paloalto TECHDOCS

Prisma Access 发行说明

5.2.0-h14 and 5.2.1

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

October 24, 2024

Table of Contents

Prisma Access 发行信息

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)	❑ Prisma Access 许可证 ❑ Minimum Required Prisma Access Version 5.2 或 5.2.1 Preferred 或 Innovation

关于 **Prisma Access** 发行更新

Prisma Access 发行和更新使您能够保持最新状态并确保用户安全。部分更新由 Palo Alto Networks 管理，例如 Prisma Access 基础设施更新，您将提前收到通知，以便您可以制定周全计划。某些更新由您自己负责，您必须安排指定版本的内容更新和软件更新。如果您使用 Panorama 来管理 Prisma Access（而不是通过 Prisma Access Cloud Management），您可以决定何时升级到最新的插件版本，以便利用该插件为 Panorama 实现的新功能。

如果您使用 Panorama Managed Prisma Access，请查看此 Panorama Managed 版本的 Panorama 和插件要求。

支持与 **Prisma Access** 配套使用的 **GlobalProtect** 版本

任何生命周期 (EoL) 尚未结束的 GlobalProtect 版本均支持与 Prisma Access 一起使用；但请注意，Prisma Access 5.2 也有针对 GlobalProtect 的推荐软件版本和必需版本。

您可以在这里详细了解 Prisma Access 包含或与其集成的产品和服务的最新更新：

最新的 **Prisma Access** 发行更新	之前的 **Prisma Access** 发行版本	**Prisma Access** 支持的服务和附加组件的更新
• Prisma Access 5.2 和 5.2.1 中的新功能 • Prisma Access Cloud Management 的新功能	• Prisma Access 版本 5.1 • Prisma Access 版本 5.0 • Prisma Access 版本 4.2 • Prisma Access 版本 4.1 • Prisma Access 版本 4.0 • Prisma Access 版本 3.2 Preferred 和 Innovation • Prisma Access 版本 3.1 Preferred 和 Innovation • Prisma Access 版本 3.0 Preferred 和 Innovation	• Prisma Access Insights • 自主 DEM • SaaS Security • 企业 DLP • GlobalProtect • Prisma SASE 多租户云管理平台 • Prisma SD-WAN

最新的 **Prisma Access** 发行更新	之前的 **Prisma Access** 发行版本	**Prisma Access** 支持的服务和附加组件的更新
	• Prisma Access 版本 2.2 Preferred • Prisma Access 发行版低于 2.2 Preferred	

Prisma Access 5.2 和 5.2.1 中的新功能

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)	❑ Prisma Access 许可证 ❑ Minimum Required Prisma Access Version 5.2 或 5.2.1 Preferred 或 Innovation

本节为您提供了 Prisma Access 5.2 和 5.2.1 Preferred 和 Innovation，以及您需要使用的推荐软件版本和必需软件版本。

本文档包含路线图信息，分享本文档仅供您参考和规划之用。这不是具有约束力的承诺，可能会发生变化。

- Prisma Access 5.2.1 Preferred 和 Innovation 的推荐软件版本
- Prisma Access 5.2.1 Preferred 和 Innovation 功能的基础设施、插件和数据平面依赖关系
- Prisma Access 5.2.1 功能

Prisma Access 5.2.1 Preferred 和 Innovation 的推荐软件版本

有两个 Prisma Access 5.2.1 版本：

- 5.2.1 Preferred 运行 PAN-OS 10.2.10 数据平面。如果您的部署运行的是较低数据平面版本，则需要将数据平面升级到 PAN-OS 10.2.10 才能实现 5.2.1 Preferred 功能。
- 5.2.1 Innovation 运行 PAN-OS 11.2.4 数据平面。需要升级到 PAN-OS 11.2.4 才能实现 5.2 Innovation 功能。

要使用 Prisma Access 5.2.1 Innovation 的新功能特点，Prisma Access 建议将您的 **Prisma Access** 升级到以下版本，然后再安装插件。

Prisma Access 版本	云服务插件版本	**5.2.1** 所需的数据平面版本	推荐的 **GlobalProtect** 版本	推荐的 **Panorama** 版本
5.2.1	5.2.0 修补程序	PAN-OS 10.2.10（5.2.1 Preferred 所必需） PAN-OS 11.2.4（5.2.1 Innovation 所必需）	6.0.7+ 6.1.3+ 6.2.1+	10.2.10+ 11.0.1+ 11.1.0 11.2.4

Prisma Access 5.2 Preferred 和 Innovation 的推荐软件版本

有两个 Prisma Access 5.2 版本：

- 5.2 Preferred 运行 PAN-OS 10.2.10 数据平面。如果您的部署运行的是较低数据平面版本，则可能需要将数据平面升级到 PAN-OS 10.2.10 才能实现 5.2 Preferred 功能。如果您是现有客户，请参阅 Prisma Access 5.2.1 Preferred 和 Innovation 功能的基础设施、插件和数据平面依赖关系 以了解是否需要升级数据平面 Prisma Access 5.2 功能。
- 5.2 Innovation 运行 11.2.3 的 PAN-OS 数据平面。需要升级到 PAN-OS 11.2.3 才能实现 5.2 Innovation 功能。

要使用 Prisma Access 5.2 Innovation 的新功能特点，Prisma Access 建议将您的 **Prisma Access** 升级到以下版本，然后再安装插件。

Prisma Access 版本	云服务插件版本	**5.2** 所需的数据平面版本	推荐的 **GlobalProtect** 版本	推荐的 **Panorama** 版本
5.2	5.2	PAN-OS 10.2.10（5.2 Preferred 所必需） PAN-OS 11.2.3（5.2 Innovation 所必需）	6.0.7+ 6.1.3+ 6.2.1+	10.2.10+ 11.0.1+ 11.1.0 11.2.3

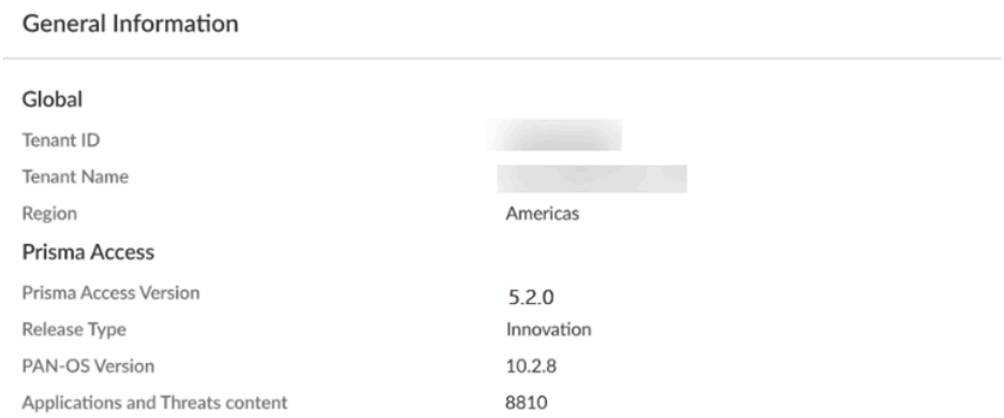
Prisma Access 5.2.1 Preferred 和 Innovation 功能的基础设施、插件和数据平面依赖关系

Prisma Access 5.2.1 功能需要以下一个或多个组件才能运行：

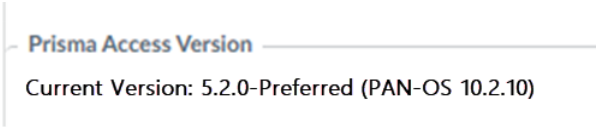
- 基础设施升级：基础设施包括底层服务后端、编排和监视基础设施。Prisma Access 会在 Prisma Access 版本的正式发布 (GA) 日期之前升级基础设施。

  在基础设施升级时，如果某些功能只需基础设施升级即可解锁，则这些功能对所有 Prisma Access 部署都能生效，无论版本如何。
- 插件升级（仅限 **Prisma Access Panorama** 托管的部署）：安装插件将激活该版本可用的功能。您可以在管理 Prisma Access 的 Panorama 上下载并安装插件。

- 数据平面升级：数据平面可以对您的网络和用户流量进行流量检查和实施安全策略。
  - 对于 Prisma Access (Managed by Strata Cloud Manager)，请转到 **Manage**（管理） > **Configuration**（配置） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Overview**（概述）。



  - 对于 Prisma Access (Managed by Panorama) 部署，要查看数据平面版本，您可以转到 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > **Service Setup**（服务设置）并查看 **Prisma Access** 版本。Prisma Access 5.2.1 Preferred 运行 PAN-OS 10.2.10，而 Prisma Access Innovation 运行 PAN-OS 11.2.4。



可以选择将数据平面升级到 *5.2.1 Innovation*，仅当您想利用需要数据平面升级的功能时才需要升级。

只有在基础设施升级后才能为 Prisma Access 激活这些功能：

- 高性能分支站点可见性
- Prisma Access Agent 可观察性
- RFC6598 Prisma Access (Managed by Strata Cloud Manager) 新部署的移动用户地址池
- 分支站点和服务连接的路由表可见性
- 针对查看和监视 ZTNA 连接器的更新
- 基于 View Agent 的显式代理
- 以色列和沙特阿拉伯 Strata 日志记录服务区域支持
- 对现有 Prisma Access 部署的原生 IPv6 支持

这些功能要求基础设施和插件升级，但不要求数据平面升级；但这些功能要求数据平面的版本至少为 10.2.4：

- Colo-Connect 的显式代理支持

- DNS 代理的显式代理支持
- 与 ZTNA 连接器的显式代理集成
- 使用通配符 FQDN 的 ZTNA 连接器策略配置更新
- 显式代理第三方企业浏览器集成

以下 5.2.1 功能要求基础设施和插件升级，并且最低需要数据平面版本 PAN-OS 10.2.10，使其成为 Prisma Access 5.2.1 Preferred 功能：

- 针对应用程序上线的 ZTNA 连接器增强功能
- 无

以下 5.2 功能要求将基础设施、插件和数据平面升级到 PAN-OS 11.2.4，使其成为 Prisma Access 5.2.1 Innovation 功能：

- 远程网络：高性能专用应用程序访问支持
- 针对移动用户的静态 IP 地址增强功能
- 查看移动用户的静态 IP 地址分配

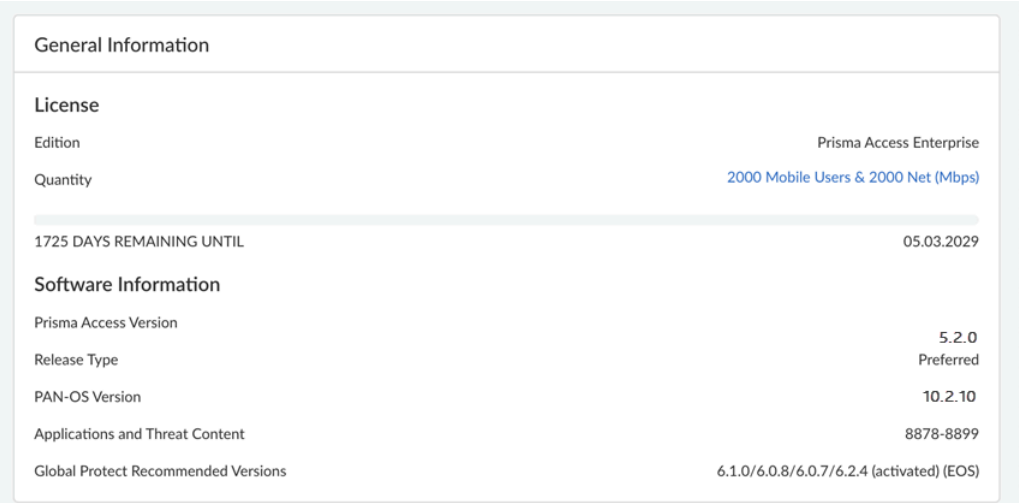
Prisma Access 5.2 Preferred 和 Innovation 功能的基础设施、插件和数据平面依赖关系

Prisma Access 5.2 能需要以下一个或多个组件才能运行：

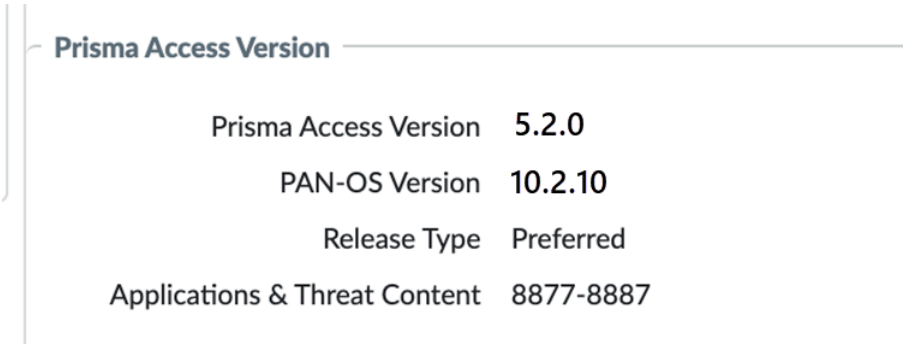
- 基础设施升级：基础设施包括底层服务后端、编排和监视基础设施。Prisma Access 会在 Prisma Access 版本的正式发布 (GA) 日期之前升级基础设施。

  在基础设施升级时，如果某些功能只需基础设施升级即可解锁，则这些功能对所有 Prisma Access 部署都能生效，无论版本如何。
- 插件升级（仅限 **Prisma Access Panorama** 托管的部署）：安装插件将激活该版本可用的功能。您可以在管理 Prisma Access 的 Panorama 上下载并安装插件。

- 数据平面升级：数据平面可以对您的网络和用户流量进行流量检查和实施安全策略。
  - 对于 Prisma Access (Managed by Strata Cloud Manager)，请转到 **Manage**（管理） > **Configuration**（配置） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Overview**（概述）。



  - 对于 Prisma Access (Managed by Panorama) 部署，要查看数据平面版本，您可以转到 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > **Service Setup**（服务设置）并查看 **Prisma Access** 版本。Prisma Access 5.2 Preferred 运行 PAN-OS 10.2.10，而 Prisma Access Innovation 运行 PAN-OS 11.2.3。



可以选择将数据平面升级到 *5.2 Innovation*，仅当您想利用需要数据平面升级的功能时才需要升级。

只有在基础设施升级后才能为 Prisma Access 激活这些功能：

- 端点 DLP
- 针对移动用户，简化了 Prisma Access 与 IP 优化的 SaaS连接，并简化了显式代理部署
- TLS 1.3 和 PubSub 支持流量复制
- 查看和监视 Colo-Connect

这些功能要求基础设施和插件升级，但不要求数据平面升级：

- 25,000 个远程网络和 50,000 个 IKE 网关支持

- 基于代理的代理流量的专用 IP 地址可见性和实施
- 显式代理用户的 IP 地址优化 - 代理部署
- 云服务插件的 RBAC 支持
- 简化 Prisma Access 专用应用连接
- 针对 AWS 的 SP 骨干集成支持
- 在 Strata Cloud Manager 中查看 Prisma Access、数据平面以及应用程序和威胁内容版本

以下 5.2 功能要求基础设施和插件升级，并且最低需要数据平面版本 PAN-OS 10.2.10，使其成为 Prisma Access 5.2 Preferred 功能：

- 远程网络 — 高性能

以下 5.2 功能要求将基础设施、插件和数据平面升级到 Prisma Access 11.2.3，使其成为 Prisma Access 5.2 Innovation 功能：

- 通过 CIAM，针对动态特权访问支持 SC-NAT
- ZTNA 连接器支持无承诺 App 上线

Prisma Access 5.2.1 功能

下表介绍了 Prisma Access 5.2.1 中正式发布的新功能。

Colo-Connect 的显式代理支持

支持以下版本： Prisma Access 5.2.1 Preferred 和 Innovation

如果您具有与主机托管设施直接连接的大型数据中心，您现在可以通过 Prisma Access 显式代理进行连接，从而实现对专用应用程序的高速访问。通过增强功能，您将在每个区域获得高达 20 Gbps 的吞吐量。

将 Colo-Connect 与显式代理集成后，您将获得以下优势：

- 显式代理自动连接到最近的 Prisma Access 计算位置，最大限度降低延迟。
- 消除了网络和路由依赖性，为专用应用提供自动化的安全隧道管理和路由。
- Colo-Connect 支持在重叠网络中检索专用应用程序，确保灵活性和可访问性

DNS 代理的显式代理支持

支持以下版本： Prisma Access (Managed by Strata Cloud Manager) 5.2.1 Preferred 和 Innovation

显式代理扩展了其支持范围，包括 DNS 代理定制。显式代理支持 DNS 设置，例如区域 DNS、自定义 DNS 等。您还可以使用第三方 DNS 解析器或本地 DNS 解析器来解析公共和专用应用程序，并且可以按 FQDN 使用。目前仅 支持此功能。

第三方企业浏览器与显式代理的安全集成

支持以下版本： Prisma Access 5.2.1 Preferred 和 Innovation

Prism Access 现在可以通过第三方企业浏览器实现对专用应用程序的安全访问。通过这一增强功能，可以在第三方企业浏览器和 Prisma Access 之间安全透明地交换用户信息，从而允许在 Prisma Access 中实施基于用户 ID 的策略规则。如果最终用户已经登录到第三方企业浏览器，则无需使用 Prisma Access 重新进行身份验证。

与 **ZTNA** 连接器的显式代理集成

支持以下版本： Prisma Access 5.2.1 Preferred 和 Innovation

通过 ZTNA 连接器连接到专用应用程序的用户现在可以通过 Prisma Access 显式代理建立连接。该集成支持容量高达 10 Gbps 的 ZTNA 连接器，用于 Prisma Access 浏览器和代理服务器。

以下是额外的优势：

- 显式代理自动连接到距离最近的 Prisma Access 计算位置，从而确保延迟最低。
- 消除网络和路由依赖关系，确保专用应用程序的自动化安全隧道管理和路由。
- ZTNA 连接器支持 Cloud Identity Engine (CIE)，后者可以自动发现专用应用程序。
- ZTNA 连接器支持检索重叠网络中的专用应用程序，从而确保灵活性和可访问性。

高性能分支站点可见性

支持以下版本： Prisma Access 5.2.1 Preferred 和 Innovation

与传统分支相比，Prisma Access 中的高性能分支 (RN-HP) 具有独特功能，这两种分支将在客户环境中共存。管理系统必须适应新的 RN-HP 分支类型，以帮助网络管理员进行故障排除。

对现有 **Prisma Access** 部署的原生 **IPv6** 支持

支持以下版本： Prisma Access 5.2.1 Preferred 和 Innovation，所有部署（从 Prisma Access 5.1.1 开始，新部署俊支持 IPv6；Prisma Access 5.2.1 中增加了对现有部署的支持）

Prisma Access 将其对 IPv6 的支持从专用应用程序扩展到对移动用户、远程网络和服务连接的全面端到端 IPv6 支持，并为现有的 Prisma Access 部署增加了本机 IPv6 支持。

支持本机 IPv6 的一个优势是具备如下功能：如果移动用户使用的是仅支持 IPv6 的端点，则移动用户可以使用 GlobalProtect 通过 IPv6 与 Prisma Access 建立连接。此外，这种支持也有助于通过互联网访问公共 SaaS 应用程序，特别是在这些目的地需要 IPv6 连接的情况下。

与 IPv4 相比，IPv6 拥有更大的地址空间，因此可以容纳几乎无限数量的唯一 IP 地址。通过本机 IPv6 支持，Prisma Access 设计为兼容 IPv6 和双栈连接，从而简化了从 IPv4 到 IPv6 的迁移过程。这种兼容性确保了向后兼容性，并使组织能够过渡到基于云和支持 IPv6 的网络。

Prisma Access 代理可观察性

支持以下版本： Prisma Access 5.2.1 Preferred 和 Innovation

Prisma Access Agent 是下一代移动访问代理，允许您使用 Prisma Access 来保护您的移动员工。Prisma Access Agent 专为当今的混合劳动力而开发，可让用户安全、便捷地访问企业应用程序和互联网，同时还可简化组织的网络、IT 和安全操作。在 Strata Cloud Manager 中，转到 **Insights**（见解） > **Activity Insights**（活动见解） > **Users**（用户）以查看有关 Prisma Access Agent 部署的信息。

远程网络 — 高性能专用应用程序访问支持

支持以下版本： Prisma Access 5.2.1 Preferred 和 Innovation

除了对互联网出口的现有支持外，Prisma Access 远程网络 - 高性能还支持访问专用应用程序。这种支持意味着您可以：

- 从由高性能远程网络连接的分支机构检索专用 app
- 使用服务连接与另一个分支通信（分支到分支流量）
- 使用服务连接与移动用户通信（移动用户到分支机构的流量）

分支站点和服务连接的路由表可见性

支持以下版本： Prisma Access 5.2.1 Preferred 和 Innovation

针对移动用户的静态 IP 地址增强功能

支持以下版本： Prisma Access 5.2.1 Innovation

Prisma Access 为移动用户添加了静态 IP 地址功能，您可以根据 Prisma Access 大区或用户 ID 为用户分配静态 IP 地址。

要增强移动用户的 IP 地址分配，除了大区和用户 ID 之外，现在还可以使用位置组和用户组作为标准。

此外，支持的 IP 地址池配置文件数量也增加到 10,000 个。

RFC6598 Prisma Access (Managed by Strata Cloud Manager) 新部署的移动用户地址池

支持以下版本： Prisma Access (Managed by Strata Cloud Manager) 5.2.1 Preferred 和 Innovation

每个 Prisma Access 部署都需要一个移动用户地址 IP 池。Prisma Access 将此地址池中的 IP 地址分配给每个与 GlobalProtect 连接的设备。为了简化 GlobalProtect 移动用户的载入，Palo Alto Networks 提供了新的 Prisma Access（由 Strata Cloud Manager 管理）部署，其默认 IP 地址池来自 RFC6598。IP 池为 100.92.0.0/16。如果您需要更多地址，或者想要使用自己的地址，您可以修改或删除此地址池，然后添加自己的 IP 地址池。

以色列和沙特阿拉伯 Strata 日志记录服务区域支持

支持以下版本： Prisma Access 5.2.1 Preferred 和 Innovation

Prisma Access 支持 Strata 日志记录服务区域“以色列”和“沙特阿拉伯”。

针对查看和监视 ZTNA 连接器的更新

支持以下版本： Prisma Access 5.2.1 Preferred 和 Innovation

零信任网络接入 (ZTNA) 连接器简化了所有应用程序的专用应用程序访问。您环境中的 ZTNA 连接器虚拟机会自动在您的专用应用程序和 之间形成隧道。从 Prisma Access 5.2.1 开始，我们修改了 ZTNA 连接器页面的外观，以方便您使用，并添加了若干表格，其中包含有关通配符、FQDN 和 IP 子网目标的详细信息。

基于 View Agent 的显式代理

支持以下版本： Prisma Access 5.2.1 Preferred 和 Innovation

等待提供描述。

查看移动用户的静态 IP 地址分配

支持以下版本： Prisma Access 5.2.1 Innovation

要监视静态 IP 池，请转到 **Insights**（见解） > **Activity Insights**（活动见解） > **Users**（用户）以在 **IP Pool Utilization**（**IP** 池利用率） 小部件中监视静态 IP 池。静态 IP 分配功能允许您为 Prisma Access 移动用户分配固定 IP 地址。如果您的网络部署使用 IP 地址作为其网络和应用程序设计的

一部分来限制用户对资源的访问，这将非常有用。使用此功能，您可以根据大区和用户来定义 IP 池。

ZTNA 连接器中安全策略的通配符 FQDN 配置

支持以下版本： Prisma Access 5.2.1 Preferred 和 Innovation

在安全策略规则中使用通配符 FQDN 目前受到协议限制。因此，目前安全策略规则中通配符 FQDN 仅支持 HTTP 和 HTTPS 协议。

通过这一项增强功能：

- 您可以根据通配符应用程序 FQDN 来配置安全策略。
- 相同的安全策略将应用于共享同一通配符 FQDN 的所有已发现应用程序。
- 当发现与通配符 FQDN 匹配的新应用程序时，流量可以通过，不再要求重新提交。

针对应用程序上线的 ZTNA 连接器增强功能

支持以下版本： Prisma Access 5.2.1 Preferred 和 Innovation

如果您的企业用户访问大量专用 app，则当您的基础架构中的应用程序数量超过 15000 时，ZTNA 连接器可能会遇到可扩展性问题。

ZTNA 连接器提供了一项增强功能，可提高可扩展性，用户可以：

- 为每个租户载入 20000 个应用程序，为每个连接器组载入 4000 个应用程序。
- 跨租户载入 400 个连接器，且每个计算区域的带宽为 16 Gbps。

用于应用程序上线的 ZTNA 连接器

支持以下版本： Prisma Access 5.2.1 Preferred 和 Innovation

如果您的企业用户访问大量专用 app，则当您的基础架构中的应用程序数量超过 15000 时，ZTNA 连接器可能会遇到可扩展性问题。

ZTNA 连接器提供了一项增强功能，可提高可扩展性，用户可以：

- 为每个租户载入 20000 个应用程序，为每个连接器组载入 4000 个应用程序。
- 跨租户载入 400 个连接器，且每个计算区域的带宽为 16 Gbps。

使用通配符 FQDN 的 ZTNA 连接器策略配置更新

支持以下版本： Prisma Access 5.2.1 Preferred 和 Innovation

在安全策略规则中使用通配符 FQDN 目前受到协议限制。因此，目前安全策略规则中通配符 FQDN 仅支持 HTTP 和 HTTPS 协议。

通过这一项增强功能：

- 您可以根据通配符应用程序 FQDN 来配置安全策略。
- 相同的安全策略将应用于共享同一通配符 FQDN 的所有已发现应用程序。
- 当发现与通配符 FQDN 匹配的新应用程序时，流量可以通过，不再要求重新提交。

Prisma Access 5.2 功能

本节介绍 Prisma Access 5.2 中正式发布的几个新功能。

25,000 个远程网络和 50,000 个 IKE 网关支持

支持以下版本： Prisma Access 5.2 Preferred 和 Innovation

要实现此功能，请联系您的 Palo Alto Networks 客户团队，他们将提交 SRE 案例来满足请求。

基于代理的代理流量的专用 IP 地址可见性和实施

支持以下版本： Prisma Access 5.2 Preferred 和 Innovation

通过分支机构的 GlobalProtect 代理连接到 Prisma Access 显式代理的用户可以利用端点的专用 IP 地址进行日志记录或应用基于 IP 地址的强制实施。

显式代理用户的 IP 地址优化 - 代理部署

支持以下版本： Prisma Access 5.2 Preferred 和 Innovation

IP 地址优化是一套体系结构增强功能，可减少部署中的 IP 地址总数，简化您的允许列表工作流，同时提高弹性并加快 Prisma Access 租户的载入速度。

IP 地址粘性

如果应用程序和网站要求用户会话在整个用户会话中保持相同的 Prisma Access 出口 IP 地址，则可以通过 IP 地址粘性来保护这些 SaaS 应用程序和网站。

简化 SaaS 应用程序载入

添加 Prisma Access 位置或在现有 Prisma Access 位置遇到扩展事件可能会导致将新的 IP 地址分配给您的显式代理部署。最佳实践是检索新的出口和网关 IP 地址，并将它们添加到 SaaS 应用程序的允许列表中。IP 地址优化减少了在大型部署中必须管理的 IP 地址数量。

端点 **DLP**

支持以下版本： Prisma Access 5.2 Preferred 和 Innovation

需要 Prisma Access Agent。

借助端点 DLP，您的安全管理员可以控制外围设备的使用（管理员让您自主选择是允许还是阻止使用外围设备），或者在外围设备连接到组织中的端点时提醒您的安全管理员。要防止敏感数据泄露到外围设备，请使用高级检测方法以及自定义数据配置文件以定义您自己的流量匹配标准，或者基于 ML 的预定义数据配置文件和正则表达式数据配置文件。

在要保护的端点上安装 之后，它会检测端点和外围设备之间的文件移动，在检测到任何文件移动时就会评估并强制执行端点 DLP 策略规则。必要时， 将流量转发给 进行检测和判定。然后， 将该判定结果传送到 ，后者采取在端点 DLP 策略规则中配置的操作。此外， 还负责在生成 DLP 事件后向最终用户显示通知。

使用 检查端点，如下所示。这假设 已成功安装，并且您配置了端点 DLP 策略规则。

1. 您组织中的用户将外围设备连接到其笔记本电脑。
2. 用户将文件从其端点移动到连接的外围设备。
3. 会将用户尝试将文件从端点移动到外围设备的行为进行登记，并评估您的端点 DLP 策略规则库。
   - 无策略规则匹配：如果未识别出端点 DLP 策略规则匹配项，则允许外围设备连接，并且端点对外围设备具有完全读写访问权限。
   - 外围设备控制策略规则：如果您创建了外围设备控制策略规则来控制访问，则 将执行策略规则中配置的允许或阻止操作。

     例如，如果端点 DLP 策略规则阻止与外围设备的连接，则 会撤销对外围设备的写入权限。在这种情况下，端点无法将文件上传到外围设备。

     相反，如果端点 DLP 策略规则允许连接到外围设备，则 授予端点对外围设备的写入访问权限。在这种情况下，端点可以将文件上传到外围设备。
   - 动态数据策略规则：允许连接外围设备。当 检测到文件从端点移动到外围设备时，文件将被转发给 以供检查和提供判定结果。 还会转发重要的文件元数据，如 `fileSHA`， 使用这些元数据来标识每个转发的文件。

     然后，如果检测到敏感数据，则 将判定结果发送到 ，并且 采取端点 DLP 策略规则操作。如果 检测到它是已经基于 `fileSHA` 检查过的文件，则 向 返回现有判定结果。 不会两次检查同一个文件。
4. 强制执行在”外围设备控制“或”动态数据“策略规则中配置的端点 DLP 策略规则操作。

5. 在适当的时候会生成一个 DLP 事件。如果您已配置最终用户缓存，则端点上会显示一条通知以提醒用户。

明确代理中国支持

支持以下版本： Prisma Access 5.2 Preferred 和 Innovation

Prisma Access 在中国支持显式代理部署。

云服务插件的 **RBAC** 支持

支持以下版本： Prisma Access (Managed by Panorama) 5.2 Preferred 和 Innovation

远程网络 — 高性能

支持以下版本： Prisma Access 5.2 Preferred 和 Innovation

Prisma Access 为高带宽 IPSec 终端提供全面的解决方案，支持大型站点、自动负载平衡、简化载入、区域冗余、单出口 IP 管理并且兼容各种 SD-WAN 解决方案（包括 Prisma SD-WAN）。这些功能共同增强了远程站点连接的可扩展性、性能和可靠性。

在业务规模扩大且办公地点在地理上逐渐分散的情况下，您可以使用 Prisma Access 性能型远程网络（也称为远程网络 - 高性能）快速连接具有高带宽的分支站点。这些网络的优势如下：

- 支持每个服务 IP 地址或服务端点地址高达 3 Gbps 的聚合带宽，减少了用于 IPSec 隧道终止的 IP 地址或 FQDN 的数量。
- 包括区域冗余，可提高可用性和容错能力。
- 使用 NAT 减少公共出口 IP 地址。
- 通过产品内推荐根据地理可用性选择地点，简化载入流程。
- 支持链路质量指标 (LQM)，其中 Prisma SD-WAN 通过主动探测公共和专用传输上的安全结构 VPN 路径以及专用 WAN 底层路径来确定链路质量。这些探测器可以持续测量网络性能指标，例如抖动、延迟和数据包丢失。这些指标，再结合特定于应用程序的性能指标和第 1 层至第 7 层的可访问性，为新的和现有应用程序流的流量转发决策提供依据。

动态特权访问的路由汇总

支持以下版本： Prisma Access (Managed by Strata Cloud Manager) 5.2 Innovation

在启用了动态权限访问的 Prisma Access 租户上，您可以在向内部部署网络通告移动用户 (MU) 路由时汇总路由。如果企业的本地设备的性能有限（例如基本云路由器），路由汇总很有用。路由汇总可减少对这些设备的需求，从而确保设备在与数据中心通信时不会超过其路由容量。

要启用路由汇总，请配置全局摘要池，该池包含可在多个项目中使用的大型 IP 池列表。然后，在 Prisma Access 服务连接中启用路由汇总。如果用户使用 Prisma 访问代理连接到某个项目，该项目的 IP 地址属于已配置的全局摘要池范围，则服务连接将通告全局摘要池，而不是较小的项目级别路由。这有助于减少发送到网络的路由数量。

通过 **CIAM**，针对动态特权访问支持 **SC-NAT**

支持以下版本： Prisma Access 5.2 Innovation

如果您使用动态权限访问 (DPA) 并已创建服务连接来访问数据中心或总部位置的专用应用程序，请使用 SC-NAT 支持。如果基础设施子网的 IP 地址重叠，DPA 环境中的多个项目可能会遇到 IP 地址耗尽的情况。为解决此问题，Prisma Access 可以为 IP 地址实施源 NAT (SNAT)，其作用是：

- 让 Prisma Access 为使用服务连接访问专用应用程序的移动用户映射单个 IP 地址
- 为您提供 SNAT 以简化路由
- 消除 IP 池重叠
- 消除 Prisma Access 和您的数据中心或总部位置之间的 IP 池 IPv4 耗尽问题

简化 **Prisma Access** 专用应用程序连接

支持以下版本： Prisma Access 5.2 Preferred 和 Innovation

访问专用应用程序的一种方法是使用服务连接，也称为服务连接 - 企业访问节点 (SC-CAN)。使用服务连接连接到专用应用程序可能会很难，原因如下：

- SC-CAN 瓶颈导致专用应用程序吞吐量不确定
- 由于中转跳数错误而导致的延迟
- 部署 SC-CAN 操作复杂

为解决这一问题，Prisma Access 增强了路由基础架构路由增强功能，其优势包括：

- 通过改进内部网络消除 SC-CAN 瓶颈
- 在需要时协调锚 SC-CAN，防止中转跳数出错和低效路由

这种设计具有以下优点：

- 更易于部署的路由设置
- 轻松设置零日
- 从给定 SC-CAN 到专用应用所在的数据中心或总部位置的带宽确定为 1 Gbps

针对移动用户，简化了 **Prisma Access** 与 **IP** 优化的 **SaaS**连接，并简化了显式代理部署

支持以下版本： Prisma Access 5.2 Preferred 和 Innovation

Prisma Access 为显式代理和移动用户 - GlobalProtect 提供了 IP 优化功能，以此扩展了该功能。

对于“Mobile Users - GlobalProtect”部署，当大量用户从某个位置访问 GlobalProtect 网关时，Prisma Access 会自动缩放该位置并添加另一个 GlobalProtect 网关。IP 优化使用 NAT 层，因此自动缩放网关会使用与先前分配的 IP 地址相同的 IP 地址，无需向组织的允许列表添加额外的 IP 地址。

Prisma Access 将 NAT 层扩展到显式代理安全处理节点 (SPN) 以及移动用户 SPN，从而减少了显式代理部署对允许列表 IP 地址的需求。如果您在代理模式或隧道和代理模式下设置移动用户和显式代理部署，则显式代理 NAT 层非常有用。

针对 **AWS** 的 **SP** 骨干集成支持

支持以下版本： Prisma Access 5.2 Preferred 和 Innovation

要实现此功能，请联系您的 Palo Alto Networks 客户团队，他们将提交 SRE 案例来满足请求。

从 Prisma Access 5.2 版开始，您（服务提供商）现在可以灵活地为客户的公共云出口流量选择 AWS 以及 GCP。您将在许可证激活中看到其他区域，您将在连接和 IP 地址池中看到 GCP 和 AWS 的选项卡有所不同，并且您还可以单独监视公共云。

TLS 1.3 和 **PubSub** 支持流量复制

支持以下版本： Prisma Access 5.2 Preferred 和 Innovation

对于采用流量复制的大型组织，您在部署和使用流量复制时可能会遇到以下难题：

- 使用数据包捕获 (PCAP) 文件的工具需要频繁查询存储桶，以处理大量的 PCAP 文件。这些工具可能会在存储桶上产生开销，并且使用时可能会受到云提供商的限制。
- 使用 PCAP 文件进行取证分析时，访问 SSL 解密后的流量可提高效率，而且大量流量都经过了 TLS 1.3 加密。

为了解决这些问题，Prisma Access 提供了以下增强功能，使第三方工具能够更高效、更易于扩展：

- 发布/订阅通知：当新的 PCAP 文件上传到存储桶时，Prisma Access 会主动发送发布/订阅通知。使用新的 PCAP 文件的发布/订阅通知后，便无需开发工具用于在存储桶中出现新文件时通知您。
- 支持 **TLS 1.3** 解密：Prisma Access 在解密 PCAP 文件时使用 TLS 1.3，因此可以更深入洞察流量。这项支持适用于远程网络部署，即您已允许对 PCAP 文件使用 SSL/TLS 解密策略规则。

查看和监视 **Colo-Connect**

支持以下版本： Prisma Access 5.2 Preferred 和 Innovation

Colo-Connect 依托于以 Colo 为基础的性能中心概念，具有高带宽专用连接，以及从现有性能中心到 Prisma Access 的第 2/3 层连接。Colo-Connect 利用云原生 GCP 互连技术为您的专用应用程序提供高带宽服务连接。转到 **Monitor**（监视） > **Data Centers**（数据中心） > **Service Connections**（服务连接），查看和监视通过云互连与混合云和本地数据中心之间的专用连接。

在 **Strata Cloud Manager** 和 **Panorama** 中查看 **Prisma Access**、数据平面以及应用程序和威胁内容版本

支持以下版本： Prisma Access (Managed by Strata Cloud Manager) 5.2 Preferred 和 Innovation

为了让您获得有关您的 Prisma Access（由 Strata Cloud Manager 管理）部署的更多信息，“Overview（概述）”页面中的“Software Information（软件信息）”区域（Strata Cloud Manager 中的 **Manage**（管理） > **Configuration**（配置） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Overview**（概述））以及 Panorama 中的 “Prisma Access Version （Prisma Access 版本）”（**Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > **Service Setup**（服务设置））提供了以下信息：

- Prisma Access 版本
- PAN-OS 数据平面版本
- 发布类型（Preferred 或 Innovation）
- 应用程序和威胁内容版本

ZTNA 连接器支持无承诺 **App** 上线

支持以下版本： Prisma Access 5.2 Innovation

通过无承诺载入增强功能，您在载入、修改或删除应用程序时可以获得更好的体验。消除了之前 5 至 10 分钟的延迟，加快了流程。您的应用程序载入时间现在只需不到 1 分钟，您能够快速高效地管理您的应用程序。此外，ZTNA 连接器的增强规模可满足管理超过 10,000 个应用程序的大型客户的需求。您可以载入更多应用程序，从而为您的运营提供更高的灵活性和效率。

Prisma Access 5.2 和 5.2.1 默认行为的更改

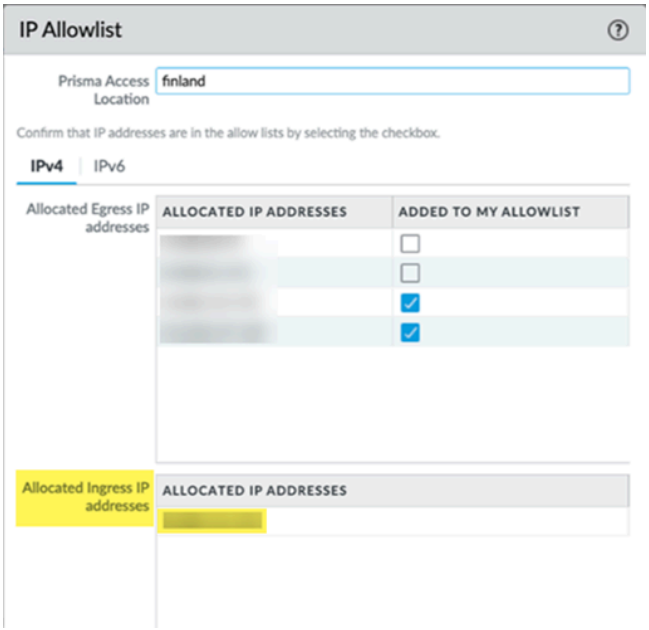
在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证 ❑ Minimum Required Prisma Access Version 5.2 或 5.2.1 Preferred 或 Innovation

以下各节详细介绍了 Prisma Access 版本 5.2 和 Prisma Access 5.2.1 的默认行为的更改。

Prisma Access 5.2.1 默认行为的更改

下表详细说明了 Prisma Access 版本 5.2.1 默认行为的更改。

组件	更改
为新的 **Prisma Access** 部署启用了 **IP** 优化	为了加快 Prisma Access 租户的上线速度并简化 IP 地址允许列表，新部署的 Prisma Access 启用了 IP 优化。 *IP* 优化部署不支持通过 IPv6 访问公共（外部）*App*；支持专用应用程序访问权限。要为您新部署的 *Prisma Access* 启用 *IPv6*，请联系您的 *Palo Alto Networks* 客户团队，他们将提交 *TAC* 案例以满足您的请求。 在设置 Prisma Access 的新部署之前，请确保所有用户运行的 GlobalProtect App 版本是 6.1.4 及更高版本、6.2.3 及更高版本或 6.3.0 及更高版本。 新部署的 *FedRAMP* 未启用 *IP* 优化。
默认移动用户：针对新的 **Prisma Access**（由 **Strata Cloud Manager** 管理）部署更改了 **GlobalProtect IP** 地址池	新的 Prisma Access（由 Strata Cloud Manager 管理）移动用户：GlobalProtect 部署具有新的默认 IP 地址池：100.92.0.0/16。与此不同的是，之前的部署使用默认 IP 地址池 100.127.0.0/16。您可以将此 RFC6598 池用于大多数用例，包括移动用户的专用应用程序访问权限。如果需要更多 IP 地址，可以在 Prisma Access UI 中添加。
对已迁移到 **IP** 优化的部署进行 **IP** 地址整合	如果您现有的 Prisma Access 已将一个或多个区域迁移到 IP 优化，并且正在使用 Prisma 允许访问列表，则某些您列为“允许”的 IP 地址已经从 **Allocated Egress IP addresses**（分配的出口 **IP** 地址）区域移至 Prisma Access UI 中的 **Allocated Ingress IP**

组件	更改
	addresses（分配的入口 **IP** 地址）区域。这一变化是作为 Prisma Access 5.2.1 基础架构升级的一部分进行 IP 地址整合的结果。您的网络仍然可以访问这些 IP 地址，您无需再将其加入允许列表。 

Prisma Access 5.2 默认行为的更改

组件	更改
PAN-OS 10.2.10 数据平面的升级注意事项	如果您选择让 Palo Alto Networks 将您的数据平面升级到 PAN-OS 10.2.10 以支持 Prisma Access 5.2 Preferred 功能，请确保在计划升级之前了解以下 10.2 版本的特定更改和升级注意事项： • 对默认行为的更改 • 升级/降级注意事项 • 针对 PAN-OS 10.2.10 和其他 PAN-OS 10.2 版本解决的问题
PAN-OS 11.2.3 数据平面的升级注意事项	如果您选择让 Palo Alto Networks 将您的数据平面升级到 PAN-OS 11.2.3 以支持 Prisma Access 5.2 创新功能，请确保在计划升级之前了解以下 11.2 版本的特定更改和升级注意事项： • 对默认行为的更改 • 升级/降级注意事项 • 针对 PAN-OS 11.2.2 和其他 PAN-OS 11.2 版本解决的问题

组件	更改
Prisma Access 5.1 中的 **Web** 界面更改	在 Prisma Access 5.1 版本中对 Prisma Access (Managed by Strata Cloud Manager) Web 界面进行了一些更改，支持最多 25,000 个远程网络。有关详细信息，请参阅25,000 个远程网络和 50,000 个 IKE 网关支持。

Prisma Access 已知问题

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证 ❑ Minimum Required Prisma Access Version 5.2 或 5.2.1 Preferred 或 Innovation

Prisma Access 存在以下已知问题。

问题 **ID**	说明
AIOPS-11286	启用 Colo-Connect 后，在多租户环境中子租户中，与交叉连接和连接相关的信息可能不是最新的。
CYR-47139	如果 ZTNA Connector 应用程序块或连接器块配置的 RFC6598 地址与显式代理地址冲突，则将在“ZTNA 连接器 - 显式代理”集成中禁用 ZTNA 连接器。 解决方法：如果您已将 ZTNA 连接器与显式代理集成，请勿将“100.64.0.0/15”、“100.72.0.0/15”和“100.88.0.0/15”子网用于： • ZTNA 连接器应用程序块 • ZTNA 连接器块 • 在 ZTNA 连接器中配置的已与应用程序关联的 IP 子网
CYR-46759	显式代理未采用 DNS 查询的 UDP 设置。
CYR-46627	如果启用了 **Accept Default Route over Service Connection**（接受服务连接的默认路由），则不支持显式代理。
CYR-46445	在 NAT 设备上处理的与端口 6081 相关的暂时性错误导致 ZTNA 连接器关闭。 解决方法：当 ZTNA 连接器流量通过 NAT 设备时，请确保 NAT 会话未映射到端口 6081。

问题 ID	说明
CYR-46349	在中国，将采用显式代理的远程网络与流量转向一起使用时，请勿使用 URL 类别配置流量转向规则。
CYR-46191	如果在启用专用应用程序访问的情况下配置了显式代理，并且将 ZTNA 连接器添加到了配置中，则可能需要从 Panorama 或 Strata Cloud Manager 中再次进行提交。 解决方法：对负责管理 Prisma Access 的 Panorama 或 Strata Cloud Manager 上的显式代理配置进行少量修改，然后再推送您的更改。
CYR-46170	如果您已启用 DDNS，并且稍后将服务子网更改推送给您的移动用户，则还必须重新启动移动用户网关上的 DDNS 插件，以便 DDNS 获取更改。 解决方法：输入以下命令： **`debug software restart process pl-ddns`**
CYR-46145	当现有 Prisma Access 租户的 Prisma Access 自主系统编号或 Prisma Access 基础设施子网更新时，在 ZTNA 连接器和相应应用程已上线的情况下，更新后将中断大约 5 分钟。
CYR-46093	如果您的部署已实现可支持最多 25,000 个远程网络和最多 50,000 个 IKE 网关的功能，则聚合带宽使用情况统计信息不显示使用情况统计信息，而是显示 `No data for the specified time period`（指定时间段无数据）。
CYR-45440	配置管理员角色时，并不总能正确保存访问信息。 解决方法：在“Admin Roles（管理员角色）”区域中单击“Plugins/Cloud Services Plugins（插件/云服务插件）”两次或更多次，以确保正确保存访问信息。再此单击“OK（确定）”和“Open（打开）”以确认更改是否已保存。
CYR-45415	对云服务插件具有只读访问权限或访问权限被禁用的管理员可以在云服务插件之外修改影响云服务行为的配置，例如模板、设备组、移除云服务配置、卸载云服务插件和加载配置文件。

问题 ID	说明
CYR-45517	在 Colo-Connect 选项卡中，只读用户可以删除上线条目。
CYR-45440	配置管理员角色时，并不总能正确保存访问信息。 解决方法：在“Admin Roles（管理员角色）”区域中单击“Plugins/Cloud Services Plugins（插件/云服务插件）”两次或更多次，以确保正确保存访问信息。再次单击 **OK**（确定）和 **Open**（打开）以确认更改是否已保存。
CYR-45415	对云服务插件具有只读访问权限或访问权限被禁用的管理员可以在云服务插件之外修改影响云服务行为的配置，例如模板、设备组、移除云服务配置、卸载云服务插件和加载配置文件。
CYR-44433	在远程网络作业成功后，其状态可能从“Success（成功）”更改为“Pending（待定）”。
CYR-44202	对云服务插件具有只读访问权限的管理用户能够修改 RBI 选项卡。
CYR-43425	如果服务连接使用 RFC 6598 地址，则无法为这些服务连接指定 **Outbound Routes for the Service**（服务的出站路由）。
CYR-43400 **Prisma Access 5.2.0** 中已经解决了此问题。请参阅 **Prisma Access 5.2.0** 已解决的问题。	对于在选中了 **Preserve User ID**（保留用户 **ID**）的 ZTNA 连接器组中登录的连接器，数据中心 App 的内部界面中的 **Actions**（操作）> **Diagnostics**（诊断）> **ping** 无效。
CYR-43262 **Prisma Access 5.2.0** 中已经解决了此问题。请参阅 **Prisma Access 5.2.0** 已解决的问题。	如果有效负载中包含 BGP 配置，用于远程网络上线的远程网络 API 请求在云服务插件中返回提交验证错误。
CYR-43222 **Prisma Access 5.2.0** 中已经解决了此问题。请参阅 **Prisma Access 5.2.0** 已解决的问题。	分配给基于用户 ID 的 ZTNA 连接器组的应用程序目标不支持探测类型 **icmp ping**。 解决方法：对应用程序使用探测类型 **none** 或 **tcp ping**。

问题 ID	说明
CYR-43147	对于自动扩展的 ZTNA 连接器，在缩减期间，如果现有的长期会话是由标记为缩减的 ZTNA 连接器进行处理，则这些长期会话可能会被提前删除。对缩减后的新流量会话不会造成影响。
CYR-43132	在 Panorama 上创建子租户期间，如果将“Mobile Users（移动用户）”配置留空，则无法为远程网络配置单元，反之亦然。
CYR-42919**Prisma Access 5.2.1** 中已经解决了此问题。请参阅**Prisma Access 5.2.1** 已解决的问题。	尝试在 ZTNA 连接器中修改或删除连接器 IP 块时，在提交和推送后未应用更改。 解决方法：再执行两次提交和推送操作以应用更改。
CYR-42312	Colo-Connect 不支持跨 NAT 的 User-ID。
CYR-42259	启用 RFC6598 时，显式代理专用应用程序访问权限不起作用。
CYR-42244	如果您作为“合并和收购的业务连续性”功能的一部分来请求更改 Prisma Access 网关名称，则更新的 FQDN 不会显示在 Strata Cloud Manager 和 Panorama 中。 解决方法：请联系您的 Palo Alto Networks 客户团队，他们将提交 SRE 案例以更新网关的 FQDN。
CYR-42188	使用显式代理专用应用程序访问权限时，TCP 上的 DNS 不起作用；但是基于 UDP 的运行正常。
CYR-42130	Serviceability Commands 区域中不显示 Colo-Connect 路由信息。
CYR-42018	如果您启用了 IP 优化，则 GlobalProtect 不支持 TLS 1.3 支持。 解决方法：最高使用TLS 版本 1.2。
CYR-41990	IPv6 到 IPv6 或 IPv6 到 IPv4 源或目标流量不支持 URL 过滤操作 **Continue**（继续） 和 **Override**（覆盖）。
CYR-41838	使用 Prisma Access API 检索“远程网络 - 高性能部署”的出口 IP 地址时，该地址会显示两次。 解决方法：忽略重复的 IP 地址。

问题 ID	说明
CYR-41813	瑞士、法国、卡塔尔或中国台湾地区不支持 ZTNA 连接器载入。没有解决方法。
CYR-41228	如果启用了 IP 优化，则无法使用 SP 互连功能。
CYR-41067	UI 的“Prisma Access Version（Prisma Access 版本）”区域中显示的 Prisma Access 版本不正确。在 Strata Cloud Manager 中，版本显示在**Manage**（管理）> **Configuration**（配置）> **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**）> **Overview**（概述）> **Prisma Access Version**（**Prisma Access** 版本）中；在 Panorama Managed Prisma Access 中，版本显示在**Panorama** > **Cloud Services**（云服务）> **Configuration**（配置）> **Service Setup**（服务设置）> **Prisma Access Version**（**Prisma Access** 版本）中。
CYR-40503	南非中部和加拿大西部位置不支持 IPv6。
CYR-40404	如果无法从连接器组中的某些 ZTNA 连接器访问应用程序，则可能无法为连接器组找到与通配符匹配的 FQDN 目标。 给定组中的所有连接器都应该能够使用 DNS 来解析应用程序并访问应用程序，以便在组中自动发现应用程序。 解决方法：将应用程序对象关联到 Strata Cloud Manager 需要的连接器组。
CYR-39930	Cortex Data Lake 日志未从启用了 IP 优化功能的租户中导出。
CYR-39795	安装云服务插件后，即使未启用显式代理，显式代理 Kerberos 服务器配置文件 (default_server_profile) 也会被 __cloud_services 用户安装。 解决方法：忽略这些更改。
CYR-39551	如果您将 Prisma Access 动态 DNS 的身份验证类型设置为 TSIG，则应为 TSIG 密钥文件上传 .key 文件。如果密钥文件的内容中包含非 ASCII 字符，则认为密钥文件无效。如果您提供的用于 TSIG 身份验证的 .key 文件包含非 ASCII 字符并且单击 **OK**（确定），则会显

问题 ID	说明
	示错误 `Please upload a file with the .key extension`（请上传扩展名为 `.key` 的文件）。 解决方法：提供有效的 tsig 密钥文件。
CYR-39153	对 ZTNA 连接器组执行升级时，升级操作期间可能会间歇性地出现故障。例如，升级状态显示为 `partial_success` 或 `failed`（虽然某些受影响的连接器之后也成功升级）。 解决方法：稍后重试升级连接器组。ZTNA 连接器会重新检查并为您提供连接器组的正确状态。
CYR-39148	配置 Colo-Connect 时，对 Colo Connect 设备组的提交和推送操作可能会间歇性失败。 解决方法：对 Colo-Connect 设备组重试提交和推送操作。
CYR-39028	如果您要将 ZTNA 连接器从 4.1 升级到更高的 Prisma Access 版本，并且 ZTNA 连接器应用程序池是在 RFC6598 地址空间（100.64.0.0/16 和 100.65.0.0/16）中配置的，则 MU-SPN 上可能会阻止 ZTNA 连接器流量。 解决方法：请联系您的 Prisma Access 团队，以更新所有 Prisma Access 租户的 SaaS 代理版本。
CYR-38619	在瑞士和法国加入的租户无法使用 ZTNA 连接器。
CYR-38120	“移动用户 - 显式代理“设置页面的列表视图中未显示所有可用的位置。 解决方法：使用地图视图选择缺失的位置。
CYR-38076	“Remote Networks Network Details（远程网络网络详细信息）”页面（**Remote Networks Setup**（远程网络设置）> **Remote Networks**（远程网络）> **EBGP Router**（**EBGP** 路由器））中未显示正确的 EBGP 路由器地址，而是显示远程网络的环回 IP 地址。
CYR-37983	如果您为移动用户 - GlobalProtect 用户启用了 IPv6，则检索 HIP 报告会导致崩溃。 解决方法：如果 GlobalProtect 客户端启用了 IPv6，请使用客户端的 IPv6 地址运行 HIP 报告。如果 GlobalProtect

问题 ID	说明
	客户端仅支持 IPv4，请使用客户端的 IPv4 地址运行 HIP 报告。
CYR-37923	创建新的 URL 类别或安全规则或 EDL 后，需要先进行本地 Panorama 提交，然后才能在 RBI 安全规则关联中使用该对象。
CYR-37906	如果在更新现有通配符对象的端口时，在端口之间输入了空格，则显示错误 `500 internal server error`（`500` 内部服务器错误）。 解决方法：不要在端口之间输入空格。例如，请输入 **`1-2,80,100-300`**，而非 **`1-2, 80, 100-300`**。
CYR-37887	如果您在 30 天试用期内使用 ZTNA 连接器，并且尚未购买许可证，则当您单击 **Enable ZTNA Connector**（启用 **ZTNA** 连接器）按钮时，载入可能会失败，并显示一条消息 `Something went wrong`（出错了）。 解决方法：刷新 UI 以完成 ZTNA 连接器功能的载入。
CYR-37826	如果两个或更多个 ZTNA 连接器应用程序具有相同的 FQDN，则 SD-WAN 门户中可能会显示消息 `Application Custom rule conflict`（应用程序自定义规则冲突）。 解决方法：此消息为误报，可以忽略。
CYR-37797	插件升级后，状态页面会要求您提供一次性密码 (OTP)。 解决方法：删除过期的许可证密钥，删除 Panorama 证书，然后检索许可证，并在检索到许可证密钥后验证许可证密钥是否有效；然后生成 OTP 进行验证。
CYR-37755	如果您在 ZTNA 连接器中配置通配符目标并尝试更改某个应用程序的端口，而该应用程序是由于该目标而被发现并已添加到 FQDN 目标，则会收到关于名称太长的错误。 解决方法：虽然应用程序名称最长可以为 32 个字符，但更改端口号会导致名称在 ZTNA 连接器基础设施中过长。如果遇到此错误，请尝试为应用程序指定一个较短的名称。

问题 **ID**	说明
CYR-37706	使用显式代理时，显示过多的威胁日志。 解决方法：忽略多余的威胁日志。这些日志对显式代理功能没有影响。
CYR-37673	单击 **Panorama** > **Cloud Services**（云服务） > **Status**（状态） > **Status**（状态） > **Remote Browser Isolation**（远程浏览器隔离） > **Active Isolated Session**（主动隔离会话）链接未能在 Prisma Access Cloud Management 和 Strata Cloud Manager 中打开 **Monitor**（监视器） > **Subscription Usage**（订阅使用情况）页面。
CYR-37500	如果您为远程网络启用了 IPv6，则不会为边缘站点显示公共 IPv6 地址。
CYR-37466	如果启用 Colo-Connect，请不要在 VLAN 上启用双向转发检测 (BFD)。
CYR-37356	如果您在 App Acceleration 许可证到期后（包括许可证的宽限期）续订许可证，续订不会立即生效。 解决方法：在续订许可证后等待大约一小时，然后再使用 App Acceleration。
CYR-37290	载入 ZTNA 连接器时收到错误 `declaim requested by root`（根用户请求了取消声明）。 解决方法：删除出现错误的连接器并创建一个新连接器。
CYR-37227	创建基于 IP 子网的连接器组有时会失败，并显示消息 `group already exists`（组已存在），即使该组不存在。 解决方法：对基于 IP 子网的连接器组使用其他名称。
CYR-37208	使用 Prisma Access Clean Pipe 时，**Network Details**（网络详细信息）页面（**Panorama** > **Cloud Services**（云服务） > **Status**（状态） > **Status**（状态） > **Network Details**（网络详细信息））不显示 Clean Pipe 条目。
CYR-36749	与 NetFlow 相关的 ZTNA 连接器流日志在 Strata Cloud Manager 日志查看器中可能不显示。

问题 ID	说明
CYR-35506	如果已为租户启用 IPv6，则删除该租户不会释放已分配给它的 IPv6 前缀，并且无法再次使用这些前缀。 解决方法：不要删除启用了 IPv6 的租户。
CYR-34999	对于 Panorama Prisma Access 租户，如果已载入 ZTNA 连接器，则服务连接的配置进度（**Panorama** > **Cloud Services**（云服务） > **Status**（状态） > **Status**（状态） > **Service Connections**（服务连接） > **Provision Progress**（配置进度））显示 ZTNA 连接器和服务连接的配置进度。
CYR-34770	如果在 Prisma Access 中为“移动用户 - GlobalProtect 部署”配置了多个门户，则必须在所有门户的客户端身份验证下面配置身份验证配置文件。如果未配置至少一个身份验证配置文件，则不会生成身份验证 Cookie，并且多门户功能将无法按预期运行。
CYR-34720	使用运行 10.1.x 的 Panorama 通过云服务插件管理 Prisma Access 时，GlobalProtect DDNS 功能不起作用。
CYR-33877	如果在显式代理设置期间选择了 **Skip authentication**（跳过身份验证）以跳过对某个地址对象的身份验证，之后希望通过取消选择 **Skip authentication**（跳过身份验证）来为该地址启用身份验证，则可在您进行更改并且提交和推送更改后，最长可能需要 24 小时更改才能生效。
CYR-33471	如果您启用多租户，创建一个新的子租户并配置“移动用户 - GlobalProtect”、“远程网络”和“Colo-Connect”设备组，然后配置 Colo-Connect 子网和 VLAN，则部分提交会失败，并显示错误 `Unable to retrieve last in-sync configuration for the device`（无法检索设备的上次同步配置）。 解决方法：首次配置 Colo-Connect 时执行“提交并推送”操作，而不是部分提交。
CYR-33454	如果您在多租户部署中配置 Prisma Access，执行“提交并推送”，然后配置 Colo-Connect，则用于提交和推送更改的选项将灰显。 解决方法：单击 **Commit**（提交） > **Commit to Panorama**（提交到 **Panorama**），然后单击

问题 **ID**	说明
	Commit（提交） > **Push to Devices**（推送到设备），然后单击 **Edit Selections**（编辑选择），然后确保 **Push Scope**（推送范围）中选择 **Colo-Connect**；然后重试“提交并推送”操作。
CYR-33199	对于经 Kerberos 身份验证的用户，当前用户计数和 90 天用户计数不正确。
CYR-33145	任何服务类型的 Prisma Access 许可证过期时，任何“全部提交”操作都将失败一般错误消息 `Commit Failed`（提交失败）。 解决方法：在执行提交之前，请确保您的所有 Prisma Access 许可证都未过期。
CYR-32687	当代理或 Kerberos 身份验证与显式代理一起使用时，EDL、类型为 **IP** 通配符掩码和 **FQDN** 的地址对象以及动态地址组对解密策略无效。 解决方法：在解密策略中使用类型为 IP 网络掩码、IP 范围或地址组的地址对象。

CYR-32666	导入先前保存的包含 Colo-Connect 配置的 Panorama 配置时，或从先前保存的配置中恢复时，如果存在以下情况，则会收到错误：
	• 您正在加载的配置已配置了 Colo-Connect 服务连接。
	• 您正在加载的 Prisma Access 配置为空。
	• 您从先前保存的配置中恢复，并且存在以下情况：
	  • 当前配置中存在 Colo-Connect 配置（带有服务连接），而要还原到的配置中不存在 Colo-Connect 配置。
	  • 当前配置中不存在 Colo-Connect 配置，而要还原到的配置中存在 Colo-Connect 配置（具有服务连接）。
	  • 当前配置中Colo-Connect 配置（带有服务连接），要还原到的配置中也存在当前配置。
	解决办法：只有 Colo-Connect 服务连接的对应 VLAN 处于 Active（活动）状态时，才能载入 Colo-Connect 服务连接。在导出或还原 Panorama 映像之前，请删除所有

问题 ID	说明
	Colo-Connect 服务连接；然后，在导入新映像后重新创建 Colo-Connect 服务连接。
CYR-32661	当 GlobalProtect 以“代理”模式或“隧道和代理”模式连接时，用户登录次数在“移动用户 - 显式代理”下面将不会计入当前用户数或过去 90 天内登录的用户数。
CYR-32564	如果使用默认 URL 类别，则 ZTNA 连接器 app 流量将被检测为威胁并针对 Prisma Access Cloud Management 丢弃。 解决方法：根据需要执行以下一个或多个步骤： 1. 创建自定义 URL 类别，然后为 ZTNA 连接器添加载入应用程序的应用程序 FQDN。 2. 如果您使用的是默认配置文件组，请克隆一个新组并附加您在步骤 1 中创建的自定义 URL 类别。如果您使用的是自定义配置文件组，请附加您在步骤 1 中创建的自定义 URL 类别。 3. 确保将克隆的配置文件组或自定义配置文件组（在步骤 2 中）附加到您创建的安全策略，以允许以 ZTNA 连接器应用程序为目标的流量。
CYR-32511	即使禁用了 IPv6，仍能配置 IPv6 DNS 地址。
CYR-32431	配置显式代理时，如果您在“Authentication Settings（身份验证设置）”下添加“Trusted Source Address （受信任的源地址）”值，配置其他设置，随后返回到“Authentication Settings （身份验证设置）”选项卡时，可能无法正确显示受信任的源地址。 解决方法：刷新用于管理 Prisma Access 的 Panorama，然后返回到“Authentication Settings（身份验证设置）”选项卡以查看地址。
CYR-32191	多租户环境中不支持 ZTNA 连接器。
CYR-32004	由于 Prisma Access 当前支持的 IPSec 配置文件数量的局限性，在部署 ZTNA 连接器时，您可以为每个租户最多载入 100 个连接器虚拟机。
CYR-31603	启用了 AWS 自动扩展的连接器组中不支持具有两个接口的 ZTNA 连接器。这是由于 AWS 自动扩展组存在以

问题 ID	说明
	下局限性：将两个接口绑定到同一子网。请参阅本文以了解详情。 解决方法：未启用 AWS 自动扩展的连接器组中支持具有两个接口的 ZTNA 连接器。确保所有具有两个接口的 ZTNA 连接器都包含在未启用 AWS 自动扩展的连接器组中。
CYR-31187	为了在 GlobalProtect 中使用 Prisma Access 显式代理连接以实现始终在线的 Internet 安全功能，除非您同时向“移动用户 - GlobalProtect”和“移动用户 - 显式代理”执行“提交并推送”，否则不会正确填充显式代理默认 PAC 文件 URL。 解决方法：在进行提交和推送时，如果在 GlobalProtect 中配置 Prisma Access 显式代理连接，请务必在推送范围中同时选择“移动用户 - GlobalProtect”和“移动用户 - 显式代理”。

CYR-30414	如果您在只有一个租户的多租户部署中启用了多个门户，然后在该单个租户上禁用了多个门户功能，但还可以在 UI 上看到这两个门户。
	
	解决方法：在管理 Prisma Access 的 Panorama 上打开一个 CLI 会话并输入以下命令，然后在 Panorama 上执行本地提交：
	
	`set plugins cloud_services multi-tenant tenants <tenant_name> mobile-users multi-portal-multi-auth no`
	
	`request plugins cloud_services gpcs multi-tenant tenant-name <tenant_name> multi_portal_on_off`

CYR-30044	在新显式代理部署的阻止设置列表中，预定义 EDL 未填充。 解决方法：载入显式代理部署，执行“提交并推送”操作，然后返回并在阻止设置中更新 EDL。
CYR-29964	尝试重用证书签名请求 (CSR) 来生成证书时导致错误“`Requested entity already exists`”。 解决方法：不要重复使用 CSR。

问题 ID	说明
CYR-29933	每小时多次尝试使用 **`verdicts:all -X "DELETE"`** API 调用时导致错误 `{"code" :8, "message" :"Too many requests"}`。 解决方法：每小时最多使用此 API 调用一次。
CYR-29700	如果在多租户 Prisma Access Panorama Managed 多租户部署中配置多个 GlobalProtect 门户，则根据用户名提交更改将失败，并显示以下错误：`"global-protect-portal-8443 should have the value "GlobalProtect_Portal_8443" but it is [None]"` 解决方法：如果您启用了多个 GlobalProtect 门户并具有 Prisma Access 多租户部署，请执行提交操作“全部提交”，而不是按用户提交。
CYR-29160	如果用于管理 Prisma Access 的 Panorama 配置为 FIPS 模式，并且您选择了 **Generate Certificate for GlobalProtect App Log Collection and Autonomous DEM**（为 **GlobalProtect App** 日志收集和自治 **DEM** 生成证书），则不会下载证书。 解决方法：在 Prisma Access 数据平面升级到 10.2.4 之前，此功能在 FIPS 模式下的 Panorama 设备上不可用。
CYR-26112	如果您没有 Net Interconnect 许可证，则大区中的所有远程网络都是完全网状的，但如果您尚未在大区中载入服务连接，则无法通过其他大区的远程网络来访问远程网络。 解决方法:购买 Net Interconnect 许可证或在大区中载入服务连接，以使远程网络与其他大区通信。

动态权限访问的已知问题

问题 ID	说明
PANG-4881	如果用户用来验证 Prisma Access Agent 的 Web 浏览器保持打开状态，则从 Web 浏览器到 Prisma Access Agent 的流量将通过隧道发送，无论转发配置文件如何配置。

问题 ID	说明
PANG-4870	在安装了 Prisma Access Agent 的 macOS 设备上，如果您移除对 Prisma Access Agent 安全扩展的磁盘完全访问权限（之前授予磁盘完全访问权限之后），Prisma Access Agent 将卡在禁用模式下。 解决办法：授予对安全扩展的访问权限，方法如下：选择 **System Settings**（系统设置）> **Privacy & Security**（隐私与安全）> **Full Disk Access**（磁盘完整访问权限），然后从 app 列表中启用 **securityExtension**。
PANG-4825	配置转发配置文件时，存在如下问题：为源应用程序、目标域和 IP 地址（路由）配置大量转发规则可能会导致 CPU 使用率过高。 解决方法：请勿为源应用程序、目标域和 IP 地址配置超过 100 个转发规则。
NETVIS-1363	在 Strata Cloud Manager 中的“Insights（见解）”中，在 Prisma Access Agent 用户连接后，用户详细信息页面中的 **Project Connectivity History**（项目连接历史记录）视图仅显示项目名称，而不显示其他详细信息。当用户未连接时，“Project Connectivity History（项目连接历史记录）”为空白。
NETVIS-1293	在“Insights（见解）”中，当 **Time Range**（时间范围）设置为 **Past 3 Hours**（过去 **3** 小时）、**Past 1 Hour**（过去 **1** 小时）和 **Past 15 Minutes**（过去 **15** 分钟）时，**Project Connectivity History**（项目连接历史记录）未显示正确数据。
NETVIS-1263	在“Insights（见解）”中，“Projects（项目）”选项卡中列出的已连接用户数可能不准确。在某些情况下，“Projects（项目）”选项卡中的连接用户数与“Users（用户）”选项卡中的用户数不一致。例如，当同一用户连接到不同设备上的两个项目时，“Projects（项目）”选项卡中的连接用户数与“Users（用户）”选项卡中的用户数不一致。
NETVIS-1207	在“Insights（见解）”中，“Projects（项目）”选项卡未显示为项目配置的所有 IP 池。而是仅显示正在使用的 IP 池。

问题 **ID**	说明
EPM-1589	配置转发配置文件时，即使 Strata Cloud Manager 允许您使用通配符配置 IP 地址，也不支持在在目标 IP 地址中使用通配符（例如 **`10.*.*.*`**），因为这会导致转发配置文件中的行为不一致。
EPM-1399	目前还不支持在 Strata Cloud Manager 中的“Dynamic Privilege Access （动态权限访问）页面的 **Projects**（项目）选项卡中更改项目名称。 解决办法：要重命名项目，请删除现有项目并执行 Access Agent 推送配置，然后使用新名称创建项目并执行 Access Agent 推送配置。
EPM-646	在启用了动态权限访问的 Prisma Access 租户上，如果您事先未配置任何项目就尝试推送 Prisma Access Agent 基础架构配置，则配置推送将失败。 解决方法：在执行推送配置之前，至少配置一个项目。
DRS-4691	在 Cloud Identity Engine 或 Strata Cloud Manager 中使用 **Text Search**（文本搜索）选项搜索用户时，请用双引号将用户组名称括起来。例如，在搜索名为 EXAMPLE.User_Group 的用户组时，请输入 "EXAMPLE.User_Group"。
DRS-4406	在 Strata Cloud Manager 中配置项目时，无法通过提供部分用户组名称来搜索用户组。 解决办法：要搜索用户组，请输入完整的用户组名称。
DOCS-5681	Prisma Access 5.2 不支持在启用了动态权限访问的租户上启用 ZTNA 连接器。 在启用了动态权限访问的租户上启用 ZTNA 连接器可能会导致路由问题。服务也可能受到影响，因为 Strata Cloud Manager 不支持在创建 ZTNA 连接器后将其删除。
DOCS-5611	如果在 Cloud Identity Engine 中授权用户组映射以进行动态权限访问，在选择希望 Prisma Access 用于身份验证的 SAML 属性时，请确保选择的 **Username Attribute**（用户名属性）中包含 **/identity/claims/name**。

问题 **ID**	说明
	如果您选择的用户名属性不正确，您的用户将无法对其项目进行身份验证。
DOCS-5463	存在以下问题：如果“Agent Settings（代理设置）”页面中未启用 **Collect HIP Data**（收集 **HIP** 数据）选项，则可能发生随机隧道断开连接的情况。因此，请勿在“Access Agent Settings（访问代理设置）”页的“Host Information Profile (HIP)（主机信息配置文件 (HIP)）”部分中禁用 **Collect HIP Data**（收集 **HIP** 数据）选项。
DOCS-3650	要使 Cloud Identity Engine 身份验证能够在启用了动态权限访问的 Prisma Access 租户上运行，请确保用户组未映射到身份提供商 (IdP) 中的多个 SAML 应用程序。 如果多个 app 映射到一个用户组，由于没有唯一映射，Cloud Identity Engine 无法确定在身份验证期间要连接到哪个 SAML app。
ADI-33262	在启用了动态特权访问的 Prisma Access 租户上，如果不事先在 Strata Cloud Manager 中配置一个项目，则 **Mobile User Container**（移动用户容器）> **Access Agent**（访问代理）配置推送将失败。 解决方法：在执行推送配置之前，至少配置一个项目。
ADI-31750	每个项目支持的 IP 池数量为 50。如果每个项目的 IP 池数量超过 50，则性能将受到影响。 解决方法：为每个项目分配的 IP 池不要超过 50 个。
ADI-31601	在启用了动态权限访问的租户上，Strata Cloud Manager 允许您为每个项目配置超过 100 个 IP 池，即使这会导致推送配置失败并出现一般错误。 解决方法：请勿为每个项目配置超过 100 个的 IP 池。
ADI-31538	存在以下问题：在设置转发配置文件时，转发配置文件类型显示为“ZTNA Agent（ZTNA 代理）”而不是“Prisma Access Agent（Prisma 访问代理）”。此外，如果您选择 **Add Forwarding Profile**（添加转发配置文件），下拉列表会显示“ZTNA Agent（ZTNA 代理）”而不是“Prisma Access Agent（Prisma 访问代理）”。

问题 ID	说明
	解决方法：无。转发配置文件类型以后将更改为“Prisma Access Agent（Prisma 访问代理）”。
ADI-31523	创建代码段时，请勿在描述中包含特殊字符。不支持包含特殊字符（如 **! ~ @ # $ % ^ & * ( ) _ +**）的代码段描述。
ADI-31306	设置转发配置文件时，存在一个问题：默认情况下，“Forwarding Profile（转发配置文件）”页面的 **Traffic Enforcement**（流量强制执行）部分中的所有选项都处于启用状态。默认情况下启用所有这些选项可能会导致意外行为或不良行为。 解决办法：针对动态权限访问禁用这些选项。
ADI-31305	设置转发配置文件时，“Forwarding Profile（转发配置文件）”页面的 **Traffic Enforcement**（流量强制执行）部分中会显示 **Enforce FQDN DNS resolution using tunnel DNS servers**（使用隧道 **DNS** 服务器强制执行 **FQDN DNS** 解析）和 **Resolve all FQDNs using DNS servers that are assigned by the tunnel (Windows agents only)**（使用隧道分配的 **DNS** 服务器解析所有 **FQDN**（仅限 **Windows** 代理）） 不应显示这两个选项，因为这两个选项的预期功能可以使用转发配置文件规则进行配置。
ADI-30902	Strata Cloud Manager 在多个配置中使用来自 Cloud Identity Engine 目录的用户和用户组信息，例如动态权限访问项目配置、Prisma Access Agent 设置、安全策略和分阶段推出配置。进行这些配置后，如果从 Cloud Identity Engine 中删除目录，但不删除引用这些用户和用户组的 Strata Cloud Manager 配置，则可能会遇到意外错误，例如“500 Internal Server Error（500 内部服务器错误）”。 解决方法：从 Cloud Identity Engine 中移除某个目录时，还必须删除引用了该目录中用户和用户组的 Strata Cloud Manager 配置。
ADI-30468	Strata Cloud Manager 中的 **Access Agent**（访问代理）> **Infrastructure Settings**（基础架构设置）页存在如下问题：“Client IP Pool Allocation（客户端 IP 池分

问题 **ID**	说明
	配）”中同时显示 **Prisma Access Managed** 和 **OnPrem DHCP Server**（本地 **DHCP** 服务器）选项。 在启用了动态权限访问的正式发布 Prisma Access 租户上配置用户时，请勿选择 **OnPrem DHCP Server**（本地 **DHCP** 服务器）选项，因为在您保存配置后便无法还原配置。动态权限访问正式发布租户不支持 **OnPrem DHCP Server**（本地 **DHCP** 服务器）选项，在未来版本中将从 Strata Cloud Manager 中移除。如果您选择 **OnPrem DHCP Server**（本地 **DHCP** 服务器）选项，则您的租户将对基本动态权限访问工作流程显示为不可用。
ADI-29665	请勿在项目名称中使用特殊字符，否则当您尝试保存项目配置时，Strata Cloud Manager 将发出错误消息“Malformed Request（请求格式错误）”。
ADI-29434	在 Strata Cloud Manager 的“Agent Settings（代理设置）”页面中，**Session timeout**（会话超时）的建议值为 7 天。
ADI-29272	在创建代码段时，如果禁用 **Session timeout**（为对象名称添加前缀）选项，请确保不要在两个不同的代码段中使用重复的代理设置名称，因为这可能会导致意外行为。
ADI-26493	在 Strata Cloud Manager 中的 **Access Agent**（访问代理）> **Infrastructure Settings**（基础架构设置）中，无法选择“客户端 IP 池分配”部分中的 **OnPrem DHCP Server**（本地 **DHCP** 服务器）选项。这在预期之内，因为动态权限访问不支持 **OnPrem DHCP Server**（本地 **DHCP** 服务器）选项。 此选项将重命名为 **OnPrem DHCP Server (Preview Only)**（本地 **DHCP** 服务器（仅限预览版）），以便启用了动态权限访问的现有 Prisma Access 租户可以正常运行。
ADI-24562	存在如下问题：允许您创建多个具有相同域和用户组的项目（前提是这些项目是通过不同配置片段进行配置的）。请避免使用此配置，因为这可能会导致某些 Strata Cloud Manager 工作流中出现意外行为。

问题 ID	说明
	解决方法：请勿使用相同的域和用户组来配置不同的项目。

Prisma Access 5.2.1 的已知问题

问题 ID	说明
CYR-47139	如果 ZTNA 连接器应用程序块、连接器块或用于连接到应用程序的 IP 子网配置了与显式代理地址冲突的 RFC6598 地址，则 ZTNA 连接器将在”ZTNA 连接器 - 显式代理”集成中被禁用。 解决方法：在配置 ZTNA 连接器以与显式代理一起使用时，请勿将 100.64.0.0/15、100.72.0.0/15 或 100.88.0.0/15 子网用于应用程序或连接器块。
CYR-46759	显式代理未采用 DNS 查询的 UDP 设置。
CYR-46627	如果启用了 **Accept Default Route over Service Connection**（接受服务连接的默认路由），则不支持显式代理。
CYR-46349	在中国，将采用显式代理的远程网络与流量转向一起使用时，请勿使用 URL 类别配置流量转向规则。
CYR-46191	如果在启用专用应用程序访问的情况下配置了显式代理，并且将 ZTNA 连接器添加到了配置中，则可能需要从 Panorama 或 Strata Cloud Manager 中再次进行提交。 解决方法：对负责管理 Prisma Access 的 Panorama 或 Strata Cloud Manager 上的显式代理配置进行少量修改，然后再推送您的更改。

Prisma Access 已解决的问题

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证 ❑ Minimum Required Prisma Access Version 5.2 或 5.2.1 Preferred 或 Innovation

以下主题介绍了 Prisma Access 5.2 和 Prisma Access 5.2.1 中已经解决的问题。

Prisma Access 5.2.1 已解决的问题

问题 **ID**	说明
CYR-45847	修复了以下问题：当某个服务子网发生更改时，该服务子网会在 Prisma Access GlobalProtect 网关上进行更新，但由于 NAT 未正确实施，GlobalProtect 隧道关闭。
CYR-45341	修复了以下问题：向 Colo-Connect 设备组的“推送”和“提交”作业超时，导致 VLAN 未被删除。
CYR-44391	修复了以下问题：在中国进行显式代理部署时，不支持使用 Cloud Identity Engine 或 SAML 进行身份验证。
CYR-43690	修复了以下问题：尝试在 ZTNA 连接器中修改或删除连接器 IP 块时，在提交和推送后未应用更改。
CYR-42919	修复了以下问题：尝试在 ZTNA 连接器中修改或删除连接器 IP 块时，在提交和推送后未应用更改。

Prisma Access 5.2.0-h14 已解决的问题

问题 ID	说明
CYR-46782	修复了以下问题：在 GlobalProtect DDNS 功能中处理 nsupdate 命令时，包含非 ASCII 字符且位于 Panorama 缓存中的域名导致错误。
CYR-46358	修复了以下问题：如果在升级到云服务插件期间，其 Colo-Connect 发生了变化，则非 Prisma Access Edition 租户上发生插件验证失败错误。
CYR-45949	修复了以下问题：如果 UI 无法访问 Prisma Access 基础架构，则不会加载“Mobile Users - Explicit Proxy onboarding location（移动用户 - 显式代理上线位置）”选项卡，并且会不断缓冲。
CYR-45932	修复了以下问题：一次性推送 (OTP) 验证失败并出现以下错误：`[get-panorama-cert.py:288] <class 'AttributeError'> ("'Pan_Plugin_Client' 对象没有属性 'whitelist_keys'`
CYR-44969	修复了以下问题：使用基于角色的管理员创建的用户无法在 UI 中看到云服务配置。
CYR-44766	修复了以下问题：使用常用 API 删除 IKE 和 IPSec 加密配置文件失败，且不会从配置中删除配置文件。

Prisma Access 5.2.0 已解决的问题

问题 ID	说明
CYR-45112	修复了以下问题：在将云服务插件升级到版本 5.1.0 或更高版本时外部网关配置灰显。
CYR-44598	修复了以下问题：Panorama Managed Prisma Access 部署的 Strata 日志记录服务状态显示 `Exception` <*customer-id*> 错误。

问题 ID	说明
CYR-43673	修复了以下问题：API 中的所有无效配置都通过 GET 调用反向中继到系统管理员。
CYR-43400	修复了以下问题：对于在选中了 **Preserve User ID**（保留用户 **ID**）的 ZTNA 连接器组中登录的连接器，数据中心 App 的内部界面中的 **Actions**（操作） > **Diagnostics**（诊断） > **ping** 无效。
CYR-43280	修复了以下问题：非法 base64 数据错误导致 DSP 无法生成差异（即使存在更改）。
CYR-43262	修复了以下问题：当有效负载中包含 BGP 配置时，用于远程网络上线的远程网络 API 请求在插件中引发提交验证错误。
CYR-43222	修复了以下问题：分配给基于用户 ID 的 ZTNA 连接器组的应用程序目标不支持探测类型 **icmp ping**。
CYR-42377	修复了以下问题：为远程故障排除和更新配置动态 DNS 注册支持时，当身份验证类型为 **Kerberos** 时，无法在管理 Prisma Access 的 Panorama 上上传未加密的 Kerberos 密钥文件。 如果使用 5.2.0 版或更高版本的插件运行 Panorama Managed 部署并选择 Kerberos 身份验证类型，请通过 .key 文件上传身份验证密钥，该文件包含从 DNS 服务器检索的 Kerberos 密钥的 base64 编码字符串，例如： `"ABCDEFGHIJKLMNOPQRSTUV5WXYZOUy5DT00ADUFabcD` 如果运行 Panorama Managed 部署时使用的插件版本低于 5.1.0，并且您选择了 Kerberos 身份验证类型，请通过 .key 文件上传身份验证密钥，该文件包含从 DNS 服务器检索的未编码 Kerberos 密钥表文件。
CYR-42191	修复了以下问题：在设置动态 DNS 支持时，有效 Kerberos 文件未正确上传且未保存在系统配置中。

问题 ID	说明
CYR-41740	修复了以下问题：如果在短时间内在同一区域中登录了超过 100 个连接器，则某些某些 ZTNA 连接器的专用应用程序访问可能会失效。
CYR-38418	修复了以下问题：启用 IPv6 后，Prisma Access 数据平面从 10.2.8-h1 升级到 10.2.8-h2 失败。
CYR-38386	修复了以下问题：自动扩展操作导致创建更多移动用户网关后，“提交”和“推送”操作失败。
CYR-37913	修复了以下问题：如果在计算中禁用了流量复制，然后在同一计算中重新启用，则流量复制功能会受到影响，并且您没有看到任何移动用户或远程网络流量被复制，并且不显示任何提交或配置失败。
CYR-37791	修复了以下问题：在用户从一个项目切换到另一个项目并连接到同一 Prisma Access 位置后，Strata Cloud Manager 中的“Monitor（监视）>Users（用户）”页面不能正确反映用户在以下时间范围内切换到的项目名称：3 小时、24 小时、7 天和 30 天。
CYR-36930	修复了以下问题：如果 GlobalProtect 移动用户启用了双堆栈（IPv4 和 IPv6）并连接到启用了 IPv6 的 Prisma Access GlobalProtect 位置，但后来为该位置禁用了 IPv6，则双堆栈用户无法连接到该位置。
CYR-27734	修复了以下问题：针对远程网络设备组，Panorama 中不显示未使用的“规则使用情况统计信息”的策略优化器。

Prisma Access 5.2 和 5.2.1 支持 Panorama

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证 ❑ Minimum Required Prisma Access Version 5.2 或 5.2.1 Preferred 或 Innovation

Prisma Access (Managed by Panorama) 版本 5.2 和 5.2.1 使用云服务插件 **5.2** 云服务插件。使用 5.2 插件的修补程序版本激活 Prisma Access 5.2.1。如果您使用 Panorama 管理 Prisma Access 并需要升级到 5.2 插件，则需要执行以下操作：

1. 查看 Poranama 所需的软件版本以支持 Prisma Access 5.2 Preferred 和 Innovation
2. 确定云服务插件需要遵循的升级路径
3. 升级云服务插件

Panorama Managed Prisma Access 5.2 和 5.2.1 的必需软件版本和建议软件版本

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证 ❑ Minimum Required Prisma Access Version 5.2 或 5.2.1 Preferred 或 Innovation

Prisma Access 5.2.1 Preferred 和 Innovation 的推荐软件版本

有两个 Prisma Access 5.2.1 版本：

- 5.2.1 Preferred 运行 PAN-OS 10.2.10 数据平面。如果您的部署运行的是较低数据平面版本，则需要将数据平面升级到 PAN-OS 10.2.10 才能实现 5.2.1 Preferred 功能。
- 5.2.1 Innovation 运行 PAN-OS 11.2.4 数据平面。需要升级到 PAN-OS 11.2.4 才能实现 5.2 Innovation 功能。

要使用 Prisma Access 5.2.1 Innovation 的新功能特点，Prisma Access 建议将您的 **Prisma Access** 升级到以下版本，然后再安装插件。

Prisma Access 版本	云服务插件版本	**5.2.1** 所需的数据平面版本	推荐的 **GlobalProtect** 版本	推荐的 **Panorama** 版本
5.2.1	5.2.0 修补程序	PAN-OS 10.2.10（5.2.1 Preferred 所必需） PAN-OS 11.2.4（5.2.1 Innovation 所必需）	6.0.7+ 6.1.3+ 6.2.1+	10.2.10+ 11.0.1+ 11.1.0 11.2.4

Prisma Access 5.2 Preferred 和 Innovation 的推荐软件版本

有两个 Prisma Access 5.2 版本：

- 5.2 Preferred 运行 PAN-OS 10.2.10 数据平面。如果您的部署运行的是较低数据平面版本，则可能需要将数据平面升级到 PAN-OS 10.2.10 才能实现 5.2 Preferred 功能。如果您是现有客户，请参阅 Prisma Access 5.2.1 Preferred 和 Innovation 功能的基础设施、插件和数据平面依赖关系 以了解是否需要升级数据平面 Prisma Access 5.2 功能。
- 5.2 Innovation 运行 11.2.3 的 PAN-OS 数据平面。需要升级到 PAN-OS 11.2.3 才能实现 5.2 Innovation 功能。

要使用 Prisma Access 5.2 Innovation 的新功能特点，Prisma Access 建议将您的 **Prisma Access** 升级到以下版本，然后再安装插件。

Prisma Access 版本	云服务插件版本	**5.2** 所需的数据平面版本	推荐的 **GlobalProtect** 版本	推荐的 **Panorama** 版本
5.2	5.2	PAN-OS 10.2.10（5.2 Preferred 所必需） PAN-OS 11.2.3（5.2 Innovation 所必需）	6.0.7+ 6.1.3+ 6.2.1+	10.2.10+ 11.0.1+ 11.1.0 11.2.3

Panorama Managed Prisma Access 的升级注意事项

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证 ❑ Minimum Required Prisma Access Version 5.2 或 5.2.1 Preferred 或 Innovation

要将云服务插件升级到 Prisma Access 5.2 或 5.2.1，请使用下列其中一种升级路径。要在 Panorama 中查找您当前的插件版本，请选择 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > **Service Setup**（服务设置），然后在 **Plugin Alert**（插件警报）区域中检查插件版本。

在升级过程中，请务必遵循每个插件版本要求的最低 Panorama 版本。

已安装的云服务插件版本	目标版本	插件升级路径
5.1	5.2 或 5.2.1	将您的插件从 Prisma Access 5.1 升级到 Prisma Access 5.2，然后再提交和推送您的更改。
5.0	5.2 或 5.2.1	1. 将您的插件从 Prisma Access 5.0 升级到 Prisma Access 5.1，然后再提交和推送您的更改。 2. 将您的插件从 Prisma Access 5.1 升级到 Prisma Access 5.2，然后再提交和推送您的更改。
4.1 和 4.2	5.2 或 5.2.1	1. 将您的插件从 Prisma Access 4.1 升级到 Prisma Access 5.0，然后再提交和推送您的更改。 2. 将您的插件从 Prisma Access 5.0 升级到 Prisma Access 5.1，然后再提交和推送您的更改。 3. 将您的插件从 Prisma Access 5.1 升级到 Prisma Access 5.2，然后再提交和推送您的更改。
4.0	5.2 或 5.2.1	1. 将您的插件升级到 Prisma Access 4.1，然后再提交和推送您的更改。 2. 将您的插件升级到 Prisma Access 5.0，然后再提交和推送您的更改。 3. 将您的插件从 Prisma Access 5.0 升级到 Prisma Access 5.1，然后再提交和推送您的更改。 4. 将您的插件从 Prisma Access 5.1 升级到 Prisma Access 5.2，然后再提交和推送您的更改。

已安装的云服务插件版本	目标版本	插件升级路径
3.0、3.1 和 3.2 Preferred	5.2 或 5.2.1	1. （仅限 3.0 插件）将您的插件升级到 Prisma Access 3.1，然后再提交和推送您的更改。 2. （仅限 3.1 插件）将您的插件升级到 Prisma Access 3.2 或 3.2.1，然后在提交和推送您的更改。 3. 将您的插件升级到 Prisma Access 3.2 或 3.2.1，然后在提交和推送您的更改。 4. 将您的插件升级到 Prisma Access 4.0，然后再提交和推送您的更改。 5. 将您的插件升级到 Prisma Access 4.1，然后再提交和推送您的更改。 6. 将您的插件升级到 Prisma Access 5.0，然后再提交和推送您的更改。 7. 将您的插件从 Prisma Access 5.0 升级到 Prisma Access 5.1，然后再提交和推送您的更改。 8. 将您的插件从 Prisma Access 5.1 升级到 Prisma Access 5.2，然后再提交和推送您的更改。
2.2 Preferred	5.2 或 5.2.1	1. 将您的插件升级到 Prisma Access 3.0，然后再提交和推送您的更改。 2. 将您的插件升级到 Prisma Access 3.1，然后再提交和推送您的更改。 3. 将您的插件升级到 Prisma Access 3.2 或 3.2.1，然后在提交和推送您的更改。 4. 将您的插件升级到 Prisma Access 4.0，然后再提交和推送您的更改。 5. 将您的插件升级到 Prisma Access 4.1，然后再提交和推送您的更改。 6. 将您的插件升级到 Prisma Access 5.0，然后再提交和推送您的更改。 7. 将您的插件从 Prisma Access 5.0 升级到 Prisma Access 5.1，然后再提交和推送您的更改。 8. 将您的插件从 Prisma Access 5.1 升级到 Prisma Access 5.2，然后再提交和推送您的更改。

已安装的云服务插件版本	目标版本	插件升级路径
低于 2.2 Preferred 的版本	5.2 或 5.2.1	**1.** 将您的插件升级到 Prisma Access 2.2，然后再提交和推送您的更改。 如果您的部署是基于低于 2.2 Preferred 的 Prisma Access 版本，则必须先升级到 2.2，然后才能升级到 3.2。不支持从 2.0 或 2.1 版本的 Prisma Access 进行升级。 **2.** 将您的插件升级到 Prisma Access 3.0，然后再提交和推送您的更改。 **3.** 将您的插件升级到 Prisma Access 3.1，然后再提交和推送您的更改。 **4.** 将您的插件升级到 Prisma Access 3.2 或 3.2.1，然后在提交和推送您的更改。 **5.** 将您的插件升级到 Prisma Access 4.0，然后再提交和推送您的更改。 **6.** 将您的插件升级到 Prisma Access 4.1，然后再提交和推送您的更改。 **7.** 将您的插件升级到 Prisma Access 5.0，然后再提交和推送您的更改。 **8.** 将您的插件从 Prisma Access 5.0 升级到 Prisma Access 5.1，然后再提交和推送您的更改。 **9.** 将您的插件从 Prisma Access 5.1 升级到 Prisma Access 5.2，然后再提交和推送您的更改。

升级云服务插件

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama) • Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Access 许可证 ❑ Minimum Required Prisma Access Version 5.2 或 5.2.1 Preferred 或 Innovation

遵循以下过程来升级云服务插件。

Prisma Access 使用 Panorama 中的云服务插件来激活其功能。

有关 Prisma Access 支持的 Panorama 软件版本的列表，请参阅 Palo Alto Networks 兼容性一览表中的所需的最低 Panorama 软件版本。

在升级插件之前，请从 Prisma Access 模板堆栈中移除任何非 Prisma Access 模板，以避免升级后出现提交验证错误，并确保管理 Prisma Access 的 Panorama 正在运行受支持的 PAN-OS 版本。

使用下列其中一项任务来下载并安装云服务插件。

仅限 ***HA*** 部署：如果您的两个 *Panorama* 设备是在高可用性 (HA) 模式下配置的，请首先在主 *HA* 对上安装插件，然后再在辅助 *HA* 对上安装。

STEP 1 | 确定要升级到的插件的升级路径。

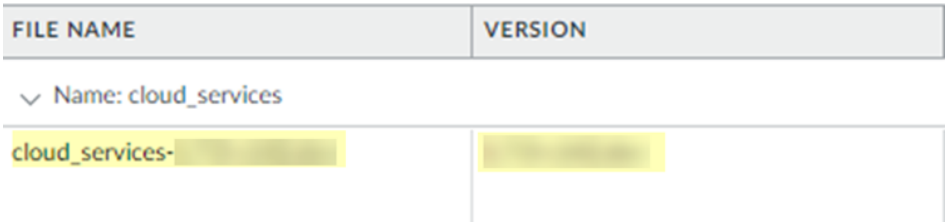
对于某些升级路径，您需要按顺序升级插件。例如，要从 3.0 Preferred 插件升级到 5.2 插件，必须先执行到 3.1、4.0、4.1、5.0 和 5.1 的临时升级，然后再升级到 5.2。

STEP 2 | 下载并安装所需的 Cloud Services 插件版本。

- 要通过从客户支持门户下载来下载并安装云服务插件，请完成以下步骤。
  1. 登录到客户支持门户，然后选择 **Software Updates**（软件更新），
  2. 在“Panorama Integration Plugin In（Panorama 集成插件）”部分中找到云服务插件并下载。

     请勿重命名插件文件，否则您将无法将其安装在 *Panorama* 上。

  3. 登录到您已获得许可且要与 Prisma Access 一起使用的 Panorama 的 Panorama Web 界面，选择 **Panorama** > **Plugins**（插件） > **Upload**（上传），然后选择 **Browse**（浏览）以浏览到您从 CSP 中下载的插件文件。
  4. **Install**（安装）插件。
- 要直接从 Panorama 下载并安装新版本的云服务插件，请完成以下步骤：
  1. 选择 **Panorama** > **Plugins**（插件），然后单击 **Check Now**（立即检查）以显示最新的云服务插件更新。

  2. 下载您要安装的插件版本。
  3. 下载后安装插件。

STEP 3 | （从低于 3.2 的版本升级到 3.2 或更高版本）选择 **Commit**（提交） > **Commit to Panorama**（提交到 **Panorama**）以在管理 Prisma Access 的 Panorama 上本地保存您的更改。

如果要将云服务插件从 3.2 以前的版本升级到 3.2 或更高版本，则只需向 Panorama 执行本地提交。如果是从高于 3.2 的版本升级，则不需要进行本地提交。

获取帮助

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)	❑ Prisma Access 许可证 ❑ Minimum Required Prisma Access Version 5.2 Preferred 和 Innovation

以下主题介绍了在何处查找有关此版本的更多信息以及如何请求支持：

- 相关文档
- 请求支持

相关文档

使用以下文档来设置和实施 Prisma Access 部署：

- 使用 Prisma Access 管理员指南来规划、安装、设置和配置 Prisma Access 以保护您的网络。
- 使用 Prisma Access 集成指南中特定于供应商的任务来使用 Prisma Access 配置移动用户身份验证并保护您的公共云和第三方 SD-WAN 部署。
- 使用 Strata 日志记录服务入门指南了解如何部署 Strata Logging Service （以前称为 Cortex Data Lake）并开始将日志从您的内部防火墙转发到 Cortex Data Lake。

访问 https://docs.paloaltonetworks.com 了解有关我们产品的更多信息。

请求支持

如需联系支持、了解支持计划、管理您的帐户或设备或打开支持案例，请访问 https://support.paloaltonetworks.com。

如需提供有关文档的反馈，请发邮件给我们：documentation@paloaltonetworks.com。

联系信息

公司总部：

Palo Alto Networks

3000 Tannery Way

Santa Clara, CA 95054

https://www.paloaltonetworks.com/company/contact-support

Palo Alto Networks, Inc.

www.paloaltonetworks.com