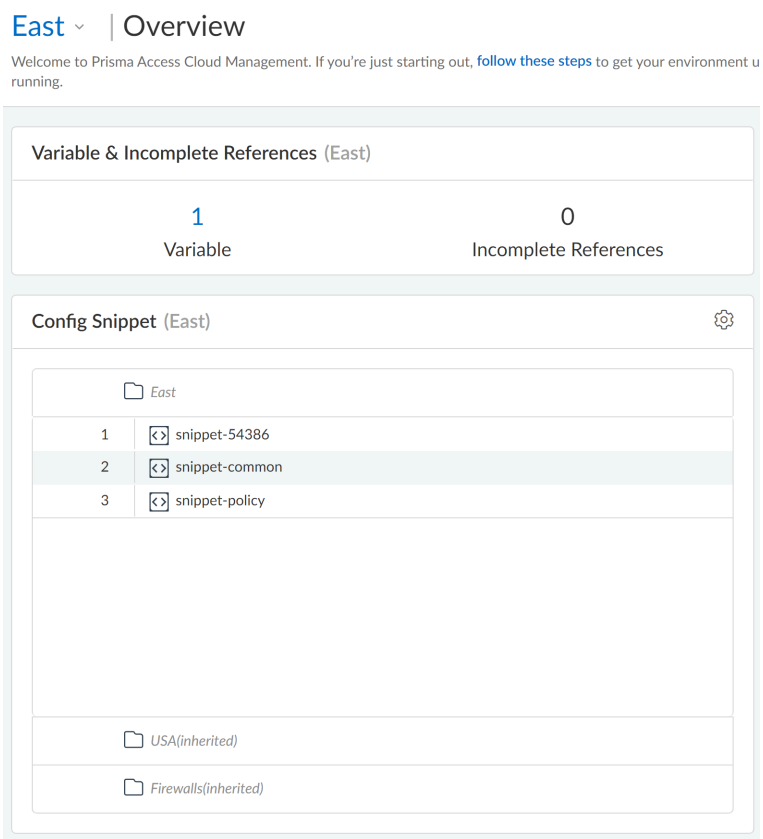
使用代码段对配置进行分组，您可以快速将其推送到防火墙或部署。

代码段是一个配置对象，它不适合与文件夹、部署或设备关联的层次结构或配置对象分组。代码段用于标准化一组防火墙或部署的通用基本配置，使您能够快速载入已知良好配置的新设备，并缩短载入新设备所需的时间。例如，您可以在远程分支机构安装新的防火墙。您可以将一组包含所有必需的网络和策略规则配置的代码段与新防火墙所属的文件夹相关联。这减少了设置防火墙以保护远程分支机构所需的时间。

如果对象值发生冲突，代码段关联具有自上而下的优先级。不允许使用具有重复名称的规则，并且在任何文件夹中创建同名代码段期间，或者如果已关联同名代码段将代码段关联到文件夹，则验证失败。

这意味着，如果第一个和最后一个关联代码段对同一个对象具有不同的值，则设备或部署会继承第一个代码段的值。此外，从代码段继承的所有配置都可以在子文件夹、部署或设备级别上被覆盖。

在文件夹层次结构中，一个代码段只能在任何文件夹层次结构中关联一次。这意味着代码段不能同时与文件夹和嵌套在其下的文件夹相关联。但是，您可以将同一个代码段与不同的文件夹或嵌套在不同文件夹下的文件夹相关联。已经与文件夹层次结构中的某个文件夹关联的代码段显示为灰色，因此在适用的情况下不能多次使用。



代码段中的跨范围配置可参考性

此功能允许您引用连接到全局范围的任何常见配置或对象，并将其推送到 Prisma Access 和 NGFW 防火墙。这些全局范围内的共享对象和配置可供所有代码段使用。与全局范围相关的代码段被视为全局代码段。在这些附加到全局范围的代码段中定义的对象可以在配置中的任何代码段中引用。

例如，您可以创建一个名为“全局变量”的代码段来合并变量并将其附加到全局范围。这确保了配置中所有其他代码段的易于引用和可用性。同样，您可以有效地管理访问策略规则、威胁防御配置文件、服务区、地址，以及其他代表标准网段的对象的自定义 URL 类别。

创建代码段

创建代码段并将其与文件夹、部署或设备相关联，以将通用基本配置应用于一组设备。您可以根据需要将任意数量的代码段与文件夹、部署或设备相关联。

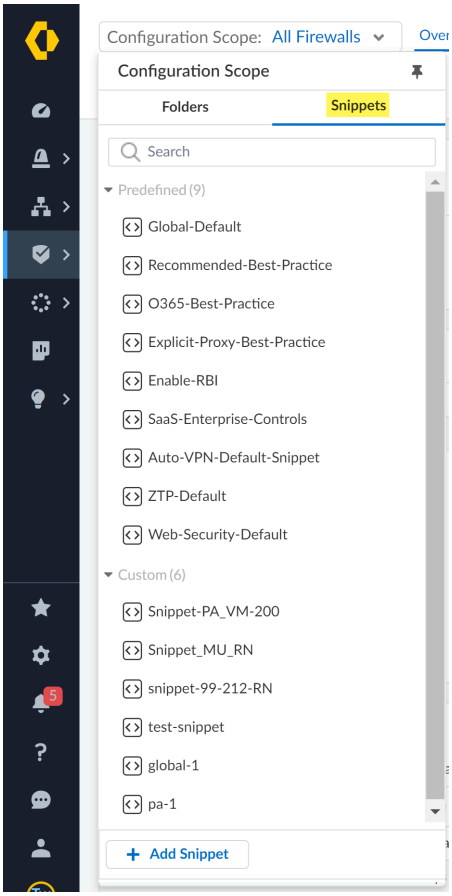
代码段可以在创建后随时修改并与任何文件夹、部署或设备重新关联。

可以删除不再使用的自定义代码段。

STEP 1 | 登录 Strata Cloud Manager。

STEP 2 | 选择 **Manage**（管理） > **Configuration**（配置） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Overview**（概览），并展开配置范围以查看 **Snippets**（代码段）。

STEP 3 | **Add Snippet**（添加代码段）。

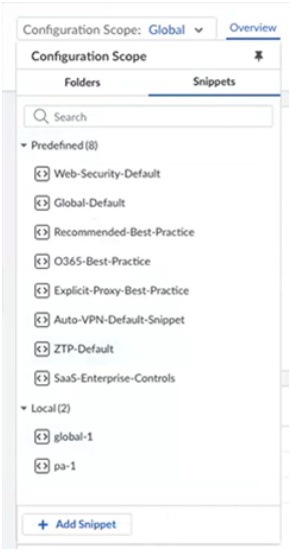


STEP 4 | 创建代码段。

1. 为该代码段指定一个描述性的 **Name**（名称）。
2. （可选）输入代码段的 **Description**（说明）。
3. （可选）分配一个或多个 **Labels**（标签）。

   您可以选择现有标签，也可以通过键入要创建的标签来创建新标签。
4. **Create**（创建）。

   新创建的代码段列在 **Local**（本地）代码段下面。发布代码段后，它们将移至“已发布的代码段”下方。



STEP 5 | 创建您的代码段配置。

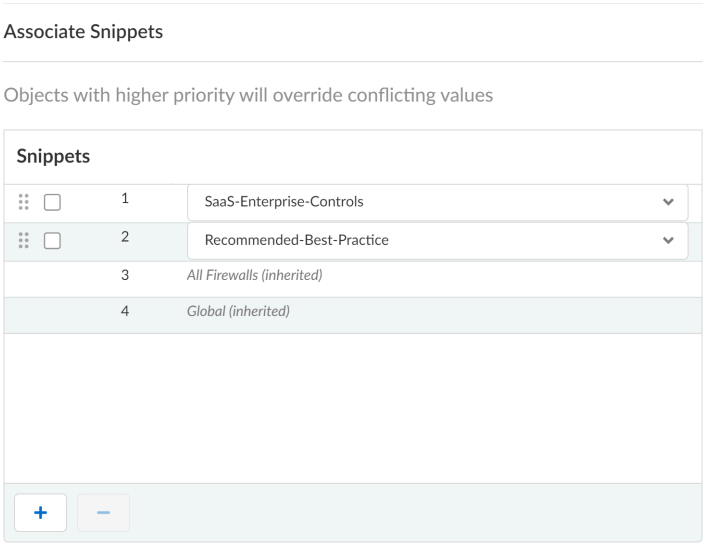
您现在处于该代码段的配置范围内。您在代码段范围内创建的所有配置仅适用于代码段。

在代码段范围内，您可以查看代码段 **Overview**（概览），以查看有关该代码段的详细信息。这包括变量数量、有关代码段创建和上次更新的信息，以及与该代码段关联的所有文件夹、部署和设备的列表等信息。

STEP 6 | 关联代码段。

1. 选择 **Manage**（管理） > **Configuration**（配置） > **NGFW and Prisma Access**（**NGFW 和 Prisma Access**） > **Overview**，并展开配置范围以查看 **Config Tree**（配置树）。
2. 选择要将代码段关联的文件夹、部署或设备。
3. 编辑 **Config Snippet**（配置代码段）。
4. 添加要关联的代码段并根据需要对其进行排序。

   如果您将代码段关联到全局范围，则该代码段将变为可引用且可供配置中的所有其他代码段使用。所有代码段都将能够引用您在附加到全局文件夹的代码段中的对象。
5. **Close**（关闭）。



STEP 7 | **Push Config**（推送配置）将您的配置更改推送到您的网络。

修改代码段

修改您的代码段配置、详细信息和关联。

可以删除不再与文件夹、部署或设备关联的自定义代码段。

STEP 1 | 登录 Strata Cloud Manager。

STEP 2 | 选择 **Manage**（管理） > **Configuration**（配置） > **NGFW and Prisma Access**（**NGFW 和 Prisma Access**） > **Overview**（概览），并展开配置范围以查看 **Snippets**（代码段）。

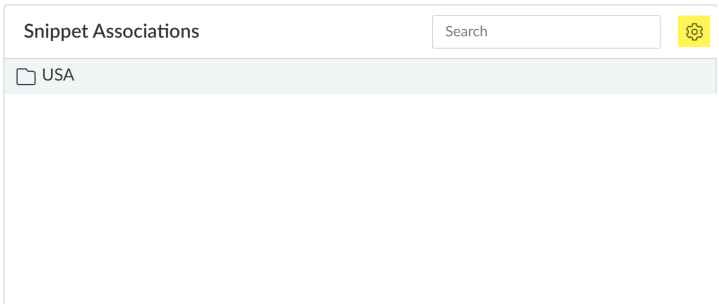
STEP 3 | 选择要修改的代码段。

选择代码段后，您将被重定向到代码段 **Overview**（概览）。

STEP 4 | （可选）编辑代码段以修改 **Name**（名称）、**Description**（说明），或者更改或分配其他 **Labels**（标签）。启用或禁用 **Pause Update**（暂停更新），以查看配置差异并决定接受更改。

STEP 5 | 编辑 **Snippet Associations**（代码段关联），将代码段与其他文件夹、部署或设备重新关联，或将代码段与其他文件夹、部署或设备相关联。

退出代码段重新关联屏幕以应用更改。



STEP 6 | 根据需要对代码段配置进行任何更改。

STEP 7 | **Push Config**（推送配置）。

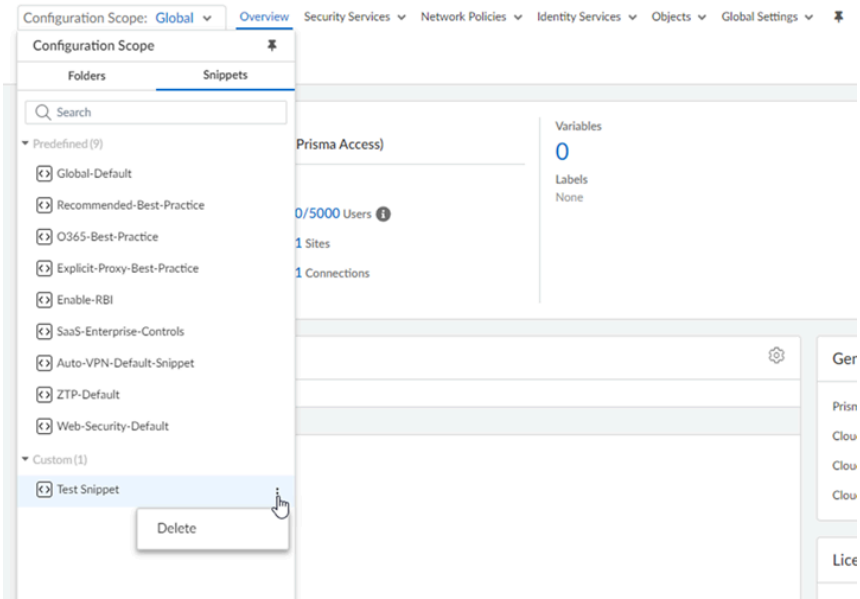
删除代码段

删除您的自定义代码段以保持配置井井有条。必须先取消代码段与任何防火墙、文件夹或部署的关联，然后才能将其删除。不支持删除预定义的代码段。

STEP 1 | 登录 Strata Cloud Manager。

STEP 2 | 选择 **Manage**（管理） > **Configuration**（配置） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Overview**（概览），并展开 **Configuration Scope**（配置范围）以查看代码段。

STEP 3 | 单击要删除的自定义代码段的三个垂直点。



STEP 4 | **Delete**（删除）该代码段。

> 无法删除当前与文件夹、部署或设备关联的代码段。首先编辑 ***Snippet Associations***（代码段关联），以移除所有现有关联，然后才能将其删除。

克隆代码段

如果您想使用现有代码段作为新代码段的模板，则可以轻松地将其克隆，这样就不必配置新对象。

克隆的代码段不与任何设备、文件夹或部署相关联，因此您可以自由地对其进行自定义，而不必在开始配置之前取消关联。

STEP 1 | 登录 Strata Cloud Manager。

STEP 2 | 选择 **Manage**（管理） > **Configuration**（配置） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Overview**（概览），并展开 **Configuration Scope**（配置范围）以查看代码段。

STEP 3 | 单击要克隆的自定义代码段的三个垂直点。

STEP 4 | **Clone**（克隆）代码段。

1. （可选）为克隆的代码段起一个新名称。

共享代码段配置

此功能为包括多租户环境在内的任何租户共享通用配置提供了一种独特而灵活的方法。您可以将各种配置保存和管理为代码段，在客户帐户下轻松地在租户之间共享这些配置。此功能为管理不同租户环境中的共享配置提供了相当大的灵活性和控制力。

此外，此功能支持对租户之间的常见场景进行集中配置管理，并监督多业务部门设置中的全球配置。

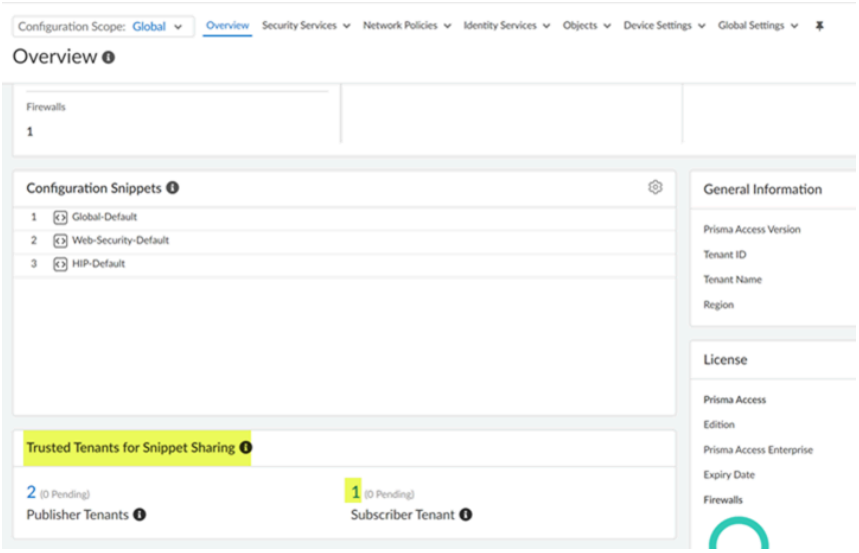
在此框架中，发布商租户与订阅者租户共享代码段，而订阅者租户则从发布商租户接收代码段。

STEP 1 | 登录 Strata Cloud Manager。

STEP 2 | 在发布商租户上，选择 **Manage**（管理） > **Configuration**（配置） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Overview**（概览），然后选择 **Global**（全局）配置范围。

STEP 3 | 在租户之间建立信任：在订阅者和发布者租户之间建立连接，以实现代码段共享。

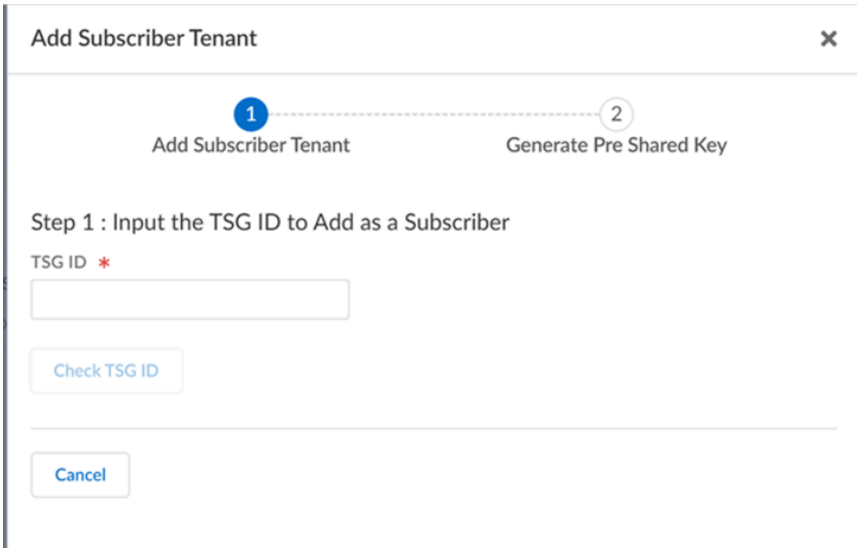
1. 单击 **Trusted Tenants for Snippet Sharing**（用于代码段共享的可信租户）下的 **Subscriber Tenant**（订阅者租户）。



2. **Add Subscriber Tenant**（添加订阅者租户）。

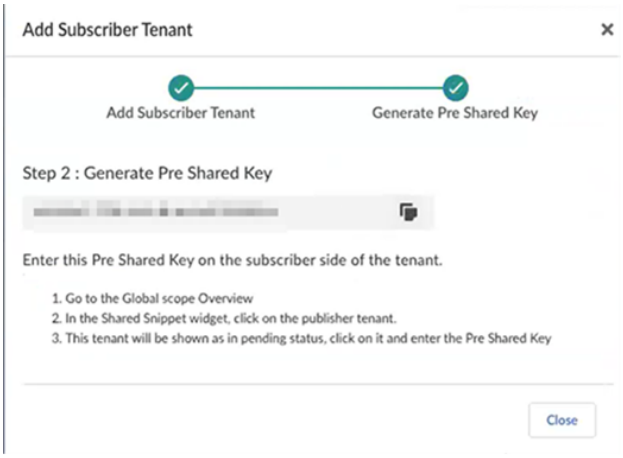
3. 输入要添加为订户租户的 **TSG ID**，然后 **Check TSG ID**（检查 **TSG ID**）。这样可以确保防止随机生成的 TSG 或基于 TSG 的序列化攻击。

   成功验证后，一条确认消息表明 TSD ID 已通过验证。



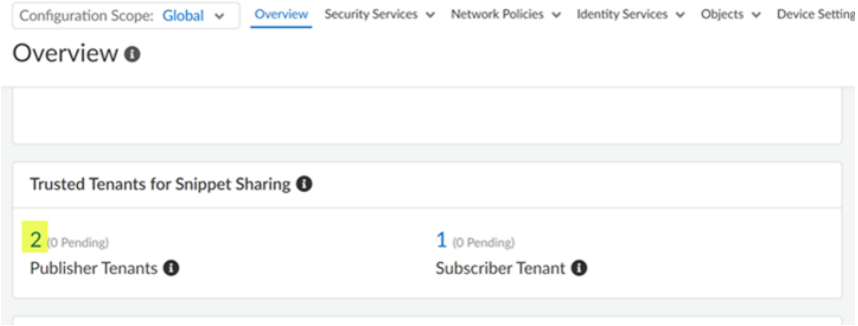
4. **Next:Generate Pre Shared Key**（下一步：生成预共享密钥）。

   复制生成的 PSK。在步骤 4 中验证发布商租户时，您将输入此 PSK。



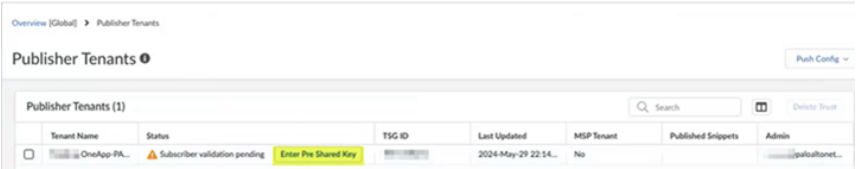
STEP 4 | 转到订阅租户，选择 **Manage**（管理） > **Configuration**（配置） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Overview**（概览），然后将配置范围设置为 **Global**（全局）。

1. **Trusted Tenants for Snippet Sharing**（代码段共享的可信租户）下的 **Publisher Tenants**（发布者租户）状态显示为 **Pending**（待处理）。



2. 单击 **Publisher Tenants**（发布商租户），并 **Enter Pre Shared Key**（输入预共享密钥）（该密钥是在上一步中生成的），然后 **Validate**（验证）订阅者租户。

   验证成功后，会显示一条消息来确认租户为可信租户，从而在订阅者与发布商租户之间建立信任。



STEP 5 | 向订阅者租户发布代码段。

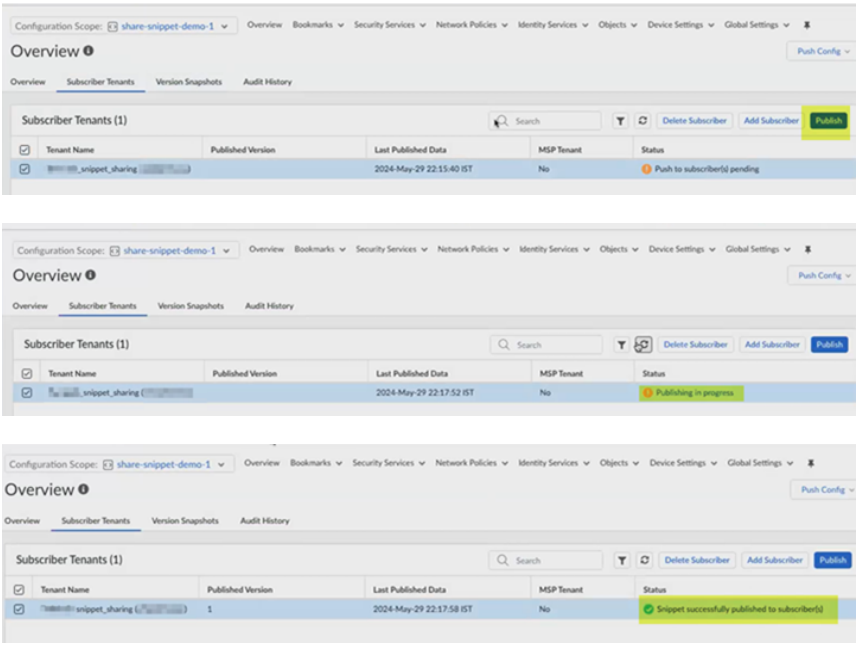
1. 创建代码段并将其与文件夹关联。

   新创建的代码段可在 **Local**（本地）代码段下找到。

   - **Overview**（概览）选项卡显示代码段的详细信息，例如名称、描述、创建时间（在订阅者端加载代码段的时间）、上次更新时间和标签的详细信息。
   - **Subscriber Tenants**（订阅者租户）选项卡显示租户名称、租户的已发布版本、上次发布日期和发布状态。
     - 单击 **Published Version**（已发布版本）来查看配置更改。
     - 在向租户发布代码段之前，**Add Subscriber**（添加订阅者）并 **Save**（保存）。
   - **Version Snapshots**（版本快照）提供您的代码段配置的历史记录。在此屏幕中，您可以将配置快照与候选配置进行比较，并 **Save Version Snapshot**（保存版本快照），或者 **Load**（加载）早期配置快照以作为候选配置。单击 **Version**（版本）号来查看配置差异。
   - **Audit History**（审核历史记录）提供管理员启动的所有操作的审计记录。它记录详细信息，例如已发布的版本号、所做的更改、变更的所有者、变更的日期和时间以及变更的具体细节。

2. 在 **Subscriber Tenant**（订阅者租户）选项卡上，选择租户名称并 **Publish**（发布）。

   这会将发布请求发送给订阅者租户。在 **Status**（状态）列中指示“代码段已成功发布给订阅者”，该代码段将在“已发布的代码段”下提供。



STEP 6 | 在订阅者租户上进行验证。

1. 转到 **Overview**（概览） > **Configuration Scope**（配置范围） > **Snippets**（代码段），然后在 **Subscribed**（已订阅）代码段下选择代码段。

   您将重定向至代码段 **Overview**（概览），其中显示了发布商租户的名称、描述、TSG ID、代码段创建时间、上次更新时间、标签和暂停更新详细信息等详细信息。

STEP 7 | 删除信任。

与文件夹或防火墙关联的订阅代码段只能克隆，不能删除。

1. 转到订阅者或发布商租户。
2. 在 **Trusted Tenants for Snippet Sharing**（用于代码段共享的可信租户）下单击 **Subscriber Tenant**（订阅者租户）。
3. 选择 **Tenant Name**（租户名称），然后选择 **Delete Trust**（删除信任）。

删除信任后，该代码段将不再与防火墙或文件夹关联，而是成为本地代码段。

代码段分类

- 已预定义：所有 Strata Cloud Manager 用户都可以访问这些代码段，使用最佳实践配置快速设置新的防火墙和部署。
- 本地：这些可编辑的代码段是在租户内创建的，无法与其他订阅者租户共享。
- 已发布：受信任的订阅者租户可以访问这些共享代码段，这些代码段无法克隆或编辑。
- 已订阅：这些代码段由发布商租户共享，可以由用户克隆，但无法编辑。

管理：变量

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW，包括由 软件 NGFW 积分提供资助的项目	这些许可证中的每一个都包括 Strata Cloud Manager 访问权限： ❑ Prisma Access ❑ AIOps for NGFW Premium ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → 您可用的特性和功能Strata Cloud Manager取决于您使用的许可证。

使用配置变量来适应设备或部署特定的配置对象。

变量是一种高级工具，允许您标准化配置，同时允许您灵活地适应特定于设备或部署的唯一配置值。变量允许您减少需要管理的代码段数量，同时允许您根据需要保留任何防火墙或特定于部署的配置值。

例如，您有一个要与多个嵌套文件夹关联的配置代码段，其中每个嵌套文件夹包含一组特定于某个地理位置的防火墙。在代码段中，您已经配置了策略规则，以限制仅对特定 IP 范围的业务关键型系统进行访问。在这种情况下，您可以为每个嵌套文件夹特定的每个 IP 范围创建一个变量，并在继承的代码段配置中使用该变量。这允许您管理和推送配置更改，同时使用更少的代码段来适应设备或部署特定的配置值。

可以在文件夹、部署或防火墙级别创建变量。为文件夹创建变量时，该变量将由嵌套在该文件夹下的所有文件夹继承。如果文件夹配置范围中的变量发生冲突，防火墙或部署将从包含嵌套文件夹的文件夹继承变量值。但是，您可以在嵌套文件夹、部署或防火墙级别重写继承的变量。

支持以下类型的变量：

变量类型	说明
AS 编号	BGP 配置中使用的自治系统编号。
计数	触发操作必须发生的事件数。
Device-ID	用于在主动/主动高可用性 (HA) 配置中分配设备优先级值的设备 ID。
设备优先级	设备优先级用于指示防火墙应在“主动-被动”高可用性 (HA) 配置中承担主动角色的首选项。
最大传出	要在服务质量 (QoS) 配置文件配置中使用的传出最大值。
FQDN	完全限定域名。

变量类型	说明
群组 **ID**	高可用性组 ID。
IP 网络掩码	静态 IP 或网络地址。
IP 范围	IP 范围。例如，**`192.168.1.10-192.168.1.20`**。
IP 通配符	允许或拒绝类似 IP 地址的 IP 掩码。例如，`10.0.0.5/255.255.0.255`。
链路标签	要在 SD-WAN 配置中使用的链路标记。
百分比	**`0`** 和 **`99`** 之间的百分比。
端口	源端口或目标端口。
QoS 配置文件	用于 QoS 配置的 QoS 配置文件。
速率	速率指定触发操作的阈值。例如，DoS 保护配置文件的警报率。
路由器 **ID**	为逻辑路由器配置边界网关协议 (BGP) 时的路由器ID。
定时器	以秒为单位的计时器，用于配置触发操作的阈值。
服务区	安全服务区。

创建一个变量

您还可以在支持变量的地方创建内联变量。

STEP 1 | 登录 Strata Cloud Manager。

STEP 2 | 选择 **Manage**（管理） > **Configuration**（配置） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Overview**（概览），然后选择要在其中创建变量的配置范围。

在 **Folders**（文件夹）中，选择要为其创建变量的文件夹或设备。

在 **Snippets**（代码段）中，选择要为其创建变量的特定代码段。

STEP 3 | 在“变量”部分中，单击显示的变量计数。

STEP 4 | **Add Variable**（添加变量）。

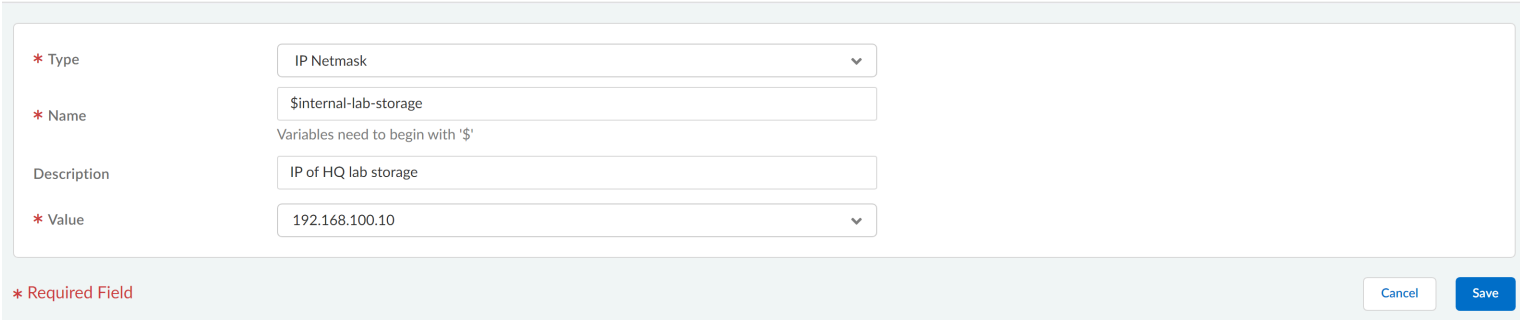
STEP 5 | 创建变量。

在本例中，创建了一个 IP子网掩码变量，用作关键内部资源的地址对象。

1. 选择变量 **Type**（类型）。
2. 给变量指定一个描述性的 **Name**（名称）。

   所有变量名必须以 **$** 开头。
3. （可选）为变量输入 **Description**（说明）。
4. 输入变量 **Value**（值）。
5. **Save**（保存）。

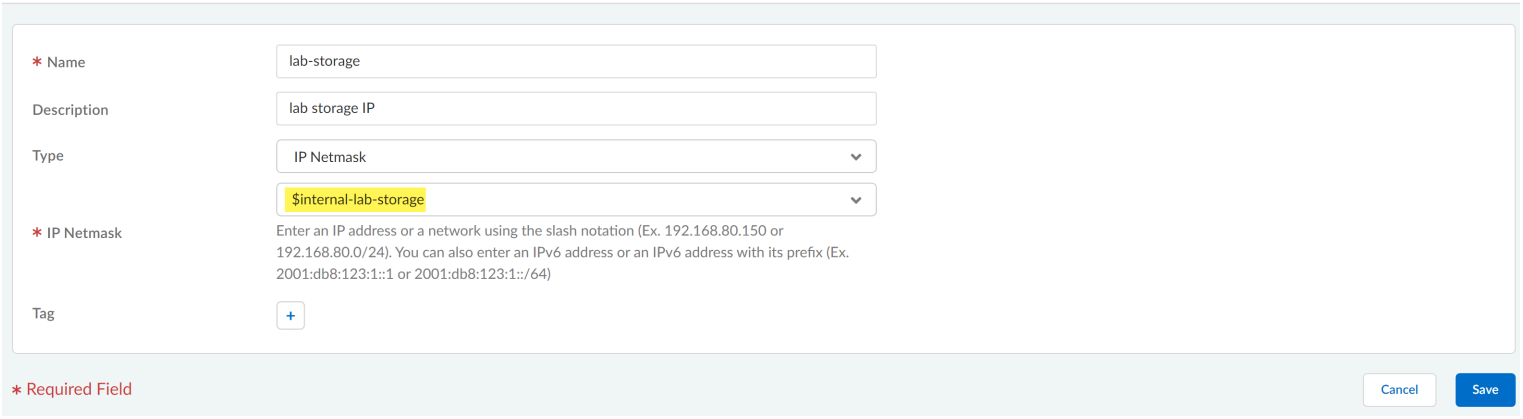
Variables



STEP 6 | 将变量添加到您的配置中。

在本例中，将在上一步中创建的 `$internal-lab-storage` 变量添加到地址对象配置中。

Addresses



STEP 7 | **Push Config**（推送配置）。

导入变量

在何处可以使用？	需要提供什么？
• Strata Cloud Manager	❑ AIOps for NGFW Premium 许可证 ❑ Prisma Access 许可证

使用 CSV 文件将变量导入到 Strata Cloud Manager 中。变量导入旨在使用新的特定于防火墙的值覆盖防火墙从文件夹层次结构继承的多个变量，或已在防火墙配置范围中配置的多个变量。

变量必须已从文件夹层次结构中继承，或在防火墙配置范围中配置为使用变量导入覆盖。不支持重新定义变量以创建全新的变量。

STEP 1 | 登录 Strata Cloud Manager。

STEP 2 | 选择 **Manage**（管理） > **Configuration**（配置） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Overview**（概览）。

STEP 3 | 在“变量”部分中，单击显示的变量计数。

STEP 4 | 选择 **CSV Export/Import**（**CSV** 导出/导入） > **Export**（导出）以导出要覆盖的变量。

Palo Alto Networks 建议您首先导出要覆盖的变量。这可以保证您上传到 Strata Cloud Manager 的 CSV 文件格式正确。这还通过确保目标文件夹和防火墙变量的属性正确来加快导入过程。

STEP 5 | 修改导出的 CSV 文件中的变量。

修改 CSV 文件以进行导入时，请考虑以下事项。

- 仅支持简单文本编辑器（如记事本）来修改导出的 CSV 文件。
- **#** 表示该变量在文件夹层次结构中创建，并由防火墙继承。

  删除 **#** 以使用特定于防火墙的值覆盖继承的变量值。

  导入时 Strata Cloud Manager 忽略附加有 **#** 的变量值，因为仅支持防火墙配置范围中的覆盖变量值。
- `-NA-` 表示该变量在防火墙配置中不存在。这意味着该变量是在防火墙所属的文件夹层次结构之外创建的。

  不支持将变量值更改为 `-NA-`。Strata Cloud Manager 会忽略任何修改为 `-NA-` 的变量值。

  不支持将特定于防火墙的值转换为值为 `-NA-` 的变量，因为该变量在防火墙配置范围中不存在。该变量必须由防火墙从文件夹层次结构中继承，或在防火墙配置范围中配置，以便使用变量导入覆盖。
- 变量值为 `None#` 或 `None` 意味着变量是用变量 **Value**（值）是作为 **None**（无）创建的。

  您可以将任何变量值修改为 `None`（无）以删除该值，但不能删除该变量。
- 对于在防火墙配置范围中创建的变量，删除变量值并将其保留为空将删除该变量。

  对于在文件夹层次结构中创建并由防火墙继承的变量，删除变量值并将其保留为空会将变量值恢复为从文件夹层次结构继承的值。

1. 找到并打开导出的 CSV 文件。导出的 CSV 文件的格式，文件名为：

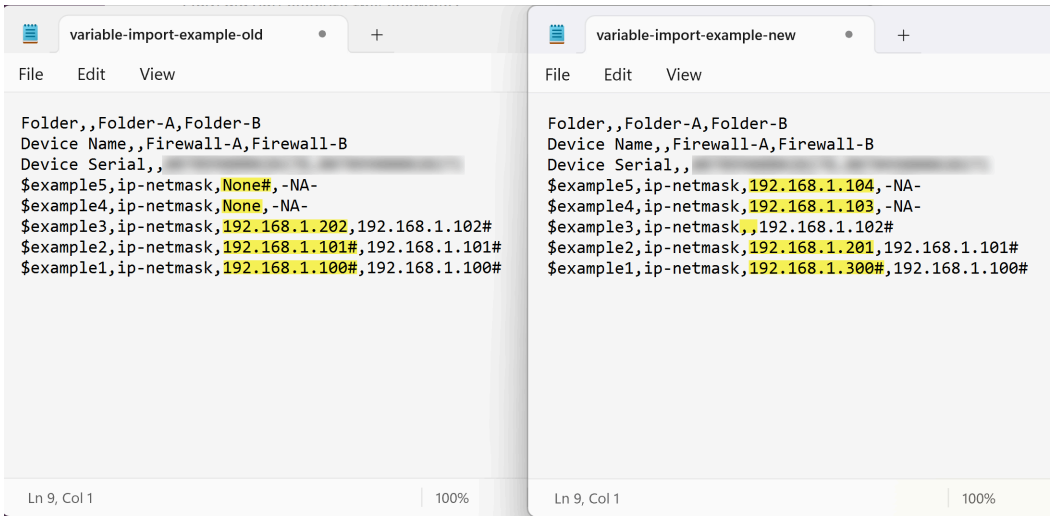
   ```
   <cloud-management-tenant-name> - Prisma Access_<export-date>_variables
   ```
2. 根据需要修改变量。

   Palo Alto Networks 建议不要修改文件夹名称、设备名称或设备序列号。这可能导致导入失败。

   在下面的示例中，对 `Firewall-A` 配置范围中的变量值进行了以下更改，以说明如何使用变量导入通过一个操作修改多个变量。

   - `$example1` — 用防火墙特定的值覆盖继承的 `None#` 值。
   - `$example2` — 用防火墙特定的值覆盖防火墙特定的 `None` 值。
   - `$example3` — 如果变量是在防火墙配置范围中创建的，则空值将删除该变量。

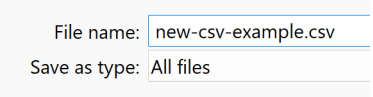
     如果变量是从文件夹层次结构继承的，并且在防火墙配置范围中被覆盖，则空值将恢复从文件夹层次结构继承的变量值。
   - `$example4` — 用防火墙特定的值覆盖继承的 `192.168.1.101` 值。
   - `$example5` — Strata Cloud Manager 忽略变量更改的示例，因为仍会附加 **#**。



STEP 6 | 保存更改。

选择 **File**（文件） > **Save**（保存），以便将更改保存到 CSV 文件中。

或者，选择 **File**（文件） > **Save As**（另存为），以便将更改保存在新的 CSV 文件中。要创建新的 CSV 文件，必须包含 **.csv** 作为文件扩展名。



STEP 7 | 将 CSV 文件导入到 Strata Cloud Manager。

1. 选择 **Manage**（管理） > **Configuration**（配置） > **Overview**（概览）。
2. 在“变量”部分中，单击显示的变量计数。
3. 选择 **CSV Export/Import**（**CSV** 导出/导入） > **Import**（导入）。
4. **Choose File**（选择文件）并选择包含您修改的变量的 CSV 文件。
5. **Import**（导入）。

导出变量

将文件夹和防火墙配置变量以 CSV 格式导出到本地设备。当跨多个防火墙检查大量变量时，导出变量非常有用。

不支持导出在文件夹级别配置接口时创建的接口变量。

STEP 1 | 登录 Strata Cloud Manager。

STEP 2 | 选择 **Manage**（管理） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Configuration**（配置） > **Overview**（概览）。

STEP 3 | 在“变量”部分中，单击显示的变量计数。

STEP 4 | 选择 **CSV Export/Import**（**CSV** 导出/导入） > **Export**（导出）。

STEP 5 | 选择包含要导出的变量的文件夹和防火墙，然后单击 **Next**（下一步）。

如果要导出在 *Strata Cloud Manager* 上创建的所有变量，请选择 ***All Firewalls***（所有防火墙）。

STEP 6 | 选择一个或多个要导出的变量。

STEP 7 | （可选）**Preview**（预览）选定变量以查看其他详细信息。

在变量预览中，您可以查看变量名称、创建变量的配置范围以及变量值等信息。

单击 **Cancel**（取消）并继续下一步，或将 **Download CSV**（下载 **CSV**）到本地设备。

STEP 8 | 以 CSV 格式 **Export**（导出）所选变量。

CSV 将导出并本地下载到您的设备。导出的 CSV 文件的格式，文件名为：

```
<cloud-management-tenant-name> - Prisma Access_<export-
date>_variables
```


管理：概述

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW，包括由 软件 NGFW 积分提供资助的项目	这些许可证中的每一个都包括 Strata Cloud Manager 访问权限： ❑ Prisma Access ❑ AIOps for NGFW Premium ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → 您可用的特性和功能Strata Cloud Manager取决于您使用的许可证。

将概述页面视为您首次设置 NGFW 和 Prisma Access 以及日常配置管理的启动点（**Manage [管理] > Configuration [配置] > NGFW and Prisma Access [NGFW 和 Prisma Access] > Overview [概览]**）。

- 全局
- Prisma Access
- Strata Cloud Manager

全局

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series, funded with Software NGFW Credits	❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Prisma Access 许可证

如果选择 **Global**（全局）配置范围，则可以查看以下详细信息：

- 您创建的全局文件夹及其变量
- 配置冲突的防火墙
- 防火墙同步状态和防火墙连接状态
- 常规信息
- 配置代码段

- 许可证
- 用于代码段共享的受信任租户
- 配置版本快照

配置概述 (Prisma Access)

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Access 许可证

如果您刚开始使用 Prisma Access：

- **Basics**（基本）检查清单展示如何启动和运行 Prisma Access；完成此处的任务和演练以开始基本设置；然后测试您的环境并构建部署。
- 以下是策略和配置文件夹的工作方式。
- 以下是如何将配置更改推送到 Prisma Access。

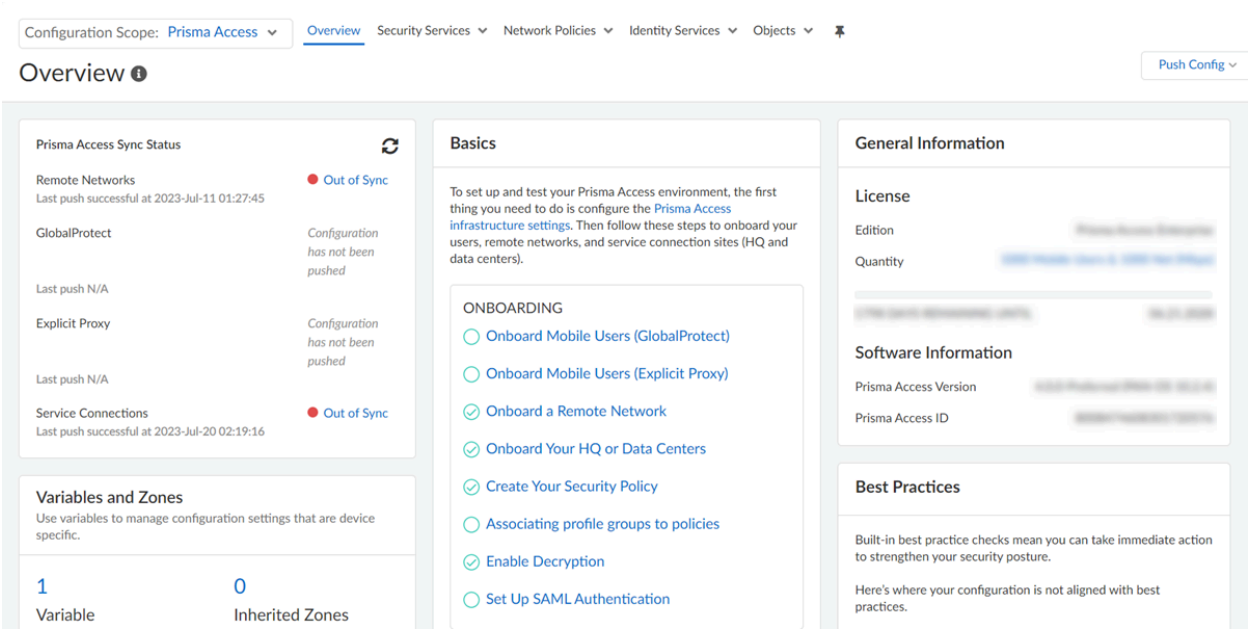
有关 **Prisma Access** 环境的详细信息：

- 查看 **License**（许可证）详细信息，以便了解您的 Prisma Access 订阅包含哪些内容。
- 关于面板显示 Prisma Access 环境的软件和租户信息。

对于日常配置管理：

- 获取配置状态概览
- 使用配置代码段标准化一组 Prisma Access 部署的通用基础配置
- 查找配置快照 - 比较配置版本并恢复（或加载）早期版本，以从对流量或安全产生意外影响的配置推送中恢复
- 通过清理未使用的对象和规则，并通过允许不使用的应用程序来收紧引入安全漏洞的规则，从而优化配置
- 确定您可以进行配置更改以加强安全状况的方面

- Y您还可以找到有关 Prisma Access 许可证及其包含内容的详细信息

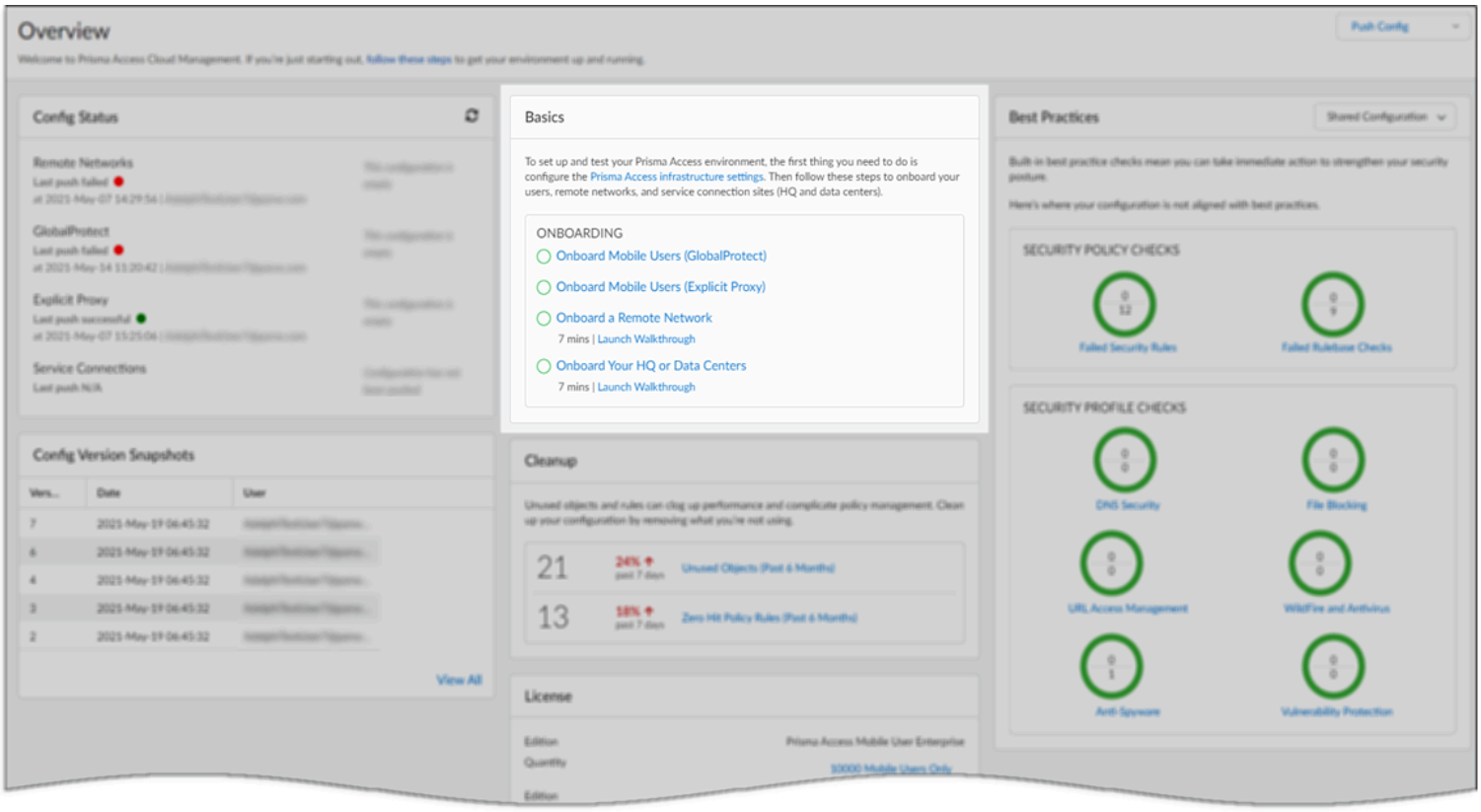


完成基本设置后，您可以开始测试环境并构建部署。

基础知识

Prisma Access 配置**Basics**（基础知识）指导您启动和运行 Prisma Access。完成此处的任务以开始基本设置，然后可以使用该设置测试环境并构建部署。

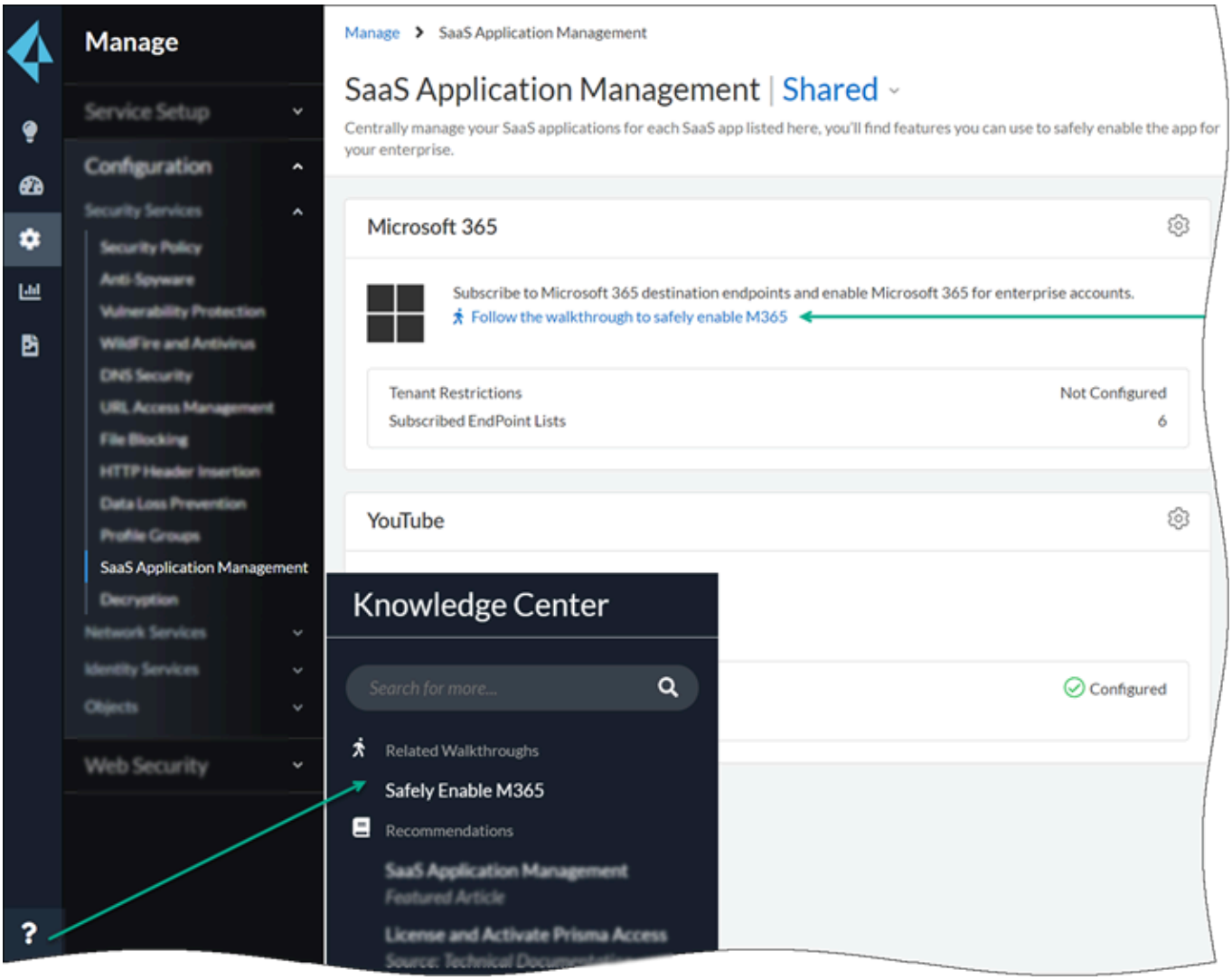
每个任务都将您链接到可以设置相关配置的页面;完成后，此列表中的任务显示为已完成。因此，您可以轻松地跟踪您的进度，如果您处于入职阶段，这尤其有用。

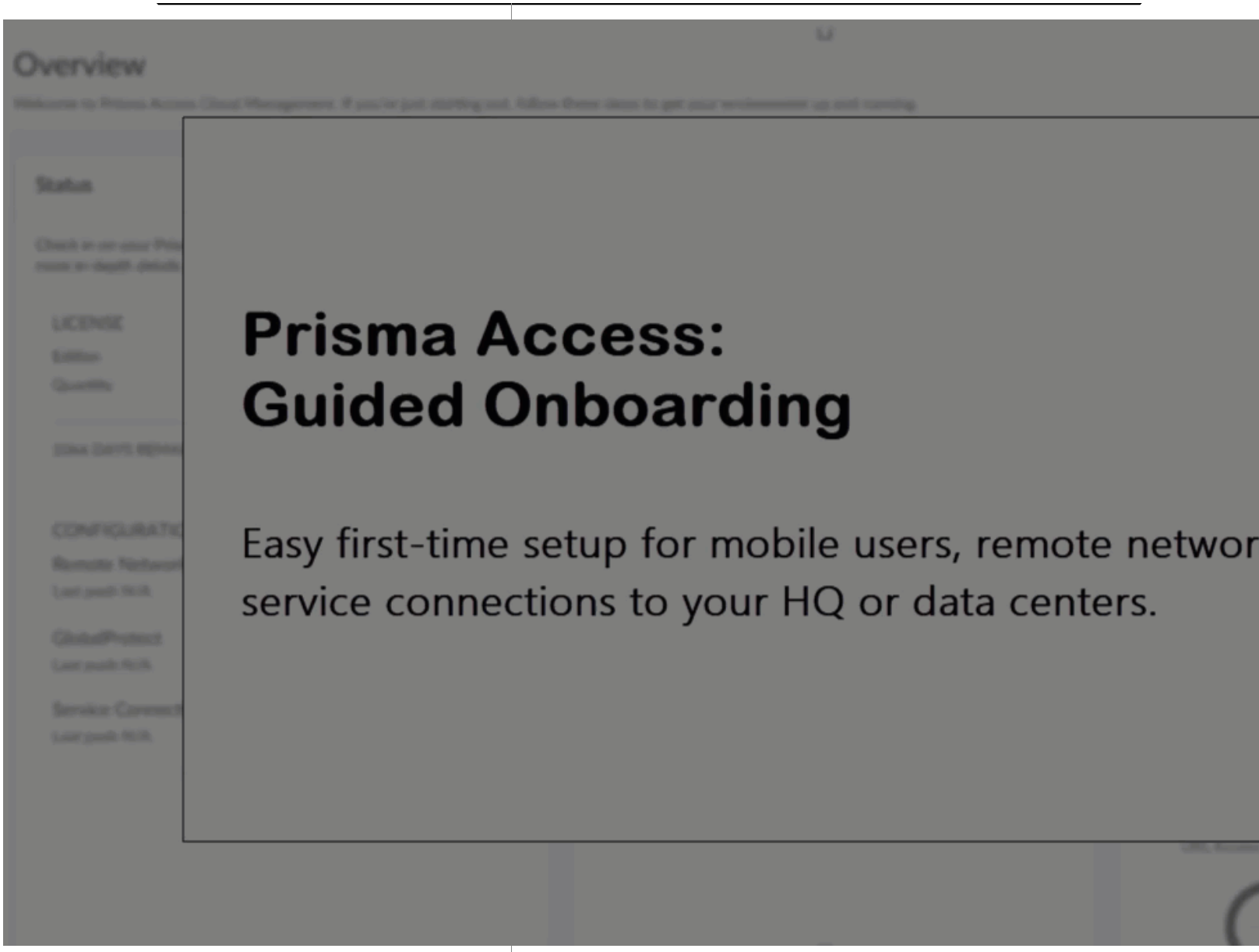


演练

一些待办事项还包括指导您完成启动和运行环境所需的基本步骤的演练。

您可以在 **Overview**（概述）指示板上进行载入演练。您可以单击帮助，查看您所在页面是否有可用的演练，并留意您可以直接在页面上启动的指导：



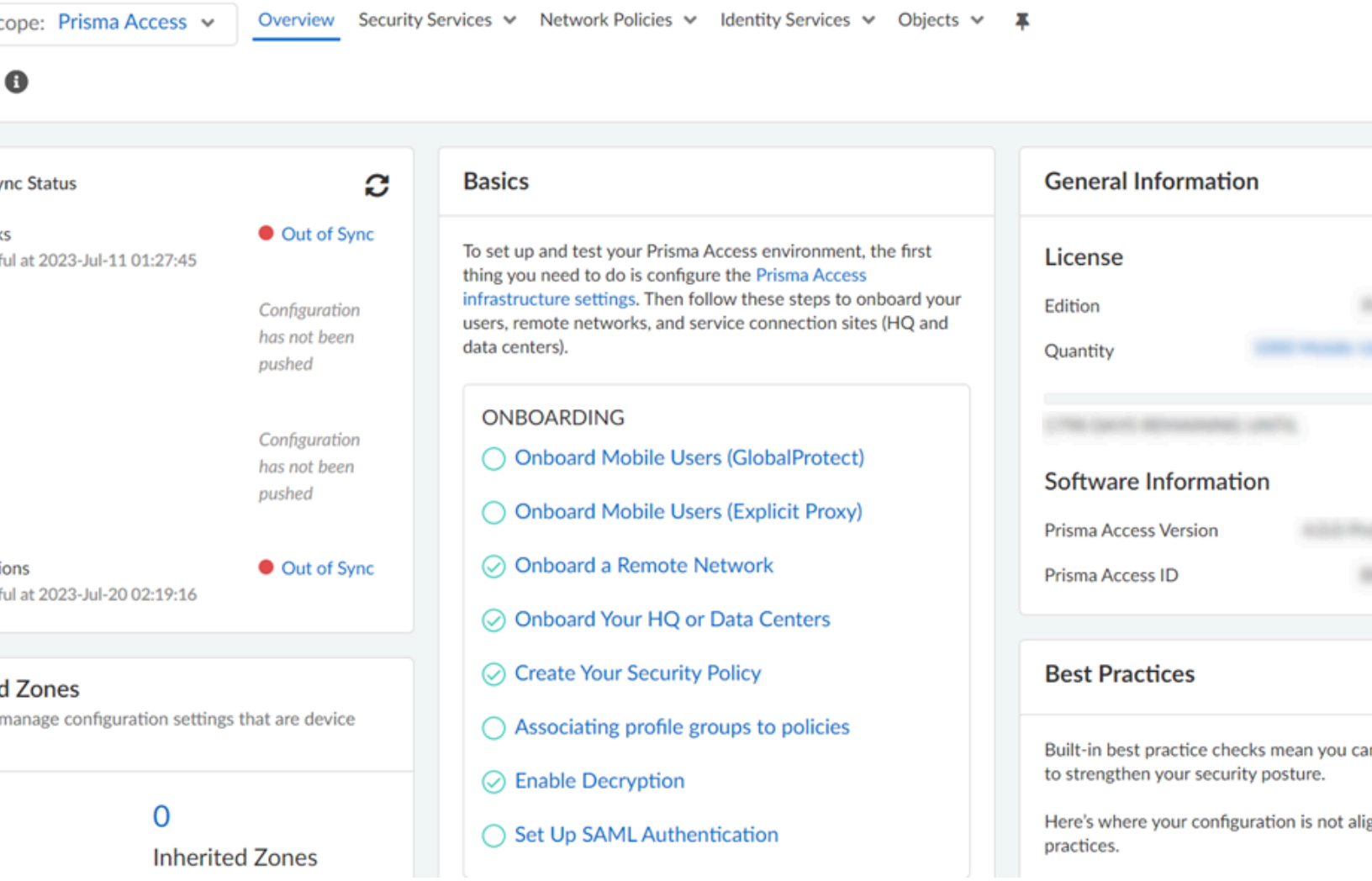


Prisma Access 同步状态

在 **Overview**（概览）页面上，您可以快速检查 Prisma Access 配置的状态。如果您看到意外情况，请深入查看以确定受影响的配置。以下是您可能会看到的状态：

- 尚未推送配置 - 到目前为止，尚未将任何配置推送到 Prisma Access。
- 此配置为空 - 用户将空白配置推送到 Prisma Access。在这种情况下，之前已经有了一个配置，因此推送到 Prisma Access 可能是为了删除该配置。转到 **Push Config**（推送配置） > **Jobs**（作业）以查看最近的更改。
- 不同步 - 用户已将配置推送到 Prisma Access，但出现与推送相关的错误或警告。这可能是一个配置问题，也可能是与推送到 Prisma Access 相关的问题。
- 同步 - 已成功将最新配置推送到 Prisma Access，并且没有错误。

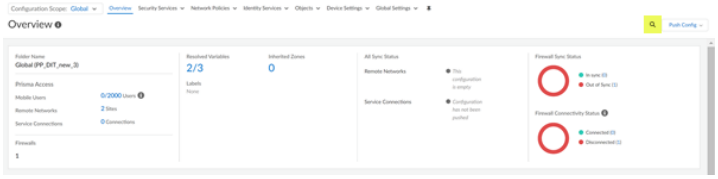
如果您看到意外情况，请单击状态以打开地图视图，其中显示您拥有移动用户（GlobalProtect 或显式代理连接）、远程网络或服务连接的位置。然后，您可以确定需要检查的配置或可能需要进行更新的位置。



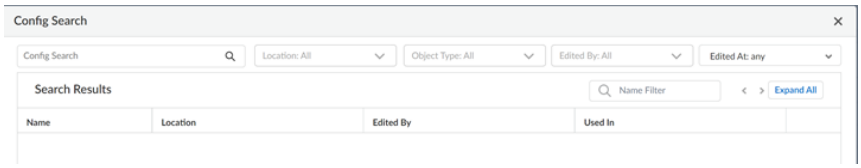
使用配置搜索进行全局查找

配置搜索允许您查找特定字符串的特定配置对象和设置，如IP地址、对象名称、引用对象、重复对象、策略名称、策略规则、特定CVE涵盖的策略、规则 UUID、预定义代码段或应用程序名称，并获取使用该对象的所有引用的列表。

1. 要启动 **Config Search**（配置搜索），请单击 Web 界面右上角 **Push Config**（推送配置）旁的 图标。**Config Search**（配置搜索）在 **Manage**（管理）下的所有页面上可用。



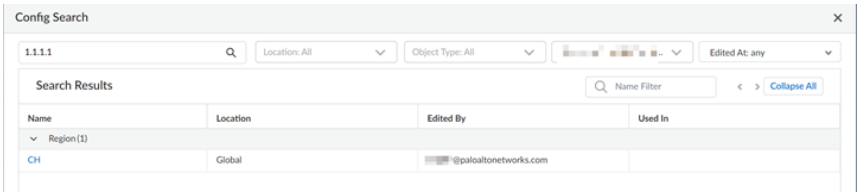
2. 在 **Config Search**（配置搜索）屏幕上，您可以使用 **Config String**（配置字符串）、**Location**（位置）、**Object Type**（对象类型）、**Edited By**（编辑者）或 **Edited At**（编辑位置）字段来进行搜索。



搜索提示：

- 要使用确切的短语进行搜索，请将该短语放在引号中。
- 搜索词条中的空格会当做 AND 运算进行处理。例如，如果您搜索“公司 政策”，则搜索结果会包含配置中存在公司和策略的实例。
- 要取消上一次搜索，请单击 **Config Search**（配置搜索）图标，该图标将显示最近 50 次搜索。单击列表中的项目可重新运行搜索。搜索历史记录列表对每个管理员帐户都是唯一的。
- 配置搜索可用于每个可搜索的字段。例如，您可以在以下对象类型中搜索安全策略：标记、服务区、地址、用户、HIP 配置文件、应用程序、UUID 和服务。
- 位置按名称和代码段分组。您可以选择多个位置进行搜索。如果不选择任何位置，则默认情况下将选择 **All**（所有）位置。
- 如果未选择对象类型，则将选择 **All**（所有）。

3. 搜索结果会进行分类，并提供指向 Strata Cloud Manager 中配置位置的链接，使您可以轻松找到搜索字符串的所有出现位置和引用。



配置概述 (Strata Cloud Manager)

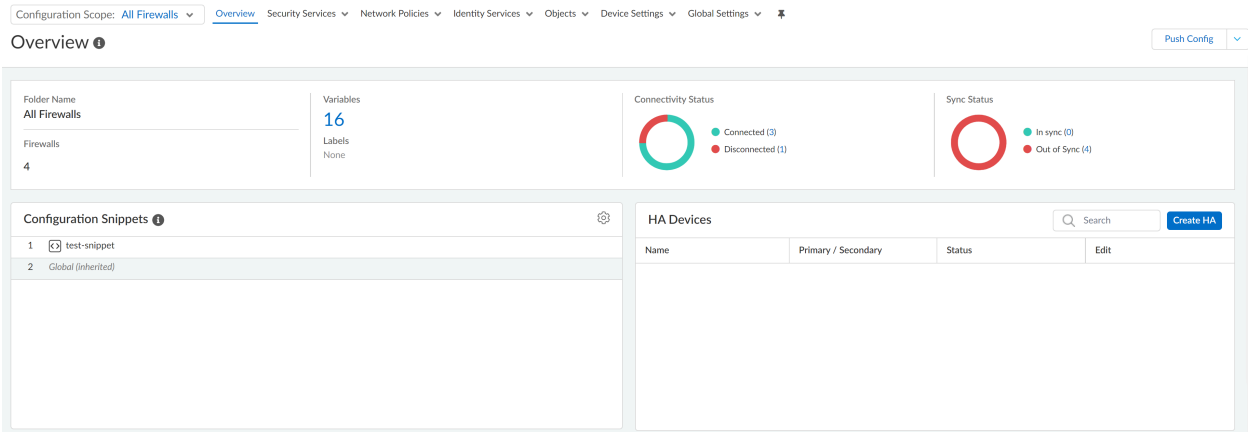
在何处可以使用？	需要提供什么？
• NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series, funded with Software NGFW Credits	❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app)

如果您刚刚开始使用 NGFW 的云管理：

- 以下是策略和配置文件夹的工作方式。
- 下面介绍如何将配置更改推送至防火墙。

对于日常配置管理：

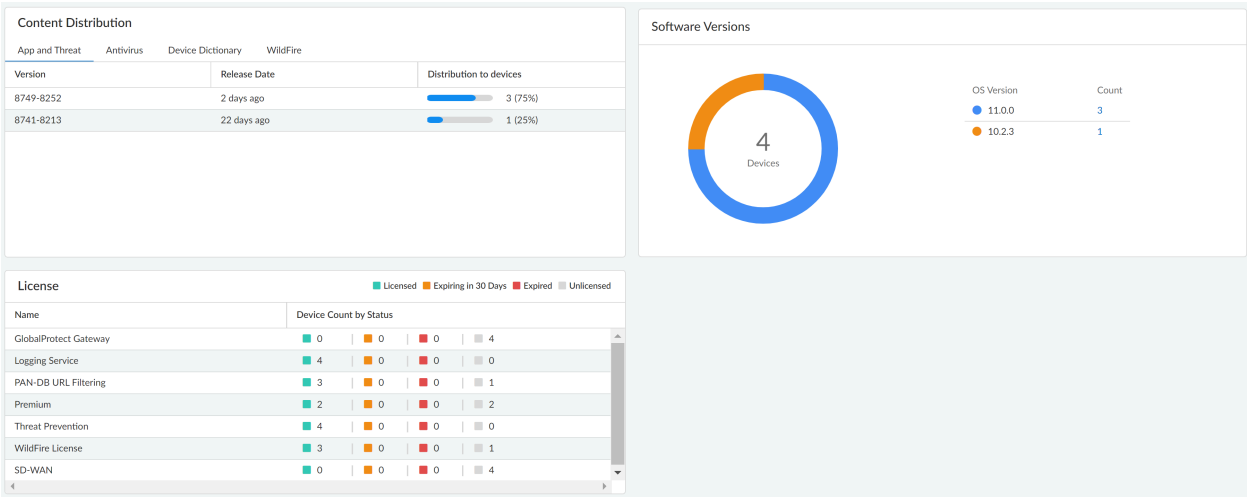
- 一目了然地了解当前文件夹的名称，添加到该文件夹的防火墙的数量，为该文件夹创建的 变量的数量。
- 获得对本地防火墙配置的可见性和控制，而无需在中心管理和单个防火墙之间切换以管理本地配置。
  - **Firewalls with config conflicts**（存在配置冲突的防火墙）显示存在冲突的防火墙数量。单击数字即可查看防火墙冲突及其位置。单击任意防火墙即可查看设备级冲突。
  - **Objects with config conflicts**（具有配置冲突的对象）显示每个防火墙的冲突数量。单击数字可以查看特定防火墙的冲突对象及其类型。单击该对象可以提供有关冲突的详细信息。
- 使用配置代码段来标准化一组托管防火墙的通用基础配置。
- 在高可用性 (HA) 配置中配置托管防火墙，以提供冗余并确保业务连续性。
- 检查管理防火墙的 **Connectivity Status**（连接状态）Strata Cloud Manager。
- 查看配置 Strata Cloud Manager 与您管理的防火墙上当前运行的配置之间的 **Sync Status**（同步状态）。



有关托管防火墙的详细信息：

- 查看内容分发和 **Software Versions**（软件版本）详细信息，了解托管防火墙上正在运行哪些动态内容更新和 PAN-OS 软件版本。

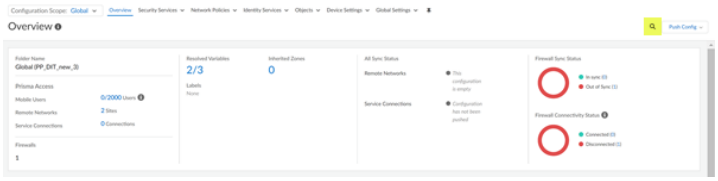
- 查看 **License**（许可证）详细信息，了解您管理的防火墙上激活了哪些许可证。



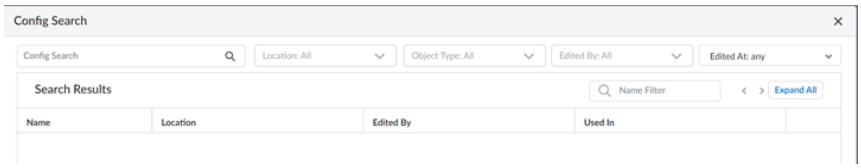
使用配置搜索进行全局查找

配置搜索使您能够搜索特定字符串的配置对象和设置，例如 IP 地址、对象名称、引用的对象、重复的对象、策略名称、策略规则、特定 CVE 涵盖的策略、规则 UUID、预定义代码段或应用程序名称，并获取使用该对象的所有引用的列表。

1. 要启动 **Config Search**（配置搜索），请单击 Web 界面右上角 **Push Config**（推送配置）旁的 图标。**Config Search**（配置搜索）在 **Manage**（管理）下的所有页面上可用。



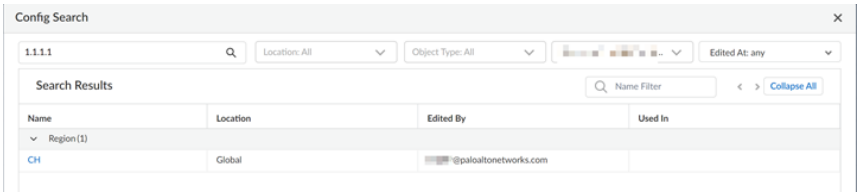
2. 在 **Config Search**（配置搜索）屏幕上，您可以使用 **Config String**（配置字符串）、**Location**（位置）、**Object Type**（对象类型）、**Edited By**（编辑者）或 **Edited At**（编辑位置）字段来进行搜索。



搜索提示：

- 要使用确切的短语进行搜索，请将该短语放在引号中。
- 搜索词条中的空格会当做 AND 运算进行处理。例如，如果您搜索“公司 政策”，则搜索结果会包含配置中存在公司和策略的实例。
- 要重新运行上一次搜索，请单击配置搜索图标，该图标会显示最近 50 次搜索。单击列表中的项目可重新运行搜索。搜索历史记录列表对每个管理员帐户都是唯一的。
- 配置搜索可用于每个可搜索的字段。例如，您可以在以下对象类型中搜索安全策略：标记、服务区、地址、用户、HIP 配置文件、应用程序、UUID 和服务。
- 位置按文件夹和代码段分组。您可以选择多个位置进行搜索。如果不选择任何位置，则默认情况下将选择 **All**（所有）位置。
- 如果未选择对象类型，则将选择 **All**（所有）。

3. 搜索结果会进行分类，并提供指向 Strata Cloud Manager 中配置位置的链接，使您可以轻松找到搜索字符串的所有出现位置和引用。



管理：安全服务

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW，包括由 软件 NGFW 积分提供资助的项目	这些许可证中的每一个都包括 Strata Cloud Manager 访问权限： ❑ Prisma Access ❑ AIOps for NGFW Premium ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → 您可用的特性和功能Strata Cloud Manager取决于您使用的许可证。

管理您的安全服务并保护您的网络、系统和用户。

转到 **Manage**（管理） > **Configuration**（配置） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Security Services**（安全服务）。

通过安全服务，您可以：

- 定义如何使用 管理：安全策略。
- 使用 管理：解密 阻止加密流量中隐藏的威胁。

管理：安全策略

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW，包括由 软件 NGFW 积分提供资助的项目	这些许可证中的每一个都包括 Strata Cloud Manager 访问权限： ❑ Prisma Access ❑ AIOps for NGFW Premium ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → 您可用的特性和功能Strata Cloud Manager取决于您使用的许可证。

在安全策略中，您可以定义在 Prisma Access 和 NGFW 部署中如何强制执行流量。所有通过您的 Strata Cloud Manager 环境的流量都会根据您的安全策略进行评估，并自上而下地应用规则。

要设置安全策略，请转到 **Manage**（管理） > **Configuration**（配置） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Security Services**（安全服务） > **Security Policy**（安全策略）。

安全策略入门

为了使安全策略为您服务，您现在可以采取以下措施。

- 创建安全策略规则 — 安全策略可让您强制实施规则并执行操作，根据需要，它可以是一般性的，也可以是特定的。
- 在规则库中跟踪规则 - 规则库中的每条规则都会自动编号；当您移动或重新排序规则时，数字会根据新顺序而变化。
- 强制执行策略规则最佳实践 - 创建或修改规则时，您可能需要规则描述、标记、审计评论等，以确保正确组织和分组您的策略规则库，并保留重要的规则历史记录以供审计。
- 测试策略规则 — 使用 Policy Analyzer 检查策略规则。
- 激活安全配置文件 — 安全配置文件用于在安全策略允许应用程序或类别后对通信进行扫描。
- 创建安全配置文件组 - 安全配置文件组是一组安全配置文件，可以将其视为一个单元，然后可以轻松地添加到安全策略中。
- 设置文件阻止 - 确定要阻止或监控的特定文件类型。
- 创建数据筛选配置文件 — 防止敏感信息离开您的网络。
- 管理 Web 安全 — 控制对互联网和 SaaS 应用程序的访问权限（常规浏览）。

管理：解密

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW，包括由 软件 NGFW 积分提供资助的项目	这些许可证中的每一个都包括 Strata Cloud Manager 访问权限： ❑ Prisma Access ❑ AIOps for NGFW Premium ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → 您可用的特性和功能Strata Cloud Manager取决于您使用的许可证。

启用解密以阻止隐藏在加密流量中的威胁。您需要做的就是导入解密证书 — 对于其他所有内容，我们内置了最佳实践设置，您可以使用这些设置来启动和运行。

在此处了解有关解密流量的更多信息。

转到 **Manage**（管理） > **Configuration**（配置） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Security Services**（安全服务） > **Decryption**（解密）。

解密概述

安全套接字套 (SSL) 和安全外壳 (SSH) 加密协议是用来保护 Web 服务器和客户端两个实体之间的流量。SSL 和 SSH 封装流量和加密数据，这样使得除客户端和服务器以外的实体使用证书确认设备之间的信任和解密数据的密钥变得毫无意义。解密 SSL 和 SSH 流量，以便：

- 防止作为加密流量隐藏的恶意软件进入您的网络。例如，攻击者破坏使用 SSL 加密的站点。员工访问此站点，并在不知情的情况下下载漏洞或恶意软件。然后，恶意软件使用受感染的员工端点在网络中横向移动，并危害其他系统。
- 防止网络泄露敏感信息。
- 确保在安全网络上运行适当的应用程序。
- 选择性地解密流量；例如，创建解密策略和配置文件，以便从解密中排除金融或运行状况站点的流量。

Strata Cloud Manager 不支持 *SSH* 代理解密。

解密策略

Strata Cloud Manager 提供两种类型的解密策略规则：SSL 转发代理到控制出站 SSL 流量，以及 SSL 入站检查到控制入站 SSL 流量。

SSL 转发代理

配置防火墙以解密前往外部站点的 SSL 流量时，防火墙将充当 SSL 转发代理。使用 SSL 转发代理解密策略进行解密，并检查从内部用户到 Web 的 SSL/TLS 流量。SSL 转发代理解密通过解密流量的方式阻止隐藏为 SSL 加密流量的恶意软件进入您的企业网络，这样，防火墙可以将解密配置文件以及安全策略和配置文件应用于流量。

SSL 入站检查

使用 SSL 入站检查可解密和检查从客户端到目标网络服务器（拥有其证书且可将该证书导入防火墙的任何服务器）之间的入站 SSL/TLS 流量。例如，假设恶意行为者想要利用 Web 服务器中的已知漏洞。入站 SSL/TLS 解密提供对流量的可见性，允许防火墙主动响应威胁。

解密配置文件

可以将解密配置文件附加到策略规则，以便将细粒度访问设置应用于流量，例如，检查服务器证书、不受支持模式和故障。

SSL 转发代理配置文件

对于附加配置文件的转发代理解密策略中定义的 SSL/TLS 出站流量，SSL 转发代理解密配置文件用于控制服务器验证、会话模式检查和失败检查。

SSL 入站检查配置文件

对于附加配置文件的入站检查解密策略中定义的 SSL/TLS 入站流量，SSL 入站检查解密配置文件用于控制会话模式检查和失败检查。

不解密配置文件

没有解密配置文件会对您选择不解密的流量执行服务器验证检查。您可以将“不解密”配置文件附加到“不解密”解密策略（用于定义从解密中排除的流量）。（请勿使用策略来排除不能解密的流量，因为网站可能会因固定证书或策略要求的相互身份验证等技术原因破解解密。相反，应将主机名添加到解密排除列表。）

解密提示

- 首先按照最佳实践策略规则来制定解密策略

  这些规则（一种用于解密流量，另一种将敏感内容排除在解密范围之外）是基于 URL 类别构建的。

- 将敏感内容排除在解密之外

  出于业务、法律或监管原因，将敏感内容排除在解密范围之外。

  - 预定义的解密排除 — Palo Alto Networks 会维护此排除项列表并定期对其进行更新。此列表在全局范围内应用，默认情况下适用于您为解密指定的所有流量。如果符合您的业务需求，您可以禁用列表条目。
  - 自定义排除 — 全局排除网站或应用程序的解密。
  - 基于策略的排除 - 使用 URL 类别和外部动态列表创建有针对性的、基于策略的解密规则。将解密策略规则操作设置为 **no-decrypt**，以便将匹配的流量排除在解密之外。

  务必将解密排除项置于策略规则的顶部，以便首先应用解密排除项。

- 考虑一下，您可以在全球范围内应用某些解密设置，并将其他解密设置定位到特定位置

  - 您的 Strata Cloud Manager 解密策略在全球范围内应用于所有 NGFW 和 Prisma Access 位置。

    管理 > 配置 > **NGFW** 和 **Prisma Access** > 安全服务 > 解密
  - 导航到每种类型的解密策略，创建针对特定防火墙、移动用户位置、远程网络站点或服务连接的策略规则

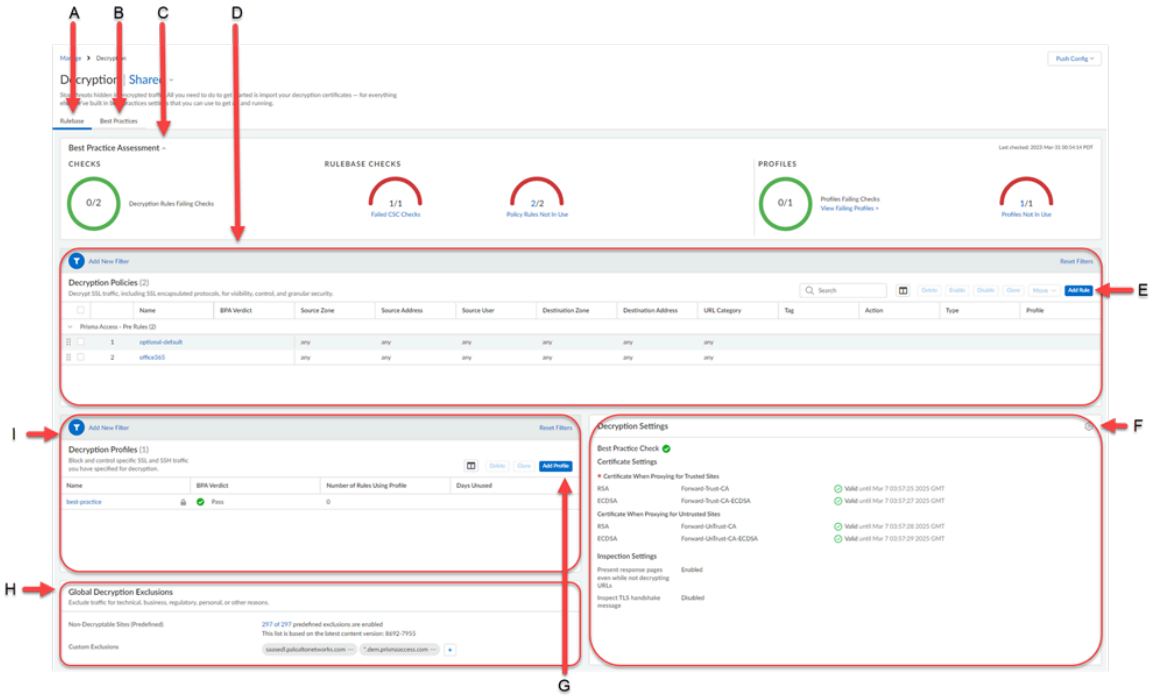
    管理 > 配置 > **NGFW** 和 **Prisma Access** > 配置范围 > 全球/防火墙/移动用户/远程网络/服务连接

- 规则顺序很重要

  解密策略规则是自上而下应用的。首先将要强制执行的规则放在解密策略规则列表的顶部。全局规则（预规则）首先应用，并且始终在特定于移动用户、远程网络和服务连接的规则之前列出。

解密一览

解密屏幕是配置解密策略和配置文件以及查看最佳实践评估的位置。



A) 规则库 — 规则库检查如何组织和管理安全策略，包括适用于许多规则的配置设置。

B) 最佳实践 — 这里可以全面了解您的功能实现如何与最佳实践保持一致。检查失败的检查，看看可以在哪些地方进行改进（您也可以查看通过的检查）。

C) 最佳实践评估 — 最佳实践分数显示在解密指示板上。这些分数使您可以快速了解最佳实践的进展。您只需一眼便能确定需要进一步调查的区域或想要采取行动来改善安全态势的区域。

D) 解密策略 — 已载入的解密策略列表。查看策略配置、策略类型（*SSL* 转发代理、*SSL* 入站检查或 *SSH* 代理）、策略操作（解密或不解密）和 BPA 判定。

E) 添加规则 — 添加和配置新的解密策略。

F) 解密设置 — 访问证书和解密设置。导入和导出证书。

G) 添加配置文件 — 添加和配置新的解密配置文件。

H) 全局解密排除 — 应用程序不在解密范围内。

I) 解密配置文件 — 已载入的解密配置文件列表。查看配置文件配置、使用配置文件的策略以及 BPA 判定。

管理：网络策略

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW，包括由 软件 NGFW 积分提供资助的项目	这些许可证中的每一个都包括 Strata Cloud Manager 访问权限： ❑ Prisma Access ❑ AIOps for NGFW Premium ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → 您可用的特性和功能Strata Cloud Manager取决于您使用的许可证。

您可以创建各种类型的网络策略来保护您的网络免受威胁和中断。它可帮助您优化网络资源分配并管理网络策略，以确定流量的优先级并配置应用程序分类。

规则是从上到下评估的，当流量与定义的规则标准匹配时，后续规则不会被评估。您应该将更具体的策略规则置于更一般的规则之上，以强制执行可能的最佳匹配条件。当为策略规则启用日志记录时，将为与该规则匹配的通信生成日志。每个规则的日志记录选项都是可配置的。

最佳实践策略规则适用于大多数策略类型，可帮助您快速安全地开始使用。虽然无法编辑这些规则以确保您始终拥有最低级别的安全性，但如果您希望将其用作自定义策略的基础，则可以克隆它们。

转到 **Manage**（管理） > **Configuration**（配置） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Network Policies**（网络策略）。

使用网络策略，您可以：

- 优先考虑对您的 管理：QoS 运营最重要的流量。
- 按照管理：应用程序替代管理 Prisma Access 如何对应用程序进行分类。

管理：QoS

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama or Strata Cloud Manager)	以下之一： ❑ Prisma Access 许可证 ❑ Strata Cloud Manager Pro → 您可用的特性和功能Strata Cloud Manager取决于您使用的许可证。

通过服务质量 (QoS)，您可以优先处理需要低延迟的关键业务流量和应用程序（如 VoIP 和视频应用程序）。要添加或编辑 QoS 策略规则，请转到 **Manage**（管理） > **Configuration**（配置） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Network Policies**（网络策略） > **QoS**。

QoS 策略规则

服务质量 (QoS) 策略规则，用于识别需要优先处理或带宽限制的流量。QoS 规则允许您在有限的网络容量下独立运行高优先级应用程序和流量。您可以使用区分服务代码点 (DSCP) 配置流量 QoS 处理。这些码点是分组报头值，其可用于请求（例如）高优先级或业务的尽力交付。Prisma Access 对传入流量强制执行 DSCP 值，并在会话流量退出防火墙时使用 DSCP 值标记会话。这意味着会话的所有入站和出站流量都将接受连续的 QoS 处理。您可以使用以下代码点配置流量QoS处理：

- 转发 **(EF)** — 可用于为流量请求低丢失率、低延迟并保证带宽。

  通常保证带有 EF 代码点值的数据包获得最高分发优先级。
- 转发 **(AF)** — 可用于为应用程序提供可靠传送。

  具有 AF 代码点的分组指示请求业务接收比尽力服务提供的更高优先级的处理。具有 EF 代码点的数据包优先于具有 AF 代码点的数据包。
- 选择器 **(CS)** — 可用于为使用 IP 优先级字段标记优先流量的网络 IP 地址设备提供向后兼容性。
- **IP** 优先级 **(ToS)** — 由传统网络IP地址用于标记优先级流量。
- 自定义代码点 — 通过输入代码点名称和二进制值来创建自定义代码点，以匹配流量。

  例如，您可以创建 QoS 策略规则来确定语音通信（如IP语音 (VOIP)）的优先级，以确保数据包传输的一致性。这确保了语音通信的一致性。

管理：应用程序替代

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW，包括由 软件 NGFW 积分提供资助的项目	这些许可证中的每一个都包括 Strata Cloud Manager 访问权限： ❑ Prisma Access ❑ AIOps for NGFW Premium ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → 您可用的特性和功能Strata Cloud Manager取决于您使用的许可证。

创建应用程序覆盖策略，指定使用快速路径第 4 层检查来处理应用程序，而不是使用 App-ID 进行第 7 层检查。这会强制安全执行节点将会话作为常规状态检查来处理，并节省应用程序处理时间。当您不想对已知 IP 地址之间的自定义应用程序进行流量检查时，可以创建应用程序覆盖策略规则。例如，如果您在非标准端口上有一个自定义应用程序，并且您知道访问该应用程序的用户受

到批准，并且两者都位于信任服务区，则您可以覆盖访问自定义应用程序的受信任用户的应用程序检查要求。

要更改 Prisma Access 对应用程序进行分类的方式，请转到 **Manage**（管理） > **Configuration**（配置） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Network Policies**（网络策略） > **Application Override**（应用程序覆盖），然后创建应用程序覆盖策略规则。

应用程序替代提示

考虑一下，当您创建应用程序覆盖策略规则时，您会限制 App-ID 对部署的流量进行分类并根据该应用程序标识执行威胁检查。为了支持内部专有应用程序，可以考虑创建包含应用程序签名的自定义应用程序（而不是应用程序覆盖规则），以便 Strata Cloud Manager 执行第 7 层检查并扫描应用程序流量中是否存在威胁。要创建自定义应用程序，请转到 **Manage**（管理） > **Configuration**（配置） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Objects**（对象） > **Applications**（应用程序）。

应用程序覆盖策略

使用下面的部分配置应用程序替代规则：

- 来源
  - 服务区 — 添加源服务区。
  - 地址 — 添加源地址、地址组或区域并指定设置。
- 目的地
  - 服务区 — 添加以选择目的地服务区。
  - 地址 — 添加源地址、地址组或区域并指定设置。
- 应用程序
  - 应用程序 — 为匹配上述规则条件的通信流选择替代应用程序。替代为自定义应用程序时，不会执行任何威胁检查。但替代为支持威胁检查的预定义应用程序时除外。

    要定义新的应用程序，请转到 **Manage**（管理） > **Configuration**（配置） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Objects**（对象） > **Applications**（应用程序）。
-
  - — 选择允许应用程序覆盖的协议（**TCP** 或 **UDP**）。
  - 端口 — 输入指定目标地址的端口号（0 - 65535）或端口号范围（端口 1 - 端口 2）。多个端口或范围必须以英文逗号分隔。

管理：基于策略的转发

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW，包括由 软件 NGFW 积分提供资助的项目	这些许可证中的每一个都包括 Strata Cloud Manager 访问权限： □ Prisma Access □ AIOps for NGFW Premium

在何处可以使用？	需要提供什么？
	❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → 您可用的特性和功能Strata Cloud Manager取决于您使用的许可证。

基于策略的转发规则可让流量从路由表中指定的下一个跃点采用备选路径，并且通常因为安全或性能的原因而用于指定传出接口。

转到 **Manage**（管理） > **Configuration**（配置） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Network Policies**（网络策略） > **Policy Based Forwarding**（基于策略的转发）。

使用基于策略的转发规则将流量引导至防火墙上的特定传出接口，并覆盖流量的默认路径。在创建基于策略的转发规则之前，您务必要了解 IPv4 地址集将被视为 IPv6 地址集的子集。

使用以下部分配置基于策略的转发规则：

- 来源
  - 服务区 — 添加源服务区。
  - 接口 — 添加源接口。
  - 地址 — 添加源地址、地址组或区域并指定设置。
  - 用户 — 添加适用该策略的用户和用户组。
- 目标
  - 地址 — 添加源地址、地址组或区域并指定设置。
- **Application and Services**（应用程序和服务）
  - **Application Entities**（应用程序条目）— 选择您希望通过备选路径路由的应用程序。

    在防火墙拥有足够的信息来确定应用程序之前，可应用基于策略的转发规则。因此，不建议将特定于应用程序的规则与基于策略的转发一起使用。只要有可能，就应使用服务对象。

    您不能在基于策略的转发规则中使用自定义应用程序、应用程序筛选器或应用程序组。
  - **Service Entities**（服务条目）— 选择您希望通过备选路径路由的服务和服务组。

- 转发
  - 操作 — 您可以通过选择以下选项来设置匹配数据包时要采取的操作：
    - 转发 — 将数据包转发至指定的传出接口。
    - 丢弃 — 丢弃数据包。
    - **PBF** — 排除与规则中定义的源、目标、应用程序或服务的条件相符的数据包。匹配的数据包使用路由表而不是 PBF。
  - 接口 — 选择您想要转发与基于策略的转发规则匹配的流量的网络信息。
  - **Next Hop**（下一个跃点）
    - **IP** 地址 — 输入要将匹配的数据包转发到的 IP 地址，或选择 IP 子网掩码类型的地址对象。
    - **FQDN** — 输入一个防火墙向其转发匹配数据包的 FQDN（或者选择或创建一个 FQDN 类型地址对象）。
    - 无 — 没有下一个跃点表明数据包的目标 IP 地址被用作下一个跃点。如果目标 IP 地址与传出接口不在同一个子网中，则转发失败。
  - 监视 — 如果未指定 IP 地址，则启用监控来验证对于目标 IP 地址或下一个跃点 IP 地址的连接性。

管理：NAT

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW，包括由 软件 NGFW 积分提供资助的项目	这些许可证中的每一个都包括 Strata Cloud Manager 访问权限： ❑ Prisma Access ❑ AIOps for NGFW Premium ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → 您可用的特性和功能Strata Cloud Manager取决于您使用的许可证。

NAT 可将私有的不可路由 IPv4 地址转换为一个或多个全球可路由 IPv4 地址，从而节省组织的可路由 IP 地址。NAT 还可用于保密需要访问公共地址的主机的真实 IP 地址，并通过执行端口转发来管理流量。可以使用 NAT 解决网络社交挑战，使用相同的 IP 子网启用网络，从而进行相互通信。

您至少可以配置 NAT 策略规则以匹配数据包的源服务区和目标服务区。除了服务区之外，您还可以根据数据包的目标接口、源和目标地址以及服务来配置匹配条件。您可以配置多个 NAT 规则。

转到 **Manage**（管理） > **Configuration**（配置） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Network Services**（网络服务） > **NAT**。

排除连通性问题 – 获得路由和隧道状态的汇总视图，并深入到具体细节以查找异常和有问题的配置。

管理：SD-WAN

在何处可以使用？	需要提供什么？
• SD-WAN	❑ 软件定义广域网许可证

SD-WAN 策略规则指定应用程序和/或服务以及流量分发配置文件，以确定防火墙如何为不属于现有会话、且符合所有其他标准（例如，源和目标服务区、源和目标 IP 地址、以及源用户等）的传入数据包选择首选路径。SD-WAN 策略规则还可指定用于延迟、抖动和数据包丢失阈值的路径质量配置文件。一旦超过其中一个阈值，防火墙将为应用程序和/或服务检测一条新路径。

要配置 SD-WAN 策略，请选择 **Manage**（管理） > **Configuration**（配置） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Network Policies**（网络策略） > **SD-WAN**。

规则

您可以在共享上下文中定义预处理规则和后处理规则作为适用于所有受管防火墙的共享策略，或在设备组上下文中使其特定于某个设备组。

- 预处理规则 — 在进行评估前添加到规则序列顶部的规则。您可以使用预处理规则来强制执行组织的可接受使用策略。例如，您可以阻止所有用户访问特定 URL 类别，或者允许所有用户访问 DNS 流量。
- 后处理规则 — 在使用预处理规则进行评估后添加到规则序列底部且在防火墙本地进行定义的规则。后继规则通常包括根据 **App-ID™**、**User-ID™** 或服务而拒绝访问流量的规则。

配置文件

创建可应用至 SD-WAN 策略规则中指定应用程序和服务集的配置文件。

路径质量

SD-WAN 允许您为具有独特网络质量要求的每组应用程序、应用程序筛选器、应用程序组、服务、服务对象和服务组对象创建路径质量配置文件，然后在 SD-WAN 策略规则中引用该配置文件。在配置文件中，为三个参数设置了最大阈值：延迟、抖动和数据包丢失。若 SD-WAN 链路超过任何一个阈值，则防火墙会为与应用了此配置文件的 SD-WAN 规则匹配的数据包选择一个新的最佳路径。

SaaS 质量

您可以通过 SD-WAN 创建软件即服务 (SaaS) 质量配置文件，以测量中心或分支防火墙与服务器侧 SaaS 应用程序之间的路径运行状况质量，从而准确地监视 SaaS 应用程序的可靠性，并在路径运行状况质量下降时更换路径。这样，防火墙可准确确定将故障转移到其他互联网直接接入 (DIA) 链路的时间。

通过 SaaS 质量配置文件，您可以使用用于监视应用程序活动的自适应学习算法指定要监视的 SaaS 应用程序，或是通过使用应用程序 IP 地址、FQDN 或 URL 指定 SaaS 应用程序。

流量分发

对于此流量分发配置文件，选择防火墙用于分发会话并在路径质量降低时故障转移到更好的路径的方法。添加防火墙在确定其用于转发 SD-WAN 流量的链路时会考虑的链路标签。将流量分发配置文件应用于所创建的每个 SD-WAN 策略规则。

纠错

如果您的 SD-WAN 流量包含对数据包丢失或损坏敏感的应用程序（例如，音频、VoIP 或视频会议），您可以将前向纠错 (FEC) 或数据包重复用作纠错方式。通过 FEC，接收防火墙（解码器）可通过部署编码器嵌入到应用程序流中奇偶校验位来恢复丢失或损坏的数据包。数据包重复是另一种纠错方式，在这种方式中，应用程序会话从一个隧道复制到第二个隧道。要使用其中一种方法，请创建纠错配置文件，并在 SD-WAN 策略规则中将其引用至特定应用程序。

（此外，您还必须通过在 SD-WAN 接口配置文件中指示接口为“纠错配置文件接口的选择条件”的方式，指定防火墙选择用于纠错的接口。）

SD-WAN 接口

创建 SD-WAN 接口配置文件，以定义 ISP 连接特征，指定链路速度以及防火墙监控链路的频率，并指定用于此链路的链路标记。一旦为多个链路指定相同的链路标记后，就可以将这些物理链路分组（捆绑）到链路包或粗管中。必须先配置 SD-WAN 接口配置文件，并将其指定用于启用了 SD-WAN 功能的以太网接口，然后才能保存以太网接口。

链路标签

创建一个链路标记，以标识在 SD-WAN 流量分发和故障转移保护期间，让应用程序和服务以特定顺序使用的一个或多个物理链路。在物理链路运行状况出现问题时，通过对多个物理链路的分组，您可以提高应用程序和服务的质量。

在计划链路分组方式时，请考虑链路的使用或用途，然后对其进行相应地分组。例如，如果配置的链路专用于低成本或非业务关键型流量，请创建链路标记，并对这些接口进行分组，确保预期流量主要在这些链路上流动，而不是在可能会影响关键业务应用程序或服务的昂贵链路上流动。

管理：身份服务

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW，包括由 软件 NGFW 积分提供资助的项目	这些许可证中的每一个都包括 Strata Cloud Manager 访问权限： ❑ Prisma Access ❑ AIOps for NGFW Premium ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → 您可用的特性和功能Strata Cloud Manager取决于您使用的许可证。

了解如何管理您的身份服务并确认只有某些用户可以访问您网络上的正确数据。

转到 **Manage**（管理） > **Configuration**（配置） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Identity Services**（身份服务）。

利用身份服务，您可以：

- 通过将 Prisma Access 连接到您的身份提供商 (IdP)，并选择要使用的身份验证方法，仅允许合法用户访问您的网络。管理：身份验证。
- 使用以下方式授予 Prisma Access 对 Active Directory 信息的只读访问权限：管理：云身份引擎。
- 一致地执行您的安全策略，并与远程网络站点或管理：身份重新分配服务连接站点（总部和数据中心）的本地设备共享身份数据。

管理：身份验证

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW，包括由 软件 NGFW 积分提供资助的项目	这些许可证中的每一个都包括 Strata Cloud Manager 访问权限： ❑ Prisma Access ❑ AIOps for NGFW Premium ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → 您可用的特性和功能Strata Cloud Manager取决于您使用的许可证。

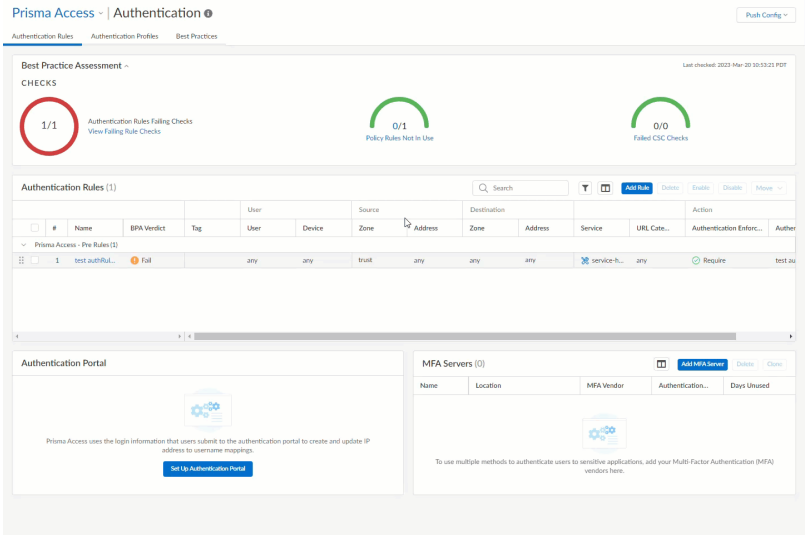
为了确保只有合法用户才能访问您最受保护的资源，Prisma Access 支持多种身份验证类型，包括对 SAML、TACACS+、RADIUS、LDAP、Kerberos、MFA、本地数据库身份验证和 SSO 的支持。

要设置身份验证策略，请转到 **Manage**（管理） > **Configuration**（配置） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Identity Services**（身份服务） > **Authentication**（身份验证）。

以下是 Prisma Access 集成以提供身份验证的服务，以及在规划身份验证设置时需要考虑的功能：

身份验证支持

SAML	如果您的用户访问网络外部的服务和应用程序，则可以使用 SAML，将 Prisma Access 与控制外部和内部服务以及应用程序访问的标识提供商 (IdP) 集成。SAML 单点登录 (SSO) 支持一次登录访问多个应用程序，当每个用户需要访问多个应用程序，并且要为每个应用程序进行身份验证时，用户的工作效率会受到影响，在这样的环境中，单点登录非常有用。在这种情况下，SAML 单点登录 (SSO) 允许一次登录访问多个应用程序。同样，SAML 单点退出 (SLO) 使用户能够通过退出一个会话来结束多个应用程序的会话。SSO 适用于通过 GlobalProtect 应用程序访问应用程序的移动用户或通过身份验证门户访问应用程序的远程网络用户。GlobalProtect 应用程序用户可以使用 SLO。 您不能在身份验证序列中使用 *SAML* 身份验证配置文件。
TACACS+	增强型终端访问控制器访问控制系统 (TACACS+) 是一组通过集中式服务器进行身份验证和授权的协议。TACACS+ 加密用户名和密码，比仅加密密码的 RADIUS 更安全。因使用 TCP，TACACS+ 也更可靠，而 RADIUS 则使用 UDP。
RADIUS	远程身份验证拨入用户服务 (RADIUS) 是一种广受支持的网络协议，提供集中式身份验证和授权。您还可以向 Prisma Access 添加 RADIUS 服务器来实现多因素身份验证。
LDAP	轻型目录访问协议 (LDAP) 是用于访问信息目录的标准协议。您可以使用 LDAP 对通过身份验证门户访问应用程序或服务的用户进行身份验证。
Kerberos	Kerberos 是一种身份验证协议，它使用唯一密钥（称为票证）来识别各方，从而实现各方之间的安全信息交换。使用 Kerberos，您可以通过身份验证门户对访问应用程序的用户进行身份验证。启用 Kerberos SSO 后，仅初次访问网络需要用户登录（例如登录到 Microsoft Windows）。首次登录后，用户可以访问网络中任何基于浏览器的服务，而无需在 SSO 会话到期之前再次登录。

	要使用 Kerberos，您首先需要一个用于对用户进行身份验证的 Prisma Access 的 Kerberos 帐户。该帐户需要创建 Kerberos Keytab，即包含防火墙或 Panorama 的主体名及哈希密码的文件。SSO 进程需要 keytab。 Kerberos SSO 仅适用于 Kerberos 环境内部的服务和应用程序。要使 SSO 用于外部服务和应用程序，请使用 SAML。
云身份引擎	云身份引擎 (CIE) 为 Prisma Access（Explicit Proxy 部署）中的移动用户提供用户识别和用户身份验证。云身份引擎与显式代理身份验证缓存服务 (ACS) 集成，并使用 SAML 身份提供商 (IdP) 为显式代理移动用户提供身份验证。
MFA	多因素身份验证 (MFA) 提供了一种实施不同类型的多种身份验证质询（称为因素）的方法，以保护您最敏感的服务和应用程序。例如，您可能需要对关键财务文档而不是搜索引擎进行严格的身份验证。 Prisma Access 具有内置的受支持的 MFA 供应商列表，该列表会随着新供应商的添加而自动更新： 
本地数据库身份验证	创建一个在 Prisma Access 上本地运行并包含用户帐户（用户名和密码或散列密码）的数据库。在您只知道哈希密码（而不是明文密码）的情况下，此类身份验证对于创建重用现有 Unix 帐户凭据的用户帐户非常有用。对于使用明文密码的帐户，您也可以定义密码复杂度和过期设置。此身份验证方法适用于通过身份验证门户或 GlobalProtect 应用程序访问服务和应用程序的用户。

身份验证功能优势

SSO	如果您使用 SAML 或 Kerberos，则可以实现单点登录 (SSO)，这使得用户只需进行一次身份验证即可访问多个服务和应用程序。SAML 和 Kerberos 支持 SSO。
身份验证门户	将符合身份验证规则的 Web 请求重定向到 Prisma Access 登录页面，并提示他们进行身份验证。Prisma Access 使用用户提交给此身份验证门户的信息来创建或更新 IP 地址到用户名的映射。 这对于远程网络特别有用，这样您就可以继续根据用户（或组）监控和强制执行流量。当用户发起与身份验证规则匹配的 Web 流量（HTTP 或 HTTPS）时，Prisma Access 会提示用户通过身份验证门户进行身份验证。Prisma Access 根据用户提交给门户的信息创建或更新 IP 地址到用户名的映射。这可以确保您确切地知道远程网络站点上谁正在访问您最敏感的应用程序和数据。
身份验证序列	如果您出于不同目的使用多种类型的身份验证，则可以设置身份验证序列来对您的配置文件进行排名。Prisma Access 根据您的排名检查每个个人资料，直到成功验证用户身份。

身份验证的工作原理

将组织的身份验证服务添加到 Prisma Access 后（操作方法），Prisma Access 会在多个点对用户进行身份验证：

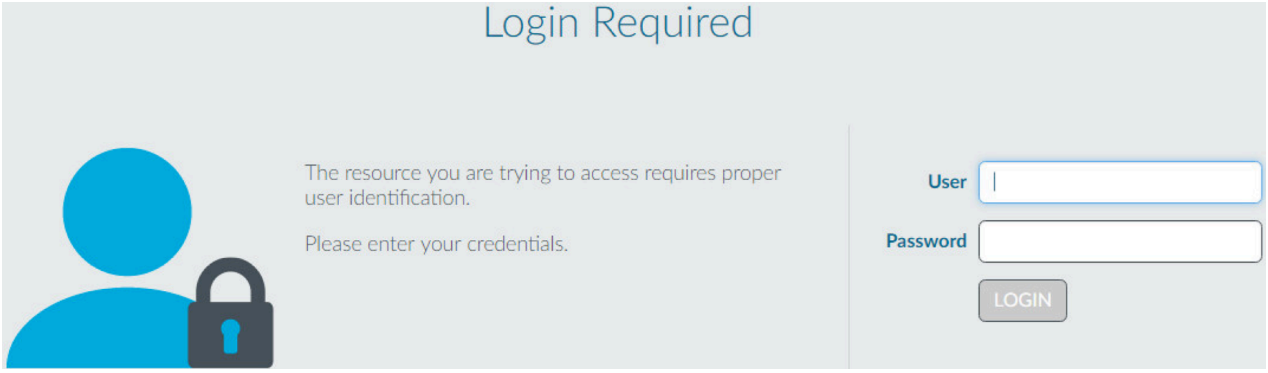
- 当他们连接到 **Prisma Access** 时

  有关您希望移动用户向 Prisma Access 进行身份验证的方法，请参阅https://docs.paloaltonetworks.com/prisma-access/administration/prisma-access-mobile-users/enable-mobile-users-to-authenticate-to-prisma-access。您不需要为远程网络上的用户定义身份验证设置来连接到 Prisma Access，因为远程网络流量是通过安全的 VPN 隧道路由的。

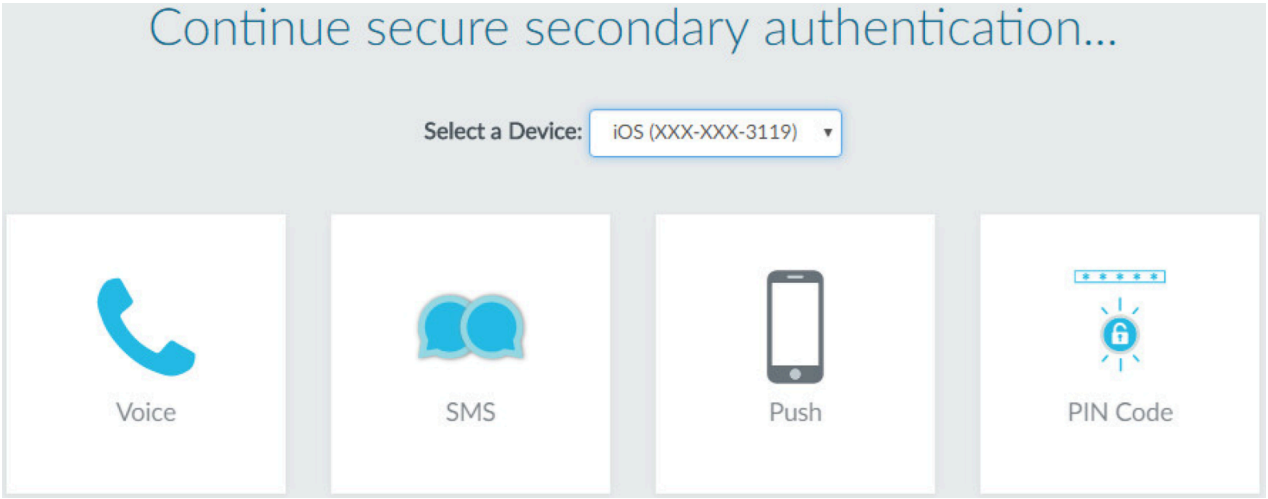
- 当用户流量满足附加身份验证的要求时

  有关如何要求用户进行身份验证（使用一种或多种方法）来访问企业应用程序和受保护的网络资源，请参阅此处。

当用户产生的网络流量符合您的身份验证要求时，Prisma Access 会通过提示用户使用一种或多种方法（因素）进行身份验证来检查用户是否合法，例如登录名和密码、语音、短信、推送或一次性密码 (OTP) 身份验证 - Prisma Access 使用的因素全部基于您在身份验证配置文件中指定的身份验证服务和设置。对于第一个因素（登录名和密码），用户通过身份验证门户进行身份验证。



对于其他因素，用户随后通过多因素身份验证登录页面进行身份验证。



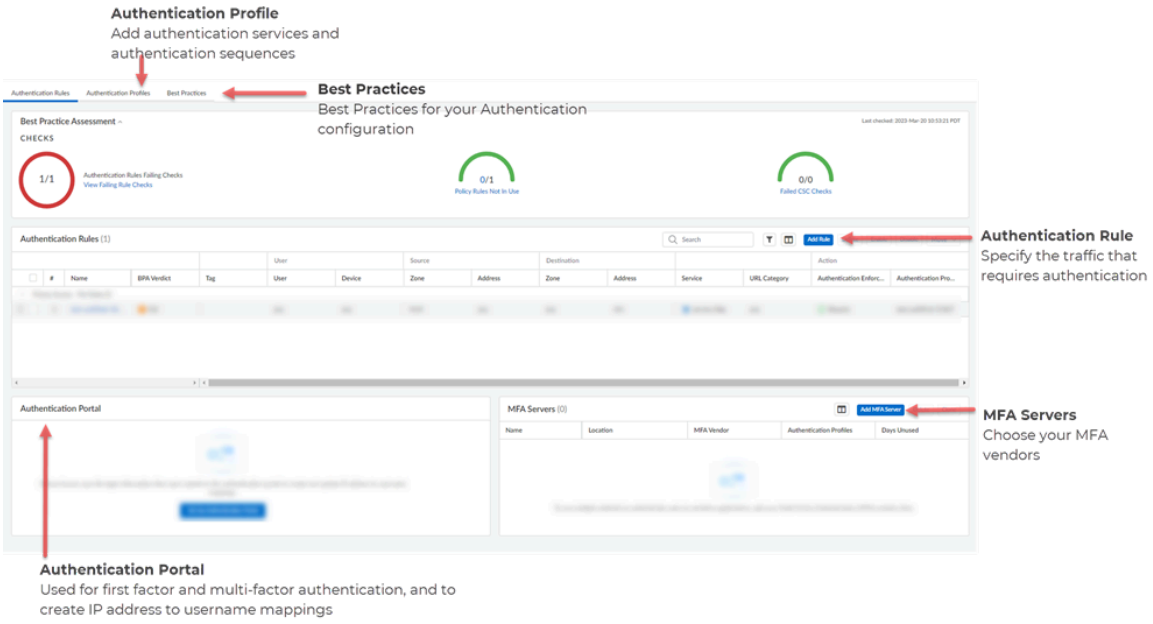
在对用户进行身份验证后，Prisma Access 会评估您的安全规则以确定是否允许访问该应用程序。Prisma Access 记录用户尝试访问您指定为安全访问的应用程序、服务或资源的所有活动。

管理：身份验证设置

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama or Strata Cloud Manager)	以下之一： ❑ Prisma Access 许可证 ❑ Strata Cloud Manager Pro → 您可用的特性和功能Strata Cloud Manager取决于您使用的许可证。

要在 Strata Cloud Manager 中使用 Prisma Access 设置身份验证，请先将身份验证服务添加到 Prisma Access。然后指定需要身份验证的流量。基于这些设置添加更多身份验证功能，如 MFA、身份验证序列，或启用 Prisma Access 以创建和更新用户名映射的 IP 地址。

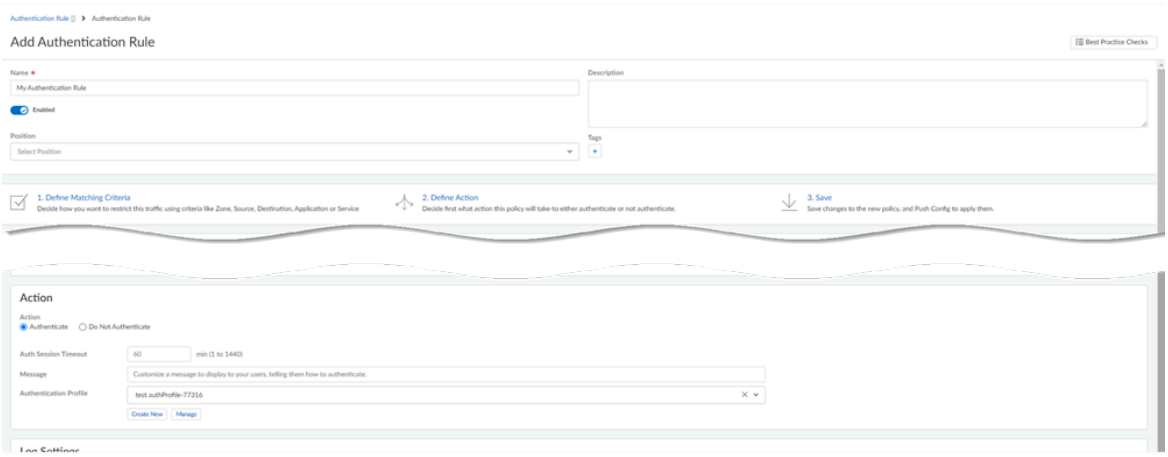
下面介绍如何开始 — 使用 Prisma Access 启用身份验证所需的所有设置都在一个位置：**Manage**（管理） > **Identity Services**（身份服务） > **Authentication**（身份验证）。



身份验证规则 此处指定需要进行身份验证的流量

设置身份验证规则的一部分包括向规则中添加身份验证配置文件。Prisma Access 检测到与身份验证规则匹配的流量时，会将身份验证配置文件中定义的身份验证方法和设置应用到匹配的流量。配置文件是定义如何要求用户进行身份验证的内容。

1. 转到 **Manage**（管理） > **Identity and Access Services**（身份和访问服务） > **Authentication**（身份验证） > **Authentication Rule**（身份验证规则）并 **Add Authentication Rule**（添加身份验证规则）。
2. 定义需要身份验证的用户、服务和 URL 类别。
3. 将规则操作设置为 **Authenticate**（身份验证），然后选择定义身份验证方法的 **Profile**（配置文件），该身份验证方法将用于与此规则匹配的通信。



身份验证配置文件 在此处添加您的身份验证服务，并定义身份验证设置

将 Prisma Access 连接到您要用于对用户进行身份验证的服务 — SAML、TACACS +、RADIUS、LDAP 或 Kerberos — 并定义身份验证设置（例如，为失败的登录尝试设置限制）。

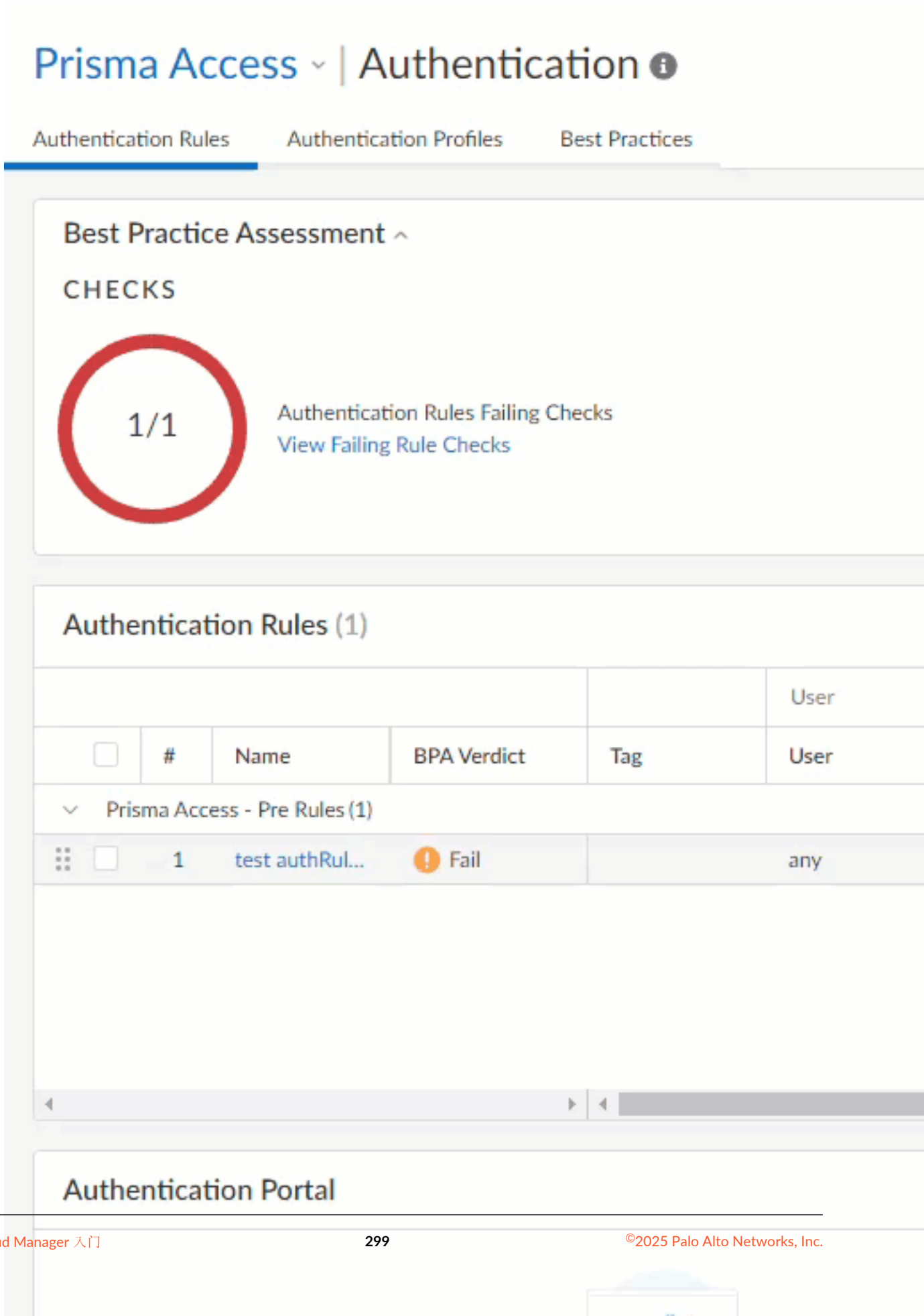
如果您使用的是本地身份验证服务，则必须首先创建服务连接，以便将本地身份验证服务连接到 *Prisma Access*。然后，返回此处设置您的身份验证配置文件。

转到 **Manage**（管理） > **Identity and Access Services**（身份和访问服务） > **Authentication**（身份验证） > **Authentication Profiles**（身份验证配置文件） > **Add Profile**（添加配置文件），并开始设置配置文件 **Auth Type**（身份验证类型）：

系统会提示您添加有关您选择的身份验证服务的详细信息，该身份验证服务将启用 Prisma Access 连接到该服务，并读取用户凭据和角色权限。配置文件中提供了用于自定义身份验证的其他设置，这些设置可能因您设置的身份验证类型而异。

MFA 服务器 指定您使用的 MFA 供应商

要使用多种方法对敏感应用程序的用户进行身份验证，请首先添加要使用的 MFA 供应商：**Add MFA Server**（添加 **MFA** 服务器）。Prisma Access 提供 MFA 供应商列表，以便您选择。

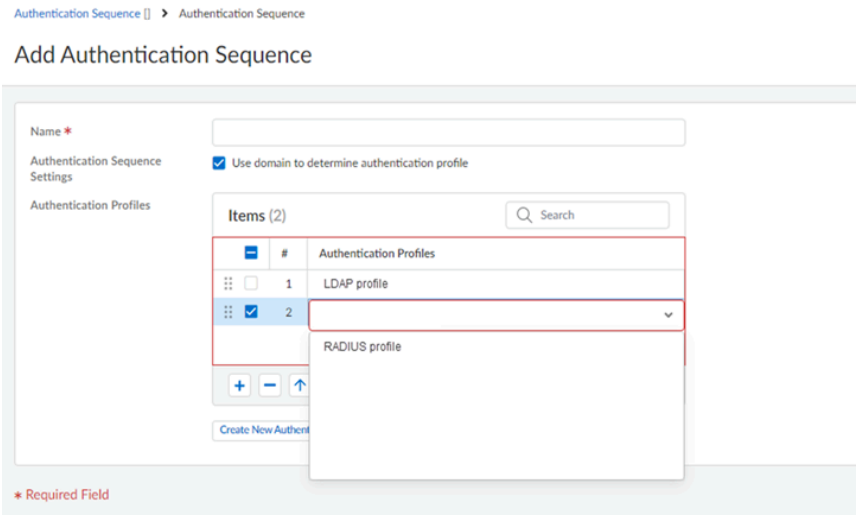


身份验证门户 为远程网络站点上的用户设置身份验证门户（也称为强制网络门户），并启用 Prisma Access 以创建 IP 地址到用户名的映射

对于第一因素身份验证（登录和密码），远程网络站点的用户必须通过身份验证门户进行身份验证。如果身份验证成功，Prisma Access 会为每个所需的附加身份验证因素显示一个 MFA 登录页面。Prisma Access 使用用户提交的凭据创建和更新 IP 地址到用户名的映射。这意味着，您将始终知道远程网络站点上谁在访问 Web 内容和企业应用程序。

身份验证顺序 按照您希望 Prisma Access 尝试的顺序对身份验证配置文件进行排名

选择 **Manage**（管理） > **Identity and Access Services**（身份和访问服务） > **Authentication**（身份验证） > **Authentication Profile**（身份验证配置文件）和 **Add Authentication Sequence**（添加身份验证顺序），对身份验证配置文件进行排序。Prisma Access 按顺序检查其中的每一个，直到成功验证用户身份。



管理：身份验证配置文件

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama or Strata Cloud Manager)	以下之一： ❑ Prisma Access 许可证 ❑ Strata Cloud Manager Pro → 您可用的特性和功能Strata Cloud Manager取决于您使用的许可证。

身份验证配置文件定义身份验证服务，对访问防火墙 Web 界面的管理员以及通过强制网络门户或 GlobalProtect 访问应用程序的最终用户的登录凭据进行验证。身份验证配置文件还定义了单点登录 (SSO) 等选项。

- Kerberos

- 云身份引擎

云身份引擎

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Access 许可证

云身份引擎 (CIE) 为 Prisma Access（Explicit Proxy 部署）中的移动用户提供用户识别和用户身份验证。云身份引擎与显式代理身份验证缓存服务 (ACS) 集成，并使用 SAML 身份提供商 (IdP) 为显式代理移动用户提供身份验证。

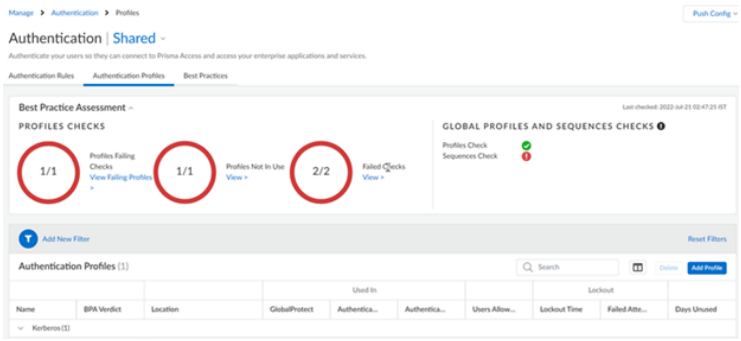
配置身份验证配置文件以使用 Cloud Identity Engine 对用户进行身份验证。

仅当启用云身份验证服务 (CAS) 时才会显示 SAML/CIE 身份验证方法。如果您的 Prisma Access 租户不支持 CIE 身份验证或 CAS，则它仅显示 SAML 身份验证方法。

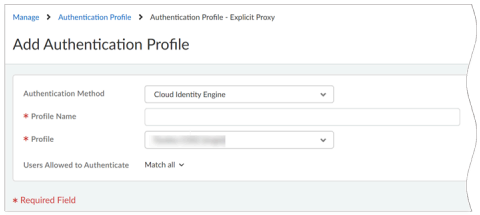
准备工作：

- 查看显式代理指南。
- 在 Cloud Identity Engine 中设置身份验证配置文件。

STEP 1 | 转到 **Manage**（管理） > **Configuration**（配置） > **Identity Services**（身份服务） > **Authentication**（身份验证），将配置范围设置为 **Explicit Proxy**（显式代理），并在 **Authentication Profiles**（身份验证配置文件）下 **Add Profile**（添加配置文件）。



STEP 2 | 选择 **Authentication Method**（身份验证方法）：**Cloud Identity Engine**（云身份引擎）。



STEP 3 | 输入唯一 **Profile Name**（配置文件名称）。

STEP 4 | 选择您在 Cloud Identity Engine 中配置的 Cloud Identity Engine 身份验证**Profile**（配置文件）。

STEP 5 | **Save**（保存）更改。

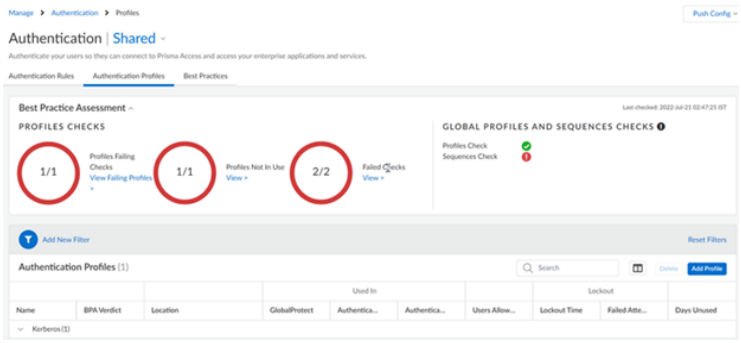
Kerberos

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Access 许可证

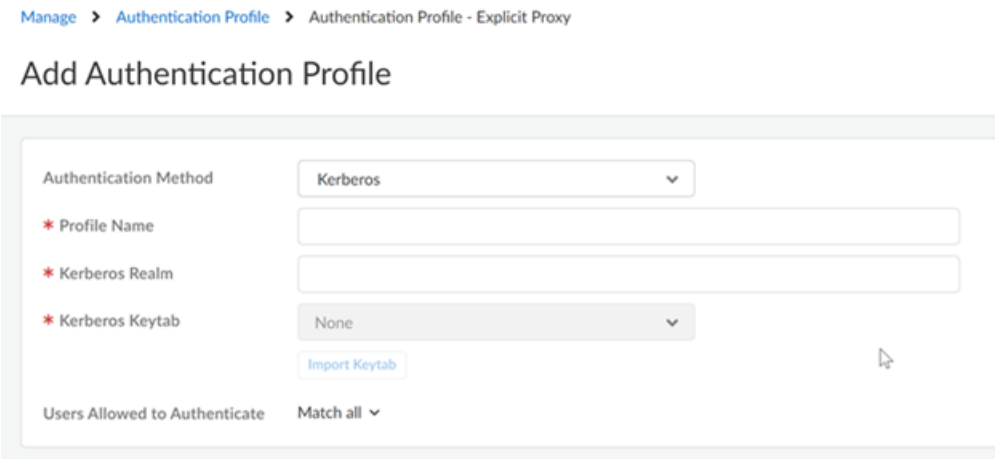
Kerberos 是一种基于“票证”的计算机网络身份验证协议，用于允许通过非安全网络进行通信的节点以安全的方式证明彼此的身份。

身份验证配置文件指定了门户或网关验证用户身份时使用的服务器配置文件。按照以下步骤为 Explicit Proxy 移动用户设置 Kerberos 身份验证配置文件以连接到 Prisma Access。

STEP 1 | 转到 **Manage**（管理） > **Configuration**（配置） > **Identity Services**（身份服务） > **Authentication**（身份验证） > **Authentication Profiles**（身份验证配置文件），并 **Add Profile**（添加配置文件）。



STEP 2 | 选择 **Authentication Method**（身份验证方法）：**Kerberos**。



STEP 3 | 输入 **Profile Name**（配置文件名称）以标识服务器配置文件。身份验证配置文件指定了门户或网关验证用户身份时使用的服务器配置文件。

STEP 4 | 输入 **Kerberos Realm**（**Kerberos** 域）（最多 127 个字符）以指定用户登录名的主机名部分。例如，用户帐户名 user@EXAMPLE.LOCAL 的领域为 EXAMPLE.LOCAL。

STEP 5 | **Import**（导入）包含 Kerberos 帐户信息的 **Kerberos Keytab** 文件。出现提示时，浏览 Keytab 文件，然后单击 **OK**（确定）。进行身份验证时，端点首先尝试使用密钥表建立 SSO。

STEP 6 | 选择 **Kerberos Keytab**。

STEP 7 | 单击 **Save**（保存）。

管理：云身份引擎

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW，包括由 软件 NGFW 积分提供资助的项目	这些许可证中的每一个都包括 Strata Cloud Manager 访问权限： ❑ Prisma Access ❑ AIOps for NGFW Premium ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → 您可用的特性和功能Strata Cloud Manager取决于您使用的许可证。

Cloud Identity Engine（目录同步）为 Prisma Access 提供对 Active Directory 信息的只读访问权限，以便您可以轻松设置和管理用户和组的安全和解密策略。

Cloud Identity Engine 可与本地 Active Directory 和 Azure Active Directory 配合使用。

要使用 Prisma Access 设置 Cloud Identity Engine，首先，请转到中心以激活 Cloud Identity Engine，并将其添加到 Prisma Access。然后转到 Prisma Access 以验证 Prisma Access 是否能够访问目录数据。

STEP 1 | 激活 Cloud Identity Engine

Cloud Identity Engine 可以与中心上任何受支持的应用程序共享 Active Directory 信息。它是免费的，不需要授权代码即可开始使用。Cloud Identity Engine 设置包括激活中心上的 Cloud Identity Engine 应用程序，配置 Cloud Identity Engine 代理以收集 Active Directory 映射，以及配置 Cloud Identity 和代理之间的相互身份验证。

确保在部署 Prisma Access 和 Strata Logging Service 的同一区域中部署 Cloud Identity Engine 实例。

STEP 2 | 为 Prisma Access 启用 Cloud Identity Engine。

您可以在首次激活 Prisma Access 时或之后的任何时间将 Prisma Access 与 Cloud Identity Engine 关联：

- 激活 **Prisma Access** 时：首次激活 Cloud Managed Prisma Access 时，您可以选择要使用的 Cloud Identity Engine 实例。请确保选择与 Prisma Access 部署在同一区域的实例。
- 激活 **Prisma Access** 后：要为现有 Prisma Access 实例启用 Cloud Identity Engine，请登录到中心。从中心设置选项卡（请参阅顶部菜单栏上的齿轮）中，选择 **Manage Apps**（管理应用程序）。找到要更新的 Prisma Access 实例，然后选择 Prisma Access 要使用的 Cloud Identity Engine 实例。

STEP 3 | 确认 Prisma Access 已连接到 Cloud Identity Engine，并且 Cloud Identity Engine 正在与 Prisma Access 共享目录信息。

- 检查您是否可以在 Prisma Access 中看到您的目录。

  转到 **Manage**（管理） > **Configuration**（配置） > **Identity Services**（身份服务） > **Cloud Identity Engine**：

- 验证您是否可以将用户和组添加到策略规则。

  选择 **Manage**（管理） > **Security Services**（安全服务） > **Security**（安全）或 **Decryption**（说明）。在安全或解密策略规则中，检查 **Users**（用户）下拉列表是否显示您的 Active Directory 用户和组条目。现在，您可以开始将这些用户和组添加到安全和解密策略规则中。

  对没有按预期强制执行的流量进行 **Troubleshoot**（故障排除） - 检查特定防火墙的状态，以了解预期策略（按配置）和强制执行的策略之间是否存在不匹配。

管理：身份重新分配

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW，包括由 软件 NGFW 积分提供资助的项目	这些许可证中的每一个都包括 Strata Cloud Manager 访问权限： ☐ Prisma Access ☐ AIOps for NGFW Premium ☐ Strata Cloud Manager Essentials ☐ Strata Cloud Manager Pro → 您可用的特性和功能Strata Cloud Manager取决于您使用的许可证。

使用 Strata Cloud Manager 设置和管理 NGFW 和 Prisma Access 的身份重新分配。

- Prisma Access
- NGFW

身份重新分配 (Prisma Access)

为了使您可以始终如一地执行安全政策，Prisma Access 共享 GlobalProtect 在整个 Prisma Access 环境中在本地发现的身份数据。Prisma Access 还可以与远程网络站点或服务连接站点（总部和数据中心）的本地设备共享身份数据。

对于 Prisma Access Cloud Management，我们在默认情况下启用了一些身份数据重新分配，对于剩余部分，我们对启用重新分配的配置非常简单（只需选中一个复选框即可选择要共享的数据）。

在“身份分配”指示板中，您可以查看身份数据的共享方式和管理数据重新分配（**Manage [管理] > Configuration [配置] > Identity Services [身份服务] > Identity Redistribution [身份重新分配]**）。

您可以重新分发的身份数据包括：

- HIP 数据
- IP 地址到标签的映射
- IP 地址到用户的映射
- 用户到标签的映射
- 隔离的设备

开始进行身份重新分配：

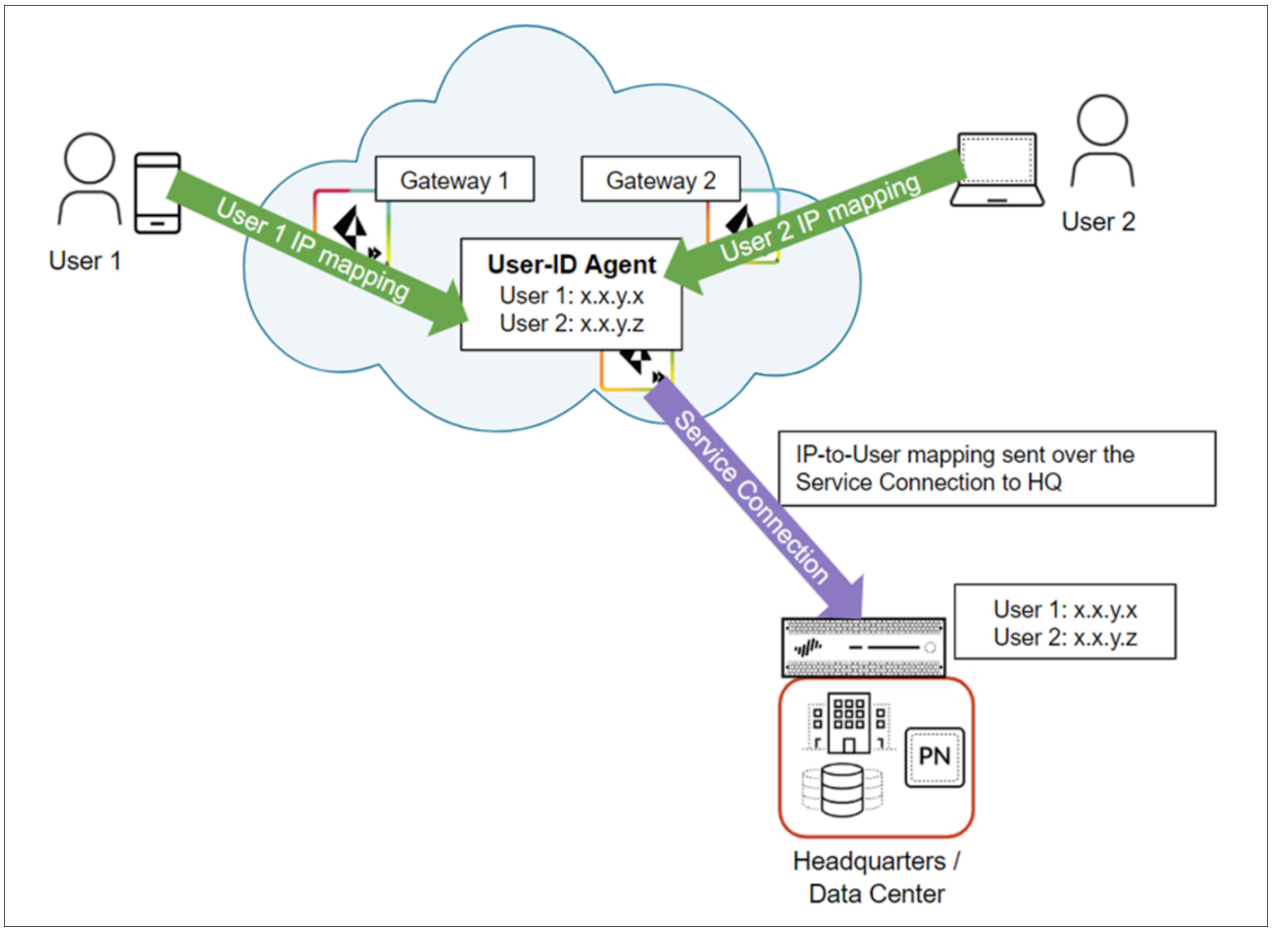
身份重新分配的工作原理

要让移动用户访问远程网络位置或总部/数据中心的资源，该资源由具有用户策略的设备提供保护，则必须将来自 Prisma Access 移动用户和远程网络用户的身份数据重新分配到该本地设备。

当用户连接到 Prisma Access 时，Prisma Access 会收集用户的身份数据并将其存储。

以下示例显示在 Prisma Access 中现有 IP 地址到用户名映射的两个移动用户。然后，Prisma Access 通过服务连接将此映射重新分发到保护总部/数据中心的本地设备。

Prisma Access Cloud Management 自动允许服务连接充当身份重新分配代理（也称为 User-ID 代理）。



设置身份重新分配

确认您的服务连接设置

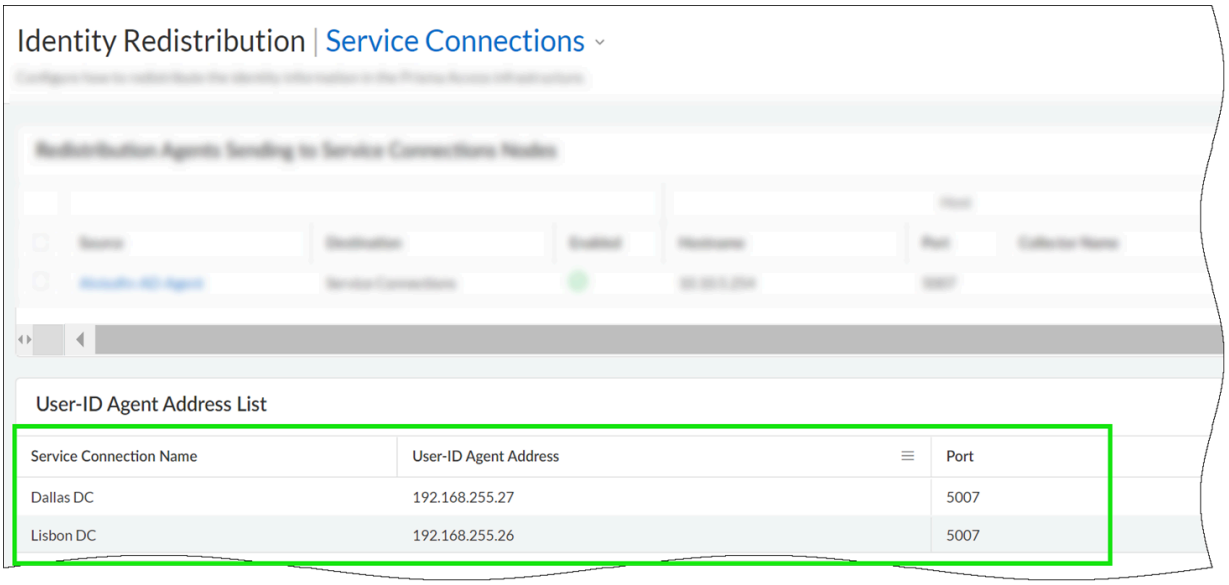
如果您尚未为总部或数据中心设置服务连接，请先配置服务连接。Prisma Access 需要服务连接才能在您的环境中共享身份数据；Prisma Access 会自动使服务连接充当再分发代理。当您看到新创建的服务连接站点被分配了用户 ID 代理地址时，它就可以用作再分发代理了（Prisma Access 会自动执行此操作，只需要几分钟）。转到 **Manage**（管理） > **Configuration**（配置） > **Identity Services**（身份服务） > **Identity Redistribution**（身份重新分配），并将范围设置为 **Service Connections**（服务连接），以便验证服务连接 User-ID 代理详细信息。

将身份数据从 Prisma Access 发送到本地设备

配置 Prisma Access 以将身份数据分发到本地设备所需的全部服务连接的用户 ID 代理信息即可。

转到 **Manage**（管理） > **Configuration**（配置） > **Identity Services**（身份服务） > **Identity Redistribution**（身份重新分配），并将配置范围设置为 **Service Connections**（服务连接），以获取服务连接 User-ID 代理的详细信息。

使用这些详细信息将 Prisma Access 配置为 Panorama 或新一代防火墙上的数据重新分配代理。

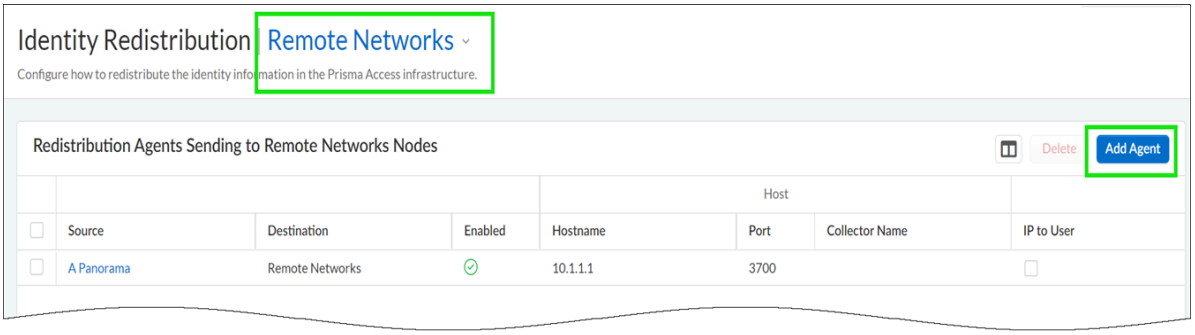


将身份数据从本地设备发送到 Prisma Access

将本地设备作为再分发代理添加到 Prisma Access；您添加的设备将能够向 Prisma Access 分发身份数据。

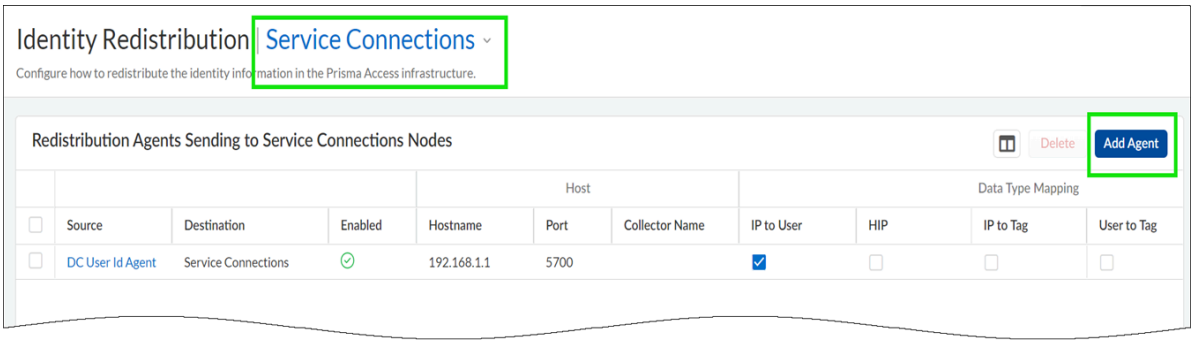
- 从远程网络站点的设备上：

  转到 **Identity Redistribution**（身份重新分配）指示板，将配置范围设置为 **Remote Networks**（远程网络），然后 **Add Agent**（添加代理）。除了指定主机详细信息外，还要选择设备与 Prisma Access 共享的数据类型。可选设置包括设备的名称和预共享密钥。



- 从服务连接站点的设备上：

  转到 **Identity Redistribution**（身份重新分配）指示板，将配置范围设置为 **Service Connections**（服务连接），然后 **Add Agent**（添加代理）。除了指定主机详细信息外，还要选择设备与 Prisma Access 共享的数据类型。可选设置包括设备的名称和预共享密钥。

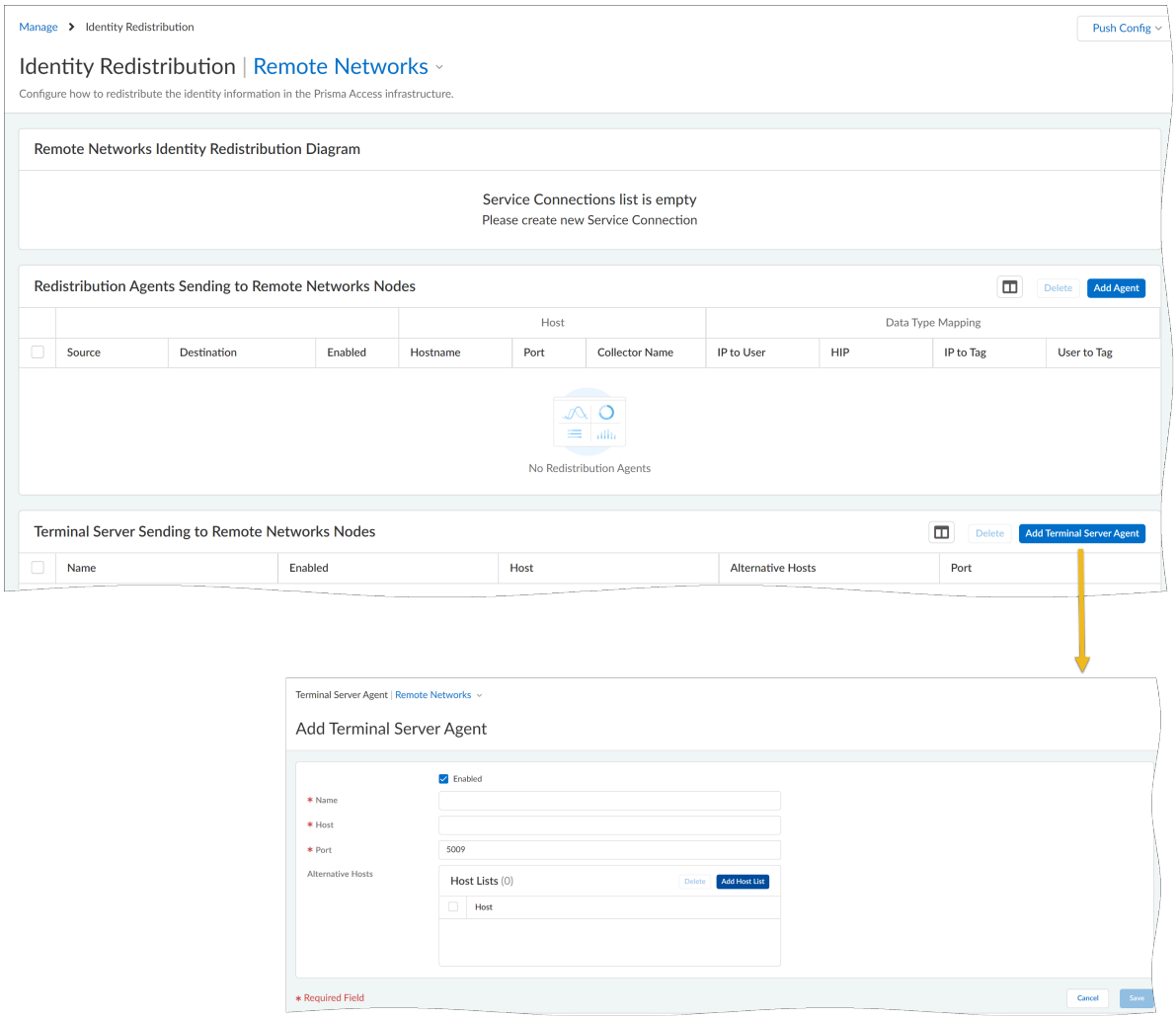


为用户映射配置终端服务器代理

终端服务器 (TS) 代理为每个用户分配一个端口范围，以识别基于 Windows 的终端服务器上的特定用户。TS 代理向 Prisma Access 通知分配的端口范围，这样 Prisma Access 就可以根据用户和用户组执行策略。

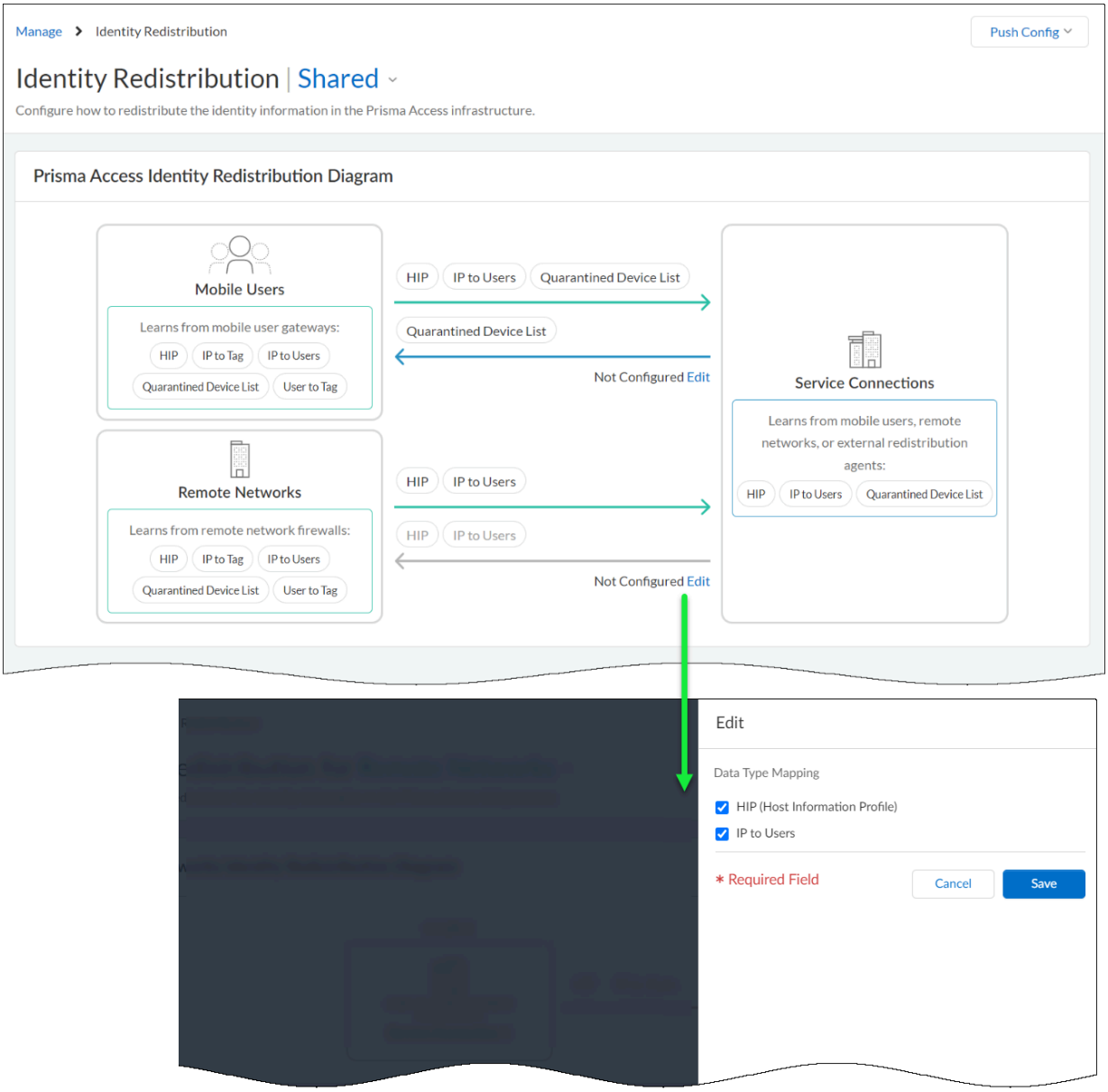
在 **Identity Redistribution**（身份重新分配）指示板上，将范围设置为 **Remote Networks**（远程网络），并在 **Terminal Server Sending to Remote Networks Nodes**（发送到远程网络节点的终端服务器）下 **Add Terminal Server Agent**（添加终端服务器代理）。

- 默认情况下，该配置为 **Enabled**（已启用）。
- 输入 TS 代理的 **Name**（名称）。
- 输入安装终端服务代理的 Windows **Host**（主机）的 IP 地址。
- 输入代理监听用户映射请求的 **Port**（端口）号。默认情况下，该端口设置为 5009。
- **Save**（保存）更改。



在您的 Prisma Access 环境中分发身份数据

在**Identity Redistribution**（身份重新分配）指示板上，**Edit**（编辑）图表以指定要从每个来源收集并在 Prisma Access 上共享的身份数据。



要激活您的更改，请将配置推送到 Prisma Access。

身份重新分配 (NGFW)

在大型网络中，您可以配置一些防火墙来通过重新分发来收集映射信息，而不是配置所有防火墙来直接查询映射信息源，从而简化资源使用情况。数据重新分发还可以提供粒度，允许您仅将指定类型的信息重新分发给所选的设备。此外，您还可以使用子网和范围筛选 IP 用户映射或 IP 标记映射，确保防火墙仅收集需要实施策略规则的映射。

若要重新分发数据，可以使用下列架构类型：

- 适用于单个区域的中心辐射型架构：

  要在防火墙之间重新分发数据，最佳做法是采用中心辐射型架构。使用此配置，中心防火墙从 Windows User-ID 客户端、Syslog 服务器、域控制器或其他防火墙等来源收集数据。配置重新分发客户端防火墙以从中心防火墙收集数据。

- 适用于多个区域的多中心辐射型架构：

  如果已在多个区域部署防火墙，且希望将数据分发给所有这些区域的防火墙，以便能实现策略规则实施的一致性，而不会受用户登录位置的影响，那么，您可以针对多个区域使用多中心辐射型架构。

- 层级式架构：

  要重新分发数据，您还可以使用层级式架构。例如，要重新分发 User-ID 信息等数据，请分层组织重新分发序列，其中，每一层都有一个或多个防火墙。在底层，在防火墙上运行的 PAN-OS 集成的 User-ID 代理和在 Windows 服务器上运行的基于 Windows 的 User-ID 代理将 IP 地址映射到用户名。每个上面的层都有防火墙来接收来自其下面的层中多达 100 个重新分发点的映射消息和身份验证时间戳。顶层防火墙汇总来自所有层的映射信息和时间戳。此部署提供了选项来为顶层防火墙中的所有用户配置策略规则，或者，为在底层防火墙中相应域中的部分用户配置特定区域或功能的策略规则。

当流量未按预期强制执行时，请使用**Troubleshooting**（故障排除）检查特定防火墙的数据平面状态，以了解预期策略（按配置）与强制执行的策略之间是否存在不匹配。

STEP 1 | 登录 Strata Cloud Manager。

STEP 2 | 确保您的 Strata Cloud Manager 部署符合配置身份重新分配的要求。

1. 为您的 Strata Cloud Manager 租户配置并激活 Cloud Identity Engine (CIE)。

   这是使用身份重新分配所必需的。

   1. 激活 Cloud Identity Engine。
   2. 设置 Cloud Identity Engine。

2. 选择 **Manage**（管理） > **Configuration**（配置） > **NGFW and Prisma Access**（**NGFW 和 Prisma Access**） > **Objects**（对象） > **Address Groups**（地址组），并将具有所需地址的动态地址组 **Add**（添加）到标记映射。

   对于地址组类型，选择 **Dynamic**（动态）。根据需要配置动态地址组并 **Save**（保存）。

3. 选择 **Manage**（管理） > **Configuration**（配置） > **NGFW and Prisma Access**（**NGFW 和 Prisma Access**） > **Objects**（对象） > **Dynamic User Groups**（动态用户组），并将具有所需用户名的动态用户组 **Add**（添加）到标记映射。

   根据需要配置动态用户组并 **Save**（保存）。

STEP 3 | 选择 **Manage**（管理） > **Configuration**（配置） > **NGFW and Prisma Access**（**NGFW 和 Prisma Access**） > **Identity Services**（身份服务） > **Identity Redistribution**（身份重新分配），并选择要配置身份重新分配的配置范围。

您可以从 **Folders**（文件夹）中选择文件夹或防火墙，或者选择 **Snippets**（代码段）来配置代码段中的身份重新分配。

STEP 4 | **Add Agent**（添加代理）。

STEP 5 | 输入代理的描述性 **Name**（名称）。

STEP 6 | 输入 **Host**（主机）IP 地址。

STEP 7 | 输入 **Port**（端口）（范围为 1-65535）。

STEP 8 | 选择 **Data Type Mapping**（数据类型映射）。

- **IP** 到用户 — User-ID 的 IP 地址到用户名映射。
- 主机信息配置文件 **(HIP)** -动态地址组的 IP 地址到标记映射。
- **IP** 到标记 — 动态用户组的用户名到标记映射。
- 用户到标记 — GlobalProtect 的 HIP 数据，包括 HIP 对象和配置文件。
- 隔离设备列表 — GlobalProtect 标识为“已隔离”的设备。

STEP 9 | **Save**（保存）。

STEP 10 | （仅限 NGFW 的云管理）为防火墙启用身份重新分配。

1. 选择 **Manage**（管理） > **Configuration**（配置） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Device Settings**（设备设置） > **Device Setup**（设备安装） > **Management**（管理），然后选择 **Customize**（自定义），以便为 **uid-agent** 服务配置服务路由。

   选择要在其中创建服务路由的配置范围。您可以从 **Folders**（文件夹）中选择文件夹或防火墙，或者选择 **Snippets**（代码段）来配置代码段中的服务路由。
2. 启用防火墙以在其他防火墙查询要重新分发的数据时进行响应。

   1. 选择 **Manage**（管理） > **Configuration**（配置） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Device Settings**（设备设置） > **Device Setup**（设备安装） > **Management**（管理），然后启用 **User-ID** 网络服务。
   2. 选择 **Manage**（管理） > **Configuration**（配置） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Device Settings**（设备设置） > **Interfaces**（接口），以创建或选择第 3 层接口。

      展开 **Advanced Settings**（高级设置）。在 **Other**（其他）中，创建或编辑管理配置文件以启用 **User-ID**。

      - 选择

STEP 11 | Push Config（推送配置）。

管理：本地用户和群组

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW，包括由 软件 NGFW 积分提供资助的项目	这些许可证中的每一个都包括 Strata Cloud Manager 访问权限： ☐ Prisma Access ☐ AIOps for NGFW Premium

在何处可以使用？	需要提供什么？
	❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → 您可用的特性和功能Strata Cloud Manager取决于您使用的许可证。

在本地存储管理员和最终用户的身份验证信息。您可以存储来自使用 GlobalProtect 或身份验证门户进行身份验证的管理员和最终用户的身份验证信息。

要配置本地数据库身份验证，您需要创建一个在防火墙上本地运行并包含用户帐户（用户名和密码或哈希密码）的数据库。您可以配置防火墙本地的用户数据库，以对访问防火墙 Web 界面的管理员以及通过身份验证门户或 GlobalProtect 访问应用程序的最终用户进行身份验证。

本地数据库身份验证可以与身份验证配置文件相关联，因此它们可以适应不同用户组需要不同身份验证设置的部署，例如 Kerberos 单点登录 (SSO) 或多因素身份验证 (MFA)。对于使用身份验证配置文件的管理员帐户，不应用密码复杂性和过期设置。此身份验证方法适用于访问防火墙的管理员以及通过身份验证门户或 GlobalProtect 访问服务和应用程序的最终用户。

转到 **Manage**（管理） > **Configuration**（配置） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Identity Services**（身份服务） > **Local Users & Groups**（本地用户和组），以便开始收集身份验证数据。

创建本地用户

STEP 1 | 登录 Strata Cloud Manager。

STEP 2 | 选择 **Manage**（管理） > **Configuration**（配置） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Identity Services**（身份服务） > **Local Users & Groups**（本地用户和组） > **Local Users**（本地用户），然后选择要创建本地用户的配置范围。

您可以从 **Folders**（文件夹）中选择文件夹或防火墙，或者选择 **Snippets**（代码段），以配置代码段中的本地用户。

STEP 3 | **Add Local User**（添加本地用户）。

STEP 4 | 输入 **User Name**（用户名）。

STEP 5 | 验证本地用户是否 **Enabled**（已启用）。

您可以取消选中（禁用），这样就不再允许用户进行身份验证，而不是从本地防火墙数据库中删除本地用户进行身份验证。

STEP 6 | 输入 **Password**（密码）和 **Confirm Password**（确认密码）。

STEP 7 | **Save**（保存）。

STEP 8 | **Push Config**（推送配置）。

创建本地用户组

将多个本地用户分组到一个本地组中，以向本地防火墙数据库添加组信息。您可以创建本地用户组来管理具有相同身份验证要求的多个本地用户。

STEP 1 | 登录 Strata Cloud Manager。

STEP 2 | 选择 **Manage**（管理） > **Configuration**（配置） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Identity Services**（身份服务） > **Local Users & Groups**（本地用户和组） > **Local User Groups**（本地用户组），然后选择要创建本地用户组的配置范围。

您可以从 **Folders**（文件夹）中选择文件夹或防火墙，或者选择 **Snippets**（代码段），以配置代码段中的本地用户组。

STEP 3 | **Add Local User Group**（添加本地用户组）。

STEP 4 | 输入本地用户组 **Name**（名称）。

STEP 5 | 添加您在上一步中创建的 **Local Users**（本地用户）。

STEP 6 | **Save**（保存）。

STEP 7 | **Push Config**（推送配置）。

管理：设备设置

在何处可以使用？	需要提供什么？
• NGFW，包括由 软件 NGFW 积分提供资助的项目	❑ Strata Cloud Manager Essentials ❑ AIOps for NGFW Premium 或 Strata Cloud Manager Pro → 您可用的特性和功能Strata Cloud Manager取决于您使用的许可证。

在 **Device Settings**（设备设置）中，您可以为云管理的防火墙配置以下设置：

设置	说明
接口	配置接口，以便让防火墙同时在多个部署中运行。 在 **Ethernet**（以太网）选项卡上，使用 **Show local device configs**（显示本地设备配置）查看本地防火墙和 Strata Cloud Manager 上的各种配置。
路由	为防火墙配置路由配置文件、逻辑路由器和静态路由。
IPSec 隧道	配置 IPSec 隧道，以便在 IP 数据包通过隧道时对其进行身份验证和加密。
DHCP	配置 DHCP，以便提供 TCP/IP 和链接层配置参数，并为 TCP/IP 网络上的动态配置主机提供网络地址。
服务区	配置服务区，以便将网络划分为功能区和组织区，从而减少攻击面。
DNS 代理	配置 DNS 代理，以便将防火墙配置为 DNS 客户端和服务器之间的中介。
设备安装	设置设备，以便配置防火墙的管理和辅助接口的服务路由、连接设置、允许的服务和管理访问设置。
代理	配置 Web 代理，以便将代理和防火墙功能整合到一个设备中。 *Strata Cloud Manager Web* 代理需要旧路由器堆栈。如果您希望启用此功能，请联系您的客户团队。

设置	说明
虚拟线路	配置虚拟线路，以便将防火墙接口集成到拓扑中，这样防火墙上两个连接的接口就不需要做任何交换或路由。
GlobalProtect	启用云托管 NGFW 作为GlobalProtect 网关和门户，为各地用户提供灵活、安全的远程访问。

管理：全局设置

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama or Strata Cloud Manager)	以下之一： ❑ Prisma Access 许可证 ❑ Strata Cloud Manager Pro → 您可用的特性和功能Strata Cloud Manager取决于您使用的许可证。

查看并配置 Strata Cloud Manager 中的全局设置**Manage [管理] > Configuration [配置] > NGFW and Prisma Access [NGFW 和 Prisma Access] > Global Settings [全局设置]**）

object	说明
SaaS 应用程序管理	集中管理每个 SaaS 应用程序的 SaaS 应用程序。SaaS 应用程序管理可让您找到可用于安全地为您的企业启用应用程序的功能。
用户指导通知模板	集中管理最终用户通知模板，如果在包含敏感数据的流量受到检查和阻止时，用户生成 Enterprise Data Loss Prevention (E-DLP)事件，则通过 AI-Powered ADEM 提醒用户。
Auto VPN	手动配置网络设备和建立 VPN 隧道是一个繁琐的过程，并且容易出现配置错误。Auto VPN 自动在网络设备之间创建 VPN 隧道。Auto VPN 使您能够创建 VPN 集群来连接多个局域网 (LAN)。带有 Auto VPN 的 SD-WAN 可以轻松部署和管理 SD-WAN 部署。

用户指导通知模板

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager)	❑ GlobalProtect app 版本 6.3 或更高版本 ❑ Enterprise Data Loss Prevention (E-DLP) 许可证 ❑ Prisma Access 移动用户许可证 ❑ Prisma Access 许可证

在何处可以使用？	需要提供什么？
	或者以下任何包含 Enterprise DLP 许可证的许可证 ❑ Prisma Access CASB 许可证 ❑ Next-Generation CASB for Prisma Access and NGFW (CASB-X) 许可证

最终用户指导通知模板允许您配置在用户生成Enterprise Data Loss Prevention (E-DLP)事件时，在 Access Experience 用户界面 (UI) 中向用户显示的通知。当下载或上传包含敏感数据的文件时，或者以 Web 表单发布包含敏感数据的非基于文件的流量时，就会生成 Enterprise DLP 事件。

要确定哪些数据被视为敏感数据，您可以添加一个或多个 **Inline DLP Rules**（**Inline DLP** 规则）。DLP 规则包含定义哪些数据被视为敏感数据的流量匹配标准。DLP 规则源自同名的 Enterprise DLP 数据配置文件。此外，您还可以配置当 **File Based**（基于文件）或 **Non-File Based**（非基于文件）的 Enterprise DLP事件发生时的自定义消息。在 Enterprise DLP 事件生成后，生成事件的用户可以查看 Data Security通知，以获取有关上传、下载或发布的敏感数据的更多信息。

无论用户生成同一事件多少次，30 秒内每个事件仅显示一条通知。例如，用户尝试将包含敏感数据的文件上传到 Box Web 应用程序，并且 Enterprise Data Loss Prevention (E-DLP) 阻止上传。然后用户立即尝试再上传同一个文件 5 次，但每次都被阻止。在这种情况下，即使用户被阻止将包含敏感日期的文件上传到 Box Web 应用程序共 6 次，也只会生成一次访问体验警报。

STEP 1 | 联系您的 Palo Alto Networks 代表，为您的租户启用最终用户指导。

STEP 2 | 在 Windows 或 macOS 上安装 GlobalProtect app 版本 6 6.3 或更高版本。

STEP 3 | 登录 Strata Cloud Manager

STEP 4 | 启用 Autonomous DEM。

在 Strata Cloud Manager 上，选择 **Workflows**（工作流） > **Prisma Access Setup**（**Prisma Access** 设置） > **GlobalProtect** > **GlobalProtect App**（**GlobalProtect** 应用程序）并 **Add App Settings**（添加应用程序设置）。您必须配置这些必需的设置，以便当用户生成 DLP 事件时，在 Access Experience UI 中向他们显示通知。

- 启用 **Autonomous DEM and GlobalProtect Log Collection for Troubleshooting**（自治 **DEM** 和 **GlobalProtect** 日志收集以进行故障排除）
- **DEM for Prisma Access**（仅限 **Windows** 和 **Mac**）— 选择 **Install and User Cannot Enable or Disable DEM**（安装且用户无法启用或禁用 **DEM**）
- **DEM for Prisma Access** 版本 **6.3** 及更高版本（仅限 **Windows** 和 **Mac**）— 选择 **Install the Agent**（安装代理）

STEP 5 | 仅限 macOS）在 Access Experience 用户界面中，选择 **Settings**（设置） > **Notifications**（通知），并启用 **Allow notifications**（允许通知）。

必须在每个用户的 Access Experience UI 中启用此设置，并且需要在用户的桌面上显示通知。根据需要配置其余的 Access Experience 通知设置。

STEP 6 | 配置 Enterprise DLP。

1. 创建解密配置文件和策略规则。

   这是 Enterprise DLP 解密和检查流量中的敏感数据所必需的。

2. 创建自定义数据模式来定义您的匹配标准。

   或者，您可以使用预定义的数据模式，而不是创建自定义数据模式。

3. 创建数据配置文件并添加数据模式。

   仅支持自定义数据配置文件。默认情况下，所有预定义的 DLP 规则的 **Action**（操作）都设置为 **Alert**（警报）。如果必须克隆预定义的数据配置文件才能编辑 DLP 规则 **Action**（操作）。

4. 修改 DLP 规则。

   - 修改 DLP 规则时，必须将 **Action**（操作）设置为 **Block**（阻止）。这是在 Access Experience UI 中生成警报所必需的。如果将 **Action**（操作）设置为 **Alert**（警报），则不会显示任何警报。
   - 将 DLP 规则添加到配置文件组并将配置文件组附加到安全策略规则。这是 Enterprise DLP 生成 DLP 事件，然后在 Access Experience UI 中生成通知所必需的。

STEP 7 | 选择 **Manage**（管理） > **Configuration**（配置） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Global Settings**（全局设置） > **User Coaching Notification Template**（用户指导通知模板），然后 **Add Notification Template**（添加通知模板）。

STEP 8 | 配置 **General Information**（常规信息）。

1. 验证 **Product Name**（产品名称）是否为 **Inline DLP**。

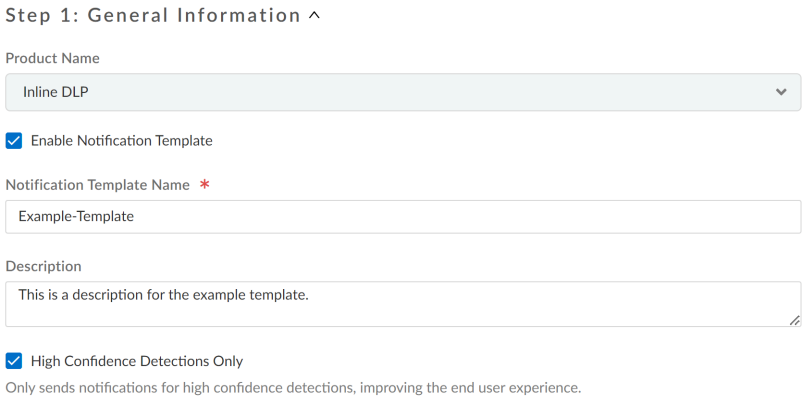
   这是默认设置，无法更改

2. 选择 **Enable Notification Template**（启用通知模板）以启用保存的模板。

   此设置已默认启用。

3. 输入描述性的 **Notification Template Name**（通知模板名称）。
4. （可选）输入通知模板的 **Description**（说明）。
5. 可选）选择 **High Confidence Detections Only**（仅高置信度检测），以便仅对高置信度流量匹配生成 Access Experience 警报。

   高置信度匹配反映检测到匹配的流量时 Enterprise DLP 的置信度。对于正则表达式 (regex) 模式，这是基于与配置的邻近关键字的字符距离。对于机器学习 (ML) 模式，该置信度由 ML 模型计算。

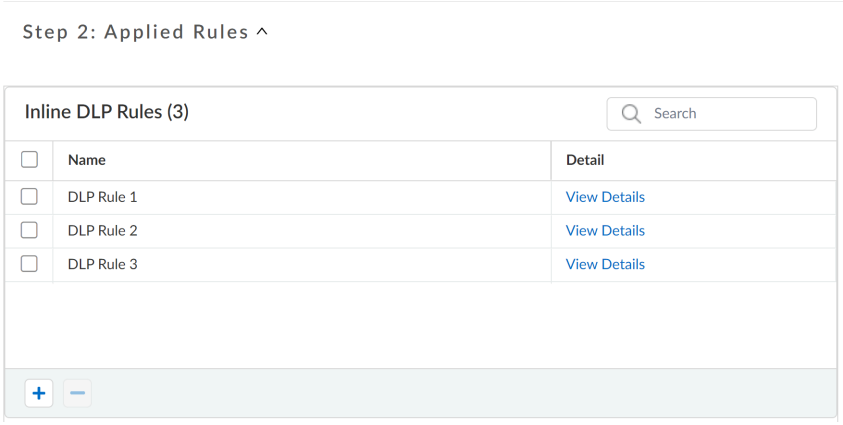


STEP 9 | 向通知模板添加一个或多个 **Applied Rules**（应用规则）。

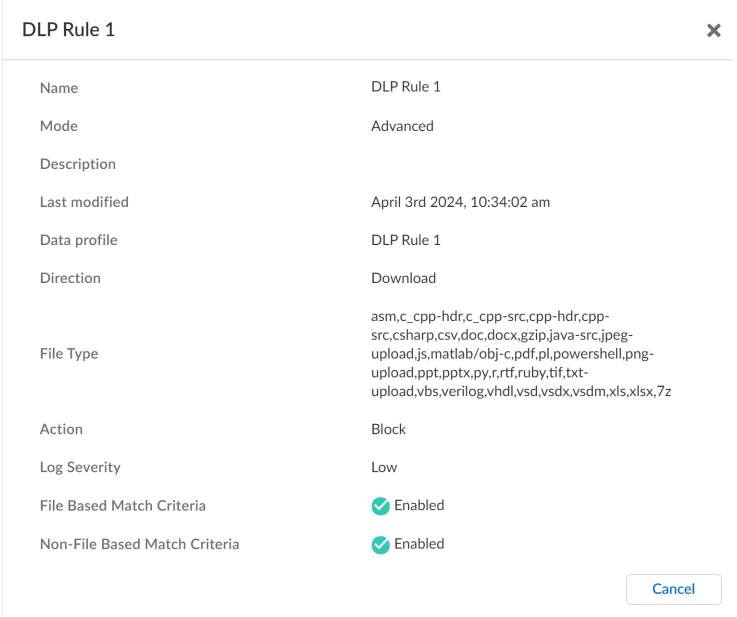
DLP 规则必须将规则 **Action**（操作）设置为 **Block**（阻止），并将其添加到附加到安全策略规则的配置文件组才能生成访问体验通知。仅添加与安全策略规则关联的配置文件组的 DLP 规

则。这是 Enterprise DLP 生成 DLP 事件，然后在 Access Experience UI 中生成通知所必需的。可以将单个 DLP 规则添加到多个用户指导通知模板。

添加到通知模板的所有 DLP 规则在以下情况下都会生成相同的 **Notification Message**（通知消息）：Enterprise DLP 阻止与 DLP 规则关联的数据配置文件相匹配的敏感数据。



对于添加的每个 DLP 规则，您可以 **View Details**（查看详细信息），以查看具体的检查详细信息。这包括流量检查 **Direction**（方向）、相应的 **File Type**（文件类型）、**Action**（操作）。以及 DLP 规则是否检查 **File Based Match Criteria**（基于文件的匹配条件）、**Non-File Based Match Criteria**（非基于文件的匹配条件）或两者。



STEP 10 | 定义当 Enterprise DLP 阻止与 DLP 规则关联的数据配置文件相匹配的敏感数据时，用户在何时收到 **Notification Message**（通知消息）。

消息模板是用户在 Enterprise DLP 阻止敏感数据时，收到的 Access Experience 提示通知。您可以在消息模板中使用以下变量。必须为每个变量加上括号。

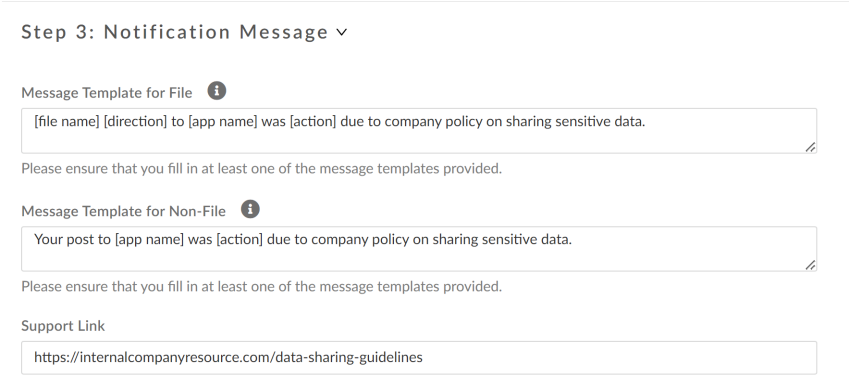
- **[**文件名**]** — 包含被 Enterprise DLP 阻止的敏感数据的文件名和扩展名。
- （仅限基于文件）**[**方向**]** — 指定 Enterprise DLP 是否阻止文件上传或下载。
- **[**应用程序名称**]** — 应用程序用户尝试上传、下载或发布非基于文件的内容。
- **[**操作**]** — Enterprise DLP 在检测到敏感数据时执行的操作。该值始终为 `Blocked`。

1. 定义基于 **Message Template for File Based**（文件的消息模板）的检测。

   如果 DLP 规则未配置基于文件的检测，请跳过此步骤。
2. 定义基于 **Message Template for Non-File**（非文件的消息模板）的检测。

   如果 DLP 规则未配置为非基于文件的检测，请跳过此步骤。
3. 添加 **Support Link**（支持链接）。

   您可以直接在 Access Experience 通知中添加链接，描述您公司共享或下载敏感数据的策略。



STEP 11 | **Save**（保存）。

STEP 12 | 生成 Enterprise DLP 事件的用户可以查看 Data Security 通知，以查看上传、下载或发布的敏感数据代码段。

管理：操作

在何处可以使用？	需要提供什么？
• NGFW (Managed by Panorama or Strata Cloud Manager) • 包括 VM 系列	❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) → 在 Strata Cloud Manager 中，您可以使用的特性和功能取决于您使用的 许可证。

故障排除

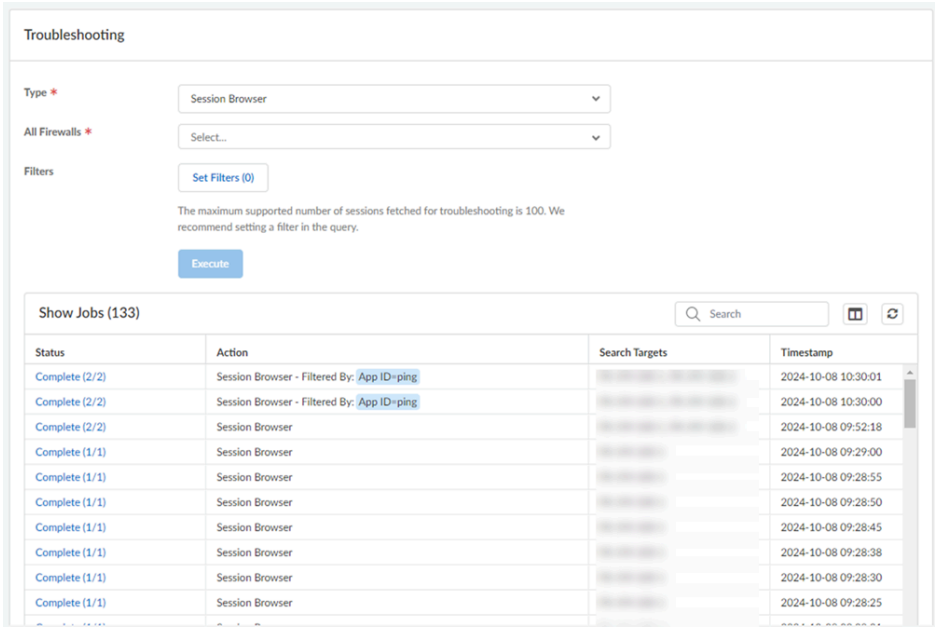
从 Strata Cloud Manager 排除 NGFW 故障，而无需在各种防火墙接口之间移动。

有关故障排除的更多信息，请单击此处。

故障排除指示板允许您排除 Strata Cloud Managed NGFW 的网络、身份和策略问题故障。使用故障排除指示板，您可以找到以下区域的异常和有问题的配置：

- ❑ DNS 代理
- ❑ NAT
- ❑ 用户组
- ❑ 动态地址组
- ❑ 动态用户组
- ❑ 用户 ID
- ❑ 会话浏览器

首先，请转到 **Manage**（管理） > **Configuration**（配置） > **NGFW and Prisma Access**（**NGFW 和 Prisma Access**） > **Operations**（操作） > **Troubleshooting**（故障排除） > **Session Browser**（会话浏览器）。



管理：IoT 策略建议

在何处可以使用？	需要提供什么？
• Prisma Access （利用 *Strata Cloud Manager* 或 *Panorama* 配置管理） • NGFW （利用 *Strata Cloud Manager* 或 *Panorama* 配置管理）	❑ 使用 Strata Cloud Manager 管理您的配置至少需要其中一个许可证；要统一管理 NGFW 和 Prisma Access，您需要同时具备以下许可证： ❑ Prisma Access 许可证 ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro ❑ 高级 IoT Security 产品（Enterprise IoT Security Plus、Industrial IoT Security 或 Medical IoT Security）的 IoT Security 订阅

IoT Security 为 Strata Cloud Manager 提供按设备配置文件组织的自动生成的安全策略规则建议。每个应用程序每个配置文件有一个建议。选择一个配置文件，选择要使用的规则建议，然后在其中执行新一代防火墙或 Prisma Access 部署类型。

入门

选择安全策略规则建议并将其应用于新一代防火墙或 Prisma Access。

STEP 1 | 为新一代防火墙创建文件夹或代码段。

如果要使用预定义文件夹或以前创建的文件夹或代码段，请跳过此步骤。*Prisma Access* 文件夹是预定义的。

文件夹本质上是存放各种规则、安全配置和对象的容器。为了导入 IoT Security IoT Security 生成的策略规则建议，文件夹将保存新一代防火墙或 Prisma Access 部署。

代码段也是一种可以与多个文件夹关联的容器类型。使用文件夹和代码段，您可以将策略规则导入任何您想要的防火墙或部署组中。

例如，您可以创建一个名为 California 的文件夹，在其中放置 60 个防火墙，然后创建另一个名为 Hawaii 的文件夹，在其中放置 15 个防火墙。然后创建一个名为 CA-HI 的代码段，并将其应用到 California 和 Hawaii 文件夹。要仅将规则建议导入 California 的防火墙时，请将范围设置为 **Folder**（文件夹），并选择 California 文件夹。如果要将规则建议同时导入到 California 和 Hawaii，请将范围设置为 **Snippet**（代码段），然后选择 CA-HI 代码段。

根据文件夹结构的层次结构，我们可能有一个父文件夹，如 California 和 Hawaii 之上的 US-West。然后，在选择 **US-West**（美国西部）并将范围设置为 **Folder**（文件夹）时，如果您导入规则建议，则 California 和 Hawaii 的两个子文件夹都将继承导入的规则。但是，如果您只想将规则导入到 California 和 Hawaii，而它们在 US-West 文件夹下具有类似 Oregon、Alaska、Washington 和 Arizona 等同级文件夹，则此方法不会奏效。那么您必须使用 CA-HI 代码段。

STEP 2 | 创建安全策略规则。

1. 选择 **Manage**（管理） > **Configuration**（配置） > **IoT Policy Recommendation**（**IoT** 策略建议）。
2. 选择一个配置文件名称。

   IoT Security 使用机器学习根据同一设备配置文件中 IoT 设备的正常、可接受的网络行为自动生成安全策略规则建议。Strata Cloud Manager 显示按应用程序组织的这些建议列表。对于每种行为，您都可以看到以下内容：

行为组件	说明
应用程序风险	这是由各种因素在风险从 1 到 5 递增的尺度上决定的应用程序固有的风险水平。
已创建安全策略	当文件夹或代码段的一个或多个名称显示在此处时，表示以前为此行为创建了安全策略规则。单击其中之一将打开一个侧面面板，其中包含配置文件、应用程序和文件夹或代码段的名称以及策略规则操作。当此处出现 **No**（否）时，表示尚未创建规则。

行为组件	说明
发现的位置	**Internal**（内部）表示目标位于本地网络上。**External**（外部）表示目标在本地网络之外。
本地已观察	**Yes**（是）表示在您的 IoT Security 租户环境中观察到该行为。**No**（否）表示在多个 IoT Security 租户环境中观察到它，但在您的环境中没有观察到它。
应用程序使用情况	**Common**（共用）表示在多个 IoT Security 租户环境中检测到应用程序。**Unique**（唯一）表示在您的环境中观察到它，但在同样配置文件中也有设备的其他租户中则没有观察到它。
目标地址和 FQDN	这是建议的策略规则的目标。可以是“任何”、IP 地址或 FQDN。
目标配置文件	当目标是内部目的地并标识了目的地的设备配置文件时，将显示配置文件。
上次查看	对于本地观察到的行为，这是最后一次观察到它的时间戳。对于未在本地观察到的常见行为，显示破折号。

3. 选择一个或多个行为，然后 **Create Security Policy**（创建安全策略）。
4. 查看将创建的安全策略规则，然后选择 Strata Cloud Manager 将应用这些规则的配置范围。

   要将规则应用于文件夹中的一个或多个新一代防火墙或 Prisma Access 部署，请选择 **Folders**（文件夹），然后从范围选择中选择文件夹。

   要将规则应用于代码段中的一个或多个新一代防火墙或 Prisma Access 部署，请选择 **Snippets**（代码段），然后从范围选择中选择代码段。
5. **Create Security Policy**（创建安全策略）。

STEP 3 | 将配置推送到新一代防火墙和 Prisma Access 部署。

1. 选择 **Manage**（管理） > **Operations**（操作） > **Push Config**（推送配置）。
2. 选择具有配置更改的文件夹，推送配置（推送配置），**Push**（推送），然后再次 **Push**（推送）。

   Strata Cloud Manager 在选定文件夹的 Job ID 列中显示 ID 编号，并在推送状态列中显示配置推送的状态。

   当推送状态从 **Pending**（待定）更改为 **Success**（成功）时，您就知道推送的配置已经开始运行。
3. 要查看推送作业的状态，请选择 **Manage**（管理） > **Operations**（操作） > **Push Status**（推送状态）。这里可以看到父作业的状态以及子作业的状态，每个防火墙或部署都有一个状态。

管理：企业 DLP

在何处可以使用？	需要提供什么？
• Prisma Access （利用 *Strata Cloud Manager* 或 *Panorama* 配置管理） • NGFW （利用 *Strata Cloud Manager* 或 *Panorama* 配置管理）	• Enterprise Data Loss Prevention (E-DLP) 许可证 • **NGFW (Managed by Panorama)** — 支持和 Panorama 设备管理许可证 • **Prisma Access (Managed by Strata Cloud Manager)** — Prisma Access 许可证 • **SaaS Security** — SaaS Security 许可证 • **NGFW (Managed by Strata Cloud Manager)** — 支持和 AIOps for NGFW Premium 许可证 或者以下任何包含 Enterprise DLP 许可证的许可证 • Prisma Access CASB 许可证 • Next-Generation CASB for Prisma Access and NGFW (CASB-X) 许可证 • Data Security 许可证

Enterprise Data Loss Prevention (E-DLP) 保护敏感信息免遭未经授权的访问、滥用、提取或共享。通过 Strata Cloud Manager 上的 Enterprise DLP，您可以实施组织的 Data Security 标准，并防止 NGFW、Prisma Access 移动用户和远程网络中的敏感数据丢失。

功能亮点

- **Enterprise Data Loss Prevention (E-DLP)** 指示板

  转到 **Manage**（管理） > **Configuration**（配置） > **Data Loss Prevention**，以便配置和管理 Enterprise DLP。

  您的 Enterprise DLP 配置在您使用的 Enterprise DLP 之间共享。因此，您可能会在这里看到在其他地方配置的设置，并且您在此处配置的某些设置也可以在其他产品中使用。

- 预定义 + 自定义 **Enterprise DLP** 设置

  Enterprise DLP 包括内置设置，您可以使用它们快速开始保护最敏感的内容：

  - 预定义的正则表达式和基于 ML 的数据模式指定您可能想要扫描和保护的常见敏感信息类型（例如信用卡和社会保险号）
  - 预定义数据配置文件通常需要相同类型执行的数据模式分组在一起

  您还可以直接在 Strata Cloud Manager 上创建自定义数据模式和配置文件。

- **DLP** 事件调查

  当流量与附加到 Strata Cloud Manager 上的安全策略规则的 DLP 数据配置文件匹配时，将生成 DLP 事件。在 DLP 事件指示板上，您可以查看触发事件的流量的详细信息，例如匹配的数据模式、流量的来源和目标、文件和文件类型。

- 扫描支持的文件格式的图像

  利用光学字符识别 (OCR) 加强您的安全态势，进一步防止意外的数据滥用、丢失或盗窃。OCR 允许 DLP 云服务扫描支持的文件类型，其中包含与您的 Enterprise DLP 筛选配置文件匹配的敏感信息。

- 精确数据匹配 **(EDM)**

  EDM 是一种先进的检测工具，用于监控和保护敏感数据免遭泄露。使用 EDM 在结构化数据源（例如数据库、目录服务器或结构化数据文件（CSV 和 TSV））中高精度检测敏感和个人身份信息 (PII)，例如社保号、医疗记录号、银行账号和信用卡号。

- 自定义文档类型

  将包含知识产权或敏感信息的自定义文档上传至 Enterprise Data Loss Prevention (E-DLP) 以创建自定义文档类型。您的自定义文档类型将用作高级数据配置文件中的匹配标准，以检测和防止泄露。

- **Email DLP**

  电子邮件 DLP 通过 AI/ML 支持的数据检测防止包含敏感信息的电子邮件泄露。例如，Enterprise DLP 可以防止敏感数据通过组织内的销售人员发送到其个人电子邮件的出站电子邮件泄露。

- **Enterprise DLP** 基于角色的访问

  您可以对 Strata Cloud Manager 内的 Enterprise DLP 内部控件启用基于角色的访问权限。这允许您控制哪些用户对 Enterprise DLP 的不同部分具有读写访问权限。

入门

STEP 1 | 在 Strata Cloud Manager 上启用 Enterprise DLP。

要设置 Enterprise DLP，您需要创建一个解密配置文件以允许 DLP 云服务检查流量。选择 **Manage**（管理） > **Configuration**（配置） > **Security Services**（安全服务） > **Decryption**（说明），然后：

1. 选择 **Manage**（管理） > **Configuration**（配置） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Security Services**（安全服务） > **Decryption**（说明），然后 **Add Rule**（添加规则）。

   预定义的解密配置文件设置允许 Enterprise DLP 检查流量。除非您需要启用 **Strip ALPN**（**Advanced Settings** [高级设置] > **SSL Forward Proxy** [**SSL** 转发代理]），否则不需要修改预定义的解密配置文件设置。

2. 将解密配置文件添加到 **SSL Forward Proxy**（**SSL** 转发代理）以解密规则。

- 启用 Enterprise DLP 的方法如下

STEP 2 | （可选）选择 **Manage**（管理） > **Configuration**（配置） > **Data Loss Prevention** > **Detection Methods**（检测方法），并创建数据模式

您可以创建自定义 Enterprise DLP 数据模式来指定哪些内容是敏感的并且需要保护 - 这就是您要筛选的内容。您可以根据正则表达式创建自定义数据模式，或者根据文件属性创建数据模式。

- 创建数据模式的方法如下

STEP 3 | 创建数据配置文件

将应该以相同方式强制执行的数据模式分组到数据配置文件中。您还可以使用数据配置文件来指定匹配的其他匹配条件和置信度级别。

- 创建数据配置文件的方法如下

STEP 4 | 创建 DLP 规则

指定您希望 Enterprise DLP 保护的流量和文件类型。设置 Enterprise DLP 在检测到 DLP 事件时要执行的操作。

- 创建 DLP 规则的方法如下

管理：SaaS Security

在何处可以使用？	需要提供什么？
• Prisma Access （利用 *Strata Cloud Manager* 或 *Panorama* 配置管理）	❑ Prisma Access 许可证

使用 SaaS Security Inline 识别经批准和未经批准的应用程序中基于云的威胁和有风险的用户活动。

SaaS Security Inline 内置于 Cloud Managed Prisma Access 中，可为您提供网络和 CASB 安全的集中视图。它提供 SaaS 可视性（包括高级分析和报告），以便您的组织能够洞察网络上经批准和未经批准的 SaaS 应用程序使用的 Data Security 风险。

云访问安全代理 (CASB) 捆绑包括 SaaS Security Inline、Enterprise Data Loss Prevention (DLP) 内联、SaaS Security API、Data Loss Prevention (DLP) API 和 SaaS Security Posture Management (SSPM)。

新一代云访问安全代理 (CASB-X) 许可证包含所有 CASB 组件，例如 SaaS Security Inline、SaaS Security API、SaaS Security Posture Management (SSPM) 和 Enterprise DLP。它可以应用于单租户环境中的云管理 Prisma Access、Panorama 管理 Prisma Access 和 Panorama 管理新一代防火墙 (NGFW) 设备。

以下是使用 **SaaS Security** 所需了解的一切***Strata Cloud Manager***。

入门

以下是在 Prisma Access Cloud Management 上启动和运行 SaaS Security Inline 的方法：

确认您的 Prisma Access 订阅中包含 SaaS Security 附加许可证。

转到 **Manage**（管理） > **Configuration**（配置） > **Overview**（概览），以便检查使用您的许可证可访问的功能。

如果您还没有激活，请在中心上激活 SaaS Security Inline 应用程序。

激活后，SaaS Security Inline 会自动发现所有 SaaS 应用程序和用户，并从存储在以下位置的 Prisma Access 日志中分析用户的 SaaS 活动和使用情况数据：Strata Logging Service。

审查和管理管理员角色和访问权限。

转到 **Settings**（设置） > **Identity and Access**（身份和访问权限），以便在 Prisma Access Cloud Management 中提供对 SaaS Security 控件的基于角色的访问权限。

为了全面管理 *SaaS Security*，用户还必须是 *SaaS Security Inline* 应用程序的管理员。从 *Prisma Access* 云管理指示板直接跳转到 ***SaaS Security*** 控制台，以便添加 *SaaS Security Inline* 管理员。

探索 Prisma Access Cloud Management 中的 **SaaS Security** 指示板。

转至 **Manage**（管理） > **Configuration**（配置） > **Security Services**（安全服务） > **SaaS Security**（**SaaS Security**）。

Prisma Access Cloud Management 直接支持所有指示板视图 。检查这些视图以识别有风险的 SaaS 应用程序和用户以及 SaaS Security Posture Management。SaaS Security Posture Management (SSPM) 通过持续监控帮助检测和补救受制裁的 SaaS 应用程序中的错误配置设置。

审查并分享 SaaS Security 报告。

SaaS Security Inline 包含一个 SaaS Security 报告，该报告提供了带有高级聚合数据和视图的应用程序使用情况快照。该报告可作为您的 SaaS Security 团队和执行管理层之间的沟通工具。您可以与您的 SaaS Security 团队共享此按需 PDF 报告以进行定期检查，或者通过电子邮件将报告发送给您的高管，以突出显示组织中正在使用的 SaaS 应用程序及其带来的安全风险。

- 有关 SaaS Security 报告的更多信息
- 以下是如何在 SaaS Security Inline 应用程序中生成 SaaS Security 报告

了解 SaaS Security 和 Prisma Access Cloud Management 还有哪些功能。

SaaS 策略建议

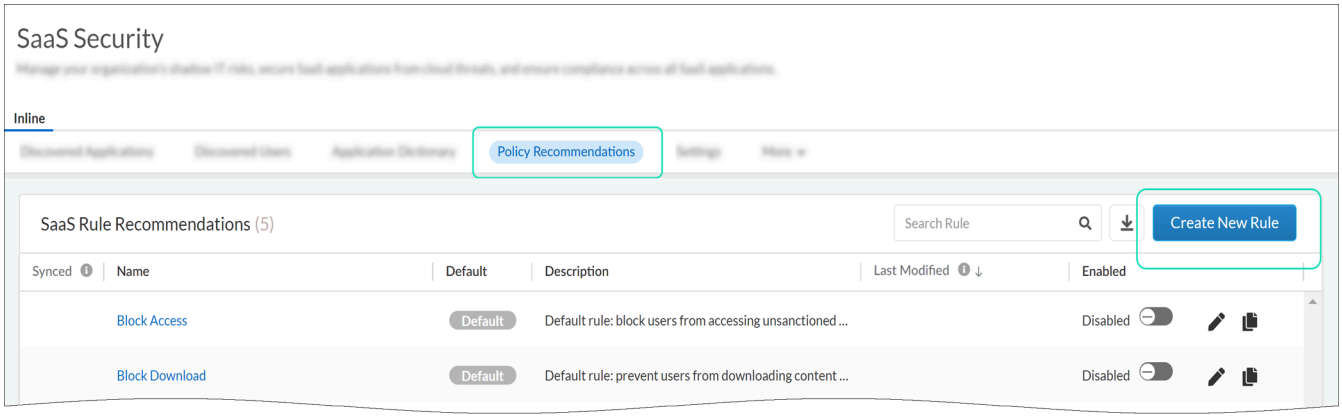
为了获得对 SaaS 应用程序的可见性和控制，SaaS Security 管理员使用 App-ID 云引擎 (ACE) 提供的特定 SaaS App-ID 创建 SaaS 规则建议。

在 Prisma Access Cloud Management 中，您现在可以查看并选择接受 SaaS Security 管理员推荐的规则。SaaS 规则建议已添加到您的 Web 访问策略中 — 您必须启用 Web Security 才能利用 SaaS 规则建议。

您可以按照以下方式开始操作 — 查看此处的工作流程以审核并接受 **SaaS** 政策建议：

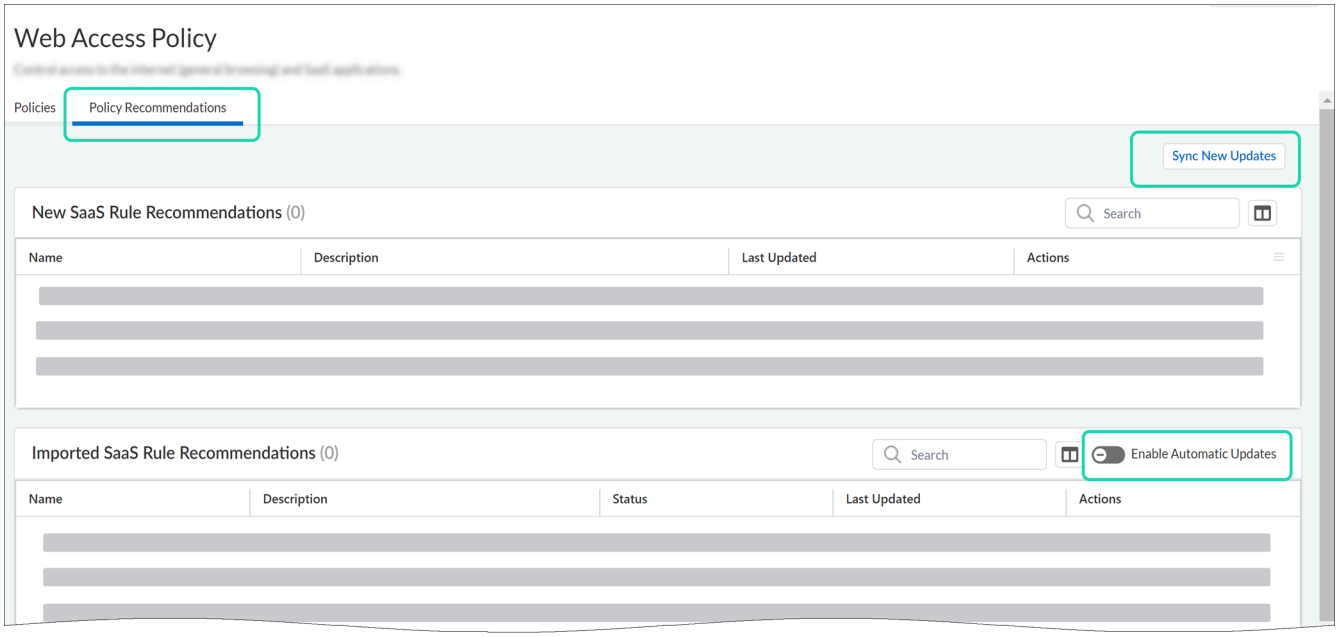
1. SaaS Security 管理员在 SaaS Security Inline 应用程序中或直接在 Prisma Access Cloud Management 中创建 SaaS 规则建议。

   # 在 Prisma Access Cloud Management 中，转到 **Manage**（管理） > **Configuration**（配置） > **Security Services**（安全服务） > **SaaS Security**

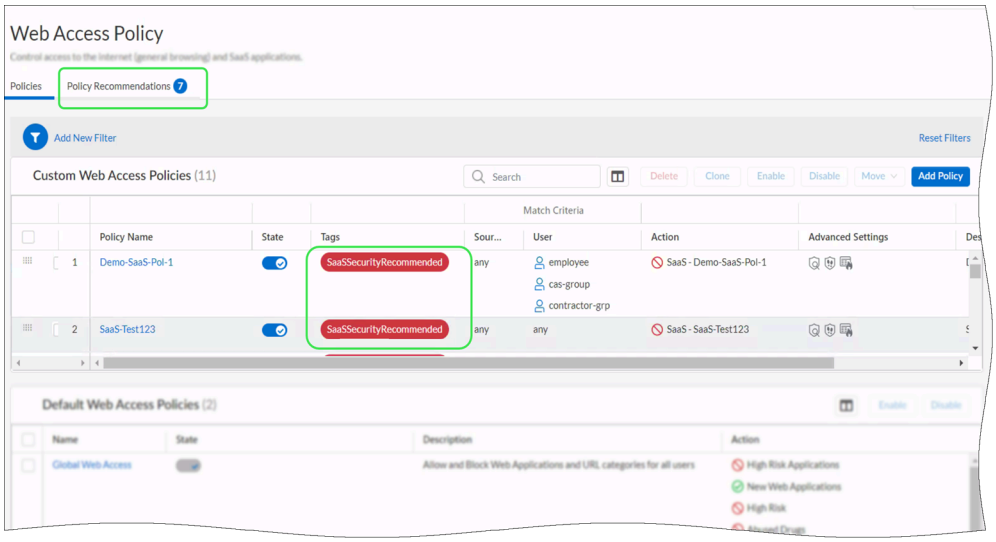


2. 您可以查看并导入 SaaS 规则建议。

   # 转到 **Manage**（管理） > **Web Security**（**Web** 安全） > **Web Access Policy**（**Web** 访问策略）



3. 您导入的 SaaS 规则建议已加标签，以便您可以轻松识别它们。



管理：Prisma SD-WAN

在何处可以使用？	我需要什么？
• Prisma SD-WAN	❑ Prisma SD-WAN 许可证

Prisma SD-WAN 提供软件定义的广域网 (SD-WAN) 解决方案，将传统广域网 (WAN) 转变为彻底简化、安全的应用程序结构 (AppFabric)，将异构底层传输虚拟化为统一的混合 WAN。系统的核心是应用性能引擎。

您可以查看细粒度的应用程序驱动分析，构建强大的策略和基于性能的 WAN 流量管理。通过即时网络 (ION) 设备，Prisma SD-WAN 简化了 WAN 的设计、构建和管理方式，将数据中心级安全性安全地扩展到网络边缘。

Prisma SD-WAN 支持流转发操作的堆叠策略。使用集中定义的策略，每个 ION 设备执行自动路径选择、流量整形或链路间主动-主动负载平衡等操作，而 Prisma SD-WAN 控制器则提供所有 WAN 链路上应用程序性能和响应时间的全面可见性。

Prisma SD-WAN 根据应用程序性能服务水平协议 (SLA) 和业务优先级来控制网络应用程序性能。您可以为使用 Strata Cloud Manager 的 Prisma SD-WAN 配置策略、资源、CloudBlades 和系统设置。

选择 **Manage**（管理） > **Prisma SD-WAN** 来管理以下配置：

- 策略
- 资源
- CloudBlades
- 系统

管理：Prisma SD-WAN 的策略

在何处可以使用？	需要提供什么？
• Prisma SD-WAN	❑ Prisma SD-WAN 许可证

Prisma SD-WAN 支持堆叠策略和原始策略。每台 ION 设备使用集中定义的策略执行诸如自动路径选择、流量整形或链路之间的主动-主动负载平衡等操作，而通过 Prisma SD-WAN 控制器则可以全面了解所有 WAN 链路上的应用程序性能和响应时间。

使用 Strata Cloud Manager 配置 Prisma SD-WAN 中的策略。

STEP 1 | 选择 **Manage**（管理） > **Prisma SD-WAN** > **Policies**（策略）。

您可以在 Prisma SD-WAN 中配置以下类型的策略：

- 路径

  为流量转发和流量整形操作配置堆叠路径策略

  。
- 性能

  配置性能策略以衡量应用程序性能和应用程序 SLA

  。
- QoS

  配置堆叠 QoS 策略以指定业务优先级。
- 安全

  配置堆叠式安全策略以定义确定分支机构内应用程序访问权限的规则。
- NAT

  配置堆叠式 NAT 策略，确保连接到公共或私有网络的内部网络的隐私

  。
- 安全（原始）

  这些是传统的安全策略。如果您是从 ION 设备软件版本 6.0.1 开始的新用户，则只能配置堆叠式安全策略。如果您配置了原始策略或旧版策略，则必须先将这些旧策略转换为堆叠策略，然后才能将设备升级到版本 6.0.1。
- 网络（原始）

  这些是传统的网络策略。如果您是从 ION 设备软件版本 6.0.1 开始的新用户，则只能配置堆叠网络策略。如果您配置了原始策略或旧版策略，则必须先将这些旧策略转换为堆叠策略，然后才能将设备升级到版本 6.0.1。

STEP 2 | 选择 **Bindings**（绑定）以将策略堆栈绑定到站点。

为了使路径、QoS、安全和 NAT 堆栈中的策略规则生效，必须将策略堆栈绑定到站点。一次只能将单个路径、QoS、安全和 NAT 堆栈绑定到一个站点。

管理：Prisma SD-WAN 的资源类型

在何处可以使用？	需要提供什么？
• Prisma SD-WAN	❑ Prisma SD-WAN 许可证

您可以在 Prisma SD-WAN 中管理不同类型的资源。

使用 Strata Cloud Manager 管理 Prisma SD-WAN 中的资源。

选择 **Manage**（管理） > **Prisma SD-WAN** > **Resources**（资源）。

在 Prisma SD-WAN 中可以管理以下类型的资源：

- 应用程序

  应用程序是 Prisma SD-WAN 解决方案的核心。网络中部署的 ION 设备会主动分析每个应用程序流，以确保维护性能、合规性和安全性策略，并为每个流使用最佳网络连接。ION 设备使用应用程序定义和指纹技术进行路径选择、QoS 和防火墙策略。

  系统应用程序默认可用，但您可以根据企业需求配置自定义应用程序。

- 电路类别

  电路类别是网络中可能存在的各种电路和连接的逻辑分组。这种分组允许简化和可重复使用整个网络的网络策略规则。例如，互联网有线宽带、计量互联网 LTE 链路、卫星互联网链路、互联网 DSL 或私有 MPLS。

- 网络环境

  网络环境对网络流量进行分段，以便对同一应用程序应用不同的网络策略规则。具有网络上下文的规则始终优先于没有网络上下文的规则。您可以创建一个或多个网络环境，但单个 LAN 网络只能属于一个网络环境。必须将网络环境附加到适当的 LAN 段才能有效。

- 服务与 DC 组

  使用服务和 DC 组将第三方端点映射到组，以便在创建网络策略规则时具有灵活性，可以解决跨站点的唯一性。其目的是无论站点位置如何，策略规则都保持不变。

- 安全服务区

  安全服务区指定了对流量进行检查和筛选的强制边界。每个安全服务区映射到与设备的物理接口、逻辑接口或子接口连接的网络。这些服务区级接口充当物理电路和虚拟电路（例如 VLAN、第 3 层 VPN 和第 2 层 VPN 电路）的代理。

- 模板

  站点配置模板可帮助您创建满足部署要求的定制站点模板，让您轻松高效地大规模部署分支机构和数据中心。使用此模板，您可以部署多个站点。您可以使用现有模板、编辑现有模板或创建新模板来部署多个站点。

- 前缀筛选器

  前缀是一个或多个单独的 IP 地址或 IP 地址子网的组。前缀与路径集策略和优先级策略一起使用。它们的范围可以是全球性的，也可以是本地性的。

- 配置文件

  使用配置文件来配置不同类型的资源的设置。

  - IPsec

    创建 IPsec 配置文件以配置分支设备和云安全服务端点之间的 IPsec VPN 连接。
  - IPFIX

    IPFIX 配置文件是一个全局 IPFIX 配置对象，它标识收集器配置、筛选器配置、导出流信息元素的模板和流采样器配置。
  - 创建接入点网络 (APN)

    创建接入点名称 (APN) 配置文件来定义蜂窝数据连接的网络路径。需要 APN 信息才能连接到蜂窝网络。
  - DNS

    配置域名系统 (DNS) 配置文件以指定 DNS 服务的配置参数。常配置的参数包括DNS服务器、域到地址映射、缓存配置、DNSSEC 配置。DNS服务配置文件创建后，绑定到设备。
  - NTP 模板

    使用网络时间协议 (NTP) 配置模板来添加或编辑 NTP 服务器。
  - 多播

    创建 WAN 多播配置配置文件并将其与分支站点关联，以便为分支站点启用多播 WAN 多播路由。
  - VRF

    创建并关联全局（默认）虚拟路由和转发表 (VRF) 配置文件并将其分配给所有分支机构和数据中心站点。
  - IoT 发现

    使用 IoT 设备可见性来识别网络中的设备。Prisma SD-WAN 分支 ION 设备检查数据包、提取信息并生成要以特定的格式发送到 Strata Logging Service 的消息。

管理：适用于 Prisma SD-WAN 的 CloudBlades

在何处可以使用？	需要提供什么？
• Prisma SD-WAN	❑ Prisma SD-WAN 许可证 ❑ 相应 CloudBlade 的 CloudBlade 许可证

使用 Prisma SD-WANCloudBlade 平台可安全访问 ION 设备，使用定制模板自动化 Web 界面工作流程，从而降低操作复杂性。

使用 Strata Cloud Manager 在 Prisma SD-WAN 中配置 CloudBlades。

选择 **Manage**（管理） > **Prisma SD-WAN** > **CloudBlade**。

您可以查看在 Prisma SD-WAN 中已订阅的 CloudBlades。按照相关 CloudBlade 集成指南中的步骤配置您的 CloudBlade。

管理：Prisma SD-WAN 的系统资源

在何处可以使用？	需要提供什么？
• Prisma SD-WAN	❑ Prisma SD-WAN 许可证

使用 **System**（系统）选项卡下的可用资源管理和监视 Prisma SD-WAN 中的用户和权限。

选择 **Manage**（管理） > **Prisma SD-WAN** > **System**（系统）。

您可以在 Prisma SD-WAN 中配置以下类型的系统资源：

- 许可证管理

  使用许可证管理生成虚拟 ION 的身份验证令牌。这提供了一组控制，以防止未经授权向环境中添加虚拟设备。

- 审计日志

  使用审计日志查看系统中的配置更改记录。您可以将这些日志用于合规性和故障排除目的。审核日志提供诸如所做的更改、更改的所有者、更改时间以及站点、系统或站点子集的更改范围等信息。

- 企业前缀

  凭借企业前缀，Prisma SD-WAN 数据中心站点可以轻松将路由和可达性传递到分支机构站点。

- **Access Management**（访问管理）
  - User Access（用户访问）
    - User Management（用户管理）

      根据企业的要求，添加具有系统角色的新用户。系统角色是每个角色的预定义权限集。这些角色包括一个或多个系统权限的集合。可用的系统角色包括根、超级管理员、IAM 管理员、网络管理员、安全管理员和仅查看用户。
    - 自定义角色

      您可以通过不同方式组合现有系统角色和权限来构建自定义角色。您可以通过组装一组系统权限或通过添加或删除系统角色的权限来创建它们。
    - 密码要求

      设置密码的字符和安全要求。您还可以设置重复使用旧密码和刷新密码的频率。
  - 设备访问权限
    - 设备工具包用户访问权限
    - 设备离线访问策略
  - 租户访问权限
    - 身份验证令牌

      配置身份验证令牌以访问 Prisma SD-WAN API。为用户生成令牌后，它可用于重复进行 API 调用，从而消除访问 API 的不必要登录。

      有权访问身份验证令牌的用户可以访问分配给令牌的所有权限。

      选择 **Manage**（管理） > **System**（系统） > **Tenant Access**（租户访问权限） > **Auth Tokens**（身份验证令牌） > **Create Auth Token**（创建身份验证令牌），以便创建身份验证令牌。
  - 身份管理
    - Cloud Identity Engine

管理：Prisma Access Browser

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Access 许可证

从 Strata Cloud Manager 中，选择 **Manage**（管理） > **Configuration**（配置） > **Prisma Access Browser**。

Prisma Access Secure Enterprise Browser (Prisma Access Browser) 是唯一通过本机集成的企业浏览器来保护托管和非托管设备的解决方案，可将保护扩展到非托管设备。参阅什么是 Prisma Access Browser？

主页

主页是您从 Strata Cloud Manager 访问 Prisma Access Browser 时的登录页面。从主页可以使用 Prisma Access Browser 指示板，以便从用户行为和浏览数据分析中获得有意义的见解。有多种指示板可用于监控您可能想要监控的特定用例，例如用户行为、数据泄露预防、网络安全和策略。每个指示板都包含一组小部件，并且一些小部件会出现在多个指示板中。

Analytics

Prisma Access Browser 事件屏幕是调查企业浏览器部署中的每个活动的关键可见性工具，以验证策略和规则是否正常运行。这是调查 Prisma Access Browser 事件的位置。

目录

- 用户目录是有关用户及其 Prisma Access Browser 连接设备、用户组成员资格以及相关策略规则的信息的中心位置。管理 Prisma Access Browser 用户
- 设备目录提供了 Prisma Access Browser 设备和设备组的名册。管理 Prisma Access Browser 设备
- Prisma Access Browser 配备了预先存在的已验证应用程序列表。已验证的应用程序列表引用了 Palo Alto Networks App-ID™ 应用程序目录，并定期与云数据库同步。您还可以创建自定义和私人应用程序。管理 Prisma Access Browser 应用程序
- Prisma Access Browser 维护一个扩展目录，其中包含最终用户在浏览器上安装的扩展。这些信息可让您维护适当的公司策略管理、管理可见性和风险分析。管理 Prisma Access Browser 扩展

策略

- 您可以使用规则来指定将受各种策略影响的用户、用户组和设备组。这些规则控制对 Web 应用程序、安全策略和自定义选项的访问。通过利用规则，您可以精确控制用户对组织工具和组件的访问。管理 Prisma Access Browser 策略规则
- Prisma Access Browser 规则的控件可以在单个规则的主体内配置规则。当您想要保存可重复使用（旧版）的配置文件并稍后将其添加到规则中时，可以使用配置文件（外部控制）。管理 Prisma Access Browser 策略配置文件
- 使用登录规则确定哪些用户和设备有权访问 Prisma Access Browser。管理 Prisma Access Browser 登录规则
- 在策略规则中定义绕过条件后，当用户尝试执行操作或访问被相应规则阻止的站点时，可以提交绕过请求。要设置绕过条件，您可以配置提示操作以启用权限请求。管理 Prisma Access Browser 请求以绕过策略规则。

管理

使用以下方式管理集成以获得附加功能：

- Microsoft 365
- Microsoft Information Protection
- Google Workspace
- Votiro
- CrowdStrike Falcon Intelligence
- OPSWAT MetaDefender
- YazamTech SelectorIT
- Symantec DLP

管理：操作

在何处可以使用？	需要提供什么？
• Prisma Access （利用 *Strata Cloud Manager* 或 *Panorama* 配置管理） • NGFW，包括由 软件 NGFW 积分提供资助的项目	❑ 使用 Strata Cloud Manager 管理您的配置，至少需要其中一个许可证；要统一管理 NGFW 和 Prisma Access，您需要两个许可证： ❑ Prisma Access 许可证 ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → Strata Cloud Manager 中为您提供的特性和功能取决于您使用的是哪个 许可证。

使用 Strata Cloud Manager 推送配置更改、查看过去的配置推送以及管理配置版本快照以加载或恢复到以前的配置版本的操作。

- 推送配置更改
- 查看配置推送的状态
- 了解如何清理配置

管理：推送配置

在何处可以使用？	需要提供什么？
• Prisma Access （利用 *Strata Cloud Manager* 或 *Panorama* 配置管理） • NGFW，包括由 软件 NGFW 积分提供资助的项目	❑ 使用 Strata Cloud Manager 管理您的配置，至少需要其中一个许可证；要统一管理 NGFW 和 Prisma Access，您需要两个许可证： ❑ Prisma Access 许可证 ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → Strata Cloud Manager 中为您提供的特性和功能取决于您使用的是哪个 许可证。

完成配置更改并准备激活它们后，您必须将更改推送到防火墙。您可以选择推送所有配置更改或选择特定管理员进行推送。首次推送配置时，需要所有管理员推送更改。您可以选择要推送到 Prisma Access 的配置更改：

- **Web** 安全

  将 Web 安全更新推送至 Prisma Access。
- 移动用户 — **GlobalProtect**

  将 Global Protect 更新推送至 Prisma Access。
- 移动用户 — 显式代理

  将显式代理更新推送至 Prisma Access。
- 远程网络

  将远程网络更新推送至 Prisma Access。
- 服务连接

  将服务连接更新推送至 Prisma Access。

您可以在正在推送另一个配置时推送一个配置。Prisma Access 按照您提交的顺序应用配置更改。

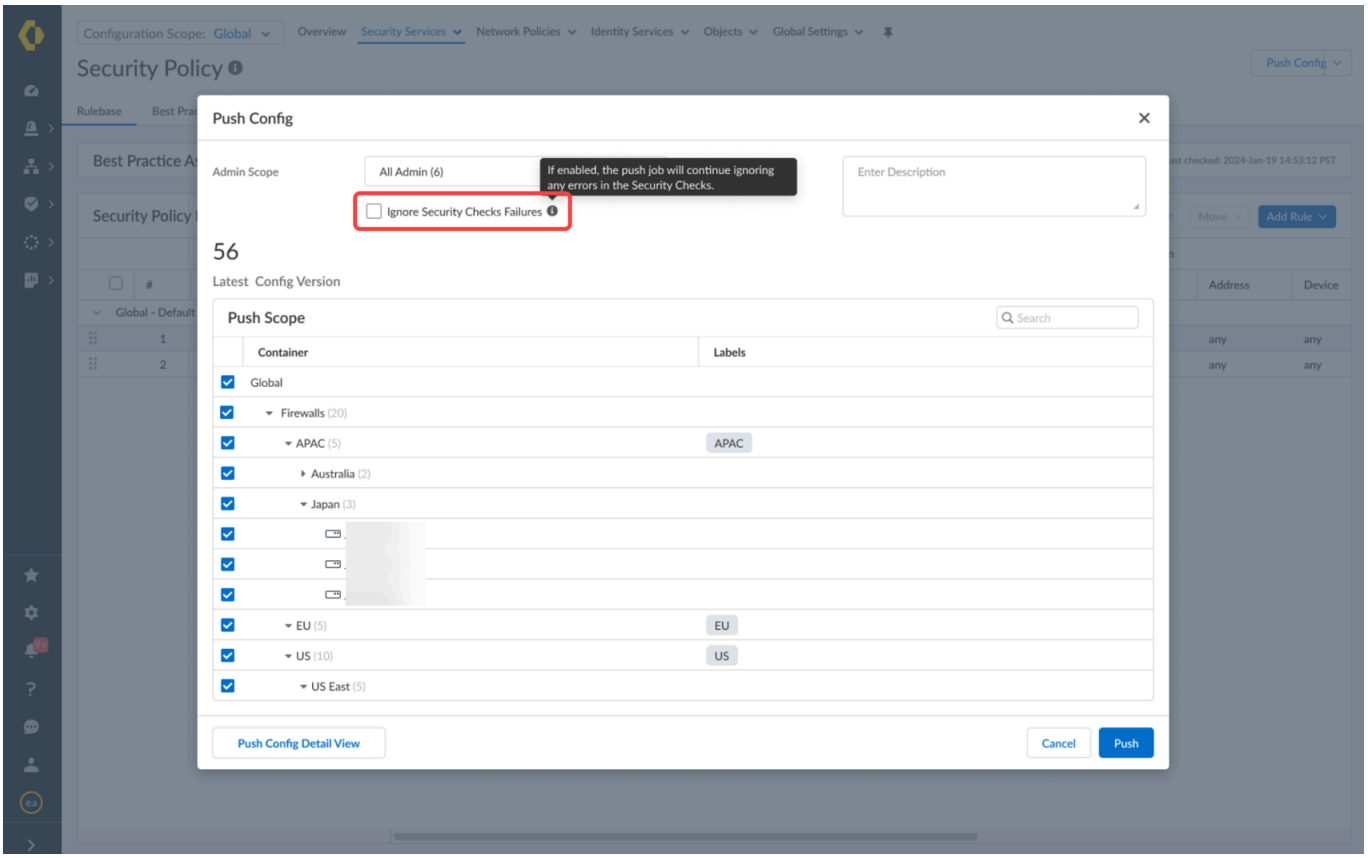
如果配置推送错误，或者更改导致网络或安全中断，您可以将 Prisma Access 配置恢复为最新运行的 Prisma Access 配置。这使您可以将 Prisma Access 配置恢复到您知道可以正常运行且不会危及网络安全的运行配置。您无法选择特定的运行配置。Prisma Access 会自动选择最后已知的运行配置并恢复到该配置。

STEP 1 | 登录 Strata Cloud Manager。

STEP 2 | 根据需要更改配置。

STEP 3 | **Push Config**（推送配置）并 **Push**（推送）您的配置更改。

或者，您可以选择 ***Manage***（管理） **> *Operations***（操作） **> *Push Config To Devices***（将配置推送到设备）。



在 **Push Config**（推送配置）对话框中，您可以 **Ignore Security Check Failures**（忽略安全检查失败）。即使某些检查会阻止该过程，此功能仍允许您继续推送操作。如果您未选中该复选框（默认设置），并且使用“阻止”操作的最佳实践检查失败，则 Strata Cloud Manager 将停止推送。

STEP 4 | （可选）**Add New Filter**（添加新筛选器）。

您可以通过应用筛选器来筛选推送范围内显示的设备。应用筛选器只会影响推送范围内显示的防火墙或 Prisma Access 部署，而不会影响您推送到的设备。

STEP 5 | 编辑推送范围。

编辑推送范围允许您将有针对性的配置更改推送到部分或全部防火墙或 Prisma Access 部署。

在以下情况下，不支持执行部分配置推送，并您必须推送整个 *Strata Cloud Manager* 配置：

- 配置一个新的租户，这是您的第一次推送配置。
- 将防火墙加入到 *Strata Cloud Manager*。
- 加入 *Prisma Access* 移动用户和远程用户。
- 重命名或移动文件夹，以便其嵌套在其他文件夹下。
- 将防火墙移至不同的文件夹。
- 重命名、关联或取消关联代码段。
- 加载配置。
- 将配置恢复为最后推送的配置或以前的配置版本快照。

- **Admin Scope**（管理员范围）— 选择要在推送中包含的管理员配置更改。默认情况下，管理范围选择当前用户，并且该用户所做的更改将推送到选定的防火墙或 Prisma Access 部署。选择 **Changes from all admins**（所有管理员的更改）包含所有管理员执行的所有配置更改。

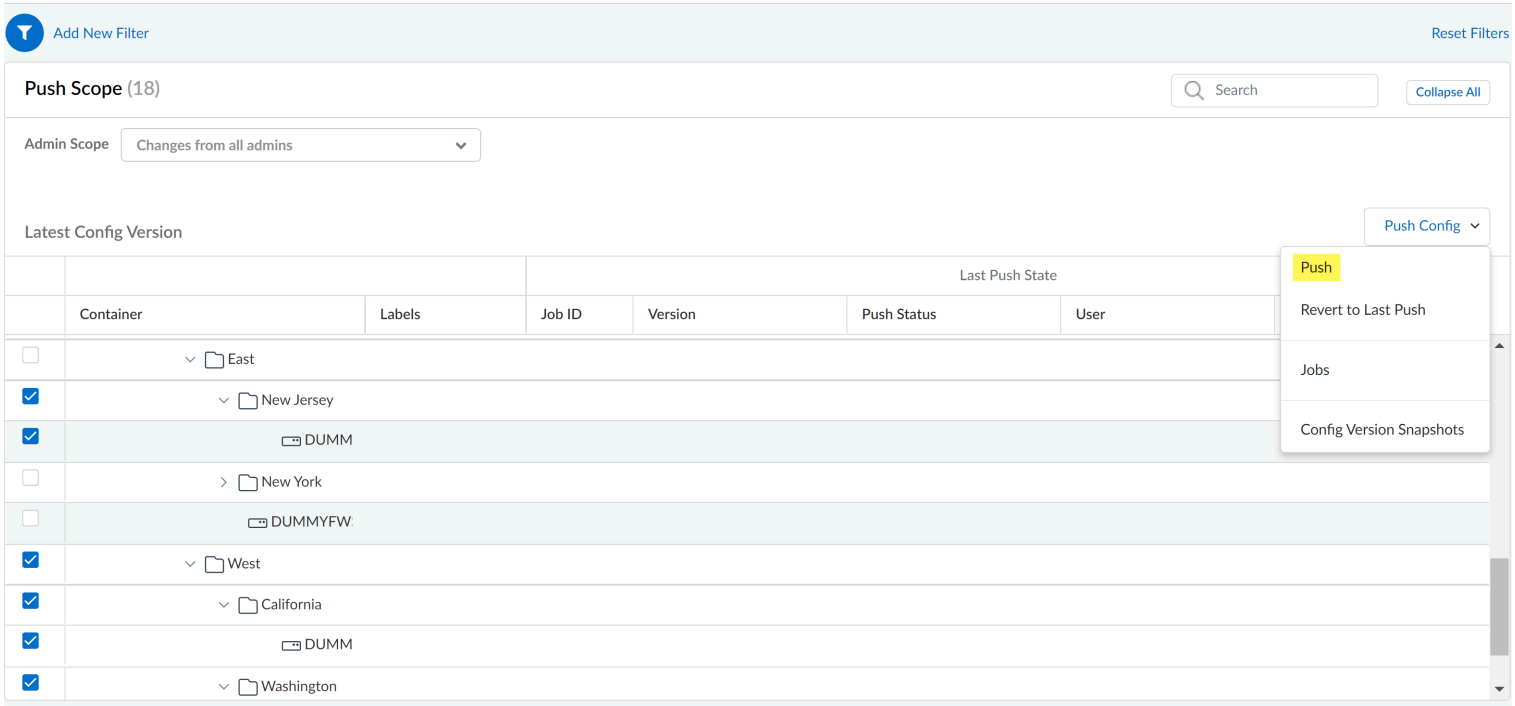
  编辑管理范围以选择特定管理员包括选定管理员所做的所有配置更改。执行第一次配置推送时不能使用此选项。不支持选择要包含在推送中的特定配置更改。

- **Push Scope**（推送范围）— 选择要推送到的部署类型或文件夹。当您选择部署或文件夹时，配置更改将被推送到所有防火墙或部署。

  当您选择包含子文件夹的文件夹时，所有子文件夹和相关的防火墙或 Prisma Access 部署都将包含在推送中。选择特定的防火墙或 Prisma Access 部署会自动选择与其关联的文件夹。

STEP 6 | **Push Config**（推送配置）并 **Push**（推送）。

查看推送目标并 **Push**（推送）。



STEP 7 | 检查配置推送状态。

如果配置推送错误，或者更改导致网络或安全中断，您可以恢复 Prisma Access 配置。

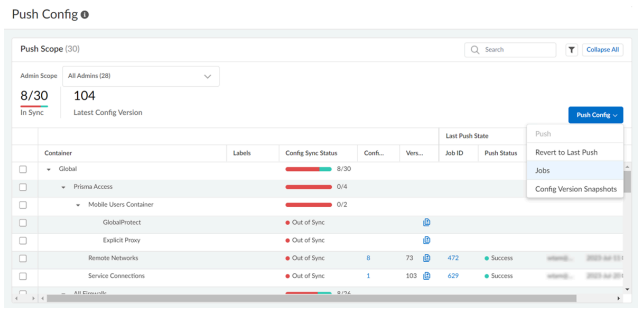
恢复、加载和比较配置版本

查看 Prisma Access 作业

您可以在 Prisma Access 上查看 **Jobs**（作业）历史记录，以显示管理员发起的操作的详细信息，以及自动更新内容和许可证。这包括任何配置提交、推送和恢复。您可以使用“作业”视图来排除失败的操作故障、调查与已完成提交相关的警告或取消待处理的提交。

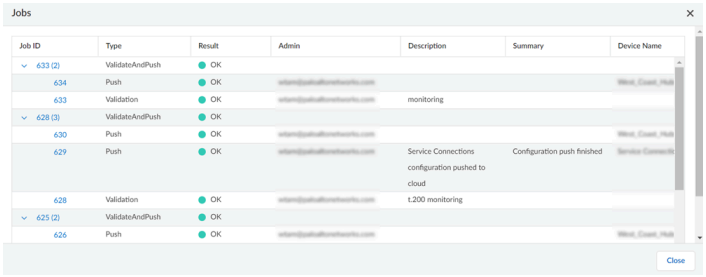
STEP 1 | 启动 Prisma Access。

STEP 2 | 在顶部菜单栏上，选择 **Push Config**（推送配置），并查看 Prisma Access **Jobs**（作业）。



STEP 3 | 执行以下任一任务：

- 调查警告或故障 — 阅读摘要列中的条目以了解警告或故障详细信息。
- 查看提交描述 — 如果管理员输入了提交描述，您可以参考描述列以了解提交的目的。
- 检查队列中的操作位置 — 查看操作位置和状态以确定操作的位置。



管理：推送状态

在何处可以使用？	需要提供什么？
• Prisma Access （利用 *Strata Cloud Manager* 或 *Panorama* 配置管理） • NGFW，包括由 软件 NGFW 积分提供资助的项目	❑ 使用 Strata Cloud Manager 管理您的配置，至少需要其中一个许可证；要统一管理 NGFW 和 Prisma Access，您需要两个许可证： ❑ Prisma Access 许可证 ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → Strata Cloud Manager 中为您提供的特性和功能取决于您使用的是哪个 许可证。

查看您过去向防火墙推送的配置的推送状态，以查看推送操作结果、发起推送的管理员以及目标防火墙等详细信息。

STEP 1 | 登录 Strata Cloud Manager。

STEP 2 | 推送您的配置更改。

STEP 3 | 选择 **Manage**（管理） > **Operation**（操作） > **Push Status**（推送状态），并找到您想要查看的配置推送操作。

STEP 4 | 展开您要查看的配置推送的 `Job ID`。

在发生任何配置推送之前，始终会执行配置 `Validation` 作业。当您推送到多个防火墙时，每个配置推送都有一个带有推送详细信息的唯一 `Job ID`。

STEP 5 | 查看有关配置推送状态的详细信息。

例如，查看推送 `Result`、发起配置推送的 `Admin`、配置推送 `Summary`、以及配置推送的 `End Time` 和 `Start Time`。

如果推送成功，则配置推送 `Result` 为 `OK`；如果推送失败，则配置推送结果为 `FAIL`。

STEP 6 | 单击推送至防火墙的配置的唯一 `Job ID` 可查看作业详细信息。

作业详细信息提供有关执行配置推送时遇到的 `Warnings` 和 `Errors` 的详细信息。例如，如果推送到防火墙失败，您可以查看作业详细信息以了解导致配置推送失败的原因。

管理：配置版本快照

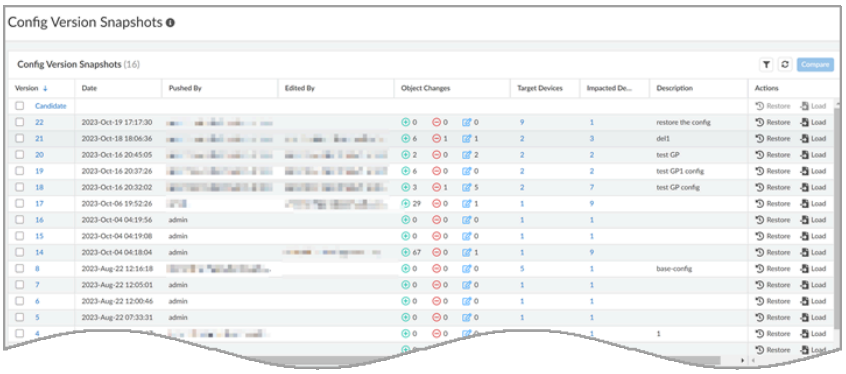
在何处可以使用？	需要提供什么？
• Prisma Access （利用 *Strata Cloud Manager* 或 *Panorama* 配置管理） • NGFW，包括由 软件 NGFW 积分提供资助的项目	❑ 使用 Strata Cloud Manager 管理您的配置，至少需要其中一个许可证；要统一管理 NGFW 和 Prisma Access，您需要两个许可证： ❑ Prisma Access 许可证 ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → Strata Cloud Manager 中为您提供的特性和功能取决于您使用的是哪个 许可证。

通过配置快照，您可以查看 Strata Cloud Manager 配置历史记录。当配置推送产生意想不到的安全隐患或对流量产生意外影响时，您可以通过恢复到早期版本来进行恢复。您还可以比较配置以查看不同版本的变化。

配置快照概述

配置快照版本屏幕是查看推送的配置，将配置快照与候选配置进行比较，以及加载或恢复旧配置的地方。

选择 **Manage**（管理） > **Operations**（操作） > **Config Version Snapshots**（配置版本快照），以查找配置快照并恢复、加载或比较版本。



1. **Add New Filter**（添加新筛选器）— 选择筛选器以按列对配置版本进行排序和筛选。
2. **Version**（版本）— 推送的配置的版本号。

   利用候选版本，您可以将 Strata Cloud Manager 当前待处理的配置更改与以前的配置版本进行比较。

   配置版本号是递增的。例如，如果您有 *10* 个版本并恢复配置版本 *2*，则配置版本将从 *10* 更改为 *11*（而不会显示为 *2*）。

3. **Date**（日期）— 推送配置的日期和时间。
4. **Pushed By**（推送者）— 推送更改的管理员。
5. **Edited By**（编辑者）— 在推送配置更改之前进行配置更改的管理员。
6. **Object Changes**（对象更改）— 查看推送配置时添加、删除或修改了多少对象。
7. **Target Devices**（目标设备）— 配置推送快照范围内的目标设备。

   执行还原操作时，您可以选择要在哪些设备上执行操作。
8. **Impacted Devices**（受影响的设备）— 自上次推送配置以来已修改的设备。设备仅被视为受先前配置推送快照的影响。

   受影响设备和目标设备

   如果您有两台设备 *A* 和 *B*，并且仅推送到设备 *A*，则 *A* 将成为目标设备和受影响设备。

   如果您随后再次推送到设备 *A* 和 *B*，则 *A* 和 *B* 都是目标设备，但只有 *B* 是受影响的设备。

   执行加载操作时，列出的设备将受到影响。
9. **Description**（说明）— 查看推送配置时提供的任何信息。
10. **Refresh**（刷新）— 更新快照表中的信息。
11. **Reset Filters**（重置筛选器）— 清除所有筛选器以显示所有配置版本。
12. **Compare**（比较）— 查看版本间的变化。

    一次只能比较两个版本。
13. **Actions**（操作）— 您可以 **Restore**（恢复）或 **Load**（加载）配置版本。

    - **Restore**（恢复）— 恢复较早的配置版本。

      恢复配置版本会直接更新原始推送范围内部署的运行配置，不需要您推送配置。

      恢复配置推送原始范围内的所有设备或部署，或选择要恢复的特定设备或部署。您无法扩展配置以包括原始范围之外的设备或部署。

      恢复配置版本不会删除或修改候选配置。正在进行的配置将被保存。恢复配置只会更新正在运行的配置版本。使用还原操作时，部署可能会显示不同步。
    - **Load**（加载）— 在 Strata Cloud Manager 中加载早期版本作为候选配置。加载旧配置后，您当前的候选配置将丢失。

      更新新的候选配置，或将配置应用于原始配置快照之外的新设备和部署，准备就绪后，请 **Push Config**（推送配置）。
    - **Save**（保存）— 将候选配置保存为命名快照以用作已知配置。有了已知的配置，您就可以轻松地将部署置于已知且可行的状态。您可以在 **Named Snapshots**命名快照之间来回切换，并且自动记录 **Version Snapshots**（版本快照）中的配置推送。

Strata Cloud Manager 最多可保存 *6* 个月的快照或 *200* 个个人快照。

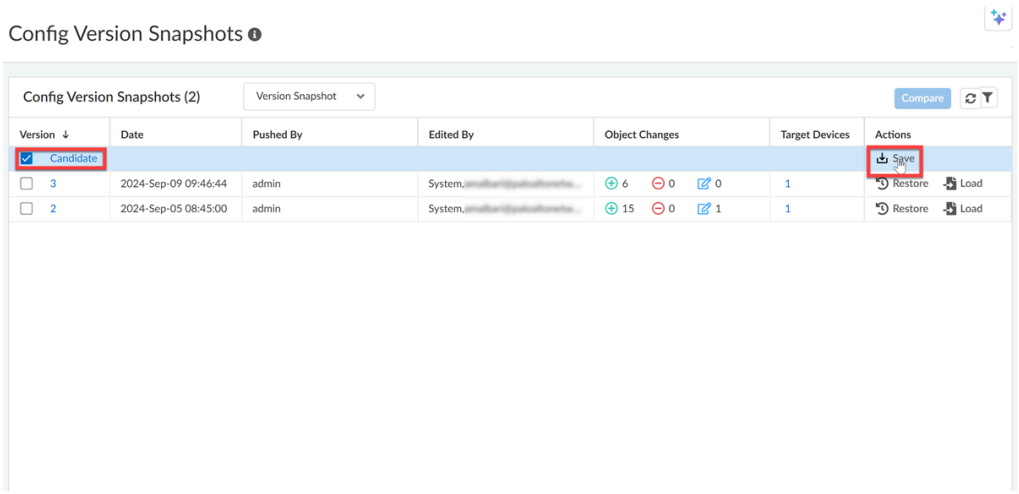
保存已命名快照

将当前候选配置另存为命名快照。您无法将部分配置保存为命名快照。保存命名快照允许您加载已知的配置状态，而不必跟踪最终将从配置版本快照表中循环删除的各个快照。

STEP 1 | 登录 Strata Cloud Manager。

STEP 2 | 选择 **Manage**（管理） > **Operations**（操作） > **Config Version Snapshots**（配置版本快照）。

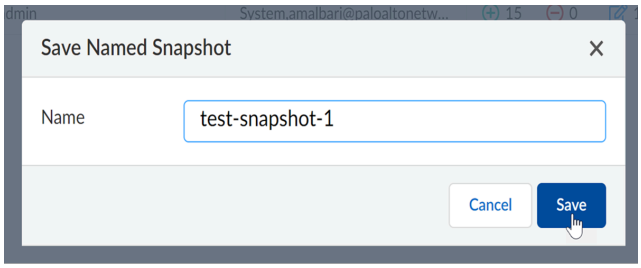
STEP 3 | 选择 **Candidate**（候选）。



STEP 4 | 单击 **Save**（保存）。

STEP 5 | 输入 **Name**（名称），最多 64 个字符。

快照名称将默认为 **config_year-month-day-timestamp**。

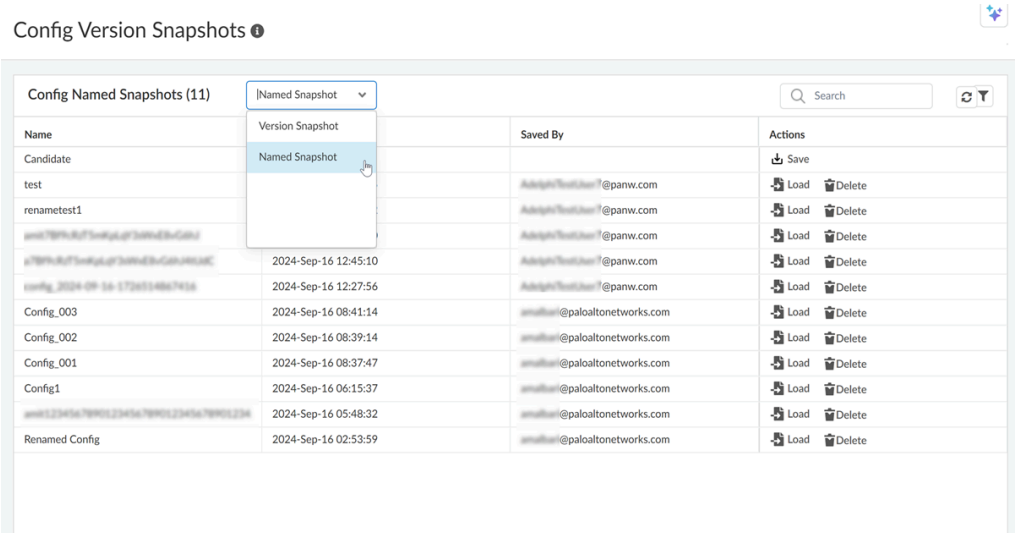


STEP 6 | **Save**（保存）您的快照。

STEP 7 | （可选）通过导航到配置版本快照表中的 **Named Snapshots**（已命名快照）来验证您的快照是否已保存。

管理已命名快照

管理员可以删除自己的已命名快照。超级用户可以删除所有已命名快照。



恢复快照

恢复之前推送的配置。恢复较旧的配置会更新部署和设备上运行的配置。这些更改未反映在 Strata Cloud Manager 中，因此部署和设备可能出现不同步。

只有在原始配置推送范围内的已配置设备才能恢复到选定版本。

STEP 1 | 登录 Strata Cloud Manager。

STEP 2 | 选择 **Manage**（管理） > **Operations**（操作） > **Config Version Snapshots**（配置版本快照）。

STEP 3 | 选择要恢复的配置版本。

1. （可选）选择版本号以查看配置快照所做的更改。

STEP 4 | **Restore**（恢复）版本。

1. （可选）选择要使用还原操作作为目标的设备。
2. **Restore**（还原）。

STEP 5 | （可选）选择 **Manage**（管理） > **Configuration**（配置） > **Operations**（操作） > **Push Config**（推送配置）以验证配置是否已恢复。

加载快照

加载较早的配置快照以用作候选配置。

加载配置后，您可以继续对其进行修改，然后再推送。

STEP 1 | 登录 Strata Cloud Manager。

STEP 2 | 选择 **Manage**（管理） > **Operations**（操作） > **Config Version Snapshots**（配置版本快照）。

STEP 3 | 选择要加载的配置版本。

1. （可选）选择版本号以查看配置快照所做的更改。

STEP 4 | **Load**（加载）版本。

STEP 5 | （可选）根据需要修改加载的候选配置。

STEP 6 | **Push Config**（推送配置）。

管理：安全态势

在何处可以使用？	需要提供什么？
• Prisma Access （利用 *Strata Cloud Manager* 或 *Panorama* 配置管理） • NGFW，包括由 软件 NGFW 积分提供资助的项目	❑ 使用 Strata Cloud Manager 管理您的配置，至少需要其中一个许可证；要统一管理 NGFW 和 Prisma Access，您需要两个许可证： ❑ Prisma Access 许可证 ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → Strata Cloud Manager 中为您提供的特性和功能取决于您使用的是哪个 许可证。

请使用这些工具来改善您的安全状况，并按照安全策略最佳实践验证您是否受到威胁保护。

- 为您的部署定制安全态势检查，以最大限度地提高管理：安全态势设置中的相关建议
- 使用配置清理来识别并删除未使用的配置对象和策略规则。
- 配置合规性检查来完善和优化过于宽松的安全规则，以便它们只允许网络中实际使用的应用程序。
- 创建您自己的 管理：安全态势设置 – 自定义现有的最佳实践检查并创建和管理特殊豁免，以更好地符合您组织的业务需求。
- 使用 Policy Analyzer 快速确保您对安全策略规则所做的更新符合您的要求，并且不会引入错误或错误配置（例如，导致规则重复或冲突的更改）。

管理：Policy Analyzer

在何处可以使用？	需要提供什么？
• NGFW（Panorama 托管） • VM-Series, funded with Software NGFW Credits（Panorama 托管） • Prisma Access (Managed by Panorama)	❑ 至少需要以下许可证之一： ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Pro ❑ 用于 Panorama 托管部署的 Panorama 云连接器插件

对安全策略规则的更新通常在时间上很敏感，需要您迅速采取行动。但是，您希望确保对安全策略规则库所做的任何更新都符合您的要求，并且不会引入错误或错误配置（例如，导致规则重复或冲突的更改）。

为了实现这一目标，Strata Cloud Manager 中的 Policy Analyzer 使您能够在实施更改请求时优化时间和资源。Policy Analyzer 不仅可以分析特定规则的可能合并或删除并提供建议以满足您的意图，还可以检查规则库中的异常情况，如阴影、冗余、泛化、关联和合并。

使用 Policy Analyzer 添加或优化安全策略规则库。

- 添加新规则之前 — 检查是否确实需要添加新规则。Policy Analyzer 建议如何最好地更改现有安全策略规则，以满足您的要求，如果可能的话，无需添加其他规则。
- 简化并优化您现有的规则库 — 找出可以更新规则的机会，最大限度地减少规则库膨胀并消除冲突，并确保流量强制执行与安全策略规则库的意图保持一致。

在提交更改之前和之后都要分析您的安全策略规则。

- 变更前策略分析 — 能够评估新规则的影响，并根据现有规则分析新规则的意图，以就如何最好地满足意图给出建议。
- 变更后策略分析 — 通过识别逐渐积累的遮蔽、冗余和其他异常，从而清理现有的规则库。

请参阅 Policy Analyzer，以了解更多信息。

管理：策略优化器

在何处可以使用？	需要提供什么？
• Prisma Access （利用 *Strata Cloud Manager* 或 *Panorama* 配置管理） • NGFW，包括由 软件 NGFW 积分提供资助的项目	❑ 使用 Strata Cloud Manager 管理您的配置至少需要其中一个许可证；对于 NGFW 和 Prisma Access 的统一管理，您同时需要两个许可证： ❑ Prisma Access 许可证 ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Pro → Strata Cloud Manager 中提供的功能取决于您使用的 许可证。

趁着策略优化器还处于早期试用阶段，赶紧尝试一下。如果您有兴趣在早期访问期之后继续使用此功能，请与您的客户团队联系。

过于宽泛的规则会带来安全漏洞，因为它们允许网络中未使用的应用程序。策略优化器使您能够将这些过于宽松的规则转换为更具体、更集中的规则，仅允许您实际使用的应用程序。

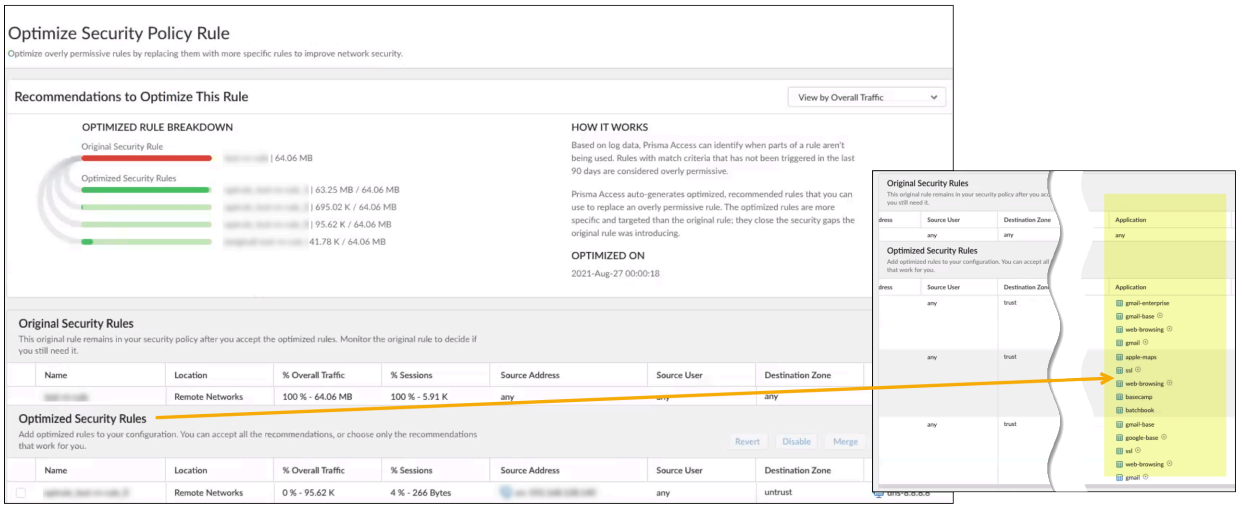
只有过去 90 天以上创建的规则才会被考虑进行策略优化。

工作原理

Strata Cloud Manager 会分析日志数据，并在允许 **any**（任何）应用程序流量时将规则归类为过于宽松，并且规则必须至少有 90 天的历史。如果这些规则允许企业不必要的流量，则可能会引入安全漏洞。

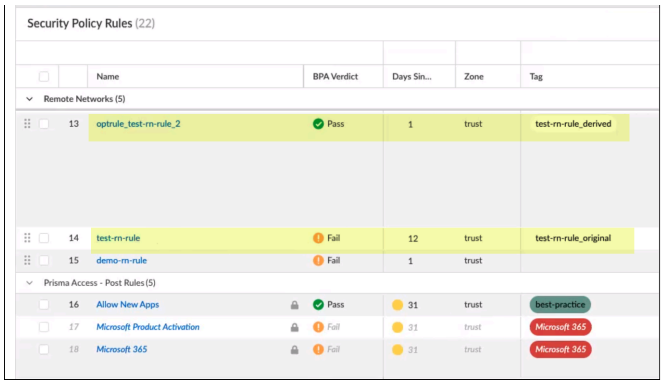
对于被认定为过于宽松的规则，Strata Cloud Manager 会自动生成您可以接受的建议以优化规则。新的推荐规则比原始规则更具体、更有针对性；它们明确允许仅在过去 90 天内在您的网络中检测到的应用程序。

选择过于宽松的规则来审查、调整和接受优化建议。用更具体的、推荐的规则替换这些规则可以增强您的安全态势。



接受优化规则的建议并不会删除原始规则。原始规则仍然列在安全策略中的新规则下方；这样您就可以监视规则，并在确信不需要时将其删除。

原始规则和优化规则都已标记，因此您可以在安全策略中轻松识别它们：



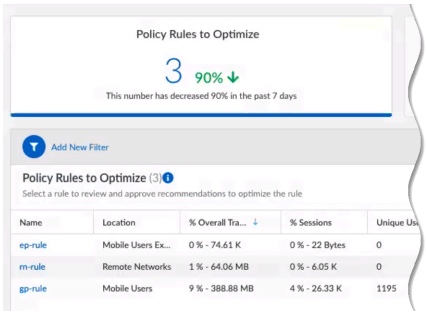
优化规则

STEP 1 | 访问 **Config Cleanup**（配置清理）以查看是否有可以优化的规则。

转至 **Manage**（管理） > **Security Posture**（安全状况） > **Policy Optimizer**（策略优化器）。

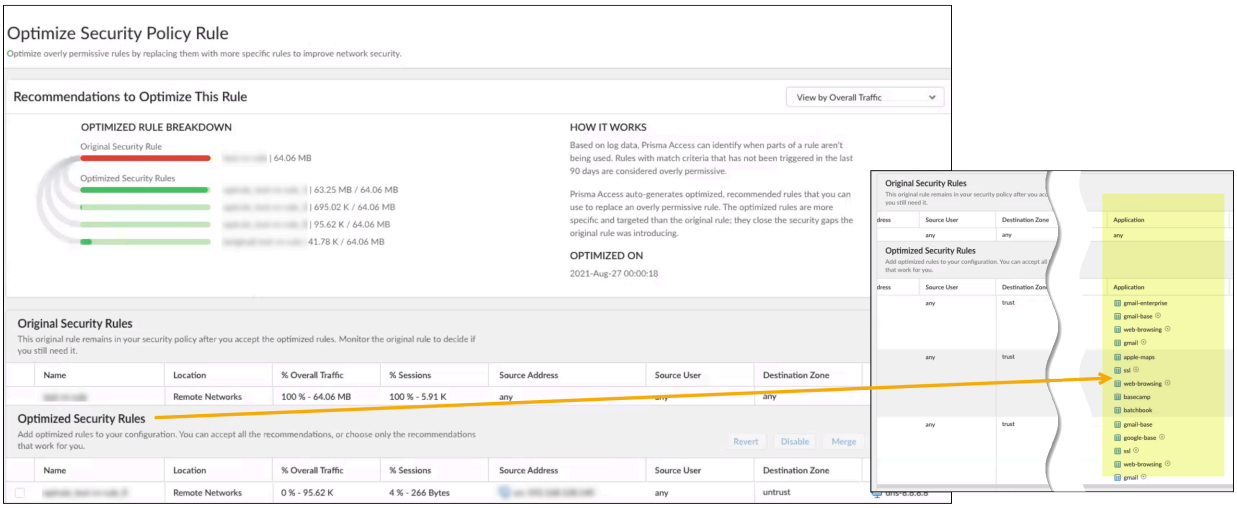
STEP 2 | 审查过于宽松的规则，并选择一条规则来查看优化建议。

如果存在多条过于宽松的规则，请重点优化对流量影响最大的规则；这将为您加强安全态势带来最显著的收益。



STEP 3 | 查看推荐的、优化的规则。

您可以看到每条新规则将覆盖多少原始规则的流量。请注意每条新规则强制执行的具体应用程序。



STEP 4 | 接受部分或全部规则建议。

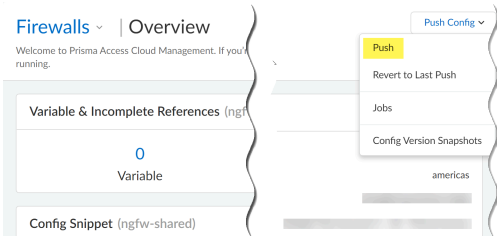
接受新的、优化的规则会将规则添加到您的规则库中。它们现在还不会处于活跃状态；这将在下一步 **Push Config**（推送配置）到 Prisma Access 时发生。

Accept All（全部接受）将按原样接受推荐的规则。您还可以在接受优化规则之前进行更改：

- 从优化中删除一条规则。将此规则添加到您想要从优化中排除的规则列表中（这次以及以后）。
- 禁用优化规则。这意味着您不接受该规则，并且该规则不会被添加到规则库中。
- 撤销您所做的所有更改。这将撤消您所做的所有编辑并将规则恢复为建议。
- 合并规则。如果您发现任何推荐的规则相似，您可能会决定这样做。

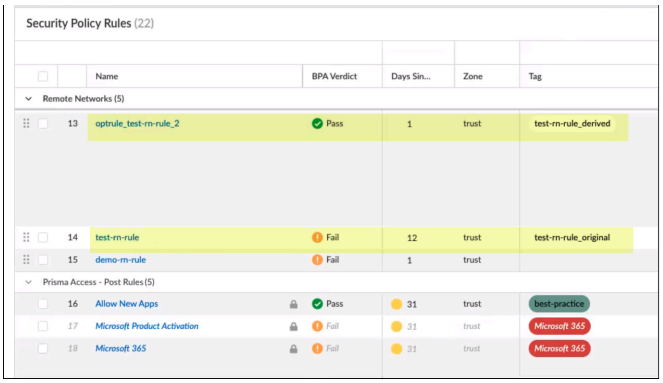
接受优化规则后，系统将提示您 **Update Rulebase**（更新规则库）。当您同意时，优化的规则将添加到您的安全策略中。然而，他们尚未实施交通管制。

STEP 5 | **Push Config**（推送配置），以便将配置更新发送到 Prisma Access 并开始执行优化规则。



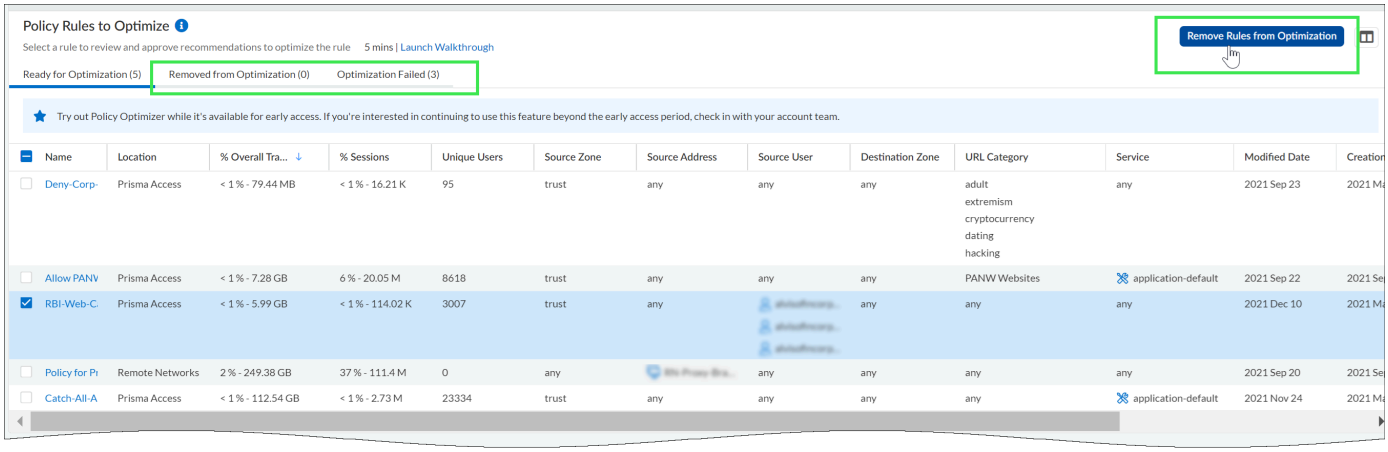
STEP 6 | 监控原始规则直到您确信不再需要它。

原始的、过于宽松的规则仍保留在您的安全策略中；它列在规则库中的优化规则下方，并带有标记，以便您可以轻松识别它。标签名称将 _original 附加到规则名称（例如，security-rule-name_original）。



从优化中排除规则

将规则移动到 **Excluded from Optimization**（从优化中排除）列表，Prisma Access 将不会对其进行优化。规则设置保持原样。

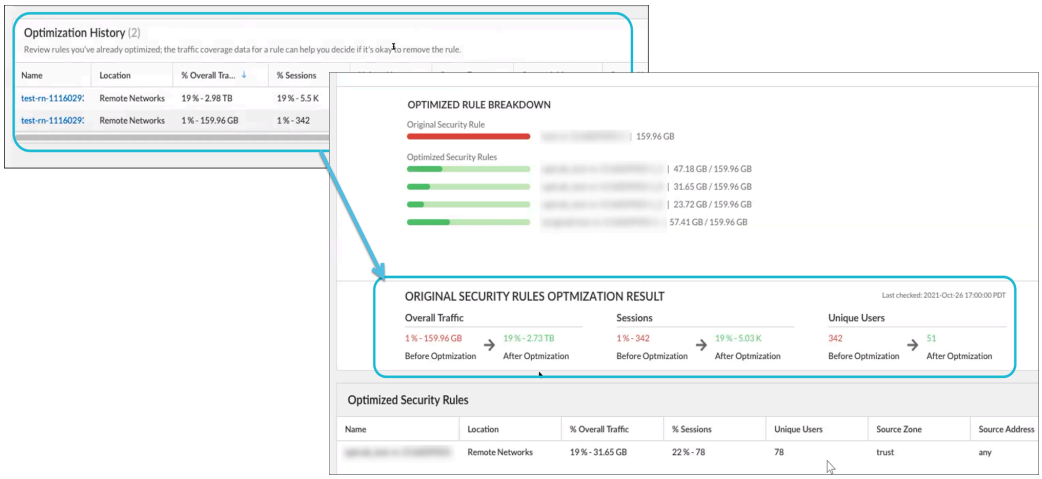


将规则移至排除列表后，请确保 **Push Config**（推送配置）；推送配置后，规则可能需要最多 24 小时才能显示在列表中。您稍后可以随时选择将规则添加回优化列表。

追踪优化结果

策略优化器显示您优化过的安全规则的历史记录。历史数据包括优化结果：将原始规则的流量覆盖范围与优化后的规则进行比较。

您看到的 **Policy Optimizer History**（策略优化器历史）数据是过去 30 天的。如果原始规则（您优化的规则）六个月内没有命中，则会从策略优化器历史记录中删除，并将其归类为零命中策略规则。



管理：配置清理

在何处可以使用？	需要提供什么？
• Prisma Access （利用 *Strata Cloud Manager* 或 *Panorama* 配置管理） • NGFW，包括由 软件 NGFW 积分提供资助的项目	❑ 使用 Strata Cloud Manager 管理您的配置至少需要其中一个许可证；对于 NGFW 和 Prisma Access 的统一管理，您同时需要两个许可证： ❑ Prisma Access 许可证 ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Pro → Strata Cloud Manager 中提供的功能取决于您使用的 许可证。

使用配置清理来识别和删除 Strata Cloud Manager 配置中未使用的配置对象和策略规则。删除未使用的配置对象可以简化防火墙管理，方法是删除乱码并仅保留安全实施所需的配置对象。

STEP 1 | 登录 Strata Cloud Manager。

STEP 2 | 选择 **Manage**（管理） > **Security Posture**（安全态势） > **Config Cleanup**（配置清除）。

STEP 3 | 选择整个 Strata Cloud Manager 配置中最近 6 个月未使用的对象和策略规则。

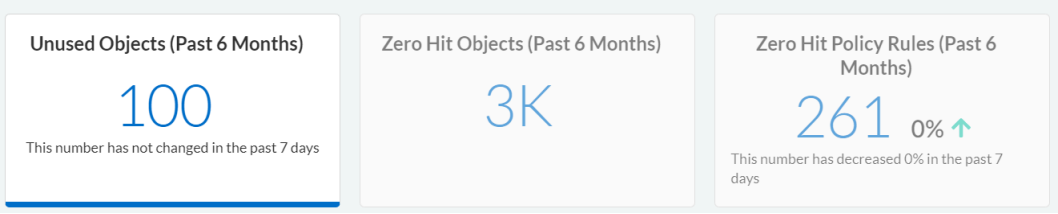
- **Policy Rules to Optimize**（要优化的策略规则）— 单击以查看过于宽松的规则，以将这些规则转换为只允许您实际使用的应用程序的更加具体、重点突出的规则。
- **Unused Objects (Past 6 Months)**（未使用的对象 [过去 6 个月]）— 任何配置或策略规则中在过去 6 个月内未使用的所有配置对象。
- **Zero Hit Objects (Past 6 Months)**（零命中对象 [过去 6 个月]）— 具有配置对象的策略规则，其中策略规则中的配置对象接收零命中。

  此处列出的配置对象仅在与其关联的策略规则中收到零命中。它们的用法可能会在它们使用的其他策略规则中收到命中。
- **Zero Hit Rules (Past 6 Months)**（零命中规则 [过去 6 个月]）— 过去 6 个月中流量匹配为零的所有策略规则。

STEP 4 | 应用其他筛选器以针对特定未使用的对象和策略规则。

Unused Objects (Past 6 Months（未使用对象 [过去 **6** 个月]）和 **Zero Hit Policy Rules (Past 6 Months)**（零命中策略规则 [过去 **6** 个月]）支持 **Add New Filter**（添加新筛选器）。

- **Unused Objects (Past 6 Months)**（未使用对象 [过去 **6** 个月]）— 您可以根据以下条件筛选和 **Delete**（删除）未使用的对象：
  - **Name**（名称）— 搜索并选择特定的配置对象名称。
  - **Location**（位置）— 在其中创建配置对象名称的配置范围。
  - **Object Type**（对象类型）— 配置对象类型。
  - **Days Unused**（未使用天数）— 配置对象被使用的天数。
    - **<50** — 未使用少于 50 天。
    - **>= 50, <= 100** - 50 到 100 天未使用。
    - **<50** — 超过 100 天未使用。
- **Zero Hit Policy Rules (Past 6 Months)**（零命中策略规则 [过去 **6** 个月]）— 您可以根据 **Name**（名称）、**Days with Zero Hits**（零命中天数）或任何 `Source`（来源）和 `Destination`（目的地）数据，筛选并 **Enable**（启用）、**Disable**（禁用）或 **Delete**（删除）零命中策略规则。



管理：安全态势设置

在何处可以使用？	需要提供什么？
• NGFW，包括由 软件 NGFW 积分提供资助的项目 • Prisma Access (Managed by Panorama or Strata Cloud Manager) • Prisma SD-WAN	这些许可证均包含对 Strata Cloud Manager 的访问权限： ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Prisma SD-WAN ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → 您可用的特性和功能Strata Cloud Manager取决于您使用的许可证。

Strata Cloud Manager 利用一组预定义的最佳实践检查，这些检查与特定于行业的标准网络安全控制保持一致，例如 CIS（互联网安全中心）和 NIST（国家标准和技术研究所）以及您根据组织的特定需求创建的自定义检查。这些检查可评估云基础架构内的配置和设置，识别与最佳实践或合规性要求的偏差。

Strata Cloud Manager 中的安全态势检查涵盖一系列安全域，包括网络安全、数据保护以及身份和访问管理。这些检查评估防火墙规则、加密、身份验证机制和配置的整体完整性。

当您的配置检测到偏差时，Strata Cloud Manager 可提供可操作的见解和补救建议，甚至可以自动执行流程的某些部分，以纠正错误配置和不符合规定的设置，从而帮助您以最少的手动干预来维护安全和符合规定的云环境。

安全态势设置集合了 AIOps 和 Strata Cloud Manager 安全检查设置页面的功能。

选择 **Manage**（管理） > **Security Posture**（安全态势） > **Settings**（设置）以查看、管理和自定义部署的安全态势检查，从而最大限度地提供相关建议。

- **Security Checks**（安全检查）– 用于评估配置的最佳做法检查列表。

  将配置与这些检查进行比较，以评估设备的安全态势并生成安全警报。您可以根据环境执行以下操作来管理这些检查：

  1. 设置自定义检查的严重性级别，以识别对部署最关键的检查。

     您可以更改自定义检查的严重性级别，但 *Palo Alto Networks* 最佳实践检查的严重性级别是固定的，无法更改。

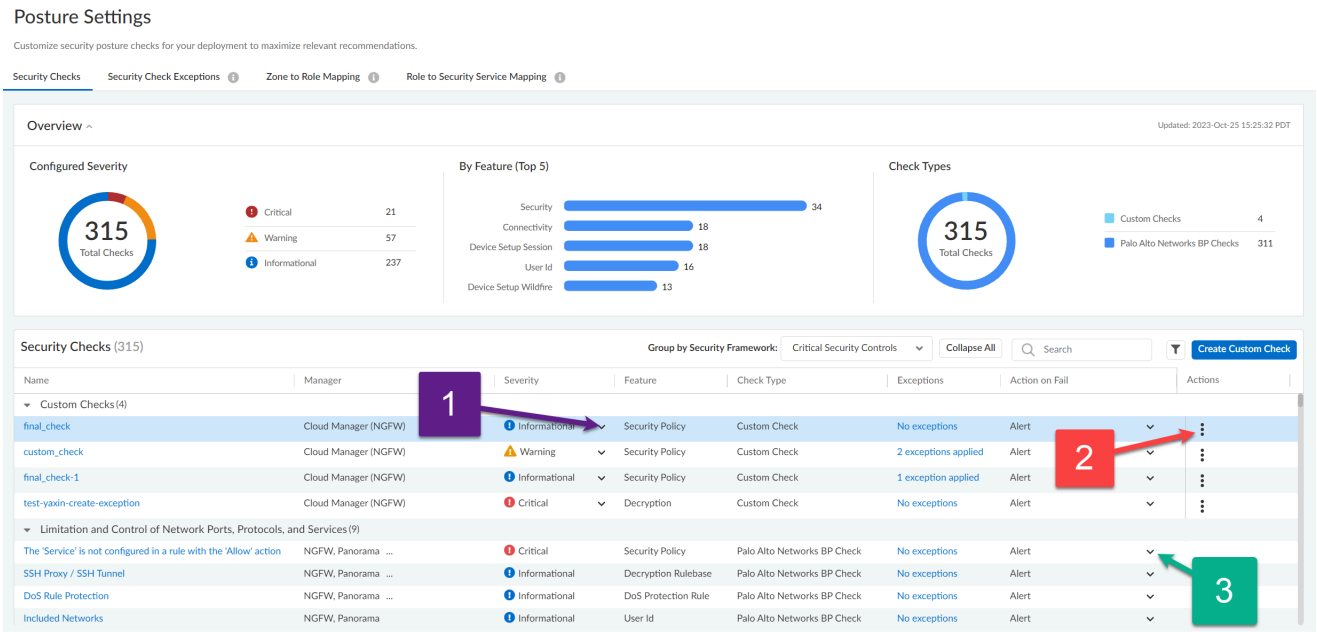
  2. 创建和删除您自己的自定义检查，克隆和编辑现有检查以创建新的检查，并为不希望应用到部署部分中的检查设置特殊例外。

     作为这些检查的初始展开的一部分，您可以克隆自定义检查框架中的检查

     。

  3. 设置检查失败时的响应。
     - **Alert**（警报）（默认）— 为失败的检查发出警报。
     - **Block**（阻止）— 在潜在错误配置进入您的部署之前阻止它们。“阻止”是指以下任意一种，具体取决于您的管理方式：
       - **Strata Cloud Manager** 的内联检查 — 防止您提交或推送不符合要求的配置，但不会阻止您在本地保存配置。
       - **Strata Cloud Manager** 上的实时*内联检查 — 甚至会阻止您保存不符合规定的配置。
       - **Panorama** 托管** — 防止您向 Panorama 提交不符合要求的配置，但不会阻止您将其保存到 Panorama 候选配置。
       - PAN-OS Web 界面、API 或 CLI 管理 — 阻止对未受云管理或 Panorama 管理的配置没有强制执行效果。

     - *由于其逻辑复杂性，一些内联检查在固定的时间表上异步运行，但不是实时的。配置中的实时检查失败将阻止您保存该配置，甚至在本地保存。
     - ** 需要 Panorama 云连接器插件来强制实施 *Panorama* 上的阻止提交操作。



- 安全检查例外

  对您指定的设备或设备组关闭单独检查。
- 服务区到角色的映射

  将 NGFW 中的服务区映射到角色以获取自定义建议。
- 角色到安全的服务映射

  管理所有 NGFW 中服务区和角色之间通信所需的安全服务。

创建自定义检查

从现有检查创建您自己的自定义检查。或者，跳到步骤 4，从头开始创建自定义检查。

STEP 1 | 选择 **Manage**（管理） > **Security Posture**（安全态势） > **Settings**（设置）。

STEP 2 | 标识要克隆的检查并 **Clone**（克隆）。

STEP 3 | **Edit**（编辑）您克隆的检查并跳到步骤 5 以进行更改。

STEP 4 | 转到 **Manage**（管理） > **Security Posture**（安全状况） > **Settings**（设置），然后选择 **Create Custom Check**（创建自定义检查）。

STEP 5 | 指定检查的 **General Information**（一般信息）。您的自定义检查必须具有名称和说明，但您还应为您的检查添加建议和理由，以帮助其他人理解您的自定义检查的意图和最佳做法。

STEP 6 | 可选选择 **Object Type**（对象类型）– 要创建检查的配置部分，用于确定在创建检查时可以选择哪些要匹配的规则属性。

STEP 7 | 使用逻辑构建器进行自定义检查。

1. 添加表达式 – 描述配置的匹配条件的单行逻辑表达式。

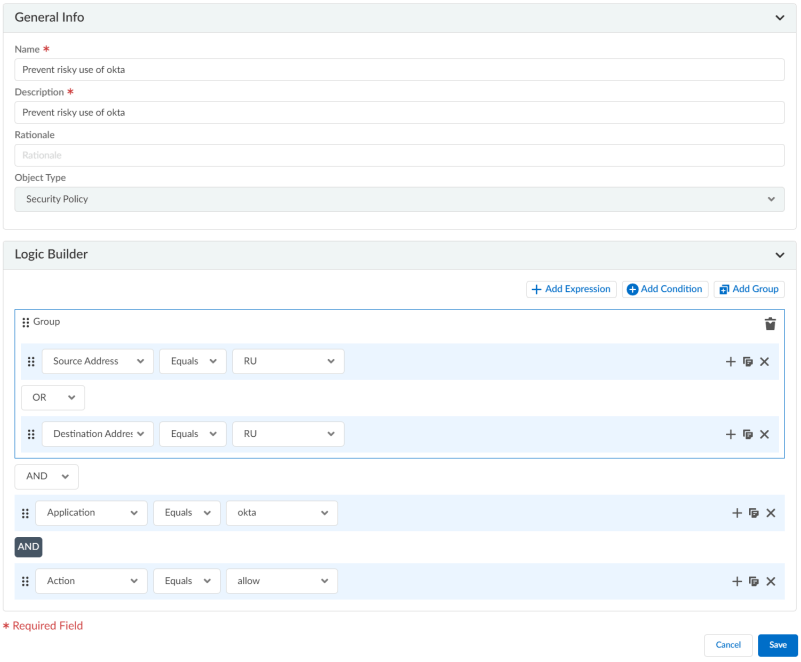
要匹配的规则属性	匹配运算符	具体标准
• 常规 - 名称、描述、职位和日程 • 源 – 服务区、地址、用户 • 目标 – 服务区和地址 • 应用程序、服务和 URL • 操作和高级检查	• 是 • 不是 • 为空 • 不为空 • 开头为 • 结尾为 • 包含 • 大于 • 在其中 • 等于或大于 • 等于或小于 • 少于 • 等于 • 不等于 • 不包含 • 全部 • 一些 • 不在其中	[文本字段]

2. 添加条件 – 使用逻辑运算符（如 AND、OR、IF、Then、ELSE 和 ELSE IF）连接或组合表达式、附加条件和组。

3. 添加组 – 创建一组表达式、条件或两者。这个组加在一起，结果为 True 或 False。

   - 添加新表达式或条件
   - 克隆表达式或条件
   - 删除表达式或条件

   本示例中的表达式在看到允许 Okta 流量进出俄罗斯 IP 地址的策略规则时发出警告。该示例只是说明了逻辑构建器的工作原理，并不是要作为推荐。



STEP 8 | **Save**（保存）您的检查。

管理您的检查

您可以在安全检查上执行下列任意 **Actions**（操作）：

- 克隆* – 创建检查的副本。
- 编辑** – 更改现有自定义检查。
- 删除** – 删除您创建的自定义复选框。

选择您要对其采取行动的检查，然后选择适当的行动。

- *一次只能克隆一个检查。
- **只能编辑或删除自定义复选框。
- 您可能需要获得管理员的权限才能编辑自定义检查。

为检查创建例外

如果需要，您可以限制部署中应用检查的位置。

STEP 1 | 选择 **Manage**（管理） > **Security Posture**（安全态势） > **Settings**（设置） > **Security Check Exceptions**（安全检查例外），然后 **Create Security Check Exception**（创建安全检查例外）。

此外，请选择 **Manage**（管理） > **Security Posture**（安全态势） > **Settings**（设置），并标识并选择要排除地检查（**Exceptions [**例外**]** 列）。

STEP 2 | 指定为检查创建例外规则所需的信息。提供例外的名称、原因和条件。

Security Check Exception（安全检查例外）功能目前仅适用于警报，以及 ***Best Practices***（最佳实践）和 ***Security Posture Insights***（安全态势见解）指示板。

STEP 3 | 可选为您的例外添加服务工单号码或说明，以帮助其他人了解您的例外背后的意图和历史。

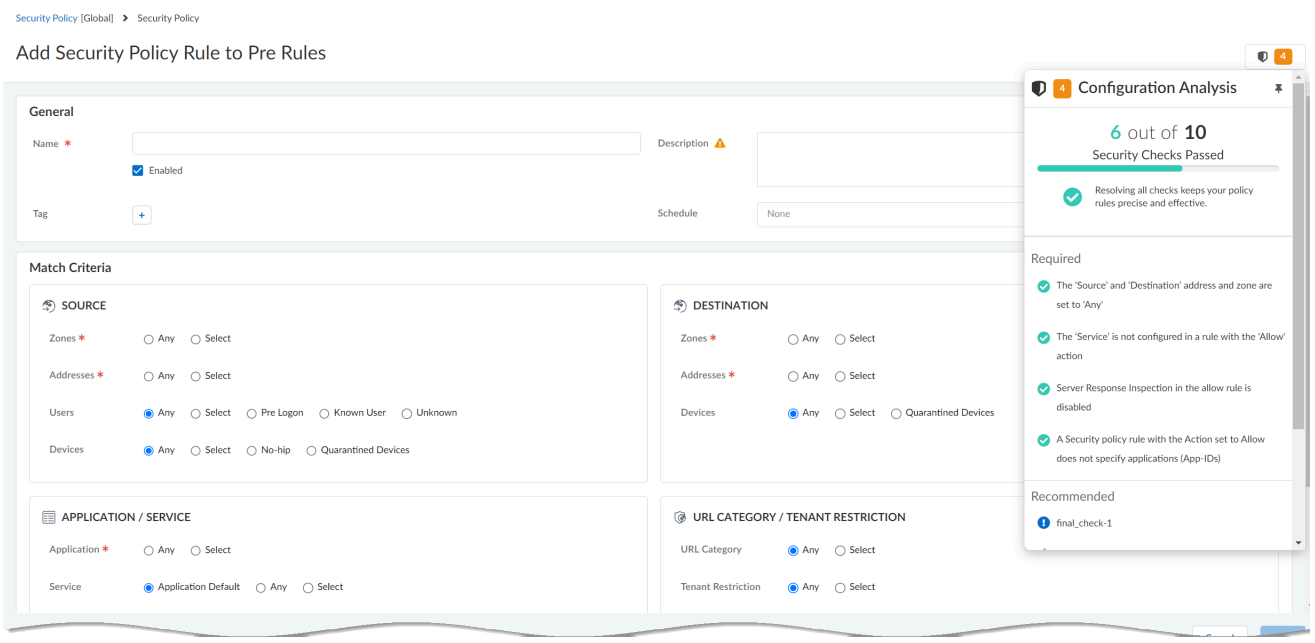
STEP 4 | **Save**（保存）您的例外。

您的检查在工作中

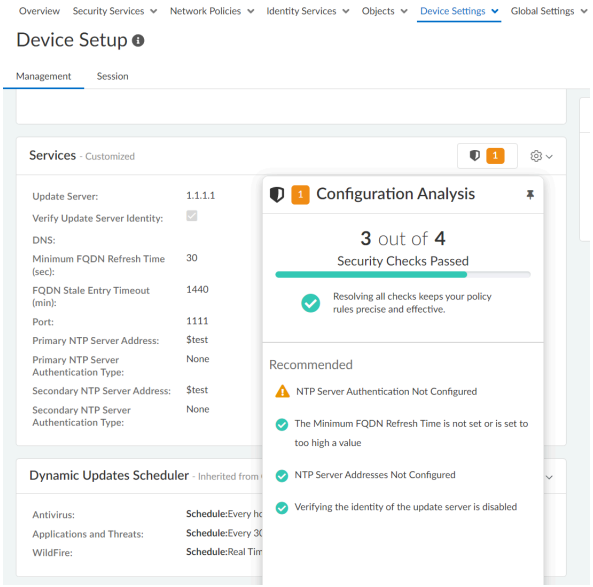
字段级检查可向您显示您的配置与最佳实践或自定义检查不一致的地方。检查提供最佳实践指导内联，以便您可以立即采取行动。

您还可以随时随地查看和管理安全检查。

- 创建和管理策略规则 – 安全策略规则允许您实施规则和采取行动，并且可以根据需要具有通用性或特定性。**Manage [**管理**] > Configuration [**配置**] > NGFW and Prisma Access [NGFW** 和 **Prisma Access] > Security Services [**安全服务**] > Security Policy [**安全策略**]**）



- 设置设备 – 配置防火墙的管理和辅助接口的服务路由、连接设置、允许的服务和管理访问设置。**Manage**（管理） > **Configuration**（配置） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Device Settings**（设备安装） > **Device Setup**（设备安装））



如果您尝试保存的配置没有通过您的通过标准，您可以选择修正问题，或者覆盖*警告并无论如何保存您的更改。

- *覆盖权限受基于角色的访问控制 *(RBAC)* 控制，必须为您的角色启用此选项才能显示。有关覆盖、自定义检查和例外的操作记录在审计日志中：***Incidents and Alerts***（事件和警报）***Log Viewer***（日志查看器）***Audit (log type)***（审核 *[日志类型]*）。
- 您对自定义检查、覆盖和异常所做的所有操作都记录在审核中：***Incidents and Alerts***（事件和警报） > ***Log Viewer***（日志查看器） > ***Audit (log type)***（审核 *[日志类型]*）。

管理：访问控制

在何处可以使用？	需要提供什么？
• Prisma Access （利用 *Strata Cloud Manager* 或 *Panorama* 配置管理） • NGFW，包括由 软件 NGFW 积分提供资助的项目	❑ 至少需要这些许可证之一才能通过 Strata Cloud Manager 管理配置；为了统一管理 NGFW 和 Prisma Access，您需要以下两者： ❑ Prisma Access 许可证 ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Pro ❑ 软件 NGFW 积分 对于 *VM-Series* 软件 *NGFW*） → Strata Cloud Manager 中提供的功能取决于您使用的 许可证。

基于角色的访问控制 (RBAC) 可让您定义管理用户（管理员）的特权和责任。每个管理员都必须拥有指定角色和身份验证方法的用户帐户。Prisma Access 云管理实现自定义 RBAC，从而使您可以管理角色或特定权限，并为管理用户分配访问权限。凭借 RBAC，您可以管理用户及其对云管理中各种资源的访问。

SaaS Security Inline 和 *Behavior Threats* 不支持 *RBAC*。***Discovered Apps***（发现的应用程序）和 ***Behavior Threats***（行为威胁）下的所有选项卡都对所有用户可见，无论为其分配的角色如何。

更多 ***RBAC*** 资源

- 谁可以使用通用服务：身份和访问权限：云托管 Prisma Access
- 什么是通用服务的一般流程：身份和访问
- 通过通用服务添加角色和权限

管理员角色

Prisma Access 上的用户是指获得管理权限的用户，而角色定义管理员对服务的访问类型。分配角色时，请指定权限组以及管理员可以管理的帐户组。中心为使用 Prisma Access 的管理员提供以下内置权限组。

- 应用程序管理员 — 具有对给定应用程序的完全访问权限，包括将来添加到应用程序的所有实例。应用程序管理员可以为应用程序实例分配角色，还可以激活该应用程序的特定应用程序实例。
- 实例管理员 — 对已分配此角色的应用程序实例的完全访问权限。实例管理员还可以让其他用户成为应用程序实例的实例管理员。如果应用程序具有预定义或自定义角色，则实例管理员可以将这些角色分配给其他用户。
- 超级读取者 — 可以查看所有配置元素、日志和设置。超级读取者无法更改其他设置。
- 审核管理员 — 只能查看和管理日志和日志设置。审核管理员不能更改其他设置。
- 加密管理员 — 可以查看日志，管理加密设置，如 IKE、IPSec、主密钥管理和证书配置。加密管理员无法查看或更改其他设置。
- 安全管理员 — 可以查看日志并管理所有设置，但不包括加密管理员角色可用的加密设置。
- **Web** 安全管理员 — 只能查看与 Web 安全相关的配置元素。
- **Data Loss Prevention** 管理员 — 可以访问 Enterprise DLP 设置，但不能将配置更改推送到 Prisma Access。
- **Data Security** 管理员 — 可以访问 Enterprise DLP 和 SaaS Security 控件，但不能将配置更改推送到 Prisma Access。
- **SaaS** 管理员 — 可以访问 SaaS Security 设置，但不能将配置更改推送到 Prisma Access。

自定义基于角色的访问控制 — 设置

下面是如何使用预定义角色或创建自定义角色，为用户分配角色，以及在访问 Prisma Access 应用程序时管理用户范围。

STEP 1 | 通过通用服务添加自定义角色

如果您需要比预定义角色所提供的更精细的访问控制，则可以添加自定义角色来定义为用户实施的权限。与预定义角色类似，自定义角色是一组权限和权限集。与预定义角色不同，每个自定义角色只能分配给定义它的租户服务组 (TSG) 下的层次结构中的用户。这避免了不同客户定义的同名自定义角色之间的名称冲突。

如果您在层次结构的顶层（父级）添加自定义角色，则该角色将分配给嵌套在下面的租户，以便父租户可以管理子租户。

STEP 2 | 通过通用服务添加用户访问

通用服务：访问和身份使您能够将用户访问添加到平台以及您创建的租户。

STEP 3 | 通过通用服务为租户用户或服务帐户分配预定义角色

如果您已经添加用户，并希望添加其他角色，还可以分配一批预定义角色。查看有关角色和权限的其他信息。

STEP 4 | 在 Prisma Access 云管理用户界面中创建新范围

Prisma Access 云管理使您能够（作为管理员）为云管理用户（非管理员）分配管理范围，以根据范围（如文件夹和代码段）关联权限。

权限是系统中允许的操作。权限表示一组特定的应用程序编程接口 (API) 调用，用于读取、写入和删除系统内的对象。所有权限都会分组到角色中。

管理：范围管理

在何处可以使用？	需要提供什么？
• Prisma Access （利用 *Strata Cloud Manager* 或 *Panorama* 配置管理） • NGFW，包括由 软件 NGFW 积分提供资助的项目	❑ 使用 Strata Cloud Manager 管理您的配置至少需要其中一个许可证；对于 NGFW 和 Prisma Access 的统一管理，您同时需要两个许可证： ❑ Prisma Access 许可证 ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Pro → Strata Cloud Manager 中提供的功能取决于您使用的 许可证。

配置范围管理以强制执行基于自定义角色的访问控制。这允许您指定哪个 Strata Cloud Manager 管理员可以访问和修改特定文件夹、防火墙、Prisma Access 部署和代码段配置。为云管理员定义范围管理可确保他们不会过度配置，并定义所选文件夹、防火墙的读写访问权限，Prisma Access 部署和代码段配置。通用服务多平台和企业角色用于定义 Strata Cloud Manager 管理员。

范围管理配置在整个 Strata Cloud Manager 租户范围内进行定义。无法针对特定文件夹、Prisma Access 或防火墙配置范围定义范围管理。

只有 *Cloud Management* 管理员或超级用户可以创建范围对象。范围管理小部件不适用于具有其他角色的用户。

STEP 1 | 登录 Strata Cloud Manager。

STEP 2 | 选择 **Manage**（管理） > **Access Control**（访问控制） > **Scope Management**（范围管理）。

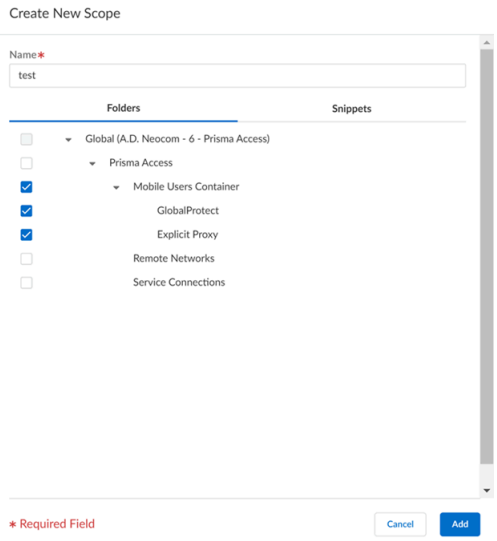
STEP 3 | **Create New Scope**（创建新的范围）。

STEP 4 | 定义范围管理配置。

范围管理配置被标记为 `scope object`。

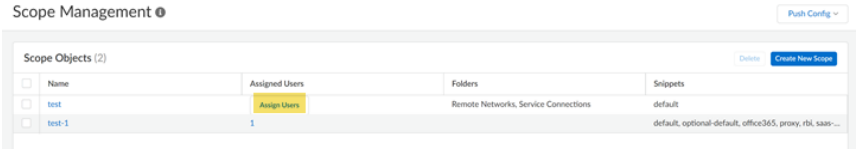
1. 输入描述性的 **Name**（名称）。
2. 选择 **Folders**（文件夹）并选中（启用）文件夹、防火墙和您想要纳入范围的 Prisma Access 部署。

   选择防火墙还包括范围管理配置中与所选防火墙关联的文件夹。仅包含直接关联的文件夹，而不包含父文件夹。
3. 选择 **Snippets**（代码段）并检查（启用）您想要包含的代码段。
4. **Add**（添加）范围对象。



STEP 5 | 应用范围管理配置到 Strata Cloud Manager 管理员。

1. **Assign Users**（分配用户）给您在上一步中创建的范围对象。



2. 为 Strata Cloud Manager 管理员选择 **Role**（角色）。例如，您可以为需要访问所有租户的所有功能的用户选择 MSP 超级用户。

   默认为 None（无）。有关每个可用角色的读写访问权限的更多信息，请参阅通用服务多平台和企业角色。

   选择特定的 *Strata Cloud Manager* 管理员和 ***Clear Role***（清除角色），以删除当前分配的公共服务角色。这会将默认的 *None* 角色应用于管理员。

3. 要修改现有范围以编辑名称，以及添加或删除文件夹，请选择范围对象，根据需要修改范围，然后 **Update**（更新）范围。
4. 要修改已分配的用户、添加更多用户或更改用户，请单击 **Assigned Users**（已分配的用户）并根据需要进行修改，然后 **Close**（关闭）窗口。

管理：IP 限制

在何处可以使用？	需要提供什么？
• Prisma Access （利用 *Strata Cloud Manager* 或 *Panorama* 配置管理） • NGFW，包括由 软件 NGFW 积分提供资助的项目	❑ 使用 Strata Cloud Manager 管理您的配置至少需要其中一个许可证；对于 NGFW 和 Prisma Access 的统一管理，您同时需要两个许可证： ❑ Prisma Access 许可证 ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Pro → Strata Cloud Manager 中提供的功能取决于您使用的 许可证。

为 Prisma Access 云管理管理员指定受信任的 IP 地址。只有从这些源 IP 地址登录（并且成功通过身份验证）的管理员才能访问 Prisma Access 云管理。

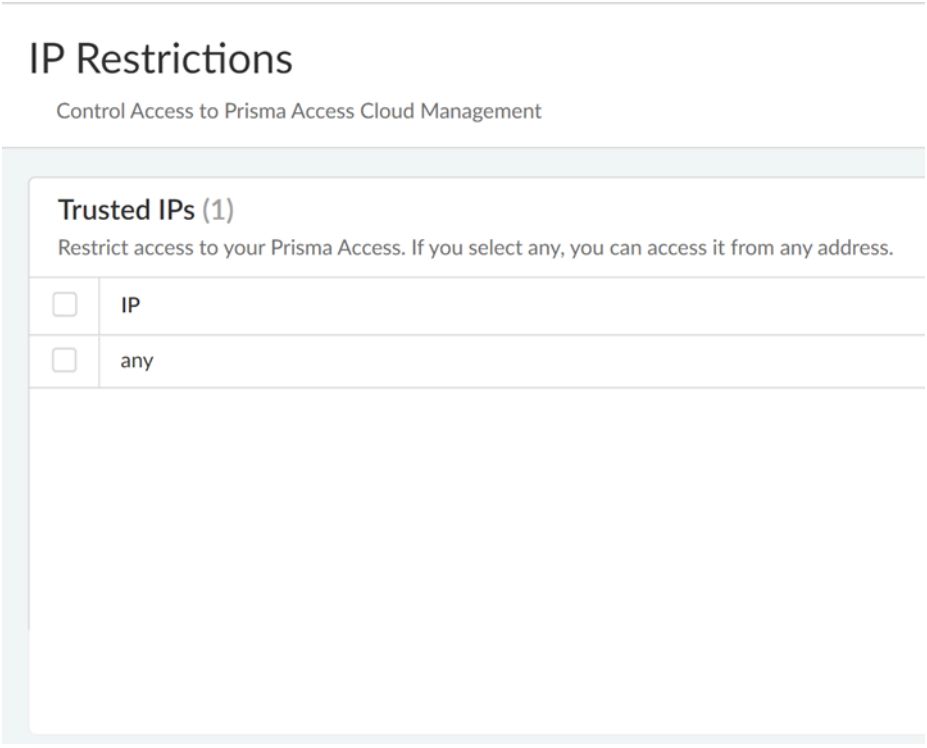
IP 地址必须是公共地址。默认情况下，不强制执行任何受信任的地址（列表设置为 **Any [任何]**）。

要开始，请转到 **Manage**（管理） > **Access Control**（访问控制） > **IP Restrictions**（**IP** 限制）。

对于 IP 限制，不支持子网地址。仅支持 IP 地址和 IP 地址范围。请勿指定与以下 IP 地址和子网重叠的任何子网，因为 Prisma Access 保留这些 IP 地址和子网供其内部使用：

- 169.254.169.253 和 169.254.169.254
- 100.64.0.0/10
- 169.254.201.0/24
- 169.254.202.0/24

我们建议使用符合 RFC 1918 和 RFC 6598 的 IP 地址池。虽然支持使用不符合 RFC 1918 和不符合 RFC 6598 的（公共）IP 地址，但我们不建议这样做，因为它可能与互联网公共 IP 地址空间发生冲突。



工作流程：Strata Cloud Manager

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • NGFW (Managed by Strata Cloud Manager) • Prisma SD-WAN	其中一个或多个许可证，具体取决于工作流程：日志记录需要 ❑ AIOps for NGFW Premium 许可证 ❑ Strata Logging Service 许可证， ❑ Prisma Access 许可证 ❑ Prisma SD-WAN ❑ 远程浏览器隔离许可证

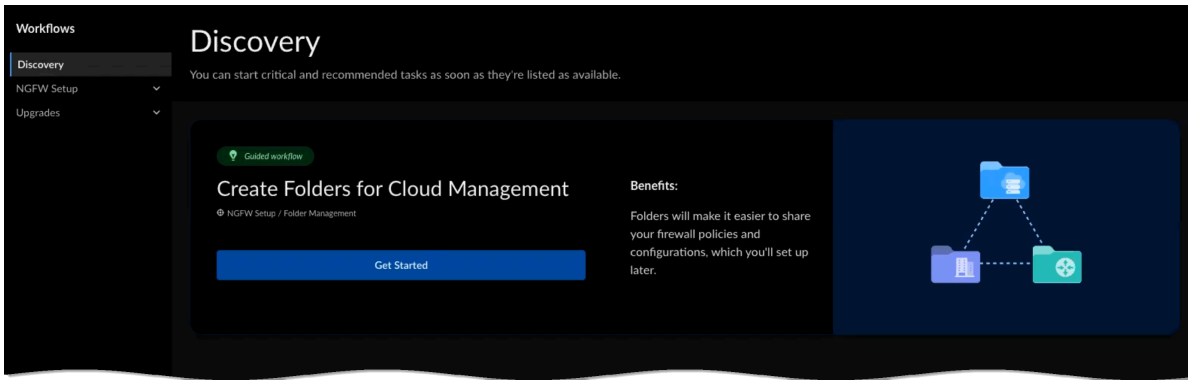
当您首次进入工作流程时，探索指示板会立即显示您可以采取的关键和建议的操作，以改善安全状况或优化配置管理。继续在此处设置和载入 NGFW、Prisma Access 移动用户和远程网络，并规划 NGFW 的软件升级。

- 探索载入任务
- 设置 Prisma Access
- 设置 NGFW
- 设置 Prisma SD-WAN
- 软件升级 (NGFW)
- 软件升级 (Prisma Access)

工作流程：发现

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • NGFW (Managed by Strata Cloud Manager) • Prisma SD-WAN	❑ AIOps for NGFW Premium 许可证或Prisma Access 许可证

在“探索”中，您可以立即开始执行关键任务和推荐任务。可能有指导性的工作流程或任务，您可以自己完成。在本主题中，我们将向您展示如何使用引导式工作流程轻松直观地创建文件夹结构并为其分配设备。



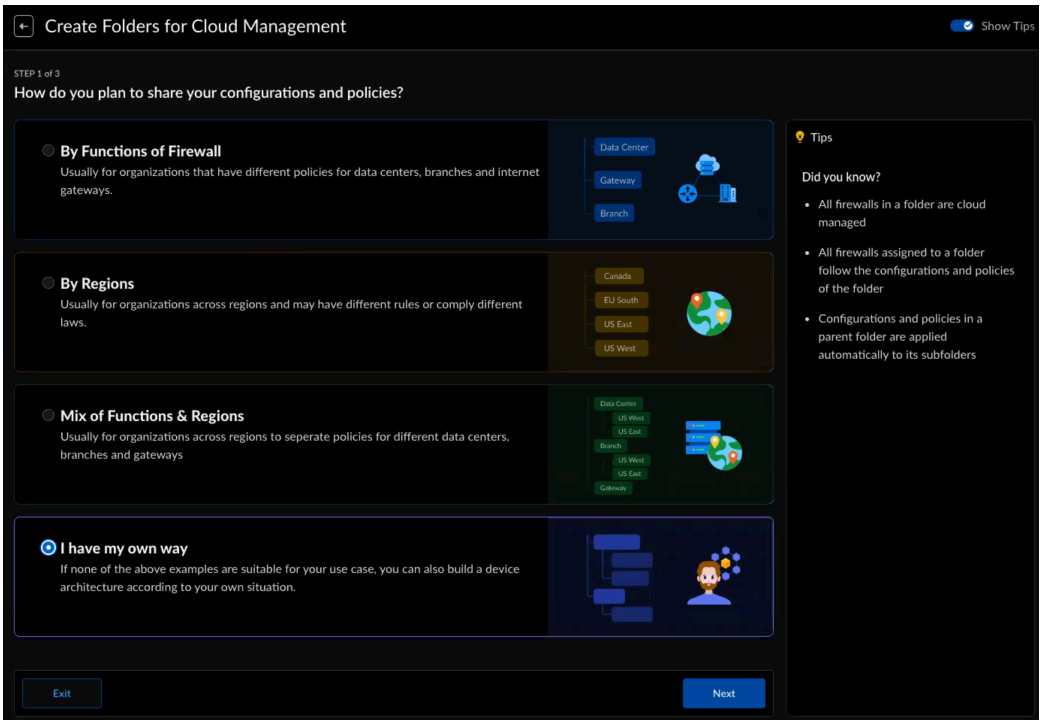
按照以下步骤为防火墙创建文件夹：

STEP 1 | 转到 **Workflows**（工作流程） > **Discovery**（发现），然后选择 **Get Started**（开始）。

STEP 2 | 选择共享策略规则和配置的方式。

- 按防火墙功能划分 — 您的组织对数据中心、分支机构和互联网网关是否有不同的策略？这可能是您的选择。
- 按地区划分 — 您的组织是否跨越有不同规则或遵守不同法律的地区？考虑此选项。
- 功能和区域组合 — 您的跨区域组织是否想针对不同的数据中心、分支机构和互联网网关单独制定策略？试试此选项。
- 我像使用自己的方式 — 如果以上例子都不适合您的用例，您也可以根据自己的情况构建设备架构。

在本示例中，我们将选择 **I have my own way**（我像使用自己的方式）选项。

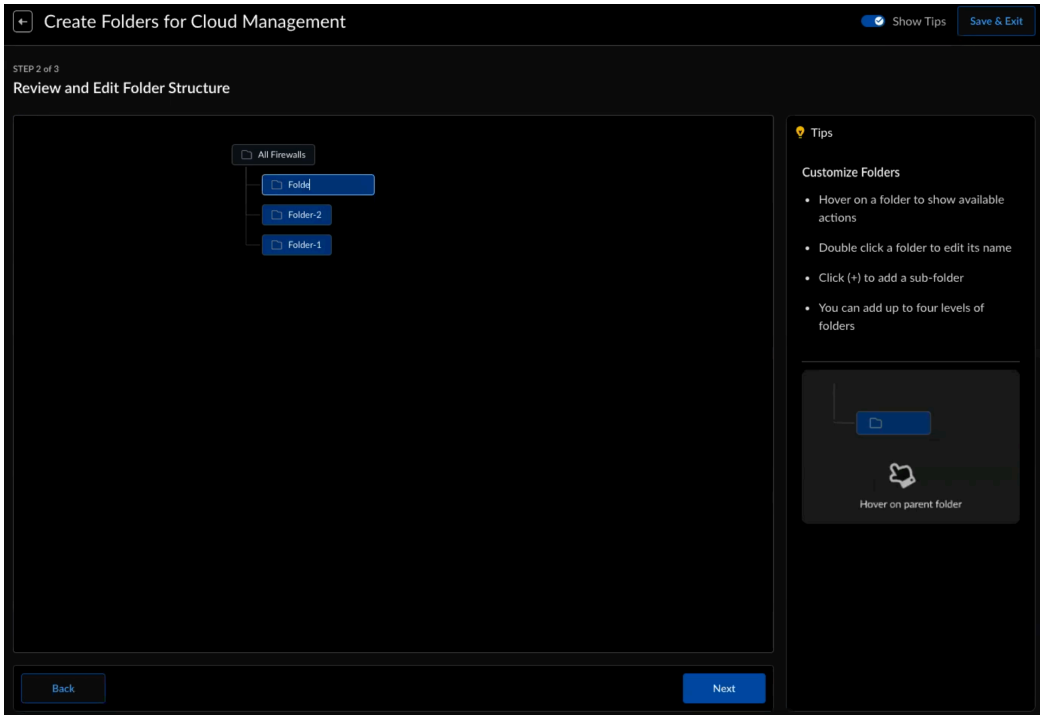


打开显示提示，以便查看帮助提示，从而帮助您做出明智的决定。

STEP 3 | 选择下一步来构建您的文件夹结构。

STEP 4 | 使用以下操作根据您在步骤 1 中选择的模板构建文件夹结构。您可以：

- **Add a new Folder**（添加新文件夹）— 将光标悬停在文件夹上可显示添加新文件夹的选项。单击 ，然后命名您的新文件夹。
- **Delete Folder**（删除文件夹）— 将光标悬停在文件夹上可显示删除该文件夹的选项。选择 ，以便删除该文件夹。
- **Rename Folder**（重命名文件夹）— 双击一个文件夹，为该文件夹键入一个新名称。按下回车键或在文本字段外单击，以便让新名称生效。
- **Expand or Collapse**（展开或折叠）包含子文件夹的文件夹节点。

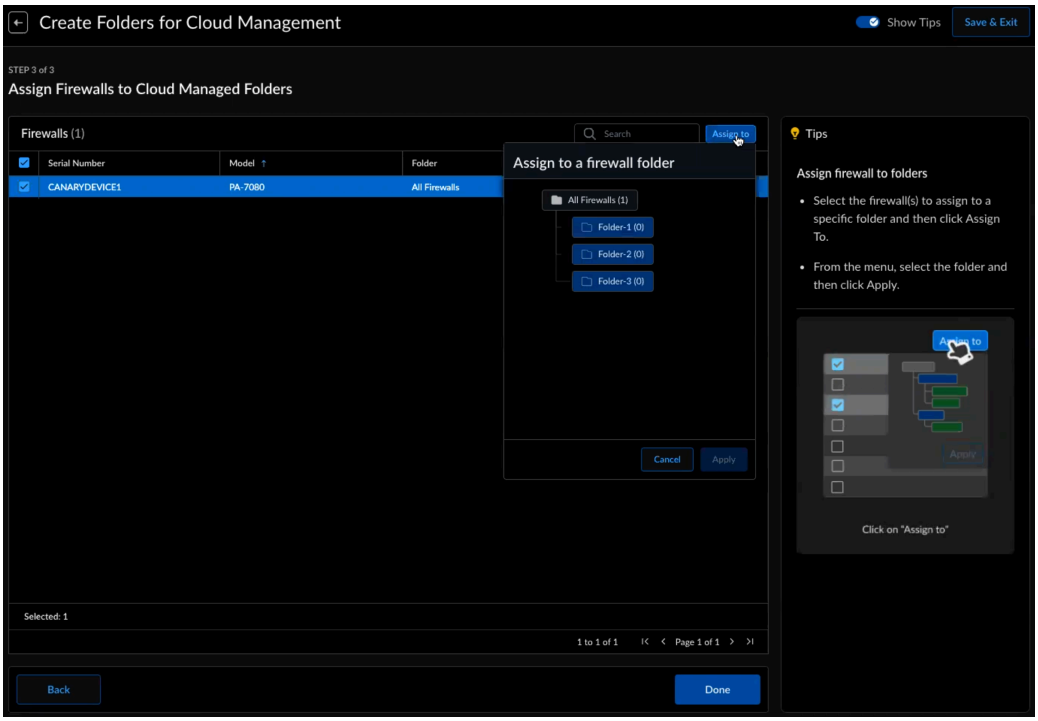


- 文件夹树结构最多可以包含四个级别。
- 无法删除或重命名顶层文件夹。
- 查看提示以获取有关某些文件夹操作的提示。
- 我们将保存您的工作，您可以随时退出，也可以稍后回来。

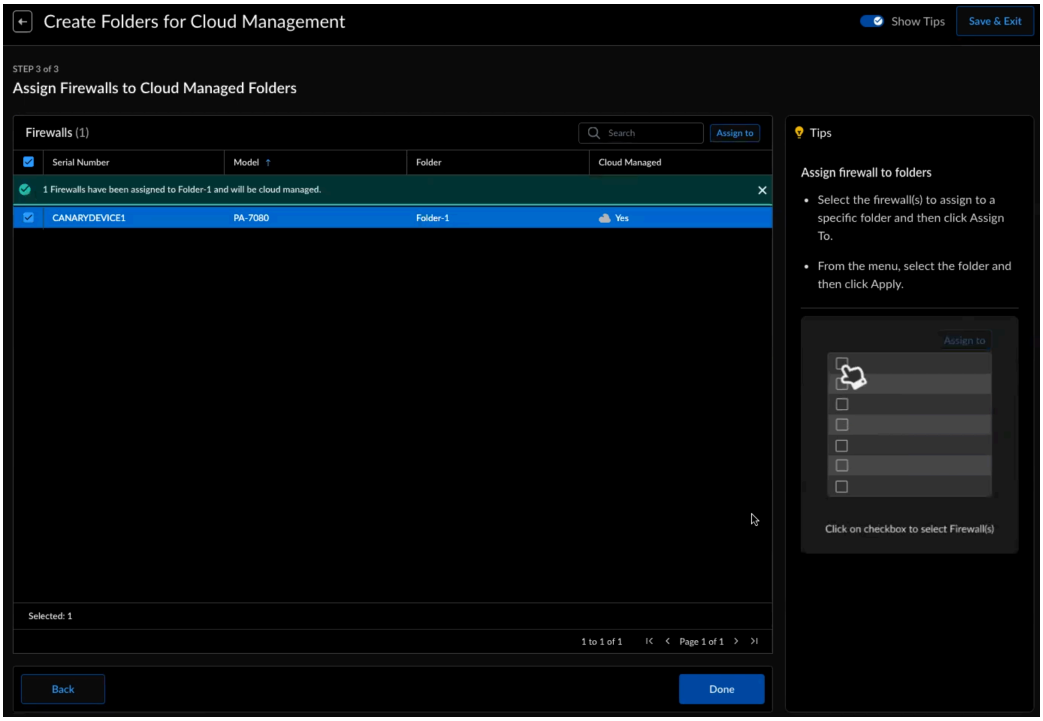
STEP 5 | 选择 **Next**（下一步），以便将防火墙分配给文件夹。

STEP 6 | 从此列表中选择一个或多个防火墙。

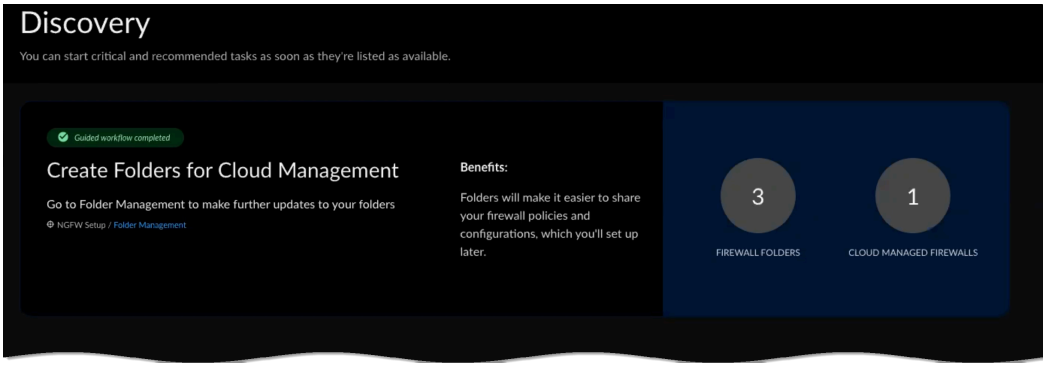
STEP 7 | 选择 **Assign To**（分配给），选择要为其分配防火墙的文件夹，然后选择 **Apply**（应用）。您分配给 **Cloud Managed**（云托管）文件夹的防火墙已启用云托管。

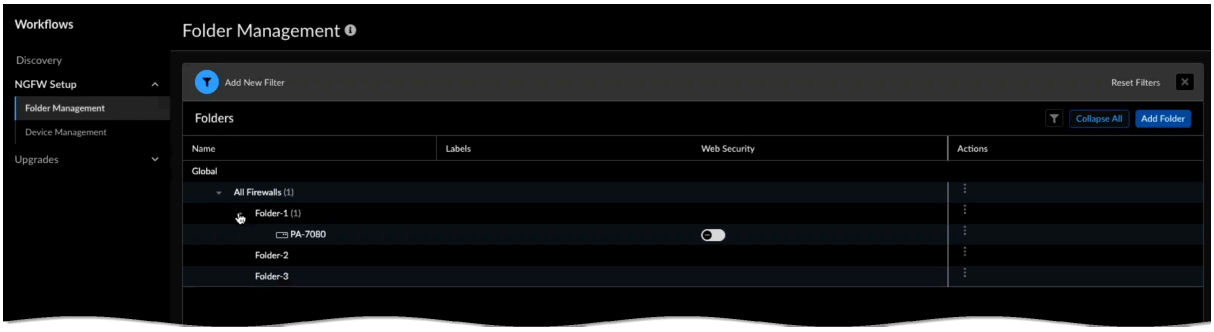


STEP 8 | 确认您的任务并选择 **Done**（完成）。



您将在主 **Discovery**（发现）页面以及 **NGFW Setup**（**NGFW** 设置）文件夹管理选项卡下看到您创建的 **> Folder Management**（文件夹管理）选项卡下看到您创建的文件夹和防火墙。





工作流程：NGFW 设置

在何处可以使用？	需要提供什么？
• NGFW (Managed by Strata Cloud Manager)	❑ Cloud Management for NGFW 需要 AIOps for NGFW Premium 许可证 ❑ 日志记录需要 Strata Logging Service 许可证 ❑ 如果您有 Prisma Access 许可证，则可以使用 **Folder Management**（文件夹管理）查看预定义的文件夹，并为文件夹启用 网络安全

作为设置 NGFW 以进行云管理的一部分，您需要将 Next-Generation Firewall 加入 Strata Cloud Manager。加入包括设置文件夹，以对需要类似设置的防火墙进行分组。了解有关 工作流程：文件夹管理 的详细信息，并使用 **Device Management**（设备管理）页面查看文件夹层次结构中所有设备的详细信息。

STEP 1 | 激活 Strata Logging Service 和 AIOps for NGFW Premium 许可证。

日志记录需要 Strata Logging Service 许可证，NGFW 的云管理需要 AIOps for NGFW Premium 许可证。

STEP 2 | 创建一个或多个文件夹。

文件夹用于对防火墙或部署类型进行逻辑分组，以简化配置管理。

STEP 3 | 将防火墙加入到 Strata Cloud Manager。

将防火墙加入 Strata Cloud Manager，您必须在防火墙上配置本地 Panorama 设置，并将防火墙与您的 Strata Cloud Manager 租户相关联。加入后，您可以继续配置防火墙的常规和会话设置。

STEP 4 | （仅限 HA）如果需要，请在高可用性 (HA) 配置中配置托管防火墙。

STEP 5 | 创建一个或多个代码段。

代码段用于对应用于文件夹、部署或单个防火墙的配置对象进行分组。这允许您标准化可快速应用和推送的常见基本配置，从而简化并加快载入流程。

STEP 6 | 创建配置对象。

配置对象是网络和策略规则配置的构建块。

STEP 7 | 创建和配置网络和策略规则配置。

STEP 8 | 从 Strata Cloud Manager推送配置更改到您的托管防火墙。

工作流程：设备管理

在何处可以使用？	需要提供什么？
• NGFW (Managed by Strata Cloud Manager)	❑ AIOps for NGFW Premium

Strata Cloud Manager 托管的 Palo Alto Networks NGFW 称为云托管设备。Strata Cloud Manager 可以管理运行 PAN-OS 10.2.3 或更新版本的防火墙。

有关 Strata Cloud Manager 的先决条件的更多信息，请单击此处。

通过 **Device Management**（设备管理）指示板**Workflows [工作流] > NGFW Setup [NGFW 设置] > Device Management [设备管理]**），您可以查看有关所有托管设备的重要设备和版本详细信息，并选择要移动到云管理的设备。

查看所有云托管 NGFW 的详细信息

Cloud Managed Devices（云托管设备）选项卡**Workflows [工作流] > NGFW Setup [NGFW 设置] > Device Management [设备管理] > Cloud Managed Devices [云托管设备]**）显示所有 SCM 内置防火墙、它们被分配到的文件夹以及有关它们的重要详细信息。

设备信息	说明
名称	NGFW 的名称及其所属的文件夹。
标签	附加到 NGFW 的任何标签。
配置同步状态	NGFW 的同步状态： • 已同步 • 不同步
HA 状态	已加入的 NGFW 的 HA 状态： • **Active**（主动）— 正常的流量处理操作状态。 • **Passive**（被动）— 正常备份状态。 • **Initiating**（正在启动）— 防火墙将在重启后处于此状态，且时长不超过 60 秒。 • **Non-functional**（无功能）— 错误状态。 • **Suspended**（挂起）— 管理员已禁用此防火墙。 • **Tentative**（试验）— 适用于主动/主动配置中的链接或路径监控事件。
序列号	已加入的 NGFW 的序列号。
模型	已加入的 NGFW 的型号。

设备信息	说明
类型	已加入的 NGFW 的类型： • VM • PA
地址	已加入的 NGFW 的 IP 地址。
许可证	已加入的 NGFW 的许可证信息 • 匹配 • 不匹配
软件版本 | 应用程序和威胁 | 防病毒 | URL 筛选	显示防火墙上目前安装的软件和内容版本。有关详细信息，请参阅防火墙软件和内容更新。
设备目录	防火墙要导入的文件。字典文件为 Strata Cloud Manager 和防火墙管理员提供设备属性列表，以便在导入推荐的安全策略规则时进行选择。
操作	已加入防火墙的操作： • 获取许可证信息 • 重新启动 • 更改路由模式 • 本地配置管理 • 强制引导

从云托管设备中删除 NGFW

Available Devices（可用设备）选项卡显示所有可供 SCM 加入的 NGFW，以及已由 Strata Cloud Manager 管理的 NGFW。

有关 *Strata Cloud Manager* 的载入流程的更多信息，请单击此处。

您可以使用可用设备选项卡将设备移入或移出 Strata Cloud Manager。

STEP 1 | 登录 Strata Cloud Manager。

STEP 2 | 选择 **Workflows**（工作流） > **NGFW Setup**（**NGFW** 设置） > **Device Management**（设备管理） > **Available Devices**（可用设备）。

1. 选择 **Back to Available Devices**（返回可用设备），以便将防火墙移出 Strata Cloud Manager。

恢复防火墙上的本地配置版本快照

您可以恢复任何版本并以 XML 格式下载配置详细信息。

STEP 1 | 登录 Strata Cloud Manager。

STEP 2 | 选择 **Workflows**（工作流） > **NGFW Setup**（**NGFW** 设置） > **Device Management**（设备管理），然后从 **Actions**（操作）中选择 **Local Configuration Management**（本地配置管理）。

STEP 3 | **Load**（加载）版本以恢复本地配置。

STEP 4 | 单击 **Yes**（是），以便将防火墙上的本地配置替换为配置版本。创建了新的提交作业。

您可以使用 **Jobs**（作业）视图来排除失败的操作故障、调查与已完成提交相关的警告或取消待处理的提交。

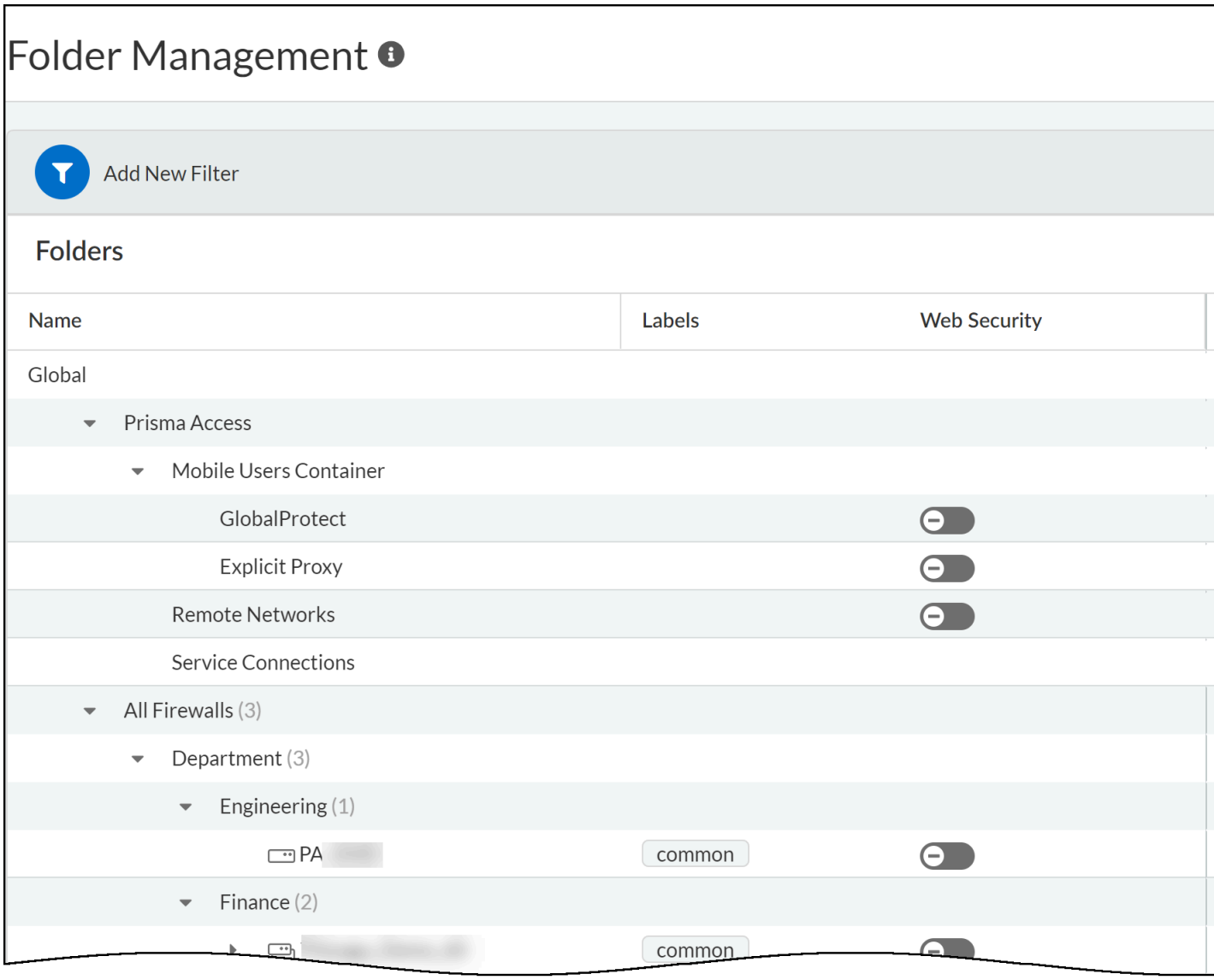
STEP 5 | **Download**（下载）所选版本的视图配置详细信息。

工作流程：文件夹管理

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • NGFW (Managed by Strata Cloud Manager)	❑ AIOps for NGFW Premium 许可证 ❑ Prisma Access 许可证

文件夹用于对防火墙或部署类型（Prisma Access 移动用户、远程网络或服务连接）进行逻辑分组，以便简化配置管理。您可以创建一个包含多个嵌套文件夹的文件夹，以对需要类似配置的防火墙和部署进行分组。嵌套文件夹也可以具有多个嵌套文件夹。

Prisma Access 的文件夹和您的 NGFW 是独立的；对于 Prisma Access 部署，您不能将 NGFW 分组到一个文件夹中。但是，您可以轻松地在所有文件夹中全局应用共享设置，或者使用 管理：代码段 轻松跨多个文件夹应用标准设置和策略要求。

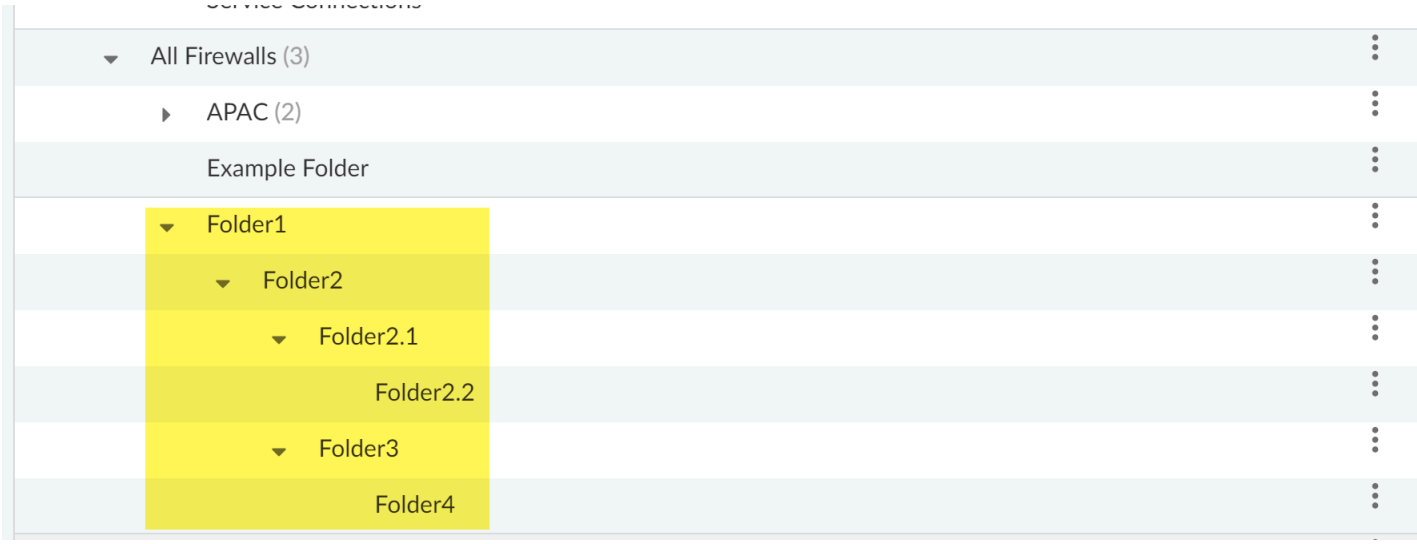


- NGFW
- Prisma Access

文件夹管理 (NGFW)

为了帮助管理文件夹和防火墙，您可以应用标签来筛选并针对特定防火墙组进行配置更改。此外，每个文件夹都显示当前安装的软件版本、动态内容发布版本以及与文件夹关联的防火墙的 GlobalProtect 应用版本。

对于防火墙文件夹，Strata Cloud Manager 在任意给定的文件夹层次结构中最多支持四个嵌套文件夹，默认的 `All Firewalls` 文件夹总是位于任意文件夹层次结构中的最顶层。例如，在设计文件夹层次结构时，请考虑以下几点。在下面的示例中，`Folder1`、`Folder2`、`Folder3` 和 `Folder4` 嵌套在 `All Firewalls` 文件夹下，您最好不要在此特定文件夹层次结构中增加任何其他文件夹。此外，`Folder2.1` 和 `Folder2.2` 嵌套在 `Folder2` 下，您也不能添加任何嵌套任何其他文件夹。



创建文件夹

创建一个文件夹来对防火墙进行逻辑分组，以简化配置管理。您可以在默认的 `Firewalls` 文件夹或其他现有文件夹下创建一个文件夹。

STEP 1 | 登录 Strata Cloud Manager。

STEP 2 | 选择 **Workflows**（工作流） > **NGFW Setup**（**NGFW** 设置） > **Folder Management**（文件夹管理），并 **Add Folder**（添加文件夹）。

STEP 3 | 给文件夹指定一个描述性的 **Name**（名称）。

STEP 4 | （可选）输入文件夹的 **Description**（说明）。

STEP 5 | （可选）分配一个或多个 **Labels**（标签）。

您可以选择现有标签，也可以键入要创建的标签来创建新标签。

STEP 6 | 指定要 **In**（在其中）创建文件夹的位置。

选择 **All Firewalls**（所有防火墙），或选择一个现有文件夹以嵌套其下的文件夹。

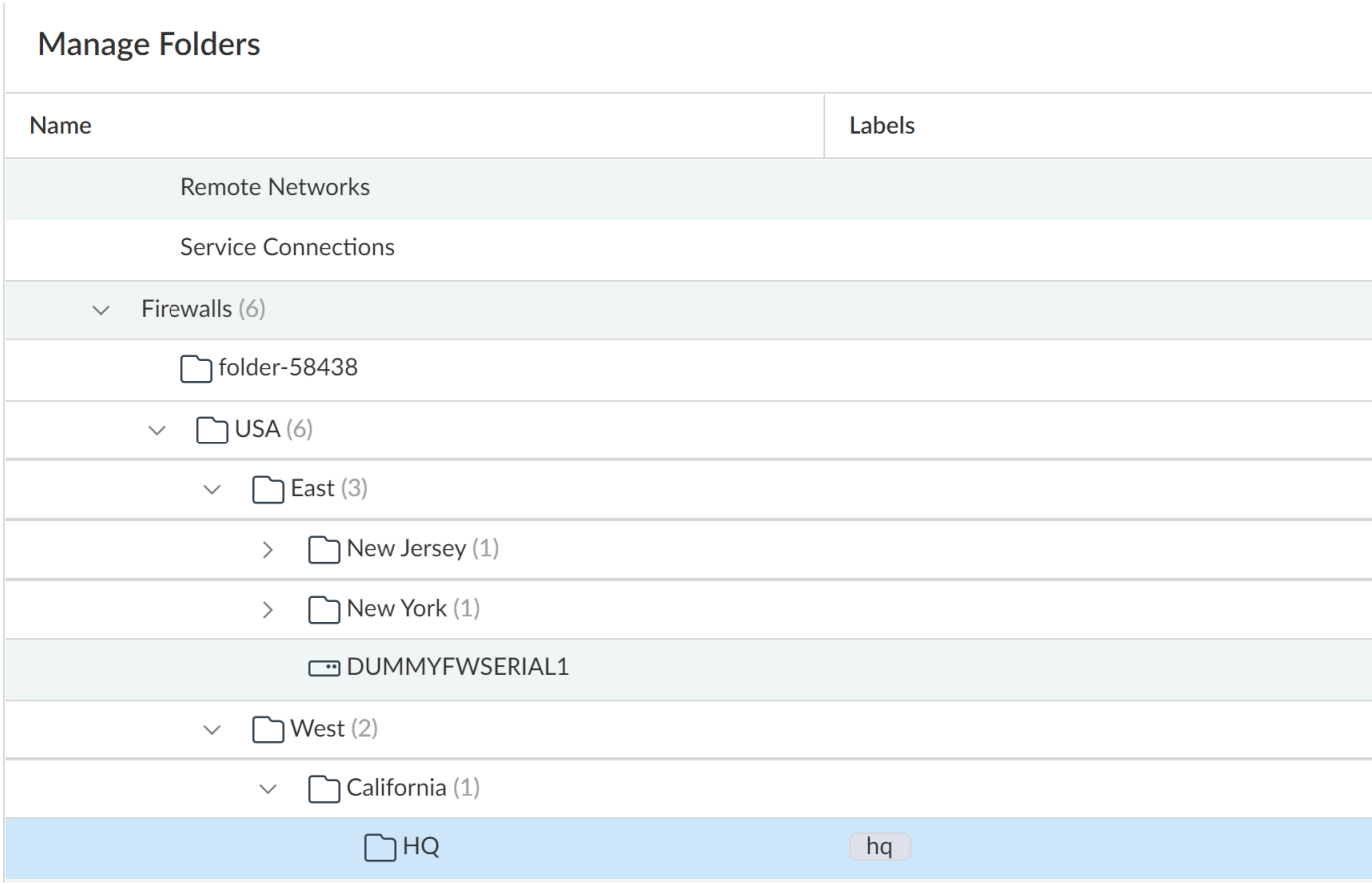
STEP 7 | **Create**（创建）文件夹。

修改文件夹

修改现有文件夹以编辑名称、描述以及添加或更改标签。此外，您可以根据需要移动或删除文件夹。

STEP 1 | 登录 Strata Cloud Manager。

STEP 2 | 选择 **Workflows**（工作流） > **NGFW Setup**（**NGFW** 设置） > **Folder Management**（文件夹管理），展开"操作"菜单。



STEP 3 | 根据需要修改文件夹。

- **Edit**（编辑）文件夹
  1. 编辑文件夹 **Name**（名称）。
  2. （可选）编辑文件夹 **Description**（说明）。
  3. 选择或创建 **Labels**（标签）。

     您可以为文件夹分配完全不同的标签或添加其他标签。
  4. **Save**（保存）。
- **Move**（移动）文件夹并选择 **Destination**（目标位置）。

  您可以通过以下方式移动文件夹。
  - 您可以移动一个文件夹以将其嵌套到其他文件夹下。
  - 您可以将嵌套文件夹移到 `Firewalls` 文件夹下。
  - 您可以将嵌套文件夹从一个文件夹移动到另一个文件夹。

  选择文件夹目标位置后 **Move**（移动）文件夹。
- **Delete Folder**（删除文件夹），然后单击 **OK**（确定），以便确认。

  您只能删除没有与之关联的防火墙且没有嵌套在其下的文件夹。

文件夹管理 (Prisma Access)

Prisma Access 文件夹是预定义的;您可以使用它们来指定配置范围，并确保 Prisma Access 部署类型（移动用户、远程网络和服务连接）接收所有全局设置，然后接收每种类型所需的或特定的设置。

在文件夹下定义的配置将由嵌套在该文件夹层次结构下的所有文件夹继承。例如，您可以在 **Prisma Access** 文件夹中配置 GlobalProtect、显式代理、远程网络和服务连接共用的设置。同样，您可以在移动用户容器中配置 GlobalProtect 和显式代理等共用的设置。

您无法编辑 Prisma Access 的文件夹层次结构。

在文件夹级别，对于 Prisma Access 移动用户、远程网络或服务连接部署，您还可以启用网络安全。

工作流程：Prisma SD-WAN 设置

在何处可以使用？	需要提供什么？
• Prisma SD-WAN	❑ Prisma SD-WAN 许可证

您可以使用 Strata Cloud Manager 在 Prisma SD-WAN 中设置分支机构站点、数据中心站点和 ION 设备。

选择 **Workflows**（工作流） > **Prisma SD-WAN Setup**（设置）。

您可以为以下各项设置工作流：

- 分支站点

  使用 **Branch Sites**（分支站点）选项卡在您的网络中设置分支站点。一个企业可以在一个网络中拥有一个或多个分支机构。创建分支时，可以选择默认域和策略规则集，并配置广域网、电路类别、电路标签和电路规范。

- 数据中心

  使用 **Data Centers**（数据中心）选项卡在您的网络中设置数据中心站点。数据中心站点连接到分支机构站点，您可以在数据中心托管企业应用程序和服务。

- 设备

  使用 **Devices**（设备）选项卡在您的网络中设置 ION 设备。ION 设备可以部署在分支机构站点或数据中心站点。它们有硬件和软件两种外形规格，可满足任何位置和任何部署场景的需求。您必须为分支机构和数据中心站点连接、声明、分配和配置 ION 设备。

工作流程：Prisma Access 设置

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager)	Prisma Access 许可证

要开始设置 Prisma Access，请选择 **Workflows**（工作流程） > **Prisma Access Setup**（设置）。

- 设置服务基础设施，从而在远程网络位置、移动用户以及总部或数据中心之间建立通信。您计划通过服务连接将这些总部和数据中心连接到 Prisma Access。服务连接提供与数据中心的连接。
- 加入移动用户并确定如何将其连接到 Prisma Access。
- 加入远程网络，以保护远程网络位置（如分支机构）以及这些分支机构中的用户。远程站点需要新一代防火墙或符合 IPSec 标准的第三方设备（包括 SD-WAN），该设备可以与服务建立 IPSec 隧道。
- 添加服务连接，使移动用户和分支机构网络中的用户都能访问总部 (HQ) 或数据中心 (DC) 内的资源。除了提供对公司资源的访问，服务连接还允许您的移动用户到达分支机构。

工作流程：Prisma Access

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager)	Prisma Access 许可证

在使用 Prisma Access 之前，为了保护您的远程网络和移动用户，您必须配置基础设施子网。

Prisma Access 使用子网创建网络主干，用于在分支网络、移动用户和 Prisma Access 安全基础设施之间的通信，并创建您计划通过服务连接连接到 Prisma Access 的总部和数据中心网络。如果您对远程网络或服务连接使用动态路由，则还必须配置符合 RFC 6696 的 BGP 私有 AS 编号。

为 Prisma Access 添加基础设施子网时，请遵循以下建议和要求。

- 使用符合 RFC 1918 的子网。尽管 Prisma Access 支持使用不符合 RFC 1918 的（公共）IP 地址，但由于可能与互联网公共 IP 地址空间发生冲突，因此不建议使用。
- 请勿指定与 169.254.169.253、169.254.169.254 和 100.64.0.0/10 子网范围重叠的任何子网，因为 Prisma Access 保留这些 IP 地址和子网供其内部使用。此子网是现有网络的扩展，因此不能与您在公司网络中使用的任何 IP 子网或您为 Prisma Access用户）或 Prisma Access网络）分配的 IP 地址池重叠。由于服务基础设施需要大量 IP 地址，因此必须指定一个 /24 子网（例如，172.16.55.0/24）。
- 输入 Prisma Access 可用于在远程网络位置、移动用户，以及总部或数据中心之间通信的基础设施子网。您计划通过服务连接将这些总部和数据中心连接到 Prisma Access。使用符合 RFC 1918 的子网作为基础设施子网。

请参阅 Prisma Access 设置以了解更多信息。

设置基础设施的 DNS

Prisma Access 允许您指定域名系统 (DNS) 服务器来解析组织内部域和外部域。Prisma Access 根据您的 DNS 服务器配置代理 DNS 请求。

设置基础设施 DNS 将提供对公司网络上的服务（如 LDAP 和 DNS 服务器）的访问，特别是，如果您计划设置服务连接以提供对总部或数据中心的这些类型资源的访问。对内部域列表中的域的 DNS 查询将发送到您的本地 DNS 服务器，以确保资源可供 Prisma Access 远程网络用户和移动用户使用。

这将设置适用于所有流量的内部域列表。如果您愿意，可以查看管理指南，了解如何创建仅适用于特定移动用户部署或远程网络站点的内部域列表。

为基础设施设置 DNS 的好处是：

- 使 Prisma Access 能够解析您的内部域名
- 设置 DNS 以解析内部和外部域
- 在域列表中的域前使用通配符 (*)，例如 *.acme.local 或 *.acme.com

有关详细信息，请参阅 Prisma Access的 DNS。

工作流程：移动用户

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Access 许可证 ❑ Strata Logging Service 许可证

在配置移动用户之前，请确保您拥有所需的许可证（Prisma Access 用于移动用户的许可证，以及具有适当防火墙存储空间的 Strata Logging Service 许可证）。如果移动用户要连接到其他已连接的网络，您将需要提供连接所需的企业接入节点 (CAN) 的零信任网络访问 (ZTNA) 或企业版 Prisma Access 许可证。

首先，请选择您的连接类型，或者您可以使用 GlobalProtect、显式代理（或同时使用两者）。对于这两种连接类型，您刚开始只需要填写一些必需的设置即可启用 Prisma Access 来配置您的移动用户环境。

1. 连接到 Prisma Access。

   确定您设置位置的移动用户应如何连接 Prisma Access。您可以在 GlobalProtect 和显式代理连接之间划分您的移动用户许可证；一些用户可以通过 GlobalProtect 连接，其他用户可以通过显式代理连接。

   安装在移动用户设备上的 GlobalProtect 应用程序会将流量发送到 Prisma Access。
2. 设置基础设施。

   设置基本基础设施设置，然后配置特定于您的连接类型（GlobalProtect 或 Explicit Proxy）的基础设施设置。

   移动用户设备上的代理自动配置 (PAC) 文件将浏览器流量重定向至 Prisma Access。

3. 选择 Prisma Access 位置。

   该地图显示您可以为用户部署 Prisma Access 的全球区域：北美、南美、欧洲、非洲、中东、亚洲、日本、澳大利亚和新西兰。此外，Prisma Access 在每个区域内提供多个位置，以确保您的用户可以连接到提供根据用户所在区域定制的用户体验的位置。为了获得最佳性能，请选择全部。或者，选择每个选定区域内用户需要访问的特定位置。通过将部署限制在单个区域，您可以更精细地控制已部署区域，并排除策略或行业法规要求的区域。

4. 添加 Prisma Access 位置。

   配置设置以添加您想要为用户提供支持的 Prisma Access 位置。

5. 对移动用户进行身份验证。

   设置用户身份验证，以便只有合法用户才能访问您的服务和应用程序。要测试您的设置，您可以添加 Prisma Access 在本地进行身份验证的用户，也可以直接设置企业级身份验证。

将初始配置推送到 Prisma Access，Prisma Access 开始配置您的移动用户环境。这可能需要最多 15 分钟。当您的移动用户位置启动并运行时，您将能够在“移动用户设置”页面、“摘要概述”页面以及 Prisma Access 见解中验证。

有关详细信息，请参阅 Prisma Access 移动用户。

工作流程：远程网络

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager)	Prisma Access 许可证

当您准备将远程网络连接 Prisma Access 时，您需要知道将接入多少个站点。此信息将帮助您确定连接要求，例如如何通过 Prisma Access 路由流量。在规划远程网络部署时，您需要知道哪些应用程序将通过 Prisma Access，以便正确配置最佳的安全策略规则。同样重要的是建立您的威胁配置文件配置。此外，您需要考虑对所有规则应用一致的威胁、URL 和 WildFire 扫描，以制定一致的威胁缓解策略。

有关更多信息，请参阅Prisma Access远程网络。

工作流程：服务连接

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager)	Prisma Access 许可证

服务连接使移动用户和分支网络的用户都可以访问总部 (HQ) 或数据中心 (DC) 的资源。除了提供对公司资源的访问，服务连接还允许您的移动用户到达分支机构。

选择 **Workflows**（工作流） > **Prisma Access Setup**（设置） > **Service Connections**（服务连接），以便添加服务连接。

您创建的第一个隧道是服务连接的主隧道。重复此工作流，以选择性地设置辅助隧道。当两个隧道都打开时，主隧道优先于辅助隧道。如果主服务连接隧道发生故障，则连接将返回辅助隧道，

直到主隧道恢复。根据您用于建立隧道的 IPSec 设备，Prisma Access 提供内置的、推荐的 IKE 和 IPSec 安全设置。您可以使用建议的设置快速入门，也可以根据您的环境需要进行自定义。

有关详细信息，请参阅 Prisma Access 服务连接。

工作流程：远程浏览器隔离

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Access 5.0 创新 ❑ 使用移动用户或远程网络许可证订阅的 Prisma Access 许可证 ❑ 远程浏览器隔离许可证

Palo Alto Networks 的远程浏览器隔离 (RBI) 是一种解决方案，它可以隔离用户托管设备和企业网络中的所有浏览活动，并将其传输到外部实体（如 Prisma Access），从而保护并隔离其平台内潜在的恶意代码和内容。

RBI 与 Prisma Access 原生集成，可让您轻松将隔离配置文件应用于现有安全策略。所有隔离的流量都经过云交付安全服务 (CDSS) 提供的分析和威胁防御，如Advanced Threat Prevention、Advanced WildFire、高级 URL 筛选、DNS Security 和 SaaS Security。

当您准备将用户加入 RBI 时，请考虑要启用哪些 URL 类别，以便用户隔离浏览。想一想您要禁止用户执行哪些浏览器操作，例如复制和粘贴功能、键盘输入以及上传、下载和打印文件等共享选项。

有关详细信息，请参阅远程浏览器隔离。

工作流程：软件升级

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • NGFW (Managed by Strata Cloud Manager)	至少需要其中一个许可证来通过 Strata Cloud Manager 管理您的配置；要统一管理 NGFW 和 Prisma Access，您将需要 NGFW 和 Prisma Access 许可证： ❑ Prisma Access 许可证 ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Pro

使用 Strata Cloud Manager 来规划和管理 NGFW 和 Prisma Access 的软件升级。以下是您可以执行的工作流程：

- 升级建议:创建升级建议以确定可升级的设备的最佳软件版本。软件升级建议 分析防火墙上启用的功能并提供自定义建议。
- Prisma Access 升级指示板:为某些 Prisma Access 升级选择首选时间窗口。
- NGFW - 计划程序:安排 PAN-OS 软件更新，以便在您选择的日期和时间将防火墙升级或降级为目标 PAN-OS 版本。
- NGFW
- Prisma Access

软件升级 (NGFW)

选择 **Workflows**（工作流） > **Software Upgrades**（软件更新） > **Upgrade Recommendations**（升级建议），通过分析设备并创建升级建议来规划设备的升级。

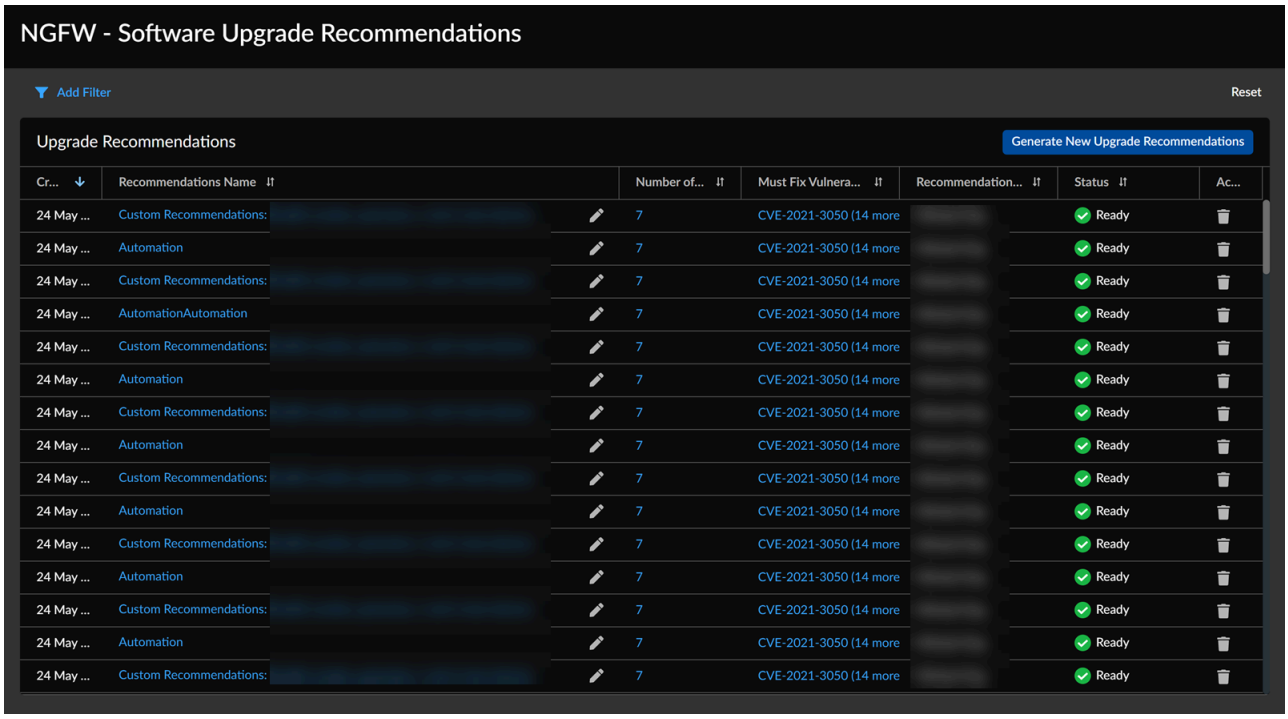
升级建议

在 **Workflows**（工作流） > **Software Upgrades**（软件升级） > **Upgrade Recommendations**（升级建议）中，您可以创建建议来确定可升级设备的最佳软件版本。软件升级建议分析防火墙上启用的功能，并提供自定义建议，其中包括：

- 您可以升级的设备的最佳软件版本。
- 有关每个推荐软件版本中的新功能、行为更改、漏洞和软件问题的信息。

升级建议的类型包括：

- 系统生成的建议，每周生成一次，包含建议的升级选项。
- 用户生成的自定义建议，这些建议是根据所选设备针对Security Advisory 摘要中的特定 CVE 生成的。
- 用户生成的建议，这些建议根据防火墙上传的技术支持文件 (TSF) 生成。



对于 **Upgrade Recommendations**（升级建议）中的每项每个，您可以：

- 查看需要升级的设备数量和必须修复漏洞。
- 编辑建议报告的名称以区分自定义报表。
- 按“创建日期”、“计划名称”和“建议生成条件”筛选建议报告。
- 删除失败或不再需要的升级建议。

单击建议报告可查看包含设备升级选项的详细报告。选择一个升级选项以查看关于新功能、**PAN-OS Known Vulnerabilities**（**PAN-OS** 已知漏洞）、**Changes of Behavior**（行为变更）和 **PAN-OS Known Issues**（**PAN-OS** 已知问题）的更多详细信息。对于 **PAN-OS Known Issues**（**PAN-OS** 已知问题）下的已知问题，请单击由报告此问题的客户数量获得 **Associated Case Count**（关联的案例计数）。

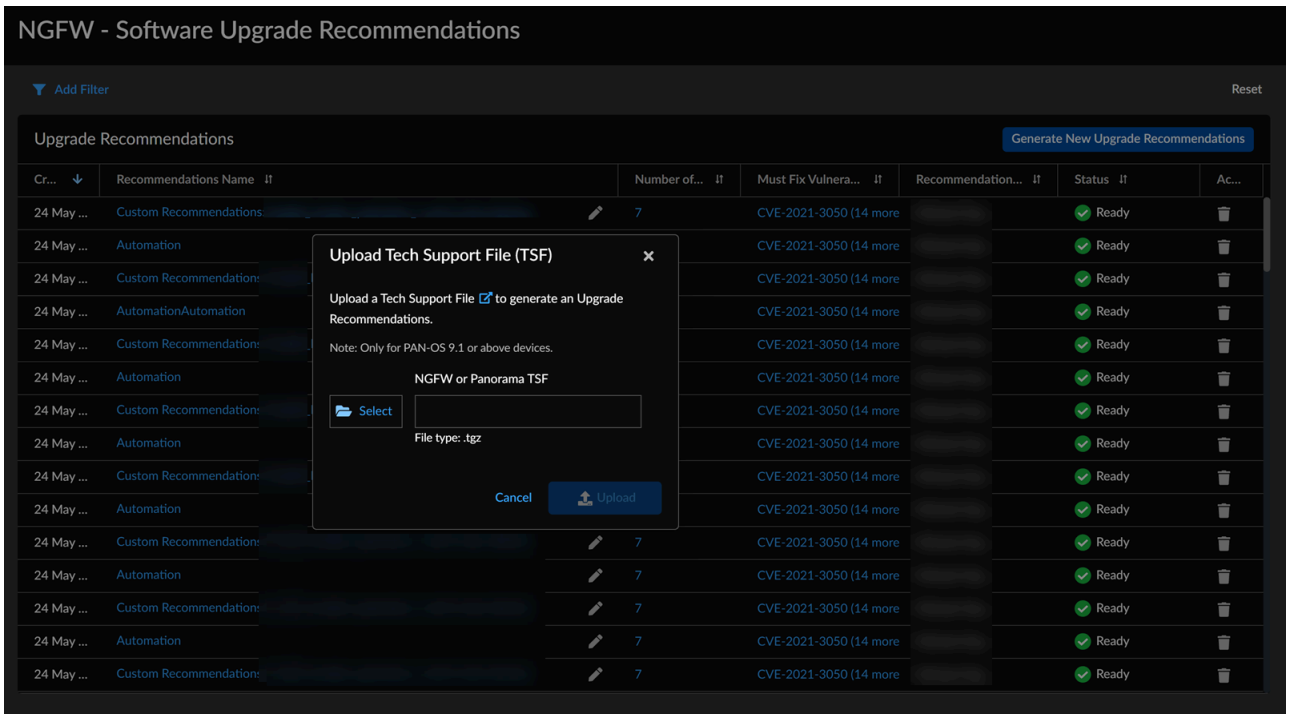
单击 **Export**（传出），以 CSV 格式下载此报告。

生成按需软件升级建议

1. 导航到 **Workflows**（工作流）> **Software Upgrades**（软件升级）> **Upgrade Recommendations**（升级建议）。
2. **Generate New Upgrade Recommendations**（生成新的升级建议）。

3. **Select**（选择）技术支持文件 (TSF) 并 **Upload**（上传）。

   - 您一次只能上传一台设备的 *TSF*，并且该 *TSF* 必须是 *.tgz* 文件格式的 *TSF*。
   - 软件升级建议支持从具有 *PAN-OS* 版本 *9.1* 或更高版本的设备使用 *TSF* 生成报告。



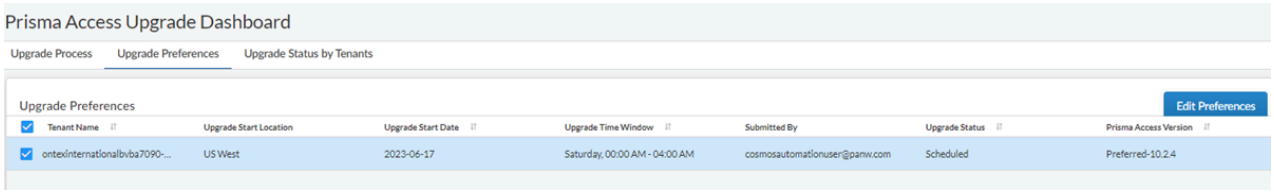
4. 查看状态显示为 **Ready**（就绪）。您还可以检查 **Status**（状态）列，查看是否存在与 TSF 文件的上传、文件格式或处理相关的任何错误。

软件升级 (Prisma Access)

选择 **Workflows**（工作流） > **Software Upgrades**（软件升级） > **Prisma Access**，以查看关于 Prisma Access 数据平面升级流程的信息。

您可以：

- 了解 Prisma Access 数据平面升级过程。
- 选择您的升级首选项：



选择一个租户名称以选择您的升级首选项。有关详细信息，请参阅为某些 Prisma Access 升级选择首选窗口。

工作流程：Prisma Access Browser

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager)	❑ 具有 Prisma Access Browser 捆绑许可证的 Prisma Access ❑ 超级用户或 Prisma Access Browser 角色

选择 **Workflows**（工作流） > **Prisma Access Setup**（设置） > **Prisma Access Browser**，以便加入您的 Prisma Access Browser。

Prisma Access Secure Enterprise Browser (Prisma Access Browser) 是唯一通过本机集成的企业浏览器来保护托管和非托管设备的解决方案，可将保护扩展到非托管设备。参阅什么是 Prisma Access Browser？

加入包括一系列步骤，您将在其中配置以下项目：

- 用户身份验证和组
- Prisma Access 集成
- 路由
- 强制实施 SSO 应用程序
- 下载和分发
- 浏览器策略

在 Strata Cloud Manager 上加入 Prisma Access Browser。

报告：Strata Cloud Manager

在何处可以使用？	需要提供什么？
• Prisma Access （利用 *Strata Cloud Manager* 或 *Panorama* 配置管理） • NGFW （利用 *Strata Cloud Manager* 或 *Panorama* 配置管理） • Prisma SD-WAN	❑ 这些许可证中的每一个都包括 Strata Cloud Manager 访问权限： ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro ❑ Prisma SD-WAN ❑ 软件 NGFW 积分 （适用于 *VM-Series* 软件 *NGFW*） ❑ WAN Clarity 报告许可证 ❑ 具有下载、共享和安排报告权限的角色 。

在 Strata Cloud Manager 中获取有关网络流量模式、带宽利用率和安全订阅数据的报告。报告提供有关您的网络的可操作见解，您可以将其用于规划和监控目的。某些 Prisma Access 和 NGFW 指示板、Activity Insights 概述和 Prisma SD-WAN 支持报告。Prisma Access 和 NGFW 用户具有使用指示板的完全权限，可以将指示板数据下载为 PDF，在其组织内共享报告，并安排报告定期发送到他们的电子邮件收件箱。报告是 Prisma SD-WAN 中的许可订阅服务。您可以下载并查看 Prisma SD-WAN 中的控制器、跨站点和电路的报告。

在 Strata Cloud Manager 中查看这些报告：

- Prisma Access 和 NGFW - 您可以从 Prisma Access 和 NGFW 指示板 和 Activity Insights 生成报告。这些图标指示板右上角的  表示此指示板支持报告。您还可以直接从 **Reports**（报告）菜单生成、下载、共享和安排报告。
- Prisma SD-WAN - 查看以下 WAN Clarity 报告：
  - WAN Clarity 分支机构报告
  - WAN Clarity 数据中心报告
  - 聚合带宽使用情况报告
- Prisma Access 和 NGFW
- Prisma SD-WAN

报告（Prisma Access 和 NGFW

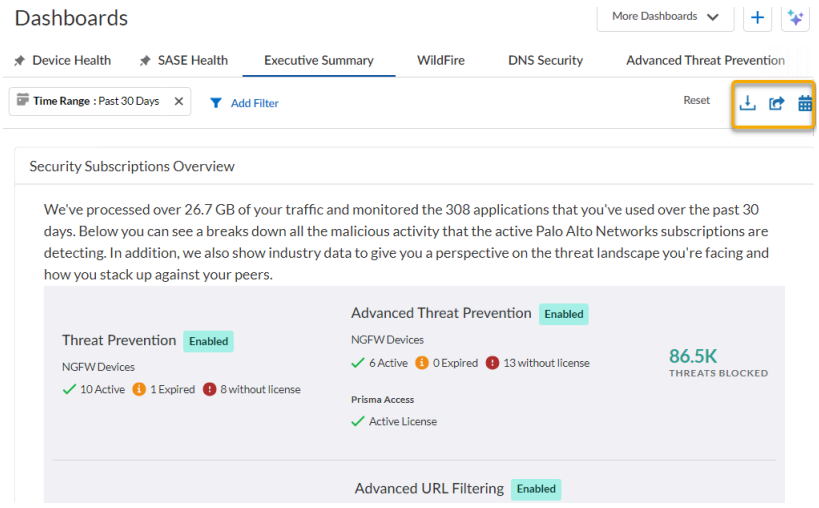
指示板和 Activity Insights 摘要可以作为 PDF 报告在您的组织内共享，并且您还可以安排报告，以便定期(每日、每周或每月）将它们发送到您的电子邮件收件箱和同事的收件箱。

这样，您可以轻松与组织中的人员共享报告，请为此应用设置云身份引擎（目录同步）。云身份引擎为应用程序提供了对 Active Directory 信息的只读访问权限。设置云身份引擎后，您可以轻松将收件人添加到计划报告。系统会根据 Cloud Identity Engine 检查您的报告收件人，如果未找到匹配项，则会执行额外的验证步骤，即根据与您的支持帐户关联的电子邮件地址域检查电子邮件地址域。这些检查可确保报告不会发送到组织外部。

您可以直接从 **Reports**（报告）菜单，或从单个 **Dashboard**（指示板）页面和 **Insights**（见解）**> Activity Insights > Overview**（概览）页面下载、共享或安排报告。报告以 PDF 形式共享和下载。

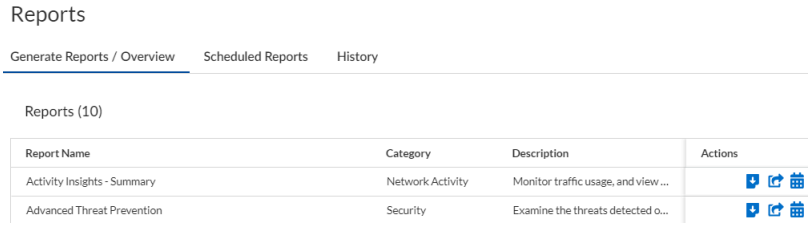
要下载、共享或安排报告，请执行以下操作：

STEP 1 | 单击 **Dashboard**（指示板）页面上的其中任何一个图标 ，或者从 **Insights**（见解）**> > Activity Insights > Overview**（概览）页面上单击。



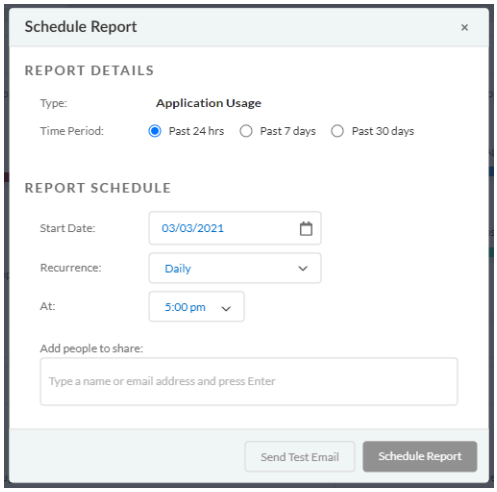
或

单击 **Strata Cloud Manager > Reports**（报告） **> Generate Reports/Overview**（生成报告/概览），然后从报告格式列表中选择其中任何一个图标 。默认情况下，根据要为其生成报告的指示板类型，使用过去 24 小时数据或 30 天数据生成报告。在计划报告时，您可以自定义要在报表中收集数据的时间段。

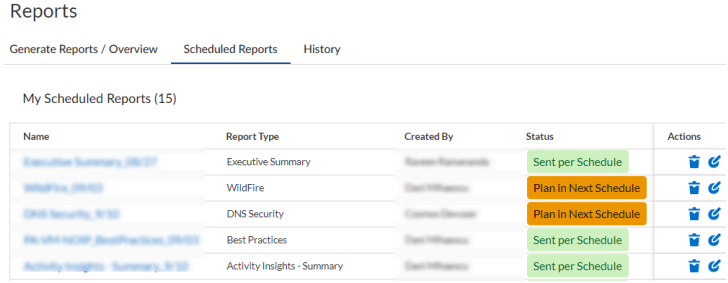


STEP 2 | 如果您正在安排报告，则需要继续定义报表参数，包括：

- 收集数据的 **Time Period**（时间段）
- **Recurrence**（重复），即您希望报告交付的频率（每日、每周或每月）



您可以从 **Strata Cloud Manager** > **Reports**（报告） > **Scheduled Reports**（计划报告）选项卡中查看、编辑或删除所有计划报告。



History（历史记录）显示过去 30 天内下载的所有报告。

报告 (Prisma SD-WAN)

Prisma SD-WAN WAN Clarity 报告提供网络中流量分配和带宽利用率的聚合视图。您可以下载整个报表包，也可以从 Prisma SD-WAN 控制器，允许进行每周趋势比较，以及跨站点和电路的比较。

报表可作为许可订阅服务立即使用。请联系 Prisma SD-WAN 销售团队以启用订阅。

Prisma SD-WANWAN Clarity 报告包括：

- WAN Clarity 分支报告
- WAN Clarity 数据中心报告
- 聚合带宽使用情况报告

要查看报告：

STEP 1 | 选择 **Reports**（报告） > **Prisma SD-WAN**。

STEP 2 | 单击 **WAN Clarity Reports**（**WAN Clarity** 报告）上的 **View Reports**（查看报告）。

STEP 3 | 选择 **Time Range**（时间范围），并在 **Report for**（报告）字段中选择以下任何一个。

- 分支
- 数据中心
- 总带宽使用情况

收藏夹：Strata Cloud Manager

在何处可以使用？	需要提供什么？
• Prisma Access （利用 *Strata Cloud Manager* 或 *Panorama* 配置管理） • NGFW （利用 *Strata Cloud Manager* 或 *Panorama* 配置管理）	❑ 这些许可证中的每一个都包括 Strata Cloud Manager 访问权限： ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro ❑ 任何租户或租户服务组 (TSG) 支持的应用程序 ❑ 根据您的需要选择角色

收藏夹功能可让您保存感兴趣的项目，然后在需要时从 Strata Cloud Manager 中的任何位置快速访问它们。您可以通过组织、编辑和删除列表内容来个性化您自己的私人列表中您最喜欢的菜单项名称。

按照如下方式管理您的收藏夹：

- 添加收藏项目
- 查看收藏项目
- 编辑收藏项目
- 删除收藏项目

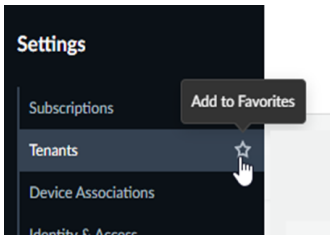
添加收藏项目

在何处可以使用？	需要提供什么？
• Prisma Access （利用 *Strata Cloud Manager* 或 *Panorama* 配置管理） • NGFW （利用 *Strata Cloud Manager* 或 *Panorama* 配置管理）	❑ 这些许可证中的每一个都包括 Strata Cloud Manager 访问权限： ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro ❑ 任何租户或租户服务组 (TSG) 支持的应用程序 ❑ 根据您的需要选择角色

如果有需要经常访问的 Strata Cloud Manager 菜单项目或页面，但您不想再搜索或导航到这些位置，则可以将这些项目保存到收藏夹列表中。

STEP 1 | 导航到要保存的菜单项或页面。

STEP 2 | 将鼠标悬停在项目上可看到星号图标。



STEP 3 | 选择星号即可将该项目添加到您的 **Favorites**（收藏夹）中。

无法将最高级菜单项添加到收藏夹中。只能将子菜单添加到收藏夹中。

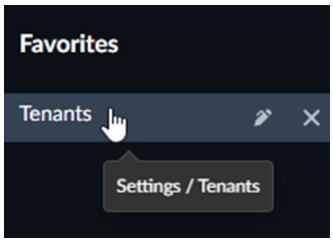
查看收藏项目

在何处可以使用？	需要提供什么？
• Prisma Access （利用 *Strata Cloud Manager* 或 *Panorama* 配置管理） • NGFW （利用 *Strata Cloud Manager* 或 *Panorama* 配置管理）	❑ 这些许可证中的每一个都包括 Strata Cloud Manager 访问权限： ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro ❑ 任何租户或租户服务组 (TSG) 支持的应用程序 ❑ 根据您的需要选择角色

添加收藏后，可以查看收藏夹及其原始位置。

STEP 1 | 选择 **Favorites**（收藏夹）。

STEP 2 | 将鼠标悬停在项目上可查看位置图标。



STEP 3 | 将显示实际位置的路径和菜单名称。

单击收藏夹列表中的项目将带您到其原始位置。

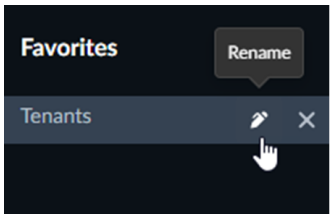
编辑收藏项目

在何处可以使用？	需要提供什么？
• Prisma Access （利用 *Strata Cloud Manager* 或 *Panorama* 配置管理） • NGFW （利用 *Strata Cloud Manager* 或 *Panorama* 配置管理）	❑ 这些许可证中的每一个都包括 Strata Cloud Manager 访问权限： ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro ❑ 任何租户或租户服务组 (TSG) 支持的应用程序 ❑ 根据您的需要选择角色

添加收藏项目后，您可以编辑收藏项目来对其进行个性化设置。

STEP 1 | 选择 **Favorites**（收藏夹）。

STEP 2 | 将鼠标悬停在项目上方可查看编辑图标。



STEP 3 | 重命名该项目。

重命名收藏夹列表中的项目不会重命名原始项目的原始位置。

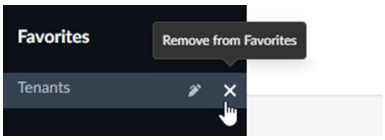
删除收藏项目

在何处可以使用？	需要提供什么？
• Prisma Access （利用 *Strata Cloud Manager* 或 *Panorama* 配置管理） • NGFW （利用 *Strata Cloud Manager* 或 *Panorama* 配置管理）	❑ 这些许可证中的每一个都包括 Strata Cloud Manager 访问权限： ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro ❑ 任何租户或租户服务组 (TSG) 支持的应用程序 ❑ 根据您的需要选择角色

添加收藏项目后，您可以从列表中删除收藏项目。

STEP 1 | 选择 **Favorites**（收藏夹）。

STEP 2 | 将鼠标悬停在项目上可查看删除图标。



STEP 3 | 单击图标从列表中删除收藏项目。

从收藏夹列表中删除项目不会删除原始位置的原始项目。

设置：Strata Cloud Manager

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager)	❑ 任何租户或租户服务组 (TSG) 支持的应用程序 ❑ 根据您的需要选择角色 ❑ Strata Logging Service 以管理日志

从 **Settings**（设置）中，您可以管理与 Strata Cloud Manager 相关的流程。这些流程包括：

订阅

查看您的产品已批准的订阅。

管理订阅。

Device Associations

最常用于设备和应用程序入门，**Device Associations** 使您能够：

- 将新设备与租户关联
- 将应用与设备关联
- 管理设备和应用关联

开始进行设备关联。

产品

如果您拥有单租户环境，请查看、启动和管理您的产品：

- 获取产品信息
- 重命名实例
- 管理共享
- 添加租户

开始产品管理。

租户

如果您是托管安全服务提供商 (MSSP) 或分布式企业，您可以创建和管理由租户表示的业务组织和单位层次结构。从 **Tenants**（租户） 可以：

- 添加租户
- 编辑租户
- 管理租户许可证

- 删除租户
- 从单租户过渡到多租户部署

开始租户管理。

身份和访问

控制所有应用程序和基于 API 的访问的用户角色和权限的身份验证和授权。通过身份和访问，您可以管理：

- 用户访问
- 服务帐户
- 角色
- 第三方身份提供商集成

开始使用身份和访问。

审核日志

查看 Strata Cloud Manager 用户发起的所有操作的记录

查看审核日志。

ION 许可证管理

为虚拟 ION 设备生成授权令牌。这提供了一组控制，以防止未经授权向环境中添加虚拟设备。

管理 ION 许可证。

用户偏好

自定义您的偏好以满足您的需求。例如，选择您的显示模式。

配置用户偏好设置。

受信任 **IP** 列表

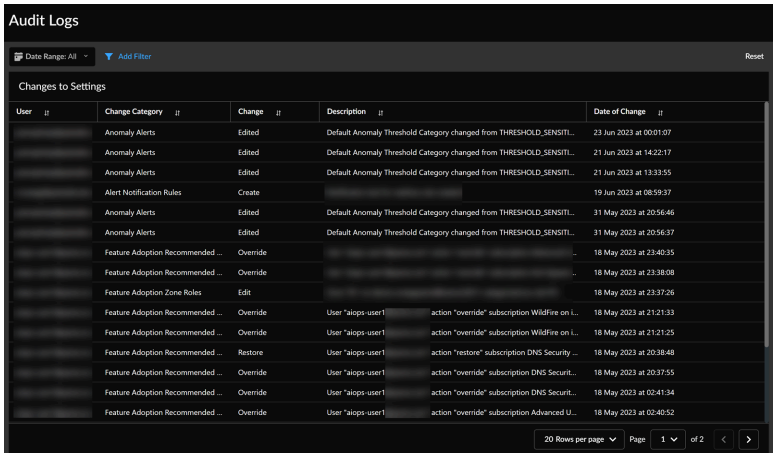
使用受信任的 IP 列表通过指定每个租户允许的 IP 地址来限制对应用程序的访问。

配置可信 IP 列表。

设置：审核日志

在何处可以使用？	需要提供什么？
• Strata Cloud Manager	❑ 其中之一： • AIOps for NGFW Free应用程序 • AIOps for NGFW Premium（使用 Strata Cloud Manager 应用程序） • Strata Cloud Manager Essentials ❑ 以下任何预定义角色：审核员、业务管理员、Data Security 管理员、部署管理员、IAM 管理员、多租户 IAM 管理员、多租户管理用户、多租户监控用户、多租户超级用户、网络管理员、安全管理员、SOC 分析师、超级用户、第 1 层支持、第 2 层支持、仅查看管理员

在 设置（**Settings**）**> Audit Logs**（审核日志）下，您可以看到由 Strata Cloud Manager 用户发起的操作列表。它提供有关所做更改、更改所有者、更改的日期和时间以及更改说明的日志。您可以将这些日志用于合规性和故障排除目的。您可以使用该功能按日期范围、用户、类别和更改类型筛选审核日志。



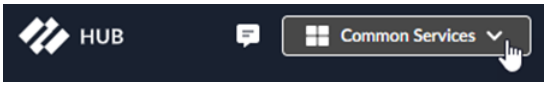
设置：受信任 IP 列表

在何处可以使用？	需要提供什么？
• Strata Cloud Manager	❑ 超级用户、多租户超级用户、多租户 IAM 管理员的 IAM 角色，或具有“受信任 IP 列表”权限集的任何自定义角色

云端交付的应用程序提供了从世界任何地方访问的便利。然而，这会导致使用被盗凭证、字典攻击和其他形式的暴力攻击等风险，从而获取应用程序的访问权限。

虽然身份和访问管理可以减轻部分风险，但您可以使用受信任的 IP 列表通过指定每个租户允许的 IP 地址来进一步限制对应用程序的访问。

默认情况下，在创建新租户期间，允许从任何 IP 地址访问 Web 界面和 API。可信 IP 列表是允许访问租户的可信 IP 地址列表。您可以使用受信任的 IP 列表来限制对单个租户的访问，也可以使用它来限制对多租户层次结构中的父租户及其子租户的访问。在多租户层次结构中，您在父租户上添加受信任的 IP 列表，该列表从父租户继承到其子租户，并从上到下强制执行。

如何从 **Strata Cloud Manager** 管理可信 **IP** 列表	如何从 **hub** 管理可信 **IP** 列表
要从 Strata Cloud Manager 管理可信 IP 列表，请选择 **Settings**（设置） > **Trusted IP List**（可信 **IP** 列表）。  您可以从 Strata Cloud Manager 和 Strata Cloud Manager Web 界面管理可信 IP 列表，API 将仅允许访问仅受信任的 IP。	要从 hub 管理可信 IP 列表，请选择 **tenant view of the hub**（中心的租户视图） > **Common Services**（通用服务） > **Trusted IP List**（可信 **IP** 列表）。  您可以从 hub 管理可信 IP 列表，但 hub 不受可信 IP 执行的约束，因此您对 hub 的访问不仅限于受信任的 IP。如果您的 IP 地址被阻止访问 Strata Cloud Manager 上您本应有权访问的的租户，并且您具有列出的权限，则可以转到 hub 并解锁您的访问权限。

添加可信 IP

删除受信任的 IP

解锁访问

添加可信 IP

在何处可以使用？	需要提供什么？
• Strata Cloud Manager	❑ 超级用户、多租户超级用户、多租户 IAM 管理员的 IAM 角色，或具有“受信任 IP 列表”权限集的任何自定义角色

为 Strata Cloud Manager 激活许可证，创建租户和管理的用户访问权限后，您可以通过将受信任的 IP 地址添加到受信任的 IP 列表来进一步限制对租户的访问。默认情况下，允许访问任何 IP 地址。

使用 Strata Cloud Manager 添加受信任的 IP。

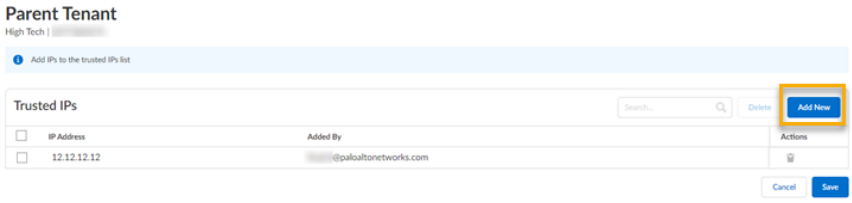
STEP 1 | 选择 **Settings**（设置） > **Trusted IP List**（受信任的 **IP** 列表）。

STEP 2 | 搜索或滚动以查找并选择您的租户。

STEP 3 | 选择 **+Add New**（+新增）。

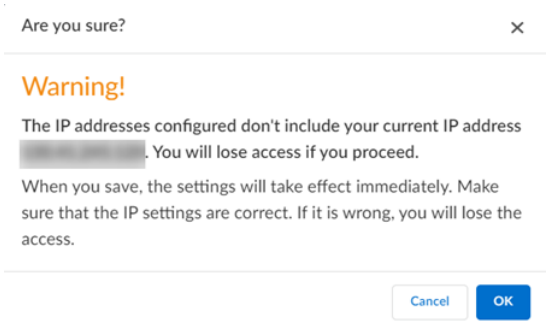
STEP 4 | 输入可以访问此租户的 **IP Address**（**IP** 地址）。

- 该字段支持 CIDR 表示法。仅允许使用 IPv4 地址。
- 您可以使用单个 IP 地址，也可以使用带子网掩码的范围，如 12.12.12.1/30。
- IP 和范围经过验证，因此对于不支持的项目显示错误。
- **Added By**（添加人）字段将自动填充。



STEP 5 | **Save**（保存）。

更改将立即生效，因此请确保您的 *IP* 地址正确，否则您可能无法访问租户。



STEP 6 | 在父租户上添加可信 IP 列表后，该列表将从父租户继承到其子租户，并从上到下强制执行。子租户也可以添加自己的可信 IP 列表。

删除受信任的 IP

在何处可以使用？	需要提供什么？
• Strata Cloud Manager	❑ 超级用户、多租户超级用户、多租户 IAM 管理员的 IAM 角色，或具有“受信任 IP 列表”权限集的任何自定义角色

将可信 IP 添加到租户的可信 IP 列表后，您可以通过删除可信 IP 地址来恢复无限制访问。

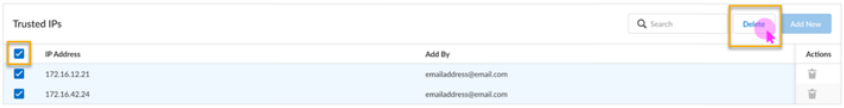
使用 Strata Cloud Manager 删除可信 IP。

STEP 1 | 选择 **Settings**（设置） > **Trusted IP List**（受信任的 **IP** 列表）。

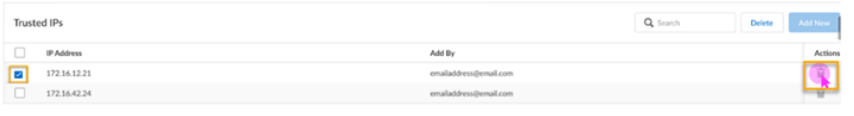
STEP 2 | 搜索或滚动以查找并选择您的租户。

STEP 3 | 使用以下任一选项：

- 删除多个 IP — 选中 **IP Address**（**IP** 地址）复选框以同时突出显示所有 IP 地址，然后选择 **Delete**（删除）按钮。



- 删除单个 IP — 选中单个 IP 的对应复选框，然后单击 **Actions**（操作） > **Delete**（删除），以便将其删除。



如果您从父租户继承了受信任的 *IP* 列表，则不能从子租户中删除它，因为这些列表是继承的。只有直接在子租户级别添加可信 *IP* 列表，才能从子租户中删除该列表。

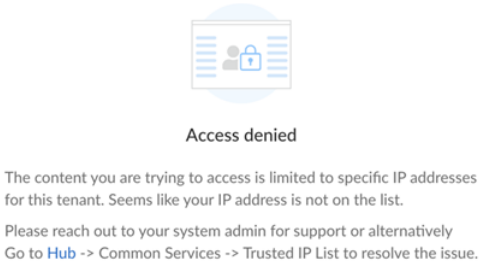
STEP 4 | 在提示下选择 **OK**（确定）。

更改会立即生效。如果您删除所有受信任的 IP，则 IP 访问权限将恢复为 **Any**（任意）。

解锁访问

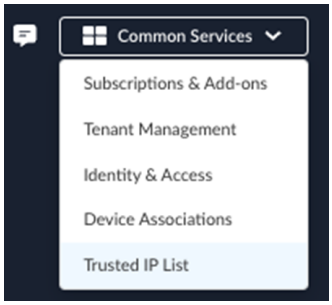
在何处可以使用？	需要提供什么？
• Strata Cloud Manager	❑ 超级用户、多租户超级用户、多租户 IAM 管理员的 IAM 角色，或具有“受信任 IP 列表”权限集的任何自定义角色

将 IP 添加到租户的受信任 IP 列表后，该访问权限将由 Strata Cloud Manager 执行。如果您的 IP 地址不在租户的受信任 IP 列表中，则您在尝试访问时会看到拒绝访问消息。



如果您的 IP 地址被您本应有权访问的租户阻止，并且您具有列出的权限，则可以前往 hub 解锁权限。

STEP 1 | 从 hub 中，选择 **tenant view of the hub**（中心的租户视图） > **Common Services**（通用服务） > **Trusted IP List**（可信 IP 列表）。



STEP 2 | 将您的 IP 地址添加到受信任的 IP 地址列表。

设置：用户偏好

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Strata Cloud Manager	以下许可证之一： ❑ AIOps for NGFW Free 或 AIOps for NGFW Premium 许可证 ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro

在 **Settings**（设置）**> User Preferences**（用户首选项）中，您可以通过修改用户首选项来自定义 Strata Cloud Manager，从而使其满足您的特定需求。这些设置包括：

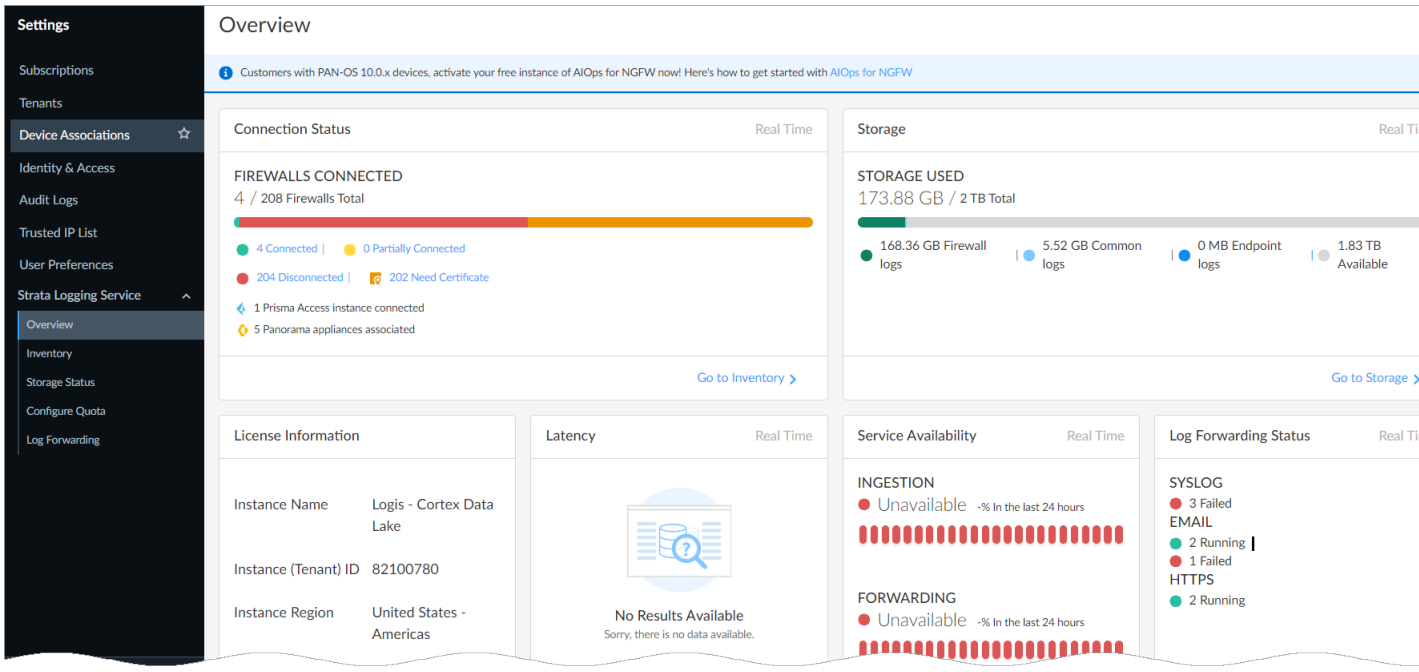
- 浅色/深色/系统模式 — 在深色和浅色显示模式之间进行选择，或选择遵循您自己的系统设置。

设置：Strata Logging Service

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by PAN-OS or Panorama) • NGFW (Managed by Strata Cloud Manager)	❑ Strata Logging Service

Strata Logging Service（原 Cortex Data Lake）是基于云的日志系统，用于存储我们的安全产品生成的上下文丰富的增强型网络日志，包括我们的 NGFW、Prisma Access 和 Cloud NGFW for AWS。借助 Strata Logging Service，您可以收集不断扩大的数据量，而无需规划本地计算和存储，而且从一开始就可以扩展。了解如何在产品中激活和部署 Strata Logging Service。

此外，您还可以使用中心上的 *Strata Logging Service* 应用程序访问和管理日志。*Strata Logging Service* 应用程序和 *Strata Cloud Manager* 中的日志记录数据都相同，只是它们的Web 界面不同。



使用 Strata Logging Service：

- 检查 Strata Logging Service 实例的状态- 单击 **Strata Logging Service** > **Overview**（概览）
- View and onboard（查看和加入）防火墙、Cloud NGFW、Prisma Access 或 Panorama 设备- 单击 **Strata Logging Service** > **Inventory**（清单）

- 已分配日志存储空间配额、可用存储空间，以及根据传入日志速率保留日志的天数 - 单击 **Strata Logging Service** > **Storage Status**（存储状态）
- 配置日志存储空间配额 - 单击 **Strata Logging Service** > **Configure Quota**（配置配额）
- 搜索、筛选和导出日志数据 - 单击 **Incidents & Alerts**（事件和警报） > **Log Viewer**（日志查看器）。日志查看器与 Strata Logging Service 应用程序中的“浏览”功能相同。
- 转发日志数据到外部服务器以进行长期存储、SOC 或内部审核--单击 **Strata Logging Service** > **Log Forwarding**（日志转发）

应用程序体验

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager)	以下许可证之一： ❑ Prisma Access 许可证 ❑ ADEM Observability 许可证或 AI-Powered ADEM 许可证

使用 **Application Experience**（应用程序体验）页面管理您的自治 DEM 用户和远程站点。查看审核日志，查看哪些管理员在所选 **Time Range**（时间范围）内对 Prisma Access 进行了身份验证。

要了解 **Upgrade Options**（升级选项），请参阅管理自治 DEM 代理。

端点代理管理

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager)	以下许可证之一： ❑ Prisma Access 许可证 ❑ ADEM Observability 许可证或 AI-Powered ADEM 许可证

使用此选项卡可以获取所有已注册的 ADEM 用户的详细信息，例如用户是在线（用户设备正在向 ADEM 服务发送保持活动消息）还是离线（ADEM 服务在过去十分钟内未收到来自用户设备的保持活动消息）、用户设备最后一次出现的时间、ADEM 用户的用户名、设备类型和主机名，以及它们正在运行什么 ADEM 代理版本。

此选项卡中表中的每一行代表单独一行中的唯一用户。每个用户/设备组合都被视为唯一的用户。例如，如果 2 个用户分别登录到 3 台设备，则唯一用户的数量将为 6。因此，用户名可以跨多行重复，具体取决于他们登录的设备数量。

在此小部件表的标题中，**Total Endpoint Agents**（端点代理总数）表示监视的设备总数。**Users**（用户数量）是用户总数，与登录的设备数量无关。这是因为许可证消耗基于用户总数，而不管每个用户登录了多少设备。

使用 **Last logged in User**（上次登录的用户）左边的复选框为端点选择进行批量配置的行。从端点代理管理表中选择条目来删除条目，将释放许可证条目。

列名	说明
上次登录的用户	一个设备可以有多个用户登录。此列列出了使用此设备登录到 GlobalProtect 的最近用户的用户 ID。

列名	说明
设备	此设备上运行的操作系统。
主机名	设备的主机名。
上次查看	从设备发送到 DEM 服务器的最后一个消息。
首次查看	DEM 服务器从该设备接收的第一个消息。
用户状态	当前用户的连接状态。
监视状态	设备上是否正在运行应用测试。
端点代理版本	设备上安装的 ADEM 代理的版本。

远程站点代理管理

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager)	以下许可证之一： ❑ Prisma Access 许可证 ❑ ADEM Observability 许可证或 AI-Powered ADEM 许可证

此选项卡为您提供了有关启用数字体验管理的分支机构 Prisma SD-WAN ION 设备的详细信息。使用此选项卡可以获取有关所有已注册 ADEM 远程站点的详细信息，例如设备型号、主机名、站点状态、监视状态（是否为站点启用了监视）、高可用性服务器的主机名（如果有）以及远程站点代理版本。

列名	说明
远程站点名称	Pisma SD-WAN 分支站点。
设备模型	Prisma SD-WAN ION 设备型号。
主机名	ION 设备的主机名。
HA 对等主机名	是否已在该站点配置高可用性备用 ION 设备。
上次查看	从 ION 设备发送到 DEM 服务器的最后一条消息。
首次查看	DEM 服务器从 ION 设备接收的第一条消息。
站点状态	站点 ION 设备与 DEM 代理的连接状态。

列名	说明
监视状态	站点是否配置为运行应用程序测试。
远程站点代理版本	ION 设备上安装的 ADEM 代理的版本。

运行状况评分概况

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager)	以下许可证之一： ❑ Prisma Access 许可证 ❑ ADEM Observability 许可证或 AI-Powered ADEM 许可证

在此选项卡中查看域名运行状况分数的详细信息。

列名	说明
域名运行状况评分指标名称	列出计算运行状况评分指标的域名。单击此列中的域名可查看其指标，例如下限和上限阈值，以及当数字超过阈值时它对总分的影响程度（占总体验分数的百分比）。目前，这些指标是管理员设置的只读指标。它们无法修改。
类型	域类型
关联用例	显示计算出的体验分数的指示板或小部件。

ADEM 审核日志

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager)	以下许可证之一： ❑ Prisma Access 许可证 ❑ ADEM Observability 许可证或 AI-Powered ADEM 许可证

查看因 API 调用而触发的所有事件的审计日志。

列名	说明
事件时间	触发事件的时间，该事件导致了日志的创建。
email	创建日志时收到通知的人员的电子邮件地址。
说明	导致事件触发从而创建日志的 API 调用。