

Strata Cloud Manager Release Notes

Contact Information

Corporate Headquarters:
Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetworks.com/company/contact-support

About the Documentation

- For the most recent version of this guide or for access to related documentation, visit the Technical Documentation portal docs.paloaltonetworks.com.
- To search for a specific topic, go to our search page docs.paloaltonetworks.com/search.html.
- Have feedback or questions for us? Leave a comment on any page in the portal, or write to us at documentation@paloaltonetworks.com.

Copyright

Palo Alto Networks, Inc.
www.paloaltonetworks.com

© 2023-2025 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.

Last Revised

September 30, 2025

Table of Contents

Strata Cloud Manager Release Information.....	11
--	-----------

New Features in Strata Cloud Manager.....	13
--	-----------

Strata Cloud Manager Delivers New Features to You in Two Ways.....	14
Latest Strata Cloud Manager Upgrade Version.....	15
Past Strata Cloud Manager Release Versions.....	16
New Features in November 2025.....	17
New Features in October 2025.....	18
New Features in September 2025.....	25
New Features in August 2025.....	42
New Features in July 2025.....	53
Identity and Access Management Support for SCIM.....	53
Strata Copilot: New Region Support.....	54
Enhanced IOC Search Functionality in Strata Cloud Manager.....	55
Strata Copilot: Accessibility Change.....	55
Direct Users in Activity Insights.....	56
New Features in June 2025.....	57
Strata Copilot: AI Canvas (Beta).....	57
Strata Copilot: Quarantine a Device.....	58
Strata Cloud Manager New Navigation Experience.....	59
Quantum Readiness for Strata Cloud Manager.....	60
Tenant-Level Data Transfer Across Prisma Access.....	60
New Features in May 2025.....	61
New Features in April 2025.....	73
Strata Cloud Manager: NGFW Alerts in April.....	73
Extended Availability of Strata Copilot in Strata Cloud Manager.....	73
Strata Copilot: New Region Support.....	74
ADEM for NGFW.....	74
IP Pool Allocation Enhancements.....	76
New Features in March 2025.....	77
Natural Language Queries for Access Analyzer.....	77
Support for VM-Series funded by Software NGFW Credits in Strata Cloud Manager Essentials.....	77
Advanced WildFire Dashboard Enhancements.....	78
License Migration for AIOps for NGFW Premium, AI-Powered ADEM, and Strata Logging Service.....	79
Strata Copilot: Visualization Type Specification in Prompts.....	79
Strata Copilot: Product Filtering for Responses.....	80
Strata Cloud Manager: NGFW Alerts in March.....	80

New Features in February 2025.....	81
Case Creation Enhancements in Strata Copilot.....	81
Strata Cloud Manager: New Best Practice Assessment Checks and Custom Checks.....	83
Strata Cloud Manager: Web Access Policy Rule Replacement: Migrate to the New Internet Access Rule.....	84
Strata Cloud Manager: Snippet Sharing - Advanced Controls and Visibility Enhancements.....	84
Strata Cloud Manager: Convert Local Configuration into Shared Snippets.....	85
Strata Cloud Manager: Unified Policy Management for SaaS Security and Internet Access Policy Rules.....	85
Prisma Access Cloud Management Region Support.....	86
Visibility Into Prisma Access Configuration Push Status.....	86
Ability to Clone GlobalProtect App Settings and Tunnel Settings.....	87
Prisma Access Browser Support in Strata Copilot.....	87
New AI-Powered Workflow for Troubleshooting Application Access.....	87
Enhanced RMA Workflow for Strata Cloud Manager.....	89
Strata Cloud Manager: NGFW Alerts in February.....	90
New Features in January 2025.....	91
User Inactivity Timeout Customization.....	91
GenAI Data in the Data Security View of the Command Center.....	91
Strata Cloud Manager: NGFW Alerts in January.....	91
New Features in December 2024.....	93
Strata Copilot.....	93
Strata Cloud Manager: NGFW Alerts in December.....	95
Cloud NGFW and Prisma Access Browser Data Integration for Command Center and Activity Insights.....	96
Domains in Activity Insights.....	96
New Features in November 2024.....	98
Autonomous Digital Experience Management (ADEM): Specific SD-WAN Path Monitoring.....	98
Strata Cloud Manager: Policy Optimizer Enhancements.....	98
Strata Cloud Manager: NGFW Support for Configuration APIs.....	99
25,000 Remote Network and 50,000 IKE Gateway Support.....	100
DNS Proxy Customizations.....	100
Named Configuration Snapshots.....	100
Session Browser for Strata Cloud Managed NGFWs.....	101
Exclude URLs and Apps From Enterprise DLP Inspection for Non-File Based Traffic.....	102
Prisma Access Cloud Management Region Support.....	102

Strata Cloud Manager: New Best Practice Assessment Checks and Custom Checks.....	103
Strata Cloud Manager: Policy Analyzer for Strata Cloud Manager Deployments.....	104
Strata Cloud Manager: Role-Based Access Control for Managing and Overriding Security Checks.....	104
Configure Source IP Address Enforcement for Authentication Cookies.....	106
Configure End User Timeout Notifications.....	106
Strata Cloud Manager: NGFW Alerts in November.....	107
New Features in October 2024.....	108
Autonomous DEM: Browser-Based Real User Monitoring (RUM).....	108
Forward Syslogs for Enterprise DLP Incidents.....	109
Simplified Application Test Configuration.....	109
Streamlined Licensing for Strata Cloud Manager.....	110
New Features in September 2024.....	111
Prisma Access: Remote Browser Isolation in China.....	111
Panorama CloudConnector Plugin 2.1.0.....	111
Prisma Access: Agent Proxy Support for Private IP from Branches.....	112
Prisma Access: Explicit Proxy China Support.....	112
Prisma Access: Static IP Enhancements for Mobile Users.....	112
Prisma Access: View Prisma Access, Dataplane, and Application and Threats Content Releases in Strata Cloud Manager and Panorama.....	113
Prisma Access: New Prisma Access Cloud Management Location.....	114
Prisma Browser Visibility.....	114
Strata Cloud Manager: Enhanced Auto VPN Configuration for Large Enterprises.....	116
Strata Cloud Manager: Advanced DNS Security.....	117
Strata Cloud Manager: Local Deep Learning for Advanced Threat Prevention.....	118
Strata Cloud Manager: New Check Box for Overriding Security Checks.....	118
GlobalProtect: Support for PAN-OS-11.2-DHCP-Based IP Address Assignments.....	119
GlobalProtect: Use Default Browser for SAML/CAS Authentication.....	120
Advanced URL Filtering: URL Categorization Check.....	120
Enhanced Report Management.....	121
New Features in August 2024.....	122
AI Access Security.....	122
Streamlined NGFW Incidents and Alerts Management.....	123
Prisma Access Browser.....	123
New Features in July 2024.....	125
Email DLP Enhancements.....	125
Browser Support for Remote Browser Isolation.....	125

Mobile Support for Remote Browser Isolation.....	126
Prisma AIRS.....	126
Dynamic Privilege Access.....	127
Panorama to Strata Cloud Manager Migration.....	127
View and Monitor Dynamic Privilege Access.....	128
Support for Deleting Connector IP Blocks.....	128
Strata Cloud Manager: Cross-Scope Referenceability in Snippets.....	129
Strata Cloud Manager: Disable Default HIP Profiles.....	129
Enterprise DLP: File Type Exclusion.....	129
Forward Email Alerts and SNMP Traps to External Servers.....	130
Configure Management Settings.....	130
New Features in June 2024.....	132
Prisma Access: Third-Party CDR Integration for Remote Browser Isolation.....	132
Strata Cloud Manager: Custom Checks for Security Profiles.....	132
Strata Cloud Manager: New Inline Best Practice Checks.....	133
Cloud Management for NGFWs: Auto VPN Configuration for HA Pairs.....	134
Prisma Access: Fast-Session Delete.....	134
Prisma Access: FQDNs for Remote Network and Service Connection IPsec Tunnels.....	134
Prisma Access: Native IPv6 Compatibility.....	135
Prisma Access: Service Connection Support for Explicit Proxy.....	135
Strata Cloud Manager: Manage and Share Common Configuration Using Snippet Sharing.....	135
Strata Cloud Manager: Global Find Using Config Search.....	136
Strata Cloud Manager: Local Configuration Management.....	136
Strata Logging Service in Strata Cloud Manager.....	137
Enterprise DLP: End User Coaching.....	137
New Features in May 2024.....	139
Strata Cloud Manager: Policy Config Memory Usage Approaching Max Limits Alert.....	139
Strata Cloud Manager: Config Memory Usage Approaching Max Limits Alert.....	139
Strata Cloud Manager: ACC Query Failure Alert.....	140
Strata Cloud Manager: Approaching Max Capacity - URLs or IPs within EDLs Alert.....	140
Strata Cloud Manager: PAN-OS Integrated User-ID Agent Monitored Server Disconnected Alert.....	141
Strata Cloud Manager: Hijacked and Misconfigured Domain Views in DNS Security Dashboard.....	142
New Features in April 2024.....	143

Cloud Management for NGFWs: Aggregate Interface Usability Enhancement.....	143
Cloud Management for NGFWs: Device Onboarding Rules.....	143
Cloud Management for NGFWs: Transparent Web Proxy.....	144
Strata Cloud Manager: Configuration Indicator.....	144
Strata Cloud Manager: External Gateway Integration for Prisma Access and On-Premises NGFWs.....	145
Strata Cloud Manager: Command Center.....	145
Strata Cloud Manager: Activity Insights.....	146
Strata Cloud Manager: View Only Administrator Role Enhancement.....	147
Strata Cloud Manager: Trusted IP List.....	147
New Features in March 2024.....	148
Changes to Monitor > Applications and Monitor > Users.....	148
AIOps for NGFW: NGFW/Panorama Management Certificate Expiration Alert.....	148
AIOps for NGFW: Probable Cause Analysis with CDL.....	149
New Features in February 2024.....	150
AIOps for NGFW: Delayed Telemetry Alert.....	150
Prisma Access: Remote Network Locations with Overlapping Subnets.....	150
Prisma Access: License Enforcement for Mobile Users (Enhancements).....	151
Prisma Access: Policy Analyzer for Panorama Managed Deployments.....	151
Cloud Management for NGFWs: UI Update for Security Checks.....	152
Cloud Management for NGFWs: Clone a Snippet.....	152
Cloud Management for NGFWs: TACACS+ Accounting.....	153
Traceability and Control of Post-Quantum Cryptography in Decryption.....	153
Cloud Management of NGFWs: GlobalProtect Portal and Gateway.....	154
Strata Cloud Manager: Private Key Export in Certificate Management.....	155
Strata Cloud Manager: New Prisma Access Cloud Management Location.....	155
User Session Inactivity Timeout.....	155
AIOps for NGFW: Logging Drive Failure Alert.....	156
New Features in January 2024.....	158
Prisma Access: Explicit Proxy Forwarding Profiles with Multiple PAC File Support.....	158
Query Usability and Performance Enhancements in Log Viewer.....	158
New Features in November 2023.....	159
Cloud Management for NGFWs: Capacity Analyzer Alerts.....	159
Prisma SD-WAN: Public Cloud High Availability (HA).....	160
Prisma Access: Cloud Delivered Enterprise Network Integration.....	161
Prisma Access: Remote Browser Isolation.....	162
Prisma Access: Service Connection Identity Redistribution Management....	163

Cloud Management for NGFWs: IPSec VPN Monitoring.....	163
Cloud Management for NGFWs: PA-450R Next-Generation Firewall Support.....	163
Cloud Management for NGFWs: PA-5445 Next-Generation Firewall.....	164
Cloud Management for NGFWs: Inline Best Practice Checks for Device Setup.....	164
Cloud Management for NGFWs: VM-Series Device Management.....	164
Cloud Management for NGFWs: Security Posture Checks.....	165
Cloud Management for NGFWs: GlobalProtect.....	165
Cloud Management for NGFWs: IP Protocol Scan Protection.....	166
Cloud Management for NGFWs: TLSv1.3 Support for SSL/TLS Service Profiles (Administrative Access).....	166
Enforcing Authentication Cookie Validation.....	167
End User Timeout Notifications.....	167
Separate Client Authentication for Portal and Gateway.....	167
Enforcing Authentication Cookie Validation.....	168
IoT Security: Device Visibility and Automatic Policy Rule Recommendations.....	168
New Features in October 2023.....	169
Prisma SD-WAN: Native SASE Integration.....	169
Prisma Access: Cisco Catalyst SD-WAN Integration.....	169
New Features in September 2023.....	170
Prisma Access: Traffic Mirroring and PCAP Support.....	170
Prisma Access: New Local Zones.....	170
Prisma Access: Microsoft Defender for Cloud Apps Integration.....	171
Cloud Management for NGFWs: New Predefined BGP Distribution Profile (Auto VPN & SD-WAN).....	171
Cloud Management for NGFWs: Custom Path Quality Profile (SD-WAN).....	172
Cloud Management for NGFWs: Pre-Shared Keys Refresh (Auto VPN & SD-WAN).....	172
Cloud Management for NGFWs: Cloud IP Tag Collection (with the Cloud Identity Engine).....	173
Cloud Management for NGFWs: Configuration Version Snapshot.....	174
Cloud Management for NGFWs: Troubleshooting for NGFW Connectivity and Policy Enforcement.....	175
Cloud Management for NGFWs: Config Cleanup.....	175
Cloud Management for NGFWs: Policy Optimizer.....	176
Cloud Management for NGFWs: Explicit Web Proxy.....	176
Strata Cloud Manager: SaaS Application Endpoint Lists and Enforcement.....	177
Strata Cloud Manager: Snippet Deletion.....	180

- Strata Cloud Manager: Enhancements to WildFire Dashboard..... 181
- Strata Cloud Manager: Advanced WildFire Analysis Data in IoC Search..... 181
- Strata Cloud Manager: Signature-Based PCAP in Threat Logs..... 181
- Strata Cloud Manager: Log Viewer Visibility Enhancements..... 182
- Known Issues..... 183**
 - Configuration Management Known Issues..... 184
 - Command Center Known Issues..... 187
 - Prisma Browser Visibility Known Issues..... 189
- Addressed Issues..... 191**
 - Command Center Known Issues..... 202
- Getting Help..... 203**
 - Related Documentation..... 204
 - Requesting Support..... 205

Strata Cloud Manager Release Information

Palo Alto Networks Strata Cloud Manager is a new AI-powered Network Security platform. With Strata Cloud Manager you can easily manage your Palo Alto Networks Network Security infrastructure – your NGFWs and SASE environment – from a single, streamlined user interface.

Strata Cloud Manager's shared security policy ensures that all your enterprise traffic gets consistent policy enforcement, and Strata Cloud Manager also leverages AI to maintain peak health for managed products, and to give you the best possible security posture.

About Strata Cloud Manager Releases

There are two ways that the Strata Cloud Manager management platform delivers new features and fixes:

- **Quarterly Scheduled Upgrades**

These scheduled release upgrades provide core Strata Cloud Manager features: these management updates enhance shared policy and expand configuration controls for the NetSec platform. For these releases, we will send an in-product notification in advance of the release, to let you know that a release upgrade window is coming up so that you can plan ahead. For a brief period during the release upgrade, you cannot make configuration changes.

- **Continuous, Seamless Deployments**

In parallel to the scheduled releases, Strata Cloud Manager continuously releases new network security capabilities as they become available for [supported NetSec products and subscriptions](#); this ensures quick enablement and support for all products and subscriptions across the NetSec platform. These features are released seamlessly, without a scheduled upgrade window and there's no impact to you.



To see the new features for a specific product area that's supported with Strata Cloud Manager, also review the product-specific release notes:

- [Prisma Access Release Notes](#)
- [Prisma SD-WAN Release Notes](#)
- [AI-Powered Autonomous DEM Release Notes](#)
- [Advanced WildFire](#)
- [Advanced Threat Prevention](#)
- [Advanced URL Filtering](#)
- [DNS Security](#)
- [SaaS Security](#)
- [Enterprise DLP](#)

New Features in Strata Cloud Manager

Strata Cloud Manager delivers new features to you in two ways: scheduled upgrades give you new management features, and we release NetSec platform feature on a continuous basis in parallel to the scheduled upgrades.

Scheduled upgrades introduce a new Strata Cloud Manager release version. Most Strata Cloud Manager instances are running the latest release version, except during the brief release roll-out period, when we upgrade Strata Cloud Manager instances in phases. You can reference the Strata Cloud Manager release version to validate that you're running the latest version, and to see which features are introduced in the latest upgrade.

Strata Cloud Manager Delivers New Features to You in Two Ways

Strata Cloud Manager supports [two types of release deployments](#): quarterly Strata Cloud Manager management upgrades and continuous, seamless updates for NetSec platform features.

- **Scheduled Upgrades → Configuration Management Features**

Quarterly, scheduled management upgrades provide core configuration management capabilities that enhance shared policy and expand configuration management controls for the NetSec platform. These features depend on a Strata Cloud Manager release version. Most instances of Strata Cloud Manager will be running the same release version, except during the release upgrade period, where upgrade windows are scheduled across a period from one to two weeks.

- **Continuous Deployments → Support for NetSec Platform Features**

Strata Cloud Manager provides continuous support for new features introduced across the NetSec platform. Continuous new feature deployment runs in parallel to the scheduled management releases, to ensure quick enablement and support for all products and subscriptions across the NetSec platform. These features are released seamlessly, without a scheduled upgrade window and there's no impact to you.

Latest Strata Cloud Manager Upgrade Version

In October 2025, we released Strata Cloud Manager **2025.R5.0**. [Here are the features we introduced with this release.](#)

Past Strata Cloud Manager Release Versions

- **2025.R4.3**→ [Features this release introduced](#)
- **2025.R4.0**→ [Features this release introduced](#)
- **2025.R3.0**→ [Features this release introduced](#)
- **2025.R1.0**→ [Features this release introduced](#)

New Features in November 2025

Here are the new features we've added to Strata Cloud Manager in November 2025.

- [NetSec Platform Features](#)

New NetSec Platform Features on Strata Cloud Manager (November 2025)

These new features follow the Strata Cloud Manager release model of [continuous feature deployment](#); as they're ready, we make them available to ensure the latest support for all products and subscriptions across the NetSec platform. There's no Strata Cloud Manager upgrade or management version requirement associated with these features; however, check if they have version or license dependencies associated with other parts of the NetSec platform (like a cloud-delivered security service subscription, or a Prisma Access version, for example)

New Features in October 2025

Here are the new features we've added to Strata Cloud Manager in October 2025.

- [2025.R5.0 Configuration Management Features](#)
- [NetSec Platform Features](#)

New Strata Cloud Manager Management Features (October 2025)

Here's the new [configuration management](#) features we've added to Strata Cloud Manager in October 2025; we use a scheduled upgrade to deliver these features to you and they are supported with the Cloud Manager 2025.R5.0 release version. Check your Strata Cloud Manager in-product notifications for updates on the release upgrade schedule. You can verify which Strata Cloud Manager release version you're running by navigating to your [configuration overview](#), and checking the **Cloud Management Version**.

Configuration Management Support by Region

October 27, 2025

Supported on:

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

Strata Cloud Manager for Configuration Management is a solution that is defined and controlled based on the region where it is deployed. You can deploy Strata Cloud Manager in the locations of your choosing, based on data location preferences and where you have the most users. This selection of locations allows for optimized performance, adherence to data residency requirements, and tailored user experiences based on geographical proximity. For this reason, we are rolling out region-specific support for Strata Cloud Manager as soon as we are able to do so for [each region](#).

You can now deploy Strata Cloud Manager in the following additional regions for Configuration Management support in the Strata Cloud Manager 2025.R5.0 release: **Brazil, Italy, Korea, Poland, and Spain**.

The Global Configuration search feature is now available across the following regions: **United States, Europe, and Singapore**.

Migration Catalog in Strata Cloud Manager

October 27, 2025

Supported for Strata Cloud Manager.

[Migration Catalog](#) addresses the lack of uniform workflows and discoverability across various migration efforts by providing a single, centralized location for all migration-related activities in

Strata Cloud Manager. This catalog serves as a launching point for migration workflows, offering visibility into available migration options and their prerequisites, which helps administrators better understand Strata Cloud Manager's migration capabilities.

When you access the Migration Catalog, you can view and select the Panorama-managed NGFW migration. The catalog implements a consistent user experience across different migration workflows based on a common stepper flow, similar to the existing Panorama-based NGFW migration. This standardization makes it easier for you to understand and navigate through the migration process regardless of which specific migration you are performing.

For migration options, the catalog explains the high-level workflow and prerequisites needed for successful configuration migration into Strata Cloud Manager. This transparency helps you prepare adequately before initiating any migration process, reducing the likelihood of encountering issues during migration and increasing the chances of a smooth transition to Strata Cloud Manager.

Panorama to Strata Cloud Manager Migration for NGFWs

October 27, 2025

Supported for:

- NGFW (Managed by Panorama)
-

If you use Panorama to manage your organizations NGFWs, [you can migrate your configurations to Strata Cloud Manager for the benefits of cloud management](#).

Strata Cloud Manager enables you to migrate your organizations NGFW hierarchy and configurations:

- ❑ **Complete migration visibility and control** — Accept and validate Panorama running configurations with pre-migration identification of unsupported elements.
- ❑ **Flexible migration options** — Choose partial or complete configuration migration based on your requirements.
- ❑ **Conflict prevention** — Automatic detection and display of previously migrated elements during subsequent migrations.
- ❑ **Automated validation** — Minimize the risk of configuration errors that could impact network security.
- ❑ **Configuration continuity** — Maintain your previous configurations throughout the migration process.

For the benefits of moving to Strata Cloud Manager, click [here](#).

Shared Configuration Management

October 27, 2025

Supported for:

- Strata Cloud Manager
-

Shared configuration management eliminates the complexity of managing security policies across multiple Palo Alto Networks services by allowing other Palo Alto Networks services to [subscribe to and receive configuration objects from Strata Cloud Manager](#). Shared configuration management allows you to independently implement features without introducing inconsistencies or delays by providing a unified way for subscribers like Prisma SD-WAN Controller or [Branch Sites for Prisma SD-WAN Ion](#) devices to access and use Strata Cloud Manager managed NGFW and Prisma Access configurations.

Palo Alto Networks services can access Strata Cloud Manager configuration objects on a read-only basis while maintaining proper synchronization and usage tracking. Shared configurations enable you to share Security Profiles such as Threat Prevention, Anti-Spyware, Vulnerability Protection, URL Filtering, and DNS Security with Prisma SD-WAN Controller instances. You can track which shared objects are actively referenced by external services, and Strata Cloud Manager automatically blocks deletion of configuration objects that are currently in use by external subscribers to prevent configuration conflicts.

When making pushes to other services, reverting those pushes should be avoided as it may cause issues with your configuration.

Zero Touch Provisioning NGFW Installer Web Application

October 27, 2025

Supported for:

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

You can now activate Palo Alto Networks NGFWs at branch locations using the [ZTP NGFW Activation web app that extends the existing Zero Touch Provisioning \(ZTP\)](#) capabilities to mobile devices. This solution enables field installers to complete NGFW onboarding and activation without requiring technical expertise or detailed knowledge of customer network configurations. The web app is browser-based and supports both iOS and Android devices, eliminating the need for separate native applications while maintaining full compatibility with existing ZTP workflows.

The ZTP NGFW Activation web app allows for QR code scanning functionality on Gen 5 or newer hardware that automatically populates device-specific information including Serial Numbers and Claim Keys directly from labels affixed to the NGFW hardware. When you scan a QR code using your mobile device's camera, the QR code contains an embedded URL that redirects you to the ZTP Activation Page along with the Serial Number and Claim Key data. The application automatically populates these fields from the scanned QR code data, and you simply need to initiate the ZTP activation process for the device.

You gain access to all existing ZTP activation features through the web app, including the ability to view activation history for devices processed within the last seven days and monitor the status of firewalls during the provisioning process. The application maintains the same security and authentication requirements as the desktop ZTP portal while optimizing the user interface for smartphones.

This web app addresses deployment scenarios where installers work across multiple branch locations and may need to activate NGFWs for different customers without carrying laptops or requiring detailed technical documentation. The solution reduces the complexity of field

deployments while maintaining the security and configuration management oversight that network security teams require for firewall provisioning workflows.

New NetSec Platform Features on Strata Cloud Manager (October 2025)

These new features follow the Strata Cloud Manager release model of [continuous feature deployment](#); as they're ready, we make them available to ensure the latest support for all products and subscriptions across the NetSec platform. There's no Strata Cloud Manager upgrade or management version requirement associated with these features; however, check if they have version or license dependencies associated with other parts of the NetSec platform (like a cloud-delivered security service subscription, or a Prisma Access version, for example)

Strata Cloud Manager: Support for NGFW Clustering

October 27, 2025

Supported for:

- Strata Cloud Manager
-



Please contact your account team to enable this feature.

You can now [configure and manage NGFW clustering for PA-7500 devices](#) directly through Strata Cloud Manager (SCM). This feature enables you to group two PA-7500 firewalls into a single logical cluster entity that operates in device redundancy mode with one routing domain. When you configure clustering, SCM treats the cluster as a unified device where you apply all policies, objects, and networking configurations to the cluster folder rather than individual devices. This approach simplifies management while providing high availability for your network infrastructure.

Strata Cloud Manager: IPS Signature Converter Support

October 27, 2025

Supported for:

- Strata Cloud Manager
-

Organizations require rapid, comprehensive threat intelligence but often struggle to leverage security advisories distributed in third-party formats like Snort and Suricata. This challenge leaves network defenses incomplete and vulnerable to emerging threats not yet covered by internal systems. Strata Cloud Manager now allows you to [create custom application signatures that can detect, monitor, and prevent network-based attacks, based on Snort signatures and Suricata rules](#).

Snort and Suricata are third party open-source intrusion prevention system (IPS) tools that utilize specialized rule formats to identify potential threats. Because organizations that share threat intelligence often distribute security advisories using these rule formats, the additional coverage can reveal threats that might not be apparent on any single IPS system. The IPS Signature

Converter functionality allows you to leverage these open-source rules for immediate threat protection on Palo Alto Networks Strata Cloud Manager by translating the IPS signatures from Snort and Suricata into custom threat signatures.

After the Snort or Suricata rules are converted, you can use these signatures to enforce security policies by incorporating the converted signatures into your Vulnerability Protection and Anti-Spyware Security Profiles.

By leveraging this conversion process, you can quickly adapt and implement a wide range of threat detection rules from the open-source community, enhancing your network's security posture with up-to-date and comprehensive threat intelligence.

Regional File Forwarding Configuration for MacOSX Dynamic Analysis

October 20, 2025

Supported for:

- NGFW and Prisma Access (managed by Strata Cloud Manager)
-

Organizations operate globally and frequently adhere to strict regional data compliance requirements when Advanced WildFire® is deployed into corporate networks for malware analysis. When using dynamic analysis for MacOSX files, meeting these geographic mandates can present a challenge. To address this control gap, [the Advanced WildFire® service now provides the ability to choose the geographic location where MacOSX files are forwarded to for Advanced WildFire dynamic analysis](#). This ensures that customers maintain precise governance over where their samples are analyzed. This feature allows administrators to designate specific regional WildFire clouds—currently those located in the US, EU, Singapore, or Japan—to analyze and classify MacOSX files with WildFire verdicts using dynamic analysis, a high-fidelity sandboxing solution that tests the suspected file in a secure, virtualized environment to observe its behavior. The sample is temporarily sent to the region designated for MacOSX dynamic analysis, during which the file is analyzed and subsequently deleted. The sample analysis results are then sent to your configured WildFire public cloud region for access. The Advanced WildFire cloud uses the sample analysis results to generate and distribute signatures used by various Palo Alto Networks products to prevent further distribution of malicious threats contained in MacOSX files. By enforcing strict geographic boundaries for analysis, organizations can balance robust threat detection with regional data residency mandates. For maximum security, the forwarding functionality is disabled by default, ensuring configuration requires deliberate authorization. This capability strengthens compliance posture while leveraging the full detection power of Advanced WildFire.

Streamline Incident Management with Unified Incident Framework

October 17, 2025

Supported for:

- NGFW and Prisma Access (managed by Strata Cloud Manager)
-

The Strata Cloud Manager [Unified Incident Framework](#) offers a consistent and centralized approach to managing incidents across your various security products. This framework addresses the challenges you face in monitoring diverse network security deployments by consolidating all incidents into a single, unified interface. This gives you comprehensive visibility into your entire security infrastructure.

The unified dashboard displays a summary of all incidents, including the total number of open incidents and breakdowns by product type, category, severity, and priority. You can readily access detailed information for each incident, encompassing the title, severity level, affected objects, recommended remediation steps, and relevant timestamps.

The framework supports flexible notification mechanisms, including email, webhooks, and integrations with ITSM systems, ensuring that you remain informed of critical issues even outside the product interface. You can customize incident settings to focus on issues pertinent to your specific deployments by defining criteria for incident generation and configuring notification preferences.

Strata Cloud Manager now organizes Security Posture Settings under the Unified Incident Framework to deliver a unified and contextual incident management experience. Previously, you could access the security posture check from **Configuration > Posture > Settings**. With the unified incident framework, these security posture settings have moved to **Incidents > Settings**. This update aligns all posture-related rules and custom checks with incident workflows, enabling easier correlation between configuration issues and the incidents they generate.

Leveraging the Unified Incident Framework provides the following benefits:

- **Consistent Incident Management:** Ensures a uniform approach to incident handling.
- **Faster troubleshooting:** Centralized visibility and detailed information facilitate quicker identification and resolution of issues.
- **Informed Decision-Making:** Comprehensive context enables a better understanding of the impact and root cause of incidents.
- **Improved Operational Efficiency:** Streamlined processes and reduced incident fatigue enhance overall operational effectiveness.

This comprehensive design helps you maintain optimal health and security across your infrastructure, reducing the overhead and inefficiencies associated with managing disparate alerting systems.

Unifying SASE and NGFW Visibility with the NetSec Health Dashboard

October 10, 2025

Supported for:

- Prisma Access and NGFW (managed by Strata Cloud Manager)
-

The [NetSec Health Dashboard](#) provides a comprehensive view of your organization's network security health across all user devices, branch sites and monitored applications. Previously, NGFW users lacked a unified way to understand the end-to-end health of users and applications across their organization. This dashboard enhances the existing SASE health dashboard by integrating the health and experience scores from both your Next-Generation Firewall (NGFW)

deployments and your Prisma Access (PA) environment into a single pane of glass. Currently, the dashboard shows unified digital experience insights from NGFW deployments for user devices only.

The interactive view in the dashboard shows the experience scores to highlight the status of user devices, sites, and applications in your organization as Good, Fair, and Poor. You can further drill down to analyze user-specific details, users' browsing experience, network segments causing degradation, and open device incidents. For sites, you can review Prisma SD-WAN and third-party connectivity data and any related open incidents. For monitored applications, the dashboard shows application availability and critical end-to-end performance metrics.

GlobalProtect: Two Factor Authentication Using OTPs

October 27, 2025

Supported for:

- NGFW (managed by Strata Cloud Manager)
-

Secure your remote access environment against credential theft by implementing robust [two-factor authentication \(2FA\) using One-Time Passwords \(OTPs\)](#). This essential security feature requires users requesting access to enter a unique OTP token sent from the authentication service to their RSA device. Implement this 2FA mechanism across your GlobalProtect® portals and gateways to ensure comprehensive protection

By default, the app reuses the same credentials used to log in to the portal and gateway. In the case of OTP authentication, this behavior causes the authentication to initially fail on the gateway. The resulting delay in prompting the user for a login often leads to the time-sensitive OTP expiring before it can be entered. To prevent this, you must configure the portals and gateways that prompt for the OTP instead of using the same credentials on a per-app configuration basis.

New Features in September 2025

Here are the new features we've added to Strata Cloud Manager in September 2025.

- [2025.R4.3 Configuration Management Features](#)
- [NetSec Platform Features](#)

New Strata Cloud Manager Management Features (September 2025)

Here's the new [configuration management](#) features we've added to Strata Cloud Manager in September 2025. Check your Strata Cloud Manager in-product notifications for updates on the release upgrade schedule. You can verify which Strata Cloud Manager release version you're running by navigating to your [configuration overview](#), and checking the **Cloud Management Version**.

Strata Cloud Manager Simplified Navigation Structure

September 25, 2025

Supported for:

- Strata Cloud Manager
-

Phased Rollout of Strata Cloud Manager New User Interface

The Strata Cloud Manager new interface will be deployed through a phased rollout based on regions, beginning September 25, 2025, and continuing through the first week of October, 2025. Region-specific support will automatically be available as deployment completes for each region.



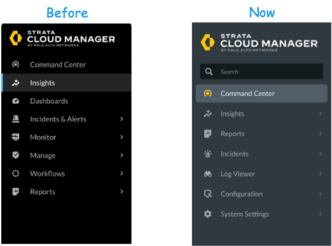
Strata Cloud Manager is not available to you to manage your instances hosted in China or in FedRAMP high regions.

Strata Cloud Manager introduces a new navigation structure designed to improve user experience and simplify the management of complex network security infrastructure by organizing options into three key workflow categories: Monitor, Investigate, and Configure. This simplified approach helps you efficiently manage and monitor your entire network security ecosystem from a single, unified interface.

The new navigation design addresses the complexity stemming from the consolidation of multiple products such as Prisma Access, AIOps for NGFW, ADEM, Prisma SD-WAN, and CDSS into a single platform. This structure provides unified insights, consolidated configuration, streamlined workflows, enhanced search, and consistent access.

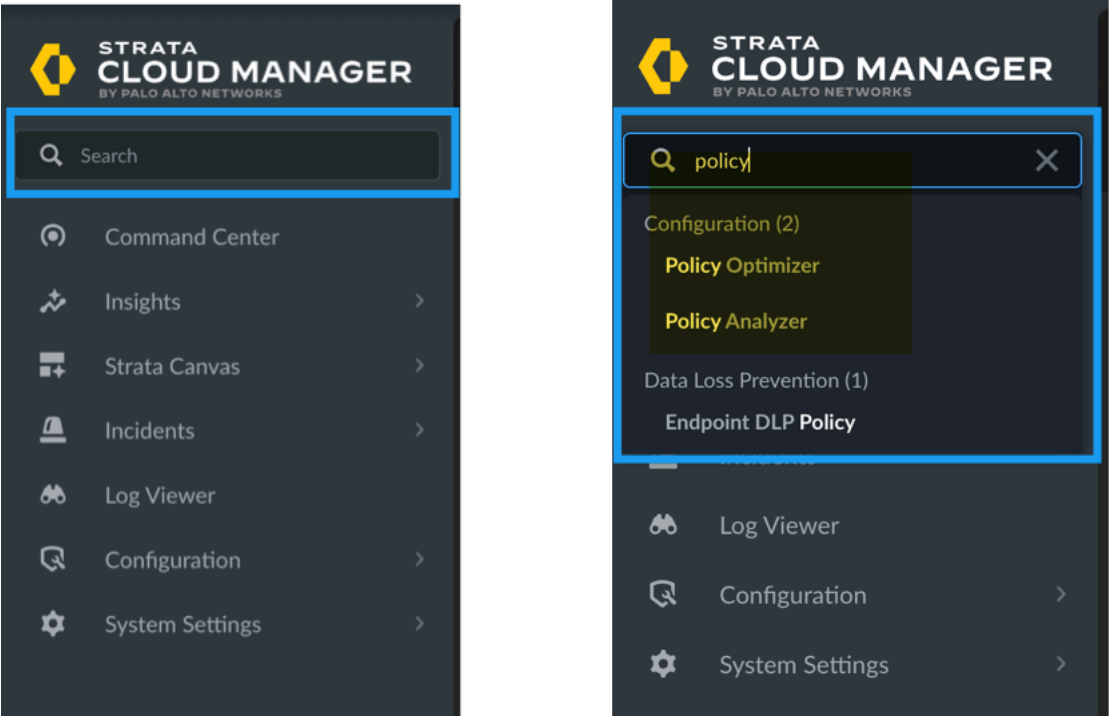
See how the left navigation has changed, what's new, and how pages map to each other now [here](#).

The following graphic shows you the difference in the left navigation panel when you first log in.



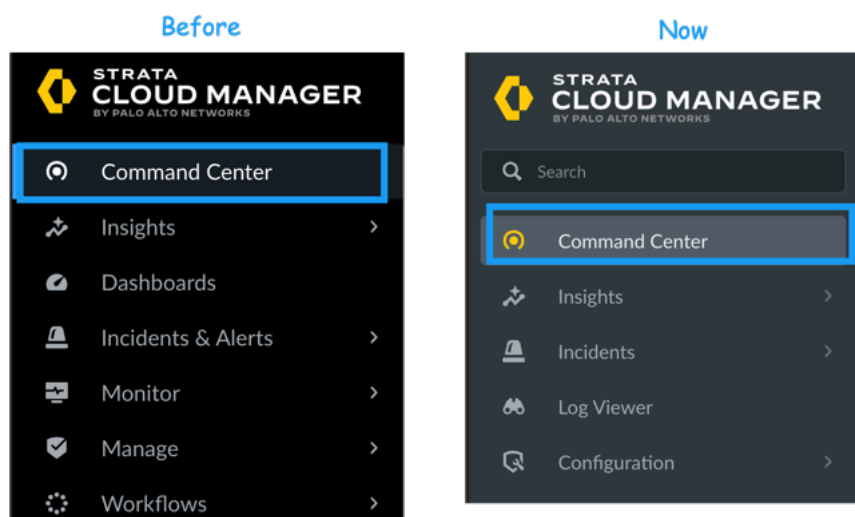
Enhanced Navigation Search

The new search capability added to the left navigation allows you to quickly locate specific pages without navigating through multiple menus.



❑ Command Center

Command Center provides high-level summaries of your Palo Alto Networks product ecosystem.

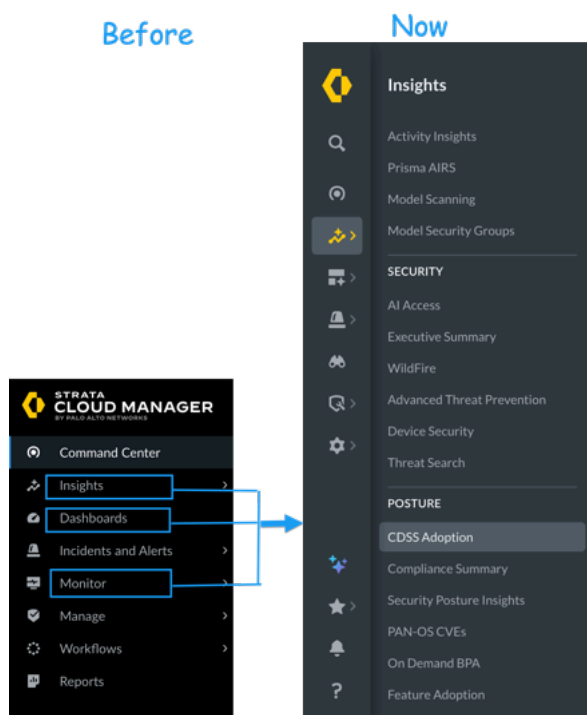


□ Visibility via Insights

You can access monitoring capabilities through the consolidated Insights section, which brings together security and operational dashboards in one location.

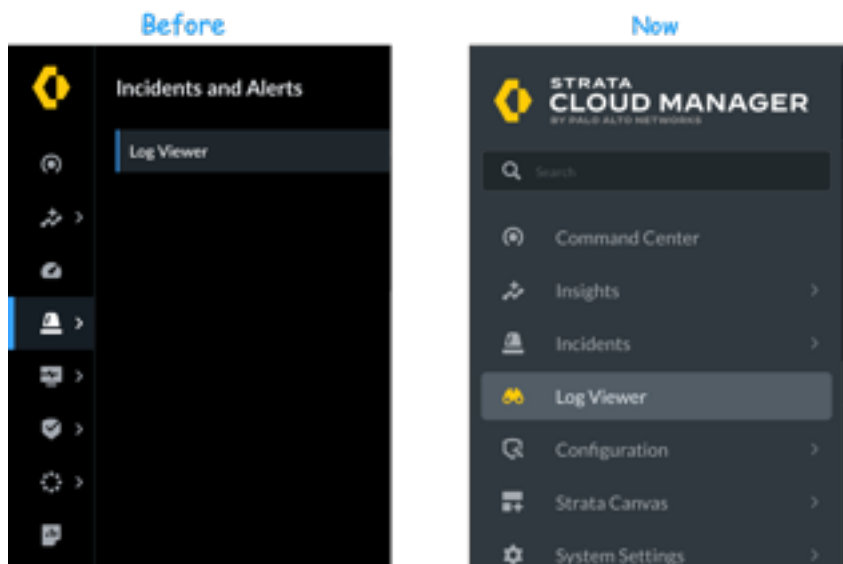
 *The DNS Security dashboard and its associated reports have been deprecated. You can access the related use cases on the **Insights > Activity Insights > Domains** [page](#).*

To view the DNS Security and Advanced DNS Security insights, generate a Security Lifecycle Review (SLR) [report](#). The DNS Security Analysis section of the SLR report provides detailed insights into various aspects of DNS activity and threats including DNS Security Analysis (Summary), Traffic Distribution, DNS Traffic Insight, Malicious Traffic Insights, Known Malware and Families, Advanced DNS Security Resolver, and DNS Zone Misconfiguration.



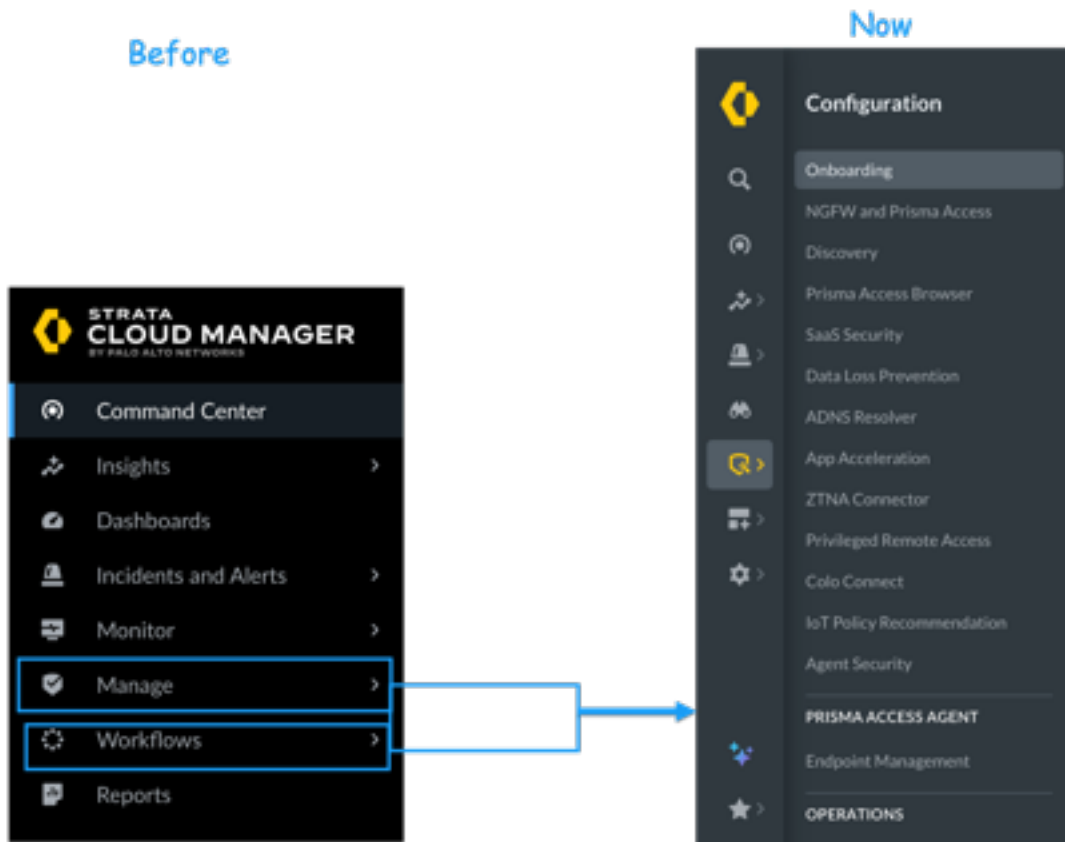
❑ Log Viewer

Log Viewer has been elevated to the first navigation level for immediate access to critical security and network logs.



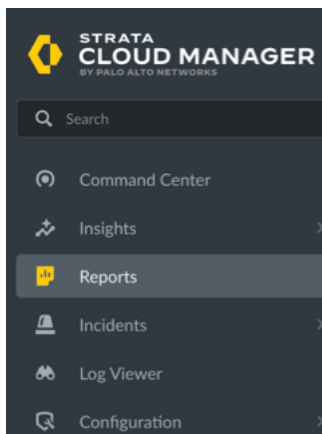
Configuration

For configuration tasks, you'll find a centralized Configuration section that brings together tasks that were previously spread across different areas in Manage and Workflows, creating a more cohesive workflow experience.



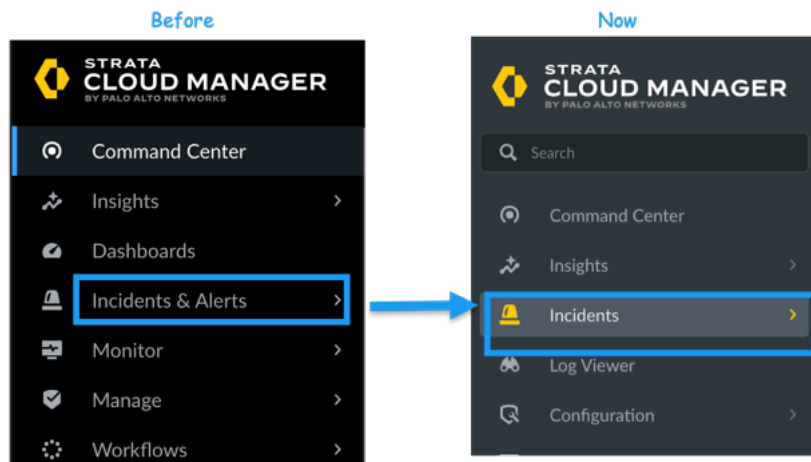
Reports

Reports allows you to download, share, or schedule delivery of reports.



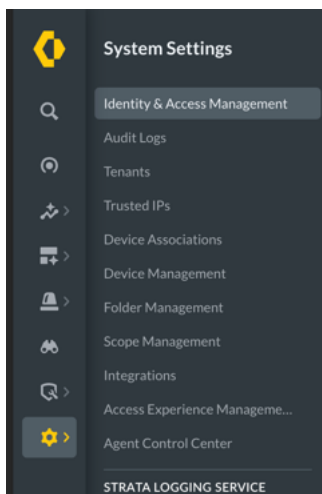
Incidents

Incidents offer a centralized view of security posture or performance anomalies.



System Settings

Renamed and positioned higher in the panel, allows you to customize user access, permissions, and other administrative preferences.



- Incidents remain unchanged, ensuring you have consistent access to support resources as you explore the new interface.

Strata Cloud Manager: Enhanced Visibility with Zero Touch Provisioning for Installers

September 25, 2025

Supported for:

- NGFW (Managed by Strata Cloud Manager)

Installers can now monitor the real-time status of the [NGFW activation during Zero Touch Provisioning \(ZTP\) deployments](#) through the ZTP Activation Page. ZTP onboarding visibility addresses the challenge that installers with minimal technical knowledge face when they have no

insight into the NGFW activation process that spans approximately 30 minutes. ZTP Activation Page now provides comprehensive bootstrap status monitoring through six sequential stages: Firewall Licensing, Content Updates, Wildfire Updates, Antivirus Updates, Routing Mode Changes, and Software Upgrades.

When you initiate NGFW activation using ZTP, you can access detailed progress information through the ZTP Activation Portal for installers and the Device Management interface for administrators. The system displays real-time status indicators for each NGFW activation stage, including spinners that provide visibility into downloads and installation.

ZTP visibility includes error handling and recovery mechanisms that allow administrators and installers to retry failed operations without requiring on-site technical support. When ZTP activation failures occur, the system provides specific error messages and retry options. For non-critical failures in antivirus or Wildfire updates, the system displays warning notifications while allowing the ZTP to continue.

Installers can also review activation history for the past 7 days through Activation History. Enhanced visibility and troubleshooting aims to reduce deployment inefficiencies and provide the seamless experience you expect from ZTP while maintaining your ability to troubleshoot issues remotely through administrator controls.

New NetSec Platform Features on Strata Cloud Manager (September 2025)

These new features follow the Strata Cloud Manager release model of [continuous feature deployment](#); as they're ready, we make them available to ensure the latest support for all products and subscriptions across the NetSec platform. There's no Strata Cloud Manager upgrade or management version requirement associated with these features; however, check if they have version or license dependencies associated with other parts of the NetSec platform (like a cloud-delivered security service subscription, or a Prisma Access version, for example).

Integrating Strata Cloud Manager Pro for NGFW with Enterprise Support Agreement (ESA)

September 26, 2025

Supported for: Strata Cloud Manager

Palo Alto Networks now enables you to leverage Strata Cloud Manager Pro for NGFW capabilities directly within your [Enterprise Support Agreements \(ESA\)](#), significantly enhancing your support experience while reducing time to resolution. This integration helps you maximize your investment in Palo Alto Networks solutions while simplifying management of your security infrastructure.

With the ESA and Strata Cloud Manager integration, you receive a single authentication code that activates both your support entitlements and Strata Cloud Manager Pro features for your NGFW deployments. This consolidation eliminates the need to purchase and manage separate subscriptions, creating a more streamlined experience. Your ESA agreement with Strata Cloud Manager Pro provides advanced monitoring, reporting, and management capabilities that help you identify and resolve security issues more quickly.

Through this integration, you gain the operational benefits of Strata Cloud Manager's advanced management capabilities combined with Palo Alto Networks support services, all within a single, cost-effective agreement that covers your entire NGFW deployment.

TechDocs Strata Copilot: Your AI Assistant on TechDocs

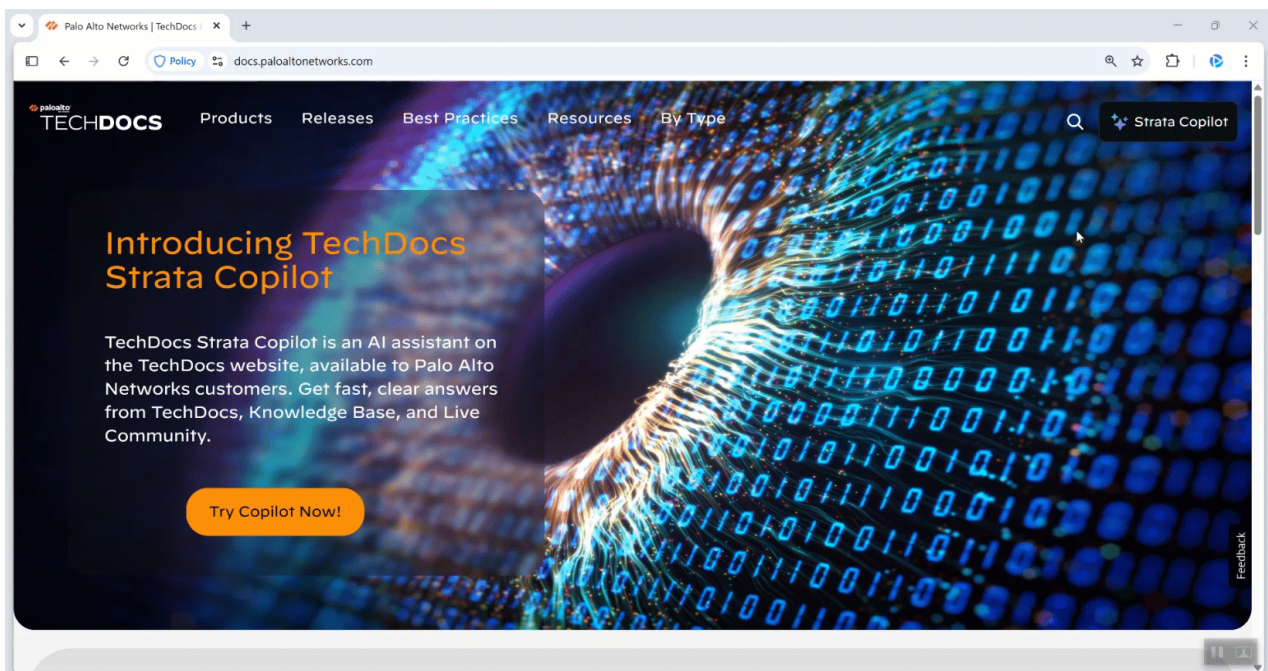
September 18, 2025

Supported on the Palo Alto Networks TechDocs website for network security products.

TechDocs Strata Copilot, an AI-powered assistant, is now available on the [Palo Alto Networks TechDocs website](#). It simplifies how you find information by letting you ask questions in natural language, which eliminates the need to search through documentation or use specific keywords.

TechDocs Strata Copilot pulls answers to your queries from a comprehensive data source, such as our Network Security Documentation, Knowledge Base articles, and LIVEcommunity. Instead of just showing you a link, TechDocs Strata Copilot provides a concise summary to give you immediate clarity.

Every answer includes direct links to the source documentation, allowing you to explore the context and verify the information. This feature enhances your self-service experience by providing instant access to critical knowledge, reducing resolution times, and helping you more efficiently manage your network security solutions.



Strata Cloud Manager: Visibility into Agent Versions for Connected Devices

September 11, 2025

Supported for: Strata Cloud Manager

[User Activity Insights](#) in Strata Cloud Manager provides clear visibility into connected gateway agent (GlobalProtect and Prisma Access) versions and subversions for connected user devices in your deployment. Previously, GlobalProtect agent version information varied by its source (Strata Logging Service, ADEM, or SaaS agent) and lacked subversion details.

You can now access both the main agent version and detailed subversion information, including patch details. The subversion details for existing GlobalProtect devices populate over a 30-day period. However, for newly added devices, the subversion details are displayed immediately upon their first connection. The GlobalProtect agent subversions are displayed for devices connected to Prisma Access only. This clear view of your agent distribution landscape helps you identify version inconsistencies and plan updates more effectively.

Strata Cloud Manager: Admin Role Profile Configuration

September 23, 2025

Supported for: NGFW (Managed by Strata Cloud Manager)

Strata Cloud Manager™ now makes it easy to create and deploy [custom admin roles](#) for managed NGFWs, allowing you to control what each administrator is allowed to do.

By setting up roles with specific permissions and assigning them to administrators you can enforce the principle of least privilege, ensuring administrators have only the access necessary for their specific job functions.

This feature gives you fine-grained control across the web interface, CLI, REST API, and XML API. You can configure detailed access permissions over various functional areas, including device configuration, network settings, security policies, monitoring capabilities, and operational tasks. For example, you can create a network admin role that has permissions to manage interfaces and routing but is restricted from changing security profiles.

By configuring custom admin roles, you can enhance your security posture, simplify compliance, and create a more organized and efficient workflow for your administrators.

Strata Cloud Manager: Custom Defined Application Settings

September 23, 2025

Supported for:

- [NGFW \(Managed by Strata Cloud Manager\)](#)
-

Strata Cloud Manager now provides users the ability to [customize predefined local and cloud-based applications](#). For each given application, you can modify the **TCP Timeout**, **TCP Half Closed**, **TCP Time Wait**, and **Risk** values to more appropriately fit the needs of your organization's network security requirements.

Strata Cloud Manager: Device Quarantine List for Cloud Managed NGFWs

September 23, 2025

Supported for: NGFW (Managed by Strata Cloud Manager)

You can now manage [device quarantine lists for NGFWs](#) acting as GlobalProtect portals and gateways directly through Strata Cloud Manager. This capability enables you to block specific devices by adding their corresponding device information to a quarantine list while using Strata Cloud Manager as your primary management interface.

When you access the device quarantine list functionality in Strata Cloud Manager, you can view quarantined devices that have been flagged by Administrators.

Strata Cloud Manager: GRE Tunnel Termination

September 23, 2025

Supported for: Strata Cloud Manager

Strata Cloud Manager allows you to configure and deploy [GRE \(Generic Routing Encapsulation\) tunnels](#) on managed NGFW platforms to establish secure, point-to-point connectivity across untrusted networks. GRE tunnels enable you to encapsulate various network layer protocols inside virtual point-to-point links, allowing you to extend your network topology across geographically distributed locations.

Strata Cloud Manager: Hardware Security Module (HSM) Integration

September 24, 2025

Supported for: Strata Cloud Manager

You can now set up a [Hardware Security Module \(HSM\)](#) to generate, store, and manage digital keys through Strata Cloud Manager. An HSM is a physical appliance that, once connected, provides both physical and logical protection of these cryptographic keys. By utilizing the management options in Strata Cloud Manager, you can specify HSM servers that use one or more of the following providers: SafeNet Network, nCipher nCshield Connect, or Thales CipherTrust Manager.

Strata Cloud Manager: Log Forwarding Card (LFC) Support

September 24, 2025

Supported for: Strata Cloud Manager

You can now configure a [PA-7000 Series Firewall Log Forwarding Card \(LFC\)](#) using Strata Cloud Manager. The LFC is a physical, high-performance slot card that forwards all dataplane logs from the firewall to an external logging system. Once installed, you can choose to configure either interface LFC 1/1 or interface LFC 1/9, as well as IPv4 or IPv6 settings, depending on your deployment needs.

Strata Cloud Manager: Master Key Management for NGFWs

September 23, 2025

Supported for: NGFW (Managed by Strata Cloud Manager)

Now you can deploy a custom [master key](#) in **Strata Cloud Manager™** to replace the default master key on your next-generation firewalls (NGFWs), adding an extra layer of protection for your sensitive data.

When you deploy a new master key, Strata Cloud Manager re-encrypts all key material to strengthen your security posture. You can define a custom lifetime for the master key (from 1 to 18, 250 days) and set reminder notifications (1 to 365 days before expiration). This allows you to rotate keys on schedule to help minimize disruption. Regular rotation is a best practice for cryptographic key management and helps you meet compliance requirements.

The **Deploy Master Key** feature supports both standalone and high-availability (HA) firewall configurations, with built-in validations to ensure secure key deployment.

Strata Cloud Manager: Netflow Monitoring

September 23, 2025

Supported for: NGFW (Managed by Strata Cloud Manager)

Strata Cloud Manager™ now provides the ability to configure and deploy [NetFlow](#) on managed next-generation firewall (NGFW) platforms. This new capability allows you to export detailed IP traffic statistics to a NetFlow collector, providing valuable data for security analysis, troubleshooting, and performance optimization. You can create server profiles to define collector destinations and export parameters, with support for Layer 3, Layer 2, virtual wire, tap, VLAN, loopback, and tunnel interfaces. This feature supports NetFlow Version 9 and both standard and enterprise templates.

Strata Cloud Manager: Policy Application Dependency Management

September 23, 2025

Supported for:

- [NGFW \(Managed by Strata Cloud Manager\)](#)
-

Strata Cloud Manager (SCM) now provides users the ability to view all dependent applications associated with a selected application while [creating Security Policy Rules](#). This makes it easier to build security policies without unintentionally excluding required dependent applications. To view the dependent applications, access the relevant Security Policy Rule, and from the **Application / Service** menu, open the **Application** dropdown and select the **Dependent Applications** button. This opens the **Dependent Applications** pane, which displays all dependent apps contained within the selected application it relies on, as well as the rules they are used in. Additionally, you can also add these dependencies directly to your current rule or an existing rule.

Strata Cloud Manager: QoS Support

September 23, 2025

Supported for:

- [NGFW \(Managed by Strata Cloud Manager\)](#)
-

QoS enables you to prioritize and manage network traffic to ensure critical applications and services receive the necessary bandwidth and resources.

You can now configure QoS on the next-generation firewalls in Strata™ Cloud Manager. Enable [QoS capabilities](#) on NGFWs through the following configuration components for traffic prioritization and bandwidth management:

QoS Profile

- Defines traffic classification rules and bandwidth allocation parameters
- Establishes service level priorities for different application types
- Configures queue management and traffic shaping policy rules

QoS Policy

- Applies QoS Profiles to specific traffic flows based on defined criteria
- Implements rule-based traffic classification and prioritization
- Enables granular control over application and user-based QoS enforcement

QoS Egress Interface Configuration

- Designates network interfaces for QoS policy rule enforcement
- Configures outbound traffic shaping and bandwidth limits
- Ensures proper queue management at interface level

By implementing QoS, you can improve overall network efficiency, enhance user experience for critical services, and align network resource allocation with your organization's priorities. With QoS, you can maximize the value of your existing network infrastructure while ensuring that your most important traffic always gets through, even during periods of high network utilization.

Strata Cloud Manager: Response Page Customization

September 23, 2025

Supported for:

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

Strata Cloud Manager™ now offers expanded [response](#) page customization, allowing you to tailor additional page types for a more consistent and user-friendly experience. These pages appear

during authentication challenges, security restrictions, or informational notices, helping users understand what is happening while maintaining your organization's branding.

Newly supported customizable pages include:

- **GlobalProtect:** Customize portal login pages, welcome screens, and help pages that guide users through the connection process.
- **Authentication Services:** Modify Multi-Factor Authentication (MFA) login pages and SAML authentication error pages to provide clear guidance during authentication challenges.
- **SSL Decryption:** Customize notification pages to inform users about traffic inspection policies and certificate errors.

Panorama to Strata Cloud Manager Migration for NGFWs

Supported for: NGFW (Managed by Panorama)

If you use Panorama to manage your organizations NGFWs, [you can migrate your configurations to Strata Cloud Manager for the benefits of cloud management](#).

Strata Cloud Manager enables you to migrate your organizations NGFW hierarchy and configurations:

- ❑ **Complete migration visibility and control** — Accept and validate Panorama running configurations with pre-migration identification of unsupported elements.
- ❑ **Flexible migration options** — Choose partial or complete configuration migration based on your requirements.
- ❑ **Conflict prevention** — Automatic detection and display of previously migrated elements during subsequent migrations.
- ❑ **Automated validation** — Minimize the risk of configuration errors that could impact network security.
- ❑ **Configuration continuity** — Maintain your previous configurations throughout the migration process.

For the benefits of moving to Strata Cloud Manager, click [here](#).

Flexible Software Upgrades for NGFWs

September 23, 2025

Supported on:

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

Administrators can now [skip reboots during PAN-OS software upgrades for cloud managed NGFWs](#), allowing you to decouple software installation from the reboot process and providing granular control over when your NGFWs restart after receiving software updates. You can schedule software downloads and installations to complete during designated maintenance

windows while deferring the actual reboot to a time that minimizes operational impact on your network services. This separation of upgrade phases prevents unexpected downtime during critical business hours and allows you to coordinate reboots across multiple firewalls in your environment.

You configure this feature through the **Software Upgrade Scheduler** and configure the update to work with the needs of your business and network.

Strata Cloud Manager: Management Features

September 23, 2025

Supported for:

- [NGFW \(Managed by Strata Cloud Manager\)](#)
-

Strata Cloud Manager now provides comprehensive IPv6 capabilities to help you manage your network infrastructure in dual-stack environments. This enhancement brings IPv6 parity with PAN-OS management capabilities, allowing you to configure and manage both IPv4 and IPv6 addressing across your NGFW deployments through the cloud management platform.

You [can now configure IPv6 addressing for management interfaces including dedicated management](#) ports and auxiliary interfaces. The management interface configuration supports both static IPv6 addressing and dynamic DHCPv6 client options with configurable parameters such as non-temporary address options, temporary address options, rapid commit, and DUID type selection. For auxiliary interfaces, you can specify IPv6 addresses with prefix lengths and configure default IPv6 gateways to ensure proper routing in your management network.

Strata Cloud Manager: IPv6 Service Route Configuration

September 23, 2025

Supported for: Strata Cloud Manager

You can configure a data port (a regular interface) to access external services, such as DNS servers, external authentication servers, Palo Alto Networks® services such as software, URL updates, licenses and AutoFocus. Strata Cloud Manager now supports configuring and deploying [IPv6 service routes](#) (in addition to IPv4 service routes) for all managed NGFW platforms.

Strata Cloud Manager: Management Service Route

September 23, 2025

Supported for: Strata Cloud Manager

The firewall uses the management (MGT) interface by default to access external services, such as DNS servers, external authentication servers, Palo Alto Networks® services such as software, URL updates, licenses and AutoFocus. An alternative to using the MGT interface is to configure a data port (a regular interface) to access these services. A service route is the path from the interface to

the service on a server. Strata Cloud Manager allows you to [customize service routes](#) for various services or Use Management Interface for all services.

Strata Cloud Manager: NDP Proxy

September 23, 2025

Supported for: Strata Cloud Manager

Strata Cloud Manager now supports Neighbor Discovery Protocol (NDP) Proxy to simplify address resolution in IPv6 environments. This feature allows the firewall to respond to link-layer address requests on behalf of devices behind it, performing a similar function to ARP for IPv4. Configuring NDP Proxy is required when you enable [IPv6-to-IPv6 Network Prefix Translation \(NPTv6\)](#). Key capabilities of NDP Proxy include:

- **Simplified Address Resolution:** The firewall automatically responds to Neighbor Solicitation messages for configured IPv6 prefixes.
- **Selective Proxying:** You can specify addresses for which the firewall will not act as a proxy (negated addresses).

Strata Cloud Manager: NGFW Alerts in September

September 22, 2025

Here are the [NGFW alerts](#) introduced in September 2025:

- Invalid or Missing Device Certificate for CDSS
 - Device Certificate Auto-Renewal May Fail – PAN-OS Upgrade Required
-

Health [alerts](#) actively monitor the health and performance of your platform in real time. This approach helps in identifying issues, predicting potential problems, and implementing remediation actions to ensure your devices function optimally. Here are some key aspects:

- **Monitoring Metrics:** Continuously monitor various metrics from the NGFWs, including CPU utilization, memory usage, disk space, network throughput, and other relevant performance indicators.
- **Anomaly Detection:** Generate alerts that dynamically adjust based on the metric's historical value and your usage trends.
- **Predictive Analysis:** Leverage historical data and patterns to predict when thresholds might be exceeded or specific events may occur. This helps forecast potential issues before they escalate.

Strata Cloud Manager: Support for Gen 5 Hardware with Zero Touch Provisioning

September 23, 2025

Supported for:

- NGFW (Managed by Strata Cloud Manager)
-

You can now use [Zero Touch Provisioning \(ZTP\)](#) to deploy Gen 5 hardware through [Strata Cloud Manager](#) with enhanced device-specific QR codes that contain your device's serial number and claim key. When you scan the QR code on your [PA-500](#) or [PA-5500](#) series NGFWs, you are automatically directed to the ZTP Activation page with the serial number and claim key pre-populated, eliminating the need for manual data entry and reducing input errors during onboarding.

New Features in August 2025

Here are the new features we've added to Strata Cloud Manager in August 2025.

- [2025.R4.0 Configuration Management Features](#)
- [NetSec Platform Features](#)

New Strata Cloud Manager Management Features (August 2025)

Here's the new [configuration management](#) features we've added to Strata Cloud Manager in August 2025; we use a scheduled upgrade to deliver these features to you and they are supported with the Cloud Manager 2025.R4.0 release version. Check your Strata Cloud Manager in-product notifications for updates on the release upgrade schedule. You can verify which Strata Cloud Manager release version you're running by navigating to your [configuration overview](#), and checking the **Cloud Management Version**.

Strata Cloud Manager: Best Practice Check for GlobalProtect Portal Traffic

August 15, 2025

Supported for:

- [NGFW \(Managed by Strata Cloud Manager\)](#)
-

The [Strata Cloud Manager Best Practice Check](#) now evaluates your configuration for the presence of a Vulnerability Protection profile that corresponds to Palo Alto Networks Best Practices for traffic destined to a GlobalProtect portal or gateway services when configured to allow. This is intended to prevent accidental deployment of security profiles that might inadvertently place the GlobalProtect interface at risk of attack using published product security vulnerabilities.

Strata Cloud Manager: Configuration Management Support by Region

August 15, 2025

Supported on:

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

Strata Cloud Manager now supports the following additional regions:

- Korea
 - Poland
 - France
 - Spain
 - South Africa
-

Strata Cloud Manager for Configuration Management is a solution that is defined and controlled based on the region where it is deployed. You can deploy Strata Cloud Manager in the locations of your choosing, based on data location preferences and where you have the most users. For this reason, we are rolling out region-specific support for Strata Cloud Manager as soon as we are able to do so for [each region](#).

Update:

Strata Cloud Manager now supports the following additional regions:

- France
- South Africa

Strata Cloud Manager: UI Enhancements

August 15, 2025

Supported on:

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

Strata Cloud Manager now includes several web interface enhancements to improve your configuration management experience. These updates optimize workflows and provide greater visibility into your network security settings.

Changes include:

- Timestamps for configuration entities: You can now see when rules were last modified with timestamps available for all configuration entities.

Security Policy Page Improvements

- Edit objects such as addresses directly on the **Security Policy** page if they're in the same scope.
- When adding or editing rules, you can choose a higher-level location for object placement, or create new objects such as applications directly in your current scope or the application's location.
- Click on an application to edit it, or create a new application in a different location.
- Visual identification has been improved with new icons for **Web Security Rules**, **Security Rules**, and **Addresses**.
- A new **Rule Type** column shows the rule type for each policy in the Security Policy Rule page. The default is Universal. You can also select Intrazone or Interzone.

Snippet Association page Improvements

- On the **Configuration > NGFW and Prisma Access > Overview > Configuration Snippets > Associate Snippets** page, you can now reorder overriding rules with drag and drop.
- Move the global default rule, or move snippets within a rulebase using the **Move** option.
- A confirmation prompt now appears before deleting a snippet, reducing the risk of accidental removals.

Objects > Applications page Enhancements

- The **Objects > Applications** page now includes filters to view applications by Custom or Tagged applications.

Strata Cloud Manager: Support for Cross-service Configuration Sharing

August 15, 2025

Supported for:

- Strata Cloud Manager
-

Shared configuration management eliminates the complexity of managing security policies across multiple Palo Alto Networks services by allowing other Palo Alto Networks services [to subscribe to and receive configuration objects from Strata Cloud Manager](#). Shared configuration management allows you to independently implement features without introducing inconsistencies or delays by providing a unified way for subscribers like Prisma SD-WAN Controller or [Branch Sites for Prisma SD-WAN](#) devices to access and use Strata Cloud Manager managed NGFW and Prisma Access configurations.

Palo Alto Networks services can access Strata Cloud Manager configuration objects on a read-only basis while maintaining proper synchronization and usage tracking. Shared configurations enable you to share Security Profiles such as Threat Prevention, Anti-Spyware, Vulnerability Protection, URL Filtering, and DNS Security with Prisma SD-WAN Controller instances. You can track which shared objects are actively referenced by external services, and Strata Cloud

Manager automatically blocks deletion of configuration objects that are currently in use by external subscribers to prevent configuration conflicts.

When making pushes to other services, reverting those pushes should be avoided as it may cause issues with your configuration.

New NetSec Platform Features on Strata Cloud Manager (August 2025)

These new features follow the Strata Cloud Manager release model of [continuous feature deployment](#); as they're ready, we make them available to ensure the latest support for all products and subscriptions across the NetSec platform. There's no Strata Cloud Manager upgrade or management version requirement associated with these features; however, check if they have version or license dependencies associated with other parts of the NetSec platform (like a cloud-delivered security service subscription, or a Prisma Access version, for example).

Strata Cloud Manager: NGFW Alerts in August

August 29, 2025

Here are the [NGFW alerts](#) introduced in August 2025:

- Firewall Logs Getting Discarded
 - Firewall Losing Logs
-

Health [alerts](#) actively monitor the health and performance of your platform in real time. This approach helps in identifying issues, predicting potential problems, and implementing remediation actions to ensure your devices function optimally. Here are some key aspects:

- **Monitoring Metrics:** Continuously monitor various metrics from the NGFWs, including CPU utilization, memory usage, disk space, network throughput, and other relevant performance indicators.
- **Anomaly Detection:** Generate alerts that dynamically adjust based on the metric's historical value and your usage trends.
- **Predictive Analysis:** Leverage historical data and patterns to predict when thresholds might be exceeded or specific events may occur. This helps forecast potential issues before they escalate.

Accelerate Insights and Enhance Security with Telemetry Autoenablement

August 28, 2025

Supported for:

- Strata Cloud Manager
 - Introduced in PAN-OS 11.2.8 and 12.1.2
-

[Telemetry autoenablement](#) for Palo Alto Networks devices streamlines the activation and configuration of telemetry, eliminating complex workflows and manual setup. This feature ensures that upon device onboarding, telemetry is automatically enabled and configured to stream data to the correct data residency region, determined by your location or existing configurations.

Strata Cloud Manager or hub now manages telemetry settings, rather than individual Panorama or firewall devices. These services store information for all devices within a tenant service group (TSG), simplifying and automating telemetry configuration. This approach removes operational hurdles, enabling full utilization of telemetry's benefits while maintaining control over data sharing preferences.

Consistent telemetry data streaming provides enhanced security, faster security responses, and access to advanced features through critical threat insights. Telemetry autoenablement ensures your devices send valuable diagnostic and usage information, significantly improving support case resolution times and offering real-time insights into performance, usage, and potential issues.

You have the ability to [manage your telemetry settings](#) at the TSG level, including the option to change the telemetry tier from Full to Diagnostic through the hub interface or Strata Cloud Manager. This tiered approach ensures you can choose the level of information shared while adhering to data privacy requirements. Additionally, all telemetry configuration changes are logged for audit purposes, assisting with compliance and security policy adherence.

Admin Role Profile Configuration

August 15, 2025

Supported for:

- [NGFW \(Managed by Strata Cloud Manager\)](#)
-

Strata Cloud Manager™ now makes it easy to create and deploy [custom admin roles](#) for managed NGFWs, allowing you to control what each administrator is allowed to do.

By setting up roles with specific permissions and assigning them to administrators you can enforce the principle of least privilege, ensuring administrators have only the access necessary for their specific job functions.

This feature gives you fine-grained control across the web interface, CLI, REST API, and XML API. You can configure detailed access permissions over various functional areas, including device configuration, network settings, security policies, monitoring capabilities, and operational tasks. For example, you can create a network admin role that has permissions to manage interfaces and routing but is restricted from changing security profiles.

By configuring custom admin roles, you can enhance your security posture, simplify compliance, and create a more organized and efficient workflow for your administrators.

Strata Cloud Manager: Custom Defined Application Settings

August 15, 2025

Supported for:

- [NGFW \(Managed by Strata Cloud Manager\)](#)
-

Strata Cloud Manager now provides users the ability to [customize predefined local and cloud-based applications](#). For each given application, you can modify the **TCP Timeout**, **TCP Half Closed**, **TCP Time Wait**, and **Risk** values to more appropriately fit the needs of your organization's network security requirements.

Support for Cross-service Configuration Sharing

August 15, 2025

Supported for:

- Strata Cloud Manager
-

Shared configuration management eliminates the complexity of managing security policies across multiple Palo Alto Networks services by allowing other Palo Alto Networks services to [subscribe to and receive configuration objects from Strata Cloud Manager](#). Shared configuration management allows you to independently implement features without introducing inconsistencies or delays by providing a unified way for subscribers like Prisma SD-WAN Controller or [Branch Sites for Prisma SD-WAN Ion](#) devices to access and use Strata Cloud Manager managed NGFW and Prisma Access configurations.

Palo Alto Networks services can access Strata Cloud Manager configuration objects on a read-only basis while maintaining proper synchronization and usage tracking. Shared configurations enable you to share Security Profiles such as Threat Prevention, Anti-Spyware, Vulnerability Protection, URL Filtering, and DNS Security with Prisma SD-WAN Controller instances. You can track which shared objects are actively referenced by external services, and Strata Cloud Manager automatically blocks deletion of configuration objects that are currently in use by external subscribers to prevent configuration conflicts.

When making pushes to other services, reverting those pushes should be avoided as it may cause issues with your configuration.

Strata Cloud Manager: IPv6 Route Configuration

August 15, 2025

Supported on:

- NGFW (Managed by Strata Cloud Manager)
-

You can configure a data port (a regular interface) to access external services, such as DNS servers, external authentication servers, Palo Alto Networks® services such as software, URL updates, licenses and AutoFocus. Strata Cloud Manager now supports configuring and deploying [IPv6 service routes](#) (in addition to IPv4 service routes) for all managed NGFW platforms.

Strata Cloud Manager: IPv6 Support

August 15, 2025

Supported for:

- [NGFW \(Managed by Strata Cloud Manager\)](#)
-

[Strata Cloud Manager](#) now provides IPv6 address support for many configurations. The following areas support both IPv4 and IPv6 addresses in the IP address fields.

- Management
 - RADIUS
 - LDAP
 - Kerberos
 - TACACS+
 - SSH Management
 - Aux1 and Aux2
 - Web Interface
 - NTP
 - Device DNS
- Security
 - Zone Protection Profile
 - Packet-Based Attack Protection
 - Reconnaissance Protection
- Networking
 - IPv6 Static Routes
 - Policy-Based Forwarding (PBF)
 - Dual Stack Support for L3 Interfaces
 - Neighbor Discovery and Duplicate Address Detection
 - NAT64 (IP to IPv6 Protocol Translation)
 - Link Layer Discovery Protocol (LLDP)
 - Bidirectional Forwarding Detection (BFD)
- User-ID
 - Captive Portal for IPv6

- Host Dynamic Address Configuration
 - DHCP Relay
 - SLAAC (Router Advertisements)
 - SLAAC (Router Preferences)
 - SLAAC (RDNSS)
- VPN
 - IKE Gateway
 - IPSec Tunnel
 - IKEv2
 - IPv6 over IPv4 IPSec Tunnel

Strata Cloud Manager: GRE Tunnel Termination

August 15, 2025

Supported for: Strata Cloud Manager

Strata Cloud Manager allows you to configure and deploy [GRE \(Generic Routing Encapsulation\) tunnels](#) on managed NGFW platforms to establish secure, point-to-point connectivity across untrusted networks. GRE tunnels enable you to encapsulate various network layer protocols inside virtual point-to-point links, allowing you to extend your network topology across geographically distributed locations.

Master Key Management for NGFWs

August 15, 2025

Supported for:

- [NGFW \(Managed by Strata Cloud Manager\)](#)
-

Now you can deploy a custom [master key](#) in **Strata Cloud Manager™** to replace the default master key on your next-generation firewalls (NGFWs), adding an extra layer of protection for your sensitive data.

When you deploy a new master key, Strata Cloud Manager re-encrypts all key material to strengthen your security posture. You can define a custom lifetime for the master key (from 1 to 18, 250 days) and set reminder notifications (1 to 365 days before expiration). This allows you to rotate keys on schedule to help minimize disruption. Regular rotation is a best practice for cryptographic key management and helps you meet compliance requirements.

The **Deploy Master Key** feature supports both standalone and high-availability (HA) firewall configurations, with built-in validations to ensure secure key deployment.

Strata Cloud Manager: Log Forwarding Card (LFC) Support

August 15, 2025

Supported for:

- [NGFW \(Managed by Strata Cloud Manager\)](#)
-

You can now configure a [PA-7000 Series Firewall Log Forwarding Card \(LFC\)](#) using Strata Cloud Manager. The LFC is a physical, high-performance slot card that forwards all dataplane logs from the firewall to an external logging system. Once installed, you can choose to configure either interface LFC 1/1 or interface LFC 1/9, as well as IPv4 or IPv6 settings, depending on your deployment needs.

Netflow Monitoring

August 15, 2025

Supported for:

- [NGFW \(Managed by Strata Cloud Manager\)](#)
-

Strata Cloud Manager™ now provides the ability to configure and deploy [NetFlow](#) on managed next-generation firewall (NGFW) platforms. This new capability allows you to export detailed IP traffic statistics to a NetFlow collector, providing valuable data for security analysis, troubleshooting, and performance optimization. You can create server profiles to define collector destinations and export parameters, with support for Layer 3, Layer 2, virtual wire, tap, VLAN, loopback, and tunnel interfaces. This feature supports NetFlow Version 9 and both standard and enterprise templates.

Response Page Customization

August 15, 2025

Supported for:

- [NGFW \(Managed by Strata Cloud Manager\)](#)
-

Strata Cloud Manager™ now offers expanded [response](#) page customization, allowing you to tailor additional page types for a more consistent and user-friendly experience. These pages appear during authentication challenges, security restrictions, or informational notices, helping users understand what is happening while maintaining your organization's branding.

Newly supported customizable pages include:

- **GlobalProtect:** Customize portal login pages, welcome screens, and help pages that guide users through the connection process.
- **Authentication Services:** Modify Multi-Factor Authentication (MFA) login pages and SAML authentication error pages to provide clear guidance during authentication challenges.

- **SSL Decryption:** Customize notification pages to inform users about traffic inspection policies and certificate errors.

Strata Cloud Manager: Hardware Security Module (HSM) Integration

August 15, 2025

Supported for:

- [NGFW \(Managed by Strata Cloud Manager\)](#)
-

You can now set up a [Hardware Security Module \(HSM\)](#) to generate, store, and manage digital keys through Strata Cloud Manager. An HSM is a physical appliance that, once connected, provides both physical and logical protection of these cryptographic keys. By utilizing the management options in Strata Cloud Manager, you can specify HSM servers that use one or more of the following providers: SafeNet Network, nCipher nCshield Connect, or Thales CipherTrust Manager.

Strata Cloud Manager: Management Service Route

August 28, 2025

Supported for: Strata Cloud Manager

The firewall uses the management (MGT) interface by default to access external services, such as DNS servers, external authentication servers, Palo Alto Networks® services such as software, URL updates, licenses and AutoFocus. An alternative to using the MGT interface is to configure a data port (a regular interface) to access these services. A service route is the path from the interface to the service on a server. Strata Cloud Manager allows you to [customize service routes](#) for various services or Use Management Interface for all services.

Strata Cloud Manager: Policy Application Dependency Management

August 15, 2025

Supported for:

- [NGFW \(Managed by Strata Cloud Manager\)](#)
-

Strata Cloud Manager (SCM) now provides users the ability to view all dependent applications associated with a selected application while [creating Security Policy Rules](#). This makes it easier to build security policies without unintentionally excluding required dependent applications. To view the dependent applications, access the relevant Security Policy Rule, and from the **Application / Service** menu, open the **Application** dropdown and select the **Dependent Applications** button. This opens the **Dependent Applications** pane, which displays all dependent apps contained within the selected application it relies on, as well as the rules they are used in. Additionally, you can also add these dependencies directly to your current rule or an existing rule.

Strata Cloud Manager Command Center: Fair Metric Classification for ADEM Operational Health View and Widgets

August 1, 2025

Supported for: Strata Cloud Manager

The Operational Health view and **User Device Experience** widgets in the Strata Cloud Manager **Command Center** now display **Fair** metrics alongside the existing **Good** and **Poor** performance indicators, providing you with more granular visibility into user session quality and network performance degradation levels. This enhanced categorization helps you better identify and address performance issues that fall between optimal and severely degraded states, enabling more precise troubleshooting and policy optimization decisions.

Strata Cloud Manager: Virtual Routers

August 15, 2025

Supported on:

- NGFW (Managed by Strata Cloud Manager)
-

[Virtual router support for cloud managed NGFWs](#) addresses some configuration gaps in Strata Cloud Manager by implementing missing capabilities that are present in Panorama, enabling seamless migration for customers with existing virtual router deployments. You benefit from this enhancement when migrating from Panorama to Strata Cloud Manager because it eliminates configuration blockers that would otherwise prevent successful migration or require extensive reconfiguration of your routing protocols. The feature specifically targets configuration options identified in current Panorama deployments, ensuring that your existing BGP, OSPF, and static routing configurations can be preserved during the migration process.

You can configure enhanced BGP parameters including authentication profiles with secret keys, dampening profiles with configurable cutoff and decay settings, advanced peer connection options such as idle hold time and incoming connection management, and sophisticated route aggregation with suppress filters. The feature provides expanded OSPF capabilities including MD5 authentication profiles with key management, password-based authentication options, and enhanced area configuration parameters. You also gain access to improved static routing options including next virtual router capabilities and advanced route table configurations for both IPv4 and IPv6 implementations.

New Features in July 2025

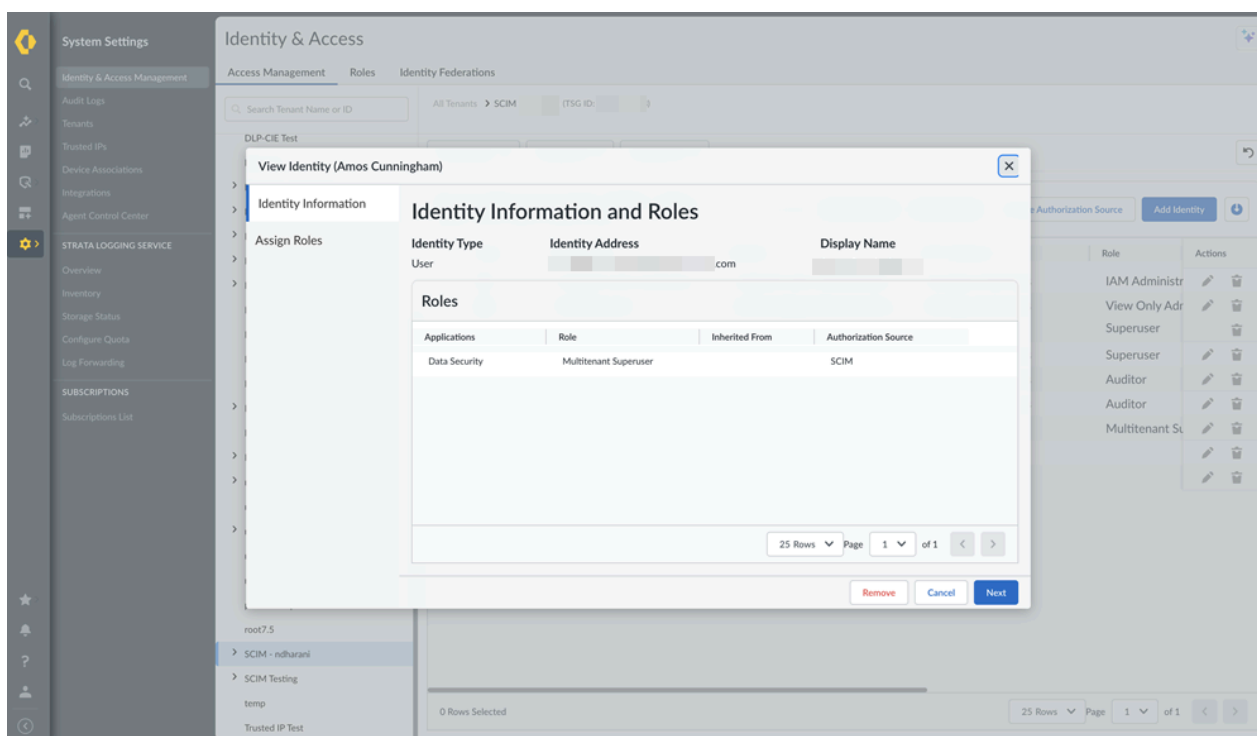
Features listed here include some feature highlights for the [products supported with](#) Strata Cloud Manager.

Identity and Access Management Support for SCIM

now supports the use of a [System for Cross-domain Identity Management \(SCIM\)](#) for identity and access management, allowing you to automatically provision and manage user access through your existing identity provider systems. This integration enhances 's security capabilities by enabling synchronization of user provisioning between your organization's identity systems and , addressing a critical need for consistent access management across cloud applications.

The SCIM implementation is fully compliant with core schemas (RFC 7643) and protocols (RFC 7644), providing a standardized approach to identity management. Currently, supports SailPoint as an identity provider for SCIM integration. You can use this feature to automate the creation, modification, and deletion of users and their access policies within directly from your SailPoint identity provider system. The SCIM leverages OAuth 2.0 Client Credentials for authentication, using service account credentials from your Tenant Service Group (TSG).

When you enable SCIM for your tenant, you can choose SCIM as an authorization source for managing access policies. You also have the option to choose authorization sources independently, giving you flexibility in how you manage user access. The SCIM integration is particularly valuable for organizations with large user bases where manual user provisioning across multiple systems would be inefficient and error-prone.



The implementation includes the ability to manage users, groups (access policies), and service accounts, allowing your identity management system to perform all necessary operations on identities. This integration helps ensure that when users change roles or leave your organization, their access rights are automatically updated across all connected systems, maintaining security and compliance with your organization's access policies.

By supporting SCIM, enables you to maintain a single source of truth for identity management, reducing administrative overhead and improving security by ensuring consistent and up-to-date access controls across your cloud environments.

Strata Copilot: New Region Support

Strata Copilot now extends its reach to [new regions](#), enhancing global accessibility. This expansion brings the powerful AI-driven assistance to users in South Africa. By increasing geographical coverage, Strata Copilot offers more organizations the opportunity to streamline their security operations, leverage intelligent insights, and improve overall efficiency in managing their Palo Alto Networks solutions in Strata Cloud Manager across these diverse locations.

Strata Copilot now supports the following additional regions:

- South Africa

Enhanced IOC Search Functionality in Strata Cloud Manager

The [Strata Cloud Manager IOC Search](#) functionality has been enhanced to help you identify and prioritize security threats by providing comprehensive context for various indicators of compromise. The IOC Search is powered by the Strata Logging Service, a cohesive cloud-based logging solution for personalized network security analytics, giving you deeper insights into potential threats across your environment.

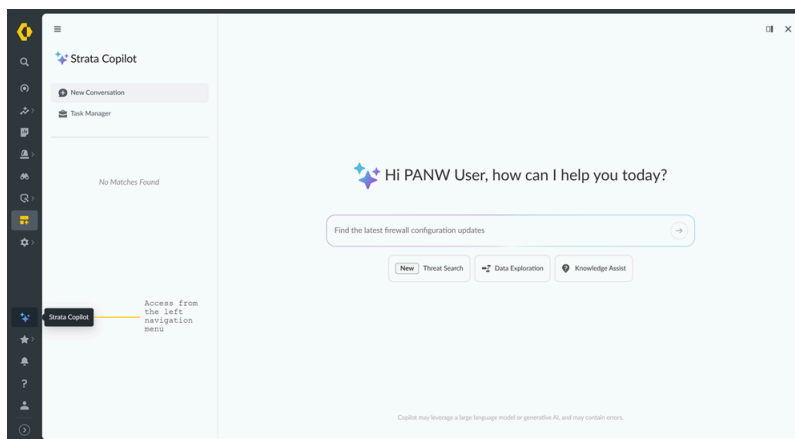
When you search for indicators such as domains, URLs, file hashes (SHA-256), IP addresses (IPv4 and IPv6), you receive detailed threat context and data telemetry specific to your tenant, your industry, and the global threat landscape. This multi-level visibility allows you to understand not only whether a specific indicator is malicious, but also its prevalence in your organization, and across the Palo Alto Networks customer base.

For each indicator you search, you can also view associated tags that provide additional context about the threats, helping you understand potential threat actor attribution, or if it is associated to a malware campaign, why it is deemed malicious.

As you investigate potential security incidents, the IOC Search gives you the enriched insights needed to make informed decisions about prioritization and response, ultimately helping you focus your security team's efforts on the most significant threats to your organization.

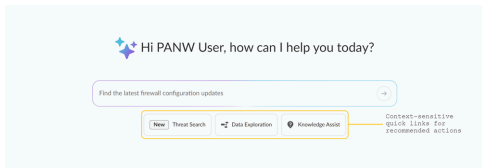
Strata Copilot: Accessibility Change

[Strata Copilot](#) has been redesigned to deliver more efficient intelligent assistance within Strata Cloud Manager. The updated interface will roll out in phases throughout July. Once deployed to your Strata Cloud Manager instance, you'll find Strata Copilot accessible directly from the left navigation panel, seamlessly integrating into your existing workflow.



The redesigned interface maintains visual consistency with Strata Cloud Manager by supporting both light and dark themes and featuring a responsive design that adapts to any screen size. For complex tasks requiring maximum screen space, you can collapse the navigation menu while retaining full access to chat functionality through the consistently placed chat box available on every page.

When you launch Strata Copilot, you will receive a personalized welcome message with suggested topics to help you quickly address common security management scenarios. As you interact with the system, contextually relevant prompts appear to guide your queries and help you formulate effective questions.



Strata Copilot now provides explanations and technical references within conversations to help you understand the reasoning behind suggestions. Complex information is presented in a structured format with specialized display components that improve comprehension of technical content.

In addition, the Best Practice Assessment functionality within Strata Copilot has also been enhanced to provide more comprehensive security insights, enabling you to evaluate your security posture without leaving the Copilot interface. This integration streamlines your security assessment workflows and provides immediate access to actionable information to improve your security stance.

Direct Users in Activity Insights

July 18, 2025

Supported for: Strata Cloud Manager

Managing network visibility and operational efficiency across diverse deployments like Prisma Access and NGFW often requires juggling multiple dashboards, leading to fragmented analysis. [Activity Insights](#) solves this critical challenge by giving you an in-depth, consolidated view of your network activities across Prisma Access and NGFW deployments. Activity Insights brings together the visualization, monitoring, and reporting capabilities from [dashboards](#) like Application Usage, Network Usage, User Activity, and Threat Insights, providing all this data in a single, unified view.

Activity Insights pairs with the new [Strata Cloud Manager Command Center](#) homepage ; for anomalies, security gaps, degraded user experiences, impacts on security and health of your network that the homepage surfaces, you can drill down into Activity Insights and other [dashboards](#) to investigate and assess next steps.

Activity Insights provides a unified view of network data in relation to applications, users, threats, URLs, and network usage. You can also view the performance of Prisma SD-WAN applications with details on health score over a time range, transaction statistics, and bandwidth utilization metrics. The advanced reporting functionality enables you to download, share, and schedule reports that cover the data in the Overview tab. The report presents data separately for each filter applied in Activity Insights.

Furthermore, Activity Insights now displays direct users who connect to your network infrastructure while disconnected from **GlobalProtect®**. Previously, ADEM collected event information for these users, but Activity Insights did not show them. Now, you can gain complete visibility into network activity regardless of connection status, significantly improving analysis and reporting capabilities.

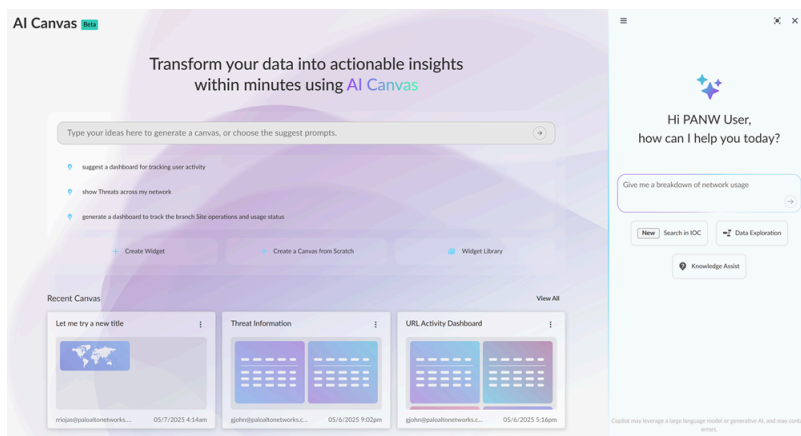
New Features in June 2025

Features listed here include some feature highlights for the [products supported with](#) Strata Cloud Manager.

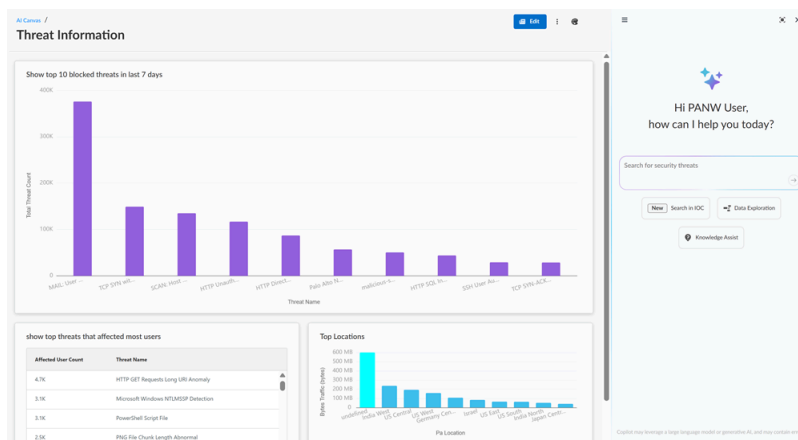
Strata Copilot: AI Canvas (Beta)

June 23, 2025

Supported for: Strata Cloud Manager



AI Canvas addresses the challenge of essential security data being hidden behind multiple clicks and filters by empowering you to interact with your data in real-time through natural language queries. When troubleshooting security issues, you often need to navigate between different dashboards and pages to piece together scattered information, which slows down your response time. With AI Canvas, you can ask questions, dynamically refine queries, and instantly uncover insights without complex queries or navigating through multiple screens.



The platform offers an intuitive, no-code interface that simplifies the creation of custom canvases and data visualization widgets tailored to your specific needs. You can easily create widgets through Strata Copilot or the AI Canvas search bar using natural language, then assemble these widgets into comprehensive dashboards with a drag-and-drop interface. The widgets provide

clear, actionable information while respecting your role-based access controls, ensuring you only see data you're authorized to access.

You can share your created canvases with others using shareable links, export visualizations in various formats, and apply canvas-level time filters that dynamically update all widgets simultaneously. In its first release, AI Canvas supports Prisma Access data and will progressively expand to include other Strata Cloud Manager areas. This integrated approach eliminates the need to export data to third-party BI tools for deeper analysis.

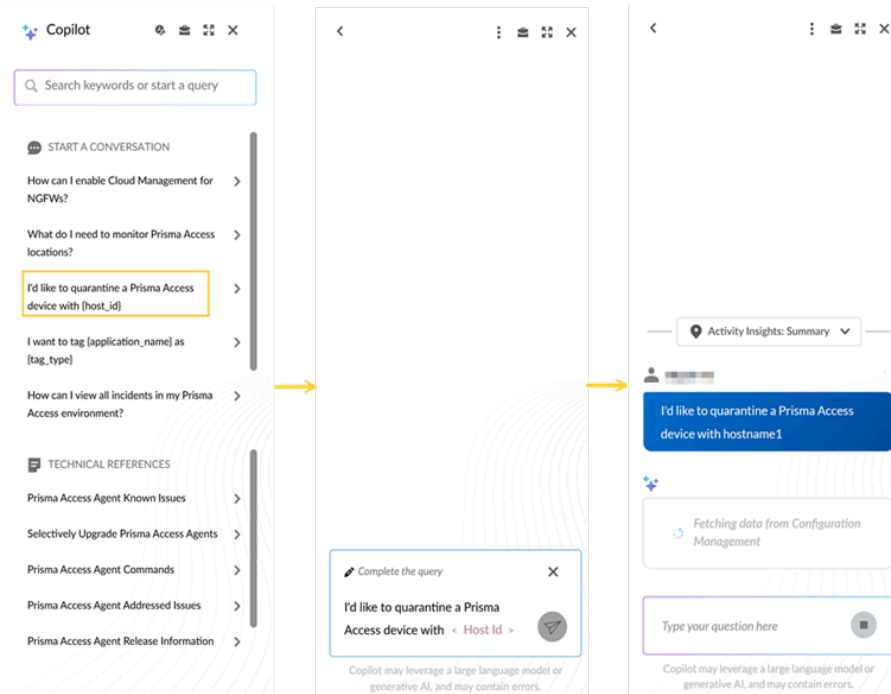
AI Canvas transforms your data exploration into a streamlined, interactive, and collaborative experience that accelerates decision-making and enhances your operational efficiency in managing network security environments.

Strata Copilot: Quarantine a Device

June 23, 2025

Supported for: Strata Cloud Manager with Prisma Access

You can now [quarantine Prisma Access devices](#) directly through Strata Copilot, enhancing your security management capabilities. This feature is conveniently accessible across key areas of the platform, including from the Strata Cloud Manager Summary, Prisma Access Configuration Overview, and Devices management pages. There, you have the flexibility to initiate device quarantine in Strata Copilot by providing either the host ID alone or both the host ID and device serial number.



When Strata Copilot processes your request to add the specified device to the quarantine list, you will see immediate feedback including a convenient link to view more details in the relevant sections of the platform. This streamlined process, allows you to quickly isolate potentially

compromised or problematic devices, thereby improving your overall network security posture and operational efficiency.

June 23, 2025

Supported on Strata Cloud Manager for Prisma Access

Strata Cloud Manager New Navigation Experience

June 16, 2025

Supported for: Strata Cloud Manager

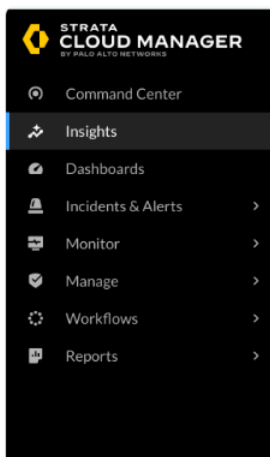
The [Strata Cloud Manager](#) user interface introduces a new redesigned navigation experience which makes it easier to find and manage key features. Designed in response to your feedback, this update focusses on simplifying navigation, reducing the need to switch between multiple sections, and improving overall efficiency.

Previously, related features were spread across multiple sections, making it difficult to locate what you needed. The new layout fixes this by grouping similar configuration workflows, providing a powerful search option, and offering a more intuitive experience.

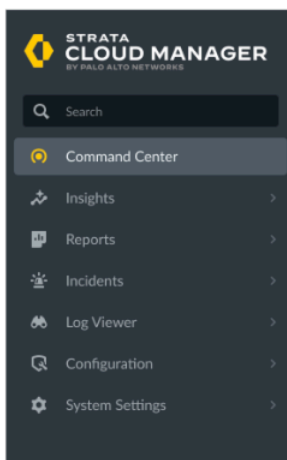
What's Changing:

- **Search:** A new search feature has been added to the left navigation, allowing you to locate features within insights, configuration, and system settings.
- **Insights:** Features from Monitor and Dashboards have been combined into a single Insights menu to bring the monitoring and visualization tools into one place.
- **Configuration:** Features from Manage and Workflows have been grouped under a new Configuration menu to reduce the need to switch between sections.
- **Unchanged Items:** Features like Help, Announcements, and Favorites will remain at the bottom of the navigation menu, as before.

Before



After



Refer to the Strata Cloud Manager navigation UI mapping document [here](#).

Quantum Readiness for Strata Cloud Manager

June 20, 2025

Supported for: NGFWs (Managed by Strata Cloud Manager)

Quantum Readiness helps you identify and remediate vulnerable cryptography across your network infrastructure. The feature categorizes cryptographic protocols, algorithms, and ciphers used in your environment as *Secure*, *Weak*, or *Vulnerable*, providing visibility into cipher suites negotiated on user endpoints, applications, NGFWs, and other network devices. You can examine SSL/TLS, VPN, and SSH protocols with metrics for encrypted throughput, sessions, and cipher usage across your infrastructure components.

This feature supports compliance with federal requirements mandating cryptography inventory for government agencies and their vendors from 2023 through 2035. You receive specific remediation guidance for vulnerable implementations, protection against future quantum computing threats, and comprehensive reporting capabilities for management and compliance purposes. Quantum Readiness provides a streamlined view into the safety of your network from quantum threats, allowing you to effectively prioritize security improvements and track your progress toward a more secure cryptographic posture.

Tenant-Level Data Transfer Across Prisma Access

June 6, 2025

Supported on:

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

Strata™ Cloud Manager now provides visibility into tenant-level data transfer usage for Prisma® Access. This feature enables you to track how much data you're using compared to your licensed allocation.

With the tenant-level data transfer tracking feature, you can monitor your usage against your licensed data transfer limit directly from Strata Cloud Manager. The Subscription Usage dashboard displays a visual representation of your tenant-level data usage for Mobile Users, Remote Networks, and combination licenses over a 12-month period starting from your license activation date.

New Features in May 2025

Here are the new features we've added to Strata Cloud Manager in May 2025.

- [2025.R3.0 Configuration Management Features](#)
- [NetSec Platform Features](#)

New Strata Cloud Manager Management Features (May 2025)

Here's the new [configuration management](#) features we've added to Strata Cloud Manager in May 2025; we use a scheduled upgrade to deliver these features to you and they are supported with the Cloud Manager 2025.R3.0 release version. Check your Strata Cloud Manager in-product notifications for updates on the release upgrade schedule. You can verify which Strata Cloud Manager release version you're running by navigating to your [configuration overview](#), and checking the **Cloud Management Version**.

Strata Cloud Manager: New Best Practice Assessment Checks and Custom Checks

May 16, 2025

Supported on Strata Cloud Manager for:

- NGFW, including those funded by [Software NGFW Credits](#)
- Prisma Access
- Prisma SD-WAN

Strata Cloud Manager introduces the following new checks:

- [Custom checks](#) include support for verifying subnet matches within IP address objects and groups.
- Inline [Best Practices Assessment \(BPA\)](#) supports all the configuration objects in Strata Cloud Manager.
- BPA check supports verifying whether a vulnerability protection security profile is applied to the GlobalProtect interface to protect the GlobalProtect services from attacks using published product security vulnerabilities.

Strata Cloud Manager lets you validate your configuration against predefined [Best Practices](#) and custom checks you create based on the needs of your organization. As you make changes to your service routes, connection settings, allowed services, and administrative access settings for the management and auxiliary interfaces for your firewalls, Strata Cloud Manager gives you assessment results inline so you can take immediate corrective action when necessary. This eliminates problems that misalignments with best practices can introduce, such as conflicts and security gaps.

Inline checks let you:

- Gauge the effectiveness of, assess the impact of, and validate changes you make to your configuration using inline assessment results.

- Prioritize and perform remediations based on the recommendations from the inline assessment.

Strata Cloud Manager: Config Cleanup Enhancements

May 16, 2025

Supported on Strata Cloud Manager for:

- NGFW, including those funded by [Software NGFW Credits](#) (Managed by Strata Cloud Manager)
- Prisma Access (Managed by Strata Cloud Manager)

Here are the enhancements for [Config Cleanup](#):

- **Role-Based Access Control (RBAC):** Access to Config Cleanup operations is governed by RBAC, allowing you to view either the Admin View or the User View based on your assigned role.
- **Unified Filtering Experience:** Seamless navigation with consistent filter dropdowns and text across the **Unused Objects**, **Zero Hit Objects**, and **Zero Hit Policy Rules** pages.
- **Advanced Filtering Options:** Use the new filter ranges (30+ Days, 60+ Days, 90+ Days) and a customizable option for precise data view control.
- **Dynamic Zero Hit Object Calculation:** Filters now recalculate **Zero Hit Objects** based on “Days with Zero Hits” in real time, providing more relevant information.
- **Streamlined Rule Details:** Explore **Zero Hit Objects Rule** details in a single-table sidecar for improved clarity and easier data interpretation.

These enhancements offer improved usability, and more precise control over your configuration cleanup process.

Do dynamic business needs often require you to deal with rapid configuration changes that result in complex configurations with a number of zero hit rules, zero hit objects, unused objects, and duplicate objects? Such configurations can lead to a poor security posture and can inadvertently increase the attack surface of your network. [Config Cleanup](#) has you covered.

Config Cleanup gives you a comprehensive view of all policy rules that have no hits, objects that aren't referenced directly or indirectly in your configuration, objects that are referenced in a policy rule but have no hits in the Traffic log during the specified time frame, and objects of the same type with different names but have the same values so that you can better:

- Manage attack surface exposure
- Prioritize remediation actions
- Remediate over time
- Respond to audit questions when they arise

Identify and remove unused configuration objects and policy rules from your configuration. Removing unused configuration objects eases administration by removing clutter and preserving only the configuration objects that are required for security enforcement.

Review unused objects and policy rules across your entire Strata Cloud Manager configuration for the last 6 months, and optimize policy rules that are overly permissive rules to convert these to be more specific, focused rules that only allow the applications you're actually using.

Together with [Policy Optimizer](#), these tools help you ensure that your policy rules stay fresh and up to date.

Strata Cloud Manager: Policy Optimizer Enhancements

May 16, 2025

Supported on Strata Cloud Manager for:

- NGFW, including those funded by [Software NGFW Credits](#) (Managed by Strata Cloud Manager)
- Prisma Access (Managed by Strata Cloud Manager)

[Policy Optimizer](#) now allows you to create address groups within policy recommendations, addressing challenges in efficiently managing firewall policies at scale. You can create source and destination address groups within recommended rules, allowing you to adjust and preview suggested groups before accepting recommendations. These enhancements streamline the process of optimizing firewall policies, helping you balance security and operational efficiency as your network grows.

Overly permissive security rules—such as those allowing "any" application traffic—are common in large networks, creating security gaps by enabling unused applications and unnecessarily increasing the attack surface. Manual review and optimization of these broad rules require extensive log analysis and introduce deployment risk. Strata Cloud Manager introduces Policy Optimizer that analyzes log data to identify overly permissive security rules. [Policy Optimizer](#) auto-generates specific, focused rule recommendations based only on the applications actively observed on your network. This capability eliminates the need for manual log analysis, strengthens your security posture, and reduces administrative overhead. Administrators receive actionable, auto-generated optimization recommendations that can be reviewed and accepted through a guided workflow, ensuring that rule consolidation and replacement are secure and policy integrity is maintained. Together with [Config Cleanup](#), these tools help you ensure that your policy rules stay fresh and up to date.

Strata Cloud Manager: IPv4 Multicast Routing Support

May 16, 2025

Supported for:NGFW (Managed by Strata Cloud Manager)

Strata Cloud Manager (SCM) now enables you to configure IPv4 multicast routing on [virtual routers](#) and [logical routers](#). You can enable [Protocol-Independent Multicast \(PIM\)](#), Internet Group Management Protocol (IGMP), and Multicast Source Discovery Protocol (MSDP) on supported interfaces. Additionally, SCM enables you to configure [PIM Interface Timer profiles](#), MSDP Timer profiles, and IGMP Interface Query profiles. You can also [create IPv4 mroutes](#), which are static

unicast routes that point to a multicast source. Logical routers support only IGMPv2 and IGMPv3 (not IGMPv1). Only logical routers support a multicast static group (virtual routers do not).

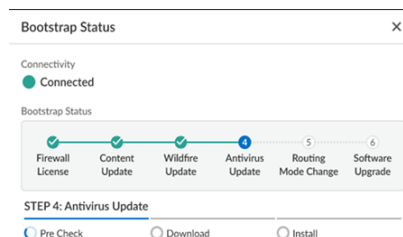
Enhanced Visibility for ZTP Onboarding

May 16, 2025

Supported for: NGFW (Managed by Strata Cloud Manager)

Installers with minimal technical knowledge often face challenges onboarding NGFWs at branch locations. [Enhanced visibility and status monitoring for Zero Touch Provisioning \(ZTP\)](#) addresses this by improving the NGFW activation process for branch locations, providing visibility and troubleshooting capabilities. Status monitoring for ZTP onboarding and bootstrapping offers real-time status updates in Strata Cloud Manager for administrators to review and monitor throughout the activation and onboarding process.

With status monitoring for onboarding and bootstrapping, you can monitor the detailed bootup status, including Firewall Licensing, Content Updates, Wildfire Updates, Antivirus Updates, Routing Mode Changes, and Software Upgrades. The feature introduces status bars and status spinners that reflect the progress of each stage, ensuring you have a clear understanding of the activation process. In case of any interruptions or errors, such as issues with device certificates, TSG ID validation, software updates, or content updates, the bootstrap status indicates where the process failed and allows you to immediately restart.



Strata Cloud Manager: Configuration Management Support by Region

May 16, 2025

Supported on:

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

Strata Cloud Manager for Configuration Management is a solution that is defined and controlled based on the region where it is deployed. You can deploy Strata Cloud Manager in the locations of your choosing, based on data location preferences and where you have the most users. For this reason, we are rolling out region-specific support for Strata Cloud Manager as soon as we are able to do so for [each region](#).

Update:

Strata Cloud Manager now supports the following additional regions:

- Saudi Arabia
- Israel
- Indonesia

Enhanced UI for Security Policy Rules and Software Update Schedules

May 16, 2025

Supported on Strata Cloud Manager

Strata Cloud Manager provides user interface improvements that streamline security operations and management efficiency. These updates focus specifically on making policy and device management more intuitive, simplifying complex workflows, improving data visibility, and ensuring a smoother user experience. The core goal is to provide administrators with greater control and clarity over their security posture and device lifecycle.

- **Precise Security Policy Rule Insertion:** [New security policy rules](#) can now be inserted immediately after a selected rule, simplifying the organization and management of rule sets.
- **NGFW Update Schedule Pagination:** NGFW [software update schedules](#) now feature pagination with clearly defined column headings, which improves both clarity and performance when handling large datasets.
- **Non-Disruptive Device Details View:** Device details for each update schedule now open in a sidebar panel instead of expanding within the main table. This allows users to view essential details without losing context or disrupting the main table's structure.

New NetSec Platform Features on Strata Cloud Manager (May 2025)

These new features follow the Strata Cloud Manager release model of [continuous feature deployment](#); as they're ready, we make them available to ensure the latest support for all products and subscriptions across the NetSec platform. There's no Strata Cloud Manager upgrade or management version requirement associated with these features; however, check if they have version or license dependencies associated with other parts of the NetSec platform (like a cloud-delivered security service subscription, or a Prisma Access version, for example).

Granular File Transfer Control in Remote Browser Isolation

Granular File Transfer Control in Remote Browser Isolation

May 30, 2025

Previously, Remote Browser Isolation (RBI) limited administrators to allowing or blocking all downloads or all uploads during isolation, regardless of file type. This lack of flexibility forced administrators to choose between allowing all file transfers, which could lead to security issues, or blocking all file transfers, which could result in usability issues and user dissatisfaction.

You can now use isolation profiles in RBI to [specify the types of files users can upload or download](#), enabling more granular control over data transfers during isolated browsing sessions. The new capability helps to enhance the security posture by reducing the attack surface and preventing various types of cybersecurity threats. It also helps in data exfiltration by controlling which categories of file types a user is able to upload.

Key use cases include permitting users to download only document files, blocking downloads of executable files, or permitting transfers of only specific approved file types. The granular controls enable you to balance security and usability by tailoring allowed file types to your organization's needs. Configuring file type filtering enhances your data loss prevention capabilities and provides an additional layer of protection against potential threats introduced through file transfers.

Strata Copilot: New Region Support

Strata Copilot: New Region Support

May 22, 2025

Strata Copilot now extends its reach to [new regions](#), enhancing global accessibility. This expansion brings the powerful AI-driven assistance to users in China, Qatar, and Saudi Arabia. By increasing geographical coverage, Strata Copilot offers more organizations the opportunity to streamline their security operations, leverage intelligent insights, and improve overall efficiency in managing their Palo Alto Networks solutions in Strata Cloud Manager across these diverse locations.

Update:

Strata Copilot now supports the following additional regions:

- China
- Qatar
- Saudi Arabia

Customizable Prisma Access Agent Session Timeout Settings

Customizable Prisma Access Agent Session Timeout Settings

May 20, 2025

Unexpected session timeouts and inactivity logouts can significantly disrupt user productivity and lead to increased helpdesk tickets. Prisma® Access Agent addresses this issue by introducing configurable notifications that alert users before their sessions expire or terminate due to inactivity. You can now set up timely warnings and custom messages to keep your users informed and provide them with the option to extend their sessions when needed.

You can [customize sessions](#) by setting their duration, scheduling logout notifications, and creating custom expiration messages. You can set the duration a user can stay logged in to a session, and also set the amount of time to wait before the agent session ends due to user inactivity. The ability to customize session timeouts and notifications helps balance user access needs with network security. It enables you to control session timeouts, keep users informed about their session status, and communicate important information.

Disable Prisma Access Agent with One-Time Password

Disable Prisma Access Agent with One-Time Password

May 20, 2025

To address the potential risks of end users disabling the Prisma® Access Agent, your users can now [use a one-time password \(OTP\) system](#) to securely disable the agent. With the OTP system, Prisma Access Agent can generate unique, single-use codes for agent disabling, enhancing security and administrative control. You can configure the OTP system on a per-user or per-user group basis, providing granular control over who can disable agents and when. When users enter the correct OTP, the agent verifies it locally and disables itself, ensuring functionality even in offline scenarios. This feature also improves auditing capabilities by logging all OTP-related activities, helping you track and monitor agent disabling events across your network. By implementing this OTP system, you can meet compliance requirements, align with industry standards, and provide a more secure and flexible solution for managing Prisma Access Agents.

IPv6 Sinkholing for Prisma Access Agent

IPv6 Sinkholing for Prisma Access Agent

May 20, 2025

While the Prisma® Access Agent routes mobile user IPv4 traffic through a protected tunnel to Prisma Access, IPv6 traffic is conventionally sent to the local network adapter on an endpoint. Prisma Access offers the ability to enhance security for dual-stack endpoints by sinkholing IPv6 traffic.

By [enabling IPv6 sinkholing](#), you can effectively mitigate risks associated with IPv6-based threats, thus reducing your overall attack surface. This feature is valuable in scenarios where you need to maintain a secure environment for mobile users accessing the internet. As endpoints can automatically fall back to IPv4 addresses, you can ensure a continuous and protected user experience without compromising on security. By implementing this capability, you strike an optimal balance between robust threat prevention and uninterrupted connectivity for your mobile workforce.

LDAP Support for Prisma Access Agent

Granular File Transfer Control in Remote Browser Isolation

May 20, 2025

Organizations transitioning to Prisma® Access Agent face challenges when their existing authentication infrastructure uses LDAP/LDAPS, as Prisma Access Agent previously only supported SAML and certificate authentication through Cloud Identity Engine (CIE). This can create significant adoption barriers, especially in regions where LDAP usage is prevalent. LDAP support for Prisma Access Agent addresses this challenge by enabling you to leverage your

existing GlobalProtect® portal LDAP authentication infrastructure, eliminating the need to reconfigure authentication methods when migrating to Prisma Access Agent.

With [LDAP authentication support](#), you can now configure your Prisma Access Agent to authenticate users against your existing directory services through the GlobalProtect portal. This integration provides a seamless authentication experience for your users while maintaining your existing security policies. The feature supports all standard LDAP configuration options, including Base DN, Bind DN, multiple LDAP servers, SSL/TLS secure connections, and server certificate verification for SSL sessions. You can also combine LDAP authentication with client certificate authentication using AND/OR logic to meet your specific security requirements.

The enhanced user experience includes support for saved user credentials, enabling seamless authentication across device states such as sleep-wake cycles, hibernation, and network transitions. When properly configured, users won't need to repeatedly enter their credentials after logging into their operating system.

By supporting LDAP authentication through the GlobalProtect portal, Prisma Access Agent provides you with a smoother migration path from GlobalProtect to Prisma Access Agent, preserving your authentication setup while enabling you to transition to a newer access agent. This feature is valuable for existing deployments where reconfiguring authentication methods would otherwise increase deployment complexity and time.

Pre-Logon for Prisma Access Agent

Pre-Logon for Prisma Access Agent

May 20, 2025

To avoid delays in critical device updates and maintain security, you need a way to connect remote corporate-owned machines to the network before users log in. The [pre-logon](#) feature for Prisma® Access Agent addresses this challenge by establishing a secure device-level connection before user authentication occurs.

This feature improves IT productivity and enhances your overall security posture by ensuring all managed devices receive essential updates and configuration changes, regardless of the user's login status. You can now perform critical management tasks—such as applying group policies, installing software updates, and synchronizing roaming profiles—without waiting for a user to log in.

Pre-logon is designed to provide consistent connectivity for your managed devices across system restarts and sleep-wake cycles. By utilizing this capability, you significantly improve the management of your remote assets and enhance security by ensuring devices are properly configured and updated before users gain full network access.

Prisma Access Agent Captive Portal Support

Prisma Access Agent Captive Portal Support

May 20, 2025

Mobile users often struggle to connect securely when working from locations with captive portals, such as hotels, cafes, and airports. These captive portals require authentication before allowing internet access. Prisma® Access Agent automatically detects when a user has connected to a network with a captive portal and opens the captive portal authentication page in its embedded browser, enabling users to authenticate without bypassing security policies. This approach enhances security by containing the captive portal interaction within the controlled environment of the embedded browser, mitigating risks associated with external browser use.

By using [captive portal support](#) with Prisma Access Agent's embedded browser functionality, you ensure that your mobile workforce maintains secure access to corporate resources across diverse network environments. It prevents scenarios where employees are unable to access the internet or corporate resources due to undetected captive portals, while also addressing security concerns related to captive portal interactions. This solution significantly reduces connectivity-related support tickets, improves overall user productivity, and provides an integrated, secure experience for your remote and traveling employees while maintaining the stringent security standards your organization requires.

Prisma Access Agent Embedded Browser Support for SAML Authentication

Prisma Access Agent Embedded Browser Support for SAML Authentication

May 20, 2025

Managing SAML authentication across various web browsers poses significant challenges for administrators, often resulting in a cumbersome user experience with annoying pop-ups and redirection issues between the access agent and browser.

The Prisma® Access Agent [embedded browser](#) addresses this issue by integrating a dedicated browser directly into the agent, providing your users with a consistent in-app experience for Prisma Access Agent logins, simplifying administration, and significantly enhancing security posture. By keeping the authentication process within the application, you eliminate the need for external browser interactions, reduce the risk of user confusion, and mitigate potential security vulnerabilities associated with browser redirections. This internal processing environment ensures strict adherence to conditional access policies, which also simplifies administrative overhead.

With support for various authentication methods and compatibility with existing Prisma Access Agent features, the embedded browser significantly improves both security and usability in your remote access infrastructure.

Transparent Proxy Support for Prisma Access Agent

Transparent Proxy Support for Prisma Access Agent

May 20, 2025

Prisma® Access Agent now supports [transparent proxy connections](#), offering always-on internet security and private app access for your mobile users. This feature enables seamless coexistence with third-party VPN agents, enhancing your organization's security posture. You can use it to secure all internet traffic from browser and nonbrowser apps, even when users are disconnected

from the tunnel. The solution forwards internet traffic to Prisma Access, preventing users from bypassing Prisma Access.

You can support various scenarios including users connecting from home, branch offices, or public Wi-Fi. It's compatible with endpoints running third-party VPNs in full or split tunnel modes. The feature prevents conflicts on endpoints and offers admin controls to maintain smooth operation. You will find this useful for maintaining consistent security across diverse networks. It supports continuous trust verification for mobile users through device posture checks. By implementing this functionality, you can enforce security policies regardless of user location or connection method, strengthening your overall security stance and strengthening your overall security posture with always-on connectivity.

Extend Prisma Access User Group Policy Support with Short Form Format

Extend Prisma Access User Group Policy Support with Short Form Format

May 16, 2025

We introduced the ability to [extend Prisma Access user group policy](#) with the short form format. Migrating security policies from NGFW to Prisma Access requires policy elements standardization. Prisma Access only supports long-form DN entries for group-based policies, while the NGFW allows using other formats such as SAML account name/Common Name and email address. This feature enables customers to define the group format choice for security policy creation, allowing standardized policy creation across Prisma Access and NGFW.

Visibility for Enterprise Browser

Visibility for Enterprise Browser

May 13, 2025

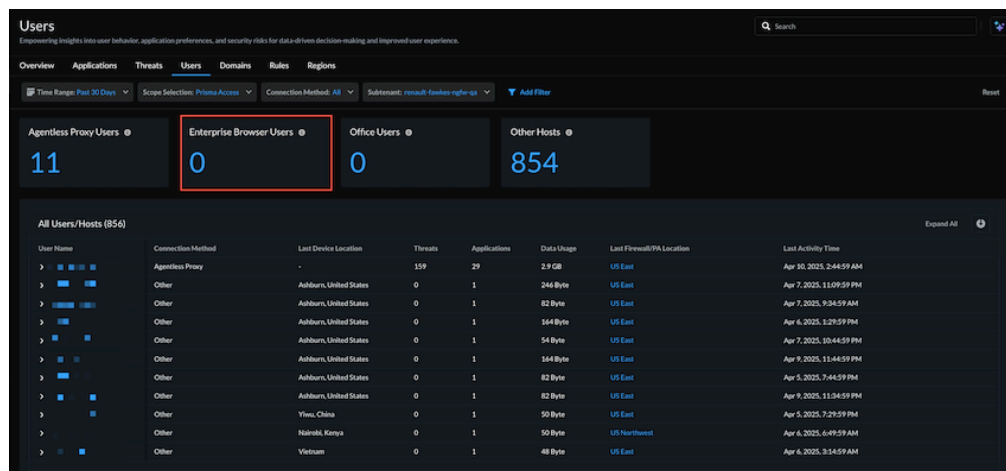
Achieving granular visibility into user activity across various enterprise browsers was previously a challenge. Now, depending on your license, offers the following new features for advanced monitoring:

- **Activity Insights > Users**

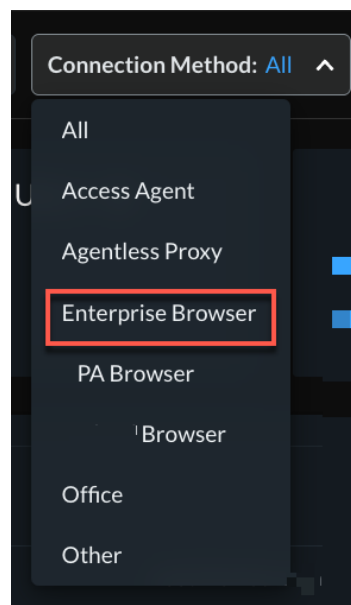
New Connection Method = Enterprise Browser

Enterprise Browser is now available as a **Connection Method** to filter user activity by **Enterprise Browsers** in Prisma[®] Access. You can view the following details:

- Active Users trend chart
- Current Active User count and list
- Risky Users
- Active Users list including User Name, Browser Type, Browser Version, Last Source IP, Last Source Location, Last Used PA Location, and Last Activity Time



If you have multiple enterprise browsers, you can switch to Prisma[®] Access Browser or any other supported third-party enterprise browser using **Connection Method**.



- **Subscription Usage for Mobile Users: Monitor > Subscription Usage > Mobile Users**

You can see the usage count under **Total Unique Users**.

- **Prisma[®] Access locations: Monitor > Prisma Access Locations**
New widget for **Explicit Proxy** locations, status, and connectivity to .

CVE Threat Research for Strata Copilot

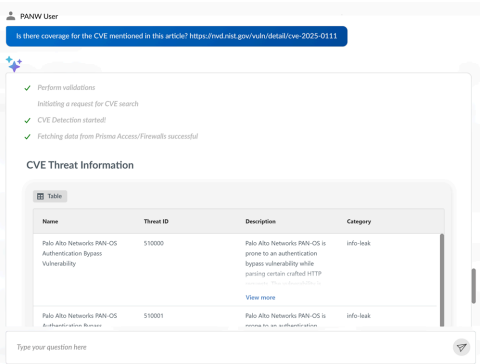
CVE Threat Research for Strata Copilot

May 9, 2025

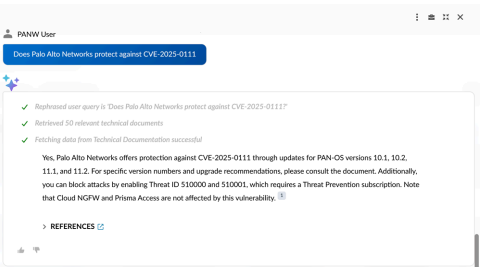
You can now quickly determine if Palo Alto Networks provides protection against specific vulnerabilities using Strata Copilot. When investigating specific CVEs, Strata Copilot searches comprehensive data sources to provide detailed protection information including unique threat IDs, descriptions, categories, compatible PAN-OS versions, release dates, and current status.

To receive information about available safeguards for deeper investigation, you can simply ask questions like:

"Is there coverage for the CVE mentioned in this article? <articleURL>"



"Does Palo Alto Networks protect against <CVE>?"



Designed for enterprise-scale performance, Strata Copilot handles large datasets related to Threat Detection and Prevention data while delivering responses in under 5 seconds for most threat intelligence queries. Strata Copilot minimizes latency between data updates and availability to ensure you always receive the most current information about CVE protection status and potential threat actor exploitation activity in your environment.

New Features in April 2025

Strata Cloud Manager: NGFW Alerts in April

April 24, 2025

Here are the [NGFW alerts](#) introduced in April 2025:

- NGFW Sent BGP Routes Beyond the Capacity of Its Peer
 - IKEv1 IPsec Tunnel Down - Peer Identification Mismatch
 - Potential Traffic Loss - Packet Buffer Exhaustion
 - PA-400 PAN-OS Version at Risk of Boot/Reboot Issues
 - Dataplane Process all_pktproc Crash - Invalid URL Cache Category Length
 - Mismatch Between Traffic Logs and Session Details for Usernames
 - gRPC Connection Failure to User-ID Edge Service
 - User Group Usage in Policies exceeding the supported limit
 - Mismatch of Server Group Mapping Users and Groups between LDAP and PAN-OS Device
 - NGFW Not Forwarding Logs - Missing Collector Preference List
-

Health [alerts](#) actively monitor the health and performance of your platform in real time. This approach helps in identifying issues, predicting potential problems, and implementing remediation actions to ensure your devices function optimally. Here are some key aspects:

- **Monitoring Metrics:** Continuously monitor various metrics from the NGFWs, including CPU utilization, memory usage, disk space, network throughput, and other relevant performance indicators.
- **Anomaly Detection:** Generate alerts that dynamically adjust based on the metric's historical value and your usage trends.
- **Predictive Analysis:** Leverage historical data and patterns to predict when thresholds might be exceeded or specific events may occur. This helps forecast potential issues before they escalate.

Extended Availability of Strata Copilot in Strata Cloud Manager

April 11, 2025

Supported on Strata Cloud Manager

You can now access [Strata Copilot](#) functionality across key Settings pages in Strata Cloud Manager, enhancing your workflow and platform experience. The Copilot icon is now available from the Subscriptions, Tenants, Device Associations, and Identity & Access pages, providing instant access to relevant technical documentation.

Strata Copilot: New Region Support

April 25, 2025

Supported on Strata Cloud Manager

Strata Copilot now extends its reach to [new regions](#), enhancing global accessibility. This expansion brings the powerful AI-driven assistance to users in Canada, France, Israel, India, Taiwan, Japan, Singapore, Indonesia, and Australia. By increasing geographical coverage, Strata Copilot offers more organizations the opportunity to streamline their security operations, leverage intelligent insights, and improve overall efficiency in managing their Palo Alto Networks solutions in Strata Cloud Manager across these diverse locations.

Update:

Strata Copilot now supports the following additional regions:

- Canada
- France
- Israel
- India
- Taiwan
- Japan
- Singapore
- Indonesia
- Australia

ADEM for NGFW

April 10, 2025

Supported for: NGFW (Managed by Strata Cloud Manager)

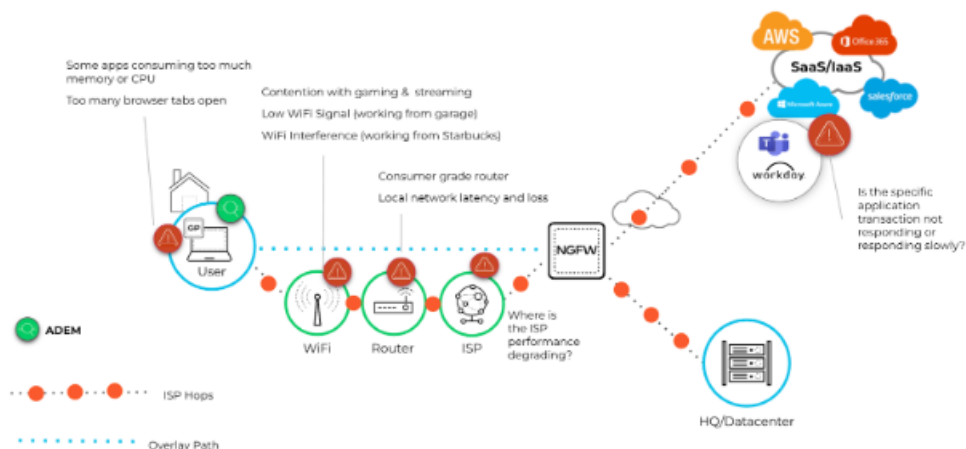
Requirements:

- Strata Cloud Manager Pro for NGFW license
 - a firewall running PAN-OS
 - 11.1.9 or a later 11.1 version
 - 11.2.6 or a later 11.2 version
 - For remote sites: a PAN-OS SD-WAN subscription
 - For mobile users: a GlobalProtect license
-

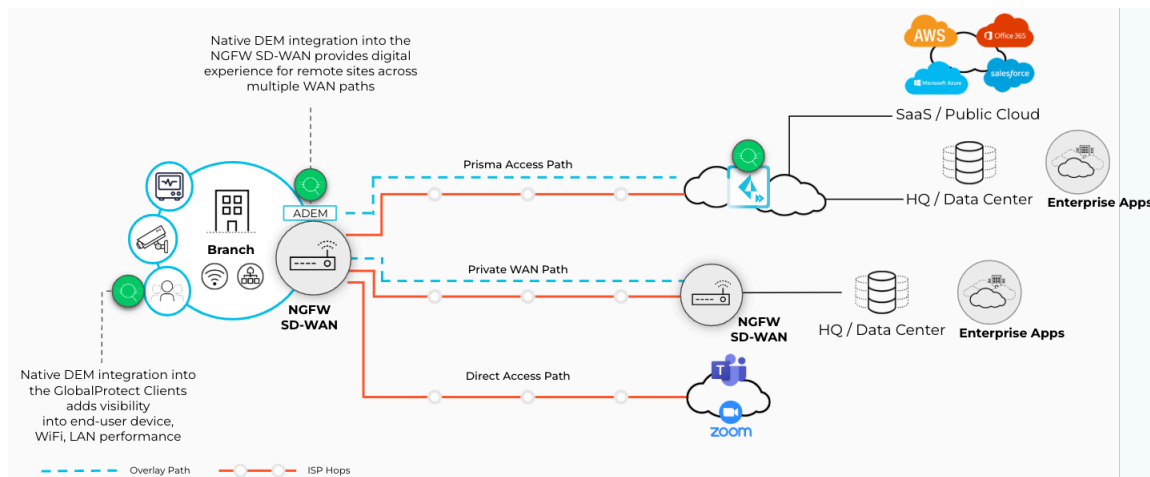
Previously, comprehensive end-to-end visibility into user and application experience was limited when traffic passed through Next-Generation Firewalls (NGFWs). now extends its end-to-end application experience and performance monitoring capabilities beyond the SASE platform

to next-generation firewalls (NGFWs) for a more comprehensive view into your users' digital experience.

Now, if you have users connecting to an NGFW with a **GlobalProtect®** Gateway installed, you can run synthetic tests from the user's endpoint to the application to gain visibility into their application experience. User experience to applications with hop by hop views and segment wise health is visible, allowing you to identify issues and better target your remediation efforts.



Similarly, if you have an NGFW configured as a branch site using **SD-WAN**, you can now monitor synthetic tests from the NGFW branch site to the application and take action upon any signs of application experience degradation.



If you have both for and for , can detect and report when a user is connecting to or to an at a given point in time so that you can easily pinpoint where an experience issue may be occurring.



This comprehensive experience data is now fully integrated and viewable in **Strata Cloud Manager**, streamlining your analysis across your entire hybrid network.

IP Pool Allocation Enhancements

April 4, 2025

Supported on Strata Cloud Manager

Prisma Access initially allowed only three main theaters (Americas, EMEA, APAC) for IP pool allocation. In this release, we now allow [users to view IP pool utilization per pool locations and subpool regions](#).

New Features in March 2025

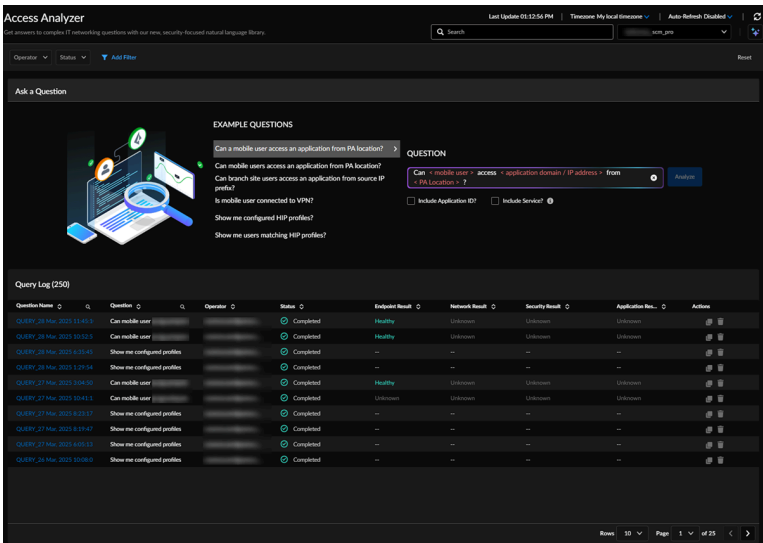
Natural Language Queries for Access Analyzer

March 31, 2025

Supported for: Prisma Access (Managed by Strata Cloud Manager) and Prisma Access (Managed by panorama)

Administrators often struggle when manually constructing complex, technical queries for access analysis, slowing down investigation. [Natural language queries for Access Analyzer](#) solve this by providing a simple interface to construct queries with ease. The new Access Analyzer workflow in Strata Cloud Manager allows you to select from predefined example questions. The interface includes dynamic placeholders you can modify, streamlining the process of inputting specific values such as usernames, devices, or locations. Ask Access Analyzer queries in Strata Copilot™ before moving over to the Access Analyzer dashboard to review query logs.

When utilizing this new functionality, you can use the powerful capabilities of Access Analyzer more effectively, enabling faster problem resolution. Coming soon, users will be able to type out the questions fully themselves. This enhancement aims to increase adoption of the tool among administrators.



Support for VM-Series funded by Software NGFW Credits in Strata Cloud Manager Essentials

March 21, 2025

Supported on Strata Cloud Manager

The Strata Cloud Manager Essentials license tier now includes support for VM-Series funded by software NGFW credits. To activate Strata Cloud Manager Essentials for VM-Series funded

by software NGFW Credits, skip selecting Strata Cloud Manager Pro or Strata Logging Service cloud subscriptions while [creating a deployment profile](#).

When activating a deployment profile for VM-Series funded by software NGFW credits in Strata Cloud Manager Essentials, you can now [onboard the Flex firewalls to Cloud Identity Engine \(CIE\)](#).

A new licensing structure for Strata Cloud Manager is now available, featuring two licensing tiers: Strata Cloud Manager Essentials and Strata Cloud Manager Pro. This unified structure streamlines the deployment of network security offerings, including AIOps for NGFW, Autonomous Digital Experience Management (ADEM), cloud management functionality, and Strata Logging Service. Strata Cloud Manager offers a unified experience with the products accessible through a single interface, though you require separate licenses for each product to integrate them into the platform.

Here's an overview of the two licensing tiers available for Strata Cloud Manager:

- **Strata Cloud Manager Essentials** is the free tier that offers basic configuration and network security lifecycle management features to streamline operations and provide essential security.
- **Strata Cloud Manager Pro** is the paid tier that includes all features of Strata Cloud Manager Essentials, plus advanced features to enhance operational health, prevent network disruptions, strengthen real-time security posture, and ADEM for monitoring user experience performance. Strata Cloud Manager Pro includes Strata Logging Service with one year of log retention and unlimited storage, enabling centralized logging and seamless data retrieval across your deployment.

Strata Cloud Manager Essentials and Strata Cloud Manager Pro are available to activate in customer support portal (CSP) accounts that don't have: Strata Logging Service with sized storage, AIOps for NGFW Free or Premium, or Prisma Access.

For a detailed comparison of the available features and to learn more about how to activate these licenses, visit [Strata Cloud Manager License](#).

Advanced WildFire Dashboard Enhancements

March 31, 2025

Supported on Strata Cloud Manager

The [Advanced WildFire Dashboard](#) available in Strata Cloud Manager now provides improved data representation of Advanced WildFire analysis data from attached Palo Alto Networks platforms. You can view comprehensive data on file submissions from additional sources, including the NGFW, Prisma Access, and Prisma Access mobile users, while also providing robust analysis details, which are now reflected in all aspects of the dashboard.

The dashboard provides updated global filtering options and widget visualizations based on the latest 90-day submission data to enable effective WildFire data analysis. Users can access insights on total sample submissions, verdicts, file type breakdowns, and signature creation, in a multitude of contexts. The dashboard also offers filtering options to focus on specific data points, such as the time range, sample source, and verdict type. Furthermore, certain widgets now offer access

to detailed analysis results, including downloadable file analysis reports in both MAEC and PDF formats for specific sample hashes, utilizing the updated [IOC search engine](#).

These granular controls enable you to identify trends, spot potential threats, and take appropriate action to enhance your security policies, while the enhanced visibility allows you to better understand your organization's security posture and make informed decisions to reduce attack surfaces.

Update:

August 14, 2025

The Advanced WildFire Dashboard now supports an additional new widget: [Prevention Statistics](#)

License Migration for AIOps for NGFW Premium, AI-Powered ADEM, and Strata Logging Service

March 14, 2025

Supported on Strata Cloud Manager

Palo Alto Networks has announced that AIOps for NGFW Premium, AI-Powered Autonomous Digital Experience Management (ADEM), and Strata Logging Service with sized storage licenses will reach their [end-of-sale on May 8, 2025](#). To ensure a smooth transition, we will automatically [migrate existing customers to alternative licenses](#) starting in March 2025 at no additional cost. These updated licenses will retain the same expiration dates and terms as the original ones. The migration process won't disrupt product functionality and requires no action from you.

Strata Copilot: Visualization Type Specification in Prompts

March 1, 2025

Supported on Strata Cloud Manager

You can now specify visualization types directly within your prompts and follow-up questions in Strata Copilot. This streamlines your data visualization process by allowing you to request specific chart types as part of your natural language queries. For example, you can input **In Sankey, show remote sites per PA location** or **Show me top 10 PA locations by threat count in a bar chart**.

Additionally, Strata Copilot maintains context awareness in conversations, enabling you to modify chart types with simple follow-up requests. After your initial query, you can easily switch visualizations by saying **Can I see that in a map?** or **Display that as a pie chart**.

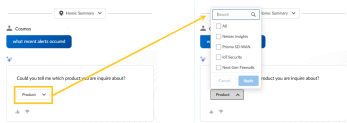
This enhancement significantly improves your workflow efficiency and user experience, enabling faster, more intuitive, and flexible data exploration within Strata Copilot. You'll enjoy seamless transitions between different visualization types as you analyze your data from various perspectives.

Strata Copilot: Product Filtering for Responses

March 1, 2025

Supported on Strata Cloud Manager

The Strata Copilot experience now provides product-specific response filtering. When multiple responses are available for different products, you can now easily isolate and focus on the information you need.



Simply select one or more products to view tailored results for each product area. This filtering streamlines your workflow by presenting only the most relevant information, saving you time and improving decision-making. The filter automatically hides when your query yields a response for a single product.

Strata Cloud Manager: NGFW Alerts in March

March 1, 2025

Here are the [NGFW alerts](#) introduced in March 2025:

- Ethernet Interface Down
 - SAML message has no Signature from IdP
-

Health [alerts](#) actively monitor the health and performance of your platform in real time. This approach helps in identifying issues, predicting potential problems, and implementing remediation actions to ensure your devices function optimally. Here are some key aspects:

- **Monitoring Metrics:** Continuously monitor various metrics from the NGFWs, including CPU utilization, memory usage, disk space, network throughput, and other relevant performance indicators.
- **Anomaly Detection:** Generate alerts that dynamically adjust based on the metric's historical value and your usage trends.
- **Predictive Analysis:** Leverage historical data and patterns to predict when thresholds might be exceeded or specific events may occur. This helps forecast potential issues before they escalate.

New Features in February 2025

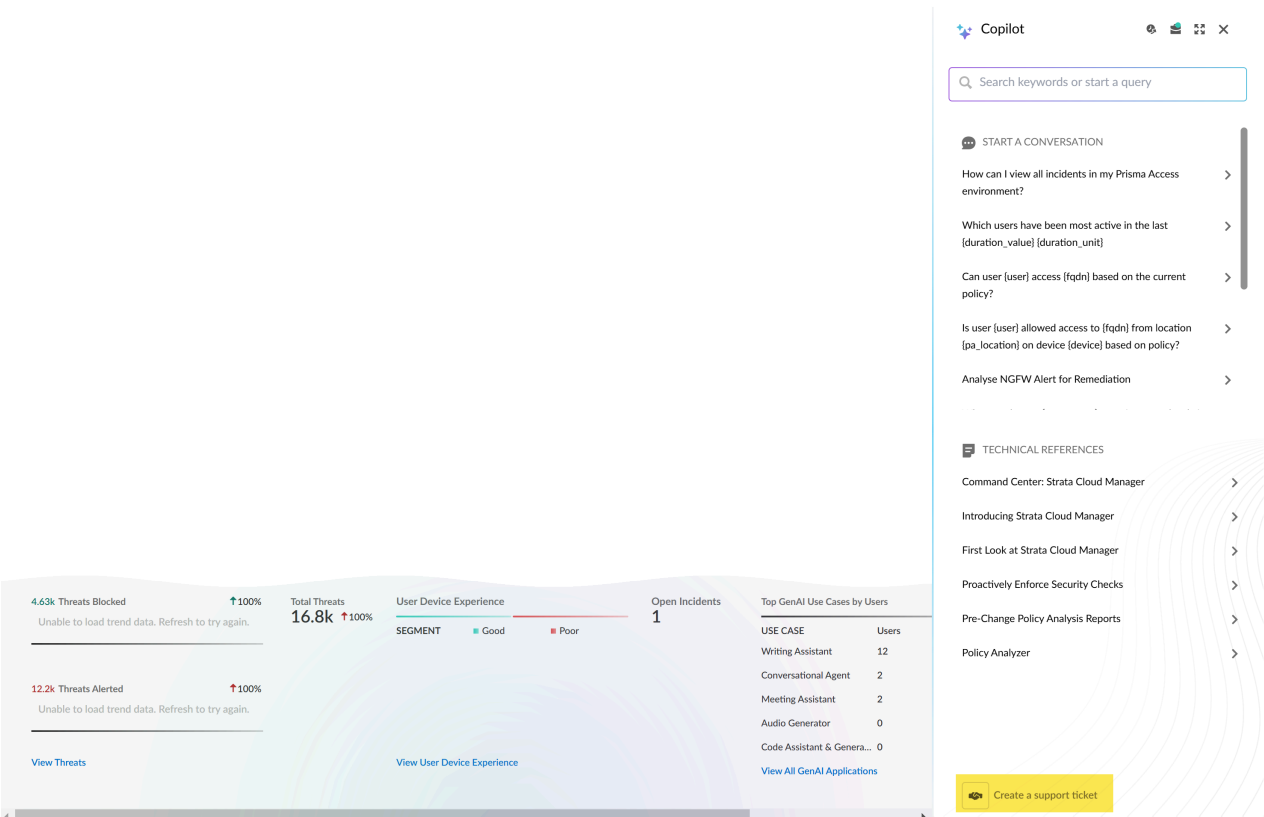
Features listed here include some feature highlights for the [products supported with](#) Strata Cloud Manager.

Case Creation Enhancements in Strata Copilot

February 21, 2025

Supported on Strata Cloud Manager

The case creation workflow in Strata Copilot is now restructured for improved efficiency, now following a more logical progression.



When **opening a case**, Strata Copilot first collects core information such as product, hostname, issue description, and severity. Depending on the nature of the issue, Strata Copilot can prompt for additional details. Once Strata Copilot gathers the necessary information, it runs an automated analysis using category-specific playbooks, including a dedicated one for commit issues. Based on this analysis, Strata Copilot suggests remediation actions if a relevant playbook is identified. As

you progress, you will see real-time updates during playbook execution. If these suggestions don't resolve your issue, you can then proceed to open your support case.

The system preserves your case creation state for one hour, allowing you to resume without losing progress if you encounter interruptions. This streamlined process ensures all required information is collected upfront, enabling more accurate analysis and potentially faster resolution of your issue.

Strata Cloud Manager: New Best Practice Assessment Checks and Custom Checks

February 14, 2025

Supported on Strata Cloud Manager for:

- NGFW, including those funded by [Software NGFW Credits](#)
- Prisma Access
- Prisma SD-WAN

Strata Cloud Manager introduces the following new checks and features:

- [Custom checks](#) support a wide range of configuration objects, including authentication profiles, device setup, security profiles, GlobalProtect configurations, network objects, and policy rules.
- Inline configuration analysis supports new configuration objects, including addresses, application groups, dynamic user groups, HIP profiles, tags, and variables.
- Custom checks support multi-objects and the `len` operator for greater flexibility.
- Custom checks validate security policies for applications within application filters, enhancing policy coverage and security.
- Supports cloning of predefined checks.
- Both [Best Practices Assessment \(BPA\)](#) and custom checks support web security policies.

Strata Cloud Manager lets you validate your configuration against predefined [Best Practices](#) and custom checks you create based on the needs of your organization. As you make changes to your service routes, connection settings, allowed services, and administrative access settings for the management and auxiliary interfaces for your firewalls, Strata Cloud Manager gives you assessment results inline so you can take immediate corrective action when necessary. This eliminates problems that misalignments with best practices can introduce, such as conflicts and security gaps.

Inline checks let you:

- Gauge the effectiveness of, assess the impact of, and validate changes you make to your configuration using inline assessment results.
- Prioritize and perform remediations based on the recommendations from the inline assessment.

Strata Cloud Manager: Web Access Policy Rule Replacement: Migrate to the New Internet Access Rule

February 14, 2025

Supported on Strata Cloud Manager for:

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

The [Internet Access](#) rule is a new policy type within the security rulebase in , which simplifies the security management, reduces rulebase complexity, and ensures consistent security control across web traffic, particularly in cloud-centric, and SaaS-driven environments.

The Internet Access rule replaces the existing Web Access policy rules with improved capabilities. Internet Access rule [migration](#) transfers your existing web Security policy rules. The system integrates Web Security policy rules and custom Web Access policy rules into the new framework during your tenant upgrades.

You can efficiently manage user access to web applications, applying functional controls, application tenant handling, and data security inspections globally or for specific applications and URLs. This rule integrates with , providing native capabilities without requiring policy recommendation workflows. You can use it alongside existing firewall access policy rules, maintaining full control over rule ordering.

[Default settings](#) allow outbound access to SaaS applications and URLs with security inspection and logging enabled. You can adjust built-in decryption rules per scope for precise control over encrypted traffic. New Strata Cloud Manager[oneapp] tenants receive an optimized out-of-the-box security configuration, while existing tenants can adopt the Internet Access rule without disrupting current setups.

Strata Cloud Manager: Snippet Sharing - Advanced Controls and Visibility Enhancements

February 14, 2025

Supported on Strata Cloud Manager for:

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

The [snippet sharing](#) enhancement improves control and visibility over shared configurations across multiple tenants. The new features include a customizable Action when disassociated property for Subscriber Tenants, which allows you to convert snippets to local or delete them when disassociated.

You can now choose between reverting snippet-related changes or keeping current versions when loading previous configurations with the **Config Version Load** functionality.

To reduce misconfiguration during publishing, you'll benefit from the validate-before-update function, while asynchronous loading of updates for subscribers enhances performance.

The UI improvements introduce **Paused Updates** status indicators and refresh capabilities for Subscribed and Published Tenants, making it easier for you to track and manage snippet statuses. Error messaging now displays snippet names instead of UUIDs, simplifying your troubleshooting process.

A new configuration indicator helps you track snippet sharing statuses efficiently. These enhancements optimize your disassociated snippet management, provide you with version control and configuration reload options, and improve error handling and status visibility.

Strata Cloud Manager: Convert Local Configuration into Shared Snippets

February 14, 2024

Supported on Strata Cloud Manager for: NGFW (Managed by Strata Cloud Manager)

now converts local firewall configurations into shared configuration snippets. You can select specific configuration elements from a firewall to create reusable snippets for multiple devices. When creating snippets, you control which configuration items to include, sharing only the necessary settings across different network segments.

Converting [local configurations to snippets](#) standardizes configurations across your network and deploys consistent settings to multiple NGFWs. This replicates successful local configurations to other devices, reduces duplication, and maintains consistency between local and shared settings.

This functionality improves network configuration management and scaling. It ensures quick propagation of best practices and optimized settings throughout your infrastructure. The functionality connects local device management with centralized configuration control for flexible network administration.

Strata Cloud Manager: Unified Policy Management for SaaS Security and Internet Access Policy Rules

February 14, 2025

Supported on Strata Cloud Manager for:

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

The [Simplified Security Policy Recommendations](#) for enhances your ability to manage and enforce SaaS app Security policy rules efficiently for and managed by . You can now create, manage, and enforce policy rules using the predefined SAAS-Inline-Pol-Recommendations snippet to enforce consistent SaaS app security.

Alternatively, you can now create an Internet Access rule instead of going through the typical policy rule recommendation workflow. As an administrator, creating an Internet Access rule allows you to gain full control over policy rule enforcement and rule ordering. The unified policy framework simplifies your policy rule creation experience, allowing you to enforce consistent SaaS app security regardless of the enforcement point, eliminate policy implementation delay, and reduce the risk of misconfigurations. This streamlined workflow enables you to fully utilize the capabilities, achieving a stronger security posture for your SaaS environment. Simplified Security Policy Recommendations for allows you to more effectively secure your SaaS apps, reduce administrative overhead, and gain clearer visibility into your posture. The Simplified Security Policy Recommendations for is valuable if you manage complex SaaS environments, require granular control over Security policy rules, or need to rapidly respond to evolving security requirements in your cloud infrastructure.

Prisma Access Cloud Management Region Support

February 14, 2025

You can now deploy Prisma Access Cloud Management in the following regions:

- Israel
- Indonesia

Supported on:

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

Strata Cloud Manager for Configuration Management is a solution that is defined and controlled based on the region where it is deployed. You can deploy Strata Cloud Manager in the locations of your choosing, based on data location preferences and where you have the most users. For this reason, we are rolling out region-specific support for Strata Cloud Manager as soon as we are able to do so for [each region](#).

Update:

Strata Cloud Manager now supports the following additional regions:

- Saudi Arabia
- Israel
- Indonesia

Visibility Into Prisma Access Configuration Push Status

February 14, 2025

Supported on Prisma Access (Managed by Strata Cloud Manager)

[Prisma Access provides enhanced visibility into your configuration pushes in deployments, allowing you to better monitor and troubleshoot configuration pushes across your network.](#) The status of In Progress jobs is improved, providing you with real-time insights into the progress of configuration pushes across different regions and service types. You can view detailed

information about each push, including specific error messages or warnings, enabling quick identification and resolution of issues. This granular visibility is useful when managing large-scale deployments or troubleshooting complex configuration changes.

By using the configuration status messages, you can ensure smoother configuration rollouts, reduce downtime, and maintain better control over your Prisma Access environment. The feature's intuitive interface provides a familiar and user-friendly experience, making it easier for you to manage your Prisma Access configurations effectively.

Ability to Clone GlobalProtect App Settings and Tunnel Settings

February 14, 2025

Supported on Prisma Access (Managed by Strata Cloud Manager)

You can clone existing GlobalProtect [tunnel settings](#) and [app settings](#). This enhancement facilitates the creation of additional tunnel and app settings if you need to support split tunneling or multiple connection settings.

Prisma Access Browser Support in Strata Copilot

February 6, 2025

Supported on Strata Cloud Manager for Prisma Access Browser

Prisma Access Browser enables comprehensive event querying and analysis through Strata Copilot, providing visibility into user activity, bandwidth usage patterns, and potential security risks. With Prisma Access Browser analytics, you can:

- Query the top interacted websites to understand browsing behavior.
- Analyze active device distribution across your network.
- Identify peak usage hours for resource planning.
- List the most active users for monitoring and compliance.
- Track file transfers to detect unauthorized data movement.
- Monitor cloud storage service interactions for security oversight.

Prisma Access Browser supports customizable time ranges for both real-time and historical data analysis. Additionally, predefined queries help streamline common data analysis tasks, improving efficiency.

Additional data sets continue to be added.

New AI-Powered Workflow for Troubleshooting Application Access

February 6, 2025

Supported on Strata Cloud Manager

Strata Copilot introduces an enhanced workflow for troubleshooting application access in the Log Viewer. This new feature streamlines how you explore Strata Logging Service logs related to access issues. When querying about a user or an application name, Strata Copilot now generates dynamic, context-aware recommendations based on your current view. These suggestions include workflows to investigate policy denials for specific users and applications within defined time frames, as well as options to grant access when necessary. This AI-driven enhancement adapts to your unique needs, making log exploration for access-related issues more intuitive and efficient, ultimately simplifying the investigation and resolution of application access challenges.

Log Viewer

Firewall/Traffic

Source User = 'panwuser'

Search

Ask AI Assistant

Traffic Analysis

Troubleshoot C

Time Zone: Pacific Standard Time

2025-0

	Time Generated ↓	Subtype	From Zone	Source Ad
☐	2025-02-07 11:07:35	end	trust	172.20.11.
☐	2025-02-07 11:07:35	end	trust	172.20.11.
☐	2025-02-07 11:07:33	end	trust	172.20.11.
☐	2025-02-07 11:07:33	end	trust	172.20.11.
☐	2025-02-07 11:07:31	end	trust	172.20.11.
☐	2025-02-07 11:07:31	end	trust	172.20.11.
☐	2025-02-07 11:07:30	end	trust	172.20.11.
☐	2025-02-07 11:07:28	end	trust	172.20.11.
☐	2025-02-07 11:07:28	end	trust	172.20.11.
☐	2025-02-07 11:07:26	end	trust	172.20.11.
☐	2025-02-07 11:07:26	end	trust	172.20.11.
☐	2025-02-07 11:07:25	end	trust	172.20.11.
☐	2025-02-07 11:07:25	end	trust	172.20.11.
☐	2025-02-07 11:07:23	end	trust	172.20.11.
☐	2025-02-07 11:07:22	end	trust	172.20.11.
☐	2025-02-07 11:07:21	end	trust	172.20.11.
☐	2025-02-07 11:07:20	end	trust	172.20.11.
☐	2025-02-07 11:07:17	end	trust	172.20.11.
☐	2025-02-07 11:07:16	end	trust	172.20.11.

Enhanced RMA Workflow for Strata Cloud Manager

February 6, 2025

Supported for: NGFW (Managed by Strata Cloud Manager), excluding VM-Series NGFWs.

The Return Merchandise Authorization (RMA) workflow in [Device Management](#) streamlines the process of replacing failed NGFWs in your network environment. This feature automates and simplifies the traditionally manual, error-prone, and time-consuming task of replacing devices. With the new RMA workflow, you can restore configurations and maintain logging, monitoring, and reporting after asset transfer. The workflow enables you to replace a failed device with a new one while automatically associating it with the same configurations and HA pairs as the old device.

RMA offers a user-friendly interface that clearly displays the status of each step in the replacement process. You can easily restore both local and shared configurations from the old device to the new one. The feature supports the replacement of devices in high availability (HA) pairs without affecting the peer device. In the case of errors or failures during the workflow, you receive instructions for recovery without requiring intervention from Palo Alto Networks.

Strata Cloud Manager: NGFW Alerts in February

February 1, 2025

Here are the [NGFW alerts](#) introduced in March 2025:

- Detect Hot Plug Events
 - Card Failure: Card start timeout - Max restarts attempted
 - Dataplane Process all_pktproc Crash - Invalid URL Cache Category Length
 - Mismatch of Server Group Mapping Users and Groups between LDAP and PAN-OS Device
-

Health [alerts](#) actively monitor the health and performance of your platform in real time. This approach helps in identifying issues, predicting potential problems, and implementing remediation actions to ensure your devices function optimally. Here are some key aspects:

- **Monitoring Metrics:** Continuously monitor various metrics from the NGFWs, including CPU utilization, memory usage, disk space, network throughput, and other relevant performance indicators.
- **Anomaly Detection:** Generate alerts that dynamically adjust based on the metric's historical value and your usage trends.
- **Predictive Analysis:** Leverage historical data and patterns to predict when thresholds might be exceeded or specific events may occur. This helps forecast potential issues before they escalate.

New Features in January 2025

Here are the latest new features introduced on Strata Cloud Manager. Features listed here include some feature highlights for the [products supported with](#) Strata Cloud Manager. For the full list of new features supported for a product you're using with Strata Cloud Manager, [see the release notes for that product](#).

User Inactivity Timeout Customization

January 17, 2025

Supported on Strata Cloud Manager

You can now tailor idle timeout settings to your specific security and compliance requirements. This enhancement enables [custom tenant-level configuration](#), ensuring users are not logged out prematurely during long tasks or enforcing shorter timeouts in highly secure environments. You can set the idle timeout value between 10 to 60 minutes, with the default remaining at 30 minutes for backward compatibility.

When no timeout value is set, new tenants automatically adopt the default timeout value from their parent tenant. Once you customize the timeout value, it becomes independent and is maintained separately for that tenant.

GenAI Data in the Data Security View of the Command Center

January 16, 2025

Supported on Strata Cloud Manager

Update: December 2024

You can now monitor and protect sensitive generative artificial intelligence applications in the Data Security view of the [Command Center](#). This update allows you to better safeguard your organization's information across various GenAI-powered tools and services.

When using an license or when applying the GenAI filter, you can now see **Data at Rest** alongside **Data in Motion** in the Command Center view and the **Top Data Profiles** widget, giving you a comprehensive view of your GenAI-related Data Security posture.

These enhancements to Strata Cloud Manager's feature set enable you to more effectively manage and secure your organization's use of GenAI technologies.

Strata Cloud Manager: NGFW Alerts in January

January 17, 2025

Here are the [NGFW alerts](#) introduced in January 2025:

- BGP Peering Issue Due to Error Subcode = Administrative Reset (4)
 - BGP peering issue due to Error subcode = Bad Peer AS (2)
 - BGP Peering Issue Due to Error Subcode = Administrative Shutdown (2)
 - BGP-peer dropping due to missing keepalives
 - BGP peering issue due to Error subcode = Peer De-configured (3)
 - BGP peering issue due to Error subcode = Connection Rejected (5)
 - Unofficial URL for WildFire | Advanced WildFire
 - Unofficial URL for Application Database
 - Unofficial URL for Cloud Services
 - Unofficial URL for PAN-DB URL Filtering | Advanced URL Filtering
 - Advanced Routing Engine: NGFW Sent BGP Routes Beyond the Capacity of Its Peer
 - NGFW received BGP Routes beyond the configured max Prefixes
 - Hot-Plug event detected
 - Slow Panorama Performance - Long Execution of show config candidate operation
 - Duplicate IP address detected on an interface
 - GRE tunnel is down - recursive routing
 - Inter Log Collector Disconnection
 - Panorama/Log Collector Disconnected from Collector Group
 - Logrcvr Out-of-Memory - LFC Memory Retention Due to Kernel Failure
 - Logrcvr Out-of-Memory - LFC Log Loss Recovery Mechanism
 - Slow Panorama Performance - Long Execution of Push Scope Operation
 - Slow Panorama Performance - Long Execution of Save, Load, or Revert config operation
-

Health [alerts](#) actively monitor the health and performance of your platform in real time. This approach helps in identifying issues, predicting potential problems, and implementing remediation actions to ensure your devices function optimally. Here are some key aspects:

- **Monitoring Metrics:** Continuously monitor various metrics from the NGFWs, including CPU utilization, memory usage, disk space, network throughput, and other relevant performance indicators.
- **Anomaly Detection:** Generate alerts that dynamically adjust based on the metric's historical value and your usage trends.
- **Predictive Analysis:** Leverage historical data and patterns to predict when thresholds might be exceeded or specific events may occur. This helps forecast potential issues before they escalate.

New Features in December 2024

Here are the latest new features introduced on Strata Cloud Manager. Features listed here include some feature highlights for the [products supported with](#) Strata Cloud Manager. For the full list of new features supported for a product you're using with Strata Cloud Manager, [see the release notes for that product](#).

Strata Copilot

December 12, 2024

Strata Copilot is the ultimate AI assistant for . Strata Copilot allows you to get real-time, actionable insights on the health and security of your network, no matter where you are in Strata Cloud Manager.

Strata Copilot harnesses the data from your NGFWs, Prisma Access, and cloud security services and combines it with Palo Alto Networks best practice guidance, to give you clear, actionable answers and can open a support case for you when needed. With increasing usage, Strata Copilot will learn from your interactions to improve and refine its responses.

Favorites

Home: Summary

Austin

How many connected branches are in each PA location?

Type your question here

Copilot may leverage a large language model or generative AI, and may contain errors.

The data and insights that Strata Copilot shares with you depends on your onboarded products and licenses. Today, Strata Copilot can give you data and insights on these product and feature areas, and we'll let you know as we add additional support:

- ❑ Prisma Access
- ❑ Autonomous DEM, including Access Analyzer
- ❑ Data Security
- ❑ AI-Powered ADEM
- ❑ AIOps for NGFW
- ❑ IoT Security
- ❑ Prisma SD-WAN

Strata Cloud Manager: NGFW Alerts in December

December 12, 2024

Here are the [NGFW alerts](#) introduced in December 2024:

- Card Failure: Path monitor failure - Max restarts attempted
- Transceiver or SFP Port - Failed to Write Value
- Card Stuck in Starting State
- Card failure with reason "Slot runtime software failure - Max restarts attempted
- DP Restart - Heartbeat Failure due to Internal Link Down
- Failed exporting config bundle via ssh
- High Disk Space Usage - Shared memory partition
- SAML message from IdP has no Assertion
- Card Failure: Card heartbeat failure - Max restarts attempted
- Incorrect Port Speed Configured - PA-850
- System Drive or Connector fault
- Incompatible SFP Media Type
- GRE tunnel is down - Tunnel Monitoring Failure
- IKEv1 IPsec Tunnel Down - IPsec Crypto Profile Configuration mismatch
- IKEv1 IPsec Tunnel Down - IKE Crypto Profile Configuration mismatch

Health [alerts](#) actively monitor the health and performance of your platform in real time. This approach helps in identifying issues, predicting potential problems, and implementing remediation actions to ensure your devices function optimally. Here are some key aspects:

- **Monitoring Metrics:** Continuously monitor various metrics from the NGFWs, including CPU utilization, memory usage, disk space, network throughput, and other relevant performance indicators.

- **Anomaly Detection:** Generate alerts that dynamically adjust based on the metric's historical value and your usage trends.
- **Predictive Analysis:** Leverage historical data and patterns to predict when thresholds might be exceeded or specific events may occur. This helps forecast potential issues before they escalate.

Cloud NGFW and Prisma Access Browser Data Integration for Command Center and Activity Insights

December 3, 2024

Supported on Strata Cloud Manager

The [Command Center](#) and [Activity Insights](#) pages now include support for Cloud Next-Generation Firewalls and Prisma® Access Browser, enhancing visibility across your network security infrastructure. This integration allows you to view Cloud NGFW and Prisma® Access Browser data alongside existing NGFW and Prisma® Access information, providing you with a more comprehensive picture of your security posture.

In the Command Center, Cloud NGFW data is incorporated into three views: Summary, Threats, and Operational Health. This means you can now monitor traffic, threats, URLs, and other security metrics from your Cloud NGFWs within the familiar Command Center interface.

Prisma® Access Browser visibility is now available in the Summary and Operational Health views of the Command Center, enabling you to review the count of Prisma® Access Browser users on your network. This enhanced visibility provides you with real-time insights into browser-based security activity and user engagement patterns.

The Activity Insights pages also benefit from this integration, allowing you to analyze Cloud NGFW or Prisma® Access Browser specific data alongside other security platforms. You can now correlate security events and trends across your entire infrastructure ecosystem, making it easier to identify patterns and optimize your security configurations based on comprehensive data analysis.

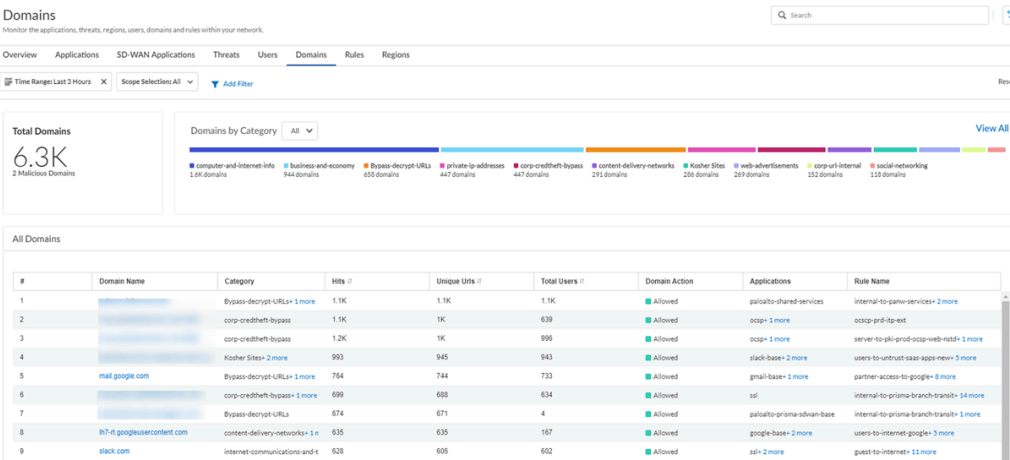
Domains in Activity Insights

December 12, 2024

Supported on Strata Cloud Manager

Monitoring critical domain activity and effectively identifying security risks requires comprehensive data visualization. [The URLs tab in Activity Insights is now the Domains tab](#), which solves this by incorporating metrics from the Advanced DNS Security service to present new visualizations, filters, and data summaries. This enhancement allows you to gain deeper insights into your domain traffic patterns and potential security risks. The Domains tab displays combined information from URL Filtering, DNS Security, Threat logs, and Traffic logs, providing a comprehensive view of domain activity within your network.

By leveraging Advanced DNS Security, you can better protect your network against DNS-based attacks, identify malicious domains more effectively, and gain a better understanding of your organization's domain traffic patterns.



New Features in November 2024

Here are the latest new features introduced on Strata Cloud Manager. Features listed here include some feature highlights for the [products supported with](#) Strata Cloud Manager. For the full list of new features supported for a product you're using with Strata Cloud Manager, [see the release notes for that product](#).

Autonomous Digital Experience Management (ADEM): Specific SD-WAN Path Monitoring

November 22, 2024

Supported for:

- Prisma Access (Managed by Strata Cloud Manager)
 - Autonomous Digital Experience Management (ADEM)
 - Prisma SD-WAN
 - SD-WAN ION version 6.4.2 or later
 - ADEM agent 3.4.7 or later
-

Previously, your synthetic application tests in [prisma](#) probed all possible network paths to an application. This often skewed your application experience scores with irrelevant data from unused paths, making it difficult and time-consuming to troubleshoot performance issues.

If you have configured [path policy rules](#) for your remote sites, you can now specify that your [synthetic application tests](#) probe a particular SD-WAN path. This allows you to test the exact path your user traffic actually follows, eliminating irrelevant data from your analysis.

Focusing on these active paths provides an application experience score that accurately reflects real-world user experience. This precision helps you resolve issues faster, make better-informed decisions to improve application performance, and significantly lower your mean time to resolution.

Strata Cloud Manager: Policy Optimizer Enhancements

November 18, 2024

Supported on Strata Cloud Manager for:

- NGFW, including those funded by [Software NGFW Credits](#) (Managed by Strata Cloud Manager)
- Prisma Access (Managed by Strata Cloud Manager)

Here are the [Policy Optimizer](#) enhancements:

- Policy Optimizer considers rules created over 15 days ago for optimization.

- After optimizing a security rule, the Policy Optimizer feature will not reselect it for optimization for the next 90 days.
 - Recommendations automatically appear in the results after optimization.
 - To optimize a rule that wasn't automatically selected by Strata Cloud Manager, add the predefined **Enable-AIOps-Optimization** tag to it.
 - Displays the reason for optimization failure.
 - Displays negated addresses in the recommendations.
-

Overly permissive security rules—such as those allowing "any" application traffic—are common in large networks, creating security gaps by enabling unused applications and unnecessarily increasing the attack surface. Manual review and optimization of these broad rules require extensive log analysis and introduce deployment risk. Strata Cloud Manager introduces Policy Optimizer that analyzes log data to identify overly permissive security rules. [Policy Optimizer](#) auto-generates specific, focused rule recommendations based only on the applications actively observed on your network. This capability eliminates the need for manual log analysis, strengthens your security posture, and reduces administrative overhead. Administrators receive actionable, auto-generated optimization recommendations that can be reviewed and accepted through a guided workflow, ensuring that rule consolidation and replacement are secure and policy integrity is maintained. Together with [Config Cleanup](#), these tools help you ensure that your policy rules stay fresh and up to date.

Strata Cloud Manager: NGFW Support for Configuration APIs

November 15, 2024

Supported on Strata Cloud Manager for:

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

The Strata Cloud Manager Configuration APIs now support both the Next Generation Firewall and Cloud Next Generation Firewall platforms. This is in addition to the already existing support for the Prisma Access (SASE) platform. To support the additional platforms, the API documentation on pan.dev has a new organization that includes a Strata Cloud Manager-specific [landing page](#). The configuration API documentation has also been broken into functional areas and then [organized by platform](#).

Other major changes include:

- A new FQDN: api.strata.paloaltonetworks.com
- [Restructuring of the API paths](#) to support the new API organization.
- [Removal of query parameters for POST, PUT, and DELETE operations](#).

There are many other changes to the configuration APIs, both to support the new platforms, and to support new functionality. For complete details on this release, please see the [Strata Cloud Manager API November 2024 Release Notes](#).

25,000 Remote Network and 50,000 IKE Gateway Support

November 15, 2024

Supported for:

- Prisma Access (Managed by Strata Cloud Manager)
-

As enterprise networks expand, the ability to onboard and manage large-scale remote networks and IKE gateways becomes critical for maintaining performance and security. To accommodate the capacity increase for Prisma® Access deployments, [the Strata Cloud Manager web interface now provides enhanced tools](#) for navigating and managing large lists of remote networks and IKE gateways. These improvements, including advanced filtering, sorting, and grouping options, ensure administrators can quickly find, manage, and monitor remote networks, IPSec tunnels, and QoS settings, which significantly improves operational efficiency at scale.

The interface now provides pagination, allowing you to choose how many rows to display on a given page. A search ability is added, allowing you to find the desired remote network in the list by typing its Name in the text box. You can also group by compute locations. All groups display in a collapsed view and the page size you selected applies to the groups. When you select a compute location to expand it, the view displays based on the page size you selected.

DNS Proxy Customizations

October 15, 2024

Supported for:

- Prisma Access (Managed by Strata Cloud Manager)
-

Organizations using Explicit Proxy often face challenges integrating their cloud security with specialized internal network infrastructure, particularly regarding custom Domain Name Service (DNS) resolution. This limitation can interrupt seamless access to both public internet applications and critical internal private resources. Explicit Proxy now expands its capabilities to include comprehensive [DNS Proxy customization](#), solving this hybrid networking challenge. This feature allows you to seamlessly integrate regional DNS, custom third-party resolvers, or existing on-premises DNS infrastructure. By supporting FQDN-based resolution, the solution guarantees that all applications—whether public or privately hosted—are resolved correctly and securely. This optimization is supported on Panorama Managed Prisma® Access, delivering a more robust and flexible security posture for hybrid environments and optimizing the user experience.

Named Configuration Snapshots

November 15, 2024

Supported for:

- Prisma Access (Managed by Strata Cloud Manager)
-

- NGFW (Managed by Strata Cloud Manager)
-

Save a configuration as a named snapshot in Strata Cloud Manager for enhanced configuration management and version control. Previously in Strata Cloud Manager, users were limited to loading only previously pushed configurations that had been committed to the firewalls. This restriction meant that administrators had to manually keep track of configuration pushes and timing if they wanted to maintain access to a known good configuration they could fall back on during troubleshooting or rollback scenarios.

Now, with the new [Config Version Snapshot](#) dashboard, you can save any in-progress configuration as a named snapshot, providing unprecedented flexibility in configuration management workflows. Having a named snapshot capability allows you to preserve specific configuration states that you can easily load to restore Strata Cloud Manager to a known working state, regardless of whether that configuration was ever pushed to production firewalls.

The named configuration snapshots feature includes a dedicated management interface with their own organized table view, where you can assign descriptive names to each snapshot for easy identification and tracking. This naming convention enables teams to maintain clear documentation of configuration milestones, test states, or backup points. For example, you might save snapshots labeled "Pre-Migration Baseline," "Security Policy Update v2.1," or "Known Good State - Q4 2024."

When you save a named snapshot, it replaces the current configuration candidate in your workspace, allowing you to immediately begin working from that restored state. This functionality is particularly valuable for testing configuration changes, maintaining configuration templates, or quickly reverting to stable configurations during incident response scenarios.

Session Browser for Strata Cloud Managed NGFWs

November 15, 2024

Supported for:

- NGFW (Managed by Strata Cloud Manager)
-

To help troubleshoot your cloud managed NGFWs, a Session Browser is now available in Strata Cloud Manager. The session browser addresses common challenges faced by security teams who are unable to interface with their NGFWs directly due to various operational constraints, such as NGFWs not being physically on location, network connectivity issues, or security policies that restrict direct device access.

The Session Browser provides real-time visibility into network traffic and session data, enabling administrators to diagnose issues remotely without requiring physical presence at the NGFW location. When reviewing session information, you can leverage advanced filtering capabilities to quickly isolate relevant data by rules, sources, destinations, or App-ID™. This granular filtering allows for efficient troubleshooting by narrowing down sessions to specific applications, user groups, or network segments that may be experiencing issues.

Beyond the core session browsing functionality, this release consolidates previously scattered [troubleshooting capabilities](#) into a unified experience. The available troubleshooting tools for DNS Proxy, User IP mapping, User Group configurations, Routing tables, Dynamic User Group

membership, Dynamic Address Group populations, NAT policy evaluation, and External Dynamic Lists are now accessible through a single dashboard. This consolidation significantly reduces the time spent navigating between different interfaces and provides a complete view of your NGFW's operational status.

This feature allows distributed security teams to maintain optimal NGFW performance and quickly resolve network issues regardless of their physical proximity to the infrastructure.

Exclude URLs and Apps From Enterprise DLP Inspection for Non-File Based Traffic

November 1, 2024

Supported for:

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

Managing a complex security policy rulebase and minimizing false positive data loss prevention incidents requires fine-grained control over network inspection settings. The [Exclude URLs and Apps for Non-File Based Traffic](#) feature enables your data security administrators to precisely define traffic inspection exceptions within a DLP rule.

Your data security administrators can now easily exclude certain URLs and apps from having their non-file based traffic forwarded to for inspection. This exclusion capability is essential for several scenarios. For example, when you have traffic containing sensitive data destined for specific, trusted URLs and you want to exclude them from incident reporting, or when you only require file-based traffic inspection for specific apps but do not need inspection of accompanying non-file based data. This prevents unnecessary processing and avoids false positive detections.

By configuring these targeted exclusions using existing Security policy rules, you significantly ease the operational overhead of managing your policy rulebase, reducing the total number of policy rules required and improving overall system efficiency. This allows you to continue enforcing your data loss prevention requirements only where they are most needed.

Prisma Access Cloud Management Region Support

November 15, 2024

You can now deploy Prisma Access Cloud Management in the Switzerland region.

Supported on:

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

Strata Cloud Manager for Configuration Management is a solution that is defined and controlled based on the region where it is deployed. You can deploy Strata Cloud Manager in the locations of your choosing, based on data location preferences and where you have the most users. For this

reason, we are rolling out region-specific support for Strata Cloud Manager as soon as we are able to do so for [each region](#).

Update:

Strata Cloud Manager now supports the following additional regions:

- Saudi Arabia
- Israel
- Indonesia

Strata Cloud Manager: New Best Practice Assessment Checks and Custom Checks

November 15, 2024

Supported on Strata Cloud Manager for:

- NGFW, including those funded by [Software NGFW Credits](#)
- Prisma Access
- Prisma SD-WAN

Strata Cloud Manager introduces the following checks:

- [Custom checks](#) include support for verifying subnet matches within IP address objects and groups.
 - Device setup supports additional checks for management interface settings, session configurations, and dynamic update scheduler settings.
 - [Best Practices Assessment \(BPA\)](#) and [Custom checks](#) are available for [AI Access Security](#).
-

Strata Cloud Manager lets you validate your configuration against predefined [Best Practices](#) and custom checks you create based on the needs of your organization. As you make changes to your service routes, connection settings, allowed services, and administrative access settings for the management and auxiliary interfaces for your firewalls, Strata Cloud Manager gives you assessment results inline so you can take immediate corrective action when necessary. This eliminates problems that misalignments with best practices can introduce, such as conflicts and security gaps.

Inline checks let you:

- Gauge the effectiveness of, assess the impact of, and validate changes you make to your configuration using inline assessment results.
- Prioritize and perform remediations based on the recommendations from the inline assessment.

Strata Cloud Manager: Policy Analyzer for Strata Cloud Manager Deployments

November 15, 2024

Supported on Strata Cloud Manager for:

- NGFW, including those funded by [Software NGFW Credits](#) (Managed by Strata Cloud Manager or Panorama)
- Prisma Access (Managed by Strata Cloud Manager or Panorama)

[Policy Analyzer](#) now supports NGFWs and Prisma Access deployments managed by Strata Cloud Manager.

Time-sensitive security policy changes carry the high risk of introducing errors, misconfigurations, or conflicts into the rulebase, requiring slow and complex manual audit processes. Policy integrity is difficult to maintain at scale, leading to decreased performance and potential security gaps. Strata Cloud Manager introduces Policy Analyzer, enabling administrators to optimize time and resources when implementing any change request. [Policy Analyzer](#) provides immediate, automated analysis of the security rulebase to ensure policy updates meet defined intent and technical requirements. It proactively checks for anomalies, such as Shadows, Redundancies, Generalizations, Correlations, and Consolidations, that otherwise require labor-intensive manual checking. By identifying conflicting or duplicate rules before deployment, Policy Analyzer streamlines change management, reduces the risk of misconfiguration, and ensures the continued performance and integrity of your network security posture.

Strata Cloud Manager: Role-Based Access Control for Managing and Overriding Security Checks

November 15, 2024

Supported on Strata Cloud Manager for:

- NGFW
- Prisma Access

You can create or edit custom checks and override the security check block actions only through the Strata Cloud Manager interface.

Strata Cloud Manager introduces new permissions to enforce access control for managing security checks, managing security check exceptions, and overriding security check block actions. These permissions offer granular control and enhance security by preventing users from making unauthorized changes to the security checks essential for maintaining compliance. The new permissions are:

- **Manage Security Checks**

[Security checks](#) are a set of predefined best practice checks and custom checks that evaluate your configuration and identify deviations.

To view predefined best practice checks and perform actions such as creating, editing, deleting, or cloning custom checks, you will now need the necessary read and write access for the **Manage Security Check** permission.

- **Manage Security Check Exceptions**

[Security check exceptions](#) allow you to turn off specific security checks for certain devices in your environment.

To manage and view the security check exceptions, you will now need the necessary read and write access for the **Manage Security Check Exception** permission.

- **Override Security Check Block Action**

You can override the security check block action in two ways:

- When you [push the configuration](#) to the firewall, you can choose to ignore security check failures and continue with the push operation.
- When you create or edit a [Security Policy Rule](#), Strata Cloud Manager validates the rules against existing security checks. If the checks fail, you can choose to override and save the rule.

To perform any of the above override operations, you will now need read and write access for **Override Security Check Block Action** permission.

The following table outlines [the predefined roles](#) and the associated new permissions:

- **Superuser**

Includes read and write access for the following permissions:

- Manage Security Checks
- Manage Security Check Exception
- Override Security Check Block Action

- **Network Administrator**

Security Administrator

View Only Administrator

Includes read-only access for the following permissions:

- Manage Security Checks
- Manage Security Check Exception

For all other predefined roles, Strata Cloud Manager hides the **Security Checks** and **Security Check Exceptions** tabs in the **Security Posture Settings**. Alternatively, you can create or edit existing [custom roles](#) and configure the necessary permissions to view, manage, and override security checks.

Configure Source IP Address Enforcement for Authentication Cookies

November 15, 2024

Supported for:

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

In mobile and roaming environments, preventing session hijacking is critical for maintaining robust security. Previously, an endpoint's authentication cookie could be used even if the device's network location changed, creating a potential security risk if the cookie was intercepted.

To mitigate this threat, you can now enforce that the GlobalProtect portal or gateway accepts authentication cookies only when the endpoint's IP address matches the original source IP address or falls within a designated network range. This security enhancement is important for maintaining session integrity in environments where users may roam within a campus or corporate subnet.

Enabling this capability ensures that if the network originally issued an authentication cookie to an endpoint within a secure network range, the cookie remains valid only for endpoints within that same network segment. By binding the authentication cookie to a designated network range, you mitigate the risk of unauthorized access attempts.

This existing feature in Panorama is now available in Prisma Access managed by Strata Cloud Manager. For more information, see [GlobalProtect – Customize App Settings](#).

Configure End User Timeout Notifications

November 15, 2024

Supported for:

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

In remote and mobile work environments, unexpected session disconnections due to login lifetime or inactivity timeouts can interrupt user workflow and lead to poor productivity. Without advance warning, users may lose their context or unsaved work.

To prevent this frustrating experience, administrators can now configure timeout settings that proactively notify end users before a GlobalProtect session disconnects. This capability allows you to customize the following to provide a better user experience:

- **Advance Warning for Expiry:** Set the amount of advance notice users receive before a session expires due to the maximum Login Lifetime or Inactivity Logout period being reached.
- **Custom Notifications:** Tailor the notification message content to clearly inform users why their session is ending and what their next steps should be.

- Administrator Logout Message: Specify whether to notify end users and customize the display message when an administrator manually logs them out of a session.

By clearly communicating when sessions are about to expire, you help users save their work and re-establish a connection without interruption, improving security posture and reducing help desk tickets related to sudden disconnections.

This existing feature in Panorama is now available in Prisma Access managed by Strata Cloud Manager. For more information, see [configure timeout settings](#).

Strata Cloud Manager: NGFW Alerts in November

November 6, 2024

Here are the [NGFW alerts](#) introduced in November 2024:

- DHCP Client IPv4 address Assignment Failure
 - User authentication unsuccessful - "max_clock_skew"
 - User authentication unsuccessful - received out-of-band SAML message
 - System Drive or Connector fault
 - PA-5450 NC card - FE100 Failure
-

Health [alerts](#) actively monitor the health and performance of your platform in real time. This approach helps in identifying issues, predicting potential problems, and implementing remediation actions to ensure your devices function optimally. Here are some key aspects:

- Monitoring Metrics: Continuously monitor various metrics from the NGFWs, including CPU utilization, memory usage, disk space, network throughput, and other relevant performance indicators.
- Anomaly Detection: Generate alerts that dynamically adjust based on the metric's historical value and your usage trends.
- Predictive Analysis: Leverage historical data and patterns to predict when thresholds might be exceeded or specific events may occur. This helps forecast potential issues before they escalate.

New Features in October 2024

Here are the latest new features introduced on Strata Cloud Manager. Features listed here include some feature highlights for the [products supported with](#) Strata Cloud Manager. For the full list of new features supported for a product you're using with Strata Cloud Manager, [see the release notes for that product](#).

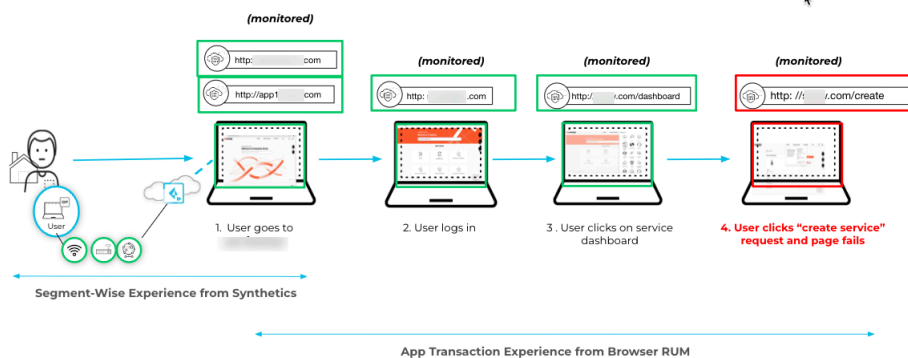
Autonomous DEM: Browser-Based Real User Monitoring (RUM)

October 31, 2024

Supported for:

- Autonomous Digital Experience Management (ADEM)
- Prisma Browser

Real User Monitoring (RUM) support is integrated into Autonomous Digital Experience Management (ADEM), marking a significant advancement in monitoring mobile user experiences. This capability utilizes a dedicated browser plugin to capture live web application performance directly from the end user's browser, providing critical visibility into real-time interactions with SaaS, internet, and data center applications. This method is essential for identifying in-browser friction points—such as slow page loads or delayed user actions—that traditional synthetic tests often fail to detect.



RUM provides the following key advantages to streamline support and optimization workflows:

- **Comprehensive View into User Experience:** Gather a set of metrics to help you understand the full user journey so that you can take the appropriate actions.
- **Enhanced Troubleshooting:** View real-time application availability, usability, and the performance of underlying dependencies, such as APIs or microservices, enabling quicker and more accurate troubleshooting.
- **Faster Remediation:** Combine RUM metrics with synthetic metrics to detect a wider range of performance degradation issues, identify root causes, and receive recommended remediation steps.

Forward Syslogs for Enterprise DLP Incidents

October 11, 2024

Supported for:

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

Security Operations Center (SOC) analysts and incident administrators require streamlined, automated workflows to effectively triage, review, and resolve data security risks. now supports [syslog forwarding](#) to enable your data security administrators to integrate into your organization's automatic incident integration within your established security operations platforms. Your data security administrator can create a Log Forwarding profile to automatically forward DLP incident syslogs to your third-party security information and event management (SIEM), Security Orchestration, and Response (SOAR), or other automated ticketing systems.

syslog forwarding provides substantial flexibility for large organizations. Your data security administrators can configure a single Log Forwarding profile for multiple enforcement points, or conversely, create a different Log Forwarding profile for each channel. They can also associate the same enforcement channel with multiple Log Forwarding profiles.

forwards DLP incident syslogs over a UDP or TCP port and requires a persistent connection to the receiving endpoint (SIEM, SOAR, or ticketing system). While automatically continues forwarding incident syslogs after connectivity is restored, the system cannot forward any syslogs that were generated during the period of disconnection. This integration into established systems allows teams to quickly incorporate data security risks into their operational cadence.

Simplified Application Test Configuration

October 31, 2024

Supported for:

- Autonomous Digital Experience Management (ADEM)
-

You can define [application tests](#) in ADEM with greater flexibility and precision to ensure better coverage of all application subdomains and dynamic services. Previously, App - IDs™ are used to define the targets for your application tests. This complexity often hindered rapid troubleshooting of user experience issues. To streamline this process and enhance coverage, Application tests in ADEM now use top-level domains or IP addresses instead of reliance on specific App - ID™ tags to define test targets. When you use a top-level domain as the target of your application test, the test automatically probes the related subdomains. This approach allows you to quickly pinpoint if any network or application components related to the subdomains are causing experience issues for users, simplifies diagnostics, and reduces mean time to resolution.

Streamlined Licensing for Strata Cloud Manager

October 16, 2024

Supported for:

- NGFW
 - Prisma Access
 - VM-Series, funded with Software NGFW Credits
-

A new licensing structure for Strata Cloud Manager is now available, featuring two licensing tiers: Strata Cloud Manager Essentials and Strata Cloud Manager Pro. This unified structure streamlines the deployment of network security offerings, including AIOps for NGFW, Autonomous Digital Experience Management (ADEM), cloud management functionality, and Strata Logging Service. Strata Cloud Manager offers a unified experience with the products accessible through a single interface, though you require separate licenses for each product to integrate them into the platform.

Here's an overview of the two licensing tiers available for Strata Cloud Manager:

- **Strata Cloud Manager Essentials** is the free tier that offers basic configuration and network security lifecycle management features to streamline operations and provide essential security.
- **Strata Cloud Manager Pro** is the paid tier that includes all features of Strata Cloud Manager Essentials, plus advanced features to enhance operational health, prevent network disruptions, strengthen real-time security posture, and ADEM for monitoring user experience performance. Strata Cloud Manager Pro includes Strata Logging Service with one year of log retention and unlimited storage, enabling centralized logging and seamless data retrieval across your deployment.

Strata Cloud Manager Essentials and Strata Cloud Manager Pro are available to activate in customer support portal (CSP) accounts that don't have: Strata Logging Service with sized storage, AIOps for NGFW Free or Premium, or Prisma Access.

For a detailed comparison of the available features and to learn more about how to activate these licenses, visit [Strata Cloud Manager License](#).

New Features in September 2024

Here are the latest new features introduced on Strata Cloud Manager. Features listed here include some feature highlights for the [products supported with Strata Cloud Manager](#). For the full list of new features supported for a product you're using with Strata Cloud Manager, [see the release notes for that product](#).

Prisma Access: Remote Browser Isolation in China

September 30, 2024

Supported for:

- Prisma Access (Managed by Strata Cloud Manager)
-

Remote Browser Isolation (RBI) is available in China to protect your users' managed devices from malware and potential zero-day attacks that result from standard web browsing activity. [RBI in China](#) works with Prisma® Access in China to isolate and transfer all browsing activity to the cloud-delivered platform. This ensures that potentially malicious code and content are secured and isolated away from your users' managed devices and the corporate network. This approach dramatically strengthens your security posture against highly evasive threats, especially those originating from risky websites.

Furthermore, the core capabilities available in RBI in China are the same as the RBI capabilities for the rest of the world, ensuring a consistent user experience globally, and the procedures for configuring RBI in China are identical to existing RBI configurations.

Panorama CloudConnector Plugin 2.1.0

September 25, 2024

Supported for:

- NGFW (Managed by Panorama or Strata Cloud Manager)
-

When managing Panorama, administrators require consistent security controls, including centralized proxy configuration, for all outgoing communications. Historically, the Panorama CloudConnector Plugin did not automatically inherit these settings, creating a security gap where essential interactions with cloud services bypassed the defined proxy policies. This lack of integration increased administrative overhead and compromised the overall consistency of the security posture.

The [Panorama CloudConnector plugin 2.1.0](#) now addresses this critical challenge by fully integrating with Panorama's centralized proxy configuration settings. This enhancement ensures that the plugin automatically uses proxy configuration defined in Panorama for all future interactions with the cloud. This integration simplifies administrative workflows, eliminates the risk of misconfiguration, and ensures unified security enforcement for connectivity to cloud platforms. See [Panorama CloudConnector Plugin Release Notes](#).

Prisma Access: Agent Proxy Support for Private IP from Branches

September 20, 2024

Supported for:

- Prisma Access (Managed by Strata Cloud Manager)
-

Visibility and enforcement based on an endpoint's [private IP address](#) was previously unavailable for users connecting via GlobalProtect[®] agent to the Explicit Proxy. This new feature solves that challenge by allowing you to now leverage the private IP addresses of endpoints for logging and to apply IP address-based enforcement. This enhancement[®] ensures consistent policy application and granular monitoring for users who connect to Prisma[®] Access Explicit Proxy through the agent from the branches.

Prisma Access: Explicit Proxy China Support

September 20, 2024

Supported for:

- Prisma Access (Managed by Strata Cloud Manager)
-

Multinational organizations operating in China face unique challenges in securing internet access for users and headless devices where VPN agents cannot be installed due to compliance reasons or network restrictions. Prisma[®] Access [explicit proxy](#) support in China addresses this critical need by providing a secure internet gateway that works without requiring default route changes to the infrastructure, while coexisting with VPN agents.

This solution also acts as a reliable proxy solution that complies with local regulations while effectively managing internet access and safeguarding sensitive information across endpoints. The explicit proxy support in China leverages AWS infrastructure with a 1:1 architecture where each Envoy proxy is paired with a proxy firewall virtual machine (VM). This architecture enables secure traffic handling while accommodating the unique networking constraints.

When you implement this solution, users connecting from branch locations **can access the internet securely** through the explicit proxy without having[®] clients installed. Additionally, headless devices such as IoT systems or servers **can route traffic** through the proxy for security inspection. The service integrates with your existing authentication methods, including SAML and Kerberos, and supports the same Security policy rules you configure for your global deployment. **Palo Alto Networks NGFW capabilities securely inspect traffic**, with logs and telemetry available through the same management interface you use for your global deployment. The architecture also supports routing specific domains to Service Connection when needed, providing flexibility for accessing both internet and private resources.

Prisma Access: Static IP Enhancements for Mobile Users

September 20, 2024

Supported for:

- Prisma Access (Managed by Strata Cloud Manager)
-

Managing mobile user access on networks that rely on IP address-based authorization is challenging because dynamic IP assignment from Prisma® Access can break access policies. The Static IP Allocation feature allows you to assign a [fixed IP address](#) to Prisma Access mobile users to address this challenge. This feature is useful if your network deployments restrict user access to resources using IP addresses as part of their network and application design. This functionality simplifies deployment and provides critical benefits:

You can [assign static IP addresses](#) for mobile users based on the Prisma Access theater or User-ID™

You can now use location groups and user groups to improve your IP address assignment for mobile users, in addition to theater and User-ID.

The supported number of IP address pool profiles is significantly increased, simplifying the management and scaling of large mobile user deployments.

Prisma Access: View Prisma Access, Dataplane, and Application and Threats Content Releases in Strata Cloud Manager and Panorama

September 20, 2024

Supported for:

- Prisma Access (Managed by Panorama or Strata Cloud Manager)
-

Managing component versions and tracking End-of-Support (EoS) dates across Prisma® Access, Dataplane, and content releases typically requires checking multiple locations. Prisma Access now lets you view the status of these components in a single page for [Prisma Access deployments managed by Strata Cloud Manager and Panorama®](#) and includes notifications that show you when your current running Panorama version and plugin versions will be EoS.

Prisma® Access consists of [components you manage](#) such as Panorama and the Cloud Services plugin, components that Prisma Access manages such as the dataplane version, and components that Prisma Access manages but whose version you can control (such as the GlobalProtect® version hosted on the Prisma Access portal). Prisma Access lets you view the status of these components in a single page and provides you with this information:

- [Prisma Access](#) version
- PAN-OS [dataplane version](#)
- Release Type (Preferred or Innovation)
- [Applications and Threats content version](#)

General Information

License

EditionPrisma Access Enterprise

Quantity2000 Mobile Users & 2000 Net (Mbps)

1725 DAYS REMAINING UNTIL05.03.2029

Software Information

Prisma Access Version5.1.0

Release TypePreferred

PAN-OS Version10.2.9

Applications and Threat Content8878-8899

Global Protect Recommended Versions6.1.0/6.0.8/6.0.7/6.2.4 (activated) (EOS)

Prisma Access Version

Prisma Access Version5.1.0

PAN-OS Version10.2.9

Release TypePreferred

Applications & Threat Content8877-8887

Prisma Access: New Prisma Access Cloud Management Location

September 20, 2024

Supported on Strata Cloud Manager for:

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

Cloud Management can now be deployed in the [Qatar region](#).

Prisma Browser Visibility

September 6, 2024

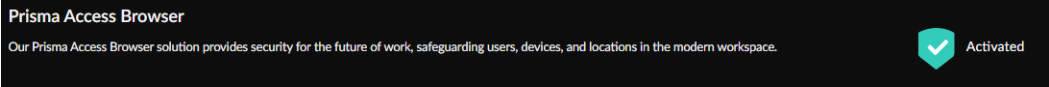
Supported for:

- Prisma Access customers with Prisma Browser and customers with Prisma Browser Standalone.
-

Depending on your license for [Prisma Access Browser Standalone](#) or [Prisma Access Browser with Prisma Access Enterprise Bundle](#), the following new items are available in Strata Cloud Manager for visibility:

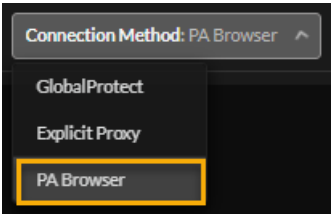
- **Monitor > Subscription Usage**

Now shows Prisma Access Browser, either fully activated or number allocated vs. available (if it's a partial allocation).

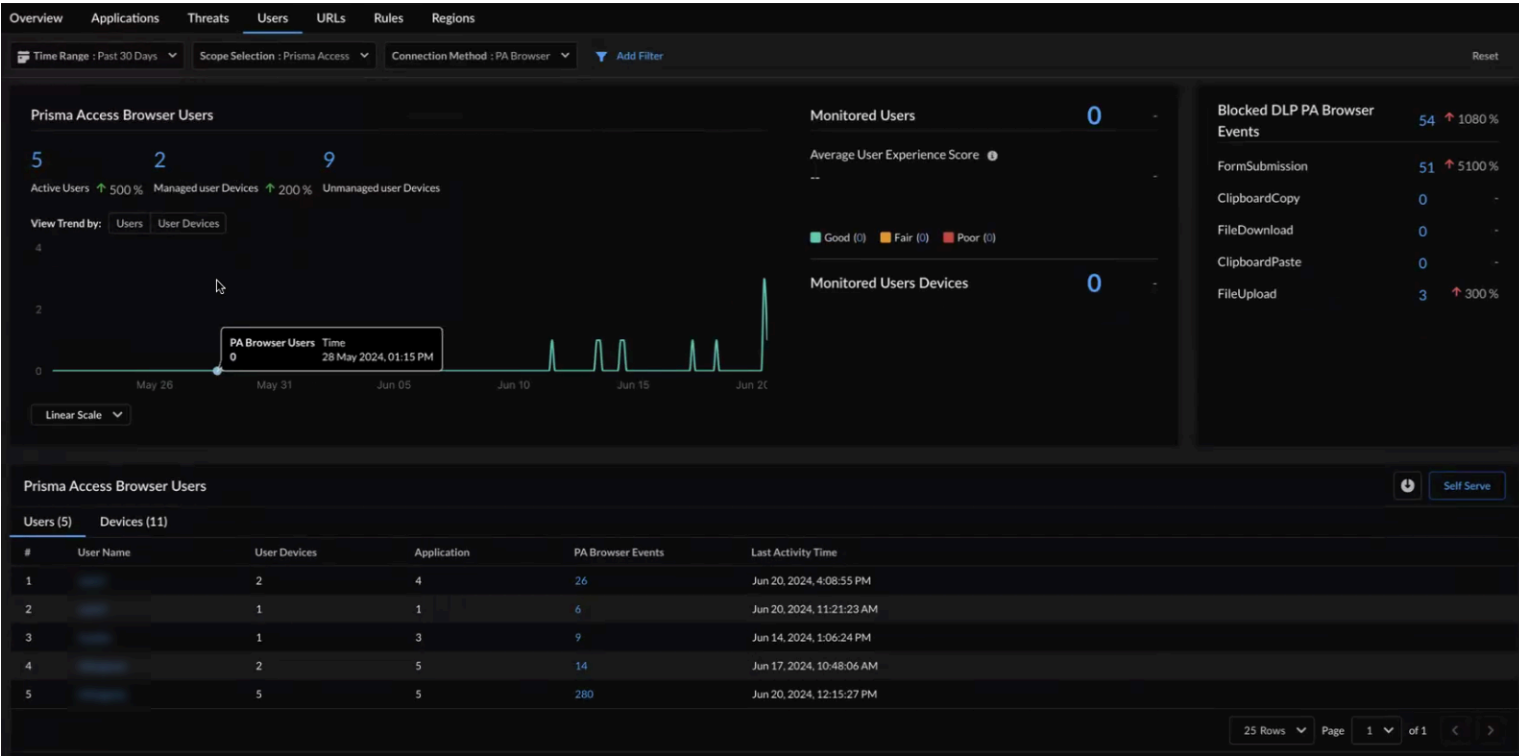


- **Activity Insights > Users**

New Connect Method = PA Browser

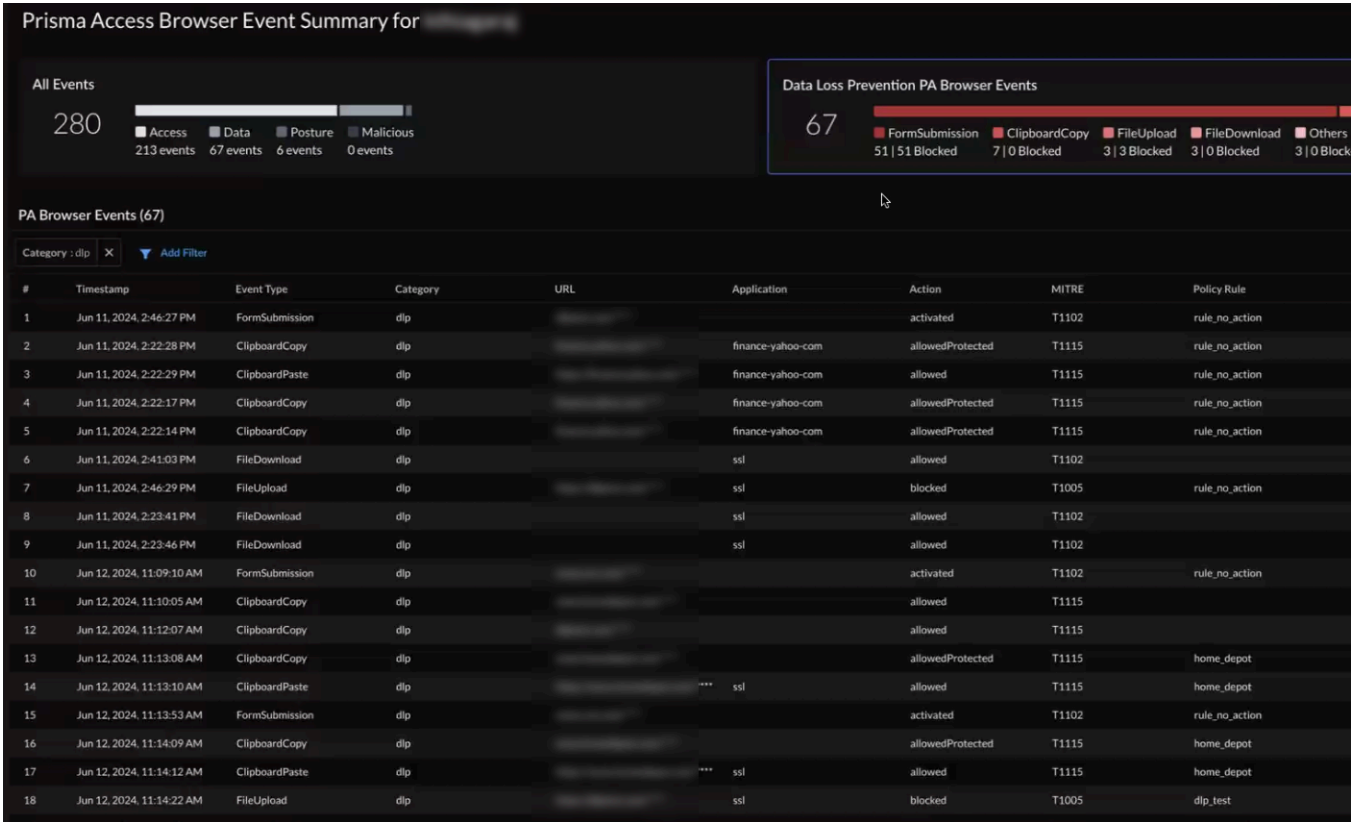


To see user and device details



- **Activity Insights > Users > details**

Select a user to drill down into details to see the new widgets such as the Prisma Access Browser Event Summary.



- **Activity Insights > Applications**

New column for count of PA Browser Events.

Application Name	Site Experience Score	Application Test Name	Application Test Time	Rule Name	PA Browser Events	Actions
------------------	-----------------------	-----------------------	-----------------------	-----------	-------------------	---------

Select the number of events and it will redirect you to the [Prisma Access Browser management pages](#).

- **Activity Insights > Applications > details**

Select an application to drill down into details to see the new widgets for PA Browser Access Events (the web apps or websites that users accessed) and PA Browser Data Events (the data control events that are performed) in the aggregate view or the breakdown view for allowed and blocked events.

Strata Cloud Manager: Enhanced Auto VPN Configuration for Large Enterprises

September 20, 2024

Supported for:

- [NGFWs \(Managed by Strata Cloud Manager\)](#)
-

It is a complex and often difficult process to add new sites and secure connectivity across all sites in distributed enterprises that have firewalls at the edge of their network. Additionally, securing these networks requires manual configuration that is time-consuming and prone to misconfiguration.

With these Auto VPN configuration enhancements, you can configure a link bundle that enables you to combine multiple physical links into one virtual SD-WAN interface. These bundles provide multiple and more robust options for path selection and failover protection that you can specify when you onboard a next-generation firewall (NGFW) as a branch device in the [VPN cluster](#) using Prisma® Access as a hub. With bundles that include more than one physical link, you maximize application quality when a physical link deteriorates.

Create a link bundle by assigning the same link tag (using an SD-WAN Interface profile) to multiple links that have similar access and SD-WAN policy rules. For example, you can create a link tag named *Low Cost Broadband* and then use it to tag your cable modem and fiber optic broadband services.

In addition to improving the Auto VPN configuration settings, we extended Auto VPN connectivity to 500 sites per tenant.

Strata Cloud Manager: Advanced DNS Security

September 20, 2024

Supported for:

- Prisma Access (Managed by Strata Cloud Manager)
 - Feature first introduced in PAN-OS 11.2.
 - Additional feature support added in Panorama Managed Prisma Access deployments in Prisma Access 5.1 Innovation
-

The [Advanced DNS Security service](#) is a new subscription offering by Palo Alto Networks that operates new domain detectors in the Advanced DNS Security cloud that inspect changes in DNS responses to detect various types of DNS hijacking in real-time. With access to Advanced DNS Security, you can detect and block DNS responses from hijacked domains and misconfigured domains. Hijacked and misconfigured domains can be introduced into your network by either directly manipulating DNS responses or by exploiting the DNS infrastructure configuration settings in order to redirect users to a malicious domain from which they initiate additional attacks. The primary difference between these two techniques is where the exploit occurs. In the case of DNS hijacking, the attackers gain the ability to resolve DNS queries to attacker-operated domains by compromising some aspect of an organization's DNS infrastructure, be it through unauthorized administrative access to a DNS provider or the DNS server itself, or an MiTM attack during the DNS resolution process. Misconfigured domains present a similar problem - the attacker seeks to incorporate their own malicious domain into an organization's DNS by taking advantage of domain configuration issues, such as outdated DNS records, which can enable attackers to take ownership of the customer's subdomain.

Advanced DNS Security can detect and categorize hijacked and misconfigured domains in real-time by operating cloud based detection engines, which provide DNS health support by analyzing DNS responses using ML-based analytics to detect malicious activity. Because these detectors are located in the cloud, you can access a wide array of detection mechanisms that are updated and deployed automatically without requiring the user to download update packages when changes to detectors are made. Upon initial release, Advanced DNS Security supports two analysis engines: DNS Misconfiguration Domains and Hijacking Domains. Additionally, DNS responses for all DNS queries are sent to the Advanced DNS Security cloud for enhanced response analysis to more accurately categorize and return a result in a real-time exchange. Analysis models are delivered through content updates, however, enhancements to existing models are performed as a cloud-side update, requiring no updates by the user. [Advanced DNS Security is enabled and configured](#) through the Anti-Spyware (or DNS Security) profile and require active Advanced DNS Security and Advanced Threat Prevention (or Threat Prevention) licenses.

Strata Cloud Manager: Local Deep Learning for Advanced Threat Prevention

September 20, 2024

Supported on Strata Cloud Manager for: Prisma Access (Managed by Strata Cloud Manager)

- First introduced in PAN-OS 11.2.
-

When handling high volumes of evasive threats or operating under challenging network conditions, relying solely on cloud-based threat analysis can introduce unwanted latency. [Local Deep Learning for Advanced Threat Prevention](#) solves this challenge by providing fast, local deep learning-based analysis for zero-day threats, complementing the [cloud-based Inline Cloud Analysis](#) component of Advanced Threat Prevention.

With an active Advanced Threat Prevention license, the system quickly analyzes known malicious traffic matching published signatures and applies the configured action, such as dropping the session. For suspicious content, the Deep Learning Analysis detection module reroutes the traffic locally for immediate analysis. Because this module is based on the proven detection engines operating in the Advanced Threat Prevention cloud, you gain the same zero-day and advanced threat detection capabilities, but with the added benefit of processing a much higher traffic volume locally. This allows you to inspect more traffic and receive rapid verdicts without the lag associated with cloud queries. Content updates deliver the latest Local Deep Learning models, ensuring your detection remains current.

Strata Cloud Manager: New Check Box for Overriding Security Checks

September 20, 2024

Supported for:

- Prisma Access (Managed by Strata Cloud Manager)
-

- NGFW (Managed by Strata Cloud Manager)
-

In security environments, strict validation checks are critical for maintaining a robust security posture, but this rigidity can sometimes be an obstacle. When pushing a configuration, a failed security check with a "block" action can halt the entire deployment process. This creates unnecessary friction in time-sensitive situations, forcing you to delay or manually reconfigure to bypass the strict rule.

Strata Cloud Manager now addresses this pain point by introducing a feature in the [Push Config dialog box](#) that allows you to override specific security check failures that would normally block a push operation. This enhancement gives you the power and flexibility to continue the deployment when you have a valid reason to proceed, ensuring you are not stalled by strict checks. This capability allows you to balance security enforcement with operational efficiency while still ensuring that all validation errors are visible for your review and necessary investigation.

GlobalProtect: Support for PAN-OS-11.2-DHCP-Based IP Address Assignments

September 20, 2024

Supported on NGFW:

- First introduced in PAN-OS 11.2.0 .
-



Starting from PAN-OS 11.2.1, the DHCP Based IP Address Assignment feature is supported for both VM-Series virtual firewall and hardware next-generation firewall platforms.

DHCP Based IP Address Assignment feature in PAN OS 11.2.0 release is supported for VM-Series Virtual Firewalls only. The feature is not supported for hardware next-generation firewall platforms.

You can now [configure a DHCP server profile on the GlobalProtect gateway to use DHCP server for managing and assigning IP addresses for the endpoints](#) connected remotely through the GlobalProtect app. Users who are using enterprise DHCP servers can enable this feature for centralized IP management and IP address assignments. When you configure a DHCP server profile on the GlobalProtect gateway and upon successful communication between the gateway and the DHCP server, the gateway obtains DHCP IP addresses from a DHCP member server. The GlobalProtect gateway then assigns the IP addresses as the tunnel IP for the endpoints that are remotely connected through the GlobalProtect app. If the DHCP server fails to respond to the gateway within the set communication timeout and retry times period, the gateway falls back to the private Static IP pool for the allocation of IP addresses for the endpoints.

When the GlobalProtect gateway assigns the DHCP IP addresses to the endpoints, you can configure their DHCP server to create Dynamic DNS (Address and Pointer Record) records for the GlobalProtect connected users. DDNS are useful for endpoint admins to do troubleshooting on the GlobalProtect connected remote user endpoints. The IP addresses get registered to the DDNS server only when you configure IP Address Management (IPAM) on Windows server, DDNS server, or on the Infoblox server.

GlobalProtect: Use Default Browser for SAML/CAS Authentication

September 20, 2024

Supported on NGFW

- First introduced in PAN-OS 11.1.0
-

This feature enables you to configure the GlobalProtect app to [use the default browser](#) to authenticate to the GlobalProtect portal through the **Client Authentication** setting of the portal configuration. You can now select the **Use Default Browser** option on the **Client Authentication** screen for the app to use the default browser for SAML/CAS authentication to authenticate to the portal for the first time. The **Use Default Browser** option is displayed on the **Client Authentication** screen only when you choose SAML/CAS as the authentication profile.

Starting from PAN-OS 11.1, you do not need to set the pre-deployment keys/plist entries to configure the app to choose whether the app should use the default browser or embedded browser instead you can configure it through the Client Authentication setting of the portal configuration.

End users can benefit from using the [default system browser for SAML authentication](#) because they can leverage the same login for GlobalProtect with their saved user credentials on the default system browser such as Chrome, Firefox, or Safari.



This feature is available starting from the PAN-OS 11.1 version. For the earlier PAN-OS versions, you must use the predeployment registry key/plist setting.

Advanced URL Filtering: URL Categorization Check

September 20, 2024

Supported for:

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

To configure URL Access Management profiles (also known as URL Filtering profiles) and Security policy rules that block and allow the intended web traffic, you need to know the current URL categorization of a website. You also use this information to [create a custom URL category](#) or troubleshoot why a website isn't blocked or allowed as expected. While you can look up any URL on Palo Alto Networks [Test A Site](#) website, doing so requires navigating away from the management interface.

To make URL lookups more convenient and efficient, PAN-OS® 11.1 adds a [URL category](#) checker where you configure URL Access Management profiles. The category checker provides in-product access to Test A Site, which queries PAN-DB, Palo Alto Networks cloud-based URL database. Enter a domain or URL, and the results panel shows two distinct sections: one for the primary URL category and one for the risk category. Each section includes a description of the

category and corresponding example sites. If you disagree with the primary URL category, you can [initiate a change request](#) from the results panel. This action redirects you to a prepopulated form on the external Test A Site website.

Enhanced Report Management

September 27, 2024

Supported for:

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

Managing network visibility often requires switching across multiple dashboards to analyze data. [Centralized Report Management](#) in eliminates this need by offering a unified system to enhance visibility of network activity within your organization and help analyze historical and track real-time data based on your needs. You can download reports using data from the dashboards and Activity Insights Summary for Prisma® Access and your Palo Alto Networks Next-Generation Firewalls (NGFWs). enables you to share and schedule reports at your preferred intervals.

Strata Cloud Manager generates reports using either the last 24 hours of data or the data from the past 30 days depending on the default time period settings on the dashboard. However, you can customize the time period for gathering data in a report when you schedule it. You can also manage scheduled and downloaded reports from the past 30 days to help you monitor and troubleshoot network activity effectively when needed.

New Features in August 2024

Here are the latest new features introduced on Strata Cloud Manager. Features listed here include some feature highlights for the [products supported with Strata Cloud Manager](#). For the full list of new features supported for a product you're using with Strata Cloud Manager, [see the release notes for that product](#)

AI Access Security

August 16, 2024

Supported for:

- NGFW (Managed by Panorama or Strata Cloud Manager)
 - Prisma Access (Managed by Panorama or Strata Cloud Manager)
-

We introduced to [enable businesses to safely adopt GenAI apps](#) across their organization by mitigating the risks associated with data leakage in prompts and malicious content in responses. includes an extensive dictionary of generative artificial intelligence (GenAI) apps to help you identify GenAI apps alongside contextual, fine-grained access control policy rules to help you prevent exfiltration of sensitive data. also provides detailed monitoring capabilities that enable you to filter for specific GenAI apps, users, and GenAI use cases, which in turn enables you to write targeted Security policy rules to strengthen your security posture that help you control the data leaving your organization for GenAI apps allowed within your organization.

GenAI apps are AI apps capable of generating text, images, videos, and other forms of data in response to user prompts and continuously learn based on user inputs. Their usage is proliferating at an astonishing rate and offer limitless opportunities for businesses. However, the nature by which GenAI apps contentiously improve presents a new danger to businesses and security administrators — how can you ensure your employees are not exposing sensitive or proprietary data to GenAI apps?

is powered by three core principals that allow your organization to safely use GenAI apps while ensuring your sensitive or proprietary data isn't exposed.

- **Identify and Control GenAI Apps**— provides robust GenAI app taxonomy, attributes, and access control tools to identify and manage which GenAI apps are sanctioned, tolerated, or unsanctioned in your corporate network.
- **Comprehensive Visualization and Reporting**—Your manage entirely from —your single pane of glass management experience across your security enforcement channels. includes a detailed dashboard that displays trends that help you to filter and explore usage based on users, data transfers, GenAI apps, and use cases across all channels. You can also generate executive summary reports to summarize GenAI app usage, policy violation metrics, and other important data security metrics.
- **Data Protection**—, the cloud-based data loss prevention service that uses AI and supervised machine learning algorithms, is the detection engine that enables you to prevent the exfiltration of sensitive data for file and non-file based uploads and text prompts.

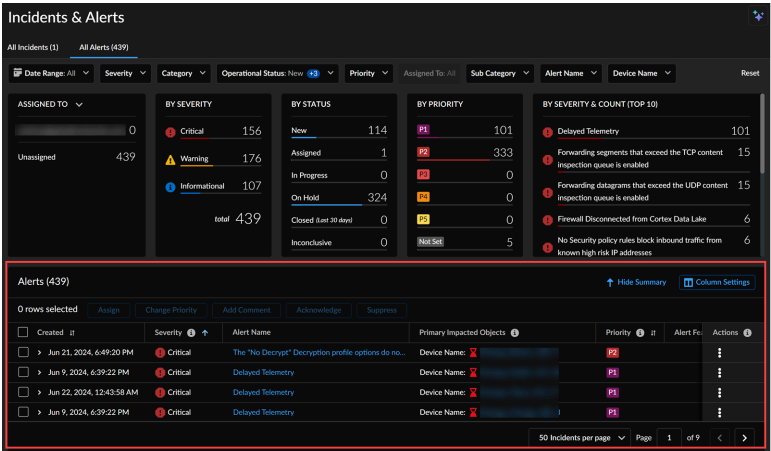
Streamlined NGFW Incidents and Alerts Management

August 15, 2024

Supported for:

- AIOps for NGFW Free
- Strata Cloud Manager

Navigating between incident summaries and detailed alert lists often requires additional steps and causes context loss, slowing down critical security response times. The Strata Cloud Manager **Incidents & Alerts** page now centralizes these views, allowing administrators to rapidly identify and respond to critical security events occurring across Next-Generation Firewalls (NGFWs). The unified view presents critical visual summaries and the corresponding detailed list side-by-side. You quickly grasp the overall context of an incident from the charts and immediately dive into the specifics without navigating away from the triage workflow. This streamlined access empowers you to conduct faster, more effective triage, helping you respond to security events with greater speed and confidence.



Prisma Access Browser

August 12, 2024

Supported for:

- Prisma Access (Managed by Strata Cloud Manager)

The **Prisma Access Secure Enterprise Browser (Prisma Access Browser)** is a browser designed specifically for enterprise use and is fortified with security features to protect users and organizations against cyberthreats like phishing, malware, eavesdropping, and data exfiltration.

The initial release of Prisma Access Browser includes the following:

- Third-Party Access: contractors, partners, consumers, or students needing secure access to SaaS or private web apps on their unmanaged devices.

- Bring Your Own Device Access: employees using personal devices (mostly mobile) for work.
- Temporary Secure Access: employees needing access to critical apps, such as Human Resources and Payroll, during agent rollouts or network merges.
- Secure Access for managed devices: employees using work devices accessing highly sensitive data.

More about [Prisma Access Browser](#).

You can create and manage role-based access control for different types of administrators of the Prisma Access Browser. This allows the main administrator in a large organization to appoint additional administrators with relevant permissions for their specific roles, including visibility and access.

After activating your Prisma Access Browser license, you can manage admin user access and assign one of the following roles that are specific to Prisma Access Browser.

More about [roles and permissions](#) and [assigning predefined roles](#).

New Features in July 2024

Here are the latest new features introduced on Strata Cloud Manager. Features listed here include some feature highlights for the [products supported with Strata Cloud Manager](#). For the full list of new features supported for a product you're using with Strata Cloud Manager, [see the release notes for that product](#)

Email DLP Enhancements

July 29, 2024

Supported for:

- Data Security
-

Enterprise Data Loss Prevention (E-DLP) introduced the following enhancements to [Email DLP](#) to strengthen your security posture when inspecting outbound emails from your organization and prevent exfiltration of sensitive data.

- You can now forward outbound Gmail and Microsoft Exchange emails to your Proofpoint server and to encrypt them on their way to the target recipient whenever Enterprise DLP detects sensitive data. Encrypting outbound emails containing sensitive data prevents unauthorized individuals from reading these email messages.
- Email DLP now supports inspection of .eml files and up to five levels of nested .eml email files. However, Enterprise DLP can only detect nested .eml files,—Enterprise DLP can't detect and inspect nested files in any other supported file types.
- (**Microsoft Exchange only**) You can now configure Enterprise DLP to send an email notification to the sender of the outbound that matches the Email DLP policy rule. This enables Enterprise DLP to detect sensitive data immediately and notify email senders who their email wasn't sent out to the intended recipient due to a data security violation. As a result, the email sender knows about the block and can modify their email appropriately and attempt to resend it.

You can use the automated email notification feature only for Email DLP policy rules where the response **Action** is **Forward email for approval to end user's manager** **Forward email for approval to admin**, or **Quarantine**.

Browser Support for Remote Browser Isolation

July 26, 2024

Supported for:

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

In addition to Google Chrome, Microsoft Edge, and Safari browsers, the Firefox browser is now supported for Remote Browser Isolation (RBI) on macOS and Windows desktop operating systems.

Refer to [How Remote Browser Isolation Works](#) for the combination of operating systems and browsers that your users can use for isolated browsing.

Mobile Support for Remote Browser Isolation

July 26, 2024

Supported for:

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

To help broaden the device support for your managed users, mobile support is added for Remote Browser Isolation (RBI) in addition to macOS and Windows desktop operating systems. Your managed users can now use Android, iOS, and iPadOS devices for isolated browsing.

Refer to [How Remote Browser Isolation Works](#) for the combination of operating systems and browsers that are supported for RBI.

Prisma AIRS

July 24, 2024

Supported for:

- Prisma AIRS (Managed by Strata Cloud Manager)
-

Palo Alto Networks Prisma AIRS is a purpose-built firewall to discover, protect, and defend the enterprise traffic flows against all potential threats focusing on addressing AI-specific vulnerabilities such as prompt injection, and denial-of-service attacks on AI models. It combines continuous runtime threat analysis of your AI applications, models, and data sets with AI powered security to stop attackers in their tracks. The Prisma AIRS leverages real-time AI-powered security protecting your AI application ecosystem from both AI-specific and conventional network attacks.

Prisma AIRS leverages critical anomaly detection capabilities and protects AI models from manipulation to ensure the reliability and integrity of AI output data. It rejects prompt injections, malicious responses, training data poisoning, malicious URLs, command and control, embedded unsafe URLs, and lateral threat movement.

Prisma AIRS uses Palo Alto Networks Strata Cloud Manager (SCM) as the main configuration and management engine. To begin with, activate and onboard your cloud service provider account on SCM. The AI Security Profile imports security capabilities from Enterprise DLP and URL Filtering for inline detection of threats in AI application traffic.

The Prisma AIRS is powered by the following four key elements:

Discover - The Prisma AIRS discovers your enterprise AI application and all other applications. The Prisma AIRS dashboard provides complete visibility and security insights of your AI and other applications in just a few clicks. You can effortlessly gain actionable intelligence on AI traffic flows covering your applications, models, user access, and infrastructure threats.

Deploy - The Prisma AIRS deployment using Terraform templates automates the deployment procedure reducing the human error, lowering the required time for manual configuration tasks, and for protecting your enterprise AI applications. Deploy your Prisma AIRS instance downloading the Terraform templates and provide permissions to your cloud service provider account projects to analyze flow logs and DNS logs.

Detect - Identify unprotected traffic flows with potential security threats to the cloud network and detect the potential security risks based on logs and recommended actions to remediate.

Defend - Shield your organization's AI application ecosystem from AI-specific and conventional network attacks by leveraging real-time AI-powered security. Get the continuous discovery of the AI network traffic on the containers and namespaces.

To learn more about AI Runtime Security activation, onboarding, and deployment, see [AI Runtime Security](#) documentation.

Dynamic Privilege Access

July 24, 2024

Supported for:

- Prisma Access (Managed by Strata Cloud Manager)
-

For Enterprise IT and IT Enabled Services (ITES) companies that need to control which users have access to their customer projects, [Dynamic Privilege Access](#) provides a seamless, secure, and compartmentalized way for your users to access only those projects that they are assigned to. Employees are typically assigned to several customer projects and are provided with siloed access to these projects so that an authorized user can access only one customer project at a time.

A new predefined role called the **Project Admin** is available to allow project administrators to create and manage project definitions. Project administrators have the ability to map projects to select Prisma Access location groups, and create IP address assignments using DHCP based on the project and location group.

Panorama to Strata Cloud Manager Migration

July 24, 2024

Supported for:

- Prisma Access (Managed by Strata Cloud Manager)
-

If you have use Panorama to manage your existing Prisma Access deployment, Palo Alto Networks introduces an [in-product workflow](#) to help you migrate your existing Prisma Access configuration to Strata Cloud Manager. Palo Alto Networks disables this migration workflow by

default but, when you're ready to migrate to cloud management, you can contact your account team to enable this feature and begin your migration.

The benefits of moving to Strata Cloud Manager include:

- Continuous Best Practice Assessments
- Secure default configurations
- Machine learning (ML)-based configuration optimization
- Simplified web security workflow
- Comprehensive and actionable visualizations
- Intuitive workflows for complex tasks
- Simple and secure management APIs
- Cloud-native architecture provides scalability, resilience, and global reach
- No Panorama hardware to manage or software to maintain

View and Monitor Dynamic Privilege Access

July 24, 2024

Supported for:

- Prisma Access (Managed by Strata Cloud Manager)
-

Dynamic Privilege Access enables Prisma Access to apply different network and Security policy rules to mobile user flows based on the project your users are working on. In the Strata Cloud Manager Command Center, you can [view user-based access information in your environment](#).

Gain visibility into your Prisma Access Agent deployment by using Strata Cloud Manager to monitor your users' project activity. In the Strata Cloud Manager Command Center, you can view [project-based access information in your environment](#).

Support for Deleting Connector IP Blocks

July 24, 2024

Supported for:

- Prisma Access (Managed by Strata Cloud Manager)
-

To allow more flexibility after you configure Connector IP Blocks, you can now [delete and update](#) the Connector IP Blocks. However, you can delete the Connector IP Blocks only after you delete all the ZTNA objects such as connectors, applications, wildcards, and connector-groups on the tenant.

Strata Cloud Manager: Cross-Scope Referenceability in Snippets

July 24, 2024

Supported for:

- Prisma Access (Managed by Panorama or Strata Cloud Manager)
 - NGFW (Managed by Panorama or Strata Cloud Manager)
-

Enterprises need to enforce configuration objects and global settings consistently across all deployments. By referencing global settings across various scopes, such as snippets or folders, organizations can streamline operations, eliminate redundant configurations, and enhance centralized management. For example, organizations can effectively manage custom URL categories for access policy rules, threat prevention profiles, zones, addresses, and other objects representing standard network segments.

This feature allows you to reference any common configurations or objects attached to a global scope and push to NGFWs or Prisma Access deployments. These shared objects and configurations within the global scope are available to all the snippets. Snippets associated with the global scope are considered a global snippet, and the objects defined within these snippets can be [referenced](#) across any snippets in the configuration. This simplifies the process of managing configurations from a single location, updating, and enforcing global standards across all deployments.

Strata Cloud Manager: Disable Default HIP Profiles

July 24, 2024

Supported for:

- Prisma Access (Managed by Panorama or Strata Cloud Manager)
 - NGFW (Managed by Panorama or Strata Cloud Manager)
-

The default HIP objects and HIP profiles in Strata Cloud Manager have been moved from the Global-Default snippet to the HIP-Default snippet, providing greater flexibility in managing the default HIP profiles. You can choose to [disable the default HIP profiles](#) by disassociating the HIP-Default snippet from the global folder.

Enterprise DLP: File Type Exclusion

July 24, 2024

Supported for:

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

Enterprise Data Loss Prevention (E-DLP) now supports creating a file type exclusion list when modifying a [DLP Rule](#) to define the type of traffic to inspect, the impacted file types, action, and log severity for the data profile match criteria. Creating a file type exclusion list, rather than an inclusion list, instructs the NGFW or Prisma Access tenant to forward all file types except for those specified in the exclusion list to Enterprise DLP for inspection and verdict rendering. A DLP Rule can be configured with an inclusion or exclusion file type list, but not both.

Forward Email Alerts and SNMP Traps to External Servers

July 24, 2024

Supported for:

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

You can now configure [email alerts](#) for log types, such as System, Config, HIP Match, Correlation, Threat, WildFire Submission, and Traffic logs. For each log type, you can set up separate email profiles that allow you to send notifications to different email servers based on the log type. You can define up to four servers within a single profile to ensure high availability. You can enable transport layer security (TLS) to prevent malicious activities, such as Simple Mail Transfer Protocol (SMTP) relay attacks and email spoofing.

You can use Simple Network Management Protocol (SNMP) traps to receive alerts for critical system events, such as hardware or software failures or changes in Palo Alto Networks firewalls. Additionally, you can receive alerts when there is any traffic that matches a firewall security rule and needs immediate attention.

Configure Management Settings

July 24, 2024

Supported for:

- NGFW (Managed by Strata Cloud Manager)
 - Prisma Access (Managed by Strata Cloud Manager)
-
- Configure Banners, Message of the Day, and Logos
- You can now include a login banner to the login page of Strata Cloud Manager. Login banner is optional text that displays critical information that administrators need to see before they log in, such as login instructions. You can add coloured bands that highlight overlaid text across the header and footer to ensure administrators see critical information, such as the classification level for firewall administration.
- You can add a message of the day that displays in a dialog after administrators log in to ensure they see important information, such as an impending system restart that can affect their tasks. The same dialog also displays messages that Palo Alto Networks embeds to highlight important information associated with a software or content release.

- **Configure Sessions Settings**

You can now customize the default session settings to better suit your requirements and optimize network performance and security. You can specify whether to apply newly configured security policy rules to sessions that are in progress. You can configure IPv6 settings, enable jumbo frames and set the maximum transmission unit (MTU), enable ERSPAN support, and tune NAT session settings.

- **Configure Management Interface Settings**

You can now configure the interface speed and set the MTU for packets sent on this interface.

New Features in June 2024

Here are the latest new features introduced on Strata Cloud Manager. Features listed here include some feature highlights for the [products supported with Strata Cloud Manager](#). For the full list of new features supported for a product you're using with Strata Cloud Manager, [see the release notes for that product](#).

Prisma Access: Third-Party CDR Integration for Remote Browser Isolation

June 28, 2024

Supported for:

- Prisma Access (Managed by Strata Cloud Manager)
-

Protect your users against zero-day threats hidden in files that they download from the internet by [integrating Remote Browser Isolation \(RBI\) with a third-party content disarm and reconstruction \(CDR\) provider](#).

When users browse the web and download various types of files to their local devices, they are exposed to zero-day threats. Even with file scanning or antivirus solutions in play, these threats could escape detection, allowing malware to be delivered to your users' managed devices and rendering them as patient-zero.

With third-party CDR integration, any files downloaded while in RBI will be disarmed and reconstructed using CDR. The CDR provider will remove the malicious content from the files and deliver the sanitized files in their original file formats to the user.

You can [integrate with Votiro](#) to utilize Votiro's CDR capabilities to process and appropriately sanitize a file before it is downloaded to the user's device from RBI, thus keeping the user protected from any potentially malicious executables embedded in the file.

Strata Cloud Manager: Custom Checks for Security Profiles

June 14, 2024

Supported for:

- NGFWs (Managed by Strata Cloud Manager)

[Custom checks](#) have been newly added to the following security profiles:

- DNS Security Profile
 - File Blocking Profile
 - Anti Spyware Profile
 - Vulnerability Protection Profile
 - Decryption Profile
-

Strata Cloud Manager lets you validate your configuration against predefined [Best Practices](#) and custom checks you create based on the needs of your organization. As you make changes to your service routes, connection settings, allowed services, and administrative access settings for the management and auxiliary interfaces for your firewalls, Strata Cloud Manager gives you assessment results inline so you can take immediate corrective action when necessary. This eliminates problems that misalignments with best practices can introduce, such as conflicts and security gaps.

Inline checks let you:

- Gauge the effectiveness of, assess the impact of, and validate changes you make to your configuration using inline assessment results.
- Prioritize and perform remediations based on the recommendations from the inline assessment.

Strata Cloud Manager: New Inline Best Practice Checks

June 14, 2024

Supported for:

- [NGFWs \(Managed by Strata Cloud Manager\)](#)

The new [inline checks](#) empower you to:

- Secure your GlobalProtect Gateway server authentication SSL/TLS Service Profile by ensuring that it is set to the minimum version "TLS 1.2," guarding against vulnerabilities inherent in weaker TLS versions.
- Safeguard your business by ensuring that you use sanctioned applications, distinguishing officially approved SaaS applications from unsanctioned ones that may be tolerated or blocked for employee use.
- Enhance monitoring by ensuring that you enable keep-alive for HA2. This helps you to monitor the connection between the device and its HA peer on the HA2 link to ensure that the connection is up.
- Optimize security by ensuring that the Authentication Portal session timeout in Redirect mode is set to greater than recommended value.
- Verify management interface settings, including connection settings, allowed services, and administrative access permissions over the management interface.
- Check session settings such as rematching sessions, accelerated aging, timeouts, and Global Packet Buffer Protection.
- Ensure dynamic updates scheduler settings for Antivirus, Applications and Threats, and WildFire are correctly configured.

Strata Cloud Manager lets you validate your configuration against predefined [Best Practices](#) and custom checks you create based on the needs of your organization. As you make changes to your service routes, connection settings, allowed services, and administrative access settings for the management and auxiliary interfaces for your firewalls, Strata Cloud Manager gives you assessment results inline so you can take immediate corrective action when necessary. This

eliminates problems that misalignments with best practices can introduce, such as conflicts and security gaps.

Inline checks let you:

- Gauge the effectiveness of, assess the impact of, and validate changes you make to your configuration using inline assessment results.
- Prioritize and perform remediations based on the recommendations from the inline assessment.

Cloud Management for NGFWs: Auto VPN Configuration for HA Pairs

June 14, 2024

Supported for:

- [NGFWs \(Managed by Strata Cloud Manager\)](#)
-

(**HA deployments only**) In an Auto VPN with SD-WAN configuration, the [Auto VPN can now generate the appropriate configuration](#) automatically for the active and passive HA peers (both branch and hub HA pairs). It enables the HA failovers to be seamless between the HA pairs.

Prisma Access: Fast-Session Delete

June 14, 2024

Supported on Strata Cloud Manager for: Prisma Access (Managed by Strata Cloud Manager)

If your Prisma® Access deployment uses a large number of sessions, and you would like to delete those sessions quickly, you can enable [fast session delete](#), which allows Prisma Access to reuse TCP port numbers before the TCP TIME_WAIT period expires. This reuse of the TCP port numbers can be useful if your deployment has a large number of SSL decrypted sessions that may be short-lived. You can choose to enable this functionality for Prisma Access Remote Networks, Service Connections, and Mobile Users—GlobalProtect®; for Mobile Users—Explicit Proxy deployments, this functionality is enabled by default and you cannot disable it.

Prisma Access: FQDNs for Remote Network and Service Connection IPsec Tunnels

June 14, 2024

Supported on Strata Cloud Manager for: Prisma Access (Managed by Strata Cloud Manager)

When you onboard a Service Connection or Remote Network connection, a public IP address is assigned for the other side of the IPsec tunnel (the [Service IP Address](#)). You use these public

IP addresses for your CPE in your branch site or headquarters or data center location. Keeping records of all the IP addresses you need to configure on your CPE can be time consuming.

Instead of IP addresses, Prisma® Access provides you FQDNs or *Service Endpoint Addresses* to use for the other end of the IPSec tunnel for Service Connections and Remote Network Connections, thus facilitating the IPSec tunnel setup on your CPE at your branch sites or headquarters or data center locations.

Prisma Access: Native IPv6 Compatibility

June 14, 2024

Supported on Strata Cloud Manager for: Prisma Access (Managed by Strata Cloud Manager)

Organizations are increasingly adopting IPv6 endpoints and require seamless, end-to-end IPv6 access across their entire Secure Access Service Edge (SASE) environment. Previously, IPv6 support in Prisma® Access was limited to private applications. This feature now encompasses comprehensive [end-to-end IPv6 support](#) for Mobile Users, Remote Networks, and Service Connections. One key benefit of native IPv6 support is the ability for Mobile Users utilizing IPv6-only endpoints to establish connections with Prisma Access via IPv6 connections using GlobalProtect®. Additionally, this support enables secure access to public SaaS applications over the internet, even when those destinations necessitate IPv6 connections. This enhancement, leveraging the significantly larger IPv6 address space, ensures compatibility with both IPv6 and dual-stack connections, accelerating your organization's migration to modern, cloud-based, and IPv6-enabled networks.

Prisma Access: Service Connection Support for Explicit Proxy

Supported in: Prisma Access (Managed by Strata Cloud Manager) deployments in Prisma Access 5.1 Preferred and Innovation

Requires GlobalProtect in Proxy Mode to access private and partner apps in a data center and a minimum PAN-OS dataplane of 10.2.10.

Explicit Proxy now supports service connections to enable you to [access resources in your data center](#). With this change, you will still be able to benefit from a proxy connection while accessing external dynamic lists, partner apps, or private apps hosted in your data center.

Strata Cloud Manager: Manage and Share Common Configuration Using Snippet Sharing

June 14, 2024

Supported on Strata Cloud Manager for:

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

→ [Learn about snippets](#)

Manually synchronizing configurations across multiple tenants is error-prone and inefficient. [Snippet sharing](#) eliminates the need for manual synchronization, transforming multitenant configuration management in **Strata Cloud Manager**. This feature simplifies the sharing of common configurations across tenants, significantly reducing the time and effort required for complex setups.

You can now save and organize configuration combinations as reusable snippets. You can easily share these reusable snippets across tenants within your account. This capability provides flexibility, control, and efficiency in managing shared configurations. Use snippet sharing to move configurations from lab to production environments, migrate settings between tenants, manage common configurations across multiple tenants from a single location, and easily handle global configurations across business units.

Strata Cloud Manager: Global Find Using Config Search

June 14, 2024

Supported on Strata Cloud Manager for:

- Prisma Access (Managed by Strata Cloud Manager)
 - [NGFWs \(Managed by Strata Cloud Manager\)](#)
-

Managing complex network security environments requires you to quickly find and modify configuration settings across multiple devices. Manually searching for every instance of a specific network object such as IP address, object name, referenced objects, duplicated objects, is inefficient, time consuming, and prone to error. Global [Configuration Search](#) available in Strata Cloud Manager, solves this challenge by providing a search functionality across your entire managed configuration.

You can search any string, such as a specific policy name, rule UUID, referenced object, or even policies associated with CVEs. The search results are categorized, providing you with direct links to the configuration location within the Strata Cloud Manager enabling easy navigation to all occurrences and references of the searched string. The search results also help you identify other objects that depend on or make reference to the search term or string. For example, when deprecating a security profile enter the profile name in Config Search to locate all instances of the profile and then click each instance to navigate to the configuration page and make the necessary change. After all references are removed, you can then delete the profile. You can do this for any configuration item that has dependencies.

Strata Cloud Manager: Local Configuration Management

June 14, 2024

Supported on Strata Cloud Manager for: NGFW (Managed by Strata Cloud Manager)

Eliminate the need for context switching from central management to individual firewalls for managing local configurations.

This [feature](#) enhances readability, simplifies troubleshooting, and reduces manual effort by providing visibility and control over local firewall configurations through Strata Cloud Manager. Additionally, it identifies any [conflicting](#) or overridden objects between local and pushed configurations, making it easier to troubleshoot.

Strata Logging Service in Strata Cloud Manager

June, 2024

In addition to the Strata Logging Service app available on the hub, you can now also use Strata Cloud Manager to manage your Strata Logging Service instances.

Supported on [Strata Cloud Manager](#) with Strata Logging Service license.



Strata Cloud Manager is not available to you to manage your instances hosted in China or in FedRAMP high regions. Continue to use the Strata Logging Service app to manage the instances in these regions.

You can now manage your instance with . The integration in provides a single, unified interface to manage your log data, enhances operational efficiency and compliance across your entire environment. This centralized management capability allows you to:

- Gain unified visibility and onboard firewalls, Cloud NGFW, Prisma Access, or Panorama appliances
- View the allocated log storage quota, available storage space, and the number of days logs are retained
- Centrally configure log storage quota and retention policies
- Search, filter, and export log data directly from
- Forward log data to external servers for long-term storage, SOC, or internal audit

This integration ensures that you can efficiently monitor your log status and manage data forwarding without switching between applications.

Enterprise DLP: End User Coaching

June 14, 2024

Supported on Strata Cloud Manager for:

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

To minimize data loss incidents and educate your workforce, now enables real-time coaching when user actions violate your organization's data security policy. [End User Coaching](#)

automatically notifies and educates users when their actions involve sensitive data that cannot leave your corporate network.

Your data security administrator can use End User Coaching to immediately notify end users through the Access Experience User Interface (UI) when they upload, download, or post content that is blocked by . Data security administrators can customize these notifications to provide detailed incident information, helping the user understand the violation and modify their content appropriately. After a user generates a DLP incident, they can view the Data Security notification history to review current and past policy violation alerts.

New Features in May 2024

Here are the latest new features introduced on Strata Cloud Manager. Features listed here include some feature highlights for the [products supported with Strata Cloud Manager](#). For the full list of new features supported for a product you're using with Strata Cloud Manager, [see the release notes for that product](#).

Strata Cloud Manager: Policy Config Memory Usage Approaching Max Limits Alert

May 16, 2024

Introducing the [Policy Config Memory Usage Approaching Max Limits](#) alert that triggers when the policy config memory usage exceeds a certain threshold. Exceeding policy config memory usage may lead to commit failure, dataplane malfunction, and consequently, the device entering non-functional state, causing a business interruption.

Supported on [Strata Cloud Manager](#) with AIOps for NGFW Premium license.

Health [alerts](#) actively monitor the health and performance of your platform in real time. This approach helps in identifying issues, predicting potential problems, and implementing remediation actions to ensure your devices function optimally. Here are some key aspects:

- **Monitoring Metrics:** Continuously monitor various metrics from the NGFWs, including CPU utilization, memory usage, disk space, network throughput, and other relevant performance indicators.
- **Anomaly Detection:** Generate alerts that dynamically adjust based on the metric's historical value and your usage trends.
- **Predictive Analysis:** Leverage historical data and patterns to predict when thresholds might be exceeded or specific events may occur. This helps forecast potential issues before they escalate.

Strata Cloud Manager: Config Memory Usage Approaching Max Limits Alert

May 16, 2024

Introducing the [Config Memory Usage Approaching Max Limits](#) alert that triggers when the configuration size on the firewall is close to reaching the maximum limit of config memory usage. During the commit process, a dedicated amount of memory is allocated. During Phase 1 and Phase 2 of the commit process, both the current config and the 'to-be-used' config are stored in memory. Exceeding 50% of VSYS Config Allocator Usage can lead to a commit failure due to insufficient config memory. With this alert, you can take remediation action to prevent a commit failure, which can ultimately lead to an HA Failover.

Supported on [Strata Cloud Manager](#) with AIOps for NGFW Premium license.

Health [alerts](#) actively monitor the health and performance of your platform in real time. This approach helps in identifying issues, predicting potential problems, and implementing remediation actions to ensure your devices function optimally. Here are some key aspects:

- **Monitoring Metrics:** Continuously monitor various metrics from the NGFWs, including CPU utilization, memory usage, disk space, network throughput, and other relevant performance indicators.
- **Anomaly Detection:** Generate alerts that dynamically adjust based on the metric's historical value and your usage trends.
- **Predictive Analysis:** Leverage historical data and patterns to predict when thresholds might be exceeded or specific events may occur. This helps forecast potential issues before they escalate.

Strata Cloud Manager: ACC Query Failure Alert

May 16, 2024

Introducing the [ACC Query Failure](#) alert that detects the failure of the Application Command Center (ACC) query. This failure can impede real-time visibility into network activity, which can compromise the ability to make informed decisions and respond effectively to security incidents.

Supported on [Strata Cloud Manager](#) with AIOps for NGFW Premium license.

Health [alerts](#) actively monitor the health and performance of your platform in real time. This approach helps in identifying issues, predicting potential problems, and implementing remediation actions to ensure your devices function optimally. Here are some key aspects:

- **Monitoring Metrics:** Continuously monitor various metrics from the NGFWs, including CPU utilization, memory usage, disk space, network throughput, and other relevant performance indicators.
- **Anomaly Detection:** Generate alerts that dynamically adjust based on the metric's historical value and your usage trends.
- **Predictive Analysis:** Leverage historical data and patterns to predict when thresholds might be exceeded or specific events may occur. This helps forecast potential issues before they escalate.

Strata Cloud Manager: Approaching Max Capacity - URLs or IPs within EDLs Alert

May 16, 2024

Introducing the [Approaching Max Capacity alert for URLs or IPs within EDLs](#) alert that triggers when the number of URLs, IPs, or Domains in the External Dynamic Lists (EDLs) used in the firewall policy approaches the maximum capacity supported by the firewall. If the capacity limit is reached, the network could become vulnerable to attacks because the firewall won't detect

any additional malicious URLs, IPs, or Domains. To mitigate this risk, remove unnecessary or unused entries from the EDLs to reduce the entries and eliminate vulnerabilities.

Supported on [Strata Cloud Manager](#) with AIOps for NGFW Premium license.

Health [alerts](#) actively monitor the health and performance of your platform in real time. This approach helps in identifying issues, predicting potential problems, and implementing remediation actions to ensure your devices function optimally. Here are some key aspects:

- **Monitoring Metrics:** Continuously monitor various metrics from the NGFWs, including CPU utilization, memory usage, disk space, network throughput, and other relevant performance indicators.
- **Anomaly Detection:** Generate alerts that dynamically adjust based on the metric's historical value and your usage trends.
- **Predictive Analysis:** Leverage historical data and patterns to predict when thresholds might be exceeded or specific events may occur. This helps forecast potential issues before they escalate.

Strata Cloud Manager: PAN-OS Integrated User-ID Agent Monitored Server Disconnected Alert

May 9, 2024

Introducing the [PAN-OS Integrated User-ID Agent Monitored Server Disconnected alert](#), which detects when the server, monitored by the PAN-OS integrated User-ID agent (Agentless User-ID), loses connection with the firewall. This monitored server is a critical component for mapping user identities to network activities. The loss of connectivity between the firewall and the monitored server by the PAN-OS integrated user-ID agent results in the loss of real-time user identification data and compromises security monitoring capabilities. This situation poses potential risks to network integrity and access control measures.

Supported on [Strata Cloud Manager](#) with AIOps for NGFW Premium license.

Health [alerts](#) actively monitor the health and performance of your platform in real time. This approach helps in identifying issues, predicting potential problems, and implementing remediation actions to ensure your devices function optimally. Here are some key aspects:

- **Monitoring Metrics:** Continuously monitor various metrics from the NGFWs, including CPU utilization, memory usage, disk space, network throughput, and other relevant performance indicators.
- **Anomaly Detection:** Generate alerts that dynamically adjust based on the metric's historical value and your usage trends.
- **Predictive Analysis:** Leverage historical data and patterns to predict when thresholds might be exceeded or specific events may occur. This helps forecast potential issues before they escalate.

Strata Cloud Manager: Hijacked and Misconfigured Domain Views in DNS Security Dashboard

May 02, 2024

With Advanced DNS Security license, you can now view the list of [hijacked domains and non-resolvable domains](#) associated with the user specified public-facing parent domain(s) in the [DNS Security dashboard](#). For each entry, there is a reason for this categorization and a traffic hit count based on the source IP. Learn how to [enable Advanced DNS Security](#).

New Features in April 2024

Here are the latest new features introduced on Strata Cloud Manager. Features listed here include some feature highlights for the [products supported with Strata Cloud Manager](#). For the full list of new features supported for a product you're using with Strata Cloud Manager, [see the release notes for that product](#).

Cloud Management for NGFWs: Aggregate Interface Usability Enhancement

April 26, 2024

Supported on Strata Cloud Manager for: [Cloud Management for NGFWs](#).

Configuring an Aggregate Ethernet interface variable in snippets or folders allows you to have reusable common configuration across the entire deployment. [Aggregate Ethernet interface](#) variable reduces duplication of configuration and significantly simplifies the process of updating and maintaining common configurations.

When you add interfaces for your firewalls, you can now configure the **Aggregate Ethernet** interface variable type in addition to the existing Layer 2, Layer 3, and tap interface types.

Cloud Management for NGFWs: Device Onboarding Rules

April 26, 2024

Supported on Strata Cloud Manager for: [Cloud Management for NGFWs](#).

Automate onboarding to with a [device onboarding rule](#), whether you're manually onboarding or onboarding using Zero Touch Provisioning (ZTP). You can associate the with a folder and apply predefined configuration when the first connects to . supports multiple device onboarding rules to define different match criteria that apply to different . Device onboarding rules are designed to simplify and greatly reduce the time spent onboarding new at scale and ensure the correct configuration is applied to newly onboarded .

Define which a rule applies to by using **Match Criteria**. This includes information such as the firewall **Model** and any **Labels** applied to the firewall during the onboarding process. You can define the rule **Action** to specify a **Target Folder** one or more are added to and the **Snippet Association** define any firewall-specific snippet configurations that need to be applied. Additionally, if you use SD-WAN or (CIE) you can also define and apply those necessary configurations in the device onboarding rule to ensure all required connectivity and user-based visibility and policy rule enforcement immediately after onboarding.

Cloud Management for NGFWs: Transparent Web Proxy

April 26, 2024

You can now use Strata Cloud Manager to configure a transparent proxy on your firewalls.

Supported on Strata Cloud Manager for:

- [Cloud Management for NGFWs](#) (with an [AIOps for NGFW Premium license](#) and the legacy router stack enabled. If you'd like this enabled, please reach out to your account team.)



Prisma[®] Access has its own, separate [method of configuring explicit proxy](#). This new feature applies only to cloud-managed firewalls.

To consolidate management, you can now [configure a web proxy on the firewalls you're managing with[®]](#). This means that if you use an NGFW as a proxy device to secure your network, you can configure your proxy settings across your deployment from a single management interface.

This interface includes an in-app Proxy Auto-Configuration (PAC) file editor so that you can edit your proxy settings and modify your PAC file all in one place whenever network changes arise.

The web proxy supports two methods for routing traffic:

- [Explicit Proxy](#)— The request contains the destination IP address of the configured proxy, and the client browser sends requests to the proxy directly. Authentication methods such as Kerberos and SAML 2.0 are supported, requiring the appropriate web proxy licensing.
- [Transparent Proxy](#)—The request contains the destination IP address of the web server and the proxy transparently intercepts the client request (either by being in-line or by traffic steering). This method requires specific networking prerequisites, including a loopback interface, User-ID configuration in the proxy zone, and specific Destination NAT (DNAT) rules defined in . Transparent proxy does not support X-Authenticated Users (XAU) or Web Cache Communications Protocol (WCCP).

You can push web proxy configurations to the following platforms:

- PA-1400
- PA-3400
- VM-Series (with a minimum of four vCPUs)

Strata Cloud Manager: Configuration Indicator

April 26, 2024

Supported on Strata Cloud Manager for:

Prisma Access (Managed by Strata Cloud Manager)

NGFW (Managed by Strata Cloud Manager)

Get clarity on the configuration elements that are applicable for a particular scope and whether they are inherited from a common configuration scope or generated by the system.

The color-coded [configuration indicators](#) help you understand where the configurations are inherited from, and also visually distinguish the object types for easy scanning.

Strata Cloud Manager: External Gateway Integration for Prisma Access and On-Premises NGFWs

April 26, 2024

Supported on Strata Cloud Manager for:

- NGFW (Managed by PAN-OS or Panorama)
 - NGFW (Managed by Strata Cloud Manager)
-

Enable integration between Prisma Access deployments and on-premises NGFWs deployed as external gateways.

In the Prisma Access configuration, when setting up the hybrid Prisma Access deployment with security service edge (SSE) and on-premises NGFWs, you can now configure the NGFWs as [external gateways](#) by referencing the NGFWs' GlobalProtect gateway IP addresses. This eliminates manual configuration and minimizes the risk of misconfiguration.

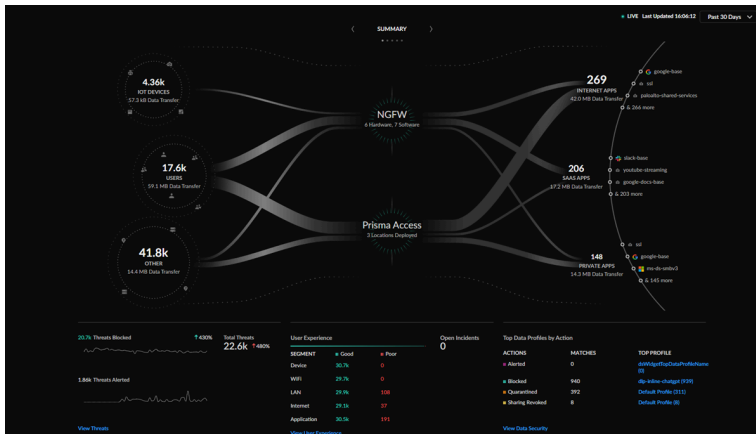
Strata Cloud Manager: Command Center

April 19, 2024

Supported on [Strata Cloud Manager](#) with an AIOps for NGFW Premium, Prisma Access, or AIOps for NGFW Free with a Strata Logging Service license.

Network security administrators often struggle with fragmented visibility across their security infrastructure, making it difficult to quickly assess overall network health, identify emerging threats, and understand the impact of security events on user experience. Traditional approaches require navigating between multiple dashboards and tools to piece together a comprehensive view of security posture.

The [Strata Cloud Manager Command Center](#) serves as your new NetSec homepage and provides your first stop to assess the health, security, and efficiency of your network. In a single view, the command center shows you all users and IoT devices accessing the internet, SaaS applications, and private apps, and demonstrates how Prisma® Access, your NGFWs, and your security services protect them.



Strata Cloud Manager: Activity Insights

April 19, 2024

Supported on [Strata Cloud Manager](#) with an AIOps for NGFW Premium, Prisma Access, or AIOps for NGFW Free with a Strata Logging Service license.

Managing network visibility and operational efficiency across diverse deployments like Prisma Access and NGFW often requires juggling multiple dashboards, leading to fragmented analysis. [Activity Insights](#) solves this critical challenge by giving you an in-depth, consolidated view of your network activities across Prisma Access and NGFW deployments. Activity Insights brings together the visualization, monitoring, and reporting capabilities from [dashboards](#) like Application Usage, Network Usage, User Activity, and Threat Insights, providing all this data in a single, unified view.

Activity Insights pairs with the new [Strata Cloud Manager Command Center](#) homepage ; for anomalies, security gaps, degraded user experiences, impacts on security and health of your network that the homepage surfaces, you can drill down into Activity Insights and other [dashboards](#) to investigate and assess next steps.

Activity Insights provides a unified view of network data in relation to applications, users, threats, URLs, and network usage. You can also view the performance of Prisma SD-WAN applications with details on health score over a time range, transaction statistics, and bandwidth utilization metrics. The advanced reporting functionality enables you to download, share, and schedule reports that cover the data in the Overview tab. The report presents data separately for each filter applied in Activity Insights.

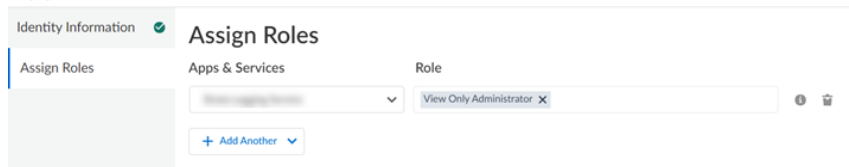
Furthermore, Activity Insights now displays direct users who connect to your network infrastructure while disconnected from **GlobalProtect®**. Previously, ADEM collected event information for these users, but Activity Insights did not show them. Now, you can gain complete visibility into network activity regardless of connection status, significantly improving analysis and reporting capabilities.

Strata Cloud Manager: View Only Administrator Role Enhancement

April 10, 2024

Supported on Strata Cloud Manager

In [Identity and Access Management](#), the **View Only Administrator** role is extended to include support for the application.



Strata Cloud Manager: Trusted IP List

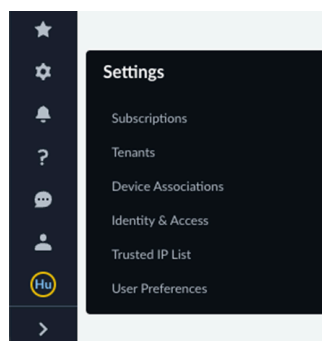
April 4, 2024

Supported on [Strata Cloud Manager](#).

The [Trusted IP List](#) is a new system setting feature introduced to The Trusted IP List system setting allows you to enhance the administrative security posture of your Strata Cloud Manager tenants. This feature allows administrators to explicitly define a list of trusted source IP addresses that are permitted to access the Strata Cloud Manager web interface and API. This provides a layer of control, moving from the default "allow all" access model to a strictly "allow-listed" environment.

This functionality is designed to seamlessly integrate with multitenant deployments. When the Trusted IP List is configured on a parent tenant, the restrictions are automatically inherited and enforced top-down across all associated child tenants, ensuring consistent security policy across the hierarchy. The enforcement specifically targets the Strata Cloud Manager access points.

The Trusted IP List can be managed directly under **Strata Cloud Manager > Settings > Trusted IP List** and supports the bulk import of multiple IP addresses via a CSV file. Furthermore, a dedicated override mechanism is available through the primary Strata Cloud Manager hub, allowing users with necessary permissions to unlock access to a tenant if their IP is inadvertently blocked.



New Features in March 2024

Here are the latest new features introduced on Strata Cloud Manager. Features listed here include some feature highlights for the [products supported with Strata Cloud Manager](#). For the full list of new features supported for a product you're using with Strata Cloud Manager, [see the release notes for that product](#).

Changes to Monitor > Applications and Monitor > Users

If you're using Strata Cloud Manager with NGFWs, in addition to Prisma Access:

The Strata Cloud Manager pages where you can monitor your applications and users, now include NGFW data.

- **Monitor > Applications**

The Prisma Access tab is now showing you NGFW data together with your Prisma Access data. This gives you a single, unified view of [applications](#) across your NGFWs and Prisma Access. If you need to view Autonomous DEM data, set the scope of the data on this tab to Prisma Access (since that data is specific to Prisma Access).

- **Monitor > Users**

The [Users](#) page is now showing you NGFW data together with your Prisma Access data, giving you a single, unified view of all your users. If you need to view Autonomous DEM data, set the scope of the data on this tab to Prisma Access (since that data is specific to Prisma Access).

These changes are a step towards some new features we will be providing you very soon! As part of the upcoming changes, you can anticipate that this page will be consolidated into a brand new, interactive view that brings together all activity insights from across your NGFWs and Prisma Access deployments. Check back here in the release notes for the latest updates.

AIOps for NGFW: NGFW/Panorama Management Certificate Expiration Alert

March 1, 2024

Introducing the [NGFW/Panorama Management Certificate Expiration](#) alert that detects the upcoming expiration of the NGFW or Panorama Management certificate on devices by April 7, 2024. When these certificates expire, it results in a loss of connection between Panorama and NGFWs, M-Series appliances operating in PAN-DB private cloud mode, WildFire appliances (WF500/B), and Peer Panoramas, regardless of their management or Log Collector modes. Consequently, expired certificates compromise centralized management and visibility, posing security risks and operational inefficiencies. This alert helps you identify the PAN-OS devices within your network that are susceptible to this issue and provides information about the remediation options.

Supported on [AIOps for NGFW Free](#) and [Strata Cloud Manager](#) with AIOps for NGFW Premium license.

Health [alerts](#) actively monitor the health and performance of your platform in real time. This approach helps in identifying issues, predicting potential problems, and implementing remediation actions to ensure your devices function optimally. Here are some key aspects:

- **Monitoring Metrics:** Continuously monitor various metrics from the NGFWs, including CPU utilization, memory usage, disk space, network throughput, and other relevant performance indicators.
- **Anomaly Detection:** Generate alerts that dynamically adjust based on the metric's historical value and your usage trends.
- **Predictive Analysis:** Leverage historical data and patterns to predict when thresholds might be exceeded or specific events may occur. This helps forecast potential issues before they escalate.

AI Ops for NGFW: Probable Cause Analysis with CDL

March 1, 2024

The [probable cause analysis](#) is enhanced to use the Cortex Data Lake (CDL) logs and provide additional metadata to identify the probable cause that led to the creation of an alert or incident. This analysis enables pinpointing the policies, applications, source zones, URLs, source IPs, and regions potentially causing the alert, thereby facilitating appropriate remediation actions. For instance, when session exhaustion triggers an **Adverse Resource Usage** alert, you can utilize the probable cause analysis to identify the primary contributors to the alert and follow the suggested remediation recommendations.

Supported on [Strata Cloud Manager](#) with AI Ops for NGFW Premium license.

To troubleshoot the issues that cause alerts, AI Ops for NGFW leverages advanced AI capabilities to provide [probable causes for alerts](#). By reviewing these probable causes, you can identify the source of the issue and follow the provided recommendations for resolving it. This feature ensures optimal network performance by mitigating disruptions and maximizing the effectiveness of your cybersecurity solution.

New Features in February 2024

Here are the latest new features introduced on Strata Cloud Manager. Features listed here include some feature highlights for the [products supported with Strata Cloud Manager](#). For the full list of new features supported for a product you're using with Strata Cloud Manager, [see the release notes for that product](#).

AIOps for NGFW: Delayed Telemetry Alert

February 23, 2024

Introducing the [Delayed Telemetry](#) alert, which actively identifies instances when Strata Cloud Manager detects a problem with receiving or processing telemetry from a device. If telemetry is missing for 6 hours, Strata Cloud Manager issues a medium severity alert. If this absence persists for more than 72 hours, Strata Cloud Manager elevates the alert severity to critical.

Upon the resumption of telemetry data processing, Strata Cloud Manager automatically closes the delayed telemetry alerts. If you remove a device, Strata Cloud Manager deletes all associated data, including delayed alerts. Additionally, Strata Cloud Manager displays an orange or red hourglass icon next to hostnames, providing quick visual cues to identify devices with potential telemetry issues.

Supported on [AIOps for NGFW Free](#) and [Strata Cloud Manager](#) with AIOps for NGFW Premium license.

Health [alerts](#) actively monitor the health and performance of your platform in real time. This approach helps in identifying issues, predicting potential problems, and implementing remediation actions to ensure your devices function optimally. Here are some key aspects:

- **Monitoring Metrics:** Continuously monitor various metrics from the NGFWs, including CPU utilization, memory usage, disk space, network throughput, and other relevant performance indicators.
- **Anomaly Detection:** Generate alerts that dynamically adjust based on the metric's historical value and your usage trends.
- **Predictive Analysis:** Leverage historical data and patterns to predict when thresholds might be exceeded or specific events may occur. This helps forecast potential issues before they escalate.

Prisma Access: Remote Network Locations with Overlapping Subnets

February 16, 2024

Supported on Strata Cloud Manager for: Prisma Access (Cloud Management)

As a general rule, you cannot have any overlapping subnets within a Prisma Access deployment. That is, the subnets for all remote network locations, your service connections, and your Prisma Access for mobile users IP address pool cannot overlap. However, in some circumstances you cannot avoid having overlapping subnets. Prisma Access allows you to onboard remote network locations with overlapping subnets, as long as you select **Overlapped Subnets** check box in the remote network settings when you [plan for remote networks](#). However, you can use overlapping subnets only in few use cases.

Prisma Access: License Enforcement for Mobile Users (Enhancements)

February 16, 2024

Supported on Strata Cloud Manager for: Prisma Access (Cloud Management)

Prisma Access [enforces policies for mobile user licenses](#) over 30 days instead of 90 days. Though there is no strict policing of the mobile user count, the service tracks the number of unique users over the last 30 days to ensure that you have purchased the proper license tier for your user base, and stricter policing of user count may be enforced if continued overages occur. This change is applicable for all types of mobile user licenses.

Prisma Access: Policy Analyzer for Panorama Managed Deployments

February 16, 2024

Supported on Strata Cloud Manager for:

- **NEW THIS MONTH** [Prisma Access \(Managed by Panorama\)](#) with an [AIOps for NGFW Premium](#) license
 - NGFW (Panorama Managed) with an [AIOps for NGFW Premium](#) license
 - VM-Series, funded with Software NGFW Credits (Panorama Managed)
-

Time-sensitive security policy changes carry the high risk of introducing errors, misconfigurations, or conflicts into the rulebase, requiring slow and complex manual audit processes. Policy integrity is difficult to maintain at scale, leading to decreased performance and potential security gaps. Strata Cloud Manager introduces Policy Analyzer, enabling administrators to optimize time and resources when implementing any change request. [Policy Analyzer](#) provides immediate, automated analysis of the security rulebase to ensure policy updates meet defined intent and technical requirements. It proactively checks for anomalies, such as Shadows, Redundancies, Generalizations, Correlations, and Consolidations, that otherwise require labor-intensive manual checking. By identifying conflicting or duplicate rules before deployment, Policy Analyzer streamlines change management, reduces the risk of misconfiguration, and ensures the continued performance and integrity of your network security posture.

Cloud Management for NGFWs: UI Update for Security Checks

February 16, 2024

Supported on Strata Cloud Manager for:

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

Security administrators rely on predefined [best practice checks](#) that align with industry standards, such as CIS (Center for Internet Security) and NIST (National Institute of Standards and Technology). However, the rigidity of applying these checks globally often forces you to manually bypass or ignore critical security findings for specific operational exceptions, risking compliance and increasing administrative overhead.

Strata Cloud Manager now addresses this by supporting real-time inline check exemptions. Exemptions allow you to restrict where security checks are applied within your deployment, rather than requiring you to disable the checks entirely. This capability ensures you maintain a robust global security posture while flexibly accommodating specific organizational needs. Additionally, essential check information is now delivered in a consolidated, contextual view, simplifying your configuration evaluation workflow and allowing you to balance security enforcement with operational efficiency.

Cloud Management for NGFWs: Clone a Snippet

February 16, 2024

Supported on Strata Cloud Manager for:

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

When you need to create similar configuration snippets with slight variations, manually rebuilding each snippet from scratch wastes valuable time and increases the risk of configuration errors. This challenge becomes particularly frustrating when you want to use an existing snippet as a foundation for new deployments or when adapting proven configurations for different network segments.

You can now [clone existing snippets in Strata Cloud Manager](#), allowing you to use any preexisting snippet as a template for new configurations. This cloning capability eliminates the need to configure completely new objects when you want to create variations of existing snippets.

Snippets are configuration objects, or groups of configuration objects, that you can associate with your folders, firewalls, and Prisma® Access deployments onboarded to Strata Cloud Manager. You use them to standardize configurations, enabling you to push changes quickly to multiple areas simultaneously. Snippets help you manage common configurations centrally for consistent security enforcement across NGFW and Prisma Access deployments.

Snippets are classified in two ways: Predefined and Custom. Predefined snippets are available to all Strata Cloud Manager users and help you quickly get your new firewalls and deployments up and running with best practice configurations. Custom snippets are any snippets that administrators create.

When you clone a snippet, the system creates an independent copy that is not associated with any devices, folders, or deployments. This allows you to customize the cloned snippet freely without having to disassociate it from existing resources before you begin making modifications.

Cloud Management for NGFWs: TACACS+ Accounting

February 16, 2024

Supported on Strata Cloud Manager for:

- NGFW (Managed by PAN-OS or Panorama)
 - NGFW (Managed by Strata Cloud Manager)
-

If you use a Terminal Access Controller Access-Control System Plus ([TACACS+](#)) server for user authorization and authentication, you can now [log accounting information](#) to fully make use of the authentication, authorization, and accounting (AAA) framework that is the basis for TACACS+.

The TACACS+ Accounting feature allows you to use a TACACS+ server profile to record user behavior, such as when a user started using a specific service, the duration of use for the service, and when they stopped using the service. The TACACS+ Accounting feature helps to create logs and records of the initiation and termination of services, as well as any services in progress during the user's session, that you can then use later if needed for auditing purposes.

When you configure and enable an Accounting server profile, the TACACS+ server provides information to the firewall about the initiation, duration, and termination of services by users. The firewall also generates a log when the TACACS+ server successfully provides the accounting records to the server that you configure in the profile. If the firewall is unable to successfully send the accounting records to any of the servers in the profile, the firewall generates a critical severity alert to the system logs.

By using your existing TACACS+ server, you can now configure it to provide even more information about the use of services by users on your network, giving you even more robust visibility into user activity on your network.

Traceability and Control of Post-Quantum Cryptography in Decryption

February 16, 2024

Supported on Strata Cloud Manager for:

- [Prisma Access \(Managed by Strata Cloud Manager\)](#) with a [Prisma Access license](#)
 - [NGFW \(Managed by Strata Cloud Manager\)](#) with an [AIOps for NGFW Premium license](#)
-

PAN-OS 11.1 is required. This feature was first introduced in [PAN-OS 11.1](#) for NGFW (Managed by PAN-OS or Panorama).

Today, [post-quantum cryptography \(PQC\)](#) algorithms and hybrid PQC algorithms (classical and PQC algorithms combined) are accessible through open-source libraries and integrated into web browsers and other technologies. Traffic encrypted by PQC or hybrid PQC algorithms cannot be decrypted yet, making these algorithms vulnerable to misuse. To address these concerns, Palo Alto Networks firewalls now [detect, block, and log the use of PQC and hybrid PQC algorithms](#) in TLSv1.3 sessions. Successful detection, blocking, and logging of PQC and hybrid PQC algorithms depends on your SSL Decryption policy rules.

If SSL traffic matches an SSL Forward Proxy or SSL Inbound Inspection Decryption policy rule, the firewall prevents negotiation with PQC, hybrid PQC, and other unsupported algorithms. Specifically, the firewall removes these algorithms from the ClientHello, forcing the client to negotiate with classical algorithms. (For a list of supported cipher suites, see [PAN-OS 11.1 Decryption Cipher Suites](#).) This enables continuous decryption and threat identification through deep packet inspection. If the client strictly negotiates PQC or hybrid PQC algorithms, the firewall drops the session. In the Decryption log for the dropped session, the error message states that the "client only supports post-quantum algorithms." To see details of successful or unsuccessful TLS handshakes in the Decryption logs, enable both options in your Decryption policy rules.

If SSL traffic matches a "no-decrypt" Decryption policy rule or doesn't match any Decryption policy rules, the firewall allows negotiation with PQC or hybrid PQC algorithms. However, details of sessions that negotiate these algorithms are available in Decryption logs only when session traffic matches a "no-decrypt" Decryption policy rule.

Additionally, new threat signatures offer additional visibility into the use of PQC and hybrid PQC algorithms in your network. These signatures monitor ServerHello responses and trigger alerts for SSL sessions that successfully negotiate with the most commonly known PQC and hybrid PQC algorithms. A Threat Prevention license is required to receive alerts.

Cloud Management of NGFWs: GlobalProtect Portal and Gateway

February 16, 2024

Supported on Strata Cloud Manager for:

- NGFW (Managed by PAN-OS or Panorama)
 - NGFW (Managed by Strata Cloud Manager)
 - GlobalProtect app
-

Whether checking email from home or updating corporate documents from an airport, the majority of today's employees work outside the physical corporate boundaries. This workforce mobility increases productivity and flexibility while simultaneously introducing significant security risks. Every time users leave the building with their laptops or smart phones, they are bypassing the corporate firewall and associated policies that are designed to protect both the user and the network. [GlobalProtect®](#) solves the security challenges introduced by roaming users by extending the network security policy that you're enforcing within the physical perimeter to all users, no matter where they are located.

You can now use [GlobalProtect with cloud-managed NGFWs](#) to secure your mobile workforce. Enable your cloud-managed NGFWs as GlobalProtect gateways and portals, in order to provide flexible, secure remote access to users everywhere.

Strata Cloud Manager: Private Key Export in Certificate Management

February 16, 2024

Supported on Strata Cloud Manager for:

- Prisma Access (Managed by Strata Cloud Manager) and Prisma Access (Managed by Panorama)
 - NGFW (Managed by PAN-OS or Panorama)
-

You can centrally manage the certificates you use to secure communication across your network.

You can now [export the private key](#) from for a self-signed certificate. However, the export of private keys for an externally signed certificate is restricted. The supported export formats are as follows:

- **Base64 Encoded Certificate (PEM)**—This is the default format. It's the most common and has the broadest support on the internet. **Export Private Key** if you want the exported file to include the private key.
- **Encrypted Private Key and Certificate (PKCS12)**—This format is more secure than PEM but isn't as common or as broadly supported. The exported file will automatically include the private key.
- **Binary Encoded Certificate (DER)**—More operating system types support this format than the others. You can't export the private key in this format.

Strata Cloud Manager: New Prisma Access Cloud Management Location

February 16, 2024

Supported on Strata Cloud Manager for:

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

Prisma Access Cloud Management can now be deployed in the India [region](#).

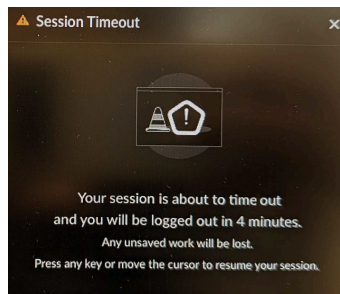
User Session Inactivity Timeout

February 15, 2024

Supported on Strata Cloud Manager

The [Strata Cloud Manager](#) now automatically ends your session after 30 minutes of inactivity. This security feature ensures the system logs out unattended sessions. You become inactive when you don't press a key or move your mouse within the Strata Cloud Manager interface. This inactivity timeout rule applies to all tenants you manage within the platform.

To help you prevent unexpected logouts and the loss of your work, we give you a pre-timeout warning. Five minutes before your 30-minute limit, a notification appears on your screen and starts a countdown. This countdown shows you the remaining time until your session expires; it stops only when approximately five seconds remain.



You must press a key or move your cursor to keep your session active and reset the timer. If you ignore the notification and remain inactive, the system immediately logs you out when the timer hits zero. If you log out, you lose any unsaved work and must sign in again to resume your tasks. We strongly recommend you save your work frequently to avoid data loss.



You were logged out due to inactivity.
You were idle for more than 30 minutes so we logged you out for your safety.
Please sign in again.
[Sign In](#)

AI Ops for NGFW: Logging Drive Failure Alert

February 6, 2024

Introducing the [Logging Drive Failure](#) alert that detects a failure in the logging drive by monitoring the firewall's disk status. This failure in the drive could potentially result in data loss, impair logging and monitoring capabilities, and activate a failover in the case of a high availability (HA) pair.

Supported on [AIOps for NGFW Free](#) and [Strata Cloud Manager](#) with AIOps for NGFW Premium license.

Health [alerts](#) actively monitor the health and performance of your platform in real time. This approach helps in identifying issues, predicting potential problems, and implementing remediation actions to ensure your devices function optimally. Here are some key aspects:

- **Monitoring Metrics:** Continuously monitor various metrics from the NGFWs, including CPU utilization, memory usage, disk space, network throughput, and other relevant performance indicators.
- **Anomaly Detection:** Generate alerts that dynamically adjust based on the metric's historical value and your usage trends.
- **Predictive Analysis:** Leverage historical data and patterns to predict when thresholds might be exceeded or specific events may occur. This helps forecast potential issues before they escalate.

New Features in January 2024

Here are the latest new features introduced on Strata Cloud Manager. Features listed here include some feature highlights for the [products supported with Strata Cloud Manager](#). For the full list of new features supported for a product you're using with Strata Cloud Manager, [see the release notes for that product](#).

Prisma Access: Explicit Proxy Forwarding Profiles with Multiple PAC File Support

January 22, 2024

Supported on Strata Cloud Manager for: Prisma Access

Managing explicit proxy traffic using single or multiple Proxy Auto-Configuration (PAC) files introduces complexity and management burden. You can now manage traffic flow and bypass rules by using [Forwarding Profiles instead of only a single PAC file](#). Forwarding Profiles enable you to define forwarding rules and objects from a dedicated interface rather than dealing with the inherent technical complexity of a PAC file.

If you currently use a PAC file, you can migrate to Forwarding Profiles by importing the PAC file into a profile. Additionally, if you manage multiple PAC files for different traffic types, you can import these PAC files into separate profiles to use them simultaneously. In addition to standard proxy deployments, you can also use Forwarding Profiles to define the flow of traffic through GlobalProtect® in Proxy or Tunnel and Proxy mode.

Query Usability and Performance Enhancements in Log Viewer

January, 2024

The enhancements in Log Viewer include:

- Option to cancel a query you no longer want to run, using the Cancel option
 - Improved query response time
 - View logs from Strata Logging Service hosted in China region
-

To maximize the efficiency of your log analysis and ensure comprehensive visibility across all regions, [Explore/ Log Viewer](#) now provide advanced query management and performance capabilities. Slow or complex queries no longer consume unnecessary time or system resources. You can now abort long-running queries, giving you direct control over execution time and minimizing resource consumption. Furthermore, the query response time is improved, enabling rapid exploration of vast log data sets. This feature also provides critical access to view logs from hosted in the China region, ensuring full regulatory and operational coverage for your global deployments. These capabilities together accelerate your ability to analyze data and respond to threats efficiently.

New Features in November 2023

Here are the latest new features introduced on Strata Cloud Manager. Features listed here include some feature highlights for the [products supported with Strata Cloud Manager](#). For the full list of new features supported for a product you're using with Strata Cloud Manager, [see the release notes for that product](#).

Cloud Management for NGFWs: Capacity Analyzer Alerts

November 20, 2023

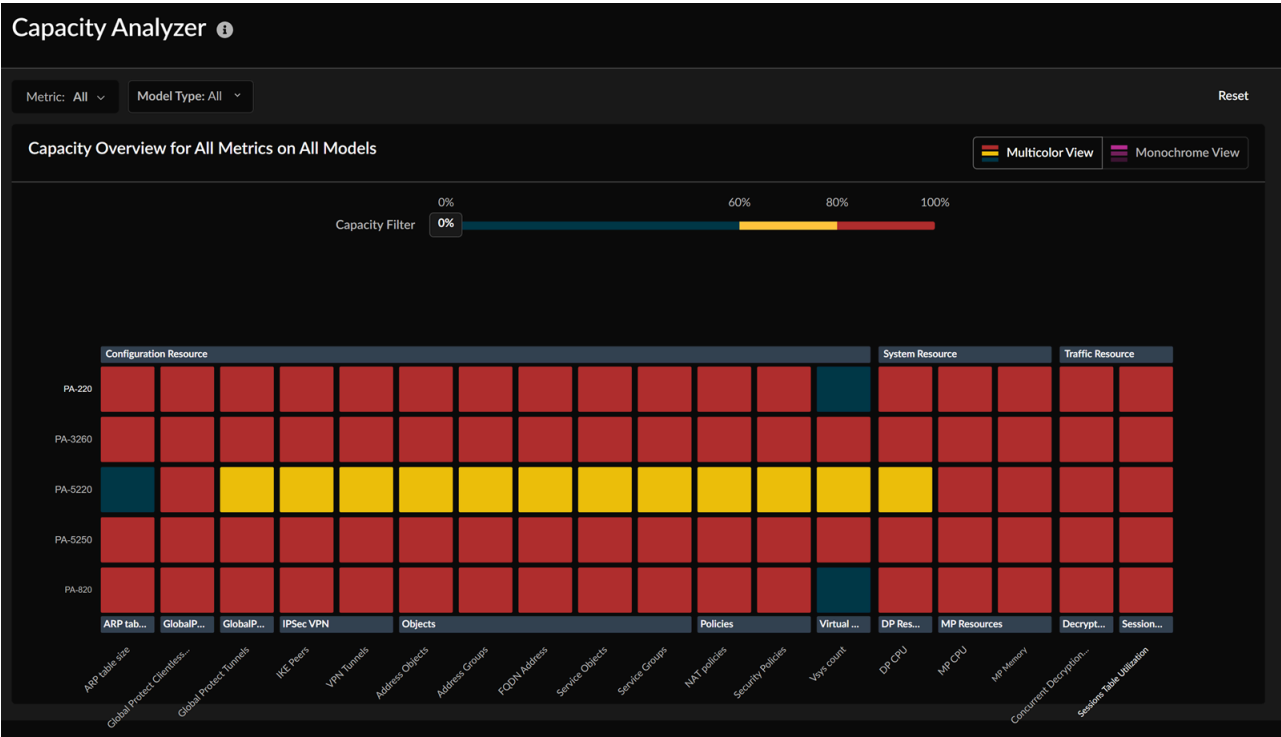
Capacity Analyzer has been enhanced to include support for alerts, assisting you in the following:

- Anticipate resource consumption nearing its maximum capacity and raise alerts.
- By using the [Capacity Analyzer Alert details page](#), you can analyze resource usage patterns at the firewall level and access a heatmap that provides a comprehensive overview of resource utilization across all their firewalls.
- Within the [Capacity Analyzer resource usage details page](#), you can explore associated alerts, pinpoint other firewalls encountering the same issue, and initiate actions to plan and remediate the problem.

Now supported for [Cloud Management for NGFWs](#) (with an [AIOps for NGFW Premium license](#))

When Next-Generation Firewalls (NGFW) approach their capacity thresholds, system performance diminishes and operational disruptions often occur. Capacity-related issues are difficult to manage and typically only become visible after the limits are breached, resulting in time-consuming, reactive remediation efforts.

The [Capacity Analyzer](#) solves this problem by monitoring device resource consumption to prevent potential bottlenecks. It provides security teams with deep, centralized visibility into resource usage patterns based on firewall model types. This capability enables proactive planning for upgrading to higher capacity firewalls based on specific needs. This proactive approach ensures that you receive early notification about potential capacity constraints, allowing you to take preemptive action to safeguard your business operations and maintain optimal performance.

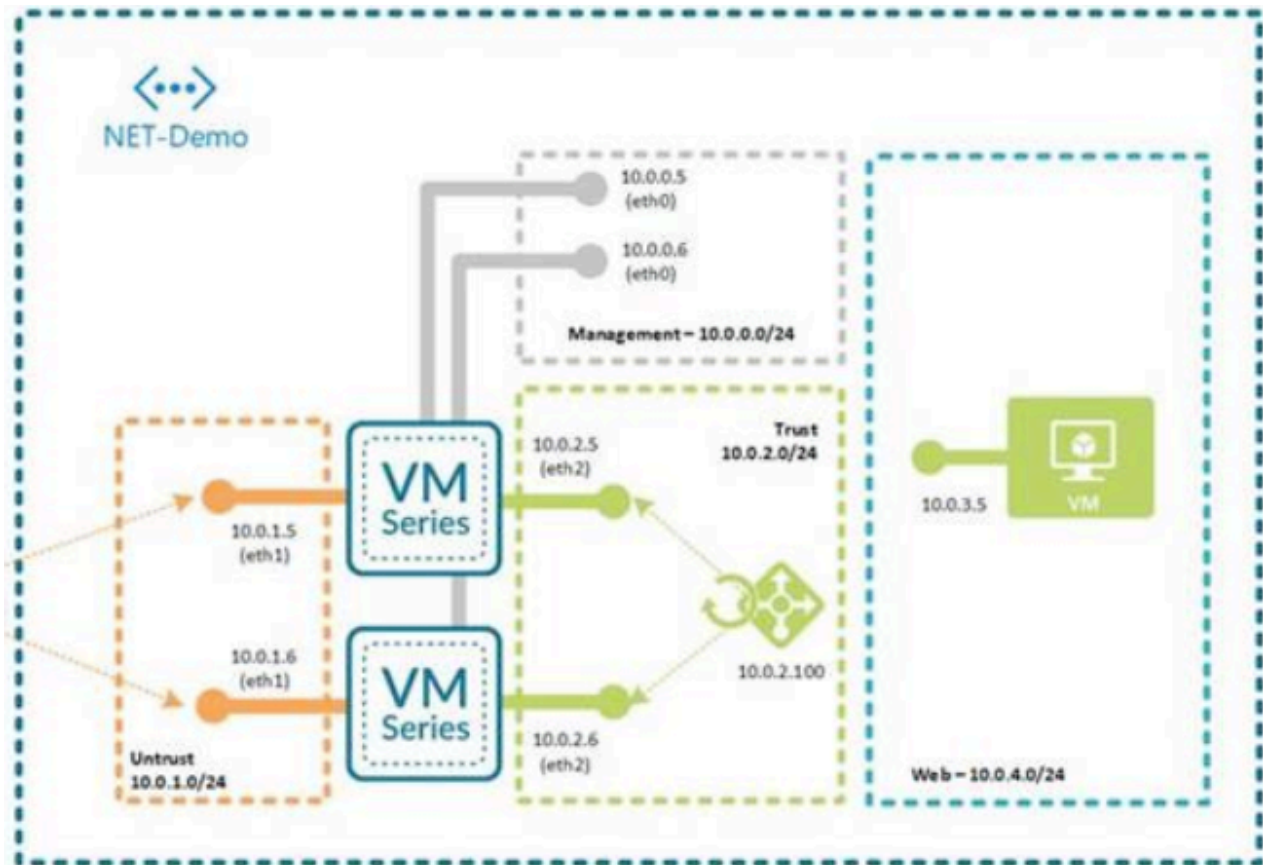


Prisma SD-WAN: Public Cloud High Availability (HA)

Maintaining network resiliency and session survivability for SD-WAN in public cloud deployments presents unique challenges, often leading to service disruptions during a device failure. To address this, Palo Alto Networks now supports [high availability \(HA\) for SD-WAN](#) on VM-Series next-generation firewalls in public cloud environments.

This feature enables an active/passive HA configuration that uses a floating IP address to ensure seamless failover between firewalls. By maintaining session state during a failover event, it minimizes downtime and preserves application performance for your users. This allows you to build resilient and reliable SD-WAN architectures in the cloud, mirroring the high availability standards traditionally found in on-premises deployments.

This HA capability is available for VM-Series firewalls in [AWS](#) and [Microsoft Azure](#).



Prisma Access: Cloud Delivered Enterprise Network Integration

Organizations using colocation (CoLo) facilities for multicloud and on-premises connectivity often face challenges like managing complex, expensive network infrastructure, dealing with inconsistent security stacks, and overcoming bandwidth limitations. Palo Alto Networks Prisma[®] Access and Google Cloud Platform's [Network Connectivity Center \(NCC\)](#) Gateway (GCP NCC gateway) bring high bandwidth, secure, and reliable connectivity to public and private apps for mobile users and users at the remote offices or branch sites.

- Managing the network infrastructure can be complex and expensive if users need to access private apps hosted by different cloud service providers (CSPs) using a CoLo facility.
- Using multiple security products to secure apps can result in having an inconsistent security stack across your network and your organization's users.
- Difficulty in achieving high-bandwidth connections to large branches or campus locations from a CoLo facility to a remote network.

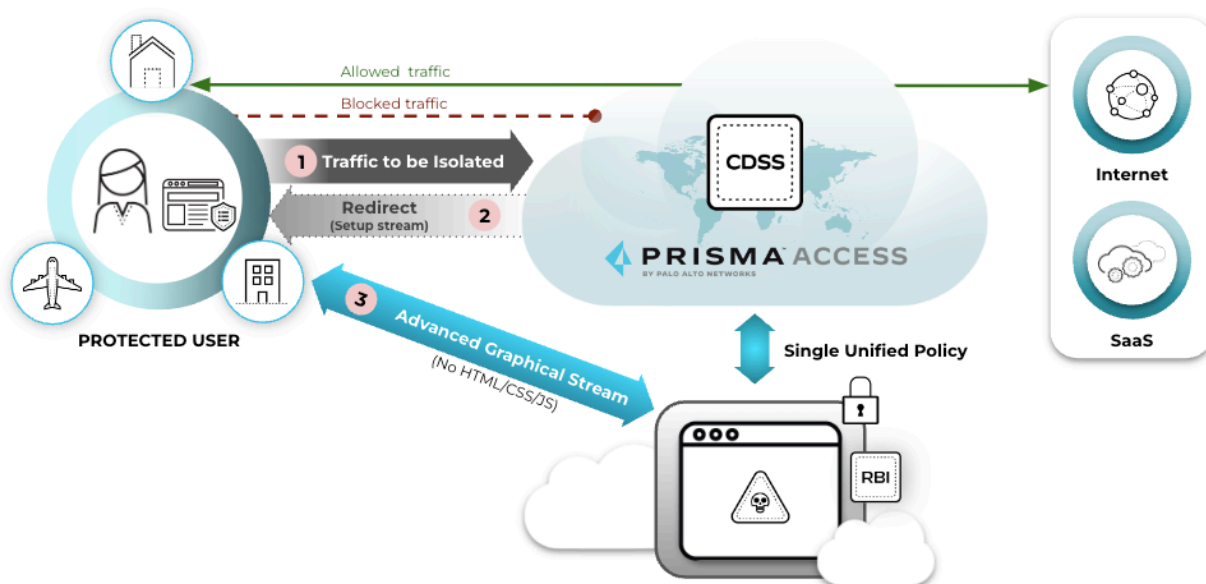
Prisma Access integrates with GCP NCC to provide security inspection for internet-bound traffic and to the private apps that are hosted in GCP, on-premises, or in a third-party cloud connected through GCP NCC. You can onboard remote sites connected through GCP NCC as either a remote network or as a service connection. This way, mobile users (on-ramp) and remote networks (off-ramp) can access public or private apps securely through Prisma Access.

Prisma Access: Remote Browser Isolation

Browser and web-based attacks are continuously evolving, resulting in security challenges for many enterprises. Web browsers, being a major entry point for malware to penetrate networks, pose a significant security risk to enterprises, prompting the increasing need to protect networks and devices from zero day attacks. Highly regulated industries, such as government and financial institutions, also require browser traffic isolation as a mandatory compliance requirement.

While most enterprises want to block 100% of attacks by using network security and endpoint security methods, such a goal might not be realistic. Most attacks start with the compromise of an endpoint that connects to malicious or compromised sites or by opening malicious content from those sites. An attacker only needs one miss to take over an endpoint and compromise the network. When this happens, the consequences of that compromise and the impact to your organization can be damaging.

Remote Browser Isolation (RBI) creates a safe isolation environment for your users' local browsers, preventing website code and files from executing on their local browser. Unlike other isolation solutions, RBI uses next-generation isolation technologies to deliver near-native experiences for users accessing websites without compromising on security.



RBI is a service that transfers all browsing activity away from your users' managed devices and corporate networks to an outside entity, such as Prisma® Access, which securely isolates potentially malicious code and content within its platform. Natively integrated with Prisma Access, RBI allows you to apply isolation profiles easily to existing security policies. Isolation profiles can restrict many user controls such as copy and paste actions, keyboard inputs, and sharing options like file uploading, downloading, and printing files to keep sensitive data and information secure.

All traffic in isolation undergoes analysis and threat prevention provided by Cloud-Delivered Security Services (CDSS), ensuring robust security before content reaches the user.

Prisma Access: Service Connection Identity Redistribution Management

Sometimes, granular controls are needed for user-ID redistribution in particularly large scale Prisma Access deployments. Service Connection Identity Redistribution Management lets you select specific service connections for [identity redistribution](#).

By default, all of your service connections, in order of proximity, are used for identity redistribution. However, you may not know which specific service connections are being used for identity redistribution at a given moment. And, depending on the number of service connections you have and the number of User-ID agents you've configured, this method for identity redistribution can test the limits of your system resources. To solve this, we now give you the option to decide which service connections you want to use for identity redistribution.

Cloud Management for NGFWs: IPSec VPN Monitoring

Because an IPSec VPN tunnel is a logical interface, it cannot reflect the status of the underlying physical link. This limitation can cause a firewall to continue routing traffic to an unusable path, leading to silent traffic loss until the failure is manually detected.

To address this, PAN-OS® now includes [IPSec tunnel monitoring](#) to actively verify connectivity to a target IP address through the tunnel. If the target becomes unreachable, the firewall marks the path as unusable and automatically initiates a failover. During failover, the existing tunnel is torn down, routing changes are triggered, and a new tunnel is established to redirect traffic. The feature provides status visibility for both the IKE gateway and individual IPSec tunnels, which allows the firewall to maintain high availability and reduce traffic loss.

Cloud Management for NGFWs: PA-450R Next-Generation Firewall Support

Securing industrial and remote environments requires a durable firewall capable of withstanding harsh conditions. The [PA-450R](#) is a rugged firewall appliance purpose-built to address this challenge. As an upgrade to the PA-220R, the PA-450R is designed for industrial, commercial, and government deployments. This hardware is also suited for installation in harsh environments with extreme temperatures and high humidity levels.

The PA-450R supports PAN-OS® 11.1 and later versions. It features two SFP/RJ-45 combo ports and six RJ-45 ports. Two of these ports are fail-open, providing a pass-through connection in the event of a power failure.

This appliance uses DC power and supports optional power redundancy. Its fanless design and rugged build allow for secure installation on a flat surface, wall, or equipment rack. This hardware meets ICS/SCADA system architecture compliance standards.

Cloud Management for NGFWs: PA-5445 Next-Generation Firewall

Securing enterprise data centers and regional headquarters demands a next-generation firewall with exceptional performance. The [PA-5445](#) addresses this need as the highest-performance fixed form-factor model in the Palo Alto Networks® firewall lineup. It features hardware resources dedicated to networking, security, signature matching, and management.

The PA-5445 supports PAN-OS® 11.1 and later versions. It achieves the highest App-ID speed (93Gbps), L7 threat inspection rate (70Gbps), and session count (48M) in a fixed form-factor firewall. For connectivity, it includes eight RJ-45 ports, twelve SFP+ ports, four SFP28 ports, and four QSFP28 ports that support breakout mode. It also features dedicated HSCI and HA1 ports for high availability control.

The PA-5445 uses AC or DC power supplies and supports optional power redundancy. This hardware occupies 2RU of rack space and is designed to mount in a 19-inch equipment rack.

Cloud Management for NGFWs: Inline Best Practice Checks for Device Setup

Strata Cloud Manager lets you validate your configuration against predefined [Best Practices](#) and custom checks you create based on the needs of your organization. As you make changes to your service routes, connection settings, allowed services, and administrative access settings for the management and auxiliary interfaces for your firewalls, Strata Cloud Manager gives you assessment results inline so you can take immediate corrective action when necessary. This eliminates problems that misalignments with best practices can introduce, such as conflicts and security gaps.

Inline checks let you:

- Gauge the effectiveness of, assess the impact of, and validate changes you make to your configuration using inline assessment results.
- Prioritize and perform remediations based on the recommendations from the inline assessment.

Cloud Management for NGFWs: VM-Series Device Management

Previously, you had to manually include information such as DNS entries and IP addresses in the `init.cfg` file when creating a firewall image for your cloud environments. This release adds support for a bootstrapping process that allows you to configure newly deployed firewalls without manually configuring them prior to deployment. This new process associates the firewall with a Panorama managed host to automate the onboarding and configuration of your software firewall.

With this functionality, the bootstrapping process:

- Automatically instantiates, onboards, and configures the firewall instance without prior knowledge of the firewall serial number.
- Automatically onboards the Strata Cloud Manager tenant, which receives the initial configuration and becomes fully operational without manual intervention.

The bootstrapping process requires specific fields to function. For instance, the `panorama-server` field specifies cloud management for your Panorama host, initiating a TLS connection to the Strata Cloud Manager service edge. Setting the value to `cloud` initiates a connection to the service edge, while any other value is interpreted as a Panorama IP address or FQDN for a direct Panorama management connection. The value defined for `panorama-server-2` is ignored when `panorama-server=cloud`.

You also need to define the Cloud Management folder using the `dgname` field, which maps the firewall. The `vm-series-auto-registration-pin-id` and `vm-series-auto-registration-pin-value` fields automate firewall instance instantiation by establishing the connection to the Strata Cloud Manager service edge. These PIN ID and PIN value fields are used to request a Thernite certificate, which authenticates the device and builds a secure connection to the cloud service, such as Strata Cloud Manager.

Cloud Management for NGFWs: Security Posture Checks

Managing configuration compliance and security best practices often requires navigating multiple, siloed settings pages, leading to inconsistent enforcement and complex exception handling. Strata Cloud Manager now unifies these critical capabilities into [Security Posture Settings](#), consolidating security check functionality previously split across AIOps and Cloud Manager pages. This unification streamlines your security workflow, allowing you to manage both predefined best practice checks (aligned with industry standards like CIS and NIST) and custom organizational checks from a single centralized location. This feature enhances policy granularity by offering a centralized **Check Exception** capability, allowing you to restrict where checks apply to your deployment rather than simply enabling or disabling them globally. Furthermore, security checks raise an Alert (default) for a failed check, or Block a configuration with failing checks from being pushed out to your deployment. security checks provide immediate, field-level feedback during policy creation, empowering you to address configuration deviations instantly and ensure alignment with best practices before any policy deployment.

Cloud Management for NGFWs: GlobalProtect

You can now use [GlobalProtect](#) with [cloud-managed NGFWs](#) to secure your mobile workforce. Enable your cloud-managed NGFWs as GlobalProtect gateways and portals, in order to provide flexible, secure remote access to users everywhere.

Whether checking email from home or updating corporate documents from an airport, the majority of today's employees work outside the physical corporate boundaries. This workforce mobility increases productivity and flexibility while simultaneously introducing significant security risks. Every time users leave the building with their laptops or smart phones, they are bypassing the corporate firewall and associated policies that are designed to protect both the user and the network. [GlobalProtect](#)™ solves the security challenges introduced by roaming users by extending the same next-generation firewall-based policies that are enforced within the physical perimeter to all users, no matter where they are located.

Cloud Management for NGFWs: IP Protocol Scan Protection

November 2, 2023

Supported on Strata Cloud Manager for:

- [Cloud Management of NGFWs](#) → Introduced with [PAN-OS 11.1](#)
-

Malicious actors scan Internet Protocol (IP) numbers to identify and exploit open and insecure protocols on target hosts. This reconnaissance technique involves cycling through IP protocol numbers to discover the IP protocols and services that the target host supports, sometimes with the help of automated tools. Starting with PAN-OS® 11.1, you can [enable reconnaissance protection](#) against IP protocol scans.

When enabled, your Next-Generation Firewall (NGFW) detects IPv4 and IPv6 protocol scans based on a specified number of scan events that occur within a specified interval. By default, your NGFW generates an alert in the Threat logs when these thresholds are met. However, you can configure the NGFW to take other actions, such as dropping subsequent packets from the source IP address to the target host for a specified time. To minimize false positives and allow legitimate activity, you can exclude the IP addresses of trusted internal groups performing vulnerability testing from this protection.

Details of each detected scan are available in Threat logs.

Cloud Management for NGFWs: TLSv1.3 Support for SSL/TLS Service Profiles (Administrative Access)

November 2, 2023

Supported on Strata Cloud Manager for:

- [Cloud Management of NGFWs](#) → Introduced with [PAN-OS 11.1](#)
-

Previously, you could not configure TLSv1.3 support for administrative access in the standard SSL/TLS service profile. In addition, you could only manage cipher suites using the command line interface (CLI). PAN-OS® 11.1 solves these challenges by enhancing the [SSL/TLS service profile](#).

You can now select TLSv1.3 as the minimum and maximum supported TLS version directly in an SSL/TLS service profile. Selecting TLSv1.3 automatically enables a set of modern and secure cipher suites. Additionally, you can customize key exchange algorithms, encryption algorithms, and authentication algorithms without using the CLI.



You can only use TLSv1.3-enabled SSL/TLS service profiles for administrative access and [GlobalProtect®](#) portals and gateways.

TLSv1.3 improves the security and performance of administrative connections to your Next-Generation Firewalls and other management interfaces. The protocol removes support for vulnerable algorithms, mandates perfect forward secrecy, and reduces connection latency through a faster TLS handshake.

Enforcing Authentication Cookie Validation

In mobile and roaming environments, preventing session hijacking is critical for maintaining robust security. Previously, an endpoint's authentication cookie could be used even if the device's network location changed, creating a potential security risk if the cookie was intercepted.

To mitigate this threat, you can now enforce that the GlobalProtect portal or gateway accepts authentication cookies only when the endpoint's IP address matches the original source IP address or falls within a designated network range. This security enhancement is important for maintaining session integrity in environments where users may roam within a campus or corporate subnet.

Enabling this capability ensures that if the network originally issued an authentication cookie to an endpoint within a secure network range, the cookie remains valid only for endpoints within that same network segment. By binding the authentication cookie to a designated network range, you mitigate the risk of unauthorized access attempts.

This existing feature in Panorama is now available in Prisma Access managed by Strata Cloud Manager. For more information, see [GlobalProtect – Customize App Settings](#).

End User Timeout Notifications

In remote and mobile work environments, unexpected session disconnections due to login lifetime or inactivity timeouts can interrupt user workflow and lead to poor productivity. Without advance warning, users may lose their context or unsaved work.

To prevent this frustrating experience, administrators can now configure timeout settings that proactively notify end users before a GlobalProtect session disconnects. This capability allows you to customize the following to provide a better user experience:

- **Advance Warning for Expiry:** Set the amount of advance notice users receive before a session expires due to the maximum Login Lifetime or Inactivity Logout period being reached.
- **Custom Notifications:** Tailor the notification message content to clearly inform users why their session is ending and what their next steps should be.
- **Administrator Logout Message:** Specify whether to notify end users and customize the display message when an administrator manually logs them out of a session.

By clearly communicating when sessions are about to expire, you help users save their work and re-establish a connection without interruption, improving security posture and reducing help desk tickets related to sudden disconnections.

This existing feature in Panorama is now available in Prisma Access managed by Strata Cloud Manager. For more information, see [configure timeout settings](#).

Separate Client Authentication for Portal and Gateway

[Prisma Access now allows you to separate client authentication for portals and gateways for enhanced security and flexibility](#). You can apply distinct certificate profiles to each. This feature is supported for both multi-portal and coexistent tenants.

Enforcing Authentication Cookie Validation

In mobile and roaming environments, preventing session hijacking is critical for maintaining robust security. Previously, an endpoint's authentication cookie could be used even if the device's network location changed, creating a potential security risk if the cookie was intercepted.

To mitigate this threat, you can now enforce that the GlobalProtect portal or gateway accepts authentication cookies only when the endpoint's IP address matches the original source IP address or falls within a designated network range. This security enhancement is important for maintaining session integrity in environments where users may roam within a campus or corporate subnet.

Enabling this capability ensures that if the network originally issued an authentication cookie to an endpoint within a secure network range, the cookie remains valid only for endpoints within that same network segment. By binding the authentication cookie to a designated network range, you mitigate the risk of unauthorized access attempts.

This existing feature in Panorama is now available in Prisma Access managed by Strata Cloud Manager. For more information, see [GlobalProtect – Customize App Settings](#).

IoT Security: Device Visibility and Automatic Policy Rule Recommendations

integrates with [IoT Security](#) to provide visibility into the devices on your network and automated policy rule recommendations for policy enforcement on next-generation firewalls and . By having functionality in , IoT device visibility and policy rule recommendations become available in the same platform you're using to manage firewalls and interact with other network security products.

When your firewalls or is subscribed to , you can use the following IoT Security features from the web interface:

- **IoT Security Dashboard:** In , there is an [IoT Security dashboard](#) with information about the devices on the network, their device profiles and operating systems, and how they are distributed by device type across subnets. For advanced products (Enterprise Plus, Industrial , or Medical), the IoT Security dashboard additionally displays the total number of active alerts to date and vulnerabilities to date.
- **Assets Inventory:** See a dynamically maintained [inventory](#) of the devices on your network with numerous attributes for each one such as its IP and MAC addresses; profile, vendor, model, and OS; and (for advanced products) its device-level risk score.
- **Security Policy Rule Recommendations:** provides with automatically generated [Security policy rule recommendations](#) organized by device profile. There is one recommendation per application per profile. Choose a profile, select the rule recommendations you want to use, and then the next-generation firewalls or sites where you want to enforce them.

New Features in October 2023

Here are the latest new features introduced on Strata Cloud Manager. Features listed here include some feature highlights for the [products supported with Strata Cloud Manager](#). For the full list of new features supported for a product you're using with Strata Cloud Manager, [see the release notes for that product](#).

Prisma SD-WAN: Native SASE Integration

October 23, 2023

Supported on Strata Cloud Manager for:

- [Prisma SD-WAN](#) starting from October 2023.
-

The native SASE integration features an [onboarding](#) process that effortlessly integrates Prisma SD-WAN with Prisma Access. With previous Prisma Access versions, you needed to configure the additional component — Prisma Access for Networks (Cloud Managed) CloudBlade to onboard Prisma SD-WAN sites to Prisma Access. The native SASE integration between Prisma SD-WAN and Prisma Access further simplifies onboarding by eliminating the need to set up the CloudBlade. Prisma Access currently supports this integration only for new Prisma SASE (Strata Cloud Manager) deployments. For Panorama Managed Prisma Access deployments, continue using CloudBlades for integration with Prisma SD-WAN. Prisma SASE Easy Onboarding works seamlessly with both Prisma Access Cloud Managed and Panorama Managed deployments.

Prisma Access: Cisco Catalyst SD-WAN Integration

October 17, 2023

Supported on Strata Cloud Manager for:

- [Prisma Access \(Cloud Management\)](#) → Introduced with Prisma Access 2.1 Preferred
-

To use [Cisco Catalyst SD-WAN](#) with Prisma® Access, you needed to create remote networks and IPSec tunnels manually. You can now onboard a remote network using IPSec tunnels between Cisco Catalyst SD-WAN and Prisma Access automatically. This feature automatically discovers eligible sites, creates the necessary remote networks, and establishes IPSec tunnels between Cisco Catalyst SD-WAN and Prisma Access, which significantly reduces manual configuration time and enables faster deployment.

Contact your Palo Alto Networks account representative to enable this functionality. After you enable the automatic creation of tunnels, configure the settings to establish the connection between Prisma Access and Cisco Catalyst SD-WAN. View the discovered sites that are eligible for the integration, and enable them accordingly. This creates remote networks and establishes IPSec tunnels. Ensure to follow all the requirements and prerequisites before you enable this functionality.

New Features in September 2023

Here are the latest new features introduced on Strata Cloud Manager. Features listed here include some feature highlights for the [products supported with Strata Cloud Manager](#). For the full list of new features supported for a product you're using with Strata Cloud Manager, [see the release notes for that product](#).

Prisma Access: Traffic Mirroring and PCAP Support

September 29, 2023

Supported on Strata Cloud Manager for:

- [Prisma Access Cloud Management](#) → Introduced with [Prisma Access 4.1](#)
-

Prisma® Access secures your traffic in real time based on traffic inspection, threat analysis, and security policies. While you can view Prisma Access logs to view security events, your organization might have a requirement to [save packet capture \(PCAP\) files for forensic and analytical purposes](#), for example:

- You need to examine your traffic using industry-specific or privately-developed monitoring and threat tools in your organization and those tools require PCAPs for additional content inspection, threat monitoring, and troubleshooting.
- After an intrusion attempt or the detection of a new zero-day threat, you need to preserve and collect PCAPs for forensic analysis both before and after the attempt. After you analyze the PCAPs and determine the root cause of the intrusion event, you could then create a new policy or implement a new security posture.
- Your organization needs to download and archive PCAPs for a specific period of time and retrieve as needed for legal or compliance requirements.
- Your organization requires PCAPs for network-level troubleshooting (for example, your networking team requires data at a packet level to debug application performance or other network issues).

To accomplish these objectives, you can enable traffic replication which uses the Prisma Access cloud to replicate traffic and encrypt PCAP files using your organization's encryption certificates.

Prisma Access: New Local Zones

September 29, 2023

New local zones:

- South America West (Lima)
- Nigeria (Lagos)
- New Zealand (Auckland)

Now supported on Strata Cloud Manager for:

- [Prisma Access Cloud Management](#) → Introduced with [Prisma Access 4.2](#)
-

[Local zones](#) place compute, storage, database, and other services close to large population and industry centers. These locations have their own compute locations.

Keep in mind the following guidelines when deploying local zones:

- Local zone locations do not support [IPv6](#).
- Local zone locations do not use Palo Alto Networks registered IP addresses.
- 1 Gbps support for remote networks is not supported.
- Remote network and service connection node redundancy across availability zones is not available if you deploy them in the same local zone, as both nodes are provisioned in a single zone.
- These local zones do not use Palo Alto Networks registered IPs. If you have problems accessing URLs, [report the website issue](#) using <https://reportasite.gpcloudservice.com/> or reach out to Palo Alto Networks support.
- Some SaaS applications might experience a higher latency in local zones when compared with non-local zone locations.

Prisma Access: Microsoft Defender for Cloud Apps Integration

September 29, 2023

Supported on Strata Cloud Manager for:

- [Prisma Access Cloud Management](#)
-

Unmanaged cloud services and shadow IT applications can introduce significant security risks to your network. To address this issue, you can now integrate Prisma® Access with [Microsoft Defender for Cloud Apps](#). This integration automatically syncs and blocks the list of unsanctioned applications inline, providing crucial closed-loop remediation. This integration enables you to gain visibility and to discover all cloud applications and shadow IT applications being used. The automated syncing and blocking provide crucial closed-loop remediation for unsanctioned applications.

Microsoft Defender is one of many Microsoft products that Prisma Access integrates with so that you can protect your applications and data on Azure, in Office 365, on the network, and the endpoint.

Cloud Management for NGFWs: New Predefined BGP Distribution Profile (Auto VPN & SD-WAN)

September 29, 2023

Supported on Strata Cloud Manager for:

- [Cloud Management for NGFWs](#) (with an [AIOps for NGFW Premium license](#))
-

Configuring full mesh connectivity and ensuring dynamic branch-to-branch communication in complex SD-WAN environments often requires manual intervention and intricate Border Gateway Protocol (BGP) setup. This process is time-consuming and can lead to configuration errors, potentially limiting the seamless flow of traffic across autonomous systems (AS).

[Auto VPN](#) simplifies network reachability management across your managed connections using SD-WAN. When you add to a VPN cluster, automatically assigns the predefined All - Connected - Routes BGP Redistribution profile by default. This BGP Redistribution profile determines network reachability based on IP prefixes available within autonomous systems (AS).

By setting the All - Connected - Routes profile as the default, you ensure SD-WAN broadcasts all connected routes to every VPN peer in the cluster. This profile handles both the necessary tunnel and route peering configuration, completing all route advertisements required for secure, dynamic branch-to-branch communication without administrative overhead. This automation immediately enables full network visibility, saving significant configuration time and ensuring a consistent routing policy across your entire VPN cluster.

Cloud Management for NGFWs: Custom Path Quality Profile (SD-WAN)

September 29, 2023

Supported on Strata Cloud Manager for:

- [Cloud Management for NGFWs](#) (with an [AI Ops for NGFW Premium license](#))
-

Managing the performance of business-critical and latency-sensitive applications across multiple [SD-WAN](#) paths requires strict, real-time quality control. Network deterioration, even brief spikes in latency, jitter, or packet loss, can severely impact user experience and service continuity. Security administrators can now create custom path quality profiles for SD-WAN to define unique network quality requirements for applications, services, and groups.

Create a custom path quality profile on Strata Cloud Manager to establish maximum thresholds for key performance indicators: latency, jitter, and packet loss percentage. Security administrators specify the maximum limit for each parameter, above which the firewall considers the path unreliable. The firewall treats these criteria as **OR conditions**, meaning if the network quality exceeds any one of the defined thresholds (latency OR jitter OR packet loss), the firewall immediately selects the new best path. Any path that has latency, jitter, and packet loss metrics less than or equal to all three defined thresholds is considered qualified, and the firewall selects the final path based on the associated Traffic Distribution profile, ensuring consistent, high-quality network resources for your most demanding applications.

Cloud Management for NGFWs: Pre-Shared Keys Refresh (Auto VPN & SD-WAN)

September 29, 2023

Supported on Strata Cloud Manager for:

- [Cloud Management for NGFWs](#) (with an [AIOps for NGFW Premium license](#))

[Auto VPN](#) allows you to configure secure connectivity between and your managed firewalls using [SD-WAN](#). Peers in the VPN cluster use a pre-shared key to mutually authenticate each other. now allows you to refresh the pre shared keys used for authenticating VPN tunnels for existing VPN clusters (**Manage > Configuration > NGFW and Prisma Access > Global Settings > Auto VPN**).

Config Push to refresh the Pre-Shared Key

Refreshing the Pre-shared key will generate a new security association (SA) for every SD-WAN firewall in the VPN cluster. This may cause a service disruption. If you are OK, check the acknowledgment service disruption, then click the Push button.

☐ Acknowledge the possible service disruption

VPN Cluster

thiyagu-sdwan1

Targets (4)

Target

Parent Location

Thiyagu_S1_168_162

All > Firewall > Thiyagu SDWAN > Spoke1

Thiyagu_S2_168_126

All > Firewall > Thiyagu SDWAN > Spoke2

Thiyagu_h1_169_172

All > Firewall > Thiyagu SDWAN > HUB1

Thiyagu_hub2_169_96

All > Firewall > Thiyagu SDWAN > HUB2

Cancel

Push

Cloud Management for NGFWs: Cloud IP Tag Collection (with the Cloud Identity Engine)

September 29, 2023

Supported on Strata Cloud Manager for:

- [Cloud Management for NGFWs](#) (with an [AIOps for NGFW Premium license](#))

Enforcing your security policy consistently across all the firewalls in your network relies on those firewalls having the most up-to-date identity information from your sources, such as cloud-based identity management systems. With the array of management systems and large numbers of users and devices, it can often be time-consuming and difficult to correlate identity information with its originating sources and ensure that it was provided to all necessary devices.

You can now use Strata Cloud Manager with the Cloud Identity Engine to manage IP address-to-tag (also known as IP-tag) mappings and simplify your security policy by creating tag-based rules. When you [configure a cloud connection](#) in the Cloud Identity Engine to your cloud-based identity management system (either Azure or AWS), you can use the Cloud Identity Engine to collect IP-tag mappings.

You can see all of your IP-tag mappings, as well as their associated sources, in the Cloud Identity Manager. Using filters to highlight the most relevant information, you can quickly identify issues with your security policy, such as a source that is currently unavailable. You can then use the Strata Cloud Manager to create tag-based security policy using [dynamic address groups](#) and distribute it to the firewalls in your network to ensure they have the latest information needed to consistently enforce security policy. You can also share the IP-tag mappings with other firewalls in your network by using [User Context segments](#) in the Cloud Identity Engine.

By leveraging the capabilities of Strata Cloud Manager with the identity information that the Cloud Identity Engine provides, you can more easily create and manage your security policy using tags.

Cloud Management for NGFWs: Configuration Version Snapshot

September 29, 2023

Supported on Strata Cloud Manager for:

- **NEW THIS MONTH** [Cloud Management for NGFWs](#) (with an [AIOps for NGFW Premium license](#))
 - [Prisma Access Cloud Management](#) (with a Prisma Access license)
-

Managing configuration pushes for cloud managed NGFWs and Prisma® Access deployments often lacks comprehensive oversight and rapid recovery options. [Config Version Snapshots](#) solve this by providing enhanced visibility and control over your security infrastructure changes, ensuring you can confidently deploy updates while maintaining the ability to quickly recover from any unintended consequences.

You can now evaluate configuration pushes with detailed analysis tools, compare your candidate configuration against previously pushed configurations to identify specific changes, and rollback recent modifications in the event of any unintended consequences from a recent push. This comparison functionality helps you understand exactly what will change before committing updates to production environments.

The system allows you to load previous configurations to use as candidates for your next configuration push, enabling you to build upon proven stable configurations and make incremental changes to expand the scope of the original setup. This iterative approach reduces risk by allowing you to test and validate changes incrementally rather than implementing large-scale modifications all at once.

When issues arise, you can restore previous configurations to immediately rollback the changes from a recent configuration push, minimizing downtime and quickly returning your security infrastructure to a known good state. This rollback capability is essential for maintaining business continuity during configuration troubleshooting scenarios.

Additionally, you can review the specific devices or deployments that are impacted or targeted by your configuration pushes, providing you with complete visibility into the full scope of changes across your entire security infrastructure. This comprehensive view ensures you understand which systems will be affected before executing any configuration updates.

Cloud Management for NGFWs: Troubleshooting for NGFW Connectivity and Policy Enforcement

September 29, 2023

Supported on Strata Cloud Manager for:

- [Cloud Management for NGFWs](#) (with an [AIOps for NGFW Premium license](#))
 - [Prisma Access Cloud Management](#) (with a Prisma Access license)
-

Troubleshoot these networking and identity features—track down and resolve connectivity issues or policy enforcement anomalies:

- [NAT](#)
- [DNS Proxy](#)
- [User Groups](#)
- [Dynamic Address Groups](#)
- [Dynamic User Groups](#)
- [User ID](#)

Network Troubleshooting for NAT and DNS Proxy

Troubleshoot your NGFWs from Strata Cloud Manager without having to move between various firewall interfaces. If you experience connectivity issues after deploying and configuring your NGFWs, you can get an aggregate view of your routing and tunnel states, and drill down to specifics to find anomalies and problematic configurations.

Identity and Policy Troubleshooting

Troubleshoot your identity-based policy rules and dynamically defined endpoints. Check the status of specific NGFWs and expose possible mismatches between how you expect a policy to work and its actual enforcement behavior.

Cloud Management for NGFWs: Config Cleanup

September 29, 2023

Supported on Strata Cloud Manager for:

- **NEW THIS MONTH** [Cloud Management for NGFWs](#) (with an [AIOps for NGFW Premium license](#))
 - [Prisma Access Cloud Management](#) (with a Prisma Access license)
-

Do dynamic business needs often require you to deal with rapid configuration changes that result in complex configurations with a number of zero hit rules, zero hit objects, unused objects, and duplicate objects? Such configurations can lead to a poor security posture and can inadvertently increase the attack surface of your network. [Config Cleanup](#) has you covered.

Config Cleanup gives you a comprehensive view of all policy rules that have no hits, objects that aren't referenced directly or indirectly in your configuration, objects that are referenced in a policy rule but have no hits in the Traffic log during the specified time frame, and objects of the same type with different names but have the same values so that you can better:

- Manage attack surface exposure
- Prioritize remediation actions
- Remediate over time
- Respond to audit questions when they arise

Identify and remove unused configuration objects and policy rules from your configuration. Removing unused configuration objects eases administration by removing clutter and preserving only the configuration objects that are required for security enforcement.

Review unused objects and policy rules across your entire Strata Cloud Manager configuration for the last 6 months, and optimize policy rules that are overly permissive rules to convert these to be more specific, focused rules that only allow the applications you're actually using.

Together with [Policy Optimizer](#), these tools help you ensure that your policy rules stay fresh and up to date.

Cloud Management for NGFWs: Policy Optimizer

September 29, 2023

Supported on Strata Cloud Manager for:

- **NEW THIS MONTH** [Cloud Management for NGFWs](#) (with an [AIOps for NGFW Premium license](#))
 - [Prisma Access Cloud Management](#) (with a Prisma Access license)
-

Overly permissive security rules—such as those allowing "any" application traffic—are common in large networks, creating security gaps by enabling unused applications and unnecessarily increasing the attack surface. Manual review and optimization of these broad rules require extensive log analysis and introduce deployment risk. Strata Cloud Manager introduces Policy Optimizer that analyzes log data to identify overly permissive security rules. [Policy Optimizer](#) auto-generates specific, focused rule recommendations based only on the applications actively observed on your network. This capability eliminates the need for manual log analysis, strengthens your security posture, and reduces administrative overhead. Administrators receive actionable, auto-generated optimization recommendations that can be reviewed and accepted through a guided workflow, ensuring that rule consolidation and replacement are secure and policy integrity is maintained. Together with [Config Cleanup](#), these tools help you ensure that your policy rules stay fresh and up to date.

Cloud Management for NGFWs: Explicit Web Proxy

September 29, 2023

Supported on Strata Cloud Manager for:

- [Cloud Management for NGFWs](#) (with an [AIOps for NGFW Premium license](#) and the legacy router stack enabled. If you'd like this enabled, please reach out to your account team.)



Prisma[®] Access has its own, separate [method of configuring explicit proxy](#). This new feature applies only to cloud-managed firewalls.

To consolidate management, you can now [configure a web proxy on the firewalls you're managing with[®]](#). This means that if you use an NGFW as a proxy device to secure your network, you can configure your proxy settings across your deployment from a single management interface.

This interface includes an in-app Proxy Auto-Configuration (PAC) file editor so that you can edit your proxy settings and modify your PAC file all in one place whenever network changes arise.

The web proxy supports two methods for routing traffic:

- [Explicit Proxy](#)— The request contains the destination IP address of the configured proxy, and the client browser sends requests to the proxy directly. Authentication methods such as Kerberos and SAML 2.0 are supported, requiring the appropriate web proxy licensing.
- [Transparent Proxy](#)—The request contains the destination IP address of the web server and the proxy transparently intercepts the client request (either by being in-line or by traffic steering). This method requires specific networking prerequisites, including a loopback interface, User-ID configuration in the proxy zone, and specific Destination NAT (DNAT) rules defined in . Transparent proxy does not support X-Authenticated Users (XAU) or Web Cache Communications Protocol (WCCP).

You can push web proxy configurations to the following platforms:

- PA-1400
- PA-3400
- VM-Series (with a minimum of four vCPUs)

Strata Cloud Manager: SaaS Application Endpoint Lists and Enforcement

September 29, 2023

Supported on Strata Cloud Manager for:

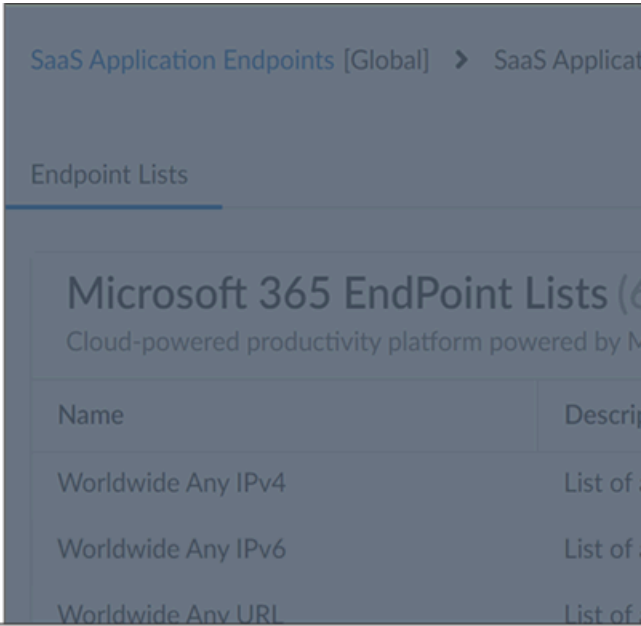
- [Cloud Management for NGFWs](#) (with an [AIOps for NGFW Premium license](#))
- [Prisma Access Cloud Management](#) (with a Prisma Access license)

SaaS providers publish lists of the IP addresses and URL endpoints their SaaS applications use, and frequently update these lists. Strata Cloud Manager now consumes application endpoint lists from the [Palo Alto Networks EDL Hosting Service](#), so that you can easily enforce policy for SaaS providers including (but not limited to):

- Microsoft
- Azure
- Amazon Web Services (AWS)
















- Google Cloud Platform (GCP)
- Salesforce (SFDC) public endpoints
- Microsoft Defender
- Zoom
- GitHub

In Strata Cloud Manager, you can now subscribe to SaaS application endpoints lists (both optional and required), and reference the lists in policies for your cloud-managed NGFWs and Prisma Access.



SaaS Application Endpoints ⓘ

SaaS Application Endpoints

SaaS Application Endpoints (15)	
Name	Description
 AWS	The world's most comprehensive and broadly adopted cloud, o
 GCP	Suite of cloud computing services that runs on the same infras
 Azure	Build, run, and manage applications across multiple clouds, on-
 SFDC	A cloud-based Customer Relationship Management (CRM) plat
 Microsoft 365	Cloud-powered productivity platform powered by Microsoft Te
 MS Intune	Cloud-based unified endpoint management for your organizati
 Zoom	Communications platform that allows users to connect with vi
 Webex	Enterprise solution for video conferencing, online meetings, sc
 Google Workspace	A collection of cloud computing, productivity and collaboration
 Github	Platform and cloud-based service for software development an
 Akamai	Content delivery network, cybersecurity, and cloud service cor
 msdefender	A defense suite that natively coordinates detection, prevention
 Datadog	An observability service for cloud-scale applications, providing
 PANW	The best enterprise cybersecurity platform that provides netw
 Okta	Provides cloud software that helps companies manage and sec



Important to know:

- This feature natively integrates the [Palo Alto Networks EDL Hosting Service](#) with Strata Cloud Manager. If you are or were previously using the EDL Hosting Service, the introduction of this feature doesn't impact any of your existing configuration. Any EDLs you've already created that reference a feed URL will continue to work as expected.
- Until now, the O365-Best-Practice snippet enabled you to directly subscribe to M365 endpoint lists in Strata Cloud Manager. With this feature, this snippet is now updated to be an application endpoint list. If you were using this snippet in a policy rule, the update is seamless, and the policy rule will reference the migrated application endpoint list.
- [SaaS Tenant Restrictions](#) continue to provide you a way limit SaaS app usage to enterprise accounts (to stop users from accessing their personal accounts on the company network).
- SaaS providers publish lists of the IP addresses and URL endpoints their SaaS applications use, and frequently update these lists. Strata Cloud Manager now hosts these SaaS application endpoint lists directly, so that you can enforce policy for application endpoints from SaaS providers including (but not limited to):

Strata Cloud Manager: Snippet Deletion

September 29, 2023

Supported on Strata Cloud Manager for:

- [Cloud Management for NGFWs](#) (with an [AIOps for NGFW Premium license](#))
 - [Prisma Access Cloud Management](#) (with a Prisma Access license)
-

Administrators often struggle with disorganized configuration scopes due to unused custom snippets cluttering their management interface. Over time, as network configurations evolve and deployments change, custom snippets can become obsolete or redundant, creating confusion during configuration management tasks and increasing the risk of accidentally applying outdated or inappropriate configurations to production environments.

You can now [delete custom snippets](#) that are no longer associated with any deployments, firewalls, or folders to keep your configuration scope organized and prevent unwanted or unused snippets from being applied by mistake. This cleanup capability helps maintain a streamlined configuration management experience and reduces the potential for configuration errors.

Snippets in Strata Cloud Manager are classified into two categories: Predefined snippets are available to all Strata Cloud Manager users and help you quickly get your new firewalls and deployments up and running with best practice configurations. Custom snippets are any snippets that administrators create for specific organizational needs.

You can delete unused custom snippets directly from the configuration scope view, providing a convenient way to maintain an organized snippet library. Note that predefined snippets available in Strata Cloud Manager cannot be deleted, ensuring that essential best practice configurations remain available to all users.

Strata Cloud Manager: Enhancements to WildFire Dashboard

September 27, 2023

Supported on Strata Cloud Manager for:

- [Cloud Management for NGFWs](#) (with an [AIOps for NGFW Free license](#) and [Advanced WildFire](#))
 - [Prisma Access Cloud Management](#) (with a Prisma Access license, which includes [Advanced WildFire](#))
-

The [Advanced WildFire dashboard](#) is now enhanced to provide a comprehensive view of sample analysis data that you can use to make informed decisions. The dashboard displays the source of WildFire sample submissions, insights into unique and new samples by threat type, and context on the most recent submissions from your network. The dashboard also enables filtering of data based on a file hash.

Strata Cloud Manager: Advanced WildFire Analysis Data in IoC Search

September 15, 2023

Supported on Strata Cloud Manager for:

- [Cloud Management for NGFWs](#) (with an [AIOps for NGFW Premium license](#) and [Advanced WildFire](#))
 - [Prisma Access Cloud Management](#) (with a Prisma Access license, which includes [Advanced WildFire](#))
-

When evasive malware bypasses your defenses, it complicates post-breach analysis. You can now view Advanced Dynamic WildFire® analysis data directly within [Threat Search](#) in . This provides the in-depth detail required for a complete and thorough investigation. This feature integrates detailed results from Advanced WildFire—the cloud-based engine that detects and prevents highly evasive malware—directly into your search results.

This new data stream complements existing static and dynamic analysis, giving you a consolidated view of file behavior. As a result, you can simplify post-attack analysis, reduce investigation time, and accelerate threat hunting, all from a single screen.

Strata Cloud Manager: Signature-Based PCAP in Threat Logs

September 15, 2023

Supported on Strata Cloud Manager for:

- [Cloud Management for NGFWs](#) (with an [AIOps for NGFW Premium license](#))
-

- [Prisma Access Cloud Management](#) (with a Prisma Access license)

You can now view and download signature-based packet captures (PCAPs), along with the inline detected PCAPs in threat logs. These packet captures provide context around a threat to help you report false-positives or learn more about the methods used by the attacker. To download a PCAP, [view threat type logs](#) in the [Log Viewer](#) and download packet captures.

Strata Cloud Manager: Log Viewer Visibility Enhancements

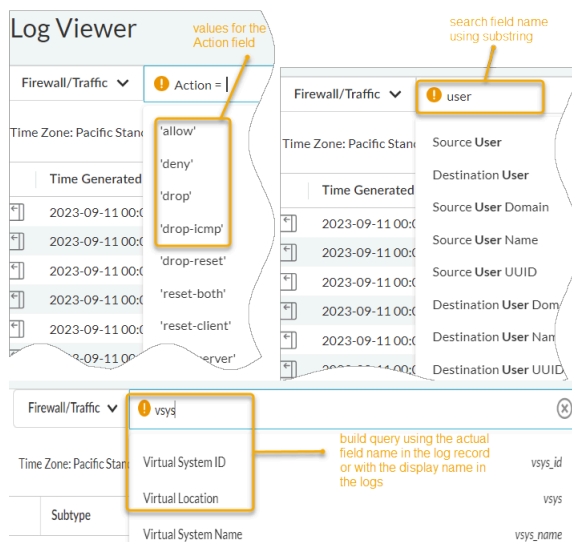
September 15, 2023

Supported on Strata Cloud Manager for:

- [Cloud Management for NGFWs](#) (with an [AIOps for NGFW Premium license](#))
- [Prisma Access Cloud Management](#) (with a Prisma Access license)

[Log Viewer](#) is enhanced to search and view relevant logs easily. The enhancements include:

- Autosuggestions for field values when you select a field in the query builder.
- Search field names using substrings (for example, search with the string 'user' returns suggestions such as source_user, destination_user).
- Search for a field based on the displayed field name in the log table and not just the actual field name in the log record. The query builder uses the displayed field name.
- Press Shift + Enter to start a new line in the query builder, and press Enter to submit a query.



Known Issues

Review the issues we're working to fix in Strata Cloud Manager.



These are known issues found in the Strata Cloud Manager platform. You can also review in-progress fixes for the subscriptions and products supported for Strata Cloud Manager here:

- [NGFW Release Notes \(AIOps for NGFW and Cloud Management for NGFW\)](#)
- [Prisma Access Release Notes](#)
- [Prisma SD-WAN Release Notes](#)
- [AI-Powered Autonomous DEM Release Notes](#)

Cloud-Delivered Security Services (CDSS) docs:

- [Advanced WildFire](#)
- [Advanced Threat Prevention](#)
- [Advanced URL Filtering](#)
- [DNS Security](#)
- [SaaS Security](#)
- [Enterprise DLP](#)

Configuration Management Known Issues

ID	Description
ADI-48921	Load results after virtual router migration displays the truncated loopback, and the firewall difference will show this difference.
ADI-40135	Added support for creating new OSPF and PSOFv3 interface Timer profiles. These custom profiles can now be selected directly from the Router Form.
ADI-50619	<p>When a URL filtering or tenant restriction profile is configured together with a SaaS Security profile and all are referenced in the same profile group, conflicts may occur. Merging them into a single URL filtering profile can result in a commit failure on the firewall.</p> <p>Workaround: Remove the SaaS Security profile from the profile group.</p>
ADI-49478	<p>In Strata Cloud Manager, the ADNS option appears under the forwarding profile settings within the connectivity object configuration, even though ADNS is not yet supported in the current Prisma Access Agent releases. The option is shown as disabled by default, but since the functionality is not implemented in the agent software, this setting should not be used.</p> <p>Workaround: Administrators should ignore the ADNS option in Strata Cloud Manager until agent support becomes available in a future release.</p>
ADI-49571	<p>When you create a snippet and associate it with a vsys, if the snippet contains an interface variable with a resolved value and you use that variable in a logical router, zone, or NAT policy, the push operation fails.</p> <p>Workaround: Avoid configuring interface, logical router, or zone settings at the snippet level when the snippet is associated with vsys.</p>
ADI-50448	As part of the NGFW migration, you need to choose the Distribution Groups to migrate. However, distribution group named All or ngfw-shared cannot be selected, as these names are reserved in Strata Cloud Manager for Global and All Firewalls, respectively.
ADI-47855	<p>When you attempt to run Push Config operations from the SASE Private Location wizard, the action fails.</p> <p>Workaround: Perform the Push Config from Strata Cloud Manager instead of from the wizard.</p>

ID	Description
ADI-43690	Local configuration management feature is not currently supported for Device Setup widgets and several other objects. Support for these will be added in a future update.
ADI-40767	The dampening profile configuration is not available under Device Settings > Routing > Profiles > BGP in Strata Cloud Manager.
ADI-40766	BGP timer profiles configuration is not available under Device Settings > Routing > Profiles > BGP .
ADI-40765	Global connection options are not available under Device Settings > Routing > Logical Routers > BGP Peer Group in Strata Cloud Manager.
ADI-35760	On the AI Access Security Use Case page (Insights > AI Access), changing the application tag for a container app does not automatically update the tags for its child apps.
ADI-35546	<p>Two discrete applications with the same App-ID are displayed in the list of Applications (Manage > Configuration > NGFW & Prisma Access > Objects > Application > Applications) and Application Filters (Manage > Configuration > NGFW & Prisma Access > Objects > Application > Applications Filters) if the application is available as part of the predefined apps provided with your currently installed dataplane version and delivered from the App-ID Cloud Engine (ACE). The two discrete App-IDs may have different attributes, such as Tags and the Risk Score.</p> <p>For example, ChatGPT is available as a predefined app and is also delivered from ACE. In this case, you see two entries of ChatGPT when you view your Applications and Application Filters.</p>
ADI-29665	Dynamic Privilege Access: Do not use special characters in project names, otherwise Strata Cloud Manager will issue a "Malformed Request" error message when you try to save the project configuration.
ADI-33262	<p>On a Prisma Access tenant where Dynamic Privilege Access is enabled, a Mobile User > Access Agent configuration push will fail without first configuring a project in Strata Cloud Manager.</p> <p>Workaround: Configure at least one project before you do a push config.</p>
ADI-33776	When configuring the Dynamic DNS feature in Prisma Access, ensure that the file name for the key file uploaded for Kerberos or TSIG key file is less than or equal to 32 characters.

ID	Description
ADI-33914	Profile hit counts are not incremented in the URL filtering profile in Strata Cloud Manager.
ADI-30768	Configure Remote Network Tunnel > Protocol doesn't support Any as the option for proxy-id- protocol configuration.
ADI-19128	When configuring a Security policy rule (Manage > Configuration > NGFW and Prisma Access > Security Services > Security Policy), you're able to select address objects created outside of your scope management configuration (Manage > Configuration > NGFW and Prisma Access > Access Control > Scope Management).
ADI-31050	Proxy zone is not listed in dropdown while creating an interface. Proxy zone is a default zone like local or internet, but in the api response, it doesn't have the interface type/layer values.
ADI-30404	With remote networks internal gateway enabled, when portal authentication profile iss modified from SAML to Local User, the show global-protect-gateway gateway does not show the authentication profile correctly.
ADI-30298	DHCP Relay local config from firewalls does not show conflicts in Strata Cloud Manager for resolved interfaces.
ADI-25671	If you use a signature in an Anti-Spyware policy rule, you are unable to change the Action that Strata Cloud Manager takes when it detects the signature.
ADI-22188	Prisma Access commit opt: Incorrect Prisma Access configuration may not be caught in the Strata Cloud Manager, but fails in firewall and the error is reported back to Strata Cloud Manager post commit.
ADI-20068	ZTNA Connector Microapp on SASE portal for Strata Cloud Manager tenants should not be used by any tenants with 10.2.* AMI version.

Command Center Known Issues

ID	Description
—	<p>The Command Center is always updated with the latest data and metrics, and may not match what is available in Activity Insights or other dashboards.</p> <p>Security subscription counts, action counts, and metrics provided in the command center bubbles display the latest data available at the time.</p> <p>This is due to a few different things:</p> <ul style="list-style-type: none"> • The way that the command center refreshes data at intervals different from the other dashboards. • The command center has more filtering options for various views and time frames. <p>You may see this data in the following command center views (including widgets, bubbles, and data flows):</p> <ul style="list-style-type: none"> ❑ Summary ❑ Threats ❑ Operational Health ❑ Data Security
AIOPS-9888	In the Users tab of Activity Insights , the Monitored Users count does not accurately reflect the total count of actual monitored users. It includes branch user
NETVIS-962	In the views of the command center, public traffic may be classified as Internal Hosts under the Other bubble when security rules are set to Allow All .
NETVIS-955	In the views of the command center, the IoT Devices bubble count does not display the expected count of devices and does not match what is in the (Monitor > Assets) dashboard.
NETVIS-927	In the Threats view of the command center, the URL Filtering bubble always shows 0 applications and data transferred when following through to the Monitor dashboard.
NETVIS-924	<p>The Strata Cloud Manager command center will be unavailable in the following regions at launch:</p> <ul style="list-style-type: none"> • Spain • Indonesia • Israel

ID	Description
	<ul style="list-style-type: none">• Poland• Saudi Arabia• Qatar• Taiwan• South Korea• Italy
NETVIS-892	<p>In the Data Security view of the command center, the Sensitive Data Users bubble displays the total count of discovered users, not just sensitive users.</p> <p>Work around: Use the SaaS Security dashboard (CASB > SaaS Security).</p>
NETVIS-806	<p>In the command center views, the IoT Devices count bubble may be 0 if Strata Logging Service Next-Generation Firewall logs do not have IoT attributes.</p>
NETVIS-736	<p>In the Operational Health view of the command center, when following through on Device Health links, time-based filters available in the command center are not available in those pages.</p>
NETVIS-479	<p>In the Data Security view of the command center, the Incidents count breakdown by Severity may be lower than anticipated. Severity is not found in all incidents, resulting in them being classified as “Low” instead of their actual severity.</p>

Prisma Browser Visibility Known Issues

ID	Description
NETVIS-2040	In Activity Insights > Applications , the Rule Name column refers to Prisma Access firewall rules. It isn't applicable to Prisma Browser Standalone tenants and should not be visible.
NETVIS-1980	Some Prisma Browser data aren't populated as expected when the same tenant has been activated with Prisma Access and Prisma Browser Standalone. The following pages might not show the Prisma Browser changes: <ol style="list-style-type: none"> 1. Activity Insights > Users 2. Activity Insights > Applications 3. Monitor > Subscription Usage
NETVIS-1908	Data usage isn't available in Prisma Browser events, so in Activity Insights > Applications > details the data transfer widget is empty for a Prisma Browser standalone tenant. However, the same might have data for Prisma Browser add-on in the presence of Prisma Access as long as data is flowing through Prisma Access firewalls.
NETVIS-1905	Data usage isn't available in Prisma Browser events, so in Activity Insights > Applications the Data Usage column is empty for a Prisma Browser standalone tenant. However, the same might have data for Prisma Browser add-on in the presence of Prisma Access as long as data is flowing through Prisma Access firewalls.
NETVIS-1904	Threat information isn't available in Prisma Browser events so in Activity Insights > Applications > details , the Total Threats by Threat Type widget is empty for Prisma Browser standalone tenant. However, the same might have data for Prisma Browser add-on in the presence of Prisma Access as long as data is flowing through Prisma Access firewalls.
NETVIS-1899, NETVIS-1862	Left navigation menu items in Strata Cloud Manager that are not relevant to Prisma Browser standalone tenants are not hidden in this release. This will be taken care of in future releases.
NETVIS-1890	In Dark Mode the Prisma Browser pages display with a light background.
NETVIS-1555	An exported PDF from the Activity Insights > Users > details page does not include all the columns from the Prisma Browser summary table. This is a general issue on the size limitations of PDF exports.

Addressed Issues

Review the issues we have recently fixed in Strata Cloud Manager.



These are addressed issues found in the Strata Cloud Manager platform. You can also review in-progress fixes for the subscriptions and products supported for Strata Cloud Manager here:

- [NGFW Release Notes \(AIOps for NGFW and Cloud Management for NGFW\)](#)
- [Prisma Access Release Notes](#)
- [Prisma SD-WAN Release Notes](#)
- [AI-Powered Autonomous DEM Release Notes](#)

Cloud-Delivered Security Services (CDSS) docs:

- [Advanced WildFire](#)
- [Advanced Threat Prevention](#)
- [Advanced URL Filtering](#)
- [DNS Security](#)
- [SaaS Security](#)
- [Enterprise DLP](#)

ADI-49121 2025.r5.0	Fixed an issue where users assigned the View Only Administrator role under Configuration > Prisma Access and NGFW , were able to force logout GlobalProtect users, even though this action should not have been permitted for their role.
ADI-48273 2025.r5.0	Fixed an issue where, after committing and pushing changes, the SASE private region name could no longer be modified.
ADI-47882 2025.r4.2	Fixed an issue where the projects page in Dynamic Privilege Access displayed an internal server error when accessed through Access > Agent > Dynamic Privilege Access > Projects . The error occurred when opening the page or attempting to edit a project.
ADI-44920 2025.r4.0	Fixed an issue where the imported SaaS recommended policy did not appear on the Security Policy page.
ADI-43740 2025.r4.0	Fixed an issue where SSL decryption certificates were not automatically configured. If decryption is required,

	<p>you must configure certificate settings manually before pushing the configuration to the device.</p> <p>To configure:</p> <ol style="list-style-type: none"> 1. Go to ManageConfigurationNGFW and Prisma Access, and set the Configuration Scope to Prisma Access, Remote Networks, GlobalProtect, or Explicit Proxy. 2. Navigate to Security ServicesDecryptionDecryption Settings. 3. On the Certificate Settings page, configure the trusted certificates. 4. Select the certificate authentication method: choose RSA, ECDSA, or both from the drop-down when proxying trusted sites. 5. Optionally, configure certificates for untrusted sites.
ADI-43675 2025.r3.1	Fixed an issue where the firewall upgrades failed at the initial stage with the message: "Version 11.1.0 not downloaded / uploaded".
ADI-44340 2025.r3.0	Fixed an issue where a commit would fail on the Firewall if a decryption policy is configured with SSL forward proxy did not include an SSL decrypt certificate. To avoid commit failure, ensure that an SSL decrypt certificate is configured.
ADI-31756 2025.r3.0	Fixed an issue where configuring Snippets by navigating to Manage > Configuration > NGFW and Prisma Access Overview and expanding the Configuration Scope to view Snippets resulted in commit failures on the firewall. The issue was caused by a key synchronization issue due to an HTTP server configuration option requiring a password.
ADI-24630 2025.r3.0	<p>Fixed an issue where a validation error appeared when assigning and pushing a snippet and rulebase with the same name. This occurred in the following navigation path:</p> <p>localhost.localdomain > container > Global > prerulebase > security > rules</p> <p>Workaround: Use unique names for snippet and rulebase to avoid this error.</p>
ADI-27372 2025.r3.0	Fixed an issue where Policy Analyzer analysis results were not available for sub-tenants in Prisma Access (Managed by Panorama) multitenant environments.

ADI-40134 2025.r2.0	Fixed an issue where creating new OSPF and OSPFv3 Global Timer profiles wasn't supported. You can now create these profiles and select them directly from the Router form.
ADI-41084 2025.r1.0	Fixed an issue The GP Portal node will get pruned if the interface is used in GP Portal is not local to the FW i.e. it has come from SCM.
ADI-41809 2025.r1.0	Fixed an issue where the HIP (Host Information Profile) objects were incorrectly displayed on the unused objects page.
ADI-38277 2025.r1.0	Fixed an issue where editing an existing WebSec rule and saving it caused a partial push to the firewall, resulting in a validation job failure.
ADI-39966 2025.r1.0	Fixed an issue where onboarding of mobile user failed with the tenant default configuration, due to the missing dir-sync configuration.
ADI-40138 2025.r1.0	Fixed an issue where the certificate profile was missing in the GlobalProtect configuration within the imported snippet.
ADI-40206 2025.r1.0	Fixed an issue where the authentication profile was missing in the client authentication of the GlobalProtect Auth Profile.
ADI-40218 2025.r1.0	Fixed an issue where client certificates from Strata Cloud Manager pushed configurations were pruned during reverse transformation. This caused the certificates to be missing when pushing the associated snippet to the firewall.
ADI-40217 2025.r1.0	Fixed an issue where interface and SSL/TLS service profiles from the Strata Cloud Manager pushed configurations were missing in the GlobalProtect portal. These profiles were pruned during reverse transformation to the Strata Cloud Manager.
ADI-40420 2025.r1.0	Fixed an issue where Gateway Satellite Tunnel Monitoring and Network Settings were pruned after reverse transform and push to firewall 2, making them unavailable post push.

ADI-40951 2025.r1.0	Fixed an issue where downgrading the firewall from Release 11.2.x to Release 10.2.using the software upgrade feature was not possible.
ADI-41054 2025.r1.0	Fixed an issue where pushing a configuration that is referencing another serial number caused the push to fail on the targeted firewall pair.
ADI-41080 2025.r1.0	Fixed an issue where all configurations in the client-less VPN node were being pruned when pushed to a different firewall.
ADI-41722 2025.r1.0	Fixed an issue that caused the bootstrap process to fail due to a software installation error.
ADI-32757 2025.r1.0	Fixed an issue where creating a decryption rule locally on the firewall using a cloned object name did not display the Conflict icon for the cloned object.
ADI-37429 2025.r1.0	Fixed an issue where an error message appeared when navigating to Authentication Profiles > Identity Services > Authentication > Authentication Profiles page.
ADI-38973 September 2024	Fixed an issue where users had to create a new policy after adding an SLS license for firewalls to begin sending logs to SLS. Existing policies pushed before the license change will not send logs to SLS.
ADI-34609 September 2024	Fixed an issue that allowed the disassociation of snippets even when the referenced HIP objects were linked to HIP profiles in the associated folder. The disassociation process didn't validate these references, leading to commit failures when users pushed changes. Consequently, administrators must either clone the referenced objects to their folder or remove the referring profiles.
ADI-36127 September 2024	Fixed an issue where customers were unable to configure regular routing type entry due to regex inconsistencies between PAN-OS and Strata Cloud Manager.
ADI-35300 September 2024	Fixed an issue where customers were unable to configure Source IP for Path Monitoring in a static route from the Strata Cloud Manager.
ADI-34819 September 2024	Fixed an issue where the view and edit functionality was broken for Address Groups when they were referenced by other rules.

ADI-36624 September 2024	Fixed an issue where the Description column for HIP Object and HIP Profile was previously hidden, causing styling issues. It is now available by default.
ADI-37190 September 2024	Fixed an issue where clicking on the config version difference for a firewall with device scope disabled resulted in an error.
ADI-36387 September 2024	Fixed an issue where the filter option in Strata Cloud Manager required a refresh after clearing the filter. You can now clear the filter without needing a refresh.
ADI-35489 September 2024	Fixed an issue where some tenants were seeing multiple snippets under security rules due to missing UUIDs. This has been addressed by ensuring all the flows have UUIDs.
ADI-36043 September 2024	Fixed an issue in the Strata Cloud Manager where, after cloning a snippet, users encountered a "Failed to find obj-uuid for command get" error when attempting to edit a variable or save other configurations. This prevented any changes to the newly cloned snippet.
ADI-35656 September 2024	Fixed an issue where devices in device associations were inaccessible, preventing certain customers from adding a new folder in Strata Cloud Manager due to a null pointer exception.
ADI-36179 September 2024	Fixed an issue where tenants with only an NGFW license and no PA license had the Data Loss Prevention Profile selection hidden. This option is now available to all the Strata Cloud Manager tenants and users who have a DLP instance.
ADI-36114 September 2024	Fixed an issue where the Strata Cloud Manager Snippet configuration page didn't load for a tenant due to un-pushed changes, which were affected by a service restart.
ADI-26131 September 2024	Fixed an issue where the Show/Hide checkbox for the Action column was not functioning properly for EDL.
ADI-37100 September 2024	Fixed an issue that caused slowness on the Push Config page due to data-related problems.
ADI-36050 September 2024	Fixed an issue where inherited interface variables from the global settings were causing errors in folders when referenced. Support has been implemented to clone routers and zones successfully.

ADI-35919 September 2024	Fixed an issue where there were inconsistencies in the HA pair display.
ADI-35445 September 2024	Fixed an issue where the HA cluster configuration displayed two clusters with the same name in the UI. Additionally, attempting to edit the HA pair resulted in a blank screen, preventing any modifications.
ADI-33775 September 2024	Fixed an issue where the Configure button for Forwarding Profiles redirected to the wrong page when Mobile Users was not enabled. Workaround: Enable Mobile Users.
ADI-34294 September 2024	Fixed an issue where the target device count on the Schedules page displayed as zero, even though the associated rule had target devices. Workaround: Clear the browser cache and reload the page. The target devices count should then display correctly.
ADI-31823 July 2024	Fixed an issue where configuring the Mobile User Infrastructure settings, if you click the Advanced Settings , the DDNS Configuration section appears in red, suggesting as a required configuration, though it is not. As a workaround, collapse and reopen the Advanced Settings section. The DDNS Configuration section won't appear as required.
ADI-34607 July 2024	Fixed an issue where PAC files larger than approximately 150 KB was failing to upload to Strata Cloud Manager, resulting in a request failed with status code 414 error.
ADI-30026 July 2024	Fixed an issue where the DHCP local pool value was displaying incorrectly. This was due to local configuration management computations not being performed on DHCP objects, which prevented conflicts from being shown.
ADI-33316 July 2024	Fixed an issue where data filtering profiles, whether custom or default, were being pruned when imported or displayed in Strata Cloud Manager.
ADI-29956 July 2024	Fixed an issue where profiles with passwords were shown as not matching, though they were.

ADI-29989 July 2024	<p>Fixed an issue with the Application UI that caused timeouts when editing a static IP pool with up to 5000 records. While the timeout issue has been fixed, there's still a delay when editing pages with a large number of records.</p>
ADI-33909 July 2024	<p>Fixed an issue where ConfigPush was failing due to Layer 3 Aggregate Ethernet group in the imported snippet.</p>
ADI-31750 June 2024	<p>Fixed an issue where the performance was impacted if the number of IP pools per project exceeded 50.</p>
ADI-30165 June 2024	<p>Fixed an issue where TACACS+ server timeout value was not shown for firewall configuration diff, even though it was configured.</p>
ADI-30721 June 2024	<p>Fixed an issue where newly onboarded firewall displayed conflicts when there were no conflicts. Also, some Strata Cloud Manager unsupported objects were shown.</p>
ADI-32068 June 2024	<p>Fixed an issue where the Mobile User > DDNS Configuration page didn't show the previously configured Dynamic DNS settings.</p> <p>As a workaround, click on a different section and then return to the Mobile User > DDNS Configuration.</p>
ADI-32094 June 2024	<p>Fixed an issue where the Dynamic DNS Support page on the Infrastructure Settings > Advanced Settings displayed a section for enabling advanced RCODE support, which is not related to the Dynamic DNS feature.</p>
ADI-32181 June 2024	<p>Fixed an issue where importing of a local configuration with an invalid master key did not throw any error message. Nodes that required encryption was disregarded which resulted in fail validation on attempt to associate snippet or push to a device.</p>
ADI-31538 June 2024	<p>Fixed an issue where, when setting up a forwarding profile, the forwarding profile Type was displayed as ZTNA Agent instead of Prisma Access Agent. Also, if you selected Add Forwarding Profile, the drop-down displayed ZTNA Agent instead of Prisma Access Agent.</p>
ADI-33611 June 2024	<p>Fixed an issue where custom certificates at the device level were moved up to All container in Strata Cloud Manager. When certificates were pushed from the Strata Cloud Manager, they were also being pushed along. If</p>

	you do not want to push certificates to other devices, it's advisable to move the certificates to the device level.
ADI-31502 June 2024	Added a validation to check agent configuration is not set to tunnel or hybrid mode when Enable Portal only for Proxy Mode on GlobalProtect is enabled under GlobalProtect setup.
ADI-23905 June 2024	Fixed an issue where unsupported Colo-Connect regions were getting displayed.
ADI-31713 June 2024	Fixed an issue where pushed configurations used in local configuration as references couldn't be imported during the Snippet import process.
ADI-32781 June 2024	Fixed an issue where the push with an incomplete HA pair was not working. To support HA devices in an Auto VPN cluster, both devices in the HA pair must be present together in the cluster. There is no validation in place for this and will fail the push.
ADI-36846	IP Optimization has the following caveats for IPv6:- If you have IP Optimization enabled, you cannot configure IPv6.- If you have IPv6 enabled, you cannot enable IP Optimization.Workaround: If you have IP Optimization enabled, make sure that you have not enabled IPv6 and, if it is enabled, disable it (Workflows > Prisma Access Setup> Prisma Access and uncheck Enable).
1. ADI-35319	Fixed an issue where the validation check was too strict, preventing changes to the BGP ASN on Colo Connect VLANs after a commit push, and displaying an incorrect error message.
ADI-32883 June 2024	Fixed an issue where the auto generated configurations such as configurations from web security and Auto VPN which caused conflicts were not marked as conflicts in the Local Configuration.
ADI-30721 June 2024	Newly onboarded firewall shows conflicts and when clicked on, there are no conflicts for them. Also, some objects that we don't support in Strata Cloud Manager are also shown.
ADI-25507 May 2024	When you enable Remote Browser Isolation (RBI) widget from the URL page, do not add any infrastructure settings, and create all RBI related configs and push, RBI configs are not present on the firewall.

ADI-25875 May 2024	When no remote networks configs are present but cden configs are present, bandwidth management does not display the per region bandwidth allocation. Instead, it is set up as day-0.
ADI-26149 May 2024	The HTTP header value field supports only 512 characters.
ADI-28737 May 2024	Remote networks explicit proxy IP addresses are not visible in Strata Cloud Manager.
ADI-28491 May 2024	The <code>load config version</code> command throws a 504 Gateway timeout error.
ADI-28737 May 2024	Remote networks explicit proxy IP addresses are not visible in Strata Cloud Manager.
ADI-30089 May 2024	ECDSA cert reverts back to default when set to None under GP folder.
ADI-30111	Compare config shows a difference between variable and actual value.
ADI-28195 April 2024	The configuration push fails if you attempt to partially push the ssl-tls-service-profile with a max version, even when the service profile doesn't have a max version defined. To resolve this issue, you must perform a full push.
ADI-25662 April 2024	Fixed an issue where you were allowed to create more than one project with the same domain and user groups if the projects were configured from different configuration snippets.
ADI-28726 April 2024	Fixed an issue where, the users who were not on the Allow List were able to authenticate.
ADI-30111 April 2024	Fixed an issue on the Compare Config page where the VLAN value differed between Configs in Cloud and Configs on Device.
ADI-30901 April 2024	Fixed an issue where, creating a dummy Kerberos server profile, along with Kerberos server was required for creating a Kerberos authentication profile.

ADI-28491 April 2024	Fixed an issue where, the load config version command was throwing a 504 Gateway timeout error.
ADI-30165 April 2024	Fixed an issue where, the TACACS+ server timeout value was not shown for firewall config diffs, even though it was configured.
ADI-30111 April 2024	Fixed an issue where, the compare configuration was showing a difference between variable and actual value.
ADI-30089 April 2024	Fixed a decryption settings issue wherein the PA level certificates need to be set to None before setting the child level certificates to None.
ADI-28737 April 2024	Fixed an issue where the Remote Networks Explicit Proxy IP addresses were not visible in Strata Cloud Manager.
ADI-25875 April 2024	Fixed an issue where the Bandwidth Management tab displayed a blank page if the MCW configuration was present under remote networks.
ADI-25723 January 2024	<p>Call /spiffy/v1/bp/result/policies/security_rule for a tenant.</p> <p>Result: id = 3 has old check_name 'The rule Description is not populated'. The response will contain the old name. Even when new BPA analysis has been completed - the check_name remains the same.</p>
ADI-25415 January 2024	Navigating to the IP allow list page in Mobile Users results in an automatic update to allow list IP addresses.
ADI-25723 January 2024	Fixed an issue where changing the configuration was necessary to generate the new BPA report.
ADI-25415 January 2024	Fixed an issue where navigating to the Mobile Users > IP Allow List page resulted in an automatic update to allow list IP addresses without saving it.
ADI-26149 January 2024	Increased the HTTP header value to support a maximum of 16K characters.
ADI-25541	Fixed an issue, where pushing any Auto VPN configuration changes resulted in all admin changes being applied to all devices within the pushed VPN cluster.

ADI-25507	Fixed an issue, wherein enabling Remote Browser Isolation (RBI) without adding any infrastructure settings and subsequently pushing the configuration changes to a remote network led to a successful push, yet the RBI configuration remained unavailable on the firewall.
ADI-25415	Fixed an issue, where the egress IP allowlist would update automatically upon navigating to Workflows > Prisma Access Setup > GlobalProtect > Prisma Access Locations page.
ADI-20135	Fixed an issue where the configured GlobalProtect IPsec Crypto profile couldn't be deleted or cloned since the Workflows > Prisma Access Setup > GlobalProtect > GlobalProtect App > Global App Settings page did not show the configured GlobalProtect IPsec Crypto profiles.
ADI-21401	Fixed an issue where the IP Restrictions weren't accurately enforced when configured with an IP address range.
ADI-23167	<p>Resolved an issue where, during a software upgrade:</p> <ul style="list-style-type: none">• Schedule object associated with completed or past schedules could not be deleted.• Grouping objects referenced by those schedule objects were also restricted from deletion, preventing the removal of grouping rules tied to past schedules <p>Previously you had to move the affected rule to the bottom of the rule order to exclude it from any firewalls. This issue has now been fixed.</p>

Command Center Known Issues

ID	Description
NETVIS-2017	<p>In the Command Center when you have a Data Security license active, clicking the DLP Inline Total Incidents value in the Incidents by Severity widget redirects you to a blank Enterprise DLP page.</p> <p>Workaround: After you get redirected to the blank Enterprise DLP page, click on DLP Incidents to load the page.</p>
NETVIS-611	<p>In the Operational Health view of the command center, when filtering by the NGFW bubble and opening the NGFW Device Health links, the data in the command center may no longer auto refresh every 5 minutes as intended.</p>
NETVIS-593	<p>In the Threats view of the command center, when filtering data with the DNS Security bubble, the malicious requests include high risk requests, not just malicious requests.</p> <p>The malicious requests count might appear larger than it actually is because of this.</p>
NETVIS-535	<p>In the Operational Health view of the command center, all apps will be classified as Internet Apps.</p> <p>ADEM will be adding support for application categorization soon.</p>
NETVIS-477	<p>In the Data Security view of the command center, the SaaS API incident count in the Security Subscriptions widget is incorrect.</p>

Getting Help

The following topics provide information on where to find more about this release and how to request support:

- [Related Documentation](#)
- [Requesting Support](#)

Related Documentation

Use the following documents to set up and implement your Prisma Access deployment:

- Use the [Strata Cloud Manager Administration guide](#) to manage your Palo Alto Networks Network Security infrastructure – your NGFWs and SASE environment – from a single, streamlined user interface.
- Use the [Prisma Access Administrator's Guide](#) to plan, install, set up, and configure Prisma Access to secure your network.
- Use the vendor-specific tasks in the [Prisma Access Integration Guide](#) to use Prisma Access to configure mobile user authentication and secure your public cloud and third-party SD-WAN deployments.
- Use the [Strata Logging Service Administration Guide](#) to learn how to activate Strata Logging Service, which you need to do before you activate Cloud Managed Prisma Access.

Visit docs.paloaltonetworks.com for more information on our products.

Requesting Support

For contacting support, for information on support programs, to manage your account or devices, or to open a support case, go to <https://support.paloaltonetworks.com>.

To provide feedback on the documentation, please write to us at: documentation@paloaltonetworks.com.

Contact Information

Corporate Headquarters:

Palo Alto Networks

3000 Tannery Way

Santa Clara, CA 95054

<https://www.paloaltonetworks.com/company/contact-support>

Palo Alto Networks, Inc.

www.paloaltonetworks.com

© 2023 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at <https://www.paloaltonetworks.com/company/trademarks.html>. All other marks mentioned herein may be trademarks of their respective companies.

