

Prisma Access Cloud Management

Too many organizations have fragmented security tools with disparate management solutions. This makes managing secure remote access at scale a headache, and maintaining consistent security policy enforcement feels impossible. Control over what remote users can access is inconsistent, often differing by location, with users accessing applications from unsecured locations or devices being granted the same level of access as users behind the firewall.

Palo Alto Networks provides a unified management experience for Prisma[®] Access, delivered from the cloud, for consistent management across the full lifecycle of the deployment—from easy onboarding to day-to-day policy management—all while giving you comprehensive visibility and helping you sustain security best practices. Managing secure remote access has never been easier.

Key Features

Configuration

- Intuitive workflows to quickly onboard remote users and locations to Prisma Access
- Out-of-the-box defaults to simplify configuration and accelerate time to value
- Cloud native platform with a unified management experience

Security Visualization and Reporting

- Centralized visibility and insights across Prisma Access
- Interactive, comprehensive reports and dashboards
- Detailed logs across applications, users, threats, and device posture

Security Posture Improvement

- Built-in Best Practice Assessments
- Inline validation to easily improve security posture
- Reporting based on the Center for Internet Security's CIS Critical Security Controls® to better mitigate risks

Automation

- Alerts and notifications for service outages
- Proactive assistance capabilities to maintain the health of the deployment
- Autonomous Digital Experience Management (ADEM) for insights across the entire service delivery path

Overview

Prisma Access Cloud Management is a simple yet powerful cloud-delivered solution that enables comprehensive security management through a single security rule base, with simplified workflows to address use cases in threat prevention, URL filtering, application awareness, user identification, sandboxing, file blocking, and access control. It provides complete visibility into the entire deployment alongside actionable insights to help improve the end user experience. This crucial simplification of security management and continuous assessment of Palo Alto Networks-defined best practices allow you to improve your organization's security posture.

Easy Onboarding

Accelerate time to value from Prisma Access with out-of-the-box default configuration and simplified onboarding workflows built into the core of Cloud Management.

Streamlined workflows and intuitive navigation let you complete complex configuration tasks with ease. You can onboard mobile users and remote networks using predefined configuration and templates. For example, pre-built tunnel configuration is available to easily onboard remote sites and branches.

Consistent Management

Prisma Access Cloud Management keeps enterprise users in mind by providing consistent management for all users, applications, and locations. Manage Prisma Access with a single security rule base for all types of traffic, inbound and internet-bound (SWG). Threat prevention, URL filtering, sandboxing, file blocking, and data filtering are additional capabilities on the same rule.

Enable security features with ease by efficiently configuring security policies, services, and other capabilities within a single flow.

Security Posture Improvement

The threat landscape is evolving, and your organization needs to keep up. Prisma Access Cloud Management continuously assesses the configuration of your entire deployment against Palo Alto Networks recommended best practices. You can leverage this information and take action to improve your organization's security posture as configuration changes in your environment over time. These best practices are integrated into the flows to detect offending configurations and help administrators remediate issues.

Peer Analysis Data

To help you understand the different protection capabilities of underutilized or unimplemented features in your environment, Prisma Access gives you visibility into how your organization's peers in the industry are benefitting from the additional security capabilities available to you.

Security Visualization and Reporting

Prisma Access Cloud Management provides visibility and reporting across threats, users, applications, and connectivity methods by pulling logs from Cortex® Data Lake. As you perform log queries and generate reports, Cloud Management dynamically pulls relevant logs and presents the results.

Interactive Dashboards

Administrators can define a time period to get aggregated visibility across network traffic, applications, and users. This interactive view allows administrators to filter data by clicking on filters of interest, such as traffic, users, and applications.

Additional dashboards can be used to view applications accessed, users, traffic, source and destination locations, source and destination IPs, security rules, threats, files, and URLs. All of these widgets provide interactive filters on aggregated data.

Log Viewer

The built-in Log Viewer assists with troubleshooting, flow tracking, and visualization of threat entry points to aid incident response. Flexible log querying capabilities, plus the ability to launch actions to create threat exceptions or quarantine hosts, help with quick resolution for security workflows. Additional context is given across flows tracking threats—URL- or file-based activity or WildFire® malware prevention service intelligence, along with context for the user, application, and other relevant details.

Reports

Aggregated reports across users, applications, and Prisma Access usage can be scheduled and emailed.

User Activity Reports show applications used and all URLs visited, including URL categories and websites over a specified period, for individual users across all of the users' devices and IPs.

App Usage Reports provide details on security risks associated with your applications, including SaaS applications traversing your network.

Prisma Access Usage Reports provide visibility into the health and performance of Prisma Access, including the status of licenses, bandwidth, and utilization across your entire deployment.

Digital Experience Monitoring

Prisma Access Insights

As an integrated component of Prisma Access Cloud Management, [Prisma Access Insights](#) provides comprehensive global visibility and monitoring for your Prisma Access service. It offers on-demand insight into the service and health of your Prisma Access deployment, plus proactive assistance capabilities, such as real-time alerts.

Autonomous Digital Experience Management

The Autonomous Digital Experience Management (ADEM) add-on for Prisma Access provides native end-to-end visibility for the secure access service edge (SASE). With ADEM, you gain segment-wise insights across the entire service delivery path, with real and synthetic traffic analysis that enables you to drive autonomous remediation of digital experience problems when they arise.

Cloud-Delivered Management Experience

With a cloud native architecture and SaaS solution, you no longer need to worry about maintaining infrastructure or software. Prisma Access Cloud Management was born in the cloud and is scalable on demand.

For more details, refer to the [Prisma Access Cloud Management technical documentation](#).