paloalto TECHDOCS

Prisma Access Browser 激活和初始配置

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

July 15, 2024

Table of Contents

使用 Prisma Access Enterprise 套餐许可证激活新的 Prisma Access Browser

在何处可以使用？	需要提供什么？
• Strata Cloud Manager • Panorama	• 产品的激活链接 • 需要 Strata Logging Service (SLS) 才能激活 • 激活时会包含并启动 Cloud Identity Engine (CIE) • 客户支持门户帐户

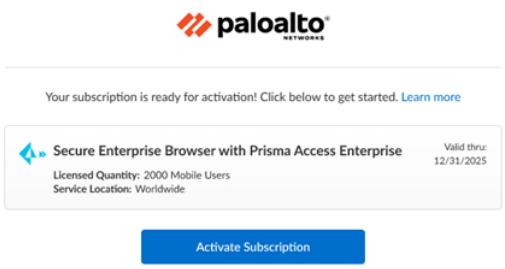
在开始此任务之前，请参阅先决条件。

- 云
- Panorama

云托管 Prisma Access Browser 套餐许可证

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

STEP 1 | 在电子邮件中选择 **Activate Subscription**（激活订阅）。



STEP 2 | 按照说明激活 Prisma Access 许可证，分配 Prisma Access 许可证并规划服务连接。

STEP 3 | 继续分配 Prisma Access Secure Enterprise Browser 许可证和附加组件。根据您的合同，**Products**（产品）或 **Add-ons**（附加组件）在默认情况下会处于启用状态。

STEP 4 | 选择使用 **Prisma Access Enterprise** 保护 **Enterprise** 浏览器的安全。

这类似于分配 PA 移动用户许可证。您可以在多个 Prisma Access 租户之间分配部分和激活 Prisma Access Browser 许可证。例如：

- 您可以购买 5,000 个单位的 Prisma Access Browser Enterprise 移动用户额度。
- 您可以：
  - 向一个 PoC 租户分配 1,000 个单位（这是所需的最低数量）
  - 向生产租户分配 3,000 个单位
  - 保留 1,000 个单位不激活，以备日后使用

STEP 5 | 请转到Prisma Access Browser管理员指南来管理您的 Prisma Access Browser。

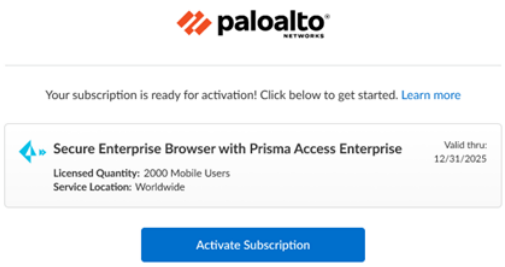
STEP 6 | （可选）分配角色，以便您的管理员可以管理 Prisma Access Browser。

Panorama 托管的 Prisma Access Browser 套装许可证

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

不适用于 *Panorama* 多租户。

STEP 1 | 在电子邮件中选择 **Activate Subscription**（激活订阅）。



STEP 2 | 按照说明激活 Prisma Access（由 Panorama 托管）许可证。

STEP 3 | 继续启用可用的附加组件。根据您的合同，**Products**（产品）或 **Add-ons**（附加组件）在默认情况下会处于启用状态。

STEP 4 | 选择使用 **Prisma Access Enterprise** 保护 **Enterprise** 浏览器的安全。

STEP 5 | 在 Panorama 中，转到 **Panorama** > **Cloud Services Plugin**（云服务插件） > **Prisma Access Browser**选项卡。

这将启动一个新选项卡，其中包含精简版的 Strata Cloud Manager，其中仅包含特定 Prisma Access Browser 视图。

STEP 6 | 请转到Prisma Access Browser管理员指南来管理您的 Prisma Access Browser。

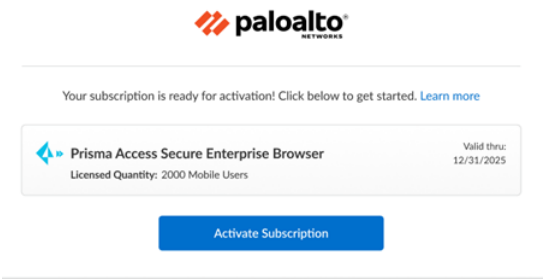
STEP 7 | （可选）分配角色，以便您的管理员可以管理 Prisma Access Browser。

激活独立 Prisma Access Browser 许可证

在何处可以使用？	需要提供什么？
• Strata Cloud Manager	• 产品的激活链接 • 激活时会包含并启动 Cloud Identity Engine (CIE) • 客户支持门户帐户

在开始此任务之前，请参阅先决条件。

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



STEP 1 | 使用您的电子邮件地址登录。

- 如果您拥有 Palo Alto Networks 客户支持帐户，请输入您注册该帐户时使用的电子邮件地址，然后选择 **Next**（下一步）。
- 如果您没有 Palo Alto Networks 客户支持帐户，则点击**Create a New Account**（创建新账户）> **Password**（密码）> **Next**（下一步）。

服务使用此电子邮件地址作为分配给您用于此许可证的租户的用户帐户。此租户以及此电子邮件地址创建的任何其他租户将具有 *Superuser* 角色。

STEP 2 | 如果您只有一个与您的用户名关联的客户支持门户帐户，则会预先填充 **Customer Support Account**（客户支持帐户）。

如果您拥有多个客户支持门户帐户，则可以预计会有其他行为。

STEP 3 | 将产品分配给您选择的 **Recipient**（收件人）。

为方便起见，提供的名称与您的客户支持门户帐户相匹配。您可以使用提供的名称，也可以更改该名称。

STEP 4 | 选择要部署产品的数据提取 **Region**（区域）。

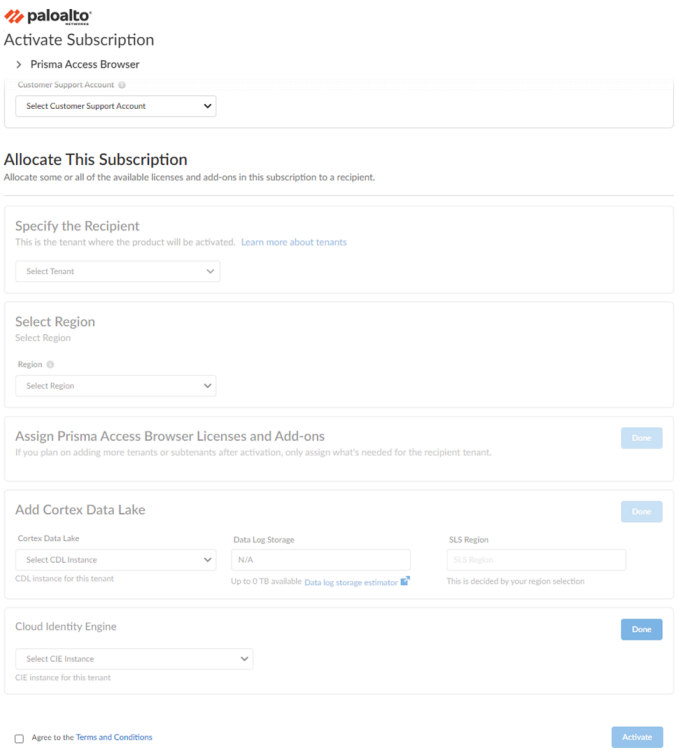
STEP 5 | 分配 Prisma Access Secure Enterprise Browser 许可证和附加组件

1. 选择 **Prisma Access Secure Enterprise Browser**。
2. 这类似于分配 PA 移动用户许可证。您可以在多个 Prisma Access 租户之间分配部分和激活 Prisma Access Browser 许可证。例如：
   - 您可购买 1000 个单位的独立 Prisma Access Browser
   - 您可以：
     - 向一个 PoC 租户分配 200 个单位（这是所需的最低数量）
     - 向生产租户分配 600 个单位
     - 保留 200 个单位不激活，以备日后使用

STEP 6 | 添加 Strata Logging Service（以前称为 Cortex Data Lake），以便用于存储租户数据，如配置、遥测日志、系统日志和统计数据。您可以选择现有实例或创建新实例。

STEP 7 | 选择云身份引擎或创建新的 CIE 实例，以识别和验证整个基础架构中的所有用户。

STEP 8 | 选中 **Agree to the terms and conditions**（同意条款和条件），并单击 **Activate**（激活）。



STEP 9 | 请转到Prisma Access Browser管理员指南来管理您的 Prisma Access Browser。

STEP 10 | （可选）分配角色，以便您的管理员可以管理 Prisma Access Browser。

在 Strata Cloud Manager 上对 Prisma Access Browser 进行初始配置

在何处可以使用？	需要提供什么？
• Strata Cloud Manager	❑ Prisma Access 和 Prisma Access Browser 套餐许可证 ❑ Superuser 或Prisma Access Browser 角色

在开始此任务之前，请参阅先决条件。

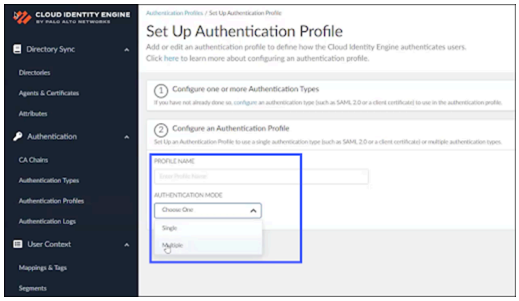
完成初始配置前任务

对 Prisma Access Browser 进行初始配置前，您必须先执行几个任务才能继续。

STEP 1 | 定义 Cloud Identity Engine 实体。这可以通过使用您在激活过程中选择的云身份引擎进行配置。

STEP 2 | 您需要身份验证配置文件和用户组，它们是初始配置流程的一部分。这些是在 Cloud Identity Engine 中配置的。有关更多信息，请参阅身份验证配置文件和用户组。

您只能有一个身份验证配置文件。如果您使用多个身份提供程序 *(IdP)*，则可以为每个配置文件配置多个 *IdP*。当您配置身份验证配置文件时，可以通过选择 ***Multiple***（多重）***Authentication Mode***（身份验证模式）来完成此操作。

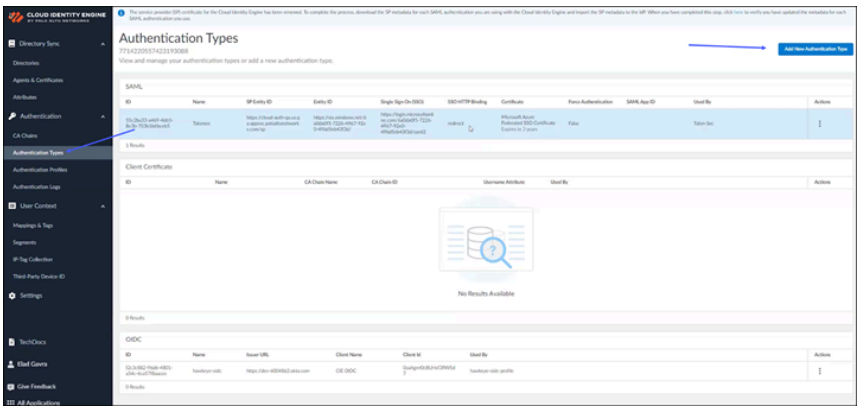


添加 IdP 配置

您可以使用当前的 SAML IdP 提供程序来管理网络中的一组登录凭据。IdP 配置是 Cloud Identity Engine 的一个组件，您可以在该工具中对其进行管理。

STEP 1 | 在 Cloud Identity Engine 中，选择 **Authentication Type**（身份验证类型）。

STEP 2 | 单击 **Add New Authentication Type**（添加新的身份验证类型）。



当您使用 *IdP* 提供程序的信息来填充用户组时，需要确保正确输入有效的电子邮件地址。*UPN* 不够用。

STEP 3 | 在“设置身份验证类型”中，单击 SAML 2.0 设置。

STEP 4 | 要继续配置您的 SAML 身份验证程序，请参阅在 Cloud Identity Engine 中配置 SAML 2.0 身份验证类型。

STEP 5 | （可选）使用 Google Workspace 集成。

对 Prisma Access Browser 进行初始配置

完成初始配置前的步骤后，您可以在 Strata Cloud Manager 上对 Prisma Access Browser 进行初始配置。

您需要在 Strata Cloud Manager 中激活并配置 Prisma Access Browser，然后才能添加用户。一般来说，这是一次性过程，您只需在激活后执行一次，但是您可以在需要修改时随时返回并执行这些任务。

您可以使用向导来完成此过程，并且可以随时修改全局配置。该向导提供了有关完成每个集成步骤的详细说明。

您可以看到的控件取决于您的 Prisma Access Browser 许可证；Strata Cloud Manager 中并非所有的初始配置功能都适用于所有许可证。

从 Strata Cloud Manager 中选择 **Workflows**（工作流） > **Prisma Access** 设置 > **Prisma Access Browser**。

第 1 步 - 用户

定义用户身份验证方法和初始配置用户组。

STEP 1 | 从下拉列表中选择 **CIE profile that will be used for User Authentication**（将用于用户身份验证的 **CIE** 配置文件）。

STEP 2 | 从用户组下拉列表中，选择能够访问 Prisma Access Browser 的 **User groups**（用户组）。

STEP 3 | 下一步：**Prisma Access** 集成。

第 2 步 - Prisma Access 集成

STEP 1 | 启用 Prisma Access 的外部连接。

1. 选择 **Go to Explicit Proxy settings**（转到显式代理设置）。
2. 这会转到 **Workflows**（工作流） > **Prisma Access** 设置 > **Explicit Proxy**（显式代理）。
3. 启用 Prisma Access Browser。
4. **Done**（完成）。

STEP 2 | 在 Prisma Access 安全策略中允许 Prisma Access Browser。

1. 选择 **Manage**（管理）> **Prisma Access** > **Security Policy**（安全策略）。
2. 这会转到 **Manage**（管理） > **Prisma Access** > **Security Policy**（安全策略）
3. 在安全策略中添加允许网络流量的规则。
4. 推送配置以接受规则。
5. **Done**（完成）。

STEP 3 | 创建服务连接。

1. 选择 **Create a service connection**（创建服务连接）。
2. 这将转到 **Workflows**（工作流） > **Prisma Access** 设置 > 服务连接，然后，请 **Add Service Connection**（添加服务连接）。
3. **Done**（完成）。
4. 下一页：路由。

第 3 步 - 路由

通过路由控制可以管理 Prisma Access Browser 处理网络流量的方式。该功能将设置 Prisma Access Browser 的默认配置。如需调整特定规则的控制粒度，请参阅流量流的浏览器自定义控制。

STEP 1 | 选择下列选项之一：

- **Only route private application traffic through Prisma Access**（仅通过 **Prisma Access** 路由私有应用程序流量）。
- 通过 **Prisma Access** 路由所有流量。

STEP 2 | （可选）当浏览器检测到它在内部网络中运行时，确保 Prisma Access Browser 流量会以最佳方式流动。基于此身份可与仅在内部网络中可用的主机建立连接。

- 输入要解析的 FQDN。
- 输入预期的 IP 地址。

STEP 3 | 下一步：强制执行 **SSO** 应用程序。

第 4 步 - 强制执行 SSO 应用程序

重要的是，用户在启用 SSO 的应用程序上进行身份验证的唯一方法是使用 Prisma Access Browser。这将确保外部参与者无法访问您的企业应用程序。要选择您的 IdP：

STEP 1 | 在选择并配置您的身份提供程序时，选择可用的 IdP。选项如下：

- Okta
- Microsoft Azure Active Directory
- PingID
- OneLogin
- VMware 工作区 ONE Access

STEP 2 | 配置本地设置时，请务必记下传出 IP 地址。

STEP 3 | 下一页：下载和分发。

第 5 步- 下载和分发

在将安装文件发送给用户之前，您可以下载 Prisma Access Browser 安装文件并在您自己的设备上进行测试。您对测试满意后，就可以下载相关安装程序，以便使用您的移动设备管理 (MDM) 应用程序进行分发。

您还可以向用户发送下载链接，以便他们自行下载 Prisma Access Browser。这是仅供 macOS 和 Windows 用户使用的单一链接。

STEP 1 | 从可用选项中选择：

- 桌面端：
  - macOS
  - Windows
- 移动端：
  - iOS
  - Android

您还可以向用户发送下载链接，以便他们自行下载 Prisma Access Browser。这是仅供 macOS 和 Windows 用户使用的单一链接。

如果您向用户发送下载链接，请提醒他们只能使用 *IdP* 服务中配置的电子邮件地址登录。

STEP 2 | 下一步：浏览器策略。

第 6 步 - 浏览器策略

您现在可以开始探索和配置 Prisma Access Browser Policy Engine，以便打造安全无虞的用户环境。

STEP 1 | 选择 **Browser Policy**（浏览器策略）。

STEP 2 | 这会转到 **Manage**（管理） > **Configuration**（配置） > **Prisma Access Browser** > **Policy**（策略） > **Rules**（规则）。

STEP 3 | 管理Prisma Access Browser政策规则。

加入新用户

初始配置工作流程是当新的最终用户开始使用浏览器时显示的一系列可配置窗口。

根据 IT 需求和要求，您可以选择最多八个单独的页面，以便允许最终用户使用他们的图片和书签来自定义浏览器，并找到有关浏览器的一些基本信息 - 一种“快速入门”指南。

初始配置向导自定义控件用于配置初始配置工作流程。您可以选择要在网络中显示的窗口。

当您创建或编辑 **Browser Customization**（浏览器自定义）配置文件并选择 **Onboarding Wizard**（初始配置向导）时，您可以在 **Manage**（管理） > **Configuration**（配置） > **Prisma Access Browser** > **Policy**（策略） > **Profiles**（配置文件）中对其进行配置。有关配置详细信息，请参阅初始配置向导的浏览器自定义控件。

分配 Prisma Access Browser 角色

在何处可以使用？	需要提供什么？
• Strata Cloud Manager	❑ 具有 Prisma Access Browser 套餐许可证或 Prisma Access Browser 独立许可证的 Prisma Access ❑ 角色：多租户 Superuser 或有权访问客户支持门户的 Superuser

您可以为 Prisma Access Browser 的不同类型管理员创建和管理基于角色的访问控制。这样，大型组织的主管理员就可以指定其他管理员，而这些管理员将具有与其特定角色相关的权限，包括可见性和访问权限。

激活许可证后，您可以管理 Admin 用户访问权限，并分配以下特定于的 Prisma Access Browser 的角色之一：

Enterprise 角色	权限	支持的应用程序
PA Browser 访问和数据管理员	用于设置和管理访问权限及数据策略，定义自定义或私有应用程序，处理与策略相关的最终用户请求的读写权限，以及对Prisma Access Browser 管理部分中清单方面（用户、设备、扩展程序）和任何可见性方面（指示板、最终用户事件）的只读权限	• Prisma Access Browser
PA Browser 自定义管理员	用于设置和管理浏览器自定义策略的读写权限，以及对 Prisma Access Browser 管理部分中清单方面（用户、设备、应用程序、扩展程序）和任何可见性方面（指示板、最终用户事件）的只读权限。	• Prisma Access Browser
PA Browser 权限申请管理员	用于处理与策略相关的最终用户请求的读写权限，以及对 Prisma Access Browser 管理部分中可见性方面（指示板、最终用户事件）的只读权限。	• Prisma Access Browser
PA Browser 安全管理员	用于设置和管理浏览器安全策略的读写权限，以及对 Prisma Access Browser 管理部分中清单方面（用户、设备、应用程序、扩展程序）和任何	• Prisma Access Browser

Enterprise 角色	权限	支持的应用程序
	可见性方面（指示板、最终用户事件）的只读权限。	
PA Browser 安全和设备状态管理员	用于设置和管理浏览器安全策略、管理设备状态组和设置登录规则的读写权限。它还为清单方面（用户、应用程序、扩展程序）以及 Prisma Access Browser 管理部分中的任何可见性方面（指示板、最终用户事件）提供只读权限。	• Prisma Access Browser
PA Browser 仅限查看分析	对 Prisma Access Browser 管理部分中任何可见性方面的只读访问权限，包括指示板、详细的最终用户事件和清单方面（用户、设备、应用程序和扩展程序）。	• Prisma Access Browser