SASE

SOLUTION GUIDE

# Securing Access to GenAI Applications

Part of the "SASE for Securing Internet" and "On-Premises Network Security for the Branch" reference architectures

OCTOBER 2025

# Table of Contents

**Preface** 3

**Purpose of This Guide** 5

Audience 5

Related Documentation 5

**Introduction** 7

Security Challenges 7

Essential Capabilities 8

Solution Overview 8

**Design Details** 10

Strata Cloud Manager 10

Visibility and Control 10

Visibility and Control for Unmanaged Devices 16

Securing Access to AI Applications Design Model 18

**Securing Access to AI Application Deployment Details** 26

Assumptions and Prerequisites 26

Configure Microsoft Entra ID Group 28

Configuring Security Policy Objects 29

Configuring NGFWs to Control Access to SaaS Applications 38

Configure Security Profile Groups with Custom URL Access Management and DLP Profiles 43

Configuring Security Policy Rules to Control Access to AI Applications 49

Using Activity Insights to Monitor and Tag GenAI Applications 54

Configuring Security Policy Pre-Rules to Control Access to AI Applications for Explicit Proxy 58

**Summary** 64

**Feedback** 65

# Preface

## GUIDE TYPES

Overview guide

Design guide

Deployment guide

Solution guide

*Overview guides* provide high-level introductions to technologies or concepts.

*Design guides* provide an architectural overview for using Palo Alto Networks® technologies to provide visibility, control, and protection to applications built in a specific environment. These guides are required reading prior to using their companion deployment guides.

*Deployment guides* provide decision criteria for deployment scenarios, as well as procedures for combining Palo Alto Networks technologies with third-party technologies in an integrated design.

*Solution guides* provide add-on solutions for post-deployment use cases.

## DOCUMENT CONVENTIONS

*Notes* provide additional information.

*Cautions* warn about possible data loss, hardware damage, or compromise of security.

Blue text indicates a configuration variable for which you need to substitute the correct value for your environment.

In the **IP** box, enter 10.5.0.4/24, and then click **OK**.

**Bold text** denotes:

- Command-line commands.

  **# show device-group** branch-offices

- User-interface elements.

  In the **Interface Type** list, choose **Layer 3**.

- Navigational paths.

  Navigate to **Network > Virtual Routers**.

- A value to be entered.

  Enter the password **admin**.

*Italic text* denotes the introduction of important terminology.

An *external dynamic* list is a file hosted on an external web server so that the firewall can import objects.

Highlighted text denotes emphasis.

Total valid entries: 755

## ABOUT PROCEDURES

These guides sometimes describe other companies' products. Although steps and screen-shots were up-to-date at the time of publication, those companies might have since changed their user interface, processes, or requirements.

## GETTING THE LATEST VERSIONS OF GUIDES

We continually update reference architecture guides. You can access the latest version of this and all guides at this location:

**https://www.paloaltonetworks.com/referencearchitectures**

## WHAT'S NEW IN THIS RELEASE

Since the last version of this guide, Palo Alto Networks made the following changes:

- Updated for Prisma® Access 5.2.2 release
- Updated navigation guidance for the new left-side navigation menu
- Updated configuration to use snippets
- Made minor updates to correct navigation and improve readability

# Purpose of This Guide

This solution guide builds on the designs described in the **SASE for Securing Internet** and **On-Premises Network Security for the Branch** reference architectures.

This solution guide describes policy design-and-deployment details for securing access to artificial intelligence (AI) applications by using the Palo Alto Networks Prisma Access cloud-delivered security platform and the Palo Alto Networks next-generation firewall (NGFW). Prisma Access and NGFWs offer industry-leading security services with best-practices security policies that help you quickly and safely enable web and SaaS applications, for all users, across all locations, by eliminating known and unknown cyberthreats.

## AUDIENCE

This guide is for technical readers, including system architects and security engineers, who want to deploy Prisma Access and NGFW policies for securing access to AI applications. It assumes the reader has an operational Prisma Access or branch infrastructure and is familiar with the basic concepts of SaaS and AI applications, networking, and security, as well as a basic understanding of internet perimeter architectures.

## RELATED DOCUMENTATION

The following documents support this guide:

- **SASE Overview**—Describes components and benefits of a SASE solution and how Palo Alto Networks delivers a full-featured SASE solution with the combination and integration of Prisma Access, Prisma SD-WAN, and cloud-delivered security services.
- **Securing Internet for Mobile Users by Using Tunnel Mode: Design Guide**—Provides design guidance for securing internet access for mobile users by using Palo Alto Networks Prisma Access tunnel mode, which provides complete visibility and control for internet and enterprise SaaS applications.
- **Securing Internet for Mobile Users by Using Tunnel Mode: Deployment Guide**—Provides implementation details for using Prisma Access to secure internet access for mobile users. Includes decision criteria for tunnel-mode deployment scenarios, as well as step-by-step procedures that achieve an integrated design.
- **Securing Internet for Mobile Users by Using Explicit Proxy: Design Guide**—Provides design guidance for securing internet access for mobile users by using Palo Alto Networks Prisma Access proxy mode, which provides complete visibility and control for internet and enterprise SaaS applications.
- **Securing Internet for Mobile Users by Using Explicit Proxy: Deployment Guide**—Provides implementation details for using Prisma Access to secure internet access for mobile users. Includes decision criteria for explicit proxy deployment scenarios, as well as step-by-step procedures that achieve an integrated design.
- **Securing Internet for Mobile Users by Using Prisma Access Browser: Design Guide**—Provides design guidance for securing internet access for mobile users by using Palo Alto Networks Prisma Access Browser, which provides complete visibility and control for internet and enterprise SaaS applications.

- **Securing Internet for Mobile Users by Using Prisma Access Browser: Deployment Guide**—Provides implementation details for using Prisma Access Browser to secure internet access for mobile users. Includes decision criteria for deployment scenarios, as well as step-by-step procedures that achieve an integrated design.
- **Secure Internet Policy Design: Solution Guide**—Provides policy design and deployment guidance for securing internet services by using the Prisma Access cloud-delivered security platform and Palo Alto Networks next-generation firewalls.
- **Enhancing Internet Security with SSL Forward-Proxy Decryption: Solution Guide**—Provides design and deployment guidance for using forward-proxy decryption in the Prisma Access cloud-delivered security platform and Palo Alto Networks next-generation firewalls.
- **Identity-Based and Posture-Based Security for SASE: Solution Guide**—Provides design and deployment guidance for obtaining and applying identity-based and posture-based policies in the Palo Alto Networks SASE platform.
- **Securing the Branch with On-Premises Network Security: Design Guide**—Provides design guidance for using Palo Alto Networks next-generation firewalls to secure branch offices. Includes descriptions of common branch office network layouts, as well as design and deployment considerations for centralized management and advanced logging capabilities.
- **Securing the Branch with On-Premises Network Security and Strata Cloud Manager: Deployment Guide**—Provides implementation details for using Palo Alto Networks next-generation firewalls to secure branch offices. Includes high-level tasks and step-by-step configuration details for centralized management and advanced logging capabilities.

Other recent guides include:

- **SASE for Securing Internet: Design Guide**—Provides design and deployment guidance for using Prisma Access and Prisma SD-WAN to secure internet access for mobile users and users located at remote-site locations.
- **SASE for Securing Internet: Deployment Guide**—Provides implementation details for using Prisma Access and Prisma SD-WAN to secure internet access for mobile users and users located at remote-site locations. Includes decision criteria for deployment scenarios, as well as step-by-step procedures to achieve an integrated design.

# Introduction

AI is the simulation of human intelligence in machines designed to think like humans and mimic their actions. Evolving from basic computational algorithms to advanced neural networks, AI has filled various facets of human life, driving advancements in areas ranging from healthcare and finance to entertainment and communication.

Among the many subsets of AI, large language models (LLMs) have emerged as groundbreaking tools in the world of natural language processing. These models, trained on vast datasets encompassing a significant portion of the internet, have the ability to understand and interact using human language. LLMs can produce content, answer queries, and even engage in meaningful and contextually relevant conversations, making them immensely valuable in diverse applications. Parallel to the evolution of LLMs, chatbots—automated conversational agents—have gained significant traction in the digital world. Initially designed for simple rule-based interactions, modern chatbots, often powered by LLMs, are capable of sophisticated dialogues, making them vital for customer support, e-commerce, and countless other applications.

## SECURITY CHALLENGES

The emergence of AI, LLMs, and chatbots raises many security concerns. Unauthorized access, data breaches, and misuse can not only harm businesses but can also lead to significant consequences such as privacy erosion, misinformation and manipulation, and liability. To ensure robust security for AI applications, one must tackle a unique set of challenges related to access control, data integrity, and data protection. These challenges arise from the complexity of AI applications and the vast amount of data they process.

Some of the most common security challenges associated with AI applications include the following:

- **Data Security and Privacy**—AI applications often process large volumes of sensitive data, which can be vulnerable to breaches and leaks.
- **Access Control and Identity Management**—Ensuring that only authorized users have access to AI tools and the data they process and generate is crucial.
- **Legacy System Integration**—Many AI applications interface with older systems that might not have been designed with modern security considerations in mind. This can create vulnerabilities at the points of integration.
- **Data Protection in Transit**—Sensitive data used by AI applications must be protected during transit which can be complex given the volume and velocity of data.
- **Real-Time Data Processing**—AI applications often process data in real-time, necessitating immediate security responses to potential threats. Real-time monitoring of user activities and access patterns is critical and must ensure that legitimate user activity is not blocked by security checks.
- **Scalability and Flexibility**—As organizations grow, their security solutions must scale accordingly without compromising security or performance. Policies must be designed to be scalable, yet granular enough to provide effective security controls.
- **Endpoint Protection**—AI applications are accessed from a multitude of devices which could be exploited as entry points for attacks.

To address the challenges listed above requires in-depth security. This includes both the applications themselves and controlling access to the applications. The primary focus of this guide is on how an organization can control access to AI applications. An organization might have only limited control over how AI applications secure data, but they do have control over which AI applications they choose to provide access to.

Securing AI applications requires a multi-faceted approach, blending traditional IT security measures with AI-specific strategies. To maintain strong security controls as AI usage increases and applications evolve requires flexible and dynamic methods to classify new applications and to respond to emerging threats.

## ESSENTIAL CAPABILITIES

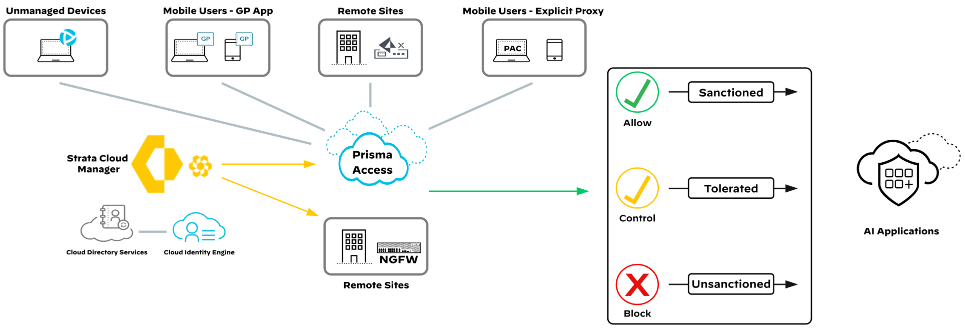
To address these security challenges, an organization must be able to control access to AI applications. To comprehensively secure AI applications, a solution must provide the following capabilities:

- Allow users to access sanctioned AI applications and restrict access to other AI applications
- Provide visibility into which AI applications an organization is using
- Prohibit uploads of private or sensitive information data to AI applications
- Control access to AI applications from managed and unmanaged devices
- Incorporate user-identity and device-posture information when granting access to AI applications

## SOLUTION OVERVIEW

When planning to enable access to AI applications, an organization must identify which applications they might need or already use, align with the business needs for the applications, and determine the user communities that require the applications. With this information, they can use security capabilities from Palo Alto Networks in order to provide secure access to AI applications.

*Figure 1  Securing Access to AI Applications solution overview*



The solution includes the following components:

- Prisma Access, NGFWs, and Strata™ Logging Service (formerly *Cortex® Data Lake*), along with the AI Access Security™ license, provide visibility and control of AI applications. After discovering the AI applications that are in use, InfoSec admins use attributes from AI Access Security in order to simplify the classification of AI applications. You can configure Prisma Access and NGFWs to enforce security policy rules that control access to AI application categories and to log user activity to Strata Logging Service (SLS).
- To identify the applications, App-ID™ Cloud Engine (ACE) provides rapid availability and delivery of App-IDs to Prisma Access and NGFWs. ACE uniquely identifies each generative AI (GenAI) application and includes a risk score for each, so you can tag the App-ID as Sanctioned, Tolerated, or Unsanctioned.
- Strata Cloud Manager (SCM) provides a single console to configure the solution and monitor activity. SCM allows you to share a common policy across Prisma Access and your on-premises NGFWs. To inform and alert on AI applications, SCM provides dashboards and activity insights.
- Enterprise Data Loss Prevention (DLP) prevents the sharing of protected data. To protect sensitive data from unauthorized sharing, when a user accesses an AI application, E-DLP inspects application traffic.
- GlobalProtect® app secures access for mobile users, enforces device posture checks before access, and determines user identity for endpoints accessing the applications. To display notifications to users when DLP policies block access, the GlobalProtect app also enables Access Experience.
- Cloud Identity Engine extends user-group membership information with Prisma Access and NGFW. Authorizing access to AI applications requires user identity and associated group membership. To control access to AI applications, you can use CIE-provided group membership.
- Prisma Access Browser (PAB) secures access to sanctioned applications from unmanaged devices. PAB provides a secure workspace for access to approved AI applications from unmanaged devices, can enforce device posture checks before access, and strictly controls browser components and extensions. PAB also provides its own DLP controls and protects sensitive data sourced by approved AI, prevents unauthorized data capture, and controls file downloads.

The next section contains more detailed information about these components and their capabilities.

# Design Details

This solution describes how Prisma Access and NGFW allow you to gain visibility and control of AI applications, ensure data governance, and mitigate the risk of data leaks and threat propagation.

## STRATA CLOUD MANAGER

Palo Alto Networks SCM provides unified management across an organizations' entire Palo Alto Networks Network Security infrastructure, both NGFWs and SASE environment, from a single, centralized user interface.

SCM consolidates a variety of tools designed to streamline the management of both physical and virtual firewalls to enhance network security. These include a hierarchical folder structure for configuration and policy, actionable insights through several dashboards, and easy troubleshooting and problem resolution.

SCM offers administrators consistent policy enforcement, easy deployment of configurations, and updates to multiple firewalls and sites. SCM identifies deployed security capabilities, and guides administrators to enable additional features based on the best practices to strengthen your security posture. SCM also enhances operational efficiency through automation and reduces complexity by unifying management tasks.

## VISIBILITY AND CONTROL

Prisma Access and NGFW provide both visibility into the use of AI applications and the ability to control users' access to those applications. Key to both visibility and control is App-ID, Decryption, Advanced URL filtering, DLP and User and group-based security policy functionality.

Prisma Access and NGFW achieve visibility and control of AI applications traffic through the following:

- Leverage App-ID to accurately identify and control applications traversing your network, segmenting by specific application categories for precise traffic filtering.
- Use decryption to inspect encrypted traffic, ensuring that hidden threats within encrypted communications are identified and mitigated.
- Implement Enterprise DLP to monitor and protect sensitive information in transit for comprehensive data protection.
- Design user and group-specific policies to provide tailored security measures, ensuring different access levels and controls based on user roles.
- Adopt Advanced URL Filtering to monitor and control web activity, blocking access to malicious or unwanted websites based on categorizations.

### App-ID

ACE integrates with Prisma Access and NGFW to provide additional App-IDs from the cloud for applications that do not have specific predefined App-IDs from the Palo Alto Networks content update team. ACE increases the number of known App-IDs, accelerates the availability and delivery of new App-IDs, and significantly improves application visibility. ACE classifies application types by category and subcategory. Within a category or subcategory, ACE also assigns a risk value, which is an assessment of relative risk. You can use the risk value to determine how to inspect, log and control your applications appropriately. ACE is enabled by default on Cloud Managed Prisma Access and NGFW with a SaaS Security Inline license.

Leveraging these cloud-delivered App-IDs, you can achieve better control and visibility over AI applications. These App-IDs can distinguish AI applications from general traffic, regardless of their transmission protocols or attempts to disguise their network footprint. This capability is crucial for managing AI tools that might dynamically change their communication patterns or use non-standard ports. Moreover, through App-IDs, administrators can enforce policies that specifically target AI applications.

## AI Access Security

AI Access Security integrates with Prisma Access and NGFW in order to provide AI-specific capabilities that include application discovery, usage monitoring, and access control.

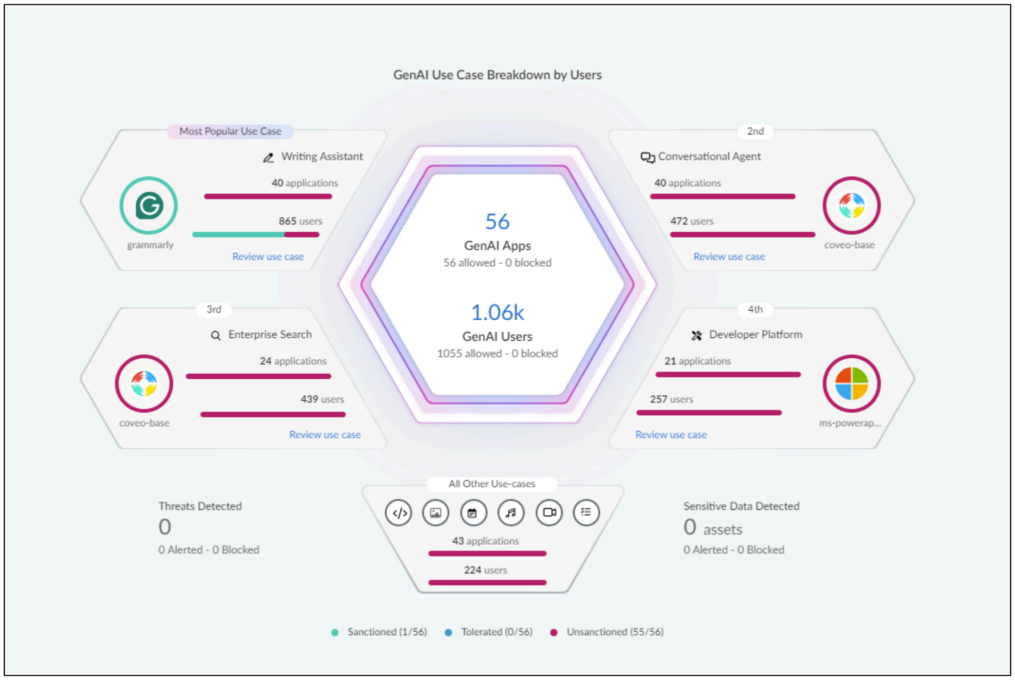
The simplest ways to license AI Access Security capabilities include:

- **AI Access Security license**—With this license, you get access to the subset of the ACE App-IDs that are tagged as GenAI. This also includes Enterprise DLP inspection for GenAI applications only.
- **CASB-PA and CASB-X licenses**—With these licenses, you get access to all AI Access Security license components, the SaaS Security Inline license that enables the full set of ACE App-IDs, and Enterprise DLP inspection for all applications. These licenses also include the SaaS Security API and SaaS Security Posture Management.

When you use SCM to manage Prisma Access and NGFW, you use the Activity Insights dashboard in order to discover applications your organization is actively using. AI Access Security includes filtering capabilities that make it easy to identify the App-IDs associated with the GenAI applications. You can then associate tags with the App-IDs, which simplifies the creation and maintenance of security policy rules.

SCM also includes AI Access Insights, which provides in-depth details on GenAI application use, including the users that are accessing the applications, the permitted and blocked applications, and whether the applications are sanctioned, tolerated, or unsanctioned.

*Figure 2  AI Access Insights dashboard*



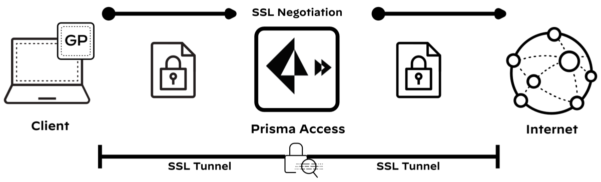
You can use AI Access Security with both traditional security policy rules and Prisma Access Web Security rules, but the scope of this guide only includes traditional security policy rules.

## Decryption

To decrypt HTTPS internet traffic from all users, Prisma Access and NGFW use the SSL forward proxy capabilities. Without decryption, security inspection and control are limited to clear-text traffic only. Because most web traffic today is HTTPS based, ensuring broad-based inspection of your user traffic requires decryption.

To secure the connection, SSL uses certificates to establish trust between the client and server. Most commonly, to establish this trust, an organization uses its own public key infrastructure to generate a trusted signing certificate for SCM. The endpoints must install the SCM root CA certificate into their certificate store so that the client session to the decrypting device can be established. You can use GlobalProtect to install the trusted root CA certificate on Windows and macOS clients. Alternatively, SCM includes built-in signing certificates that you can use for testing.

*Figure 3  SSL forward proxy with Prisma Access*



## Enterprise DLP

With the industry's first cloud-delivered DLP service, this solution provides data protection and compliance controls consistently across SaaS applications. This solution delivers the following data-security capabilities:

- **Highest levels of detection accuracy**—This solution automatically detects sensitive content via ML data classification and an extensive number of described data identifiers using regular expressions (regex) or keywords (examples: credit card or ID numbers, financial records, General Data Protection Regulation (GDPR), or other data privacy and compliance-related information) and applies customizable data profiles and Boolean logic to scan for collective types of data.
- **Scanning, classification, and protection**—This solution analyzes all data stored within SaaS applications in order to make sure policy violations, exposures, and regulatory compliance are properly addressed.
- **Exposure analysis**—To reduce incidents and inaccurate detection, this solution analyzes public, external, and internal sharing of files, as well as precise context criteria (example: number of occurrences and pattern logic).
- **Exact data matching**—An advanced data-fingerprinting method detects specific sensitive data such as personally identifiable information (PII) and prevents exfiltration.
- **Secure collaboration applications**—Ensuring high accuracy and fewer false positives, this solution automatically identifies sensitive information even within the context of unstructured users' conversations by using deep learning, natural language processing, artificial intelligence models, and advanced optical character recognition (OCR).
- **Detection of flexible document properties**—Third-party data tagging augments the identification of sensitive data. This solution also includes file-blocking profiles that you can use to prevent file types from being downloaded, which is an important part of a cloud data protection strategy.
- **Automated incident workflows**—Policy-based response actions include user alerts and auto-remediation.

To evaluate the content of data being sent (data-in-motion) to AI applications, you use Enterprise DLP. *Enterprise DLP* is a cloud-based service that is natively integrated into existing security control points such as SaaS Security Inline (Prisma Access and NGFW). It provides instantaneous protection for data by applying consistent data-security policies at scale.

To avoid data loss and data theft, Enterprise DLP discovers, monitors, and protects your sensitive data. The service detects sensitive data by using a combination of techniques that include regex, keywords, and ML. The service applies customizable data profiles by using Boolean logic, which provides much more granular data-matching options and accuracy than just using search patterns. The service contains 1000+ data patterns and 20+ data profiles, including profiles for GDPR, California Consumer Privacy Act (CCPA) and PII. You can also create your own DLP profiles.

Data security is an important aspect of SaaS security, one of the key outcomes of data security is to protect sensitive data from being exposed. The design goals for SaaS data security are the following:

- Prevent disclosure of PII
- Prevent theft of intellectual property information

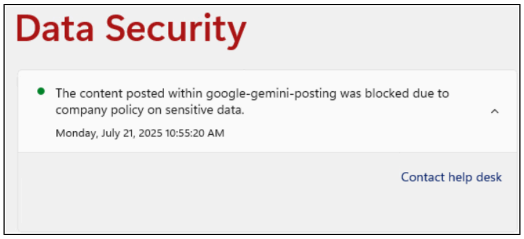
- Meet compliance with external standards such as GDPR, CCPA, Payment Card Industry Data Security Standard (PCI DSS), and Health Insurance Portability and Accountability Act (HIPAA).
- Protect sensitive data from malicious or well-meaning insiders.

The process for securing SaaS data is as follows:

1. Identify business-critical and/or PII data.
2. Identify business-required regulatory compliance standards.
3. Identify file types and storage locations.
4. Choose data profiles based on data patterns and matching logic that meet your requirements.
5. Using the data profiles identified, create data-asset policies in order to secure data being sent to AI applications.
6. Apply data profiles in your security policies in order to secure data uploads to AI applications.
7. Monitor and remediate incidents.

When Enterprise DLP detects unauthorized sharing of sensitive data, it creates an incident. If the DLP policy rule that created the incident includes a Block action, then Enterprise DLP causes Prisma Access or NGFW to block the data transfer. After a block, the application indicates that an error occurred but typically provides no further context on the cause. To provide more details to the user, Enterprise DLP includes an End User Coaching feature that allows you to display a Data Security notification within the Access Experience Endpoint Agent when it takes a block action.

This notification includes the application name and the action taken for non-file-based incidents. To provide further information, you can also include a link to a support site.



Data Security

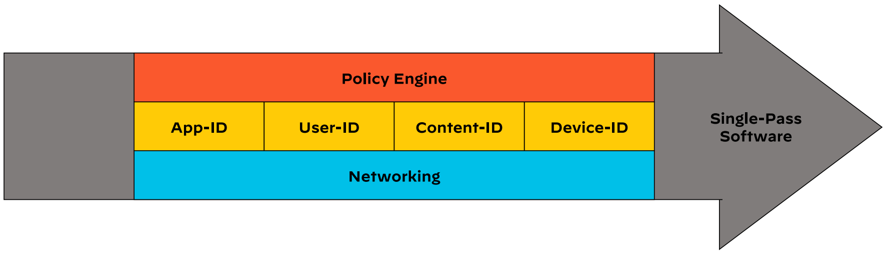
The content posted within google-gemini-posting was blocked due to company policy on sensitive data.

Monday, July 21, 2025 10:55:20 AM

## Identity

Palo Alto Networks incorporates identity-based security in the core of their next-generation firewalls and Prisma Access. Called *User-ID*™, identity-based security is an integral part Palo Alto Networks single-pass architecture.

*Figure 4  User-ID as part of the single-pass architecture*



User-ID accurately and continually maps IP addresses to users and users to groups. As a user accesses network resources from different locations or from different devices, the IP address (or addresses, if the user is using more than one device) associated with that user is updated automatically. User and group information is obtained from the user's company identity providers, and the IP address association is obtained from authentication events.

To create identity-based policies, Prisma Access and NGFW must have a list of all available users and their corresponding group memberships. Prisma Access and NGFW do this by integrating with several sources of user and group membership data. Prisma Access and NGFW use this information to populate the source list for users and groups in security policies, enabling you to create identity-based policies.

In this guide, you use the GlobalProtect app as the preferred solution for obtaining IP-to-user mapping. GlobalProtect provides the IP-to-user mapping directly to Prisma Access or the NGFW. Mobile users authenticate when they create the VPN tunnel to access Prisma Access. If they are on an internal network, the users do not need to establish a secure tunnel to the gateway and instead authenticate only via an internal gateway. In addition to authentication, the internal gateway redistributes User-ID information to the rest of the Prisma Access infrastructure and on-premises NGFWs. You can deploy the internal gateway natively in Prisma Access, on an on-premises NGFW, or on a NGFW hosted in the public cloud.

## Advanced URL Filtering

Advanced URL Filtering in Prisma Access offers a next-generation approach to monitoring and controlling web activity, ensuring that organizations can navigate the vast digital landscape securely. This feature goes beyond conventional URL filtering by providing detailed insights into web traffic and offering dynamic controls based on real-time analysis.

This feature’s capabilities include the following:

- **Granular categorization**—Advanced URL Filtering categorizes websites and web content into detailed categories and subcategories, allowing for more precise filtering decisions.
- **Real-time analysis**—Instead of relying solely on static databases, the feature analyzes websites in real-time, ensuring that newly created or updated content is appropriately categorized and acted upon.
- **Threat intelligence integration**—Advanced URL Filtering integrates seamlessly with Palo Alto Network's threat intelligence, offering protection against newly discovered malicious URLs or web-based threats.

- **Detailed reporting**—Gain insights into web activity, including allowed and blocked requests, categories accessed, and potential policy violations.
- **Cloud integration**—As a part of Prisma Access, Advanced URL Filtering is inherently designed to work seamlessly in cloud environments, ensuring consistent web protection regardless of where users or resources are located.

## VISIBILITY AND CONTROL FOR UNMANAGED DEVICES

When a user needs to access a sanctioned GenAI application from an unmanaged device, you must provide an access method that prohibits the leaking of private or sensitive information.

Prisma Access Browser is a secure enterprise browser tailored to protect against modern threats and to provide the browsing experience users are familiar with.

Deployment details for Prisma Access Browser are beyond the scope of this guide. For additional information about Prisma Access Browser, see the **Securing Access from Unmanaged Devices Using Prisma Access Browser: Solution Guide**.

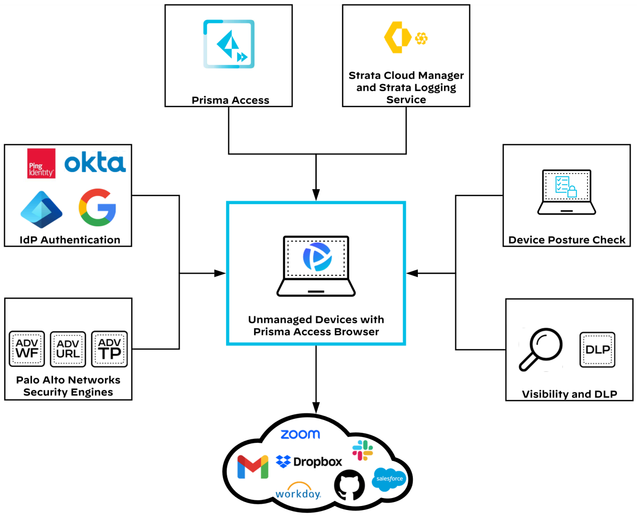
Prisma Access Browser effectively turns the browser into a protected work environment, allowing IT and security departments to closely monitor and manage the use of web and cloud applications by all users, regardless of their location or the device used. As a locked-down browser, Prisma Access Browser significantly reduces the potential attack surface by disabling sensitive components that are often targeted, such as certain vulnerable plugins. It also prevents the installation or execution of malicious extensions, thereby limiting the avenues for unauthorized access and data compromise.

Prisma Access Browser records detailed information about all user activity while they use the browser. This includes not only what the user is accessing but also what actions they are taking. This granular insight enhances IT staff's visibility into user behavior, allowing for real-time monitoring, proactive threat detection, and efficient incident response.

Additionally, Prisma Access Browser secures all browser assets by encrypting them in the computer's storage and memory. This protection shields information from infostealers and screen-scrapers that target browsers and steal access tokens, cookies, credentials, credit-card details, and data used to generate user profiles. Prisma Access Browser prevents unauthorized interception and tampering of information, thus preserving the confidentiality and integrity of the data accessed or transmitted via the browser.

Prisma Access Browser employs multiple security functions that all come together to secure access to corporate resources.

*Figure 5  Prisma Access Browser security*


Prisma Access
Strata Cloud Manager and Strata Logging Service
okta
IdP Authentication
Unmanaged Devices with Prisma Access Browser
Device Posture Check
ADV WF
ADV URL
ADV TP
Palo Alto Networks Security Engines
DLP
Visibility and DLP
zoom
Dropbox
workday
salesforce

## Access Controls

Prisma Access Browser also allows for just-in-time (JIT) controls that grant users temporary access rights to resources for only a specified amount of time. This approach reduces the risk associated with permanent privileges by decreasing the organization's attack surface.

You can configure the JIT controls in the following three ways:

- **Warn and allow**—Informs the user about the risks and sensitivity and allows access.
- **Warn and allow to proceed with a reason**—Informs the user about the risks and sensitivity and requires the user to enter a reason to continue.
- **Permission request**—Requires the user to send a permission request to an admin in order to gain access. An admin approves or denies the requested access, and then the user is notified.

### Palo Alto Networks Security Engines

To secure user traffic, Prisma Access Browser integrates with the following Palo Alto Networks security engines:

- **Advanced URL Filtering**—Advanced URL Filtering is a security feature that provides robust protection against web-based threats. It employs real-time analysis to inspect web traffic and URLs, effectively identifying and blocking access to malicious websites. The filtering leverages a comprehensive database of categorized URLs and applies machine learning in order to detect and prevent threats as they emerge. This proactive approach ensures that even new or previously unknown web-based threats are quickly identified and addressed, offering businesses a dynamic line of defense against a constantly evolving threat landscape.

- **Advanced WildFire**—WildFire® is a cloud-based service that provides threat analysis and prevention. WildFire identifies and protects against unknown, zero-day malware and advanced persistent threats (APTs). It operates by analyzing files and content in a secure cloud environment, using a combination of static and dynamic analysis techniques—including machine learning—to uncover malicious behavior. When Advanced WildFire detects a new threat, it generates signatures and updates that it distributes to Palo Alto Networks customers, enabling their security systems to automatically block the threat. This service allows organizations to benefit from rapid detection, analysis, and dissemination of protection mechanisms against newly emerging cyber threats, ensuring continuous defense against sophisticated attacks.

### Advanced DLP

A key feature of Prisma Access Browser is its browser-based DLP. This feature takes advantage of the browser's ability to access data in its unencrypted form, eliminating the complexity of setting up SSL decryption. This simplicity streamlines the implementation of robust data protection measures that you can tailor to individual users and specific applications. IT security teams can leverage this to effectively guard against data leakage with minimal effort and precise control.

### Device Posture Checks

Prisma Access Browser allows administrators to enforce device-posture checks in order to ensure the device that the browser is running on is compliant. To prevent compromised and non-compliant devices from accessing applications and data, these posture checks occur every 90 seconds.

Administrators can define compliant devices by creating device groups based on operating system, serial numbers, active endpoint protection, and more. They can enforce these device groups in sign-on rules in order to allow or block user access to Prisma Access Browser.

## SECURING ACCESS TO AI APPLICATIONS DESIGN MODEL

Most organizations recognize that they must provide some access to AI applications rather than simply blocking access outright. However, they must carefully balance the requirement to remain secure with the need to provide legitimate access to selected applications.

There are three levels of SaaS application adoption that organizations commonly use. When discussing AI application policy, this guide uses the following terminology:

*Sanctioned* applications are chosen and approved to fulfill a business need. They are critical to the business and typically allowed without restrictions on application functionality. The organization typically subscribes to and supports the use of these applications, often tying them into the business's directory services for single sign-on.

*Tolerated* applications are important to the organization or a subset of users within the organization but are not officially supported by the organization. Organizations might allow full access to tolerated applications to all users, or they might limit access to a subset of functionality (such as download only) or a subset of users (such as the marketing department).

*Unsanctioned* applications are known to be detrimental to the organization and are blocked without exception. There are many reasons to classify an application as unsanctioned, such as being known threat vectors, hosting in dangerous geographic regions with poor security and governance controls, having bad end-user license agreements or service-level agreements, or simply not being relevant to the business.

In this design you provide visibility and control for your AI applications. You use the combination of the following methods:

- Categorize AI applications as Sanctioned, Tolerated, or Unsanctioned so that you can simplify your security policy rules.
- Implement DLP policy to prevent the external sharing of PII and other types of protected data.
- Apply group-based policies to control user access to AI applications.

## Using Security Policy for Visibility and Control of AI Applications

You apply control and achieve visibility of AI applications by using Prisma Access and NGFW *security policy*. Security policy rule definitions require several constructs that help you specify the traffic that you want Prisma Access to inspect, as well as the security services to apply:

- Using multiple policy objects in a security rule allows you to make the rule more concise. Policy objects represent a group of discrete identities that match specific traffic criteria like source, destination, applications, services, and URL categories.
- Each security-policy rule has an action that allows or denies the traffic that matches the list of policy objects.
- For allowed traffic, the security policy provides additional inspection and enforcement by using security profile groups. Security profile groups are collections of security settings that define the security services to be applied to traffic permitted by the initial access control rules.

This design describes how you can use Prisma Access and NGFW to achieve visibility and control for AI applications by using security-policy rules.

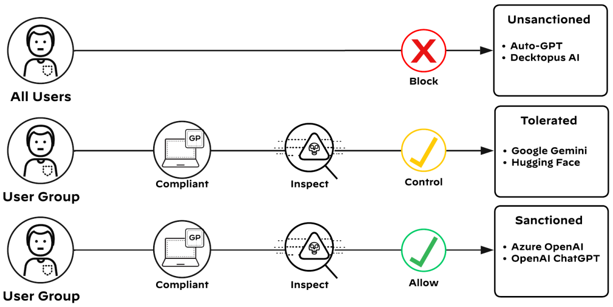
Using application filters in SCM allows organizations to categorize and match multiple App-IDs based on various criteria such as application category, risk level, and more. This approach not only streamlines the process of application identification but also future proofs the security infrastructure. As new applications emerge and are classified within these predefined categories, they are automatically included without manual updates.

### Application Filters in Strata Cloud Manager

Application filters help simplify the process of writing security policies by grouping applications based on common characteristics. For AI applications, we recommend creating four distinct application filters:

- **AI-Sanctioned**—This filter will consist of AI applications that are approved by the organization for use. These applications have been vetted, tested, and are considered secure and beneficial for organizational operations. In this design you explicitly select the sanctioned GenAI App-IDs.
- **AI-Tolerated**—This filter is designed for AI applications that come with certain levels of risks but are still deemed acceptable for use within constraints. These are applications that might not be fully endorsed but are tolerated because of specific operational needs. In this design, for some tolerated GenAI App-IDs, you explicitly select them regardless of their ACE risk value.
- **AI-Tolerated-LowRisk**—This filter is designed for AI applications that come with certain levels of risks but are still deemed acceptable for use within constraints. These are applications that might not be fully endorsed but are tolerated because of specific operational needs. In this design, you select these by matching any GenAI App-IDs with ACE risk values of 1 and 2. Security policy rules that match this application filter should follow rules that match an application filter that includes an explicit tag for Tolerated.
- **AI-Unsanctioned**—AI applications that are categorized under the AI-Unsanctioned filter are considered high risk and are not approved for use within the organization. The applications falling under this category might introduce significant vulnerabilities or are not in line with the organization's security policies and standards. In this design, you implicitly select these by matching any GenAI applications. Security policy rules that match this application filter should be evaluated last.

*Figure 6  Applying application filters to categorize AI applications*



Using application filters to group AI applications into these three categories allows your organization to implement a straightforward set of security-policy rules that are easy to maintain. You can add new applications to the sanctioned category simply by assigning the appropriate tag to the application. The security policies also automatically include new AI applications delivered through ACE by using the subcategory and risk value.

Although App-ID easily identifies and classifies most common AI applications, such as the chatbots ChatGPT and Bard, there might be instances where the classification is not clear. For example, the educational platform Khan Academy natively incorporates AI elements as part of the Khanmigo tutoring application. App-ID might not classify such embedded AI capabilities as belonging in the AI application subcategory, and therefore an application filter that uses that subcategory might not always match embedded AI capabilities. To match these applications, you would need to add an explicit tag as part of your AI security policy.

The recommended approach to use application filters serves as a solid foundation upon which organizations can refine and enhance their application control strategies. However, periodic review of the observed applications is necessary to ensure that your organization achieves the desired results.

## Using DLP Policy for Visibility and Control of AI Applications

The vast amounts of data AI applications handle necessitate strict visibility and control mechanisms to prevent data leaks and ensure compliance with data protection regulations. In this context, Prisma Access's Enterprise DLP capabilities emerge as a powerful tool for safeguarding sensitive information.

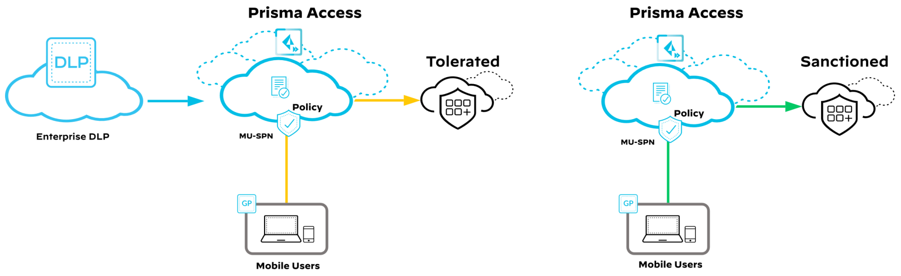
In this design you use the following DLP capabilities:

- **Nested data profiles for comprehensive protection**—To integrate the patterns from multiple built-in categories, we recommend creating a nested data profile. In this design the nested profile should encapsulate PII and Sensitive Content data profiles, thereby creating a layered defense against potential data leaks.
- **Integrating data profiles into security rules**—To ensure that the DLP configurations are actively protecting your AI applications, you will add the DLP profiles to specific security-policy rules.

In this design, your organization uses the following DLP policy:

- For sanctioned AI applications, you can bypass the DLP inspection, because they have been officially approved, having undergone rigorous vetting, testing, and deemed secure and advantageous for the organization. These applications have been approved for use after meeting all your security requirements.
- For tolerated AI applications, it is crucial to enforce a policy that prohibits the uploading of private or sensitive data. Although these applications are not fully sanctioned, they are permitted for specific operational needs. Such a policy ensures the protection of sensitive data.

*Figure 7 DLP policy required only for tolerated applications*



This design not only enhances visibility but also secure control over the data processed by AI applications, ensuring compliance and safeguarding sensitive information.

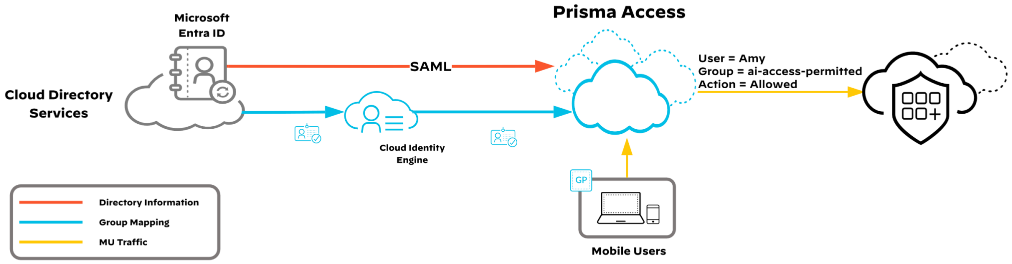
## Group-Based Security Policy for Access to AI Applications

In your organization, ensuring the right people have access to the right tools is essential for maintaining organizational security and efficiency. To limit access to AI applications for authorized users, you implement a group-based security policy. In this design, the organization authorizes AI usage based on the following workflow:

- **Complete training requirements**—Any users who wish to access AI applications must undergo a mandatory training program. This program should cover the basics of the AI tools, their functionalities, potential risks, and best practices for safe and effective use.
- **Manager approval**—After completing the training, their manager must approve access. The manager's role is to ensure that the user has not only completed the training but also understands and can adhere to the guidelines laid out during the training.
- **User-group creation**—When a user has been approved by their manager, IT or the relevant department should add them to a specific user group. This group is designated to have access rights to the AI applications. These user groups can be maintained in Active Directory or any identity and access management tool that the organization uses.

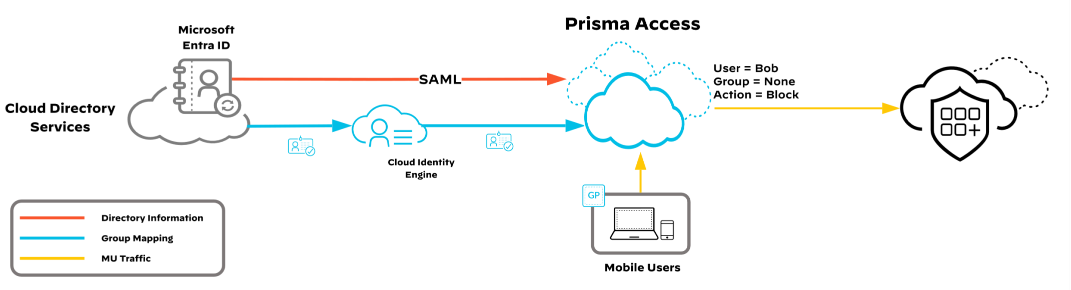
AI applications should be configured to recognize and grant access only to users within the approved user group. Any access requests from outside this group should be automatically denied. Regular audits should be conducted to ensure that only the designated user group has access to sanctioned and tolerated AI applications and that no unauthorized users can access AI applications. Given the dynamic nature of organizations—users frequently change roles, move between departments, or even leave the organization—it's essential to conduct periodic reviews. These reviews ensure that only the current, relevant users have access and prevent potential security risks from inoperative accounts or those no longer requiring access.

*Figure 8  Only authorized users are allowed to access AI applications*



By implementing a group-based security policy, your organization can maintain a controlled environment where only trained and approved personnel have access to AI applications. Not only does this approach safeguard sensitive tools and data, but it also promotes a culture of responsibility and awareness among users.

*Figure 9  Unauthorized users are not permitted to access AI applications*



### Synchronizing User and Group Information from Identity Providers

To implement a security policy based on user groups, you need to integrate to your organization's identity provider, such as Active Directory.

You can find additional in-depth information on this topic in the **Identity-Based and Posture-Based Security for SASE: Solution Guide**.

Although you can create security-policy rules for specific users, when using User-ID in a policy, you typically build the policy around groups of users instead of individual users. Prisma Access and NGFW do not obtain group information from the authentication process, and group membership information cannot be redistributed from other sources. Instead, Prisma Access and NGFW obtains the group mapping information from an identity provider such as a cloud-based source like Microsoft Entra ID.

In this design, use Cloud Identity Engine (CIE) to consolidate directory information into a single source that Prisma Access and NGFW use. CIE can retrieve directory information from multiple sources, including on-premises LDAP and cloud-based directories.

CIE uses read-only APIs to retrieve user and group information from cloud-based identity providers. For on-premises LDAP servers, CIE uses an agent to collect and periodically push group information to the engine from the servers. When connecting CIE to an on-premises LDAP server, you also need configure the NGFW at the data-center edge with a policy that allows traffic from the Cloud Identity agent on the server to the cloud-based CIE. Directory data from cloud-based and on-premises sources is secured via end-end encryption.

The Cloud Identity Engine Directory Sync service then distributes group information to Prisma Access and NGFW to include in your security policies.

Although CIE provides user lists and their group mappings from identity providers to Prisma Access and NGFW, it does not map those users to network traffic. To enforce policies based on identity, you must map IP addresses to the user IDs.

You accomplish this mapping through an authentication event. There are several different types of authentication events that you can use to map IP addresses to users, each with various levels of fidelity. For mobile users and branch users this design uses GlobalProtect authentication and authentication policy to derive the IP-to-user mapping. Similarly, for users accessing via explicit proxy, this design leverages per-session authentication cookies to derive user identity, thereby bypassing the need for IP-to-user mapping.

## Identity for AI Application Access

Identity-based policies can help organizations monitor and manage secure access to sanctioned and tolerated AI applications. In the SASE environment, both mobile and remote-site users pass through Prisma Access before accessing internet applications. In the on-premises environment, remote-site users pass through an NGFW. Before Prisma Access and NGFW can enforce identity-based and posture-based policies, IP addresses must be mapped to the users and security posture information must be retrieved from the devices. For mobile users, this happens as soon as they connect to Prisma Access. For remote-site users, it depends upon the authentication method used.

### Using GlobalProtect for Remote-Site User Access to Internet Applications

The preferred method used to derive the IP-address-to-user mapping information for endpoints on remote-site networks is to use the GlobalProtect app with an internal gateway. The GlobalProtect app authenticates users and can secure communication for devices by using tunneling and encryption. However, many organizations do not require encryption and tunneling for devices already on the private network.

Although remote sites connect to Prisma Access for direct internet access, remote-site networks use SD-WAN for internal communication to the central site. When on an internal network that has a remote-network connection to Prisma Access, the GlobalProtect app connects to a GlobalProtect internal gateway deployed on the Prisma Access RN-SPN, providing a secure and accurate method for identifying traffic by user. Internal gateways do not require encrypted tunnel connections.

At branch locations with NGFWs that do not connect to Prisma Access for direct internet access, the devices behind the firewall are still considered to be on an internal network. When on an internal network, the GlobalProtect app connects to a GlobalProtect internal gateway deployed on an NGFW hosted in the public cloud, providing a secure and accurate method for identifying traffic by user. The internal gateways redistribute User-ID information to the branch NGFWs. For these locations, the Prisma Access GlobalProtect portal assigns the internal gateway that the branch should use, and the GlobalProtect app profile must include that gateway in the list of internal gateways.

### Using Explicit Proxy for Mobile-User and Remote-Site User Access to Internet Applications

Another method of obtaining user-identifying information is through the Prisma SASE explicit proxy. You can use this method for both mobile users and site-based users. This design uses SAML for authentication, although other methods, such as Kerberos, are available. This design builds on the design described in the **Securing Internet for Mobile Users by Using Explicit Proxy: Design Guide**.

There are two methods for deploying explicit proxy. When you use GlobalProtect with the proxy agent, the User-ID information is sent to Prisma Access when the user connects. When using explicit proxy without GlobalProtect, endpoints use a proxy auto-configuration file to send HTTP and HTTPS traffic to the Prisma SASE proxy. The proxy inspects the traffic and checks for the authentication cookie set up by the Prisma SASE explicit proxy. The cookie contains information that identifies the mobile user. If Prisma SASE explicit proxy determines that the user has not been authenticated, it redirects the user to the SAML identity provider.

The User-ID obtained from the authentication cookie does not get mapped to an IP address. Because the security-processing node (SPN) derives the ID from the presence of a valid cookie on the endpoint, IP-to-user mapping is not required for explicit-proxy users.

## Access Experience

Access Experience is an add-on service to Prisma Access that provides native, end-to-end visibility of the entire service delivery path. Access Experience continuously monitors each segment from the endpoint to the application and identifies baseline metrics for each application. In addition, Access Experience provides visibility into any deviations or events that degrade the user experience across each segment between the end user and the application, whether it's the endpoint, Wi-Fi, LAN, router, ISP, Prisma Access, or the application (SaaS, IaaS, or data center). Access Experience continuously monitors every segment in the service delivery path and provides insights that help you quickly isolate the segment that is causing digital experience problems and simplify remediation, including providing the user with recommendations to allow for self-remediation. Access Experience also provides Data Security notifications to the user for Enterprise DLP End User Coaching.

For further information about AI Powered ADEM Access Experience see the **AI-Powered Autonomous Digital Experience Management: Solution Guide**.

You should configure the GlobalProtect app profile used for Access-Experience-enabled users for Windows and/or macOS operating systems only. To control the users and devices that run Access Experience, you can further use User-ID and device-match criteria.

After you configure Prisma Access GlobalProtect to enable Access Experience for a user, the next time the user connects to the Prisma Access GlobalProtect portal, the GlobalProtect app activates the Access Experience User Agent on the endpoint. The Access Experience data-collection process runs in the background and requires no user input.

For endpoint registration and telemetry reporting, you need a security policy that allows HTTPS traffic between the mobile users running Access Experience and the cloud-based Access Experience services. For the list of FQDNs for the cloud services, see the TechDocs topic **Enable ADEM to Monitor Mobile-User Experience**. If you are using decryption on your NGFW, to bypass decryption, you must create a decryption policy that allows traffic to the specified Access Experience FQDNs. If you are using a Prisma Access GlobalProtect tenant, Palo Alto Networks manages predefined global decryption exclusions for Access Experience and no action is required.

# Securing Access to AI Application Deployment Details

This section provides guidelines your organization can follow in order to deploy a security policy to control access to AI applications.

Using shared policies at the Prisma Access configuration scope, these procedures support both mobile users (GlobalProtect and explicit proxy) and remote networks. Shared policies provide consistent security across all connection types and locations.

Similarly, when managing NGFWs using SCM, you can use shared policies for an on-premises device configuration scope for NGFWs.

The following procedures apply for both Prisma Access and NGFW except where specified.

## ASSUMPTIONS AND PREREQUISITES

These procedures assume that you have deployed your Prisma Access infrastructure as described in **SASE for Securing Internet: Deployment Guide** for GlobalProtect and Prisma SD-WAN deployment or either the **Securing Internet for Mobile Users by Using Tunnel Mode: Deployment Guide** or the **Securing Internet for Mobile Users by Using Explicit Proxy: Deployment Guide** for GlobalProtect deployment.

Your Prisma Access deployment should consist of the following:

- Cloud-managed Prisma Access
- Cloud Identity Engine
- A Business Premium or Enterprise license
- An AI Access or SaaS Security Inline license
- An Enterprise DLP license
- GlobalProtect app with Access Experience endpoint agent

Your organization should have a PKI infrastructure and has access to a certificate authority (CA) that has issued trusted certificates and deployed them to your endpoint devices. You can use this CA to issue decryption certificates.

**Note**

When you use explicit proxy for internet access, GlobalProtect is not required.

These procedures assume that you have deployed your branch infrastructure as described in **Securing the Branch with On-Premises Network Security: Design Guide** and **Securing the Branch with On-Premises Network Security and Strata Cloud Manager: Deployment Guide**.

Deploying this solution with NGFWs does not require Prisma Access but does require the following:

- You have an active SCM tenant with an SLS license.
- You use SCM for centrally managing your firewall devices and configuration.
- Cloud management for NGFW is enabled on your SCM tenant.
- Firewall logging uses SLS.
- The tested PAN-OS® version in this deployment guide is 11.2.4 for all devices.
- Sufficient licenses for the expected number of NGFWs.
- Your firewalls have been activated with AIOPS for NGFW Premium license (required for firewalls to be managed by SCM).
- An AI Access or SaaS Security Inline license.
- If your SCM tenant includes an active SaaS Security license, your firewalls must also have been activated with a SaaS Security (SaaS Inline) license.

Before you configure your security-policy rules, you must have an inventory of the AI applications that you want to allow on your network and distinguish between those AI applications you administer and officially sanction and those that you simply want users to be able to use safely (tolerate). After you identify the AI applications you want to allow, you can map them to specific security-policy rules.

You can use the described set of policies to add controls for AI applications to an existing deployment. These procedures assume that you have already configured security policies to allow basic web browsing and use best-practice security profiles while supporting operating system functionality for Windows and Apple endpoints.

This guide also assumes that you have previously activated and configured CIE as described in the **Identity-Based and Posture-Based Security for SASE: Solution Guide** and that you have set up your decryption policies as described in the **Enhancing Internet Security with SSL Forward-Proxy Decryption: Solution Guide**.

## Validation Environment

At the time of writing, we used the following environment to validate this design:

- Prisma Access version 5.2.2 Innovation (PAN-OS 11.2.7)
- Cloud Management version 2025-r3.0
- PA-VM Series 2 version 11.2.4-h9 (on-premises firewall) with the GlobalProtect Gateway License
- GlobalProtect app version: 6.3.2
- Access Experience endpoint agent version: 5.6.14

## Procedures

### Configure Microsoft Entra ID Group

1.1 Assign Group Membership for Authorized Users

The **Identity-Based and Posture-Based Security for SASE: Solution Guide** includes most of the configuration details for CIE integration with Microsoft Entra ID. The following procedure includes only the configuration details for assigning group membership to users that your organization has authorized to access AI applications.

## 1.1 Assign Group Membership for Authorized Users

Later in this guide, you create group-based policy rules that use information from Microsoft Entra ID. In this procedure, you create the Microsoft Entra ID group and assign example users to the group.

**Step 1:** Log in to the Azure Resource Manager at **https://portal.azure.com**.

**Step 2:** Navigate to **Home > Microsoft Entra ID**.

First, you create the group.

**Step 3:** On the left, select **Manage > Groups**, and then click **New Group**.

**Step 4:** In the **Group Name** box, enter AI-access-permitted, and then click **Create**.

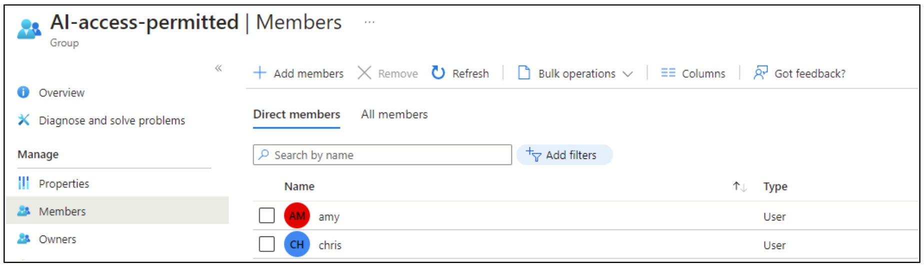
Next, you add members to the group.

**Step 5:** In the list of groups, click AI-access-permitted, and then on the left, select **Manage > Members**.

**Step 6:** Click **Add Members**.

**Step 7:** In the Add members pane, for each user that you want to assign to the group, select the row (example: amy or chris), and then click **Select**.

**Step 8:** Review group membership to ensure it includes your example users.



| Name | Type |
|---|---|
| □ AM amy | User |
| □ CH chris | User |

## Procedures

### Configuring Security Policy Objects

2.1 Access Strata Cloud Manager

2.2 Verify Security Policy

2.3 Enable Decryption

2.4 Create Tags

2.5 Associate the Application-Tagging Snippet

2.6 Create Snippets

2.7 Tag Applications

2.8 Configure Application Filters

2.9 Push Configuration Updates to Prisma Access and On-Premises NGFWs

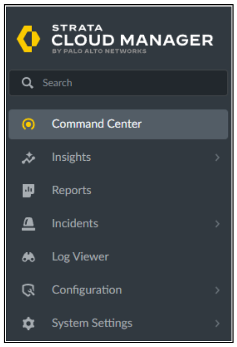
A security-policy rule definition requires the use of several objects that help you specify the traffic that you want Prisma Access to inspect. Policy objects in a security rule allow you to refer to a group of discrete identifiers that match specific traffic criteria such as source, destination, applications, services, and URL categories.

## 2.1 Access Strata Cloud Manager

SCM provides a single management pane that combines Prisma Access, NGFW, and Prisma SD-WAN tasks.

**Step 1:** Log in to **SCM**.

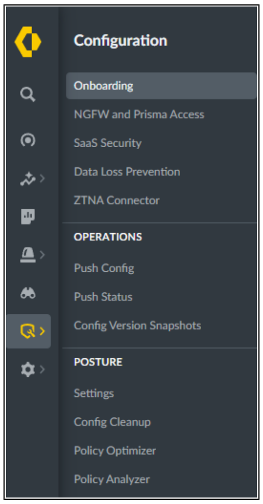
To navigate to specific functions, you use the left panel. If the left panel is collapsed, to see the text labels that describe each function, you can expand it by clicking the chevron at the bottom of the left panel.



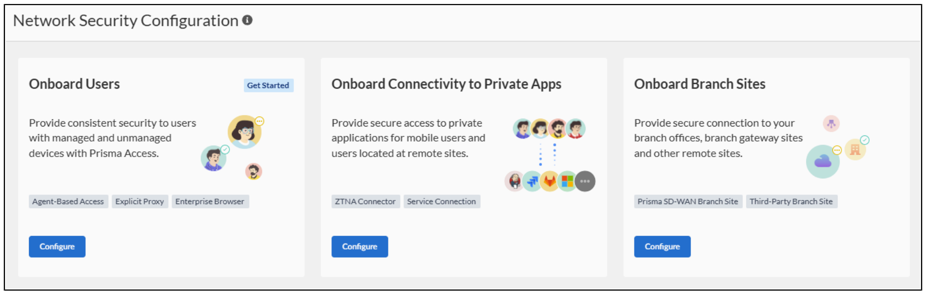
**Step 2:** For effective navigation within SCM, familiarize yourself with the icons. You access initial setup, configuration, and operations tasks by using *Configuration* commands.

Next, you familiarize yourself with SCM functions.

**Step 3:** Click **Configuration**. The Configuration pane appears.



The *Onboarding* function provides simple workflows for most Prisma Access services.


Network Security Configuration

Onboard Users

Provide consistent security to users with managed and unmanaged devices with Prisma Access.

Onboard Connectivity to Private Apps

Provide secure access to private applications for mobile users and users located at remote sites.

Onboard Branch Sites

Provide secure connection to your branch offices, branch gateway sites and other remote sites.

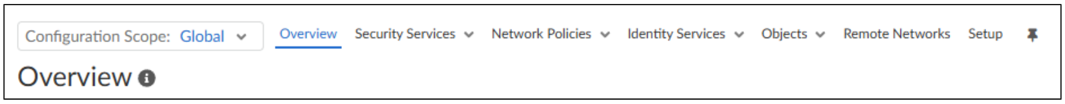
After the initial setup is complete, you access most operational tasks by using *NGFW and Prisma Access* functions. When you use these functions, SCM uses inheritance in order to maintain certain configuration parameters. Settings you make at a higher-level configuration scope, such as Global, are also available as read-only within lower-level scopes, such as Prisma Access and All Firewalls. Each time you start a session with SCM, your configuration scope is set to the same scope selected in the previous session. If you choose a different configuration scope, SCM maintains this choice across all configuration screens that rely on a configuration scope.

By default, SCM uses the Folders tab, which allows you to select configuration scopes for Prisma Access and All Firewalls. For most of the procedures, this guide uses snippets for configuration. By using snippets, you develop modular policies that can be shared and reused across multiple configuration scopes. However, certain configuration elements are best managed within folder-based configuration scopes.

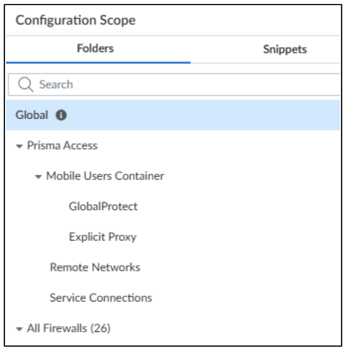
**Step 4:** Continuing in SCM, navigate to **Configuration > NGFW and Prisma Access**. The Overview tab appears.

**Note**

If the Cloud Management for NGFW feature has not been enabled for your tenant, you do not see All Firewalls under Folder Management or Configuration Scope. To enable this feature, contact your Palo Alto Networks representative.



**Step 5:** In the **Configuration Scope** list, click the thumbtack. The Configuration Scope pane now remains visible in this position for all configuration screens. All procedures in this guide assume that you have pinned the Configuration Scope pane.



## 2.2 Verify Security Policy

Verify that you have set up your security policies as described in the **Secure Internet Policy Design: Solution Guide**.

In that guide, you must complete the following tasks in SCM:

- Create zone variables.
- Create rules for blocking high-risk applications.
- Create rules for allowing common internet traffic and general web browsing.
- Create rules to allow access to IT-sanctioned and IT-tolerated applications.

The Secure Internet Policy Design: Solution Guide uses SCM snippets to modularize the configuration elements, and you build on those snippets in this guide.

## 2.3 Enable Decryption

Verify that you have set up your decryption policies as described in the **Enhancing Internet Security with SSL Forward-Proxy Decryption: Solution Guide**.

In that guide, you must complete the following tasks in SCM:

- Import root CA, forward trust, and forward untrust certificates.
- Create the decryption profiles.
- Create the decryption policy rules.

As in this guide, the SSL Forward-Proxy Decryption: Solution Guide uses SCM snippets to modularize the configuration elements.

If you complete the tasks in the solution guide, the GlobalProtect app automatically installs the imported root CA certificate into the local trusted root certificate store of the client machines when they connect. If you plan to install your root CA certificates manually, the guide also includes procedures for their installation.

## 2.4 Create Tags

In this procedure, you define new tags for security-policy rules. For informational purposes only, these tags allow you to easily identify the function of a security-policy rule.

*Table 1 Tag objects*

| Tag | Color | Comment |
|---|---|---|
| AI-Sanctioned | Green | IT-sanctioned AI apps |
| AI-Tolerated | Yellow | IT-tolerated AI apps |
| AI-Unsanctioned | Red | IT-unsanctioned AI apps |

**Step 1:** In SCM, navigate to **Configuration > NGFW and Prisma Access**, and then from the **Objects** menu, choose **Tags**.

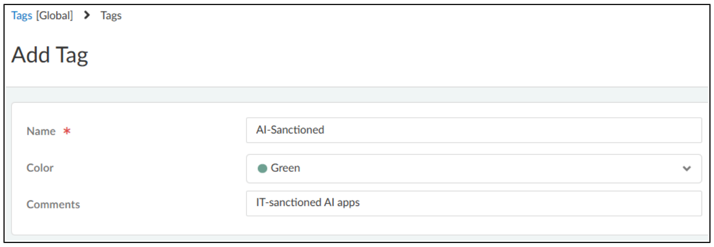
**Step 2:** In the Configuration Scope pane, on the Folders tab, select **Global**.

**Step 3:** Click **Add Tag**.

**Step 4:** In the **Name** box, type **AI-Sanctioned**.

**Step 5:** In the **Color** list, choose **Green**.

**Step 6:** In the **Comments** box, enter a valid comment, and then click **Save**.

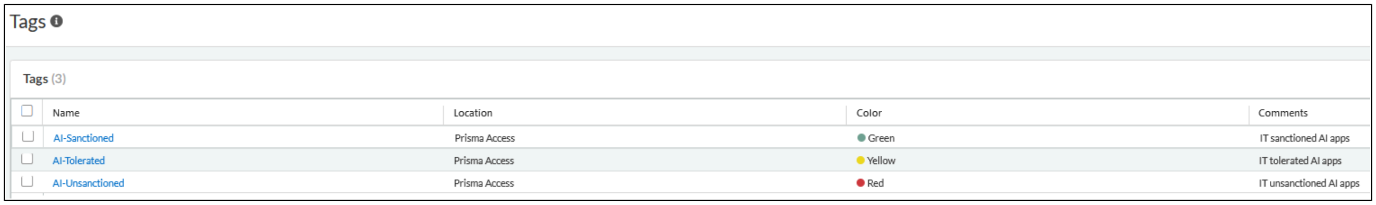


Add Tag

| | |
|---|---|
| Name * | AI-Sanctioned |
| Color | ● Green |
| Comments | IT-sanctioned AI apps |

**Step 7:** For each of the remaining tags in Table 1, repeat Step 3 through Step 6.

**Step 8:** Verify all tags.



Tags

Tags (3)

| □ | Name | Location | Color | Comments |
|---|---|---|---|---|
| □ | AI-Sanctioned | Prisma Access | ● Green | IT sanctioned AI apps |
| □ | AI-Tolerated | Prisma Access | ● Yellow | IT tolerated AI apps |
| □ | AI-Unsanctioned | Prisma Access | ● Red | IT unsanctioned AI apps |

## 2.5 Associate the Application-Tagging Snippet

SCM provides a predefined snippet *Application-Tagging* that you should use for tagging applications. You should associate this snippet with the Prisma Access configuration scope and any other folders that need the application tags.

Activity Insights and AI Access Insights use the tags from this snippet when they display applications and when you use the tagging workflow.

**Caution**

Do not associate the Application-Tagging snippet to the Global configuration scope.

If you tag an ACE App-ID within a snippet that you associate to the Global configuration scope, then all devices within your cloud-managed tenant must have a SaaS Security Inline or AI Access Security license. Without one of those licenses, the configuration push to a device fails.

**Step 1:** Continuing in SCM, navigate to **Configuration > NGFW and Prisma Access**. The Overview page appears.

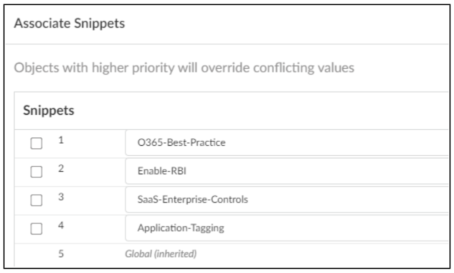
**Step 2:** In the Configuration Scope pane, on the Folders tab, select **Prisma Access.**

**Step 3:** In the Configuration Snippets pane, click the edit cog.

**Step 4:** In the Associate Snippets pane, click the plus sign (+). SCM inserts a new row.

**Step 5:** In the new row box, click the chevron, and in the resulting list, choose **Application-Tagging**, and then click **Close**.

**Step 6:** As needed for an NGFW deployment, repeat this procedure by using the NGFW configuration scope in Step 2 (example: **On-Premises Remote Sites**).



Associate Snippets

Objects with higher priority will override conflicting values

Snippets

| □ | | |
|---|---|---|
| □ | 1 | O365-Best-Practice |
| □ | 2 | Enable-RBI |
| □ | 3 | SaaS-Enterprise-Controls |
| □ | 4 | Application-Tagging |
| | 5 | *Global (inherited)* |

## 2.6 Create Snippets

In this procedure, you create two snippets for policy rules for your AI application security policy. The first is for general AI-application access. The second snippet is optional for policy exceptions when accessing AI applications using explicit proxy without GlobalProtect.

*Table 2 AI Access Policy Snippets*

| Configuration scope snippet | Comment |
|---|---|
| Policy-AI_Access | General policy for AI application access |
| Policy-AI_Access_Proxy | Policy for AI application access when using explicit proxy |

**Step 1:** Continuing in SCM, navigate to **Configuration > NGFW and Prisma Access**.

**Step 2:** In the Configuration Scope pane, on the Snippets tab, click **Add Snippet**. The Create Snippet pane appears.

**Step 3:** In the **Name** box, enter **Policy-AI_Access**.

**Step 4:** In the **Description** box, enter an appropriate description, and then click **Create**.

**Step 5:** For the remaining entries in Table 2, repeat Step 2 through Step 4.

## 2.7 Tag Applications

This method for assigning tags assumes that you know which App-IDs you want to tag. This guide includes an alternative method for assigning tags (Procedure 6.2) that is more suitable when you do not know the App-IDs in advance.

In this procedure, you assign the predefined Sanctioned and Tolerated tags to IT-sanctioned and IT-tolerated App-IDs that your security-policy rules require. IT-unsanctioned App-IDs should remain untagged. You need to apply the tags within the Application-Tagging snippet. By tagging the App-IDs in this snippet, you need to tag the App-ID only once.

> **Note**
>
> Activity Insights and AI Access Insights recognize only the Sanctioned and Tolerated tags. Applications without these tags are assumed to be Unsanctioned.
>
> SCM uses these tags for all applications, not just GenAI applications. Limiting the Insights view to GenAI applications requires that you apply the additional display filter [GenAI application: TRUE].

You should adjust IT-sanctioned and IT-tolerated App-IDs according to your specific business needs.

For a Prisma Access deployment, because you associate the Application-Tagging snippet to the Prisma Access configuration scope, the tags are visible within that scope. For an NGFW deployment, because you associate the snippet with the parent level scope for the NGFW devices, the tags are visible within that scope.

**Caution**

Do not apply the tags to ACE App-IDs at the Global configuration scope.

If you tag an ACE App-ID at the Global configuration scope, then all devices within your cloud-managed tenant must have a SaaS Security Inline or an AI Access Security license. Without one of those licenses, the configuration push to a device fails.

*Table 3 App-ID tags*

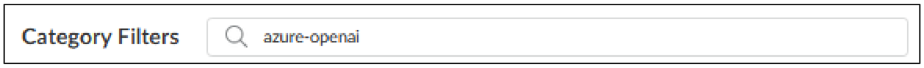
| AI resource | App-IDs | Tag |
|---|---|---|
| Azure OpenAI | azure-openai<br>azure-openai-api<br>azure-openai-encrypted<br>azure-openai-studio | Sanctioned |
| OpenAI ChatGPT | openai-base<br>openai-chatgpt<br>openai-chatgpt-download<br>openai-chatgpt-uploading | Sanctioned |
| Google Gemini | google-gemini<br>google-gemini-delete<br>google-gemini-downloading<br>google-gemini-editing<br>google-gemini-posting<br>google-gemini-uploading<br>google-gemini-models | Tolerated |
| Hugging Face | huggingface-base<br>huggingface-download<br>huggingface-upload | Tolerated |

**Step 1:** Continuing in SCM, navigate to **Configuration > NGFW and Prisma Access**, and then from the **Objects** menu, choose **Application > Applications**.

**Step 2:** In the Configuration Scope pane, on the Snippets tab, select **Application-Tagging**.

**Step 3:** In the Category Filters pane, click **Clear Filters**.

**Step 4:** In the search box, enter the azure-openai, and then press **ENTER**.



Category Filters

azure-openai

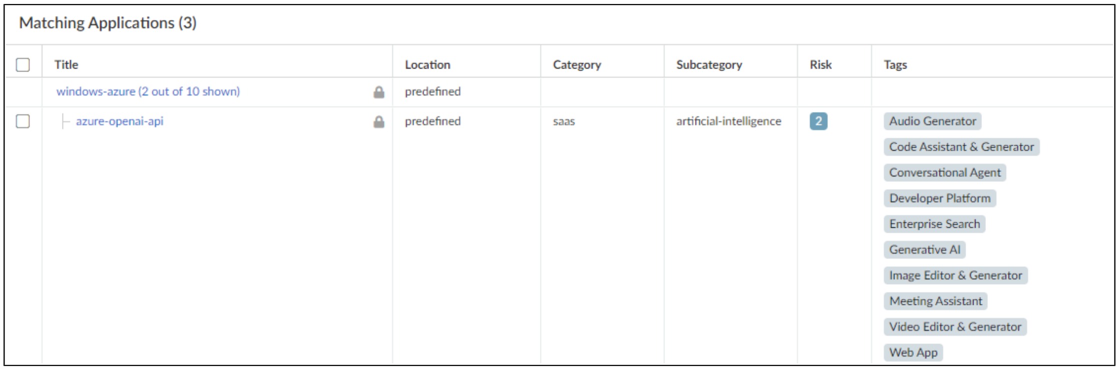
**Note**

When looking for a wider list of related applications, you can search using a less specific string.

**Step 5:** In the Matching Applications pane, select the row for azure-openai-api, and then click **Add/Edit Tag**. The Edit Application Tags pane appears.

**Note**

You can assign tags to only one App-ID at a time.

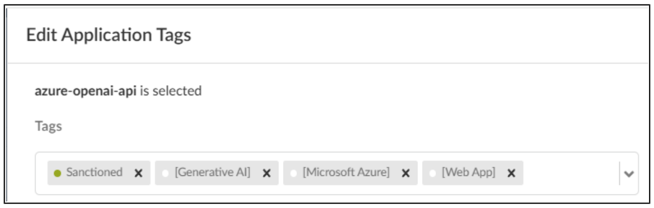


Matching Applications (3)

| □ | Title | Location | Category | Subcategory | Risk | Tags |
|---|---|---|---|---|---|---|
| | windows-azure (2 out of 10 shown) | predefined | | | | |
| □ | ├ azure-openai-api | predefined | saas | artificial-intelligence | 2 | Audio Generator<br>Code Assistant & Generator<br>Conversational Agent<br>Developer Platform<br>Enterprise Search<br>Generative AI<br>Image Editor & Generator<br>Meeting Assistant<br>Video Editor & Generator<br>Web App |

**Step 6:** In the Application Tag dialog box, under Tags, click plus (+).

**Step 7:** In the **Tags** list, search for and select Sanctioned, and then click **Save**.



Edit Application Tags

**azure-openai-api** is selected

Tags

● Sanctioned ✕ [Generative AI] ✕ [Microsoft Azure] ✕ [Web App] ✕

**Step 8:** For each of the remaining App-IDs in Table 3, repeat Step 3 through Step 7.

## 2.8 Configure Application Filters

In this procedure, you configure application filters for the security-policy rules. You configure an application filter for IT-sanctioned and IT-tolerated AI apps by using the predefined tags: Sanctioned, Tolerated, and [Generative AI]. To include additional IT-tolerated AI apps, you create a separate application filter based on the App-ID risk value.

The application filters use tags that you previously applied in the Application-Tagging snippet. This and following procedures assume that this snippet is associated with the required configuration scopes.

**Note**

The application filter does not apply tags to any App-IDs and does not affect the application display for Activity Insights or AI Access Insights.

Any App-ID without an explicit tag of Sanctioned or Tolerated displays as Unsanctioned.

The function of the application filters in Table 4 depends on the order in which they are applied in security-policy rules. To be evaluated properly, the security-policy rules must follow the same ordering as the table.

*Table 4 Application filters*

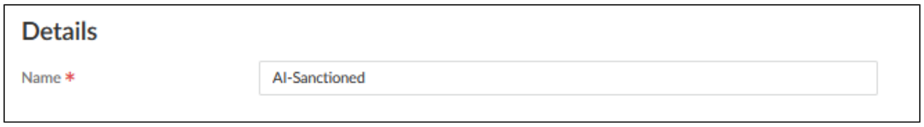
| Application filter | Tag | Risk |
|---|---|---|
| AI-Sanctioned | Sanctioned<br>[Generative AI] | — |
| AI-Tolerated | Tolerated<br>[Generative AI] | — |
| AI-Tolerated-LowRisk | [Generative AI] | 1, 2 (lower relative risk) |
| AI-Unsanctioned | [Generative AI] | — |

**Step 1:** Continuing in SCM, navigate to **Configuration > NGFW and Prisma Access**.

**Step 2:** In the Configuration Scope pane, on the Folders tab, choose **Global**, and then, from the **Objects** menu, choose **Application > Application Filters**.

**Step 3:** In the Applications Filters pane, click **Add Application Filter**.

**Step 4:** In the Details pane, in the **Name** box, enter **AI-Sanctioned**.



Details

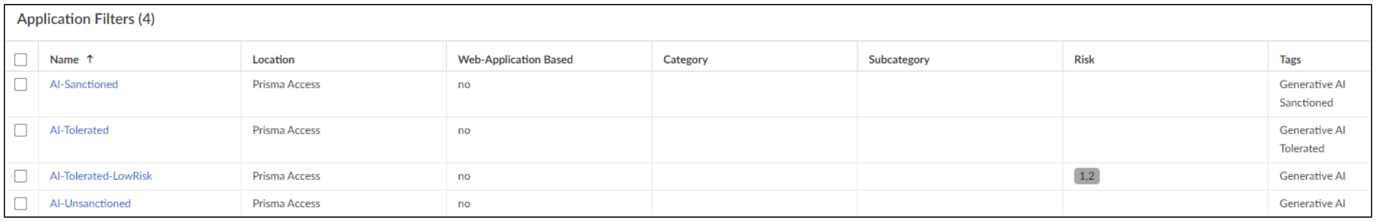
Name * AI-Sanctioned

**Step 5:** If the application filter is tag based, in the Category Filters pane, in the Tags column, click **Sanctioned** and **[Generative AI]**, and then click **Save**.

**Step 6:** If the application filter is risk based, in the Risk column, click the risk values specified in Table 4 (example: **1** and **2**), and then click **Save**.

**Step 7:** For each of the application filters in Table 4, repeat Step 3 through Step 6

**Step 8:** Verify all application filters and corresponding tags.



Application Filters (4)

| ☐ | Name ↑ | Location | Web-Application Based | Category | Subcategory | Risk | Tags |
|---|---|---|---|---|---|---|---|
| ☐ | AI-Sanctioned | Prisma Access | no | | | | Generative AI<br>Sanctioned |
| ☐ | AI-Tolerated | Prisma Access | no | | | | Generative AI<br>Tolerated |
| ☐ | AI-Tolerated-LowRisk | Prisma Access | no | | | 1,2 | Generative AI |
| ☐ | AI-Unsanctioned | Prisma Access | no | | | | Generative AI |

## 2.9 Push Configuration Updates to Prisma Access and On-Premises NGFWs

Next, you enable all the objects you configured during this group of procedures.

**Step 1:** Continuing in SCM, navigate to **Configuration > Push Config**.

**Step 2:** Select **Mobile Users Container**, **Remote Networks**, and On-Premises Remote Sites and then click **Push**.

Note

For this and subsequent procedures, if you are deploying only mobile users or remote networks in Prisma Access or on-premises NGFWs, you push the configuration for the connection types in use.

**Step 3:** Click **Push Config**, and then choose **Push**.

**Step 4:** In the Push dialog box, in the **Description** box, enter a description and then click **Push**.

**Step 5:** In the Jobs dialog box, when the push job result changes to OK, click **Done**.

## Procedures

### Configuring NGFWs to Control Access to SaaS Applications

3.1 Add Service Route

3.2 Update Application Group for Identity Redistribution

3.3 Create a Service for TCP Port 5007

3.4 Add Security-Policy Rule for User-ID Agent SSL

3.5 Configure Identity Redistribution

These procedures include the additional configuration elements required for NGFWs to control access to AI applications by propagating User-ID information from the Prisma Access to the NGFWs.

These procedures assume that you have configured your user devices to use the GlobalProtect app to connect to Prisma Access when they are remote. You have also configured the GlobalProtect app settings profile for branch users to use an existing GlobalProtect internal gateway hosted in the public cloud. The configuration details for the internal gateway are beyond the scope of this guide.

## 3.1 Add Service Route

For your remote-site devices to use their dataplane interfaces across a public network in order to access a User-ID redistribution device such as a GlobalProtect internal gateway, you must add the service route for uid-agent.

**Step 1:** In SCM, navigate to **Configuration > NGFW and Prisma Access**, and then from the **Device Settings** menu, choose **Device Setup**.

**Step 2:** In the Configuration Scope pane, on the Folders tab, choose **Remote Site L2**.

**Step 3:** In the Service Route Settings pane, click **Customize Service Route**.

**Step 4:** In the Service Route Settings pane, select **Customize**.

**Step 5:** On the IPv4 tab, in the Service column, click **uid-agent (UID agent(s))**. The Service Route Settings pane appears.

**Step 6:** In the **Source Interface** list, choose $**LOOPBACK1** (loopback.**1**).

**Step 7:** In the **Source Address** list, choose **100.64.0.255/32**, click **Update** and then click **Save**.

## 3.2 Update Application Group for Identity Redistribution

The previously configured application group, **DevMgmt-PaloAlto**, does not include the paloalto-userid-agent App-ID. To access a User-ID redistribution device such as a GlobalProtect internal gateway, you must update the existing application group to include the App-ID.

**Step 1:** Continuing in SCM, navigate to **Configuration > NGFW and Prisma Access**, and then from the **Objects** menu, choose **Application > Application Groups**.

**Step 2:** In the Configuration Scope pane, select **Remote Site L2**.

**Step 3:** In the Application Groups pane, click **DevMgmt-PaloAlto**.

**Step 4:** In the **Application** list, open the list by clicking the chevron.

**Step 5:** On the Application tab, search for and select **paloalto-userid-agent**, and then click **Save**.

**Step 6:** As needed, repeat this procedure, using the **Remote Site L2 HA** configuration scope in Step 2.

## 3.3 Create a Service for TCP Port 5007

To ensure your policy always permits User-ID agent traffic between the remote-site NGFW and hosted internal gateway, first you create an additional service.

**Step 1:** Continuing in SCM, navigate to **Configuration > NGFW and Prisma Access**, and then from the **Objects** menu, choose **Service > Services**.

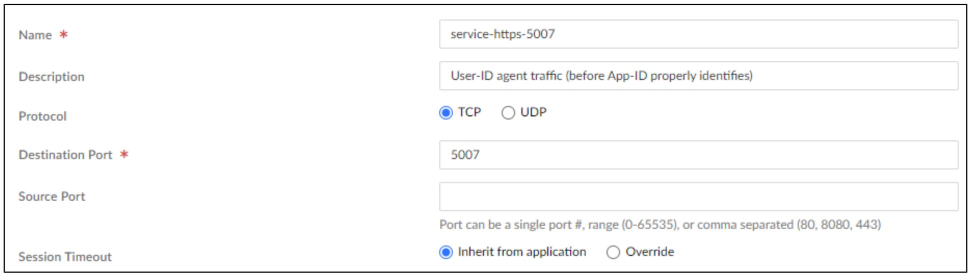
**Step 2:** In the Configuration Scope pane, on the Folders tab, select **On-Premises Remote Sites**.

**Step 3:** Click **Add Service**.

**Step 4:** In the **Name** box, enter service-https-5007.

**Step 5:** In the **Description** box, enter a valid description.

**Step 6:** In the **Destination Port** box, enter 5007, and then click **OK**.



| | |
|---|---|
| Name * | service-https-5007 |
| Description | User-ID agent traffic (before App-ID properly identifies) |
| Protocol | ● TCP ○ UDP |
| Destination Port * | 5007 |
| Source Port | <br>Port can be a single port #, range (0-65535), or comma separated (80, 8080, 443) |
| Session Timeout | ● Inherit from application ○ Override |

## 3.4 Add Security-Policy Rule for User-ID Agent SSL

To ensure your policy always permits User-ID agent traffic between the remote-site NGFW and hosted internal gateway, you create an additional policy rule that allows traffic to the hosted internal gateway before the device identifies the traffic by using App-ID. This rule is rarely matched, but it is useful in certain situations. This rule supports an SSL connection to the hosted internal gateway over TCP port 5007.

When you create the service in the On-Premises Remote Sites scope, both the Remote Site L2 scope and Remote Site L2 HA scope inherit the service.

You have two options: standard and HA remote-file firewalls. If you have both firewall types, perform both options.

### Option 1: Standard Remote-Site Firewalls

**Step 1:** Continuing in SCM, navigate to **Configuration > NGFW and Prisma Access**, and then from the **Security Services** menu, choose **Security Policy**.

**Step 2:** In the Configuration Scope pane, on the Folders tab, select Remote Site L2.

**Step 3:** In the Security Policy Rules pane, click **Add Rule,** and then choose **Pre Rule > Security Rule**.

**Step 4:** In the **Name** box, enter DevMgmt-SSL_5007.

**Step 5:** In the Source pane, for Zones, select **Select**.

**Step 6:** In the **Zones** list, choose zone-internal-MGMT.

**Step 7:** For Addresses, select **Select**.

**Step 8:** In the **Addresses** list, on the Address tab, select ServiceRoute-Loopback.

**Step 9:** In the Destination pane, for Zones, select **Select**.

**Step 10:** In the **Zones** list, choose zone-public.

**Step 11:** In the Applications/Service pane, for Application, select **Select**.

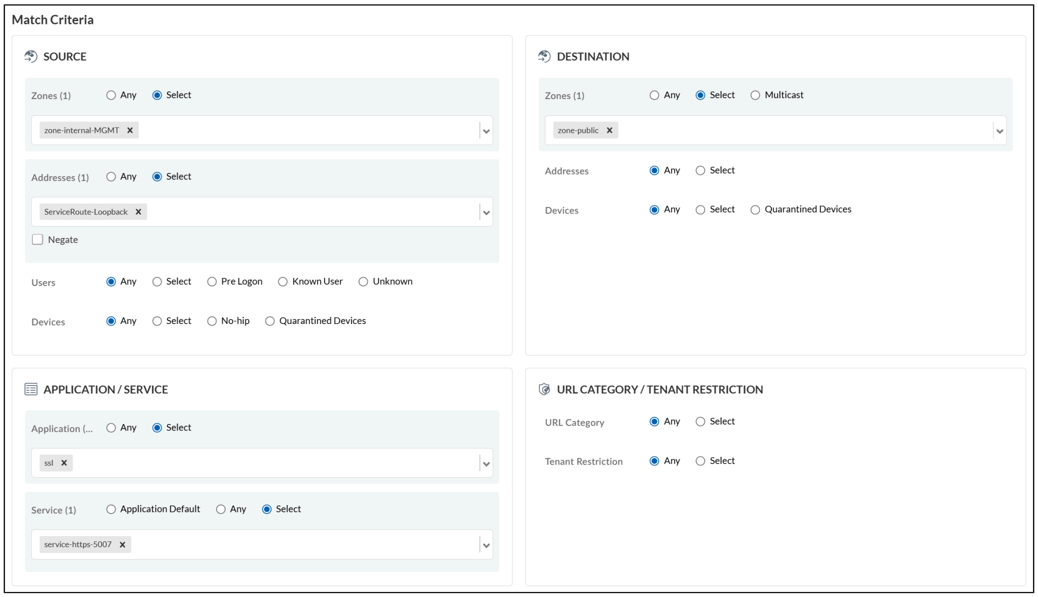
**Step 12:** In the **Application** list, on the Applications tab, search for and select ssl.

**Step 13:** For Service, select **Select**,

**Step 14:** In the **Service** list, on the Services tab, select service-https-5007.

**Step 15:** In the Actions pane, in the **Action** list, choose **Allow.**

**Step 16:** In the **Profile Group** list, choose best-practice-NO_URL, and then click **Save**.



Match Criteria

SOURCE

Zones (1) ○ Any ● Select

zone-internal-MGMT ✕

Addresses (1) ○ Any ● Select

ServiceRoute-Loopback ✕

□ Negate

Users ● Any ○ Select ○ Pre Logon ○ Known User ○ Unknown

Devices ● Any ○ Select ○ No-hip ○ Quarantined Devices

DESTINATION

Zones (1) ○ Any ● Select ○ Multicast

zone-public ✕

Addresses ● Any ○ Select

Devices ● Any ○ Select ○ Quarantined Devices

APPLICATION / SERVICE

Application (... ○ Any ● Select

ssl ✕

Service (1) ○ Application Default ○ Any ● Select

service-https-5007 ✕

URL CATEGORY / TENANT RESTRICTION

URL Category ● Any ○ Select

Tenant Restriction ● Any ○ Select

When you create a new rule, SCM places the new rule at the bottom of the rule list. You must move this rule so that it follows the existing security-policy rule DevMgmt-SSL_3978 that you created in **Securing the Branch with On-Premises Network Security and Strata Cloud Manager: Deployment Guide**.

**Step 17:** On the Security Policy page, select the row for DevMgmt-SSL_5007.

**Step 18:** Click **Move**, and then choose **Move Up**.

**Step 19:** Until the rule is properly located, repeat Step 19.

## Option 2: HA Remote-Site Firewalls

**Step 1:** Continuing in SCM, navigate to **Configuration > NGFW and Prisma Access**, and then from the **Security Services** menu, choose **Security Policy**.

**Step 2:** In the Configuration Scope pane, on the Folders tab, choose Remote Site L2 HA.

**Step 3:** In the Security Policy Rules pane, click **Add Rule,** and then choose **Pre Rule > Security Rule**.

**Step 4:** In the **Name** box, enter DevMgmt-SSL_5007.

**Step 5:** In the Source pane, for Zones, select **Select**.

**Step 6:** In the **Zones** list, choose **zone-private.**

**Step 7:** For Addresses, select **Select**.

**Step 8:** In the **Addresses** list, on the Address Group tab, select **DevMgmt-Firewalls**.

**Step 9:** In the Destination pane, for Zones, select **Select**.

**Step 10:** In the **Zones** list, choose **zone-public**.

**Step 11:** On the Applications/Service pane, for Application, select **Select**.

**Step 12:** In the **Application** list, on the Applications tab, search for and select **ssl**.

**Step 13:** For Service, select **Select**,

**Step 14:** In the **Service** list, on the Services tab, select **service-https-5007**.

**Step 15:** In the Actions pane, in the Action list, choose **Allow**.

**Step 16:** In the **Profile Group** list, choose **best-practice-NO_URL**, and then click **Save**

When you create a new rule, SCM places the new rule at the bottom of the rule list. You must move this rule so that it follows the existing security-policy rule **DevMgmt-SSL_3978** that you created in **Securing the Branch with On-Premises Network Security and Strata Cloud Manager: Deployment Guide**.

**Step 17:** On the Security Policy page, select the row for **DevMgmt-SSL_5007**.

**Step 18:** Click **Move**, and then choose **Move Up**.

**Step 19:** Until the rule is properly located, repeat Step 18.

## 3.5 Configure Identity Redistribution

This procedure assumes that you have deployed an NGFW in the public cloud and configured it as a GlobalProtect internal gateway using the same authentication method as your Prisma Access deployment.

You also configure data redistribution on the internal gateway so that your on-premises NGFWs can connect to it to download User-ID information.

**Step 1:** Continuing in SCM, navigate to **Configuration > NGFW and Prisma Access**, and then from the **Identity Services** menu, choose **Identity Redistribution**.

**Step 2:** In the Configuration Scope pane, on the Folders tab, choose **On-Premises Remote Sites**.

**Step 3:** Click **Add Agent**.

**Step 4:** In the **Name** box, enter **Hosted Internal Gateway**.

**Step 5:** In the **Host** box, enter **4.255.198.41**.

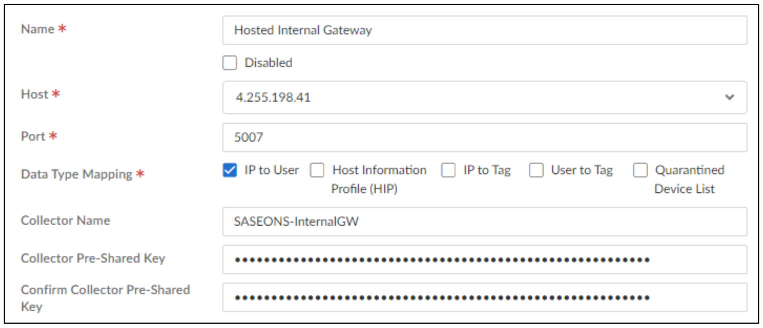
**Step 6:** In the **Port** box, enter **5007**.

**Step 7:** In the **Data Type Mapping** section, select **IP to User**.

**Step 8:** In the **Collector Name** box, enter SASE-ONS-InternalGW.

**Step 9:** In the **Collector Pre-Shared Key** box, enter the passphrase.

**Step 10:** In the **Confirm Collector Pre-Shared Key** box, re-enter the passphrase.



| | |
|---|---|
| Name * | Hosted Internal Gateway |
| | □ Disabled |
| Host * | 4.255.198.41 |
| Port * | 5007 |
| Data Type Mapping * | ☑ IP to User □ Host Information Profile (HIP) □ IP to Tag □ User to Tag □ Quarantined Device List |
| Collector Name | SASEONS-InternalGW |
| Collector Pre-Shared Key | •••••••••••••••••••••••••••••••••••••••••••••••••••••• |
| Confirm Collector Pre-Shared Key | •••••••••••••••••••••••••••••••••••••••••••••••••••••• |

**Step 11:** Click **Save**.

## Procedures

### Configure Security Profile Groups with Custom URL Access Management and DLP Profiles

4.1 Create and Modify the URL Access Management Profile

4.2 Configure Data Loss Prevention Data Profile

4.3 Configure User Coaching for the Access Experience Endpoint Agent

4.4 Update the GlobalProtect App Settings Profile and Enable Access Experience

4.5 Create and Modify the Security Profile Groups

Before you configure the security profile groups that you will associate with your security-policy rules, you need to create a new URL access management profile and a new DLP data profile.

The default best-practice profile group includes the best-practice URL access management profile and does not include a DLP data profile. To integrate the URL access management profile and DLP data profile, you create new security profile groups that you will associate with security-policy rules later in this guide.

## 4.1 Create and Modify the URL Access Management Profile

The default best-practice URL access management profile has the Site Access action for the artificial-intelligence URL category set to *allow*. To ensure that the traffic logs and URL logs display this category rather than other URL categories (if there are multiple categories assigned for the URL), you change this value to *alert*.

You cannot edit the default best-practice URL access management profile. To make a modification, you must clone the default profile and then modify the clone. By creating the clone in the Global configuration scope, you can reference the clone in any child configuration scope.

**Step 1:** In SCM, navigate to **Configuration > NGFW and Prisma Access**, and then, from the **Security Services** menu, choose **URL Access Management**.

**Step 2:** In the Configuration Scope pane, on the Folders tab, choose **Global**.

**Step 3:** In the URL Access Management Profile pane, select **best-practice**, click **Clone,** and then click **Clone** again.

SCM creates a clone named best-practice-1.

**Step 4:** Click **best-practice-1**.

**Step 5:** In the **Name** box, enter **best-practice-ai**.

**Step 6:** In the Access Control pane, select the row for **AI (artificial-intelligence)**.

**Step 7:** Click **Set Access**, and then choose **Alert**.

**Step 8:** Click **Set Submission**, choose **Alert**, and then click **Save**.

## 4.2 Configure Data Loss Prevention Data Profile

The default DLP data profiles only match sensitive data contained in files. You can enable matching of sensitive data for non-file-based communications, such as an AI chatbot.

If you want to create a DLP data profile that includes multiple data categories, you must create a nested data profile. Although, you cannot edit the built-in DLP data profiles that Prisma Access includes, you can edit the default policy of the nest data profile that contains included profiles.

In this example, you create a DLP policy to monitor non-file-based communications that include sensitive data matched by the PII and Sensitive Content built-in DLP data profiles.

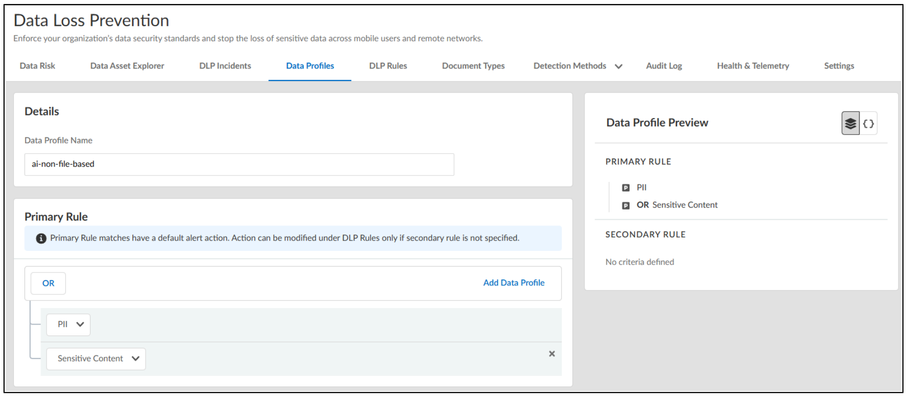
**Step 1:** Continuing in SCM, navigate to **Configuration > Data Loss Prevention**.

**Step 2:** On the Data Profile tab, click **Add Data Profile**, and then click **With Nested Data Profiles**.

**Step 3:** In the **Data Profile Name** box, enter **ai-non-file-based**.

**Step 4:** In the Primary Rule pane, in the **Add Data Profile** list, choose **PII**.

**Step 5:** In the Primary Rule pane, click **Add Data Profile**, and then in the **Add Data Profile** list, choose Sensitive Content, and then click **Save**.



Data Loss Prevention

Enforce your organization's data security standards and stop the loss of sensitive data across mobile users and remote networks.

Details

Data Profile Name: ai-non-file-based

Primary Rule

Primary Rule matches have a default alert action. Action can be modified under DLP Rules only if secondary rule is not specified.

PII

Sensitive Content

Data Profile Preview

PRIMARY RULE

PII

OR Sensitive Content

SECONDARY RULE

No criteria defined

Next, you modify the DLP rules to include non-file-based communications.

**Step 6:** On the DLP Rules tab, in the row for ai-non-file-based, in the Action column, click the three-dot menu, and then choose **Edit**.

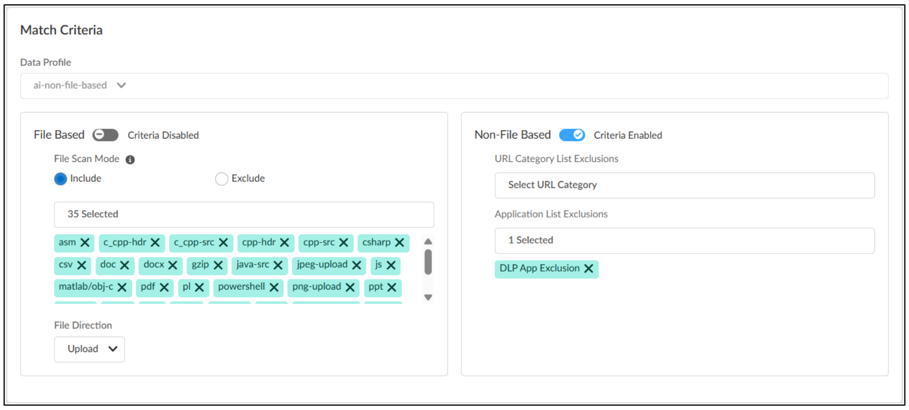
**Step 7:** In the Match Criteria pane, disable **File Based**.

**Step 8:** Enable **Non-File Based**.

> **Note**
>
> In this example, you configure a Block action that SCM logs with a Medium severity. For your organization, choose the appropriate action and severity according to your security policy.

**Step 9:** In the Action & Log pane, in the **Action** list, choose **Block**.

**Step 10:** In the **Log Severity** list, choose **Medium**, and then click **Save**.



Match Criteria

Data Profile: ai-non-file-based

File Based — Criteria Disabled

File Scan Mode

● Include ○ Exclude

35 Selected

asm ✕ c_cpp-hdr ✕ c_cpp-src ✕ cpp-hdr ✕ cpp-src ✕ csharp ✕ csv ✕ doc ✕ docx ✕ gzip ✕ java-src ✕ jpeg-upload ✕ js ✕ matlab/obj-c ✕ pdf ✕ pl ✕ powershell ✕ png-upload ✕ ppt ✕

File Direction: Upload

Non-File Based — Criteria Enabled

URL Category List Exclusions: Select URL Category

Application List Exclusions: 1 Selected

DLP App Exclusion ✕

## 4.3 Configure User Coaching for the Access Experience Endpoint Agent

When using DLP, you might wish to provide additional feedback to the end user when activity matches a DLP rule with a block action.

DLP can send notifications to Windows and macOS users with the Access Experience endpoint agent. To customize the notifications, you use User Coaching Notification Templates.

**Step 1:** Continuing in SCM, navigate to **Configuration > NGFW and Prisma Access**.

**Step 2:** In the Configuration Scope pane, on the Folders tab, choose **Global**.

**Step 3:** On the Setup tab, in the User Coaching Notification Templates pane, click the edit cog.

**Step 4:** Click **Add Notification Template**.

**Step 5:** In the **Notification Template Name** box, enter **AI non-file based**.

**Step 6:** In the **Description** box, enter **User notification for ai-non-file-based DLP rule**.

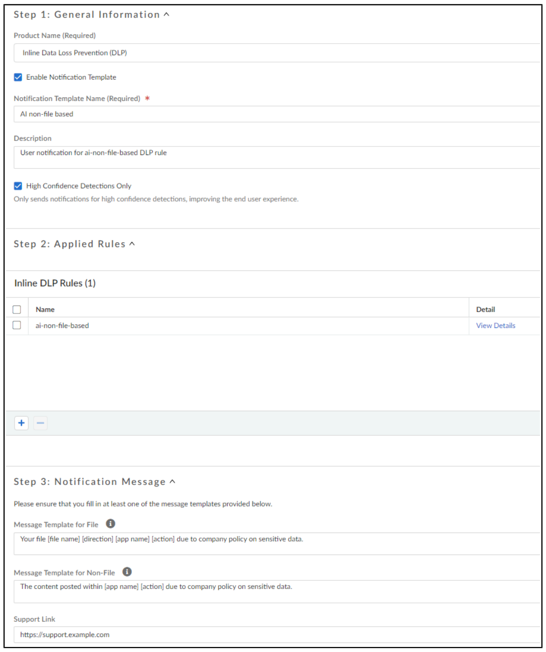
**Step 7:** Select **High Confidence Detections Only**.

**Step 8:** Expand **Step 2: Applied Rules**, and then, in the Inline DLP Rules pane, click the plus sign (+)

**Step 9:** In the new row, in the Name column, click the chevron, and in the resulting list, choose **ai-non-file-based**.

**Step 10:** Expand **Step 3: Notification Message** section.

**Step 11:** In the **Support Link** box, enter a link to a web site that provides additional information, and then click **Save**.



Step 1: General Information ^

Product Name (Required)

Inline Data Loss Prevention (DLP)

☑ Enable Notification Template

Notification Template Name (Required) *

AI non-file based

Description

User notification for ai-non-file-based DLP rule

☑ High Confidence Detections Only

Only sends notifications for high confidence detections, improving the end user experience.

Step 2: Applied Rules ^

Inline DLP Rules (1)

| □ | Name | Detail |
|---|---|---|
| □ | ai-non-file-based | View Details |

Step 3: Notification Message ^

Please ensure that you fill in at least one of the message templates provided below.

Message Template for File

Your file [file name] [direction] [app name] [action] due to company policy on sensitive data.

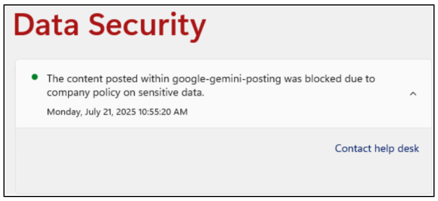
Message Template for Non-File

The content posted within [app name] [action] due to company policy on sensitive data.

Support Link

https://support.example.com

On an Access Experience endpoint agent notification, a user can access the site specified in the support link box by clicking Contact Help Desk.



Data Security

- The content posted within google-gemini-posting was blocked due to company policy on sensitive data.

Monday, July 21, 2025 10:55:20 AM

Contact help desk

## 4.4 Update the GlobalProtect App Settings Profile and Enable Access Experience

In this procedure, you modify the existing GlobalProtect app settings profile, specifically for the Windows and macOS clients that run the Access Experience User Agent . This procedure assumes that you have previously configured this as described in **AI-Powered Autonomous Digital Experience Management: Solution Guide** and that you have deployed GlobalProtect as described in **Securing Internet for Mobile Users by Using Tunnel Mode: Design Guide**.

**Step 1:** Continuing in SCM, navigate to **Configuration > NGFW and Prisma Access**.

**Step 2:** In the Configuration Scope pane, on the Folders tab, choose **GlobalProtect**.

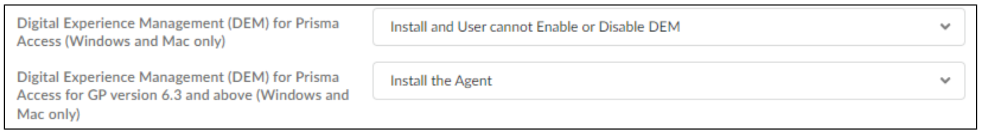
**Step 3:** On the Overview page, in the Prisma Access Infrastructure Setup pane, click **GlobalProtect**.

**Step 4:** On the GlobalProtect App tab, in the App Settings pane, click **GP Full Tunnel**.

**Step 5:** In the App Configuration pane, click **Show Advanced Options**, and then expand **User Behavior**.

**Step 6:** In the **Digital Experience Management (DEM) for Prisma Access for GP version 6.3 and above (Windows and Mac only)** list, choose **Install the Agent**.

**Step 7:** Customize any other GlobalProtect app settings per your requirements, and then click **Save**.



| | |
|---|---|
| Digital Experience Management (DEM) for Prisma Access (Windows and Mac only) | Install and User cannot Enable or Disable DEM |
| Digital Experience Management (DEM) for Prisma Access for GP version 6.3 and above (Windows and Mac only) | Install the Agent |

## 4.5 Create and Modify the Security Profile Groups

You cannot edit the default best-practice security profile group. To make modifications, you must clone the default profile and then modify the clones. By creating the clones in the Global configuration scope, you can reference the clones in any child configuration scope.

You will create two security profile groups. For IT-sanctioned AI applications, you apply a URL access management profile that has an alert action. For IT-tolerated AI applications, you apply a URL access management profile that has an alert action and a DLP profile to prevent the copy/paste upload/download of PII and other sensitive data.

*Table 5  Security profile groups for IT-sanctioned and IT-tolerated applications*

| Profile group | URL access management profile | DLP profile | Comments |
|---|---|---|---|
| best-practice-ai | best-practice-ai | — | Used for IT-sanctioned AI applications. |
| best-practice-ai-dlp | best-practice-ai | ai-non-file-based | Used for IT-tolerated AI applications. |

**Step 1:** Continuing in SCM, navigate to **Configuration > NGFW and Prisma Access** and from the **Security Services** menu, choose **Profile Groups**.

**Step 2:** In the Configuration Scope pane, on the Folders tab, choose **Global.**

**Step 3:** In the Profile Groups pane, select **best-practice**, click **Clone**, and then click **Clone** again.

SCM creates a clone named best-practice-1.

**Step 4:** Click **best-practice-1**.

**Step 5:** In the **Name** box, enter best-practice-ai.

**Step 6:** In the **URL Access Manage Profile** list, choose best-practice-ai, and then click **Save**.

**Step 7:** In the Profile Groups pane, select **best-practice**, click **Clone**, and then click **Clone** again.

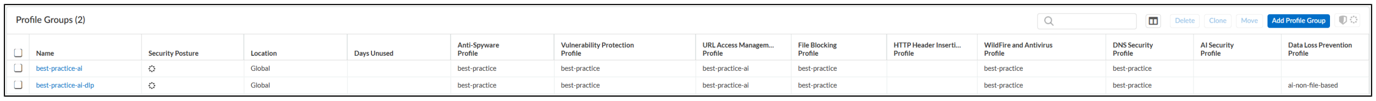
SCM creates a clone named best-practice-1.

**Step 8:** Click **best-practice-1**.

**Step 9:** In the **Name** box, enter best-practice-ai-dlp.

**Step 10:** In the **URL Access Manage Profile** list, choose best-practice-ai.

**Step 11:** In the **Data Loss Prevention Profile** list, choose ai-non-file-based, and then click **Save**.



| □ | Name | Security Posture | Location | Days Unused | Anti-Spyware Profile | Vulnerability Protection Profile | URL Access Managem... Profile | File Blocking Profile | HTTP Header Inserti... Profile | WildFire and Antivirus Profile | DNS Security Profile | AI Security Profile | Data Loss Prevention Profile |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| □ | best-practice-ai | ○ | Global | | best-practice | best-practice | best-practice-ai | best-practice | | best-practice | best-practice | | |
| □ | best-practice-ai-dlp | ○ | Global | | best-practice | best-practice | best-practice-ai | best-practice | | best-practice | best-practice | | ai-non-file-based |

**Procedures**

## Configuring Security Policy Rules to Control Access to AI Applications

5.1 Allow IT-Sanctioned AI Applications for Authorized Users

5.2 Allow IT-Tolerated AI Applications for Authorized Users

5.3 Block Access to Sanctioned and Tolerated AI Applications for Unauthorized Users

5.4 Block Access to Unsanctioned AI Applications for All Users

5.5 Associate Snippet with Prisma Access and NGFW folders

5.6 Adjust Policy Order

5.7 Push Configuration Updates to Prisma Access and On-Premises NGFWs

Next, you configure the set of pre-rules that you use to control access to sanctioned, tolerated, and unsanctioned AI applications for authorized users.

The set of rules you configure in Procedure 5.1 through Procedure 5.4 controls access for mobile users that connect to Prisma Access using the GlobalProtect App in tunnel mode or proxy mode and for branch users that connect to Prisma Access using a remote-network connection.

If you have mobile users that connect to Prisma Access using traditional explicit proxy mode (non-GP-app-based), you also need to add an additional set of rules later in this guide, by completing Procedure 7.1 through Procedure 7.4.

## 5.1 Allow IT-Sanctioned AI Applications for Authorized Users

This security-policy rule allows IT-sanctioned AI applications for users in the specified Entra ID group. The sanctioned AI applications are those that are explicitly tagged with [Generative AI] and Sanctioned. You should customize your list to allow the sanctioned AI applications your organization needs.

This rule is highly specific, and you should insert it above more general rules that should logically follow.

**Note**

Monitoring the Activity Insights and SLS traffic logs for specific corporate endpoints helps you determine the App-IDs of traffic in your environment.

**Step 1:** In SCM, navigate to **Configuration > NGFW and Prisma Access** and then, from the **Security Services** menu, choose **Security Policy**.

**Step 2:** In the Configuration Scope pane, on the Snippets tab, select **Policy-AI_Access**.

**Step 3:** In the Security Policy Rules pane, click **Add Rule**, and then choose **Security Rule**.

**Step 4:** In the **Name** box, enter IT Sanctioned AI Apps.

**Step 5:** In the **Description** box, enter IT sanctioned - no DLP, match both group and filter.

**Step 6:** For Tag, click the plus sign (+), and then choose AI-Sanctioned.

**Step 7:** In the Source pane, for Zones, select **Any**.

**Step 8:** For Addresses, select **Any**.

**Step 9:** For Users, select **Select**.

**Step 10:** In the **Users** list, on the User Groups tab, search for and select ai-access-permitted.

**Step 11:** In the Application/Service pane, for Application, select **Select.**

**Step 12:** In the **Application** list, on the Applications Filters tab, select AI-Sanctioned.

**Step 13:** In the Destination pane, for Zones, select **Select**.

**Step 14:** In the **Zones** list, select the public zone variable (example: $ZONE-PUBLIC).

**Step 15:** For Addresses, select **Any**.

**Step 16:** In the Action pane, in the **Action** list, choose **Allow**.

**Step 17:** In the **Profile Group** list, choose best-practice-ai, and then click **Save**.

## 5.2 Allow IT-Tolerated AI Applications for Authorized Users

This security-policy rule allows IT-tolerated AI applications for users in the specified Entra ID group. The tolerated AI applications are either those that are explicitly tagged with [Generative AI] and Tolerated and or those tagged with [Generative AI] and a risk value of 1 or 2. You should customize your list to allow the tolerated applications your organization needs.

> **Note**
>
> Monitoring the Activity Insights and SLS traffic logs for specific corporate endpoints helps you determine the App-IDs of traffic in your environment.

This rule is highly specific, and it should immediately follow the rule you created in Procedure 5.1.

**Step 1:** Continuing in SCM, navigate to **Configuration > NGFW and Prisma Access**, and then, from the **Security Services** menu, choose **Security Policy**.

**Step 2:** In the Configuration Scope pane, on the Snippets tab, select Policy-AI_Access.

**Step 3:** In the Security Policy Rules pane, click **Add Rule**, and then choose **Security Rule**.

**Step 4:** In the **Name** box, enter IT Tolerated AI Apps.

**Step 5:** In the **Description** box, enter IT tolerated - requires DLP, match both group and filter.

**Step 6:** For Tag, click the plus sign (+), and then choose AI-Tolerated.

**Step 7:** In the Source pane, for Zones, select **Any**.

**Step 8:** For Addresses, select **Any**.

**Step 9:** For Users, select **Select**.

**Step 10:** In the **Users** list, on the User Groups tab, search for and select ai-access-permitted.

**Step 11:** In the Application/Service pane, for Application, select **Select.**

**Step 12:** In the **Application** list, on the Applications Filters tab, select AI-Tolerated and AI-Tolerated-LowRisk.

**Step 13:** In the Destination pane, for Zones, select **Select**.

**Step 14:** In the **Zones** list, choose the public zone variable (example: $ZONE-PUBLIC).

**Step 15:** For Addresses, select **Any**.

**Step 16:** In the Action pane, in the **Action** list, choose **Allow**.

**Step 17:** In the **Profile Group** list, choose best-practice-ai-dlp, and then click **Save**.

## 5.3 Block Access to Sanctioned and Tolerated AI Applications for Unauthorized Users

This security-policy rule blocks access to both IT-sanctioned AI applications and IT-tolerated AI applications for unauthorized users (any non-members of the active-directory group used in Procedure 5.1 and Procedure 5.2)

This rule is highly specific, and it should immediately follow the rule you created in Procedure 5.2.

**Step 1:** Continuing in SCM, navigate to **Configuration > NGFW and Prisma Access**, and then, from the **Security Services** menu, choose **Security Policy**.

**Step 2:** In the Configuration Scope pane, on the Snippets tab, select Policy-AI_Access.

**Step 3:** In the Security Policy Rules pane, click **Add Rule**, and then choose **Security Rule**.

**Step 4:** In the **Name** box, enter IT Sanctioned and Tolerated AI Apps - Block Unauthorized Users.

**Step 5:** In the **Description** box, enter Block access to Sanctioned and Tolerated, match filters.

**Step 6:** For Tags, click the plus sign (+), and then choose AI-Sanctioned.

**Step 7:** Click the plus (+) again, and then choose AI-Tolerated.

**Step 8:** In the Source pane, for Zones, select **Any**.

**Step 9:** For Addresses, select **Any**.

**Step 10:** In the Application/Service pane, for Application, select **Select.**

**Step 11:** In the **Application** list, on the Applications Filters tab, select AI-Sanctioned, AI-Tolerated, and AI-Tolerated-LowRisk.

**Step 12:** In the Destination pane, for Zones, select **Select**.

**Step 13:** In the **Zones** list, choose the public zone variable (example: $ZONE-PUBLIC).

**Step 14:** For Addresses, select **Any**.

**Step 15:** In the Actions pane, in the **Action** list, choose **Deny**.

**Step 16:** In the **Profile Group** list, choose **best-practice**, and then click **Save**.

## 5.4 Block Access to Unsanctioned AI Applications for All Users

This security-policy rule blocks access to IT-unsanctioned AI applications for all users.

This rule is highly specific, and it should immediately follow the rule you created in Procedure 5.3.

**Step 1:** Continuing in SCM, navigate to **Configuration > NGFW and Prisma Access**, and then, from the **Security Services** menu, choose **Security Policy**.

**Step 2:** In the Configuration Scope pane, on the Snippets tab, select **Policy-AI_Access**.

**Step 3:** In the Security Policy Rules pane, click **Add Rule**, and then choose **Security Rule**.

**Step 4:** In the **Name** box, enter **IT Unsanctioned AI Apps**.

**Step 5:** In the **Description** box, enter **Block access to Unsanctioned, match filters**.

**Step 6:** For Tags, click the plus sign (+), and then choose **AI-Unsanctioned**.

**Step 7:** In the Source pane, for Zones, select **Any**.

**Step 8:** For Addresses, select **Any**.

**Step 9:** In the Application/Service pane, for Application, select **Select**.

**Step 10:** In the **Applications** list, on the Applications Filters tab, select **AI-Unsanctioned**.

**Step 11:** In the Destination pane, for Zones, select **Select**.

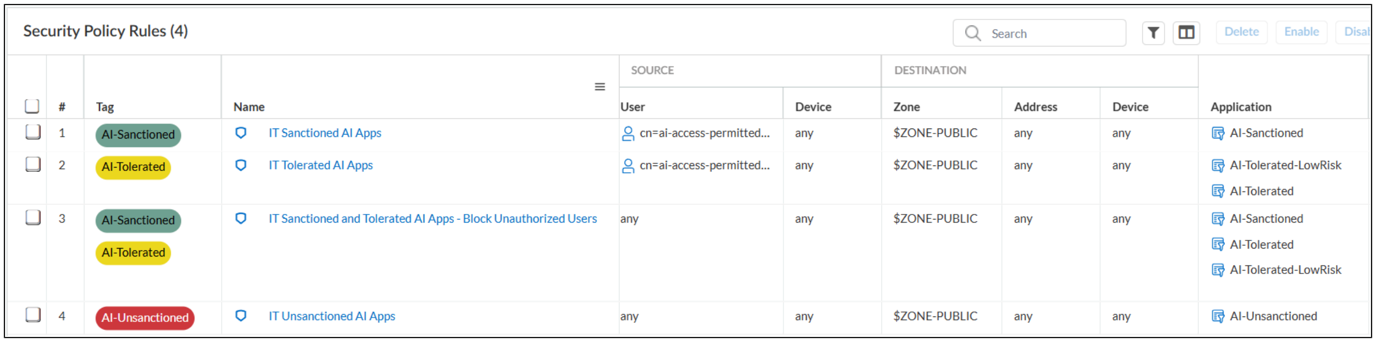
**Step 12:** In the **Zones** list, choose the public zone variable (example: $ZONE-PUBLIC).

**Step 13:** For Addresses, select **Any**.

**Step 14:** In the Actions pane, in the **Action** list, choose **Deny**.

**Step 15:** In the **Profile Group** list, choose **best-practice**, and then click **Save**.

**Step 16:** Verify that you have inserted the security-policy rules from Procedure 5.1 through Procedure 5.4 in the specified order.



|  |  |  |  | SOURCE |  | DESTINATION |  |  |  |
|---|---|---|---|---|---|---|---|---|---|
| ☐ | # | Tag | Name | User | Device | Zone | Address | Device | Application |
| ☐ | 1 | AI-Sanctioned | IT Sanctioned AI Apps | cn=ai-access-permitted... | any | $ZONE-PUBLIC | any | any | AI-Sanctioned |
| ☐ | 2 | AI-Tolerated | IT Tolerated AI Apps | cn=ai-access-permitted... | any | $ZONE-PUBLIC | any | any | AI-Tolerated-LowRisk<br>AI-Tolerated |
| ☐ | 3 | AI-Sanctioned<br>AI-Tolerated | IT Sanctioned and Tolerated AI Apps - Block Unauthorized Users | any | any | $ZONE-PUBLIC | any | any | AI-Sanctioned<br>AI-Tolerated<br>AI-Tolerated-LowRisk |
| ☐ | 4 | AI-Unsanctioned | IT Unsanctioned AI Apps | any | any | $ZONE-PUBLIC | any | any | AI-Unsanctioned |

## 5.5 Associate Snippet with Prisma Access and NGFW folders

In this procedure, you associate the Policy-AI_Access snippet with the Prisma Access and the NGFW folder (example: On-Premises Remote Sites) for your SCM managed firewalls.

**Step 1:** Continuing in SCM, navigate to **Configuration > NGFW and Prisma Access**.

**Step 2:** In the Configuration Scope pane, on the Snippets tab, select Policy-AI_Access.

**Step 3:** On the Overview page, in the Snippet Associations pane, click the edit cog. The Snippet Associations pane appears.

**Step 4:** In the Config Trees table, select **Prisma Access** and On-Premises Remote Sites, and then close the pane.

## 5.6 Adjust Policy Order

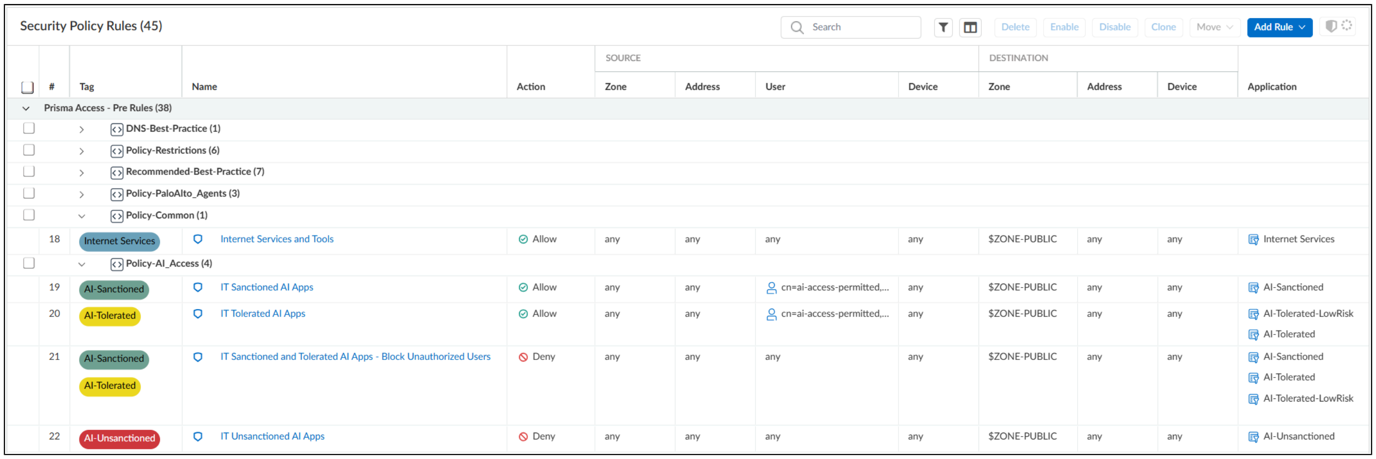
After adding your policy snippets to the Prisma Access and NGFW folders, you might need to change the security policy, to adjust the order of the snippets in the security policy. You place this new snippet towards the top of the policy just after the Policy_Common snippet you created by following the procedures in the **Secure Internet Policy Design: Solution Guide**.

**Step 1:** Continuing in SCM, navigate to **Configuration > NGFW and Prisma Access**.

**Step 2:** In the Configuration Scope pane, on the Folders tab, select **Prisma Access**.

**Step 3:** From the **Security Services** menu, choose **Security Policy**.

**Step 4:** In the Prisma Access - Pre Rules pane, move the Policy-AI_Access snippet so that it is the first snippet to follow the Policy-Common snippet.



Security Policy Rules (45)

| | | | | | SOURCE | | | | DESTINATION | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| □ | # | Tag | Name | Action | Zone | Address | User | Device | Zone | Address | Device | Application |
| Prisma Access - Pre Rules (38) | | | | | | | | | | | | |
| □ | | DNS-Best-Practice (1) | | | | | | | | | | |
| □ | | Policy-Restrictions (6) | | | | | | | | | | |
| □ | | Recommended-Best-Practice (7) | | | | | | | | | | |
| □ | | Policy-PaloAlto_Agents (3) | | | | | | | | | | |
| □ | | Policy-Common (1) | | | | | | | | | | |
| | 18 | Internet Services | Internet Services and Tools | Allow | any | any | any | any | $ZONE-PUBLIC | any | any | Internet Services |
| □ | | Policy-AI_Access (4) | | | | | | | | | | |
| | 19 | AI-Sanctioned | IT Sanctioned AI Apps | Allow | any | any | cn=ai-access-permitted,... | any | $ZONE-PUBLIC | any | any | AI-Sanctioned |
| | 20 | AI-Tolerated | IT Tolerated AI Apps | Allow | any | any | cn=ai-access-permitted,... | any | $ZONE-PUBLIC | any | any | AI-Tolerated-LowRisk<br>AI-Tolerated |
| | 21 | AI-Sanctioned<br>AI-Tolerated | IT Sanctioned and Tolerated AI Apps - Block Unauthorized Users | Deny | any | any | any | any | $ZONE-PUBLIC | any | any | AI-Sanctioned<br>AI-Tolerated<br>AI-Tolerated-LowRisk |
| | 22 | AI-Unsanctioned | IT Unsanctioned AI Apps | Deny | any | any | any | any | $ZONE-PUBLIC | any | any | AI-Unsanctioned |

**Step 5:** As needed for a NGFW deployment, repeat Step 2 through Step 4 by using the NGFW configuration scope in Step 2 (example: On-Premises Remote Sites).

**Step 6:** As needed for a NGFW deployment, using the NGFW configuration scope (example: On-Premises Remote Sites), in the Pre Rules pane, move the **Recommended-Best-Practice** snippet so that it follows the Policy-Common snippet.

## 5.7 Push Configuration Updates to Prisma Access and On-Premises NGFWs

Next, you configure the devices with updated tags that you configured during this and the previous group of procedures.

**Step 1:** Continuing in SCM, navigate to **Configuration > NGFW and Prisma Access**.

**Step 2:** Click **Push Config**, and then click **Push**.

**Step 3:** In the Push Config dialog box, in the **Description** box, enter a description.

**Step 4:** Select **Mobile Users Container**, **Remote Networks**, and On-Premises Remote Sites and then click **Push**.

**Step 5:** In the Jobs dialog box, when the push job result changes to OK, click **Done**.

## Procedures

### Using Activity Insights to Monitor and Tag GenAI Applications

6.1 Access Activity Insights and Set Filters

6.2 Tag Applications Directly from Activity Insights

6.3 Push Configuration Updates to Prisma Access and On-Premises NGFWs

Activity Insights provides a centralized location for monitoring network traffic, applications, threats, and other important metrics. SCM includes predefined filters that allow you to customize the display to show only GenAI applications. You can use Activity Insights to highlight active applications, their data usage, and their current tag.

## 6.1 Access Activity Insights and Set Filters

When you are monitoring for GenAI applications, Activity Insights provides a list of the applications that Prisma Access has reported to SLS. This list commonly also includes applications that your organization has blocked. SCM populates the display by using the tags you set in the Application-Tagging snippet in Procedure 2.7.

**Note**

Activity Insights recognizes only the Sanctioned and Tolerated tags. Applications without these tags are assumed to be Unsanctioned.

Depending on the applications your organization uses, you typically see applications that you did not explicitly tag. These applications display as Unsanctioned. After you observe an unknown GenAI application in Activity Insights, you can choose to update the set of Sanctioned or Tolerated applications.

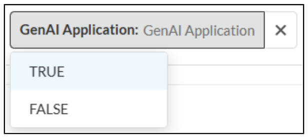
To update the tags, you can repeat Procedure 2.7 for the application, or you can use the tagging workflow described in the following procedure.

**Step 1:** In SCM, navigate to **Insights > Activity Insights**.

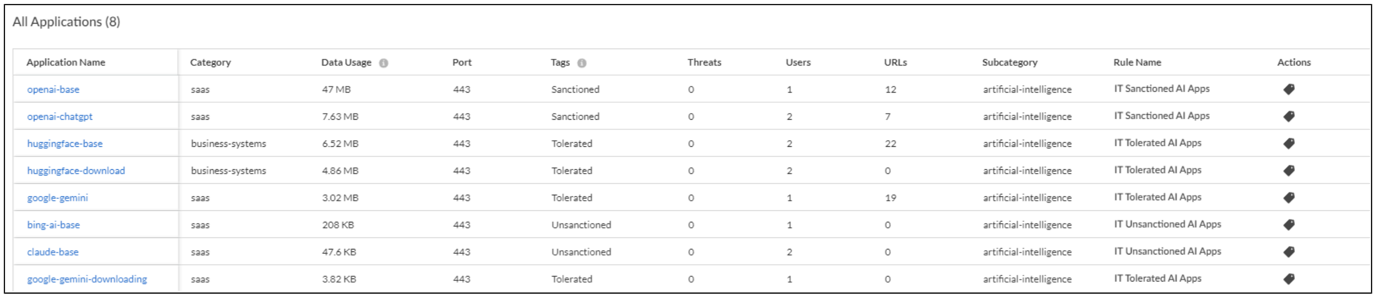
**Step 2:** On the Applications tab, click **Add Filter**.

**Step 3:** In the resulting list, search for and select **GenAI Application**. SCM adds the GenAI Application filter to the set of filters.

**Step 4:** In the **GenAI Application** list, choose **True**.



**Step 5:** If you need to change the time range, click **Time Range**, and then choose the range you need (for example: **Past 24 Hours**).



All Applications (8)

| Application Name | Category | Data Usage | Port | Tags | Threats | Users | URLs | Subcategory | Rule Name | Actions |
|---|---|---|---|---|---|---|---|---|---|---|
| openai-base | saas | 47 MB | 443 | Sanctioned | 0 | 1 | 12 | artificial-intelligence | IT Sanctioned AI Apps | 🏷 |
| openai-chatgpt | saas | 7.63 MB | 443 | Sanctioned | 0 | 2 | 7 | artificial-intelligence | IT Sanctioned AI Apps | 🏷 |
| huggingface-base | business-systems | 6.52 MB | 443 | Tolerated | 0 | 2 | 22 | artificial-intelligence | IT Tolerated AI Apps | 🏷 |
| huggingface-download | business-systems | 4.86 MB | 443 | Tolerated | 0 | 2 | 0 | artificial-intelligence | IT Tolerated AI Apps | 🏷 |
| google-gemini | saas | 3.02 MB | 443 | Tolerated | 0 | 1 | 19 | artificial-intelligence | IT Tolerated AI Apps | 🏷 |
| bing-ai-base | saas | 208 KB | 443 | Unsanctioned | 0 | 1 | 0 | artificial-intelligence | IT Unsanctioned AI Apps | 🏷 |
| claude-base | saas | 47.6 KB | 443 | Unsanctioned | 0 | 2 | 0 | artificial-intelligence | IT Unsanctioned AI Apps | 🏷 |
| google-gemini-downloading | saas | 3.82 KB | 443 | Tolerated | 0 | 1 | 0 | artificial-intelligence | IT Tolerated AI Apps | 🏷 |

## 6.2 Tag Applications Directly from Activity Insights

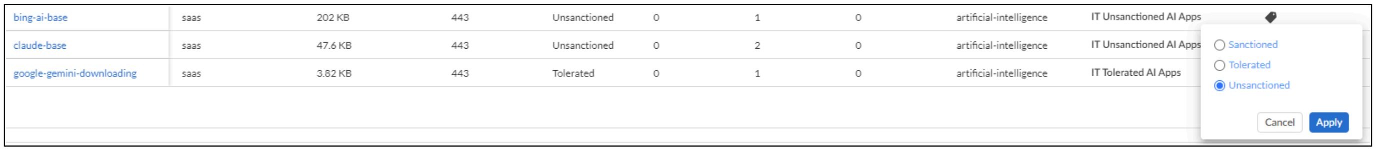
In the previous procedure, you used Activity Insights to display the active GenAI applications. You can use the Activity Insights tagging workflow to tag applications without navigating to the Objects > Applications screens.

This tagging workflow allows you to assign one of these tags to an application:

- Sanctioned
- Tolerated
- Unsanctioned (remove Sanctioned or Tolerated tag)

**Step 1:** Identify an application that should have a different tag (example: bing-ai-base should be tagged as Tolerated).

**Step 2:** In the row for bing-ai-base, in the Actions column, click the tag icon.

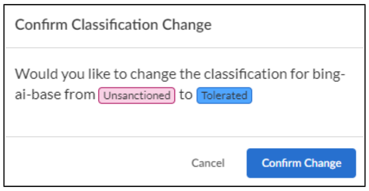


| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| bing-ai-base | saas | 202 KB | 443 | Unsanctioned | 0 | 1 | 0 | artificial-intelligence | IT Unsanctioned AI Apps | |
| claude-base | saas | 47.6 KB | 443 | Unsanctioned | 0 | 2 | 0 | artificial-intelligence | IT Unsanctioned AI Apps | |
| google-gemini-downloading | saas | 3.82 KB | 443 | Tolerated | 0 | 1 | 0 | artificial-intelligence | IT Tolerated AI Apps | |

○ Sanctioned
○ Tolerated
● Unsanctioned

**Step 3:** Choose **Tolerated**, and then click **Apply**.

**Step 4:** In the Confirm Classification Change window, click **Confirm Change**. SCM updates the tag for bing-ai-base in the Application-Tagging snippet.

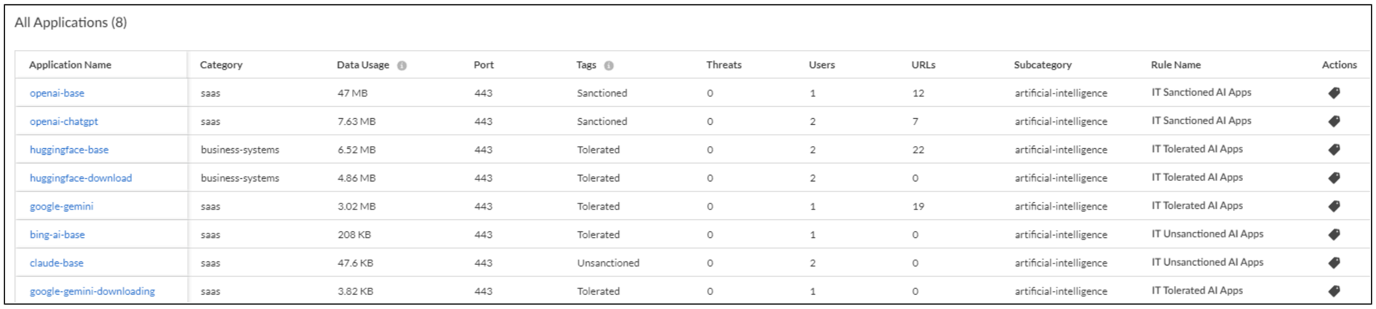


Confirm Classification Change

Would you like to change the classification for bing-ai-base from Unsanctioned to Tolerated

**Step 5:** Verify that Activity Insights displays the updated tag for your application.

> **Note**
>
> The Rule Name that Activity Insights displays corresponds to the rule that originally matched the application. After you update the tag, the application might match a different rule or might show matches for multiple rules until the older log entries age out.



All Applications (8)

| Application Name | Category | Data Usage | Port | Tags | Threats | Users | URLs | Subcategory | Rule Name | Actions |
|---|---|---|---|---|---|---|---|---|---|---|
| openai-base | saas | 47 MB | 443 | Sanctioned | 0 | 1 | 12 | artificial-intelligence | IT Sanctioned AI Apps | |
| openai-chatgpt | saas | 7.63 MB | 443 | Sanctioned | 0 | 2 | 7 | artificial-intelligence | IT Sanctioned AI Apps | |
| huggingface-base | business-systems | 6.52 MB | 443 | Tolerated | 0 | 2 | 22 | artificial-intelligence | IT Tolerated AI Apps | |
| huggingface-download | business-systems | 4.86 MB | 443 | Tolerated | 0 | 2 | 0 | artificial-intelligence | IT Tolerated AI Apps | |
| google-gemini | saas | 3.02 MB | 443 | Tolerated | 0 | 1 | 19 | artificial-intelligence | IT Tolerated AI Apps | |
| bing-ai-base | saas | 208 KB | 443 | Tolerated | 0 | 1 | 0 | artificial-intelligence | IT Unsanctioned AI Apps | |
| claude-base | saas | 47.6 KB | 443 | Unsanctioned | 0 | 2 | 0 | artificial-intelligence | IT Unsanctioned AI Apps | |
| google-gemini-downloading | saas | 3.82 KB | 443 | Tolerated | 0 | 1 | 0 | artificial-intelligence | IT Tolerated AI Apps | |

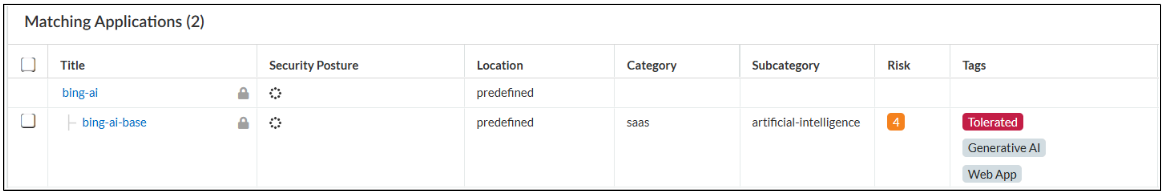
You can also verify the updated tag in the Application-Tagging snippet.

**Step 6:** Navigate to **Configuration > NGFW and Prisma Access** and from the **Objects** menu, choose **Application > Applications**.

**Step 7:** In the Configuration Scope pane, on the Snippets tab, select **Application-Tagging**.

**Step 8:** In the Category Filters pane, click **Clear Filters**.

**Step 9:** In the search box, enter **bing-ai-base**, and then press **ENTER**.



Matching Applications (2)

| ☐ | Title | Security Posture | Location | Category | Subcategory | Risk | Tags |
|---|---|---|---|---|---|---|---|
| | bing-ai | | predefined | | | | |
| ☐ | ├ bing-ai-base | | predefined | saas | artificial-intelligence | 4 | Tolerated<br>Generative AI<br>Web App |

## 6.3 Push Configuration Updates to Prisma Access and On-Premises NGFWs

Next, you configure the devices with updated tags that you configured during this and the previous group of procedures.

**Step 1:** Continuing in SCM, navigate to **Configuration > NGFW and Prisma Access**.

**Step 2:** Click **Push Config**, and then click **Push**.

**Step 3:** In the Push Config dialog box, in the **Description** box, enter a description.

**Step 4:** Select **Mobile Users Container**, **Remote Networks**, and On-Premises Remote Sites and then click **Push**.

**Step 5:** In the Jobs dialog box, when the push job result changes to OK, click **Done**.

Procedures

## Configuring Security Policy Pre-Rules to Control Access to AI Applications for Explicit Proxy

7.1 Add Local User

7.2 Block Access to Sanctioned and Tolerated AI Applications for Unknown Branch Users

7.3 Permit Access to Sanctioned and Tolerated AI Applications for All Other Unknown Users

7.4 Permit Access to Sanctioned and Tolerated AI Applications for CORS Requests

7.5 Associate Snippet with Prisma Access and NGFW folders

7.6 Adjust Policy Order

7.7 Push Configuration Updates to Prisma Access

If you do not use traditional explicit proxy mode to connect to Prisma Access, skip this set of procedures.

You use this set of procedures to support mobile users that connect to Prisma Access using traditional explicit proxy mode (non-GP-app-based). With traditional explicit proxy mode, when you want to implement a user-based or group-based policy to restrict access to a web site, you must include a rule to pre-authorize access to the site for unknown users. In this design, you add a rule permitting access to IT-sanctioned and IT-tolerated AI applications for unknown users.

The purpose of a pre-authorization rule is to allow initial access to a web site, so that the explicit proxy can issue an authentication cookie to the user for access to the site. After the user completes this process, by using the authentication cookie, the user session now includes valid user information and session traffic matches user-based and group-based policy rules. At this point, the user session no longer matches the unknown-user rule.

**Note**

The unknown-user rule does not permit unauthenticated users to use Prisma SASE explicit proxy as an open proxy. If a source never authenticates, the Prisma Access EP-SPN blocks traffic from that source.

Mobile users that connect to Prisma Access using the GlobalProtect app with tunnel mode or proxy mode always have a known User-ID and do not require an unknown-user rule. However, branch users have a known User-ID only when they use the GlobalProtect app with a GlobalProtect internal gateway. To prevent access from any unknown branch users that might use the unknown-user rule, you should block access for unknown-user traffic that originates from branch locations.

If the web site you are controlling access to includes objects hosted from a domain that is different from the domain to which the request is being made, you need to enable support for *cross-origin request-sharing* (CORS) traffic. A CORS request does contain an authentication cookie. However, if the source address of the request has already been authenticated, the user is identified as *swg-authenticated-ip-user*.

To support CORS requests, you need to add the *swg-authenticated-ip-user* as a local user within the Prisma Access configuration scope. After you create the local user, you can add a rule permitting access to IT-sanctioned and IT-tolerated AI applications for this user.

## 7.1 Add Local User

In this procedure, you add the *swg-authenticated-ip-user* as a local user within the Prisma Access configuration scope. You must assign a passphrase for the user account, but the value does not matter.

**Step 1:** In SCM, navigate to **Configuration > NGFW and Prisma Access**, and then, from the **Identity Services** menu, choose **Local Users & Groups**.

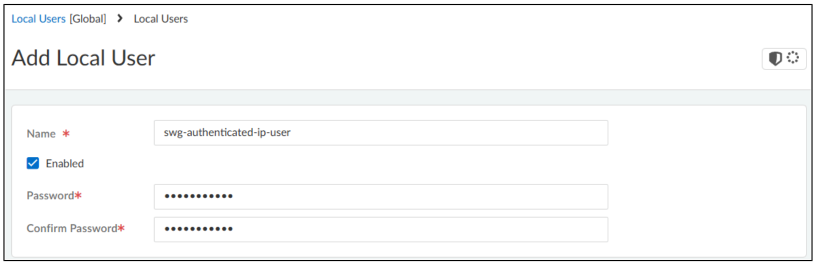
**Step 2:** In the Configuration Scope pane, on the Folders tab, choose **Global**.

**Step 3:** Click **Add Local User**.

**Step 4:** In the **Name** box, enter **swg-authenticated-ip-user**.

**Step 5:** In the **Password** box, enter a complex passphrase.

**Step 6:** In the **Confirm Password** box, re-enter the passphrase, and then click **Save**.



Name * swg-authenticated-ip-user

☑ Enabled

Password* •••••••••••

Confirm Password* •••••••••••

## 7.2 Block Access to Sanctioned and Tolerated AI Applications for Unknown Branch Users

This security-policy rule blocks access both to IT-sanctioned AI applications and to IT-tolerated AI applications, for unknown users located at remote-site locations. This procedure assumes that you have already created an address object that specifies the IP-address range(s) that your organization uses at any remote sites.

This rule is highly specific, and you should insert it above the set of rules that you created in Procedure 5.1, Procedure 5.2, Procedure 5.3, and Procedure 5.4.

**Step 1:** Continuing in SCM, navigate to **Configuration > NGFW and Prisma Access**, and then, from the **Security Services** menu, choose **Security Policy**.

**Step 2:** In the Configuration Scope pane, on the Snippets tab, select Policy-AI_Access_Proxy.

**Step 3:** In the Security Policy Rules pane, click **Add Rule**, and then choose **Security Rule**.

**Step 4:** In the **Name** box, enter IT Sanctioned and Tolerated AI - Block Unknown RN.

**Step 5:** In the **Description** box, enter Block unknown RN users by source IP.

**Step 6:** For Tags, click the plus sign (+), and then choose **AI-Sanctioned**.

**Step 7:** Click the plus (+) again, and then choose **AI-Tolerated**.

**Step 8:** In the Source pane, for Zones, select **Any**.

**Step 9:** In the Source pane, for Addresses, select **Select**.

**Step 10:** In the Addresses list, on the Address tab, select **Net-PrismaSDWAN-RemoteSites**.

**Step 11:** In the Source pane, for Users, click **Unknown**.

**Step 12:** In the Application/Service pane, for Application, select **Select.**

**Step 13:** In the **Application** list, on the Applications Filters tab, select **AI-Sanctioned**, **AI-Tolerated**, and **AI-Tolerated-LowRisk**.

**Step 14:** In the Destination pane, for Zones, select **Select**.

**Step 15:** In the **Zones** list, choose the public zone variable (example: **$ZONE-PUBLIC**).

**Step 16:** For Addresses, select **Any**.

**Step 17:** In the Actions pane, in the **Action** list, choose **Deny**, and then click **Save**.

## 7.3 Permit Access to Sanctioned and Tolerated AI Applications for All Other Unknown Users

This security-policy rule permits access to both IT-sanctioned AI applications and IT-tolerated AI applications for unknown users. This rule only applies to users who access Prisma Access by using traditional explicit proxy mode.

This rule is highly specific, and it should immediately follow the rule you created in Procedure 7.2.

**Step 1:** Continuing in SCM, navigate to **Configuration > NGFW and Prisma Access**, and then, from the **Security Services** menu, choose **Security Policy**.

**Step 2:** In the Configuration Scope pane, on the Snippets tab, select **Policy-AI_Access_Proxy**.

**Step 3:** In the Security Policy Rules pane, click **Add Rule**, and then choose **Security Rule**.

**Step 4:** In the **Name** box, enter **IT Sanctioned and Tolerated AI - Permit Unknown**.

**Step 5:** In the **Description** box, enter **IT sanctioned and IT tolerated unknown user pre-authorization rule (to support Explicit Proxy)**.

**Step 6:** For Tags, click the plus sign (+), and then choose **AI-Sanctioned**.

**Step 7:** Click the plus (+) again, and then choose **AI-Tolerated**.

**Step 8:** In the Source pane, for Zones, select **Any**.

**Step 9:** For Addresses, select **Any**.

**Step 10:** For Users, select **Unknown**.

**Step 11:** In the Application/Service pane, for Application, choose **Select.**

**Step 12:** In the **Application** list, on the Applications Filters tab, select **AI-Sanctioned**, **AI-Tolerated**, and **AI-Tolerated-LowRisk**.

**Step 13:** In the Destination pane, for Zones, select **Select**.

**Step 14:** In the **Zones** list, choose the public zone variable (example: **$ZONE-PUBLIC**).

**Step 15:** For Addresses, select **Any**.

**Step 16:** In the Actions pane, in the **Action** list, choose **Allow**.

**Step 17:** In the **Profile Group** list, choose **best-practice-ai**, and then click **Save**.

## 7.4 Permit Access to Sanctioned and Tolerated AI Applications for CORS Requests

This security-policy rule permits access both to IT-sanctioned AI applications and to IT-tolerated AI applications, for the user *swg-authenticated-ip-user*. This rule only applies to CORS requests for users accessing Prisma Access by using traditional explicit proxy mode

This rule is highly specific, and it should immediately follow the rule you created in Procedure 7.3.

**Step 1:** Continuing in SCM, navigate to **Configuration > NGFW and Prisma Access**, and then, from the **Security Services** menu, choose **Security Policy**.

**Step 2:** In the Configuration Scope pane, on the Snippets tab, select **Policy-AI_Access_Proxy**.

**Step 3:** In the Security Policy Rules pane, click **Add Rule**, and then choose **Security Rule**.

**Step 4:** In the **Name** box, enter **IT Sanctioned and Tolerated AI - Permit CORS Requests**.

**Step 5:** In the **Description** box, enter **IT sanctioned and IT tolerated for CORS requests (from swg-authenticated-ip-user)**.

**Step 6:** For Tags, click the plus sign (+), and then choose **AI-Sanctioned**.

**Step 7:** Click the plus (+) again, and then choose **AI-Tolerated**.

**Step 8:** In the Source pane, for Zones, select **Any**.

**Step 9:** For Addresses, select **Any**.

**Step 10:** For Users, select **Select**.

**Step 11:** In the **Users** list, on the Users tab, search for and select **swg-authenticated-ip-user**.

**Step 12:** In the Application/Service pane, for Application, select **Select.**

**Step 13:** In the **Application** list, on the Applications Filters tab, select **AI-Sanctioned**, **AI-Tolerated**, and **AI-Tolerated-LowRisk**.

**Step 14:** In the Destination pane, for Zones, select **Select**.

**Step 15:** In the Zones list, choose the public zone variable (example: **$ZONE-PUBLIC**).

**Step 16:** For Addresses, select **Any**.

**Step 17:** In the Actions pane, in the **Action** list, choose **Allow.**

**Step 18:** In the **Profile Group** list, choose **best-practice-ai**, and then click **Save**.

## 7.5 Associate Snippet with Prisma Access and NGFW folders

In this procedure, you associate the **Policy-AI_Access_Proxy** snippet with the Prisma Access and the NGFW folder (example: **On-Premises Remote Sites**) for your SCM managed firewalls.

**Step 1:** Continuing in SCM, navigate to **Configuration > NGFW and Prisma Access**.

**Step 2:** In the Configuration Scope pane, on the Snippets tab, select **Policy-AI_Access_Proxy**.

**Step 3:** On the Overview page, in the Snippet Associations pane, click the edit cog. The Snippet Associations pane appears.

**Step 4:** In the Config Trees table, select **Prisma Access** and **On-Premises Remote Sites** and close the pane.

## 7.6 Adjust Policy Order

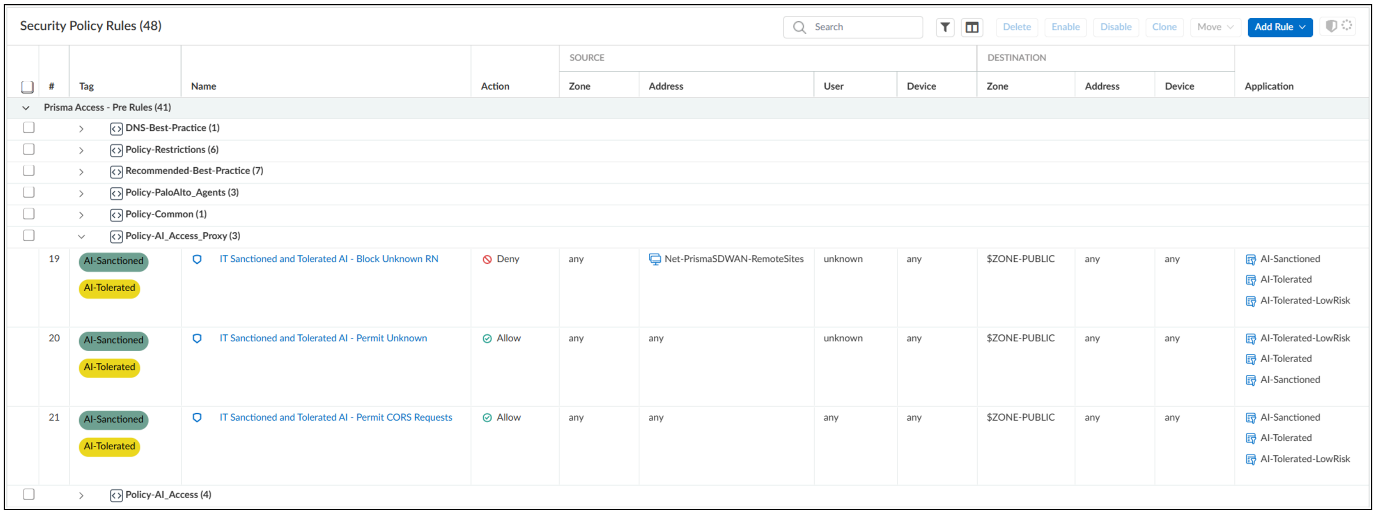
After adding your policy snippets to the Prisma Access and NGFW folders, you might need to change the security policy, to adjust the order of the snippets in the security policy. You place this new snippet before the **Policy_Access_AI** snippet you configured in "Configuring Security Policy Rules to Control Access to AI Applications".

**Step 1:** Continuing in SCM, navigate to **Configuration > NGFW and Prisma Access**.

**Step 2:** In the Configuration Scope pane, on the Folders tab, select **Prisma Access**.

**Step 3:** From the **Security Services** menu, choose **Security Policy**.

**Step 4:** In the Prisma Access - Pre Rules pane, move the **Policy-AI_Access_Proxy** snippet so that it is the first snippet prior to the **Policy-AI_Access** snippet.



Security Policy Rules (48)

| | | | | | SOURCE | | | | DESTINATION | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| □ | # | Tag | Name | Action | Zone | Address | User | Device | Zone | Address | Device | Application |
| Prisma Access - Pre Rules (41) | | | | | | | | | | | | |
| □ | | DNS-Best-Practice (1) | | | | | | | | | | |
| □ | | Policy-Restrictions (6) | | | | | | | | | | |
| □ | | Recommended-Best-Practice (7) | | | | | | | | | | |
| □ | | Policy-PaloAlto_Agents (3) | | | | | | | | | | |
| □ | | Policy-Common (1) | | | | | | | | | | |
| □ | | Policy-AI_Access_Proxy (3) | | | | | | | | | | |
| | 19 | AI-Sanctioned<br>AI-Tolerated | IT Sanctioned and Tolerated AI - Block Unknown RN | Deny | any | Net-PrismaSDWAN-RemoteSites | unknown | any | $ZONE-PUBLIC | any | any | AI-Sanctioned<br>AI-Tolerated<br>AI-Tolerated-LowRisk |
| | 20 | AI-Sanctioned<br>AI-Tolerated | IT Sanctioned and Tolerated AI - Permit Unknown | Allow | any | any | unknown | any | $ZONE-PUBLIC | any | any | AI-Tolerated-LowRisk<br>AI-Tolerated<br>AI-Sanctioned |
| | 21 | AI-Sanctioned<br>AI-Tolerated | IT Sanctioned and Tolerated AI - Permit CORS Requests | Allow | any | any | any | any | $ZONE-PUBLIC | any | any | AI-Sanctioned<br>AI-Tolerated<br>AI-Tolerated-LowRisk |
| □ | | Policy-AI_Access (4) | | | | | | | | | | |

**Step 5:** As needed for a NGFW deployment, repeat Step 2 through Step 4 by using the NGFW configuration scope in Step 2 (example: **On-Premises Remote Sites**).

**Step 6:** As needed for a NGFW deployment, using the NGFW configuration scope (example: **On-Premises Remote Sites**), in the Pre Rules pane, move the **Recommended-Best-Practice** snippet so that it is prior to the **Policy-AI_Access** snippet.

## 7.7 Push Configuration Updates to Prisma Access

Next, you enable all security policies that you configured during this group of procedures.

**Step 1:** Continuing in SCM, navigate to **Configuration > NGFW and Prisma Access**.

**Step 2:** Click **Push Config**, and then click **Push**.

**Step 3:** In the Push Config dialog box, in the **Description** box, enter a description.

**Step 4:** Select **Mobile Users Container**, **Remote Networks**, and **On-Premises Remote Sites**, and then click **Push**.

**Step 5:** In the Jobs dialog box, when the push job result changes to OK, click **Done.**

# Summary

In the world of digital innovation, AI applications have emerged as powerful tools. As these AI-driven applications become increasingly integral, securing access to them is paramount. This document has walked you through the intricacies of securing access to AI applications, providing insights into the design, deployment, and the importance of robust security measures.

AI chatbots, given their ability to process and store vast amounts of data, can be susceptible to cyber threats. Ensuring secure access to these chatbots is not just about safeguarding an application but is vital for protecting sensitive data and maintaining user trust.

Using AI Access Security capabilities, Palo Alto Networks' Prisma Access and NGFW play a pivotal role in enhancing the security landscape. By implementing granular security rules, Prisma Access and NGFW ensure that only authorized entities can interact with AI applications. These security rules can be tailored to suit the unique needs of your organization, providing flexibility while maintaining a strong security posture.

Prisma Access and NGFW go beyond traditional security measures by integrating Data Loss Prevention (DLP) capabilities. By scrutinizing data in transit, Prisma Access and NGFW can identify and mitigate potential data leaks or unauthorized data access, ensuring that the interactions with AI applications are secure and compliant with data protection regulations.

In summary, securing access to AI applications is an essential step in realizing their full potential without compromising on security. Prisma Access and NGFW stand out as a comprehensive solution, offering tailored security rules and robust DLP capabilities, ensuring access to AI applications are not just efficient but also secure and trustworthy.

# Feedback

You can use the **feedback form** to send comments about this guide.

## HEADQUARTERS

Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054, USA
https://www.paloaltonetworks.com

Phone: +1 (408) 753-4000
Sales: +1 (866) 320-4788
Fax: +1 (408) 753-4001
info@paloaltonetworks.com

You can use the **feedback form** to send comments about this guide.