



Service description document: Strata Cloud Manager

Strata Cloud Manager – Service Definition Document

Service Overview

Strata Cloud Manager is a cloud-delivered, AI-powered management service that provides unified visibility, proactive operations, and consistent policy management across Palo Alto Networks network security infrastructure. It enables centralised administration of next-generation firewalls, SASE, and SD-WAN environments through a single management interface.

The service uses predictive analytics, automation, and best-practice intelligence to reduce operational complexity, improve security posture, and prevent network disruptions.

Service Description

Strata Cloud Manager delivers a unified, AI-driven management platform for network security operations. It provides real-time visibility, predictive analytics, and automated best-practice enforcement across distributed firewall and SASE environments. The service helps organisations simplify operations, maintain consistent policies, and proactively identify risks before they impact service availability.

Service Features

- Unified management interface for network security infrastructure
- AI-driven Strata Copilot for operational insights
- Predictive analytics and AIOps capabilities
- Real-time best practice configuration checks
- Policy analysis and optimisation
- Autonomous Digital Experience Management
- Compliance reporting and audit summaries
- Hierarchical configuration management
- Automated incident ticketing integration
- Device lifecycle and software management

Service Benefits

- Improved operational efficiency and reduced overhead
- Continuous network uptime and resilience
- Significant reduction in configuration errors
- Optimised and consistent security posture
- Faster troubleshooting and decision-making
- Simplified Zero Trust adoption
- Enhanced digital user experience
- Audit-ready compliance reporting
- Simplified lifecycle and upgrade management
- Global scalability without increased complexity

Service Scope

Strata Cloud Manager is delivered as a public cloud service.

The service acts as an extension to Palo Alto Networks next-generation firewalls, Prisma Access, and Prisma SD-WAN, providing a single management plane across these platforms. It can also integrate with external workflow and incident management systems to automate operational processes.

System Requirements

- Supported devices
- Supported operating systems
- Reliable internet connectivity

Service Constraints

The service requires active internet connectivity to access the cloud-based management platform and analytics services.

Support Model

eir Business provides access to vendor-backed support services in line with Palo Alto Networks support offerings.

Support tiers include Standard, Premium, and Platinum, with defined response targets based on incident severity. Optional Technical Account Management and professional services support are available at additional cost.

Support channels include online ticketing and phone support, with availability depending on the selected support tier.

Service Management and Access

The service is accessed through a secure, web-based management interface. It supports all major modern browsers and provides role-based access controls, audit logging, and API-driven automation.

An API is available to support configuration management, reporting, monitoring, and third-party integrations.

Onboarding and Offboarding

eir Business supports onboarding through documentation, training resources, and optional professional services.

At contract end, customers can export logs, reports, and configuration data using supported open formats. Assistance with data migration or transition to alternative solutions can be provided if required.

Data Protection and Security

Data is protected in transit using industry-standard encryption protocols, including TLS and IPsec where applicable. Data at rest is protected using encryption and secure storage services operated by Palo Alto Networks cloud infrastructure partners.

The service complies with recognised security and governance standards, including ISO/IEC 27001 and related frameworks. Regular penetration testing, vulnerability management, and continuous monitoring are performed to maintain service integrity.

Availability and Resilience

Strata Cloud Manager is designed for high availability using a globally distributed, resilient cloud architecture. The service targets 99.99% availability, supported by redundancy, fault tolerance, and proactive monitoring. Service credits apply where availability commitments are not met, in line with published SLAs.

Compliance and Governance

The service follows formal security governance processes aligned with international standards. Palo Alto Networks maintains documented policies covering risk management, operational security, secure development, and incident response.

Audit logs and service activity data are retained in accordance with defined retention policies and are accessible to customers through the management interface.

Pricing

Pricing is subscription-based and dependent on the selected service tier and scale of deployment. Pricing details are provided separately in the G-Cloud pricing document.

