

The Palo Alto Networks logo, featuring a stylized orange and red icon to the left of the word "paloalto" in a lowercase, sans-serif font.

TECHDOCS

AI Access Security 激活和初始配置

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

Palo Alto Networks, Inc.

www.paloaltonetworks.com

© 2024-2026 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.

Last Revised

April 16, 2026

Table of Contents

AI Access Security 许可证	5
AI Access Security 许可证包含了什么?	6
AI Access Security 设置先决条件	11
激活 AI Access Security 许可证.....	13
将 AI Access Security 评估许可证转换为生产许可证.....	25
续订 AI Access Security 许可证.....	27

AI Access Security 许可证

查看可用的 AI Access Security 许可证，开始在您的网络上[安全地采用和控制](#)对生成式人工智能 (GenAI) 应用程序的访问。

- **AI Access Security** 许可证

AI Access Security 许可证是独立许可证。它包括以下三种类型的许可证：

- **AI Access Security EVAL** — 用于 AI Access Security 的评估许可证。如果您已激活 EVAL 许可证，则必须在评估期结束后[将评估许可证转换为生产许可证](#)，以继续安全地控制对 GenAI 应用程序的访问并安全地采用它们。
- **AI Access Security LAB** — 特定于您实验室环境的 AI Access Security 许可证。此许可证不适用于生产环境。
- **AI Access Security** — 用于 AI Access Security 的生产许可证。

- **CASB-PA**和 **CASB-X**

AI Access Security 默认包含在 CASB-PA 和 CASB-X 许可证中。激活 AI Access Security 不需要额外的操作。激活这两个许可证中的任何一个后，您可以开始使用 AI Access Security 安全地采用 GenAI 应用程序。

- **Prisma Access Browser** [独立许可证](#)

AI Access Security 默认包含在 Prisma Access Browser 独立许可证中。激活 AI Access Security 不需要额外的操作。激活此许可证后，您可以开始使用 AI Access Security 安全地采用 GenAI 应用程序。

AI Access Security 许可证包含了什么？

AI Access Security 包含的内容取决于租户上是否激活了其他许可证。

包含的 AI Access Security 功能取决于当前在 NGFW 或 Prisma Access 租户上运行的 PAN-OS 或数据平面版本。有关包含哪些功能的更多信息，请参阅[设置先决条件](#)。

- 仅限 **AI Access Security**

当只有 AI Access Security 许可证处于活动状态时，这适用于由 Panorama 或 Strata Cloud Manager 管理的 NGFW 或 Prisma Access。

PAN-OS 或数据平面版本	NGFW 和 Prisma Access (由 Panorama 或 Strata Cloud Manager 管理)
<p>11.2.2-h1 及更高版本</p> <p>Prisma Access 5.1 Innovation 及更高版本</p>	<ul style="list-style-type: none"> • 通过动态内容更新和 App-ID 云引擎 (ACE) 提供对超过 2,250 个 GenAI 应用程序的可见性。 • 定义策略规则以控制对 GenAI 应用程序和非 GenAI 应用程序的访问。 • 仅对受支持的 GenAI 应用程序进行Enterprise DLP检查和判定。 包含敏感数据的流量匹配结果不会转发到 Enterprise DLP 进行非 GenAI 应用程序的检查和判定。 • 访问 Strata Cloud Manager Command Center 以获取 GenAI 可见性。 • 访问 AI Access Security Activity Insights 仪表盘，以查看详细的 GenAI 应用程序使用数据、用户以及在您的网络上发生的常见 GenAI 用例。 • 在 Strata Cloud Manager 上标记 GenAI 应用程序，以反映该应用程序是否在您的组织内获得批准，并用于基于标签的策略执行。 AI Access Security不会将 GenAI 应用程序标签同步到 Panorama。 • 仅为发现的 GenAI 应用程序生成报告。 • 在应用程序字典中查看 GenAI 应用程序，以了解有关特定 GenAI 应用程序、供应商、合规性和风险特征的更多信息，这些特征是这些 SaaS 应用程序的基础。 • 查看作为第三方连接应用程序/插件安装的 GenAI 应用程序，位于 7 个 SaaS 市场应用程序中。 • 对驻留在 ChatGPT 企业应用程序中的静态数据的可见性和控制。

- **AI Access Security 和 Enterprise DLP 许可证**

当 AI Access Security 和 Enterprise DLP 许可证均处于活动状态时，这适用于由 Panorama 或 Strata Cloud Manager 管理的 NGFW 或 Prisma Access。

PAN-OS 或数据平面版本	NGFW 和 Prisma Access (由 Panorama 或 Strata Cloud Manager 管理)
11.2.2-h1 及更高版本 Prisma Access 5.1 Innovation 及更高版本	<ul style="list-style-type: none"> • 通过动态内容更新和 App-ID 云引擎 (ACE) 提供对超过 2,250 个 GenAI 应用程序的可见性。 • 定义策略规则以控制对 GenAI 应用程序和非 GenAI 应用程序的访问。 • 对受支持的 GenAI 和非 GenAI 应用程序进行Enterprise DLP检查和判定。 • 访问 Strata Cloud Manager Command Center 以获取 GenAI 可见性。 • 访问 AI Access Security Activity Insights 仪表盘，以查看详细的 GenAI 应用程序使用数据、用户以及在您的网络上发生的常见 GenAI 用例。 • 在 Strata Cloud Manager 上标记 GenAI 应用程序，以反映该应用程序是否在您的组织内获得批准，并用于基于标签的策略执行。 AI Access Security不会将 GenAI 应用程序标签同步到 Panorama。 • 仅为发现的 GenAI 应用程序生成报告。 • 在应用程序字典中查看 GenAI 应用程序，以了解有关特定 GenAI 应用程序、供应商、合规性和风险特征的更多信息，这些特征是这些 SaaS 应用程序的基础。 • 查看作为第三方连接应用程序/插件安装的 GenAI 应用程序，位于 7 个 SaaS 市场应用程序中。 • 对驻留在 ChatGPT 企业应用程序中的静态数据的可见性和控制。

- **CASB-PA 和 CASB-X 许可证**

当 CASB-PA 或 CASB-X 许可证处于活动状态时，这适用于由 Strata Cloud Manager 管理的 NGFW 或 Prisma Access。

PAN-OS 或数据平面版本	CASB-PA和 CASB-X
10.2 11.1 Prisma Access 5.0 Preferred 和 Innovation 及更高版本	<ul style="list-style-type: none"> • 通过动态内容更新和 App-ID 云引擎 (ACE) 提供对超过 2,250 个 GenAI 应用程序的可见性。 • 定义策略规则以控制对 GenAI 应用程序和非 GenAI 应用程序的访问。 • 对受支持的 GenAI 和非 GenAI 应用程序进行Enterprise DLP检查和判定。 • 访问 Strata Cloud Manager Command Center 以获取 GenAI 可见性。

PAN-OS 或数据平面版本	CASB-PA和 CASB-X
<p>Prisma Access 5.1 Preferred 及更高版本</p>	<ul style="list-style-type: none"> • 访问 AI Access Security Activity Insights 仪表盘，以查看详细的 GenAI 应用程序使用数据、用户以及在您的网络上发生的常见 GenAI 用例。 • 查看以下内容，了解所有 SaaS 内联应用程序（包括 GenAI 应用程序）： <ul style="list-style-type: none"> • 指示板 • 用户 • 应用程序字典 • 应用程序 • 报告 • 策略建议 • 查看所有第三方插件 (SSPM)，包括 GenAI 插件。 • 查看所有受制裁的 SaaS 应用程序（静态数据）的资产详情，包括 GenAI 应用程序。
<p>11.2.2-h1 及更高版本</p> <p>Prisma Access 5.1 Innovation 及更高版本</p>	<ul style="list-style-type: none"> • 通过动态内容更新和 App-ID 云引擎 (ACE) 提供对超过 2,250 个 GenAI 应用程序的可见性。 • 定义策略规则以控制对 GenAI 应用程序和非 GenAI 应用程序的访问。 • 对受支持的 GenAI 和非 GenAI 应用程序进行Enterprise DLP检查和判定。 • 访问 Strata Cloud Manager Command Center 以获取 GenAI 可见性。 • 访问 AI Access Security Activity Insights 仪表盘，以查看详细的 GenAI 应用程序使用数据、用户以及在您的网络上发生的常见 GenAI 用例。 • 在 Strata Cloud Manager 上标记 GenAI 应用程序，以反映该应用程序是否在您的组织内获得批准，并用于基于标签的策略执行。 <p>AI Access Security不会将 GenAI 应用程序标签同步到 Panorama。</p> <ul style="list-style-type: none"> • 查看以下内容，了解所有 SaaS 内联应用程序（包括 GenAI 应用程序）： <ul style="list-style-type: none"> • 指示板 • 用户 • 应用程序字典 • 应用程序 • 报告 • 策略建议 • 查看所有第三方插件 (SSPM)，包括 GenAI 插件。

PAN-OS 或数据平面
版本

CASB-PA和 CASB-X

- 查看所有受制裁的 SaaS 应用程序（静态数据）的[资产详情](#)，包括 GenAI 应用程序。

AI Access Security 设置先决条件

查看使用 AI Access Security 的先决条件。先决条件描述了使用 AI Access Security 所需的最低 PAN-OS 和 Prisma Access 数据平面版本以及任何其他服务。

[查看](#)不同的 AI Access Security 许可证和 PAN-OS 版本组合，了解有关 AI Access Security 支持哪些功能的更多信息。

- **NGFW 和 Prisma Access**（由 **Panorama** 管理）

从 Panorama 管理 AI Access Security 配置时，请参阅 **AI Access Security** 许可证先决条件，并且只有 AI Access Security 许可证已激活。

从 Panorama 管理 AI Access Security 配置时，请参阅 **CASB-PA** 和 **CASB-X** 许可证先决条件，并拥有激活的 CASB-PA 或 CASB-X 许可证。

先决条件	AI Access Security 许可证	CASB-PA 和 CASB-X 许可证
PAN-OS 或数据平面	PAN-OS 11.2.2-h1	<ul style="list-style-type: none"> • PAN-OS 10.2.3 和 Prisma Access 5.0 Preferred 和 Innovation • PAN-OS 11.1.0 和 Prisma Access 5.1 Preferred • PAN-OS 11.2.2-h1 和 Prisma Access 5.1 Innovation <p>查看 Prisma Access 发行说明，了解所需的最低 Prisma Access 版本详细信息。</p>
数据筛选	Enterprise DLP 插件 5.0.4 或更高版本	<p>查看 兼容性列表，了解您的 PAN-OS 版本支持的 Enterprise DLP 插件版本。</p> <p>当您激活 AI Access Security、CASB-PA 和 CASB-X 许可证时 AI Access Security 包含 Enterprise DLP。</p>
管理	Strata Cloud Manager Essentials 或 Strata Cloud Manager Pro 了解更多 关于每个许可证包括的内容。	不适用
云服务插件	云服务插件 5.1	

先决条件	AI Access Security 许可证	CASB-PA 和 CASB-X 许可证
记录	Strata Logging Service	

• **NGFW 和 Prisma Access**（由 **Strata Cloud Manager** 管理）

从 Strata Cloud Manager 管理 AI Access Security 配置时，请参阅 **AI Access Security** 许可证先决条件，并且只有 AI Access Security 许可证已激活。

从 Strata Cloud Manager 管理 AI Access Security 配置时，请参阅 **CASB-PA** 和 **CASB-X** 许可证先决条件，并拥有激活的 CASB-PA 或 CASB-X 许可证。

先决条件	AI Access Security 许可证	CASB-PA 和 CASB-X 许可证
PAN-OS 或数据平面	PAN-OS 11.2.2-h1	<ul style="list-style-type: none"> • PAN-OS 10.2.3 和 Prisma Access 5.0 Preferred 和 Innovation • PAN-OS 11.1.0 和 Prisma Access 5.1 Preferred • PAN-OS 11.2.2-h1 和 Prisma Access 5.1 Innovation <p>查看 Prisma Access 发行说明，了解所需的最低 Prisma Access 版本详细信息。</p>
数据筛选	当您激活 AI Access Security、CASB-PA 和 CASB-X 许可证时 AI Access Security 包含 Enterprise DLP。	
管理	Strata Cloud Manager Essentials 或 Strata Cloud Manager Pro 了解更多 关于每个许可证包括的内容。	不适用
记录	Strata Logging Service	

激活 AI Access Security 许可证

激活您的 AI Access Security 许可证，使您的组织能够安全地由员工采用生成式人工智能 (GenAI) 应用程序。AI Access Security 激活是通过购买 AI Access Security 许可证后，由 Palo Alto Networks 提供的 Magic 链接执行的。这些步骤假设您已经拥有激活所需的所有许可证授权码和 Magic 链接。

购买 AI Access Security 许可证后，您必须使用 Palo Alto Networks 发送给您的 Magic 链接激活许可证。激活 CASB-PA 或 CASB-X 许可证时已包含 AI Access Security。在您激活 CASB-PA 或 CASB-X 许可证后，无需进一步操作即可激活 AI Access Security。

- [新的部署](#)
- [现有部署](#)

激活 AI Access Security 许可证（新部署）

STEP 1 | 安装并执行 NGFW 的初始配置。

这包括激活所有必需的支持许可证。

STEP 2 | 为您的 NGFW 或 Prisma Access 租户设置管理。

- **NGFW (Managed by Panorama)**

1. 设置 Panorama。

- **M-Series** 设备 — 在 **Management Only**（仅管理）或 **Panorama** 模式下设置 M-Series 设备。
- **Panorama** 虚拟设备 — 在 **Management Only**（仅管理）或 **Panorama** 模式下安装首选管理程序上的 Panorama 虚拟设备

2. 部署 Strata Logging Service。

3. 注册 Panorama。

4. 激活 Panorama 支持许可证。

5. 激活 Panorama 设备管理许可证（**M-Series** 设备或 **Panorama** 虚拟设备）。

6. 将托管防火墙添加到 Panorama 管理中。

7. 将 Panorama 升级到 AI Access Security 支持的最低 **PAN-OS** 版本。

8. 将您的 NGFW 升级到 AI Access Security 支持的最低 **PAN-OS** 版本。

- **NGFW (Managed by Strata Cloud Manager)**

1. 部署 Strata Logging Service。

Strata Cloud Manager 需要 Strata Logging Service 才能进行日志记录。

2. 激活 Strata Cloud Manager Essentials 或 Strata Cloud Manager Pro 许可证。

3. 将您的 NGFW 接入 Strata Cloud Manager。

4. 安装最新动态内容更新，将 NGFW 升级到 AI Access Security 支持的最低 **PAN-OS** 版本。

- **Prisma Access (Managed by Panorama)**

1. 设置 Panorama。

- **M-Series** 设备 — 在 **Management Only**（仅管理）或 **Panorama** 模式下设置 M-Series 设备。
- **Panorama** 虚拟设备 — 在 **Management Only**（仅管理）或 **Panorama** 模式下安装首选管理程序上的 Panorama 虚拟设备

2. 部署 Strata Logging Service。

3. 注册 Panorama。

4. 激活 Panorama 支持许可证。

5. 激活 Panorama 设备管理许可证（**M-Series** 设备或 **Panorama** 虚拟设备）。

6. 将 Panorama 升级到 AI Access Security 支持的最低 **PAN-OS** 版本。

7. 安装 Panorama 上的云服务插件。

8. 设置 Panorama Managed Prisma Access。

- **Prisma Access (Managed by Strata Cloud Manager)**

1. 部署 Strata Logging Service。

Strata Cloud Manager 需要 Strata Logging Service 才能进行日志记录。

2. 激活 Strata Cloud Manager 上的 Prisma Access 许可证。

3. 设置 Prisma Access。

STEP 3 | 设置 Enterprise Data Loss Prevention (E-DLP)。

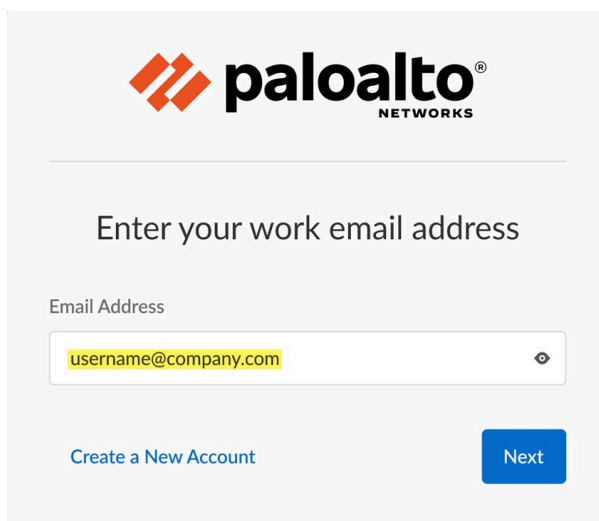
- **NGFW (Managed by Panorama)**
 1. 安装 Panorama 上的 Enterprise DLP 插件。
 2. 启用 NGFW 的 Enterprise DLP。
 3. 根据需要编辑 Enterprise DLP 云内容、数据过滤和片段设置。
- **NGFW (Managed by Strata Cloud Manager)**
 1. 启用 NGFW 的 Enterprise DLP。
 2. 根据需要编辑 Enterprise DLP 数据过滤和片段设置。
- **Prisma Access (Managed by Panorama)**
 1. 安装 Panorama 上的 Enterprise DLP 插件。
 2. 启用 Prisma Access 的 Enterprise DLP。
 3. 根据需要编辑 Enterprise DLP 云内容、数据过滤和片段设置。
- **Prisma Access (Managed by Strata Cloud Manager)**
 1. 启用 NGFW 的 Enterprise DLP。
 2. 根据需要编辑 Enterprise DLP 数据过滤和片段设置。

STEP 4 | 点击购买 AI Access Security 订阅时 Palo Alto Networks 为您提供的 Magic 链接。

STEP 5 | 单击 **Activate Subscription**（激活订阅）开始激活 AI Access Security。

STEP 6 | 输入您的 Palo Alto Networks 客户支持门户 (CSP) 电子邮件地址。此电子邮件地址必须与接收用于激活 AI Access Security 的 Magic 链接的电子邮件地址一致。

如果收到 AI Access Security 激活链接的电子邮件地址还没有有效的 CSP 帐户，请 **Create a New Account**（创建新帐户）。新创建的帐户将自动与您为其激活 AI Access Security 并分配 **多租户超级用户角色** 的同一租户关联。



STEP 7 | (仅限多租户) 在 **Customer Support Account** (客户支持帐户) 部分, 选择与您激活AI Access Security许可证的租户关联的Palo Alto Networks客户支持帐户。

如果您有单租户客户支持门户帐户, 请跳过此步骤。默认情况下, 您的客户支持帐户处于选中状态。

STEP 8 | (仅限多租户) 在 **Allocate This Subscription** (分配此订阅) 部分, 选择要为其激活AI Access Security的租户服务组(TSG)。您可以选择父租户或子租户。

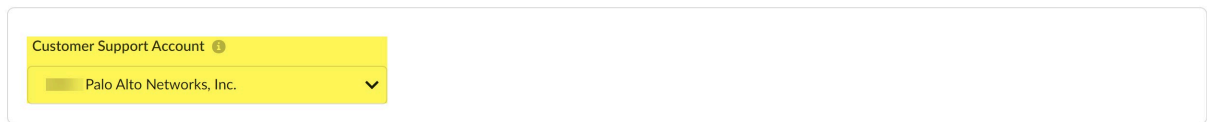
AI Access Security 仅对选定的租户激活。如果选择父租户, 则不会为任何子租户激活 AI Access Security。

如果您只有一个租户客户支持门户帐户, 请跳过此步骤。默认情况下已选中。

STEP 9 | 查看租户 **Region** (区域)。此区域基于部署的NGFW或Prisma Access租户区域预先填充, 无法更改。

Select Customer Support Account


This account is used for the registration and support of the products and add-ons that are bundled with this subscription. [Learn more](#)



A screenshot of a dropdown menu titled "Customer Support Account". The selected option is "Palo Alto Networks, Inc." with a downward arrow icon.

Allocate This Subscription

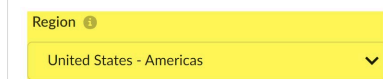
Allocate the available licenses and add-ons in this subscription to a recipient.



A screenshot of a form field labeled "Recipient:" with the value "Palo Alto Networks, Inc." and an "Edit" link to the right.

Select Region

Select Region



A screenshot of a dropdown menu titled "Region". The selected option is "United States - Americas" with a downward arrow icon.

STEP 10 | 在**Assign Licenses** (分配许可证) 部分, 单击 **Done** (完成) 以分配所有AI Access Security许可证。验证您的 **AI Access Security License** (AI Access Security 许可证) 是否已**Fully Assigned** (完全分配)

STEP 11 | 如果您的租户上Enterprise Data Loss Prevention (E-DLP)处于活动状态，请验证是否选择了 **Data Loss Prevention**（数据丢失防护）实例。

如果租户上已经处于活动状态，则默认选择您的 Enterprise DLP 实例。

如果没有已激活的Enterprise DLP，请跳过此步骤。启用AI Access Security不需要Enterprise DLP。如果 Enterprise DLP 实例尚未激活，则会在许可证激活过程中创建一个实例。查看如果 [不续订AI Access Security许可证](#)，Enterprise DLP会发生什么。

Data Security Access Licenses : **Fully Assigned** [Edit](#)

LICENSES

AI Access Security for PA and Next-Generation Firewall: 30 Users

Data Loss Prevention (Optional)

Select an existing Data Loss Prevention instance that you want to use in this tenant. Data Loss Prevention is set of tools and processes that allow you to protect sensitive information against unauthorized access, misuse, extraction, or sharing.

Palo Alto Networks, Inc. ▼

STEP 12 | 同意条款和条件。

STEP 13 | 激活。

您将被重定向到 [Tenant Management](#)（租户管理）页面，此时 **AI Access Security Activation Status**（激活状态）开始 **Initializing**（初始化）。

AI Access Security许可证显示为 **Data Security**（数据安全），并且具有以 **AIX** 开头的序列号。**Activation Status**（激活状态）显示为 **Complete**（完成）后继续下一步。

Products	Deployment Profiles	Tenant Acquisition History		
Products	Activation Status	License Capacity	Serial Number	Expiration Date
IoT Security	Complete	N/A	N/A	
Strata Logging Service	Complete	Data Space: 1 TB		02/24/2026
AI Ops for NGFW	Complete	N/A	N/A	
Enterprise DLP	Complete	N/A	N/A	
Demisto	Complete	N/A	N/A	
Cortex XSOAR	Complete	N/A	N/A	
SaaS Security	Complete	N/A	N/A	
Armis	Complete	N/A	N/A	
Cloud Identity Engine	Complete	N/A	N/A	
AI Ops for NGFW Free	Complete	N/A	N/A	
Data Security	Complete	AI Access Security for PA and Next-Gen	AIX	08/19/2025

STEP 14 | (仅限 NGFW) 将 AI Access Security 许可证与您的 NGFW 关联。

需要关联 AI Access Security 许可证才能为您的 NGFW 激活许可证。

1. 在 Strata Cloud Manager 菜单中，选择 **Settings** (设置) > **Device Associations** (设备关联)。

Strata Cloud Manager 菜单位于 Strata Cloud Manager 的左下角。

2. 在 Strata Cloud Manager 菜单中，选择 **System Settings** (系统设置) > **Device Associations** (设备关联)。

Strata Cloud Manager 菜单位于 Strata Cloud Manager 的左下角。

3. **Associate Apps** (关联应用程序)。
4. 在许可产品中，选择 **Data Security** (数据安全)。
5. 选择要为其激活 AI Access Security 的 NGFW。
6. **Save** (保存)。

STEP 15 | 验证您是否成功激活 AI Access Security。

1. 登录到 Palo Alto Networks [客户支持门户 \(CSP\)](#)。
2. 选择 **Products** (产品) > **Assets** (资产)。
3. 根据您激活 AI Access Security 的实施点选择 **NGFW** 或 **Prisma Access** 租户。
4. 使用过滤器定位您的 NGFW 或 Prisma Access 租户。
5. 展开活动许可证列表或单击 **Licenses & Subscriptions** (许可证和订阅)。
6. 验证 AI Access Security 许可证是否已激活。

DNS Security				10/10/2025
SD WAN				10/10/2025
IoT Security				10/25/2026
Advanced URL Filtering				10/10/2025
SaaS Security Inline Eval				10/15/2024
DLP				10/15/2025
PAN-DB URL Filtering				10/10/2025
Advanced Threat Prevention				10/10/2025
Decryption Port Mirror				Perpetual
Cortex Data Lake				02/24/2026
Advanced WildFire License				10/10/2025
WildFire License				10/10/2025
AI Ops for NGFW				09/23/2026
AI Access Security for Next-Generation Firewall				08/19/2025

STEP 16 | 开始使用 AI Access Security。

激活 AI Access Security 许可证（现有部署）

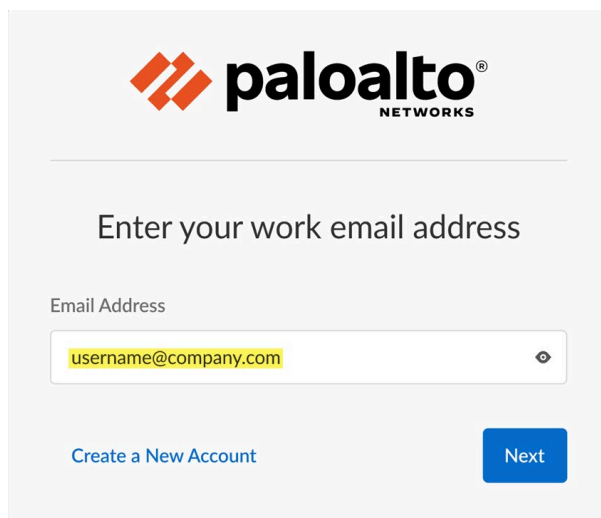
此过程假设您只需要激活 AI Access Security 许可证，并且所有先决条件许可证都已激活，并且已根据需要成功设置 NGFW、Prisma Access、Panorama™ management server 和 Strata Cloud Manager。

STEP 1 | 点击购买 AI Access Security 订阅时 Palo Alto Networks 为您提供的 Magic 链接。

STEP 2 | 单击 **Activate Subscription**（激活订阅）开始激活 AI Access Security。

STEP 3 | 输入您的 Palo Alto Networks 客户支持门户 (CSP) 电子邮件地址。此电子邮件地址必须与接收用于激活 AI Access Security 的 Magic 链接的电子邮件地址一致。

如果收到 AI Access Security 激活链接的电子邮件地址还没有有效的 CSP 帐户，请 **Create a New Account**（创建新帐户）。新创建的帐户将自动与您为其激活 AI Access Security 并分配 **多租户超级用户角色** 的同一租户关联。



STEP 4 |（仅限多租户）在 **Customer Support Account**（客户支持帐户）部分，选择与您激活 AI Access Security 许可证的租户关联的 Palo Alto Networks 客户支持帐户。

如果您有单租户客户支持门户帐户，请跳过此步骤。默认情况下，您的客户支持帐户处于选中状态。

STEP 5 |（仅限多租户）在 **Allocate This Subscription**（分配此订阅）部分，选择要为其激活 AI Access Security 的 **租户服务组 (TSG)**。您可以选择父租户或子租户。

AI Access Security 仅对选定的租户激活。如果选择父租户，则不会为任何子租户激活 AI Access Security。

如果您只有一个租户客户支持门户帐户，请跳过此步骤。默认情况下已选中。

STEP 6 | 查看租户 **Region**（区域）。此区域基于部署的NGFW或Prisma Access租户区域预先填充，无法更改。

Select Customer Support Account

This account is used for the registration and support of the products and add-ons that are bundled with this subscription. [Learn more](#)

Customer Support Account ⓘ

Palo Alto Networks, Inc. ▼

Allocate This Subscription

Allocate the available licenses and add-ons in this subscription to a recipient.

Recipient: Palo Alto Networks, Inc. [Edit](#)

Select Region

Select Region

Region ⓘ

United States - Americas ▼

STEP 7 | 在**Assign Licenses**（分配许可证）部分，单击 **Done**（完成）以分配所有AI Access Security许可证。验证 **AI Access Security License**（AI Access Security 许可证）是否已 **Fully Assigned**（完全分配）

STEP 8 | 如果您的租户上Enterprise Data Loss Prevention (E-DLP)处于活动状态，请验证是否选择了 **Data Loss Prevention**（数据丢失防护）实例。

如果租户上已经处于活动状态，则默认选择您的 Enterprise DLP 实例。

如果没有已激活的Enterprise DLP，请跳过此步骤。启用AI Access Security不需要Enterprise DLP。如果 Enterprise DLP 实例尚未激活，则会在许可证激活过程中创建一个实例。查看如果 [不续订AI Access Security许可证](#)，Enterprise DLP会发生什么。

Data Security Access Licenses : Fully Assigned [Edit](#)

LICENSES

AI Access Security for PA and Next-Generation Firewall: 30 Users

Data Loss Prevention (Optional)

Select an existing Data Loss Prevention instance that you want to use in this tenant. Data Loss Prevention is set of tools and processes that allow you to protect sensitive information against unauthorized access, misuse, extraction, or sharing.

Palo Alto Networks, Inc. ▼

STEP 9 | 同意条款和条件。

STEP 10 | 激活。

您将被重定向到 **Tenant Management**（租户管理）页面，此时 **AI Access Security Activation Status**（激活状态）开始 **Initializing**（初始化）。

AI Access Security 许可证显示为 **Data Security**（数据安全），并且具有以 **AIX** 开头的序列号。**Activation Status**（激活状态）显示为 **Complete**（完成）后继续下一步。

Products	Deployment Profiles	Tenant Acquisition History		
Products	Activation Status	License Capacity	Serial Number	Expiration Date
IoT Security	Complete	N/A	N/A	
Strata Logging Service	Complete	Data Space: 1 TB		02/24/2026
AI Ops for NGFW	Complete	N/A	N/A	
Enterprise DLP	Complete	N/A	N/A	
Demisto	Complete	N/A	N/A	
Cortex XSOAR	Complete	N/A	N/A	
SaaS Security	Complete	N/A	N/A	
Armis	Complete	N/A	N/A	
Cloud Identity Engine	Complete	N/A	N/A	
AI Ops for NGFW Free	Complete	N/A	N/A	
Data Security	Complete	AI Access Security for PA and Next-Gen	AIX	08/19/2025

STEP 11 |（仅限 NGFW）将 AI Access Security 许可证与您的 NGFW 关联。

需要关联 AI Access Security 许可证才能为您的 NGFW 激活许可证。

1. 在 Strata Cloud Manager 菜单中，选择 **Settings**（设置） > **Device Associations**（设备关联）。
Strata Cloud Manager 菜单位于 Strata Cloud Manager 的左下角。
2. 在 Strata Cloud Manager 菜单中，选择 **System Settings**（系统设置） > **Device Associations**（设备关联）。
Strata Cloud Manager 菜单位于 Strata Cloud Manager 的左下角。
3. **Associate Apps**（关联应用程序）。
4. 在许可产品中，选择 **Data Security**（数据安全）。
5. 选择要为其激活 AI Access Security 的 NGFW。
6. **Save**（保存）。

STEP 12 | 验证您是否成功激活 AI Access Security。

1. 登录到 Palo Alto Networks [客户支持门户 \(CSP\)](#)。
2. 选择 **Products** (产品) > **Assets** (资产)。
3. 根据您激活 AI Access Security 的实施点选择 **NGFW** 或 **Prisma Access** 租户。
4. 使用过滤器定位您的 NGFW 或 Prisma Access 租户。
5. 展开活动许可证列表或单击 **Licenses & Subscriptions** (许可证和订阅)。
6. 验证 AI Access Security 许可证是否已激活。

DNS Security				10/10/2025
SD WAN				10/10/2025
IoT Security				10/25/2026
Advanced URL Filtering				10/10/2025
SaaS Security Inline Eval				10/15/2024
DLP				10/15/2025
PAN-DB URL Filtering				10/10/2025
Advanced Threat Prevention				10/10/2025
Decryption Port Mirror				Perpetual
Cortex Data Lake				02/24/2026
Advanced WildFire License				10/10/2025
WildFire License				10/10/2025
AI Ops for NGFW				09/23/2026
AI Access Security for Next-Generation Firewall				08/19/2025

STEP 13 | 开始使用 AI Access Security。

将 AI Access Security 评估许可证转换为生产许可证

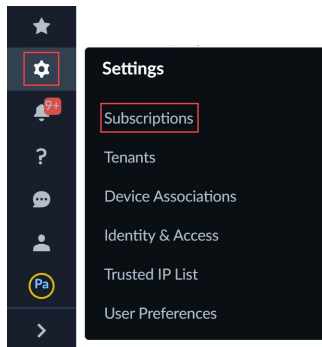
如果您已激活 AI Access Security **EVAL license**（评估许可证），则必须在评估期结束后将评估许可证转换为生产许可证，才能继续安全地控制对 GenAI 应用程序的访问和采用。如果不将评估许可证转换为生产许可证：

- 包含敏感数据的流量不再转发给 Enterprise Data Loss Prevention (E-DLP) 进行检查和判定。
- Enterprise DLP 不可再访问。
 - Panorama™ management server—Objects（对象）> DLP
 - Strata Cloud Manager—Manage（管理）> Configuration（配置）> Data Loss Prevention（数据丢失预防）
- 将保留为 AI Access Security 创建的 Web 安全性和安全策略规则。

STEP 1 | 登录 Strata Cloud Manager

STEP 2 | 在 Strata Cloud Manager 菜单中，选择 **Settings**（设置）> **Subscriptions**（订阅）。

Strata Cloud Manager 菜单位于 Strata Cloud Manager 的左下角。



STEP 3 | 选择 **System Settings**（系统设置）> **Subscriptions**（订阅）。

STEP 4 | 查找 AI Access Security 评估许可证，然后选择 **Actions**（操作）> **Eval to Prod Request**（评估到生产请求）。

STEP 5 | 为租户指定所需的生产许可证条款。您的 Palo Alto Networks 客户代表会审核请求以创建报价。

在您的生产许可证请求中指定以下信息。

- **License Quantity**（许可证数量）— 可以使用 AI Access Security 的个人数量。
- **Term**（期限）— 您 AI Access Security 订阅的长度。

STEP 6 | **Send Request**（发送请求）。

续订 **AI Access Security** 许可证

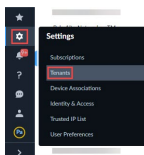
您可以续订即将到期的 **AI Access Security** 许可证，以继续安全地采用 **GenAI** 应用程序。即将到期的 **AI Access Security** 不会自动续订，需要您手动续订。如果 **AI Access Security** 过期：

- 包含敏感数据的流量不再转发给 **Enterprise Data Loss Prevention (E-DLP)** 进行检查和判定。
- **Enterprise DLP** 不可再访问。
 - **Panorama™ management server—Objects**（对象） > **DLP**
 - **Strata Cloud Manager—Manage**（管理） > **Configuration**（配置） > **Data Loss Prevention**（数据丢失预防）
- 将保留为 **AI Access Security** 创建的 **Web** 安全性和安全策略规则。

STEP 1 | 联系您的 Palo Alto Networks 销售代表并请求续订您的 **AI Access Security** 许可证。

STEP 2 | [登录](#) Strata Cloud Manager

STEP 3 | 从左下角菜单中选择 **Settings**（设置） > **Tenants**（租户）。



STEP 4 | 选择 **System Settings**（系统设置） > **Tenants**（租户）。

STEP 5 | 选择您要续订 **AI Access Security** 许可证的租户。

您可以选择父租户或子租户。需要立即采取行动续订许可证的租户，其信息标记为蓝色圆圈。

STEP 6 | **Edit**（编辑）租户许可证。

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

